Sinusoida Vol. XXII No. 2, April 2020
ISSN 1411 - 4593

# IMPLEMENTASI SECURE SOCKET LAYER PADA VIRTUAL PRIVATE NETWORK UNTUK PENGAMANAN KOMUNIKASI VIDEO CONFERENCE

**Gesang Purwoko dan Irmayani**
Prodi Teknik Elektro, FTI-ISTN, Jakarta
gesngpurwoko16@gmail.com dan ir.irmayani@istn.ac.id

**Abstrak :** Dalam penelitian ini dilakukan scenario test pengamanan video *conference* menggunakan VPN SSL. Video conference dilakukan antara Kantor Pusat Kementerian Luar Negeri di Jakarta dengan Kantor Perwakilan RI di Canberra, Davao City dan Kopenhagen dan kemudian dilakukan analisa terhadap faktor keamanan maupun *Quality of Service* (QoS). Hasil pengujian untuk faktor keamanan menunjukkan bahwa video *conference* yang dilakukan dengan pengamanan VPN SSL tidak dapat dilihat informasi protocol seperti IP address, user ID, RTP dan SIP karena semua data telah dienkripsi dan dikapsulisasi. Selain itu hasil pengujian untuk *quality of service* menunjukkan bahwa hasil pengukuran parameter *throughput*, *delay*, *jitter* dan *packet loss* masih memenuhi persyaratan rekomendasi ITU dan menunjukkan tingkat performansi yang baik.

**Kata Kunci** Video *Conference*, VPN SSL, Keamanan, *Quality of Service*

***Abstract :*** *In this research, a video conference security test scenario using SSL VPN is conducted. Video conferencing was conducted between the Ministry of Foreign Affairs Headquarters in Jakarta and the Indonesian Representative Office in Canberra, Davao City and Copenhagen and then an analysis of security factors as well as Quality of Service (QoS) was carried out. The test results for the analysis show that video conferencing conducted with SSL VPN security cannot be used to find out protocols such as IP address, user ID, RTP current and SIP Flow because all data has been encrypted and encapsulated. In addition, the test results for service quality show that the results of throughput, delay, jitter and packet loss parameters are still needed.*

***Keywords :*** *Video Conference, SSL VPN, Security, Quality of Service*

## 1. Pendahuluan

Untuk berkomunikasi antara kantor pusat dengan kantor-kantor perwakilan yang letaknya saling berjauhan hingga ke belahan dunia yang berbeda dapat menggunakan jaringan umum (*public network*). Sistem komunikasi Video *Conference* melalui jalur internet menjadi suatu kebutuhan layanan yang sering digunakan untuk keperluan koordinasi, penyampaian laporan dan diskusi antar satuan kerja. Untuk memenuhi kebutuhan terhadap keamanan dalam komunikasi data pada jaringan umum (*public network*) salah satu solusi yang dapat digunakan adalah pemanfaatan *tunnel Virtual Private Network* (VPN). Dengan sistem SSL (Secure Socket Layer) dalam penggunaan Video *Conference* pada jalur VPN diharapkan dapat meningkatkan keamanan layanan komunikasi antara kantor Pusat dengan semua kantor perwakilan yang saling berjauhan.

Pengujian proeses Video *Conference* dilakukan antara Kantor Pusat Kementerian Luar Negeri RI dengan Kantor Perwakilan RI di Canberra, Davao City dan Kopenhagen.

## 2. Dasar Teori

### *2.1 Video Conference*

*Video conference* adalah koneksi video secara langsung antara orang-orang yang berada pada tempat yang berbeda-beda yang bertujuan untuk komunikasi dan interaksi [1]. Perkembangan video *conference* yang pesat hingga menggantikan layanan telepon standar karena selain dapat dilakukan melalui PC saat ini juga bisa dilakukan dengan perangkat *mobile*/*Smartphone*.

Polycom merupakan sistem *teleconference* baik audio maupun video. Pada Polycom menyediakan Polycom RealPresence desktop dimana sistem menggunakan video HD, komunikasi suara, sharing data pada semua level dari organisasi dengan mudah dan cepat, dimanapun berada, di kantor / rumah / dalam perjalanan. Isi komunikasi dapat berupa rapat,

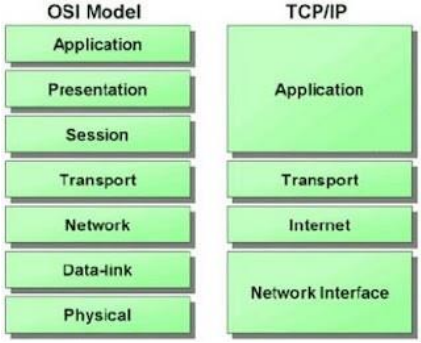
Sinusoida Vol. XXII No. 2, April 2020
ISSN 1411 - 4593

training, memberikan arahan pada kegiatan, dll.

### 2.2 Transmission Control Protocol/Internet Protocol (TCP/IP)

TCP/IP merupakan protokol yang mengatur komunikasi data antar komputer pada jaringan internet sehingga untuk berkomunikasi tidak bergantung pada jenis dan sistem operasi computer [5].

Pada dasarnya model referensi TCP/IP merupakan versi pemadatan model OSI (Gambar 2.1). Model TCP/IP terdiri dari empat lapisan yaitu *application layer, transport layer, internet layer dan network access layer*.




Gambar 2.1 Perbandingan Layer OSI Model dan TCP/IP

IP merupakan protokol pada network layer bersifat *connection-less* dan *unreliable* yang digunakan oleh *protocol* TCP/IP untuk melakukan pengalamatan dan routing data antar host pada jaringan berbasis TCP/IP. IP melihat alamat dari tipe paket lalu dengan menggunakan routing table menentukan tujuan paket tersebut melalui jalur terbaik. IP menerima segmen dari *transport layer*, difragmentasikan menjadi datagram yang dilengkapi dengan alamat IP dari pengirim dan penerima jika diperlukan, lalu menata kembali datagram tersebut menjadi segmen pada sisi penerima.

Data *transport layer* dipecah menjadi datagram-datagram yang dapat dibawa oleh IP. Tiap datagram dilepas dalam jaringan komputer dan akan mencari rute ke komputer tujuan sendiri secara otomatis. Pada *header internet protocol* selain IP address dari komputer penerima dan komputer pengirim juga terdapat informasi yang mencakup jenis dari *protocol transport layer* (TCP atau UDP) dan *Time-To-Live* (TTL) yang menentukan berapa lama IP dapat berada di dalam jaringan. Nilai TTL akan dikurangi satu jika IP melewati sebuah komputer. Jika IP tidak berhasil menemukan alamat tujuan, maka dengan adanya TTL IP akan mati dengan sendirinya pada saat TTL bernilai nol.

TCP berada pada transport layer yang bersifat connection oriented dan reliable. Pada sisi pengirim, TCP memecah aliran byte data menjadi pesan diskrit dan meneruskannya ke internet layer. Pada sisi penerima, TCP merakit kembali pesan diskrit tersebut menjadi aliran output. Selain itu, TCP juga mengandalikan aliran untuk memastikan bahwa pengirim yang cepat tidak akan membanjiri penerima yang lambat dengan pesan-pesan.

Pertukaran data terjadi melalui proses sinkronisasi dimana pada proses ini dibentuk virtual connection. Pada proses 3-way handshakes, memeriksa apakah kedua sisi siap untuk melakukan transmisi data dan dapat mengijinkan device untuk menentukan sequence number. Untuk membentuk koneksi TCP, komputer pengirim harus menggunakan nomor port tertentu dari layanan yang ada di server, misalnya port 32 untuk layanan FTP atau port 25 untuk layanan SMTP.

### *2.3 Virtual Private Network (VPN)*

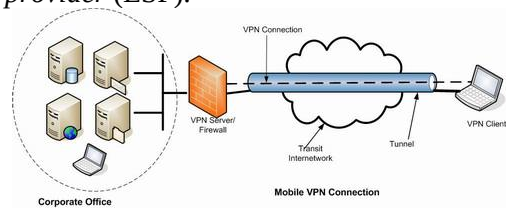
VPN merupakan suatu jaringan *private* yang mempergunakan sarana jaringan komunikasi publik (dalam hal ini Internet) dengan memakai *tunnelling protocol* dan prosedur pengamanan. Data yang dikirimkan melalui VPN terenkripsi sehingga cukup aman dan rahasianya tetap terjaga, meskipun dikirimkannya melalui jaringan internet.

Teknologi yang digunakan dalam VPN merupakan perpaduan dari teknologi *tunneling* dengan teknologi enkripsi.

Didalam implementasinya VPN dibagi menjadi dua jenis yaitu *remote access* VPN dan *site-to-site* VPN:

1. ***Remote Access* VPN**

   Jenis VPN ini digunakan oleh *user* yang ingin terhubung ke jaringan khusus internal dari berbagai lokasi yang jauh (*remote*). Biasanya perusahaan yang ingin membuat jaringan VPN tipe ini akan bekerjasama dengan *enterprise service provider* (ESP).



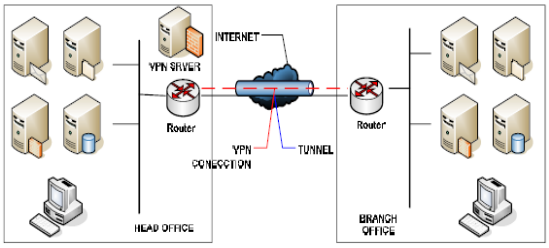

Gambar 2.2 *Remote Access* VPN

Sinusoida Vol. XXII No. 2, April 2020
ISSN 1411 - 4593

Perusahaan yang memiliki pegawai yang ada di lapangan dalam jumlah besar umumnya menggunakan *remote access* VPN untuk membangun WAN. VPN tipe ini akan memberikan keamanan, dengan mengenkripsi koneksi antara jaringan lokal perusahaan dengan pegawainya yang ada di lapangan.

2. ***Site-to-site* VPN**

*Site-to-site* VPN jenis ini menghubungkan antara dua tempat yang letaknya berjauhan, seperti halnya kantor pusat dengan kantor cabang atau suatu perusahaan dengan perusahaan mitra kerjanya. Pada Gambar 2.3 VPN yang digunakan untuk menghubungkan kantor pusat dengan kantor cabang, implementasi ini termasuk jenis intranet *site-to-site* VPN. VPN beroperasi pada topologi yang berbeda dan lebih rumit dari jaringan point to point. Hal ini memungkinkan remote komputer bertindak seolah-olah berada di jaringan LAN.




**Gambar 2.3 *Site-to-site* VPN**

Data yang dikirimkan melalui VPN terenkripsi sehingga cukup aman dan rahasianya tetap terjaga, meskipun dikirimkan melalui jaringan internet.

VPN mendukung banyak protokol jaringan seperti PPTP, L2TP, IPSec dan SOCKS. Protokol ini membantu cara kerja VPN untuk memproses otentikasi. VPN klien dapat membuat sambungan dan mengidentifikasi orang-orang yang diberi wewenang di jaringan. Beberapa solusi yang ditawarkan oleh VPN adalah memberikan konektivitas jarak jauh, *file sharing*, konferensi video dan layanan lain yang berhubungan dengan jaringan. Berbagai fitur yang sudah ditawarkan melalui layanan internet dapat ditawarkan melalui VPN karena dapat bekerja pada jaringan pribadi dan publik, intinya VPN adalah jaringan privat fleksible.

### 2.4 *Secure Socket Layer* (SSL)

*Secure Socket Layer* (SSL) merupakan protokol kriprografi yang umum digunakan untuk mengelola keamanan komunikasi transmisi pesan di internet yang merupakan protokol berlapis. Dalam tiap lapisannya, sebuah data terdiri dari panjang, deskripsi dan isi. SSL mengambil data untuk dikirimkan, dipecahkan ke dalam blok-blok yang teratur, kemudian dikompres jika perlu, menerapkan MAC (*Message Authentication Code)*, dienkripsi dan hasilnya dikirimkan. Di tempat tujuan, data didekripsi, verifikasi, dekompres dan disusun kembali.

Fungsi SSL pada komunikasi aman sama seperti fungsi TCP pada komunikasi normal yaitu menyediakan sebuah infrastruktur komunikasi standar dimana sebuah aplikasi dapat menggunakannya dengan mudah dan hampir tidak dapat terlihat (invisible).

### *2.5* Parameter *Quality of Service* (QoS)

*Quality of Service* (QoS) adalah kemampuan suatu jaringan untuk menyediakan layanan yang baik dengan menyediakan bandwith, mengatasi jitter dan delay. Parameter QoS adalah *latency*, *jitter*, *packet loss*, *throughput*, MOS, *echo cancellation* dan PDD. QoS sangat ditentukan oleh kualitas jaringan yang digunakan. Terdapat beberapa factor yang dapat menurunkan nilai QoS, seperti : Redaman, Distorsi, dan Noise.

## 3. Metode VPN SSL untuk Pengamanan Data

### 3.1 Metode VPN SSL

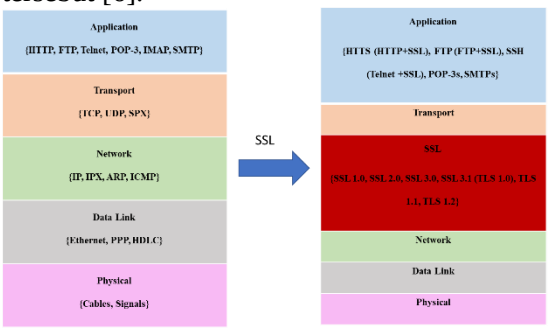
SSL awalnya dibuat untuk mengamankan lalu lintas web, namun pada saat ini digunakan juga untuk mengamankan protokol aplikasi non-web (seperti SMTP, LDAP, POP, IMAP, dan TELNET). SSL menyediakan sertifikat digital berbasis otentikasi klien dan server, pengecekan integritas, dan kerahasiaan. SSL memberikan kerahasiaan pada layer transportasi melalui kriptografi kunci rahasia, manajemen kunci dan otentikasi melalui kriptografi kunci publik [8].

Secara umum layer komunikasi antara client dan server dapat digambarkan pada Gambar 3.1. Tabel sebelah kiri memperlihatkan komunikasi yang dilakukan menggunakan jalur terbuka (tanpa SSL) dibagi menjadi 5 layer yakni *application*, *transport*, *network*, *data link* dan *physical*.

Sinusoida Vol. XXII No. 2, April 2020
ISSN 1411 - 4593

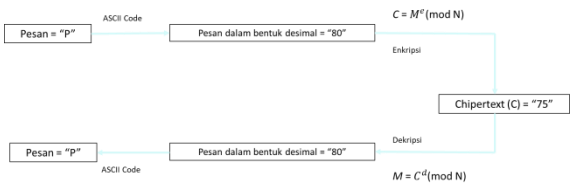
Layer tersebut akan mengalami penambahan 1 layer ketika SSL digunakan seperti diperlihatkan pada Gambar 3.1 tabel sebelah kanan. Dimana semua *traffic* antara SSL server dan SSL client dienkripsi menggunakan *shared key* dan algoritma enkripsi yang telah dinegosiasikan. Hal ini beroperasi selama proses SSL *Handshake*, yang muncul pada sesi awal (*initialization*) [3].

VPN dengan SSL menggunakan salah satu teknologi enkripsi yaitu *asymmetric encryption*. Pada algoritma asymmetric terdapat dua buah kunci, yaitu kunci publik (*public key*) untuk enkripsi dan kunci private (*private key*) untuk dekripsi. Ketika seseorang A akan mengirimkan pesan ke B, maka A akan mengenkripsi pesan tersebut menggunakan kunci publik B dan B akan membuka pesan yang diterimanya menggunakan kunci private. Kelebihan pada sistem *asymmetric* karena user cukup menyimpan secara rahasia kunci private miliknya, sedangkan kunci publik dapat disebarkan ke seluruh user yang ingin berkomunikasi dengannya tanpa khawatir orang yang tidak berhak dapat membuka pesan menggunakan kunci publik yang telah disebar tersebut [6].



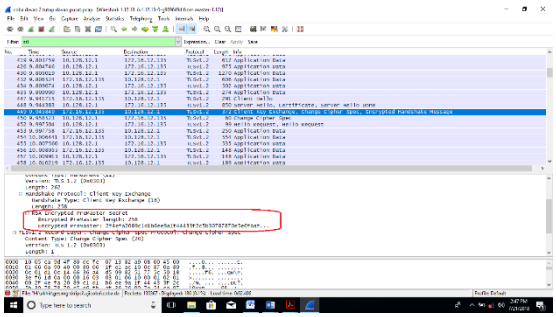

Gambar 3.1 Layer Komunikasi Sebelum dan Setelah Menggunakan SSL

*Asymmetric* enkripsi ini terjadi pada proses awal SSL yakni proses pembentukan sub-protokol SSL *Handshaking* (gambar 3.2).




Gambar 3.2 Alur *Assymetric Encryption* pada subprotokol SSL Handshake

Pada Gambar 3.3 dapat dilihat bahwa public key *(encrypted premaster key)* dari algoritma enkripsi yang digunakan memiliki panjang 256 bit. Artinya untuk mendapatkan *private key* dari *public key* sepanjang 256 bit tersebut, akan sangat sulit. Hal ini dikarenakan sulitnya mendapatkan dua bilangan prima p dan q yang jika dikalikan menghasilkan bilangan sepanjang 256 bit tersebut (pxq = N). Hal ini menunjukkan bahwa tidak mudah untuk mendekripsi pesan yang dikirimkan jika user tidak memiliki *private key* dan membutuhkan waktu yang cukup lama.



Gambar 3.3 Penggunaan algoritma RSA

SSL disusun oleh dua sub-protokol yaitu [7]:

1. SSL Handshaking

SSL Handshaking adalah sub-protokol untuk membangun koneksi yang aman untuk berkomunikasi. Sub-protokol handshaking diperlihatkan pada Gambar 3.4. SSL dimulai dengan pengiriman pesan Hello dari Client ke Server (1). Server merespon dengan mengirim pesan Hello (2) dan sertifikat digital ke client untuk otentikasi (3).

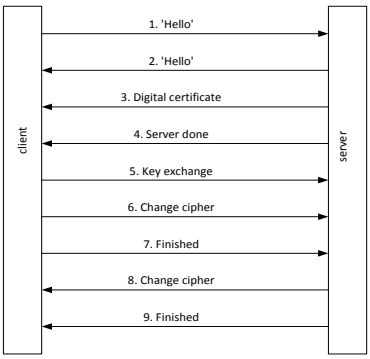
Sertifikat digital berisi kunci *public server*. Di dalam browser *client* terdapat daftar CA yang dipercaya. Jika sertifikat digital ditandatangani oleh salah satu CA di dalam daftar tersebut, maka *client* dapat memverifikasi kunci public *server*. Setelah proses otentikasi selesai, server mengirimkan pesan *server done* (4) kepada *client*. Selanjutnya *server* dan *client* menyepakati *session key* untuk melanjutkan transaksi melalui proses yang disebut key change (5).

*Session key* adalah kunci rahasia yang digunakan selama transaksi. Komunikasi *client-server* dilakukan dengan menggunakan *session key* ini. Data yang akan ditransmisikan dienkripsi terlebih dahulu dengan *session key* melalui protocol TCP/IP. Proses *exchange key* diawali dengan *client* mengirim nilai acak yang disebut *premaster-key* pada *server*.

Nilai acak ini dikirim dalam bentuk terenkripsi. Melalui perhitungan yang cukup kompleks,

Sinusoida Vol. XXII No. 2, April 2020
ISSN 1411 - 4593

*client* dan *server* menghitung *session key* yang diturunkan dari *premaster key*. Setelah pertukaran kunci, *client* dan *server* menyepakati algoritma enkripsi (6). *Client* mengirim pesan bahwa ia sudah selesai membangun sub-protocol (7).
Server merespon *client* dengan mengirim pesan 8 dan 9. Sampai di sini, proses pembentukan kanal yang aman sudah selesai.

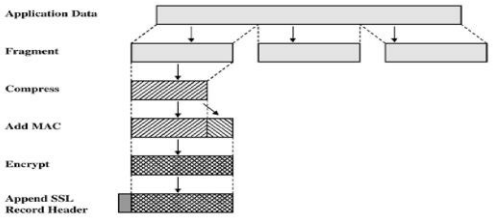



Gambar 3.4 Sub-protokol *handshaking* untuk membangun koneksi yang aman [7]

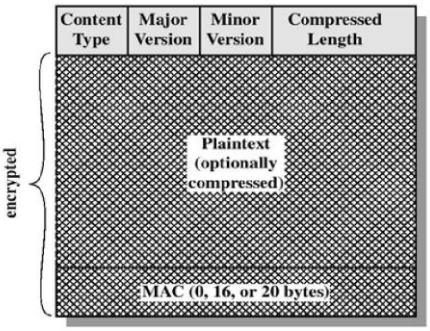
2. SSL Record

Setelah kanal yang sudah aman dibentuk, *client* dan *server* menggunakannya untuk menjalankan sub protokol kedua (SSL *record*) untuk saling berkirim pesan. Pesan dari *client* ke *server* (dan sebaliknya) dikirim dalam bentuk terenkripsi (pesan dienkripsi dengan *session key*). Tetapi sebelum pesan dikirim dengan TCP/IP, protocol SSL melakukan proses pembungkusan data sebagai berikut.
Pertama, pesan dipecah menjadi sejumlah blok. Setiap blok diberi nomor urut sekuensial. Setiap blok kemudian dikompresi. kompresi tersebut menggunakan *lossless compression* dan tidak boleh menambah panjang konten melebihi 1024 bytes. Selanjutnya hasil kompresi disambung dengan *session key*. Key atau kunci tersebut kemudian di-hash dengan algoritma MD5 (atau algoritma hash lain yang disepakati). Nilai hash ini ditambahan ke setiap blok sebagai MAC (*Message Authentication Code*). Jadi, MAC dihitung sebagai berikut: MAC = Hash (*session key, compressed data block*).
Hasilnya kemudian dienkripsi dengan algoritma kriptografi simetri (misalnya RC4).

Selanjutnya pesan yang telah diubah tersebut dienkripsi (misalkan dengan di-hash) baru kemudian dikirimkan. Ketika tambahan tersebut di-hash maka itulah MAC. Diharapkan sulit bagi orang lain yang tidak dikehendaki untuk mengubah *chipertext*. Karena penerima yang dikehendaki akan mencocokan MAC yang diterima dengan yang telah diketahui bersama antara pengirim dan penerima yang dikehendaki. Apabila nilai MAC tidak cocok maka *chipertext* yang diterimapun dapat disimpulkan berbeda dengan *chipertext* yang dikirimkan. Sehingga diharapkan dengan ditambahkannya MAC, *plaintext* yang diterima merupakan *plaintext* yang sama yang dikirimkan oleh pengirim pesan.
Langkah terakhir dari SSL Record adalah penambahan header (2 atau 3 byte), baru kemudian dikirim melalui koneksi TCP/IP aman yang terbentuk sebelumnya. Proses pembungkusan pesan oleh sub protocol SSL record diperlihatkan pada Gambar 3.5 dan Format SSL *record* ditunjukkan pada Gambar 3.6.

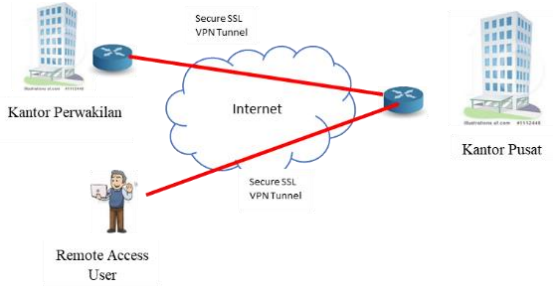



Gambar 3.5 Pembungkusan Pesan oleh SSL *Record*




Gambar 3.6 Format Data SSL *Record*
Cara kerja VPN-SSL [8]

VPN server pada VPN SSL bertugas membentuk tunnel, melakukan *validitas certificate*, dan sebagai *gateaway* antar VPN Client [6].



Sinusoida Vol. XXII No. 2, April 2020
ISSN 1411 - 4593

Gambar 3.7 *Secure SSL VPN Access Model*

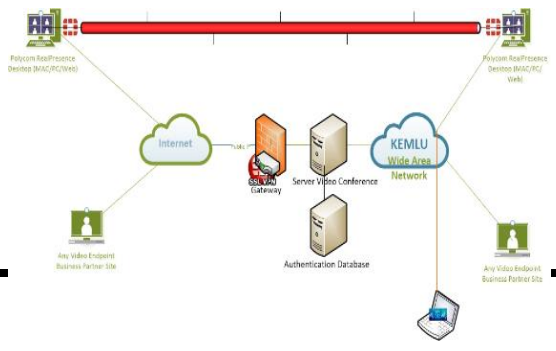
Gambar 3.7 merupakan konfigurasi jaringan video *conference* dengan menggunakan VPN SSL yang dilakukan antara Kantor Pusat dengan Kantor Perwakilan, antar Kantor Perwakilan dan Kantor Pusat dengan *Remote Access User*.

Pada penelitian ini dilakukan implementasi VPN SSL pada video conference yang dilakukan antara Kantor Pusat Kementerian Luar Negeri dengan Kantor Perwakilan (dua user/*client*). Uji analisis keamanan dan *Quality of Service* dilakukan dengan menganalisis paket data (berupa audio visual) yang mengalir di jaringan VPN yang berbasis SSL. VPN yang berbasis SSL akan melakukan enkripsi terhadap kunci dan proses transfer data dari server menuju client maupun sebaliknya.

Dalam melakukan sambungan video *conference* pada jalur VPN SSL menggunakan menggunakan Forticlient untuk dapat masuk jalur VPN SSL. Sedangkan Polycom digunakan sebagai multipoint control unit agar antar client dapat melakukan komunikasi konferensi video.

Gambar 3.8 diilustrasikan arsitektur jaringan VPN SSL dengan digunakan Fortinet, Polycom, dan Wireshark. Untuk aplikasi *sniffer*, Wireshark digunakan sebagai alat yang berfungsi untuk menangkap paket-paket data yang dikirimkan sehingga dapat digunakan sebagai pengujian parameter-parameter keamanan.

Pada saat komputer atau PC sudah terhubung dengan VPN maka jalur VPN antar dua cabang dikunci dengan kunci khusus, dan hanya komputer yang memiliki kunci ini yang dapat membuka dan tampak di data pengirim, alamat IP pada komputer *client* akan berubah dan mendapatkan IP baru yang diberikan oleh *server* VPN. Jalur *tunnel* VPN yang terbentuk tersebut mengamankan data video *conference* yang dilakukan.




Gambar 3.8 Ilustrasi Arsitektur Jaringan VPN SSL

Pada saat komputer atau PC sudah terhubung dengan VPN maka jalur VPN antar dua cabang dikunci dengan kunci khusus, dan hanya komputer yang memiliki kunci ini yang dapat membuka dan tampak di data pengirim, alamat IP pada komputer *client* akan berubah dan mendapatkan IP baru yang diberikan oleh *server* VPN. Jalur *tunnel* VPN yang terbentuk tersebut mengamankan data video *conference* yang dilakukan.

Untuk analisis data pada implementasi VPN SSL dengan Video *Conference* akan dilakukan dengan dua konfigurasi:

1. *Untrusted network* (jaringan terbuka).
2. *Trusted network* (jaringan tertutup) dengan menggunakan VPN SSL.

Kebutuhan Perangkat Lunak yaitu Polycom, Fortinet, dan Wireshark pada penelitian ini digunakan untuk melihat SIP dan RTP pada video *conference.*

Session Initiation Protocol (SIP) merupakan *Session*, meliputi panggilan telepon internet, distribusi multimedia dan multimedia conference, protokol yang digunakan untuk inisiasi, modifikasi dan terminasi sesi komunikasi VoIP. SIP digunakan untuk set-up video dan audio *conference* atau kirim pesan singkat.

Real-time Transport Protocol (RTP), didefinisikan sebagai standarisasi paket untuk mengirimkan audio dan video pada jaringan Internet yang menyediakan fungsi-fungsi *end-to-end network transport* yang sesuai untuk aplikasi-aplikasi transmisi data real-time seperti audio, video atau simulasi data, melalui *multicast* atau *unicast network services*.

## 4. Pengujian dan Analisis

### 4.1 Pengujian Keamanan Sistem VPN SSL

1. Pengujian keamanan sistem VPN SSL.
   Pertama akan dilakukan pengujian pada aspek keamanan dari VPN SSL. Pengujian ini dilakukan pada dua konfigurasi jaringan:
   1. Jaringan terbuka
   2. Jaringan tertutup (dengan VPN SSL)
2. Pengujian *Quality of Service* video *conference* pada VPN SSL

Sinusoida Vol. XXII No. 2, April 2020
ISSN 1411 - 4593

Setelah dilakukan pengujian terhadap aspek keamanan VPN SSL, selanjutnya dilakukan pengujian Quality of Service terhadap jaringan tertutup yang menggunakan VPN SSL. Pengujian ini dilakukan dengan melakukan pengukuran pada parameter-parameter *troughput*, *delay*, *jitter* dan *packet loss*.

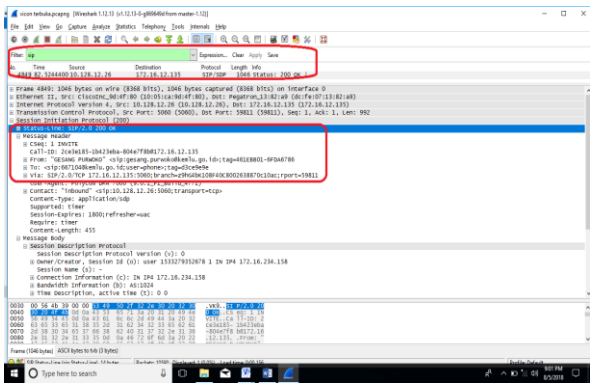
Dalam pengujian tersebut di atas, akan menggunakan aplikasi Wireshark sebagai *sniffing tool*.

### 4.1.1 Jaringan Terbuka

Gambar 4.1 menunjukkan pihak ketiga menggunakan peralatan dan pengalaman *sniffing* untuk memonitor jaringan. Pihak ketiga dapat memonitor internet dan *copy packets* ke komputer/jaringannya. Hasil sniffing pada jaringan ketika dilakukan filter SIP dapat dilihat pada Gambar 4.2.

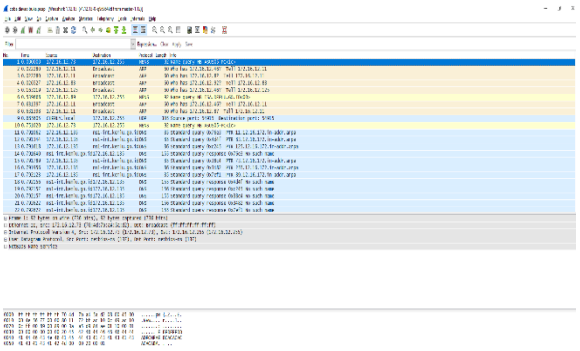

Gambar 4.1 Ilustrasi pihak ketiga(laptop) yang melakukan *Sniffing*

Dari gambar 4.1, dapat dilihat informasi SIP antara lain IP pengirim dan penerima serta informasi mengenai paket data yang sedang berlangsung. Pada percobaan ini dilakukan video *conference* masing-masing dua client antara Kantor Pusat Kemenlu dengan Kantor Perwakilan di Canberra, Davao City dan Kopenhagen menggunakan aplikasi Polycom dengan waktu yang berbeda.



Gambar 4.2. Tampilan hasil sniffing

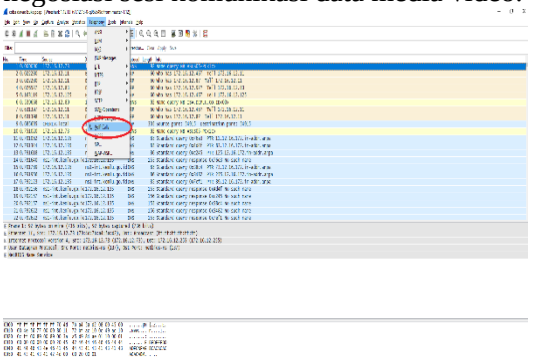
Sebagai contah tampilan aplikasi Wireshark dari percobaan video conference antara Kantor Pusat Kementerian Luar Negeri dengan kantor Perwakilan Davao City dapat dilihat pada gambar 4.3.



Gambar 4.3 Tampilan Wireshark Video Conference dengan Perwakilan Davao City

Untuk analisa protokol SIP Flows pada Tab ‘Telephony’ dan kemudian dipilih ‘SIP Flows’ atau ‘VOIP calls’ seperti pada gambar 4.4 dengan tanda lingkaran merah.

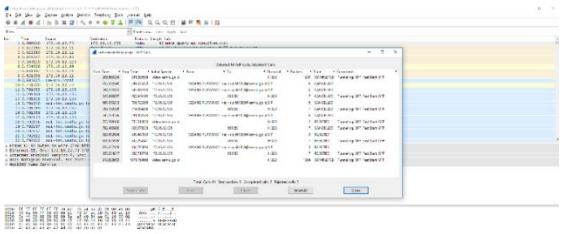
SIP ini adalah protokol yang digunakan untuk inisiasi, modifikasi dan terminasi sesi komunikasi VoIP dan digunakan untuk negosiasi sesi komunikasi data media video.



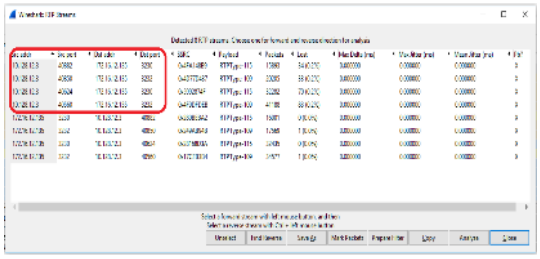
Gambar 4.4 Tampilan Wireshark Video *Conference* untuk menampilkan SIP

Pada tampilan SIP Flows jaringan terbuka, dapat dilihat IP user/client dan Username atau ID yang sedang melakukan video conference seperti terlihat pada. Gambar 4.5. pada Wireshark tertangkap bahwa IP 172.16.12.135 dari komputer dan user, terlihat yang sedang melakukan sesi komunikasi.

Sinusoida Vol. XXII No. 2, April 2020
ISSN 1411 - 4593

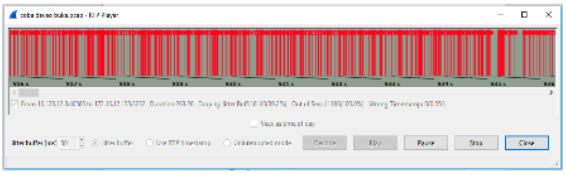


Gambar 4.5 Tampilan Wireshark untuk SIP Flows



Gambar 4.6 Tampilan Wireshark Detail RTP Stream

Pada Gambar 4.6, bagian tanda merah memperlihatkan bahwa client melakukan proses login dan dapat diketahui informasi alamat IP komputer serta port yang sedang melakukan komunikasi. Ini dikarenakan jaringan yang tidak dilalui VPN SSL tidak terenkripsi. Pada RTP Streams tersebut masih dapat dianalisa paket yang sedang dikirimkan ditunjukkan pada gambar 4.7.



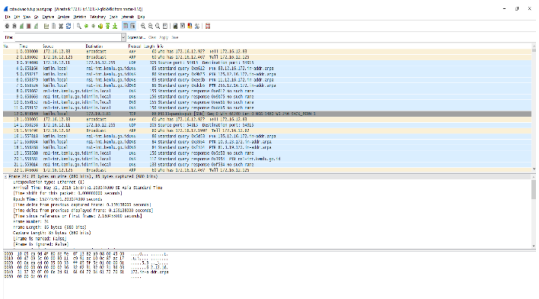
Gambar 4.7 Tampilan Kiriman Paket

Pada Gambar 4.7 terlihat bahwa pihak ketiga, dalam hal ini digunakan wireshark, dapat memonitor komunikasi video conference tersebut dan *packet* bisa didapatkan. Pihak lain yang tidak berkepentingan tersebut dapat menganalisa dan kemudian mengektsrak data yang dikirimkan. Dengan demikian video *conference* yang dilakukan menjadi tidak aman.

### 4.1.2 Jaringan Tertutup (Menggunakan VPN SSL)

Untuk analisa pada jaringan tertutup dengan menjalankan aplikasi VPN SSL, aplikasi video *conference* Polycom, dan aplikasi Wireshark pada laptop/PC. Berikut ini disajikan gambar tampilan wireshark tahap demi tahap proses VPN SSL selama komunikasi video conference dengan perwakilan Davao City.

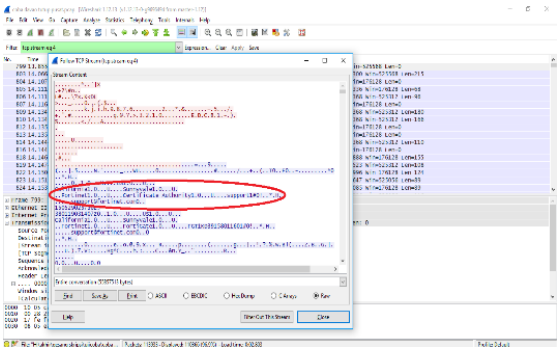
Pada jaringan tertutup proses analisa keamanan sama seperti pada jaringan terbuka yaitu dengan menganalisa protokol yang sedang berjalan yaitu SIP dan RTP.



Gambar 4.8 Tampilan wireshark Percobaan Video *Conference* dengan VPN SSL

Pada jaringan tertutup ini juga dianalisa proses pembentukan SSL handshake yang terjadi pada saat sesi komunikasi terbentuk antara *client* dan *server*.

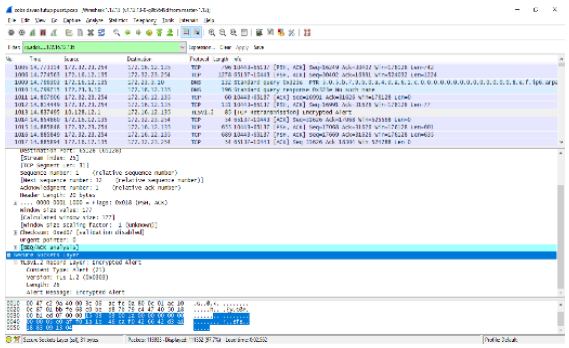
Pada Gambar 4.9 menunjukkan dari hasil analisa wireshark dipilih '*follow TCP stream*' bahwa komputer yang digunakan untuk video *conference* berada pada jaringan VPN SSL Fortinet.



Gambar 4.9 Tampilan Wireshark dengan Fortinet VPN SSL

Pada Gambar 4.10 menunjukkan hasil analisa wireshark, PC yang digunakan untuk video conference IP 172.16.12.135 pada bagian *Secure Socket Layer* dilakukan proses SSL *Handshake* untuk menjalankan aplikasi Polycom.

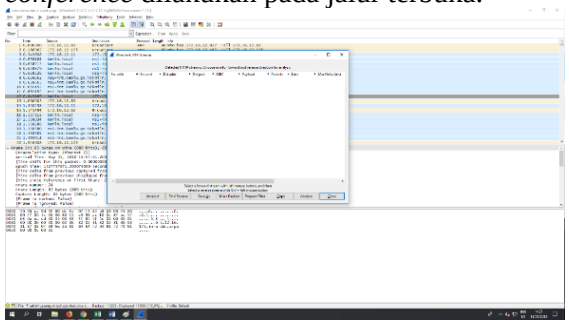
Sinusoida Vol. XXII No. 2, April 2020
ISSN 1411 - 4593



Gambar 4.10 Tampilan Wireshark pada SSL setelah Enkripsi

**RTP pada jaringan tertutup**

Seperti halnya pada konfigurasi jaringan terbuka untuk melihat protokol RTP, klik tab Telephony dan pilih RTP kemudian pilih RTP All Streams. Ketika jaringan menggunakan VPN, pada tampilan RTP Streams berbeda dengan pada saat komunikasi dilakukan pada jaringan terbuka, pada bagian ini tidak terlihat IP user/*client* dan User ID yang sedang melakukan video *conference*. Pada gambar 4.11 merupakan tampilan dari hasil RTP Streams dimana pada saat dilakukan analisis RTP tidak dapat dilihat alamat komputer IP yang sedang melakukan video *conference* ini berbeda dengan pada saat komunuikasi video *conference* dilakukan pada jalur terbuka.

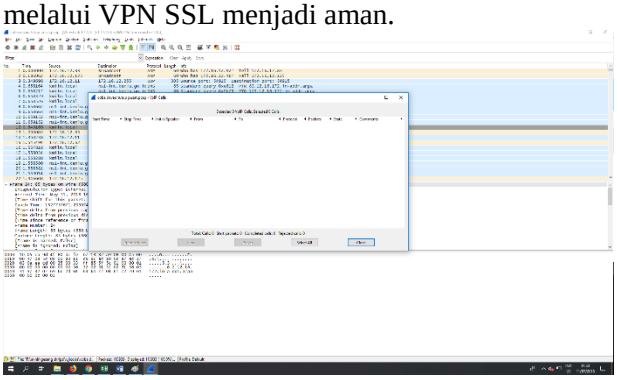


Gambar 4.11 Tampilan Wireshark VPN SSL RTP *Streams*

**SIP *Flows* pada jaringan tertutup.**

Kemudian untuk melihat protokol SIP seperti hanya pada konfigurasi jaringan terbuka, klik tab Telephony dan pilih SIP Flows.

Ketika telah terbentuk VPN, pada tampilan SIP Flows juga tidak terlihat alamat IP user/client dan User ID yang sedang melakukan video conference. Di sinilah aspek *confidentiality* dari VPN. Hal ini dapat dilihat pada Gambar 4.5 SIP Flows. Pada Gambar 4.12 karena semua data telah dienkripsi dan dikapsulisasi sehingga tidak ada informasi user ID dan IP Address yang terlihat dan jaringan yang melalui VPN SSL menjadi aman.



Gambar 4.12 Tampilan wireshark SIP Flows saat komunikasi VPN SSL

Data pengujian pada jaringan tanpa VPN SSL dan jaringan dengan VPN SSL pada tabel 4.1.

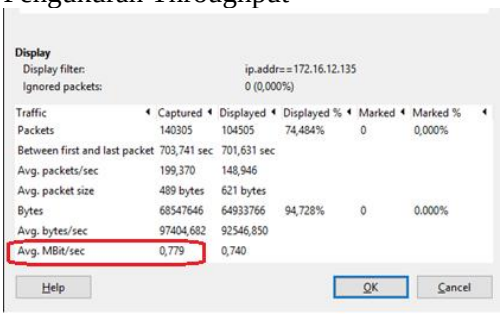
Tabel 4.1 Data Pengujian VPN SSL

| Parameter | Tanpa VPN SSL | Dengan VPN SSL |
|---|---|---|
| User ID dan IP Address | Terlihat | Tidak Terlihat |
| RTP Streams | Terlihat | Tidak Terlihat |
| SIP Flows | Terlihat | Tidak Terlihat |

**4.2 Pengujian *Quality of Service***

Pada proses analisis ini akan dilakukan pengujian/pengukuran parameter-parameter Qos yaitu: *troughput*, *delay*, *jitter* dan *packet loss* dalam hubungan komunikasi video conference (audio dan visual).

1. Pengukuran Throughput



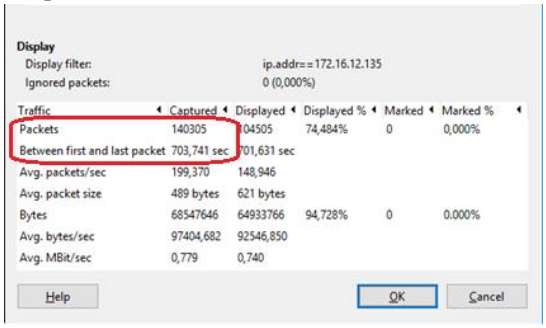

Gambar 4.13 Hasil Pengukuran Throughput Vicon1 ke perwakilan Canberra

Untuk mendapatkan nilai throughput, dapat digunakan hasil dari parameter yang telah ditangkap oleh Wireshark seperti pada data Vicon1 ke perwakilan Canberra pada Gambar 4.13. Dari data tersebut di atas, didapatkan nilai throughput pada Vicon1 ke perwakilan Canberra sebesar 0,779 Mbit/sec.

2. Pengukuran Delay

Sinusoida Vol. XXII No. 2, April 2020
ISSN 1411 - 4593

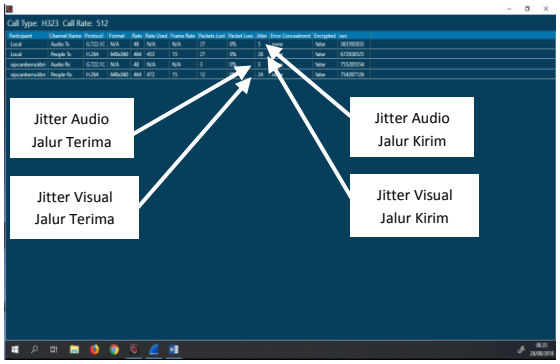
Untuk pengukuran delay, pada penelitian ini dilakukan dengan menggunakan aplikasi wireshark.




Gambar 4.14 Hasil Pengukuran Delay Vicon1 ke Perwakilan Canberra

Gambar 4.14 untuk menghitung delay dapat dilakukan dengan membagi selisih waktu pengiriman paket pertama dan terakhir.
Delay Vicon1 Canberra = 5,015 ms.
Dari hasil pengukuran tersebut berada pada kategori delay sangat bagus, bagus, jelek atau sangat jelek, dibandingkan dengan standard ITU-T (*International Telecommunication Union*).

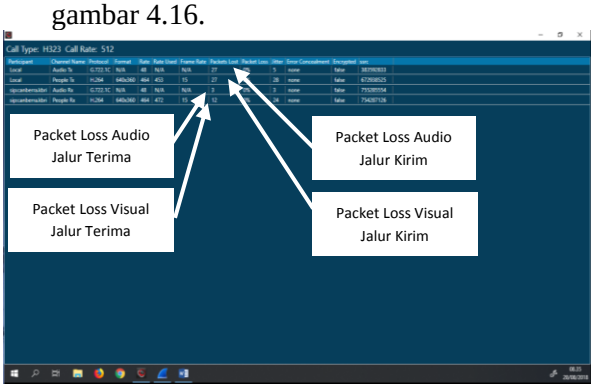
3. Pengukuran Jitter
   *Jitter* adalah variasi waktu kedatangan paket. *Jitter* diukur antara paket sekarang dengan paket yang datang sebelumnya.
   Pada Gambar 4.15 dapat dilihat hasil pengukuran jitter pada Polycom untuk data vicon1 ke Perwakilan Canberra. Pada kolom jitter dapat dilihat nilai jitter audio menunjukkan angka 5 ms pada jalur kirim dan 3 ms pada jalur terima sehingga nilai jitter audio vicon1 ke Perwakilan Canberra tersebut adalah rata-rata dari kedua nilai jitter tersebut, yaitu: (5+3)/2 = 4 ms.




Gambar 4.15 Hasil Pengukuran Jitter pada Polycom

Sedangkan jitter visualnya didapatkan dari nilai rata-rata jitter visual jalur kirim 28 ms dan jitter visual jalur terima 24 ms, yaitu: (28+24)/2 = 26 ms.

4. Pengukuran *Packet Loss*
   Pengukuran ini bertujuan untuk melakukan evaluasi *jitter* pada hubungan antar *client* dan *server* selama video *conference* berlangsung, sehingga dapat disimpulkan seberapa baik kualitas video *conference* yang didapatkan.
   Untuk mendapatkan nilai *packet loss* dapat dilihat dari hasil pengukuran aplikasi Polycom seperti pada pengambilan data Video Conference ke Perwakilan Canberra gambar 4.16.




Gambar 4.16 Hasil Pengukuran *Packet Loss* Vicon1 ke perwakilan Canberra

Dari Gambar 4.16, dapat dilihat bahwa hasil pengukuran packet loss menunjukkan nilai *packet loss* audio jalur kirim sebesar 0% dan *packet loss* audio jalur terima sebesar 0% sehingga nilai *packet loss*-nya adalah rata-rata dari kedua nilai tersebut yaitu 0%. Untuk hasil pengukuran *packet loss* visual diperoleh pada jalur kirim sebesar 0% dan jalur terima sebesar 0% sehingga nilai *packet loss* visualnya adalah rata-rata dari kedua nilai packet loss tersebut, yaitu 0%.
Hasil pengukuran komunikasi dari kantor pusat ke kantor perwakilan di Canberra pada jalur terbuka tanpa VPN SSL ditunjukkan pada tabel 4.2.

Tabel 4.2 Hasil Pengukuran QoS pada Video *Conference* ke Kantor Perwakilan Canberra Jalur Terbuka

Sinusoida Vol. XXII No. 2, April 2020
ISSN 1411 - 4593

| No | Analisa Kerja | Waktu Percakapan | Durasi (menit) | Throughput | Delay (ms) | Jitter (ms) | | Packet Loss (%) | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Audio | Visual | Audio | Visual |
| 1 | ViCon 1 | 08.28-08.35 | 7 | 0,779 | 5,015 | 4 | 26 | 0 | 0 |
| 2 | ViCon 2 | 14.35-15.03 | 8 | 0.963 | 4,191 | 3,5 | 23 | 1 | 1 |
| 3 | ViCon 3 | 15.25-15.33 | 8 | 0.671 | 5,555 | 3 | 24,5 | 1 | 0,5 |

Hasil pengukuran komunikasi dari kantor pusat ke kantor perwakilan di Canberra pada jalur tertutup dengan VPN SSL ditunjukkan pada tabel 4.3.

Tabel 4.3 Hasil Pengukuran QoS pada Video *Conference* ke Kantor Perwakilan Canberra Jalur Tertutup

| No | Analisa Kerja | Waktu Percakapan | Durasi (menit) | Throughput | Delay (ms) | Jitter (ms) | | Packet Loss (%) | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Audio | Visual | Audio | Visual |
| 1 | ViCon 1 | 08.53-09.00 | 7 | 1,095 | 3,241 | 2 | 22,5 | 0 | 0 |
| 2 | ViCon 2 | 09.32-09.40 | 8 | 1,063 | 3,247 | 2,5 | 21,5 | 0 | 0 |
| 3 | Vicon3 | 14.39-14.47 | 8 | 1,081 | 3,141 | 3,5 | 23 | 2 | 1 |

Hasil pengukuran komunikasi dari kantor pusat ke kantor perwakilan di Davao City pada jalur terbuka tanpa VPN SSL ditunjukkan pada tabel 4.4.

Tabel 4.4 Hasil Pengukuran QoS pada Video *Conference* ke Kantor Perwakilan Davao City Jalur Terbuka

| No. | Analisa Kerja | Waktu Percakapan | Durasi (menit) | Throughput | Delay (ms) | Jitter (ms) | | Packet Loss (%) | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Audio | Visual | Audio | Visual |
| 1 | ViCon 1 | 12.51-12.59 | 8 | 1,819 | 3,059 | 3,5 | 10,5 | 2,5 | 2,5 |
| 2 | ViCon 2 | 13.09-13.17 | 8 | 1,800 | 3,025 | 3 | 10,5 | 2 | 2,5 |
| 3 | ViCon 3 | 13.27-13.35 | 8 | 1,904 | 2,876 | 3,5 | 11,5 | 1,5 | 2 |

Hasil pengukuran komunikasi dari kantor pusat ke kantor perwakilan di Davao City pada jalur tertutup dengan VPN SSL ditunjukkan pada tabel 4.5.

Tabel 4.5 Hasil Pengukuran QoS pada Video *Conference* ke Kantor Perwakilan Davao City Jalur Tertutup

| No. | Analisa Kerja | Waktu Percakapan | Durasi (menit) | Throughput | Delay (ms) | Jitter (ms) | | Packet Loss (%) | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Audio | Visual | Audio | Visual |
| 1 | ViCon 1 | 13.00-13.08 | 8 | 1,974 | 2,392 | 9 | 12,5 | 2 | 4 |
| 2 | ViCon 2 | 13.18-13.26 | 8 | 2,036 | 2,290 | 2 | 11 | 2 | 4 |
| 3 | ViCon 3 | 13.36-13.44 | 8 | 1.913 | 2,480 | 3 | 12,5 | 1,5 | 1,5 |

Hasil pengukuran komunikasi dari kantor pusat ke kantor perwakilan di Kopenhagen pada jalur terbuka tanpa VPN SSL ditunjukkan pada tabel 4.6.

Tabel 4.6 Hasil Pengukuran QoS pada Video *Conference* ke Kantor Perwakilan Kopenhagen Jalur Terbuka

| No. | Analisa Kerja | Waktu Percakapan | Durasi (menit) | Throughput | Delay (ms) | Jitter (ms) | | Packet Loss (%) | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Audio | Visual | Audio | Visual |
| 1 | ViCon 1 | 15.11-15.20 | 9 | 0,673 | 5,663 | 2,5 | 0 | 3 | 1,5 |
| 2 | ViCon 2 | 15.55-16.03 | 8 | 1,005 | 4,064 | 3 | 0 | 3 | 2 |
| 3 | ViCon 3 | 16.13-16.21 | 8 | 1,027 | 3,881 | 3 | 0 | 0,5 | 0 |

Hasil pengukuran komunikasi dari kantor pusat ke kantor perwakilan di kopenhagen pada jalur tertutup dengan VPN SSL ditunjukkan pada tabel 4.7.

Tabel 4.7 Hasil Pengukuran QoS pada Video *Conference* ke Kantor Perwakilan Kopenhagen Jalur Tertutup

| No. | Analisa Kerja | Waktu Percakapan | Durasi (menit) | Throughput | Delay (ms) | Jitter (ms) | | Packet Loss (%) | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Audio | Visual | Audio | Visual |
| 1 | ViCon 1 | 15.41-15.50 | 9 | 1,055 | 3,450 | 2 | 0 | 5,5 | 4 |
| 2 | ViCon 2 | 16.04-16.12 | 8 | 1,122 | 3,251 | 2 | 0 | 3 | 3 |
| 3 | Vicon 3 | 16.24-16.32. | 8 | 1,132 | 3,306 | 2 | 0 | 0 | 0 |

4.3. Analisa Hasil Pengukuran QOS

Setelah didapatkan data ujicoba dari konfigurasi pertama dan kedua selanjutnya dilakukan analisa terhadap kualitas video *conference*, parameter QoS (Quality of Service) yang dianalisa meliputi *packet loss*, *delay*, *jitter*. Pada penelitian ini juga dilakukan pengukuran *throughput* untuk mengetahui besarnya *bandwidth* yang diperlukan aplikasi video conference pada saat ujicoba dan mengetahui pengaruh *throughput*.

### 4.3.1 Analisa Hasil Pengukuran *Throughput*

Pengukuran ini bertujuan untuk mengetahui besar *throughput* pada hubungan antar *server* dan *client* sesuai dengan efek dari masing-masing percobaan, yaitu misalnya pengaruh konfigurasi jaringan pada Perwakilan Canberra, Davao City dan Kopenhagen.

Berdasarkan pengukuran yang telah dilakukan, nilai *throughput* yang diperoleh pada jalur terbuka ke Perwakilan Canberra nilai berada di kisaran 0,6 – 0,9 Mbit/sec sedangkan pada jalur tertutup berada pada kisaran nilai 1 Mbit/sec. Untuk jalur terbuka ke Perwakilan Davao City, nilai throughputnya berada pada kisaran 1,8-1,9 Mbit/sec sedangkan pada jalur tertutup berada pada kisaran 1,9 – 2 Mbit/sec. Untuk jalur terbuka ke Perwakilan Kopenhagen, nilai throughputnya berada pada kisaran 0,6 – 1 Mbit/sec sedangkan pada jalur tertutup pada

Sinusoida Vol. XXII No. 2, April 2020
ISSN 1411 - 4593

kisaran 1- 1,1 Mbit/sec. Hal ini menunjukkan bahwa terdapat peningkatan nilai *throughput* pada hasil percobaan video *conference* jalur tertutup (dengan VPN SSL) dan secara keseluruhan percobaan video conference yang dilakukan berjalan lancar.

#### 4.3.2 Analisa Hasil Pengukuran *Delay*

Berdasarkan hasil pengukuran yang telah dilakukan, pada jalur terbuka ke Perwakilan Canberra diperoleh nilai delay pada kisaran 4,1 – 5,5 ms sedangkan pada jalur tertutup pada kisaran 3,1 – 3,2 ms. Untuk hasil pengukuran ke Perwakilan Davao City, pada jalur terbuka diperoleh nilai delay pada kisaran 2,8 – 3 ms sedangkan pada jalur tertutup pada kisaran 2,2 – 2,4 ms. Untuk hasil pengukuran ke Perwakilan Kopenhagen, pada jalur terbuka diperoleh nilai delay pada kisaran 3,8 – 5,6 ms sedangkan pada jalur tertutup pada kisaran 3,2 – 3,4 ms. Secara keseluruhan nilai *delay* yang diperoleh berada pada kisaran di bawah 150 ms yang artinya berada pada kategori baik dan *acceptable for most users*. Selain itu, dapat dilihat bahwa terdapat penurunan nilai *delay* pada video conference jalur tertutup menggunakan VPN SSL.

Berdasarkan Kategori Besar *Delay* ITU-T, maka keseluruhan nilai *delay* hasil pengukuran jalur terbuka dan tertutup masuk pada kategori baik.

#### 4.3.3 Analisa Hasil Pengukuran *Jitter*

Pada percobaan video *conference* Kantor Pusat Kemenlu dengan Kantor Perwakilan Canberra, Davao City dan Kopenhagen diperoleh nilai *jitter* baik audio maupun visual hampir sama dan dalam kisaran yang cukup kecil (dibawah 30 ms).

Nilai *jitter* visual yang paling besar diperoleh pada video *conference* ke Perwakilan Canberra baik pada jalur terbuka maupun tertutup yang berada pada kisaran 21-26 ms. Dan nilai *jitter* visual tersebut lebih besar dibandingkan dengan nilai *jitter* audio. Hal ini juga ditunjukkan pada hasil pengukuran video *conference* ke Perwakilan Davao city dimana nilai jitter visual lebih besar daripada nilai *jitter* audio. Namun hal sebaliknya terjadi pada hasil pengukuran nilai *jitter* video *conference* ke Perwakilan Kopenhagen dimana nilai *jitter* audio lebih besar daripada nilai *jitter* visual.

Dari semua percobaan yang telah dijalankan, nilai *jitter* yang dihasilkan kurang lebih sama dan nilai *jitter* tersebut masih dalam batas standar yang ditentukan ITU. *Jitter* yang makin besar akan mengakibatkan keterlambatan paket data berikutnya sehingga paket itu akan dibuang dan akan menyebabkan adanya *packet loss*. Dalam layanan *streaming* multimedia, dibutuhkan nilai *jitter* yang kecil dan cenderung stabil. Hal ini akan memberikan laju kedatangan paket yang bersifat kontinyu sehingga paket-paket yang datang kedalam *buffer* tidak berlebih/berkurang.

#### 4.3.4 Analisa Hasil Pengukuran *Packet loss*

Secara keseluruhan terlihat bahwa nilai *packet loss* pada percobaan video *conference* ke masing-masing ketiga perwakilan RI tersebut masih dalam standar dari ITU-T, yaitu di bawah 10%. Nilai *packet loss* terkecil diperoleh dari hasil pengukuran video conference ke Perwakilan Canberra dimana nilainya baik pada jalur terbuka maupun tertutup berada pada kirasan 2% ke bawah.

## 5. Simpulan

Dari hasil percobaan dan analisa data yang dilakukan dapat disimpulkan bahwa:

1. Dari kegiatan video *conference* pada jaringan tertutup dengan VPN SSL menunjukkan bahwa pada Wireshark sebagai alat *sniffing* informasi protokol berupa *user* ID dan alamat IP u*ser* dari komputer yang melakukan komunikasi dengan aplikasi Polycom tidak dapat dilihat dan paket data berupa RTP dan SIP juga tidak dapat dilihat. Jika dibandingkan dalam pengujian video *conference* yang dilakukan pada jaringan terbuka dapat dilihat *user* ID pengguna dan alamat IP komputer dari pengguna aplikasi Polycom serta dapat dilihat RTP dan SIP.
2. Aplikasi video *conference* dapat digunakan dengan baik dalam jaringan di Kantor Pusat Kemenlu dengan masing-masing ketiga Perwakilan RI. Hal ini ditunjukkan dengan tingkat performansi video *conference* yang memenuhi persyaratan rekomendasi ITU-T G.114, yaitu nilai *delay* 0 – 50 ms yang berarti dapat diterima untuk sebagian besar pengguna aplikasi (*acceptable for most user applications*), *jitter* yang diperoleh kurang dari 30 ms yang berarti masih dapat diterima dengan baik, *packet loss* di bawah 10% yang berarti masih termasuk dalam

Sinusoida Vol. XXII No. 2, April 2020
ISSN 1411 - 4593

rekomendasi. Dari hasil pengukuran percobaan video conference jalur tertutup dengan VPN SSL, terdapat peningkatan nilai *throughput* dan penurunan nilai *delay* jika dibandingkan dengan video conference pada jalur terbuka.

## DAFTAR PUSTAKA

1. Harsha Pandey and P.P. Pande. 2014. Video conferencing: An Efficient E-Learning Tool for Distance Education. India.
2. Winarno Sugeng, Jazi Eko Istiyanto, Khabib Mustofa and Ahmad Ashari. 2015. The Impact of QoS Changes towards Network Performance.
3. Joseph Steinberg and Timothy Speed. 2005. United Kingdom. Understanding SSL VPN. Packt Publishing.
4. Agus Kurniawan. 2012. Network Forensics, Panduan Analisis dan Investigasi Paket Data Jaringan Menggunakan Wireshark. Yogyakarta. Penerbit ANDI
5. Onno W. Purbo. 2018. Intenet-TCP/IP: Konsep & Implementasi. Yogyakarta. Penerbit ANDI.
6. K. Luqman. 2014. Implementasi dan Analisis SSL VPN sebagai solusi keamanan jaringan. UKSW.
7. Mohamad Abdul Kadir. 2011. Studi Eksplorasi Secure VoIP with SSL VPN. Bandung. Institute Teknologi Bandung.
8. Xavier Garcia Faura. 2005. Understanding VPN Tunnels Over SSL. SANS Institute
9. Samad S. Kolahi, Yuqing Cao, Hong Chen. 2017. Impact of SSL Security on Bandwith and Delay in IEEE 802.11n WLAN Using Windows 7. Unitec Institute of Technology. New Zealand
10. Muhammad Khoirul Umam, L. Budi Handoko, M.Kom. 2015. Analisis Kinerja Jaringan Wlan Menggunakan Metode Action Research Pada Dinas Perhubungan Komunikasi Dan Informasi Kabupaten Pemalang. Universitas Dian Nuswantoro.