ISSN : 1410 - 7104

Rancang Bangun Jaringan PABX Berbasis IP Menggunakan Metode IPsec VPN Gateway

IP-Based PABX Network Design Using the IPsec VPN Gateway Method

Djoko Suprijatmono[1] dan Deni Sutendi Kartawijaya[2]
Program Studi Teknik Elektro, Fakultas Teknologi Industri, Institut Sains dan Teknologi Nasional, Jakarta
Email : [1]djokojte@istn.ac.id; [2]wijayadeni110908@gmail.com

Abstrak --- *Layanan komunikasi telepon yang saat ini digunakan di kantor Pusat Kementerian Luar Negeri dan kantor Perwakilan RI di luar negeri menggunakan sistem PABX yang belum terhubung satu dengan lainnya. Kemudian dikembangkan sistem komunikasi suara yang akan menghubungkan sistem PABX berbasis IP di kantor Pusat Kementerian Luar Negeri di Jakarta dengan perangkat PABX di semua kantor Perwakilan RI di luar negeri, melalui jaringan internet dengan penerapan metode IP-Sec VPN gateway untuk interkoneksi jaringan komunikasinya.*
Dari penelitian yang dilakukan, interkoneksi antara sistem PABX berbasis IP di kantor pusat Jakarta dengan kantor perwakilan di Johor Bahru, Malaysia dan Davao City, Filipina, dapat diimplementasikan dengan baik dengan kualitas suara yang cukup baik. Hasil analisis QoS yang dilakukan berdasarkan parameter data troughput, delay, jitter dan packet loss yang diukur selama komunikasi suara berlangsung berada pada nilai yang cukup baik berdasarkan standar yang ada. Untuk nilai pengukuran delay, pada pengujian komunikasi data suara ke Johor Bahru menunjukkan nilai 19-32 ms dan pada pengujian komunikasi data suara ke Davao City menunjukkan nilai 12,671-25,939 ms, yang mana keduanya berada pada kategori bagus sesuai standar ITU-T. Untuk nilai pengukuran packet loss, pada pengujian komunikasi data suara ke Johor Bahru menunjukkan nilai rata-rata 0%, yang berada pada kategori sangat bagus sesuai standar Typhon, sedangkan pada pengujian komunikasi data suara ke Davao City menunjukkan nilai rata-rata 13,09% yang berada pada kategori sedang sesuai standar Typhon.

Kata Kunci : *PABX berbasis IP, IPSec VPN, QoS, troughput, delay, jitter, packet loss.*

Abstract *--- Telephony communication services that is currently used in the offices of the Ministry of Foreign Affairs and the Indonesian Representative offices abroad, use a PABX system that is stand alone and disconnected to each other. The new telephony communications system will be developed, connect IP-based PABX system at the Ministry of Foreign Affairs's head office in Jakarta with PABX equipment in all Indonesian Representative offices abroad, through internet with IP-Sec VPN gateway method for interconnection of its communication network.*
From the research conducted, the interconnection between IP-based PABX system at Jakarta head office with representative offices in Johor Bahru, Malaysia and Davao City, Philippines, can be implemented well with good quality. QoS analysis results are conducted based on the parameters of data throughput, delay, jitter and packet loss measured during voice communications take place at a good enough value based on existing standards. For the value of delay measurement, the voice data communications test to Johor Bahru shows the value of 19-32 ms and on testing voice data communications to Davao City shows the value of 12,671-25,939 ms, both of which are in good category according to ITU-T standard. For the measurement of packet loss, the test of voice data communications to Johor Bahru shows an average value of 0%, which is in very good category according to Typhon standard, whereas in the test of voice data communications to Davao City shows the average value of 13.09% which is in the medium category according to Typhon standard.

Keywords : IP-based PABX, IPSec VPN, QoS, troughput, delay, jitter, packet loss.

1. PENDAHULUAN

Kebutuhan manusia akan informasi dan komunikasi pada saat ini semakin berkembang sehingga teknologi telekomunikasi terus berkembang untuk memenuhi kebutuhan tersebut. Layanan komunikasi telepon yang saat ini digunakan di kantor Pusat Kementerian Luar Negeri dan kantor Perwakilan RI di luar negeri menggunakan sistem PABX yang belum terhubung satu dengan lainnya.

Dengan kondisi tersebut, saat ini sedang dikembangkan sistem komunikasi suara yang akan menghubungkan sistem PABX berbasis IP di kantor Pusat Kementerian Luar Negeri di Jakarta dengan perangkat PABX di semua kantor Perwakilan RI di luar negeri, khususnya yang berada pada wilayah perbatasan Indonesia, melalui jaringan internet dengan mengimplementasikan teknologi IP-Sec VPN gateway untuk interkoneksi jaringan komunikasinya.

Dengan interkoneksi antar PABX berbasis IP tersebut diharapkan dapat meningkatkan efektifitas layanan komunikasi telepon antara kantor Pusat dengan semua kantor Perwaklian RI di luar negeri sehingga dapat mendukung kegiatan diplomasi Indonesia terutama pada wilayah perbatasan.

Pokok permasalahan pada penulisan makalah ini adalah bagaimana merancang dan mengimplementasikan jaringan komunikasi suara antar PABX berbasis IP dengan metode IP-Security VPN.

Pada makalah ini, penulis membatasi permasalahan pada hal-hal sebagai berikut :

a. Merancang jaringan komunikasi suara antar PABX berbasis IP dengan metode IPsec VPN gateway.
b. Mengimplementasikan interkoneksi jaringan PABX berbasis IP menggunakan metode IPsec VPN gateway.
c. Menganalisis dan menguji Quality of Services (QoS) menggunakan parameter-parameter troughput, delay, jitter dan packet loss.
d. Kasus yang dianalisis adalah perancangan dan implementasi jaringan komunikasi suara antar PABX berbasis IP antara Kementerian Luar Negeri dan kantor Perwakilan RI di Johor Bahru, Malaysia dan di Davao City, Filipina yang berbatasan dengan Indonesia.

2. METODA

2.1 PABX Berbasis IP

Berkat kemajuan teknologi informasi dan komunikasi (TIK), PABX konvensional dikembangkan menjadi PABX berbasis IP, dimana sinyal analog yang digunakan pada jaringan telepon analog dikonversi menjadi sinyal digital yang dapat disalurkan melalui internet protocol (IP). Infrastruktur jaringan juga dapat menggunakan jaringan komputer (ethernet) yang sudah ada sehingga tidak perlu menarik kabel khusus untuk jaringan PABX berbasis IP ini. Perusahaan tidak perlu mengganggu/mengubah infrastruktur komunikasi eksternal yang ada:

Sebuah PABX berbasis IP dapat terhubung ke jalur PSTN tradisional melalui gateway VOIP sehingga perusahaan dapat tetap menggunakan nomor telepon regular.

PABX berbasis IP adalah perangkat switching komunikasi telepon dan data berbasis teknologi Internet Protocol (IP) yang mengendalikan ekstensi telepon analog (TDM) maupun ekstensi Telepon IP [4]. PABX berbasis IP ini dapat menyediakan panggilan telepon melalui jaringan data IP, dimana semua percakapan yang terjadi akan dikirim sebagai paket data melalui jaringan IP.

PABX berbasis IP memiliki teknologi canggih dan mencakup fitur-fitur yang canggih pula sehingga memberikan kebutuhan komunikasi yang efektif dan efesien. Fungsi-fungsi yang dapat dilakukan antara lain penyambungan, pengendalian, dan pemutusan hubungan telepon; translasi protokol komunikasi; translasi media komunikasi atau transcoding; serta pengendalian perangkat-perangkat IP Teleponi seperti VoIP Gateway, Access Gateway, dan Trunk Gateway.

2.2 Konsep IPsec VPN

IP Security (IP Sec) adalah sebuah protokol yang digunakan untuk mengamankan transmisi datagram dalam sebuah internetwork berbasis TCP/IP[3]. IPSec mendefiniskan beberapa standar untuk melakukan enkripsi data dan juga integritas data pada lapisan kedua dalam DARPA Reference Model (internetwork layer). IPSec melakukan enkripsi terhadap data pada lapisan yang sama dengan protokol IP dan menggunakan teknik tunneling untuk mengirimkan informasi melalui jaringan internet atau dalam jaringan intranet secara aman. IPSec didefinisikan oleh badan Internet Engineering Task Force (IETF) dan diimplementasikan di dalam banyak sistem operasi. IPSec mendukung dua buah sesi komunikasi keamanan, yakni sebagai berikut :

a. Protokol Authentication Header (AH) menawarkan otentikasi pengguna dan perlindungan dari beberapa serangan dan juga menyediakan fungsi otentikasi terhadap data serta integritas terhadap data. Protokol ini mengizinkan penerima untuk merasa yakin bahwa identitas si pengirim adalah benar adanya, dan data pun tidak dimodifikasi selama transmisi. Namun, protokol AH tidak menawarkan fungsi enkripsi terhadap data yang ditransmisikannya. Informasi AH dimasukkan ke dalam header paket IP yang dikirimkan dan dapat digunakan secara sendirian atau bersamaan dengan protokol Encapsulating Security Payload.

b. Protokol Encapsulating Security Payload (ESP) melakukan enkapsulasi serta enkripsi terhadap data pengguna untuk meningkatkan kerahasiaan data. ESP juga dapat memiliki skema otentikasi dan perlindungan dari beberapa serangan dan dapat digunakan secara sendirian atau bersamaan dengan Authentication Header. Sama seperti halnya AH, informasi mengenai ESP juga dimasukkan ke dalam header paket IP yang dikirimkan.

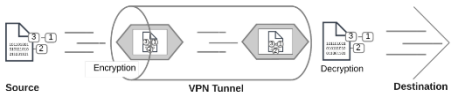
IPSec protocol diciptakan oleh kelompok kerja IPSec dibawah naungan IETF. Arsitektur dan komponen dasar dari IPSec VPN seperti yang didefinisikan oleh RFC2401 adalah:

- Security protocols: Authentication Header (AH) dan encapsulation security payload (ESP).
- Key management: ISAKMP, IKE, SKEME.
- Algorithms: enkripsi dan authentikasi.

2.3 VPN Tunnel

Jalur data antara komputer pengguna dan private network melalui VPN disebut tunnel.

Seperti halnya tunnel fisik, jalur data dapat diakses dari kedua ujung tunnel tersebut. Dalam skenario telekomunikasi, tunnel ini terhubung antara aplikasi VPN client pada komputer pengguna atau perangkat VPN gateway dengan perangkat VPN gateway/server di sisi private network kantor. Hal ini dimungkinkan dengan proses enkapsulasi, paket-paket IPsec berjalan dari ujung sisi tunnel yang satu hingga ujung tunnel di sisi yang lain yang berisi data paket yang dipertukarkan antara local pengguna dan remote private network. Proses enkripsi pada paket data memastikan pihak luar yang melakukan intersepsi tidak dapat membaca isi datanya.



Gambar 1. Ilustrasi pembentukan *VPN tunnel*

IPsec VPN tunnel dapat dibangun diantara:

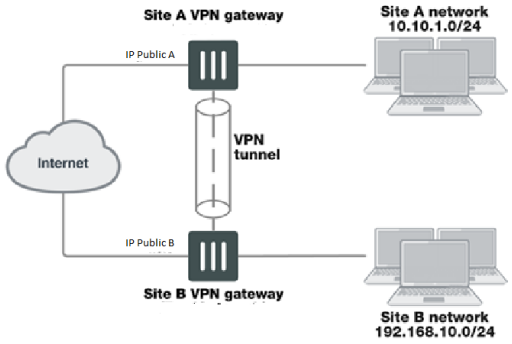
- Komputer yang dilengkapi dengan aplikasi VPN *client* dengan perangkat *VPN gateway*.
- 2 perangkat VPN gateway

2.4 VPN *Gateway*

Gateway adalah router yang menghubungkan jaringan lokal ke jaringan lain. Pengaturan default gateway di properti TCP / IP komputer menentukan gateway untuk jaringan lokal.

VPN Gateway berfungsi sebagai salah satu ujung VPN tunnel untuk menerima paket IPsec yang masuk, mendekripsikan paket data yang dienkapsulasi dan menyampaikan paket data ke jaringan lokal. Juga, mengenkripsi paket data yang ditujukan ke ujung VPN tunnel lainnya, mengenkapsulasi paket data, dan mengirimkan paket IPsec ke VPN gateway tujuan. VPN Gateway adalah suatu perangkat VPN karena melindungi private network di belakangnya, memastikan keamanan data VPN yang tidak terenkripsi. Gateway juga bisa merupakan aplikasi VPN client yang berjalan di sebuah komputer selama data yang tidak terenkripsi aman di dalam komputer tersebut.

Alamat IP VPN gateway biasanya merupakan alamat IP dari antarmuka jaringan yang terhubung ke internet. Gambar berikut menunjukkan koneksi VPN antara dua private network dengan unit VPN server yang berfungsi sebagai VPN Gateway. Konfigurasi ini biasa disebut sebagai Gateway-to-Gateway IPsec VPN.



Gambar 2. *Gateway-to-gateway IPsec VPN tunnel* antara 2 *private network*

Meskipun trafik IPsec pada kenyataanya melewati banyak router di internet, VPN tunnel dapat digambarkan sebagai koneksi aman yang sederhana antara dua unit Router / VPN gateway. Pengguna pada dua private network tidak perlu mengetahui VPN tunnel. Aplikasi pada komputer masing-masing menghasilkan paket dengan alamat sumber dan alamat tujuan yang sesuai seperti biasanya, untuk kemudian VPN gateway akan mengelola semua detail enkripsi, enkapsulasi, dan pengiriman paket data ke VPN gateway di posisi remote. Data hanya dienkapsulasi di dalam paket IPsec pada VPN tunnel antara dua VPN gateway. Di antara komputer pengguna dan gateway, datanya berada pada private network yang aman dan dalam paket IP biasa.

Misalnya pengguna 1 pada jaringan site A, dengan alamat IP 10.10.1.7, mengirimkan paket dengan alamat IP tujuan 192.168.10.8, alamat pengguna 2 berada pada jaringan Site B. Router / VPN gateway unit pada site A dikonfigurasi untuk mengirimkan paket dengan tujuan pada jaringan 192.168.10.0 melalui VPN, terenkripsi dan dienkapsulasi. Demikian pula dengan unit Router / VPN gateway pada site B dikonfigurasi untuk mengirimkan paket dengan tujuan pada jaringan 10.10.1.0 melalui VPN tunnel ke VPN gateway site A.

Pada jaringan site-to-site atau gateway-to-gateway VPN, unit Router / VPN gateway memiliki alamat IP statis (tetap) dan masing-masing unit dapat memulai komunikasi.

2.5 Quality of Service (Q0S)

Quality of Service (QoS) didefinisikan sebagai suatu pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat dari suatu layanan [3]. QoS mengacu pada kemampuan jaringan untuk menyediakan layanan yang lebih baik pada trafik jaringan tertentu melalui teknologi yang berbeda-beda. Tujuan dari QoS adalah untuk memenuhi kebutuhan-kebutuhan layanan yang berbeda, yang menggunakan infrastruktur yang sama. QoS menawarkan kemampuan untuk mendefinisikan

atribut-atribut layanan yang disediakan, baik secara kualitatif maupun kuantitatif. Berbagai aplikasi memiliki jenis kebutuhan yang berbeda. Misalnya transaksi data bersifat sensitif terhadap distorsi tetapi kurang sensitif terhadap delay. Sebalikanya, komunikasi suara bersifat sensitif terhadap delay dan kurang sensitif terhadap kesalahan.

Performansi jaringan merujuk ke tingkat kecepatan dan kehandalan penyampaian berbagai jenis beban data di dalam suatu komunikasi. Performansi merupakan kumpulan berbagai besaran teknis, antara lain:

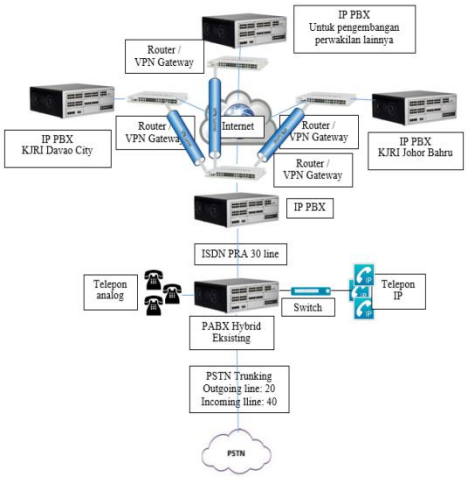
a. Troughput, yaitu kecepatan (rate) transfer data efektif, yang diukur dalan bit/s. Header-header dalam paket-paket data mengurangi nilai troughput. Maka penggunaan sebuah saluran secara bersama-sama juga akan mengurangi nilai ini. Yang menyebabkan troughput yang didapat tidak sebesar bandwidth adalah routing protocol, broadcast traffic, collision, header, dan sebagainya.
b. Packet Loss, adalah jumlah paket yang hilang. Umumnya perangkat jaringan memiliki buffer untuk menampung data yang diterima. Jika terjadi kongesti yang cukup lama, buffer akan penuh, dan data baru tidak dapat diterima. Paket yang hilang ini harus dikirim ulang, yang akan membutuhkan waktu tambahan.
c. Delay, adalah waktu yang dibutuhkan data untuk menempuh jarak dari asal ke tujuan. Delay ini bisa dipengaruhi oleh jarak (misalnya akibat pemakaian satelit), atau kongesti (yang memperpanjang antrian), atau bisa juga akibat waktu olah yang lama (misalnya proses digitalisasi dan kompresi data).
d. Jitter atau variasi delay, diakibatkan oleh variasi-variasi dalam panjang antrian, dalam waktu pengolahan data, dalam waktu yang dibutuhkan untuk retransmisi data (karena jalur yang digunakan juga berbeda), dan juga dalam waktu penghimpunan ulang paket-paket di akhir perjalanan. [3]

2.6 Perancangan Sistem PABX Berbasis IP pada masing-masing kantor

Pada tahap awal makalah ini penulis merancang sistem PABX berbasis IP di kantor pusat dan kantor perwakilan di KJRI Johor Bahru, Malaysia serta kantor KJRI Davao City, Filipina.

2.6.1 Sistem PABX di kantor pusat

Perancangan sistem PABX di kantor pusat dapat dijelaskan seperti pada gambar berikut :



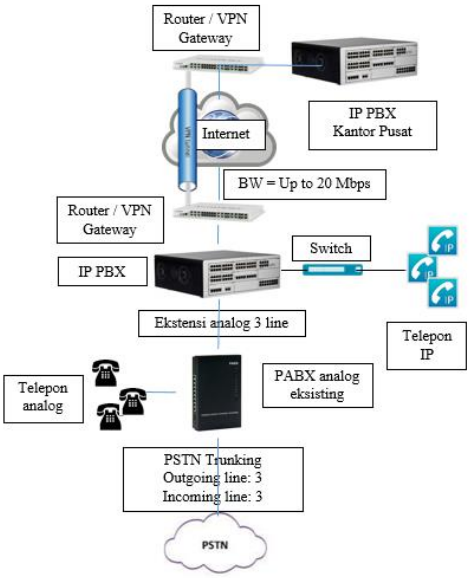
Gambar 3. Sistem PABX di kantor Pusat

Seperti pada gambar 3. di atas, sistem PABX di kantor pusat terdiri dari PABX eksisting yang saat ini memiliki 1093 telepon ekstensi analog, 19 telepon SIP dan 219 telepon IP, dan terhubung ke jaringan PSTN melalui trunk gateway. Jalur Hunting outgoing call sebanyak 20 jalur, dimana pada saat bersamaan pengguna di pusat dapat melakukan panggilan keluar, baik ke PSTN maupun ke GSM sebanyak 20 panggilan. Jalur Hunting incoming call sebanyak 40 jalur, pada saat bersamaan panggilan dari luar baik dari nomor PSTN maupun dari GSM dapat menghubungi kantor pusat sebanyak 40 panggilan. PABX ini berfungsi sebagai sentral switching dan sistem kontrol bagi semua nomor ekstensi baik analog, SIP maupun telepon IP agar dapat saling berkomunikasi antara sesama ekstensi, melakukan panggilan ke PSTN dan seluler dari semua nomor ekstensi maupun menerima panggilan dari PSTN dan seluler. Selanjutnya semua nomor ekstensi di pusat dapat berkomunikasi dengan PABX di perwakilan Johor Bahru dan Davao City dengan mengatur dial plan melalui IP PBX.

Untuk menghubungkan ke sistem PABX perwakilan, dipasang satu buah IP PBX yang terkoneksi ke PABX perwakilan melalui jalur IPSec VPN gateway. IP PBX ini digunakan sebagai pusat koneksi antara sistem PABX kantor pusat ke kantor perwakilan KJRI Johor Bahru dan kantor KJRI Davao City, juga untuk koneksi ke sistem PABX di perwakilan lainnya untuk pengembangan interkoneksi di masa mendatang. Sesuai pengaturan, IP PBX ini terkoneksi dengan PABX eksisting melalui jalur ISDN PRA sebanyak 30 kanal, sehingga pada saat bersamaan komunikasi antara pengguna di kantor pusat dengan pengguna di perwakilan dapat dilakukan sebanyak 30 jalur komunikasi.

2.6.2 Sistem PABX di perwakilan KJRI Johor Bahru, Malaysia.

Perancangan sistem PABX di kantor KJRI Johor Bahru dapat dijelaskan seperti pada gambar berikut :



Gambar 4. Sistem PABX di perwakilan KJRI Johor Bahru.

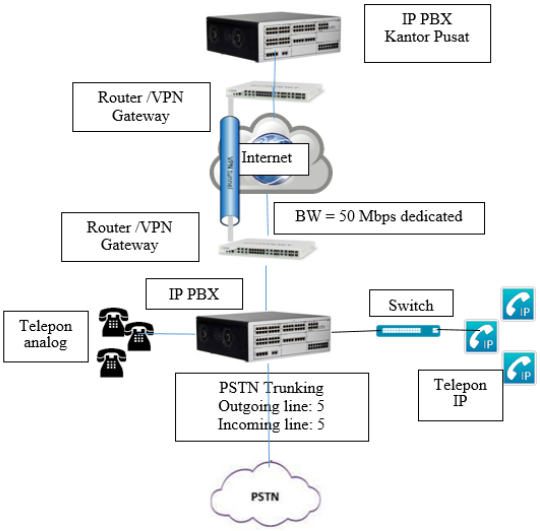
Seperti terlihat pada gambar 4 di atas, sistem PABX di kantor KJRI Johor Bahru terdiri dari PABX eksisting analog yang saat ini memiliki 27 telepon ekstensi analog dan terhubung ke jaringan PSTN melalui trunk gateway. Jalur Hunting incoming dan outgoing call sebanyak 3 jalur, dimana pada saat bersamaan pengguna di Johor Bahru dapat melakukan panggilan keluar, ke PSTN atau ke GSM maupun menerima panggilan dari luar, dari nomor PSTN atau dari GSM sebanyak 3 panggilan. PABX ini berfungsi sebagai sentral switching dan sistem kontrol bagi semua nomor ekstensi analog agar dapat saling berkomunikasi antara sesama ekstensi, melakukan panggilan ke PSTN dan seluler dari semua nomor ekstensi maupun menerima panggilan dari PSTN dan seluler. Selanjutnya semua nomor ekstensi di Johor Bahru dapat berkomunikasi dengan PABX di pusat dengan mengatur dial plan melalui IP PBX.

Untuk menghubungkan ke sistem PABX pusat , dipasang satu buah IP PBX yang terkoneksi ke PABX pusat melalui jalur IPSec VPN gateway. IP PBX ini digunakan sebagai pusat koneksi antara sistem PABX kantor Johor Bahru ke kantor pusat. Sesuai pengaturan, IP PBX ini terkoneksi dengan PABX analog eksisting melalui jalur ekstensi analog sebanyak 3 kanal, sehingga pada saat bersamaan komunikasi antara pengguna di kantor Johor Bahru dengan pengguna di pusat dapat dilakukan sebanyak 3 jalur komunikasi. Kemudian ditambahkan 5 buah telepon IP pada IP PBX ini, yang langsung terhubung ke IP PBX melalui jaringan LAN, sehingga semua telepon IP dapat berkomunikasi ke kantor pusat secara bersamaan.

Bandwidth internet yang dimiliki oleh perwakilan Johor Bahru memiliki kapasitas up to 20 Mbps ADSL channel, dan tidak diatur pembagian bandwidth yang dialokasikan untuk jalur interkoneksi IPSec VPN gateway antara Johor Bahru ke kantor pusat.

2.7 Sistem PABX di perwakilan KJRI Davao City, Filipina.

Dikarenakan kondisi yang ada, sistem PABX analog eksisting di kantor perwakilan KJRI Davao City tidak dipergunakan lagi dan diganti dengan IP PBX yang baru, dengan perancangan seperti dijelaskan pada gambar berikut :



Gambar 5. Sistem PABX di perwakilan KJRI Davao City

Seperti terlihat pada gambar 5 di atas, sistem PABX di kantor KJRI Davao City terdiri dari IP PBX yang terdiri dari 25 telepon ekstensi analog dan 5 telepon IP. IP PBX ini terkoneksi langsung ke PABX pusat melalui jalur IPSec VPN gateway, sehingga semua pengguna di Davao City dapat melakukan panggilan ke pusat secara bersama-sama, namun akan dibatasi oleh sistem PABX yang ada di pusat, dimana hanya 30 panggilan yang dapat dilakukan di sistem PABX pusat yang terkoneksi ke perwakilan.

Bandwidth internet yang dimiliki oleh perwakilan Davao City memiliki kapasitas 50 Mbps dedicated channel, namun tidak diatur pembagian bandwidth yang dialokasikan khusus untuk jalur interkoneksi IPSec VPN gateway antara Davao City ke kantor pusat.

2.7.1 Sistem Penomoran Ekstensi

Dengan interkoneksi antar IP PBX di pusat dengan KJRI Johor Bahru dan KJRI Davao City, tidak merubah sistem penomoran ekstensi yang ada disemua lokasi sehingga tidak merubah konfigurasi

yang sudah ada. Penambahan dilakukan di semua lokasi kantor ini ada pada cara melakukan panggilan ke ekstensi di kantor yang dituju dengan mengkonfigurasi pada masing-masing IP PBX. Penambahannya adalah sebagai berikut:

Pada kantor pusat:
- Kantor pusat untuk melakukan panggilan ke Kantor KJRI Johor Bahru adalah memasukkan digit *5 dilanjutkan 60494, kemudian ada greeting selamat datang KJRI Johor Bahru, selanjutnya memasukkan nomor ekstensi analog yang dituju. Sedangkan untuk melakukan panggilan ke nomor ekstensi telepon IP KJRI Johor bahru, tekan *5 diikuti no ekstensi telepon IP yang dituju.
- Kantor pusat untuk melakukan panggilan ke Kantor KJRI Davao City adalah memasukkan digit *5 dilanjutkan nomor ekstensi yang dituju, baik untuk ekstensi analog maupun telepon IP.

Pada kantor KJRI Johor Bahru:
- Untuk melakukan panggilan ke pusat dari ekstensi analog, dengan menekan 7, setelah terdengar musik, tekan 12 lalu diikuti nomor ekstensi pusat yang dituju.
- Untuk melakukan panggilan ke pusat dari telepon IP, dengan menekan 12 dilanjutkan nomor ekstensi pusat yang dituju.
-

Pada kantor KJRI Davao City:
- Untuk melakukan panggilan ke pusat baik dari ekstensi analog maupun telepon IP, dengan menekan 12 lalu diikuti nomor ekstensi pusat yang dituju.

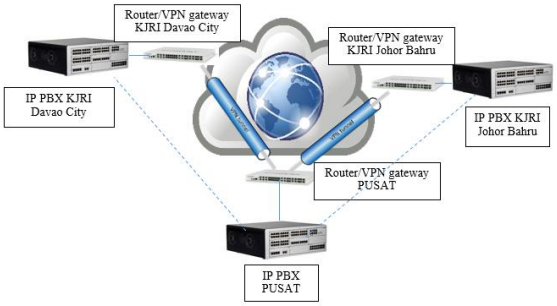
Penomoran yang digunakan untuk melakukan akses panggilan antar kantor ini dapat disesuaikan kembali sesuai dengan kebutuhan dan disesuaikan dengan konfigurasi yang ada di setiap lokasi.

2.7.2 Perancangan jaringan IP*sec* VPN *gateway* untuk interkoneksi antar IP PBX

Tahap kedua pada makalah ini penulis melakukan perancangan jaringan IPSec VPN gateway sebagai media interkoneksi PABX berbasis IP antara kantor pusat dengan kantor perwakilan di KJRI Johor Bahru, Malaysia dan KJRI Davao City, Filipina sehingga komunikasi suara antara pusat dengan KJRI Johor Bahru dan KJRI Davao City dapat dilakukan secara internal.

Untuk menghubungkan sistem PABX di kantor pusat dengan sistem PABX di Johor Bahru dan Davao City, maka perlu adanya proses tunneling antar site tersebut. Karena proses IPSec merupakan mekanisme end-to-end tunneling antar router/vpn gateway, dan saat ini ada 2 perwakilan yang akan dihubungkan ke pusat, maka diperlukan adanya 2 proses tunnel yang dikonfigurasikan pada router/VPN gateway di sisi kantor pusat.

Hal pertama yang dilakukan adalah menentukan topologi jaringan IPSec VPN antara kantor pusat dengan kantor perwakilan Johor Bahru dan Davao City seperti pada gambar berikut:



Gambar 6. Topologi Jaringan *IPsec VPN gateway-to-gateway*

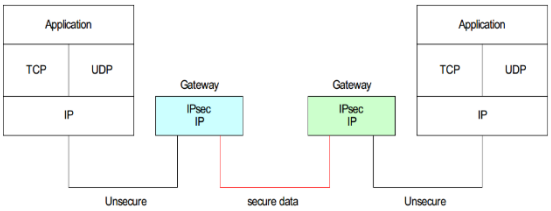
Seperti pada gambar 6 di atas, topologi jaringan IPsec VPN yang digunakan untuk menghubungkan semua PABX berbasis IP tersebut menggunakan topologi star, namun sesuai kebijakan institusi, komunikasi yang digunakan tetap point-to-point, yaitu antara kantor pusat dengan kantor Johor Bahru dan antara kantor pusat dengan kantor Davao City. Sedangkan antara kantor Johor Bahru dan kantor Davao City tidak dibentuk tunnel.

Selanjutnya adalah melakukan konfigurasi pada router/vpn gateway kantor pusat dengan dibentuknya 2 tunnel IPSec VPN gateway dengan parameter masing-masing untuk pusat-Johor bahru dan pusat-Davao City. Setelah itu, router/VPN Gateway pada masing-masing kantor perwakilan baik Johor Bahru maupun Davao City dikonfigurasi untuk membentuk tunnel IPSec VPN gateway ke pusat.

2.7.3 Proses Pembentukan Tunnel IPSec VPN

Mode IPSec yang digunakan untuk gateway-to-gateway adalah tunnel mode. Seperti terlihat pada gambar 5.7, gateway mengenkapsulasi keseluruhan paket, termasuk original header dari IP, kemudian menambahkan header IP baru pada paket data, lalu mengirimkannya melalui jaringan publik menuju gateway yang kedua, dimana informasi akan didekripsi dan bentuk asli informasi akan sampai ke penerima.

Proses pengamanan yang dilakukan adalah pada masing-masing ujung router/VPN gateway, sehingga apabila ada yang mencoba melakukan penyadapan di jalur internet (man in the middle) tidak dapat memperoleh data yang dikomunikasikan dengan adanya tunnel serta proses enkripsi dan dekripsi yang dilakukan pada masing-masing router/VPN gateway

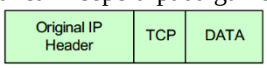


Gambar 7. IPsec VPN *tunnel mode* [1]

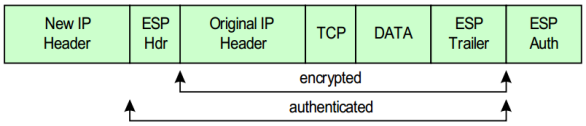
Proses pembentukan IPSec VPN tunnel mode antara pusat dengan Johor Bahru. Dimulai dengan router/VPN gateway pusat memulai IKE dengan peer router/VPN gateway Johor Bahru. Kemudian router/VPN gateway pusat menawarkan algoritma enkripsi, algoritma hash (untuk otentifikasi). Kemudian router/VPN gateway pusat membangkitkan bilangan acak/key, dan mengirimkannya bersama kunci public ke router/VPN gateway Johor Bahru. Kemudian router/VPN gateway Johor Bahru menggunakan kunci public Router/VPN gateway pusat untuk mendekrip bilangan acak/key yang telah dienkrip dan kemudian memverifikasi Router/VPN gateway Johror Bahru ke router/VPN gateway pusat. Kemudian router/VPN gateway pusat menggunakan kunci private untuk menandatangani bilangan acak/key dan mengirimkannya kembali ke Router/VPN gateway Johor Bahru. Router/VPN gateway Johor Bahru menggunakan kunci private untuk menandatangani bilangan acak/key dan mengirinkannya kembali ke Router/VPN gateway pusat. Router/VPN gateway pusat menggunakan kunci public untuk mendekrip bilangan acak/key yang dienkrip kemudian memverifikasi ke Router/VPN gateway Johor Bahru. Router/VPN gateway Johor Bahru menggunakan kunci public Router/VPN gateway pusat untuk mendekrip bilangan acak/key yang dienkrip kemudian memverifikasi ke Router/VPN gateway pusat. Router/VPN gateway pusat memulai quick mode negotiation dengan Router/VPN gateway Johor Bahru dengan membangkitkan dan mengirimkan security parameter index (SPI). Router/VPN gateway Johor Bahru memverifikasi bahwa SPI belum digunakan olehnya dan mengkonfirmasi bahwa Router/VPN gateway pusat dapat menggunakan SPI tersebut, sambil Router/VPN gateway Johor Bahru juga mengirimkan SPI miliknya sendiri ke Router/VPN gateway pusat. Router/VPN gateway pusat mengkonfirmasi SPI milik Router/VPN gateway Johor Bahru dan mengirimkan alamat dari host IP PBX pusat yang akan menggunakan IPSec SA. Router/VPN gateway Johor Bahru mengkonfirmasi ke Router/VPN gateway pusat bahwa dapat mendukung IPSec untuk IP PBX pusat dan sekaligus mengirimkan alamat IP PBX Johor Bahru ke Router/VPN gateway pusat. Router/VPN gateway pusat mengkonfirmasi ke Router/VPN gateway Johor Bahru bahwa dapat mendukung IPSec untuk IP PBX Johor Bahru dan mengirimkan atribut IPSec (umur SA dan algoritma enkripsi ke Router/VPN gateway Johor Bahru). Router/VPN gateway Johor Bahru memverifikasi bahwa atribut IPSec yang dikirimkan Router/VPN gateway pusat dan membangun pasangan SA IPSec (inbound dan outbound) untuk IP PBX Johor Bahru untuk berkomunikasi dengan IP PBX pusat. Router/VPN gateway pusat menerima konfirmasi atribut IPSec Johor Bahru dan membangun pasangan SA IPsec (inbound dan outbound) untuk IP PBX pusat untuk berkomunikasi dengan IP PBX Johor Bahru. Selanjutnya tunnel akan terbentuk. Untuk selanjutnya komunikasi data dari dan menuju masing-masing router/VPN gateway akan diproses enkripsi dan dekripsi data oleh masing-masing router/VPN gateway.

Proses tunneling yang sama terjadi pada pembentukan tunnel IPSec VPN antara router/VPN gateway pusat dengan router/VPN gateway di Davao City.

Implementasi Encapsulating Security Payload (ESP) pada paket IP seperti pada gambar berikut:



Gambar 5.8. Paket IP sebelum diimplementasikan ESP [1]



Gambar 8. Paket IPSec pada tunnel mode dengan ESP [1].

Seperti pada gambar 8, paket data suara dari host PABX menuju router/VPN gateway dalam bentuk paket TCP/IP, kemudian router/VPN gateway akan melakukan enkapsulasi dan enkripsi dengan protocol ESP IPSec sehingga paket data berubah seperti dalam bentuk gambar 3.12, dimana paket TCP/IP termasuk data payload dan header IP original akan dienkrip dan diberikan IP Header baru untuk paket IPSec yang akan dikirimkan menuju router/VPN gateway tujuan. Router/VPN gateway di tujuan, setelah menerima paket IPSec akan melakukan dekripsi sehingga bentuk paket data akan kembali seperti pada gambar 3.11, untuk selanjutnya disampaikan ke host yang dituju.

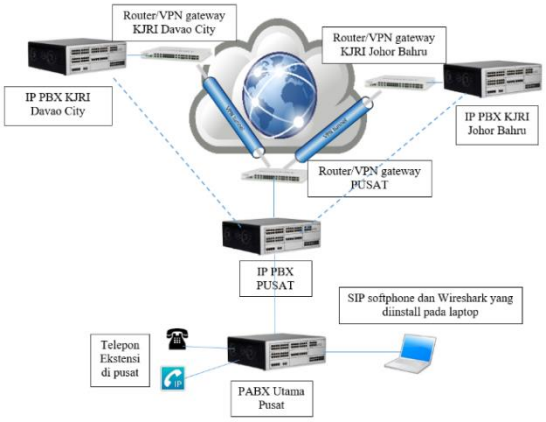
Setelah konfigurasi semua router/VPN gateway dilakukan, maka akan terbentuk tunnel koneksi IPsec VPN gateway-to-gateway antara pusat dengan KJRI Johor Bahru dan KJRI Davao City. Pada kondisi ini, IP PBX pusat dapat mengenali IP PBX di Johor Bahru dan IP PBX di Davao City seolah-olah berada pada jaringan lokal yang sama. Begitu pun sebaliknya, baik IP PBX di Johor Bahru maupun IP PBX Davao City mengenali IP PBX di pusat seolah-olah berada pada jaringan lokal yang sama. Sehingga IP PBX

pusat dapat berkomunikasi secara internal baik dengan IP PBX Johor Bahru maupun IP PBX Davao City, dan sebaliknya dari IP PBX Johor Bahru maupun dari IP PBX Davao City dapat berkomunikasi secara internal dengan IP PBX pusat.

Untuk saat ini sesuai kebijakan institusi, interkoneksi IP PBX antara KJRI Johor Bahru dan KJRI Davao City belum dibangun, sehingga komunikasi internal antara IP PBX di KJRI Johor Bahru dan KJRI Davao City belum dapat dilakukan.

2.7.4 Skema Pengambilan Data Pada Sistem

Untuk pengambilan data pada implementasi interkoneksi PABX berbasis IP dengan metode IPsec VPN ini, penulis menggunakan skema sistem sebagai berikut:



Gambar 9. Skema pengambilan data untuk komunikasi suara antar PABX berbasis IP

Pengambilan data dilakukan seperti pada gambar 9, dengan mengkonfigurasi SIP softphone yang dijalankan pada sebuah perangkat laptop yang terisntall aplikasi wireshark dan terkoneksi ke server PABX di kantor pusat melalui koneksi jaringan lokal pusat, sehingga dapat berkomunikasi secara internal ke semua nomor telepon ekstensi baik yang ada di pusat maupun di perwakilan.

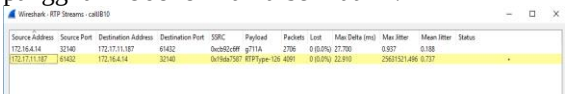
Untuk menguji parameter-parameter QoS, maka sebelum dilakukan pengambilan data koneksi komunikasi suara, pada laptop yang terinstall SIP softphone, dijalankan terlebih dahulu aplikasi wireshark yang akan mengambil data-data komunikasi yang dilakukan.

3. ANALISA DAN PEMBAHASAN.

Pada bab ini akan dijelaskan langkah-langkah analisis yang dilakukan untuk mengukur QoS jaringan pada parameter-parameter troughput, Delay, jitter dan packet loss pada jaringan interkoneksi IP PBX Kementerian Luar Negeri dan perwakilan RI.

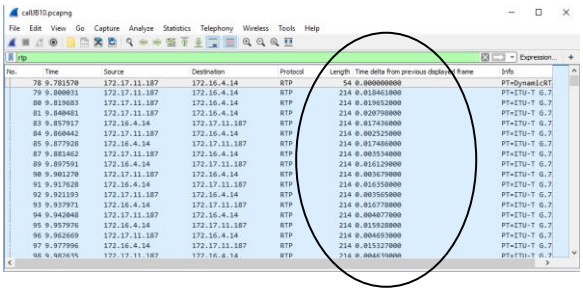
Pada proses analisis ini akan dilakukan /pengukuran parameter-parameter Qos yaitu: troughput, delay, jitter dan packet loss dalam hubungan komunikasi suara yang terjadi pada jaringan interkoneksi PABX berbasis IP yang menggunakan penerapan IPsec VPN gateway-to-gateway.

- Untuk mendapatkan nilai jitter dan packet loss dapat dilihat dari hasil pengukuran aplikasi wireshark seperti pada pengambilan data ke-10 panggilan ke Johor Bahru berikut ini:



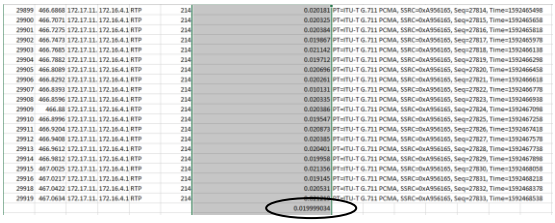
Gambar 10. Tampilan hasil pengukuran packet loss dan jitter pada wireshark

- Untuk mendapatkan hasil pengukuran delay dapat digunakan hasil dari parameter yang telah ditangkap oleh aplikasi wireshark seperti pada data panggilan ke-10 ke Johor Bahru berikut:



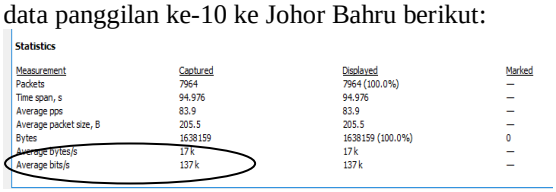
Gambar 11. Tampilan time delta pada wireshark untuk data panggilan ke-10 ke Johor Bahru

Untuk mengukur delay dapat dilakukan dengan menkonversikan tabel pada wireshark ke dalam tabel Microsoft Excel, kemudian diambil nilai rata-rata dari kolom time delta tersebut.



Gambar 12. Hasil konversi dari tampilan capture aplikasi wireshark ke dalam bentuk MS. Excel untuk data panggilan ke-10 ke Johor Bahru

- Untuk mendapatkan nilai pengukuran troughput, dapat digunakan hasil dari parameter yang telah ditangkap oleh wireshark seperti pada data panggilan ke-10 ke Johor Bahru berikut:



Statistics

Measurement	Captured	Displayed	Marked
Packets	7964	7964 (100.0%)	—
Time span, s	94.976	94.976	—
Average pps	83.9	83.9	—
Average packet size, B	205.5	205.5	—
Bytes	1638159	1638159 (100.0%)	0
Average bytes/s	17 k	17 k	—
Average bits/s	137 k	137 k	—

Gambar 13. Pengukuran troughput pada data panggilan ke-10 ke Johor Bahru.

Tabel 1. Hasil Pengukuran QoS untuk panggilan ke nomor ekstensi Pusat 3405:

No	Analisa Kerja	Waktu percakapan	Durasi	Troughput	Delay (ms)	Jitter (ms)	Packet Loss (%)
1	Panggilan 1	14:17 WIB	00:05:08	153 kbps	19 ms	0,78 ms	0 %
2	Panggilan 2	14.36 WIB	00:10:16	77 kbps	20 ms	0,44 ms	0 %
3	Panggilan 3	14:39 WIB	00:08:14	157 kbps	19,99 ms	0,60 ms	0 %
4	Panggilan 4	14:56 WIB	00:03:49	283 kbps	19,99 ms	0,50 ms	0 %
5	Panggilan 5	15:30 WIB	00:04:51	164 kbps	20 ms	0,46 ms	0 %
6	Panggilan 6	09.03 WIB	00:04:35	95 kbps	19,99 ms	0,49 ms	0 %
7	Panggilan 7	10.02 WIB	00:09:11	98 kbps	20 ms	0,51 ms	0 %
8	Panggilan 8	10.15 WIB	00:04:37	95 kbps	20 ms	0,47 ms	0 %
9	Panggilan 9	10:50 WIB	00:05:09	93 kbps	19,99 ms	0,49 ms	0 %
10	Panggilan 10	11.20 WIB	00:07:40	25 kbps	19,99 ms	0,48 ms	0 %

Tabel 2. Hasil Pengukuran QoS pada panggilan ke nomor ekstensi di KJRI Johor Bahru 115:Cara dial: *560494, setelah ada voice greeting tekan ext. 115

No	Analisa Kerja	Waktu percakapan	Durasi	Troughput	Delay (ms)	Jitter (ms)	Packet Loss (%)
1	Panggilan 1	10:22 WIB	00:06:28	126 kbps	32,676 ms	2,776 ms	0 %
2	Panggilan 2	13:12 WIB	00:09:45	99 kbps	19,992 ms	0,494 ms	0 %
3	Panggilan 3	13:51 WIB	00:05:27	128 kbps	19,977 ms	0,47 ms	0 %
4	Panggilan 4	15:07 WIB	00:07:01	133 kbps	19,989 ms	0,485 ms	0 %
5	Panggilan 5	15:30 WIB	00:03:48	116 kbps	19,984 ms	0,462 ms	0 %
6	Panggilan 6	09:10 WIB	00:07:29	217 kbps	20,711 ms	0,447 ms	0 %
7	Panggilan 7	09.20 WIB	00:03:08	145 kbps	19,996 ms	0,492 ms	0 %
8	Panggilan 8	09.45 WIB	00:03:25	77 kbps	19,995 ms	0,466 ms	0 %
9	Panggilan 9	10:02 WIB	00:03:57	113 kbps	19,996 ms	0,491 ms	0 %
10	Panggilan 10	16:00 WIB	00:03:10	137 kbps	19,997 ms	0,463 ms	0 %

Tabel 3. Hasil Pengukuran QoS pada panggilan ke nomor ekstensi di KJRI Davao City 63206:
Cara dial: *563206

No	Analisa Kerja	Waktu percakapan	Durasi	Troughput	Delay (ms)	Jitter (ms)	Packet Loss (%)
1	Panggilan 1	08.38	00:10:15	533 Kbps	25,263 ms	0,585 ms	44,1 %
2	Panggilan 2	09:05	00:06:10	135 Kbps	25,939 ms	0,456 ms	43,05 %
3	Panggilan 3	10:15	00:04:35	144 Kbps	14,288 ms	0,451 ms	0 %
4	Panggilan 4	10:35	00:03:40	491 Kbps	13,933 ms	0,452 ms	0 %
5	Panggilan 5	11:05	00:04:03	128 Kbps	15,226 ms	0,437 ms	0 %
6	Panggilan 6	13:15	00:04:10	217 Kbps	12,671 ms	0,489 ms	47,35 %
7	Panggilan 7	13:45	00:03:24	132 Kbps	13,486 ms	0,449 ms	0 %
8	Panggilan 8	14:05	00:04:55	114 Kbps	15,396 ms	0,458 ms	0 %
9	Panggilan 9	14:25	00:03:45	123 Kbps	14,382 ms	0,479 ms	0 %
10	Panggilan 10	14:45	00:04:20	135 Kbps	25,555 ms	0,422 ms	43,75 %

Pada Tabel 1, 2. dan Tabel 3 di atas menunjukkan hasil pengukuran dan perhitungan troughput, delay, jitter dan packet loss yang diperoleh dari data-data yang ditangkap laptop yang terinstall wireshark dan SIP softphone yang melakukan panggilan ke nomor ekstensi pusat dan nomor ekstensi perwakilan. Panggilan yang dilakukan sebanyak masing-masing 10 kali dengan durasi sekitar tiga sampai sepuluh menit menghasilkan nilai dengan selisih yang tidak terlalu besar baik itu untuk panggilan ke ekstensi di pusat maupun ke nomor ekstensi di perwakilan. Dapat dilihat bahwa hasil pengukuran software wireshark pada pada komunikasi data yang dilakukan seperti pada tabel berikut:

Tabel 4

Tabel 4. Perbandingan hasil pengukuran QoS untuk pemanggilan nomor ekstensi pusat dan nomor ekstensi perwakilan:

No	Jenis pengukuran	Troughput	Delay	Jitter	Packet Loss	Keterangan QoS
1	Pemanggilan nomor ekstensi pusat	25 – 283 Kbps	19 – 20 ms	0,46 – 0,78 ms	0 %	
2	Pemanggilan Nomor ekstensi perwakilan KJRI Johor Bahru	77 – 217 Kbps	19 – 32 ms	0,46 – 2,78 ms	0 %	Delay kategori bagus (standar ITU) Packet loss kategori bagus sekali (standar Typhon)
3	Pemanggilan Nomor ekstensi perwakilan KJRI Davao City	123 – 533 Kbps	12,671 – 25,939 ms	0,422 – 0,585 ms	Rata-rata 13,09%	Delay kategori bagus (standar ITU) Packet loss kategori sedang (standar Typhon)

Dengan melihat hasil yang diperoleh dapat dikatakan bahwa hasil pengukuran dan perhitungan pada nilai delay yang didapat baik untuk pemanggilan ke nomor ekstensi pusat maupun nomor ekstensi perwakilan berada pada kategori yang diperbolehkan (bagus), sesuai dengan standar ITU-T (International Telecommunication Union). Sedangkan nilai packet loss dari hasil pengukuran berada pada kategori (sangat bagus) untuk percobaan pemanggilan ke ekstensi pusat dan ekstensi Johor Bahru, dan berada pada kategori (sedang) ke ekstensi Davao City, berdasarkan standar Tiphon (*Telecommunications and Internet Protocol Harmonization Over Networks*).

Tabel 5. Kategori Besar Delay Berdasarkan Standar ITU-T.

Kategori Delay	Besar Delay
Sangat Bagus	< 9 ms
Bagus	9 s/d 50 ms
Jelek	51 s/d 450 ms
Sangat Jelek	>450 ms

Tabel 6. Kategori paket loss versi Tiphon

KATEGORI DEGREDASI	PACKET LOSS
Sangat bagus	0
Bagus	3 %
Sedang	15 %
Jelek	25 %

Pada komunikasi data yang dilakukan untuk menyampaikan pesan suara juga didapatkan nilai troughput yang terjadi tidak terlalu besar yaitu antara 25 – 283 kbps untuk komunikasi ke perwakilan Johor Bahru, sedangkan untuk komunikasi ke Davao City antara 123 – 533 Kbps, dimana Bandwidth yang disediakan masih sangat mencukupi untuk komunikasi suara pada interkoneksi IP PBX.

Dari hasil pengamatan yang telah dilakukan dapat dikatakan bahwa implementasi jaringan PABX berbasis IP dengan menggunakan metode IP Sec VPN yang dibangun antara kantor pusat Kementerian Luar Negeri dan perwakilan KJRI Johor Bahru dan KJRI Davao City dapat diimplementasikan dengan baik dan memiliki kualitas layanan yang relatif bagus.

4. SIMPULAN

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

- Komunikasi suara dapat dilakukan dengan baik antara PABX pusat dan perwakilan, sehingga jaringan interkoneksi PABX berbasis IP menggunakan metode IPsec VPN gateway antara Kementerian Luar Negeri dengan perwakilan Indonesia, KJRI Johor Bahru di Malaysia dan KJRI Davao City di Filipina dapat diimplementasikan dengan baik.
- Jaringan IPSec VPN gateway digunakan untuk menghubungkan jaringan lokal di pusat dengan jaringan lokal di perwakilan, sehingga masing-masing PABX berbasis IP dapat berkomunikasi secara internal.
- Nilai pengukuran delay Komunikasi suara melalui jaringan interkoneksi PABX berbasis IP menggunakan IPSec VPN sesuai dengan skema simulasi sistem pada saat pengujian menunjukkan nilai 19 – 32 ms untuk komunikasi ke Johor Bahru, dan untuk komunikasi ke Davao City menunjukkan nilai 12,671 – 25,939 ms, oleh karena itu nilai delay pada layanan komunikasi suara berada pada kategori (bagus) sesuai standar dari ITU-T (International Telecommunication Union).
- Nilai pengukuran packet loss dari hasil pengukuran menunjukan nilai 0% untuk komunikasi ke ekstensi Johor Bahru, sehingga berada pada kategori (sangat bagus) berdasarkan standar Tiphon (Telecommunications and Internet Protocol Harmonization Over Networks). Sedangkan untuk komunikasi ke Davao City berada pada rata-rata 13,09 %, sehingga berada pada kategori (sedang).
- Dengan kualitas suara percakapan yang jelas, maka performansi komunikasi suara pada interkoneksi PABX berbasis IP melalui jaringan IPsec VPN ini menunjukan kualitas yang cukup baik.
- Pada saat komunikasi suara dilakukan dimana pada saat ujicoba baik pada waktu pagi maupun siang hari tidak menunjukan perbedaan yang signifikan, dengan nilai troughput yang didapat pada pengukuran antara 25 – 533 kbps, oleh karena itu Kondisi trafik tidak terlalu mempengaruhi kualitas layanan.

DAFTAR PUSTAKA

1. Ardiyansyah, Bambang. 2008. Keamanan Jaringan Komputer Implementasi IPSec pada VPN. Palembang: Universitas Sriwijaya.
2. Arlan, Reza, Trendy Munadi, dan Nur Andini. 2016. Implementasi dan Analisis Sistem Keamanan IP Security (IPSEC) di dalam Multi Protocol Label Switching-Virtual Private Network (MPLS-VPN). E-Proceeding of Engineering. Vol.3 No.3, Desember 2016. ISSN 2355-9365. Bandung: Universitas Telkom.
3. Chappel, Laura. 2012. Wireshark Network Analysis, The Official Wireshark Certified Network Analyst Study Guide. Protocol Analysis Institute. Dba. Chappel University.
4. Gatot S. 2009. Analisa Perbandingan QoS: Pengaruh Implementasi Enkripsi 3DES dan AES pada MPLS-VPN untuk Layanan IP-Based Video Telephony. Jakarta: Universitas Indonesia.
5. Ismail, Firza, Rendy Munadi, dan Asep mulyana. 2013. Analisis Implementasi Interkoneksi IP PBX Panasonic, IP PBX Siemens, dan Server Trixbox, Untuk Layanan VoIP. Bandung: Universitas Telkom.
6. Kerta, Johan Muliadi dkk. 2010. Analisa dan Perancangan Jaringan Berbasis VPN pada PT. Finroll. Comtech. Vol.1 No.2, Desember 2010: ISSN 737 – 748. Jakarta: Bina Nusantara University.
7. Khuluq, Husnul dkk. 2016. Implementasi VoIP (Voice Over Internet Protocol) Server Berbasis Raspberry PI Sebagai Media Komunikasi. Jurnal Ilmiah Edutic. Vol.3 No. 1, November 2016. E-ISSN 2528-7303. Gresik: Sekolah Tinggi Teknik Qomaruddin.
8. Munadi, Rendy. 2011. Teknik Switching. Bandung: Informatika.
9. Pratama, I Putu Agus Eka. 2015. Handbook Jaringan Komputer. Bandung: Informatika.
10. Sofana, Iwan. 2015. Membangun Jaringan Komputer. Bandung: Informatika.
11. Warman, Indra dan Johari Maknun. 2014. Implementasi Voice Over Internet Protocol (VoIP) IP Phone Sebagai Media Komunikasi Pengganti Private Automatic Branch Exchange (PABX). Padang: Institut Teknologi Padang.

ISSN : 1410 - 7104