Perbandingan Kinerja Virtual Private Network Antara Vpn *Tunnel* Dan *Internet Protocols Security*

Tamsir Ariyadi[1], Muhamad Agung Prabowo[2]
Teknik Komputer, Universitas Bina Darma Palembang[1,2]
Jalan Ahmad Yani No. 03 Plaju Palembang Sumatera Selatan, Indonesia
E-mail: tamsirariyadi@binadarma.ac.id[1], muhammadagungprabowo@gmail.com[2]

Abstract – The need for communication in supporting inter-company interactions is very closely related to the development of information technology through computer networks. Virtual Private Network or commonly called VPN has an important role in the development of security systems in the internet network, especially in restricting access rights to servers, databases, and the like in minimizing the onsany access to important corporate data. VPNs have some wrong types such as VPN Tunnel and IPSec, VPN Tunnel has a simpler concept compared to IPSec because it can connect servers and clients remoteaccess that only requires 1 router connected on the server side. IPSec has a higher level of security compared to VPN Tunnels with communication lines equipped with cryptography. IPSec running on L2TP has a better level of performance than VPN Tunnel based on the results that have been obtained, due to the concept that requires the router to be connected point-to-point.

Keywords - *Virtual Private Network* (VPN), *IPSec, Tunneling, Quality of Service, Peformance.*

Intisari – Dibutuhkannya komunikasi dalam menunjang interaksi antar perusahaan yang memiliki kaitan yang sangat erat terhadap perkembangan teknologi informasi melalui jaringan komputer. *Virtual Private Network* atau biasa disebut VPN memiliki peran penting dalam perkembangan sistem keamanan dalam jaringan internet, terutama dalam membatasi hak akses terhadap *server, database*, dan sejenisnya dalam meminimalisir terjadinya akses illegal terhadap data-data penting perusahaan. VPN memiliki beberapa tipe salah seperti VPN *Tunnel* dan IPSec, VPN *Tunnel* memiliki konsep yang lebih sederhana dibandingkan dengan IPSec karena dapat menghubungkan *server* dan *client* secara *remoteaccess* yang hanya membutuhkan 1 *router* saja yang terhubung pada sisi *server*. IPSec memiliki tingkat keamanan yang lebih tinggi dibandingkan dengan VPN *Tunnel* dengan jalur komunikasi dilengkapi dengan kriptografi. IPSec yang berjalan pada L2TP memiliki tingkat kinerja yang lebih baik dibandingkan VPN *Tunnel* berdasarkan hasil yang telah di dapatkan, karena konsep yang mengharuskan *router* terkoneksi secara *point-to-point.*

Kata Kunci - *Virtual Private Network (VPN), IPSec, Tunneling, Quality of Service, Peformance.*

I. PENDAHULUAN

Kebutuhan jaringan dan komunikasi data dalam mendukung interaksi antar perusahaan tentu saja memiliki kaitan yang sangat erat terhadap perkembangan teknologi informasi melalui jaringan komputer. Umumnya pada era saat ini, beberapa perusahan bahkan hampir seluruh perusahaan menerapkan sistem hosting yang memanfaatkan pihak ketiga untuk berinteraksi maupun mengirimkan akses data kepada kantor cabang yang dimiliki oleh perusahaan. Dari uraian di atas timbul pertanyaan tentang bagaimana cara agar perusahaan dapat langsung memberikan akses secara langsung ke kantor cabang tanpa *project management,* menggunakan pihak ketiga. Setelah mencari informasi dari beragai sumber, hal ini dapat dilakukan dengan menerapkan teknologi *Virtual Private Network (VPN)* pada jaringan. Menurut *Internet Engineering Task* Force (IETF) VPN adalah sebuah tiruan dari

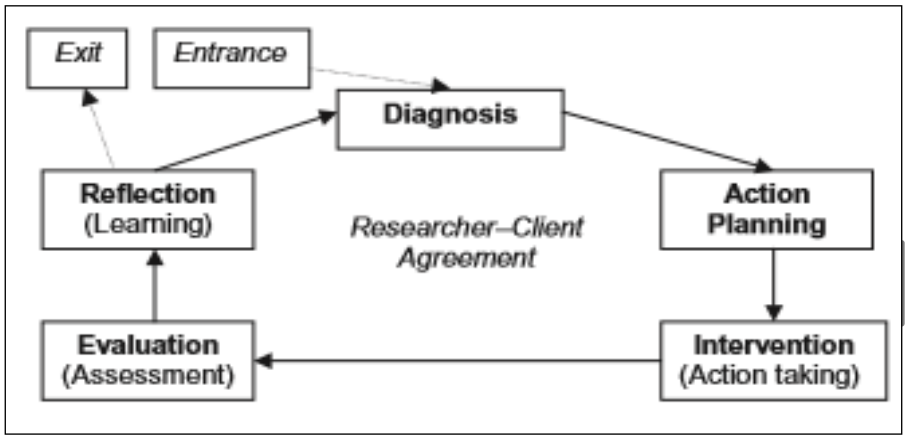
Private Wide Area Network (WAN) yang menggunakan fasilitas IP Public seperti Internet atau IP private dari Backbone. Terdapat beberapa jenis dari VPN yang dapat diterapkan, seperti *Point to Point Tunneling Protocol (PPTP), Layer 2 Transfer Protocol (L2TP), Internet Protocol Security (IPSec), Secure Socket Tunneling Protocol (SSTP)*, dan SSL.[1]

Beberapa jenis VPN berikut, penulis melakukan penelitian dengan mengambil VPN *tunneling* pada layer 2 dan *IPSec* pada layer 3 sebagai objek untuk dilakukan perbandingan kinerja dengan mengukur performa keduanya dengan menggunakan metode *Ouality of Service (QoS)*, seperti *delay*, *jitter, packet loss*, dan*throughput,* untuk mengetahui mana yang terbaik. Namun sebelum itu kita ketahui dulu apa definisi dari VPN *tunnelling* dan IPSec. Menurut Joko Triyono (*Tunneling* merupakan metode untuk *transferdata* dari sebuah *multicast* paket yang di enkapsulasi dengan metode *unicast* yang dikirim dari satu jaringan ke jaringan yang lain dengan memanfaatkan jaringan internet terselubung. Sedangkan *IPSec*, menurut Nurkholis Madjid (2006) adalah sebuah *framework* standar terbuka yang dikembangkan oleh *Internet Engineering Task Force* (*IETF*)yang menyediakan keamanan untuk transmisi informasi yang bersifat sensitive melalui jaringan, berfungsi untuk melindungi dan melakukan otentifikasi paket IP antara perangkat *IPSec* (*peer*). [2][3]

Untuk melakukan penelitian penulis akan membangun sebuah Briset sendiri yang berlokasi di lab yang menggunakan *Fiber Optic*. B Riset ini sendiri dilengkapi dengan perangkat seperti Router Mikrotik yang dapat digunakan untuk mendukung penelitian. Masing-masing memiliki IP *Public* yang sudah ditentukan karena dibutuhkan setidaknya 2 IP *Public* yang akan digunakan untuk membangun *Virtual Private Network* itu sendiri.

II. SIGNIFIKANSI STUDI

Tahapan penelitian ini akan dijabarkan, supaya penelitian berjalan secara sistematis dan terarah sesuai. Agar rencana yang dilakukan mendapatkan hasil yang baik dan outputnya bisa menjadi rujukan penelitian selanjutnya. Dalam melakukan penelitian menggunakan beberapa langkah yaitu Melakukan Diagnosa, Membuat Rencana Tindakan, Melakukan Tindakan, Melakukan Evaluasi dan Melakukan Pembelajaran.



Gambar 1. Tahapan Penelitian

Dalam hal melakukan kajian setiap langkah maka metode yang digunakan adalah penelitian tindakan (*Action Research*). Penelitian tindakan merupakan penelitian pada upaya pemecahan masalah atau perbaikan yang dirancang menggunakan penelitian tindakan (*classroom action research*) yang bersifat reflektif dan kolaboratif. Prosedur pelaksanaan penelitian tindakan berupa susatu siklus yang setiap langkah nya terdiri dari lima tahap, yaitu diagnosa, perencanaan, tindakan, observasi dan refleksi [4].
Adapun tahapannya sebagai berikut

A. Melakukan Diagnosa

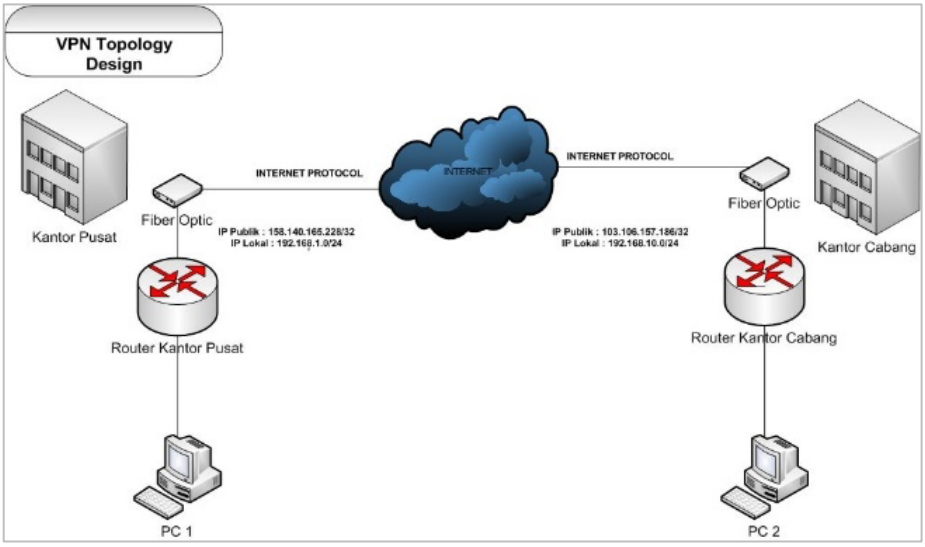
Berdasarkan penelitian sebelumnya oleh Dessyanto Boedi yang berjudul "Perbandingan Kinerja IPSec dan SSL"**.** Penelitian ini menjelaskan secara teori deskriptif tentang bagaimana cara kerja *IPSec* dan juga *SSL VPN* pada jaringan. Adapun parameter yang menjadi titik perbandingan yaitu berdasarkan Algoritma Autentifikasi, Metode Autentifikasi, *MAC, Mode* Koneksi, *Remote Access*, Kriptografi, dan lain sebagainya.[5]

Kemudian pada tahap ini penulis melakukan diagnosa dengan melakukan identifikasi terhadap kedua jenis VPN agar dapat menentukan pokok dan pemecahan masalah terhadap objek yang diteliti, berdasarkan data awal yang telah penulis dapatkan, VPN memiliki beberapa jenis yang dapat diterapkan salah satunya adalah VPN *Tunnel* dan IPSec. Dapat disimpulkan bahwa kedua jenis VPN memiliki cara kerja, algoritma, dan enkripsi yang berbeda, namun memiliki tujuan yang sama yaitu membuat suatu jaringan khusus melalui jaringan umum seperti internet, kedua VPN ini juga dapat diterpkan ke dalam beberapa tipe sama seperti *remote access* VPN , dan *site-to-site* VPN.

Pokok permasalahannya adalah bagaimana kita dapat mengetahui kekurangan dan kelebihan dari kedua VPN tersebut dan mana yang lebih baik, agar dapat menentukan jenis VPN yang sesuai kebutuhan. Setelah melakukan diagnosa dengan mengidentifikasi kedua jenis VPN tersebut, hal ini dapat diketahui dengan melakukan pengujian dalam segi kinerja atau peforma pada tiap VPN dalam mengirimkan paket data antara *server* dan *client* dalam jaringan VPN tersebut, dengan cara melakukan pengukuran QoS berdasarkan 4 parameter yaitu, *throughput, delay, packet loss,* dan *jitter*. Hasil dari pengukuran tersebut dapat dilakukan perbandingan untuk mengetahui kekurangan dan kelebihan dari masing-masing VPN berdasarkan 4 parameter yang terdapat pada QoS, baik itu dari segi *thorughput, delay, packet loss,* maupun *jitter*.

B. Membuat Rencana Tindakan

Pada tahap ini penulis menyusun rencana tindakan (*planning*) sebelum masuk ke tahap selanjutnya yaitu *action taking* mengenai hal-hal apa saja yang akan dilakukan untuk membangun jaringan VPN, baik itu VPN *Tunnel* dan juga IPSsec. Adapun tindakan yang akan dilakukan yaitu, melakukan desain perancangan topologi dan menentukan alat dan bahan yang dibutuhkan.



Gambar 2. Desain Topologi

Pada gambar 2 adalah topologi atas, terdapat 2 *router* yang akan berfungsi menjadi *server* dan *client* VPN dari masing-masing kantor yang terhubung melalui *Fiber Optic* dan memiliki IP Publik sendiri yang langsung terhubung ke jaringan internet. Kantor Pusat memiliki IP Publik 158.140.165.228/32 dengan *network* IP Lokal 192.168.1.0/24. Sedangkan Kantor Cabang memiliki IP Publik 103.106.157.186/32 dengan *network* IP Lokal 192.168.10.0/24.

C. Melakukan Tindakan

Pada tahap ini penulis melakukan konfigrasi sebelum menuju ke tahap simulasi. Berikut ini beberpa tindakan yang dilakukan sebelum melakukan simulasi, adapun sebagai berikut:

a) Menghubungkan Router ke jaringansebelum melakukan tahap konfigurasi, dengan menghubungkan *router* mikrotik ke modem ISP dan juga ke dalam jaringan lokal atau jaringan LAN.
b) Melakukan konfigurasi dasar pada mikrotik agar dapat terhubung ke jaringan WAN maupun LAN.
c) Melakukan konfgurasi VPN pada mikrotik dalam upaya membangun sebuah jaringan VPN baik dari *server* maupun *client*.

D. Melakukan Evaluasi

Setelah jaringan VPN berhasil dikonfigurasi, dan *client* VPN sudah bisa mengakses jaringan VPN ke *server*, maka langkah selanjutnya adalah masuk ke tahap evaluasi, dengan melakukan pengukuran QoS terhadap jaringan VPN menggunakan *software* yang telah ditentukan.

E. Melakukan Pembelajaran

Setelah melakukan pengukuran yang dilakukan selama beberapa hari berdasarkan parameter yang ada pada *QoS*. Tahap perbandingan ini akan disajikan atau dipaparkan dalam bentuk tabel perbandingan, di mana akan terlihat sisi kekurangan dan kelebihan dari kedua jenis VPN tersebut.

F. Pengukuran dengan QoS

Pengukuran yang digunakan dalam penelitian ini adalah *Quality of Service (QoS)*. Qos adalah kemampuan suatu jaringan dalam menyediakan layanan yang baik dengan menyediakan bandwidth, mengatasi jitter dam delay. Adapun parameter dalam *QoS* adalah *throughput, delay, packet loss*, dan *jitter*.[6] Adapun parameter dalam *QoS* sebagai berikut:

1) *Throughput*
   Merupakan kecepatan (*rate*) transfer data efektif, yang di ukur dalam bps. *Throughput* juga merupakan jumlah total kedatangan paket yang sukses yang diamati pada tujuan selama interval waktu tertentu dibagi oleh durasi interval waktu tersebut.
2) *Delay*
   Delay adalah waktu yang dibutuhkan data untuk menempuh jarak dari *client* ke VPN Server dan sebaliknya. *Delay* dapat dipengaruhi oleh jarak, media fisik kongesti atau juga waktu proses lama.
3) *Packet Loss*
   Jumlah total paket yang hilang atau yang disebut *packet loss.* Hal dapat terjadi karena *collision* dan *congestion* pada jaringan selama pengiriman paket data.
4) *Jitter*
   Jitter merupakan variasi-variasi dalam panjangnya antrian, dalam waktu pengolahan data dan juga dalam waktu penghimpunan ulang paket-paket diakhir perjalanan*jitter. Jitter* lazimnya disebut variasi *delay.*

G. Virtual Private Network (VPN)

Teknologi *Virtual Private Network* (VPN) merupakan sebuah fungsi *logic* dari *switch*, yaitu sebuah fungsi yang dikonfigurasi menggunakan *software*. VPNmemungkinkan koneksi jarak jauh (*remote access*) yang aman dengan menggunakan jaringan internet untuk akses ke LAN di kantor.

1. VPN Tunel

Teknologi *tunneling* adalah teknologi yang bertugas menangani dan menyediakan koneksi *point-to-point* dari sumber sampai ke tujuannya.Mengapa disebut *tunnel,*karena *point-to-point* ini sebernarnya berjalan menggunakan jaringan internet umum, namun koneksi tersebut tidak memperdulikan paket-paket yang melintasi jaringan yang sama, karena koneksi *point-to-point* membangun jaringan sendiri di dalam jaringan umum untuk dilalui, sehingga hanya dapat dilalui oleh si pembuat koneksi tersebut [7] [8].

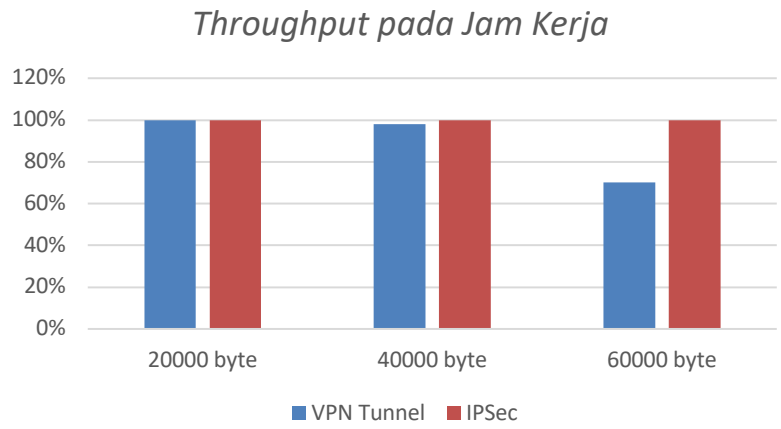
2. Internet Protocol Security (IPSec)

IPSec adalah sekumpulan daripada protokol yang membantu dalam melindungi komunikasi melalui jaringan IP. IPSec protokol bekerja bersamaan dalam variasi kombinasi yang menyediakan keamanan untuk berkomunikasi. Protokol IPsec adalah tambahan ke IP yang memungkinkan mengirim dan menerima paket Internet yang dilindungi secara kriptografi. Header IPsec khusus mengidentifikasi jenis perlindungan kriptografi yang diterapkan pada paket dan termasuk informasi lain yang diperlukan untuk *decoding* dari paket yang dilindungi [9][10][11].

III. HASIL DAN PEMBAHASAN

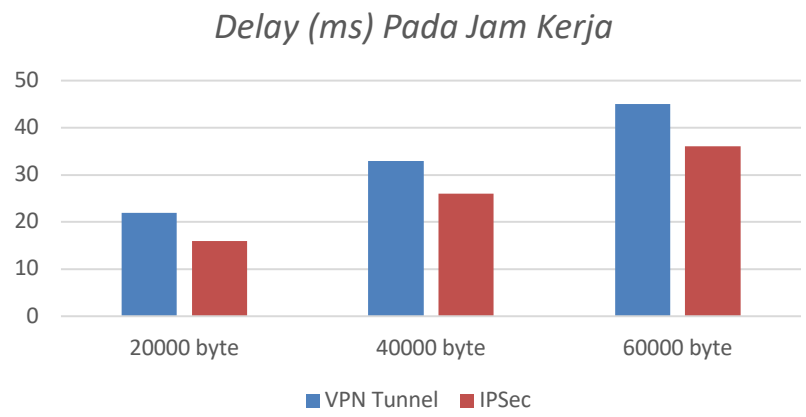
A. Hasil

Pengukuran ini dilakukan secara bertahap dimana tahap pertama dengan besaran data 20000 byte/s, tahap kedua 40000 byte/s, dan tahap ketiga 60000 byte/s. Waktu pengukuran ini terbagi ke dalam 2 bagian yaitu pengukuran pada jam kerja dan pengukuran diluar jam kerja. Tiap bagian pengukuran dapat memakan waktu kurang lebih 3-4 jam.



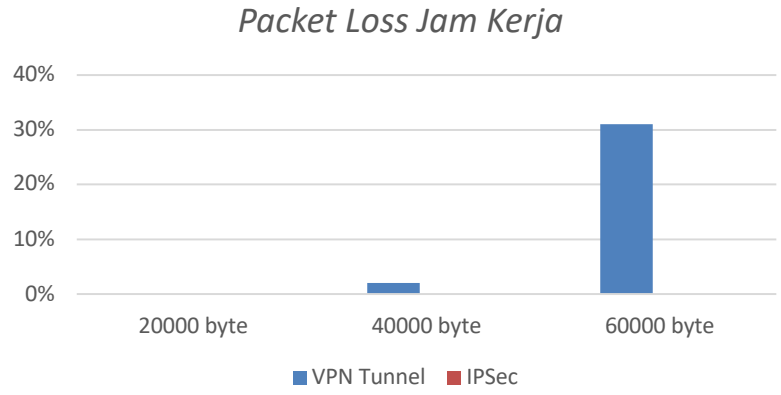
Gambar 3. Throughput pada jam kerja

Berdasarkan gambar 3 dapat dilihat pada uji coba tahap pertama dengan ukuran paket 20000 byte/s kedua VPN memiliki nilai persentase *throughput* yang sama yaitu 100%. Sedangkan untuk tahap yang kedua dengan ukuran paket 40000 byte/s IPSec lebih unggul dengan persentase 100% sedangkan *Tunnel* dengan persentase 98%. Sedangkan untuk tahap ketiga 60000 byte/s IPSec lebih unggul dengan persentase 100% sedangkan *Tunnel* 70%.



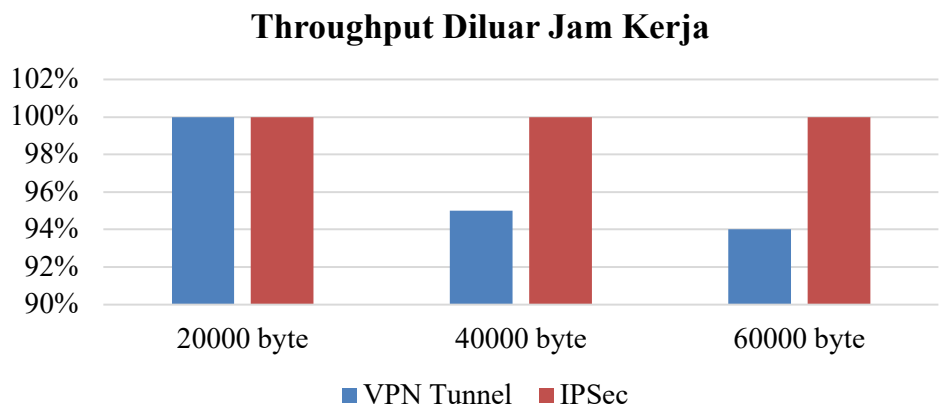
Gambar 4. Delay pada jam kerja

Berdasarkan gambar 4 dapat dilihat pada uji coba tahap pertama dengan ukuran paket 20000 byte/s VPN *Tunnel* memiliki waktu *delay* yang lebih lama selama 22 ms, sedangkan IPSec memiliki waktu selama 16 ms. Sedangkan untuk tahap yang kedua dengan ukuran paket 40000 byte/s VPN *Tunnel* memiliki waktu *delay* yang lebih lama selama 33 ms, sedangkan IPSec memiliki waktu *delay* selsama 26 ms. Sedangkan untuk tahap ketiga dengan ukutan paket 60000 byte/s VPN *Tunnel* memiliki waktu *delay* yang lebih lama selama 45 ms, sedangkan IPSec memiliki waktu *delay* selama 36 ms.



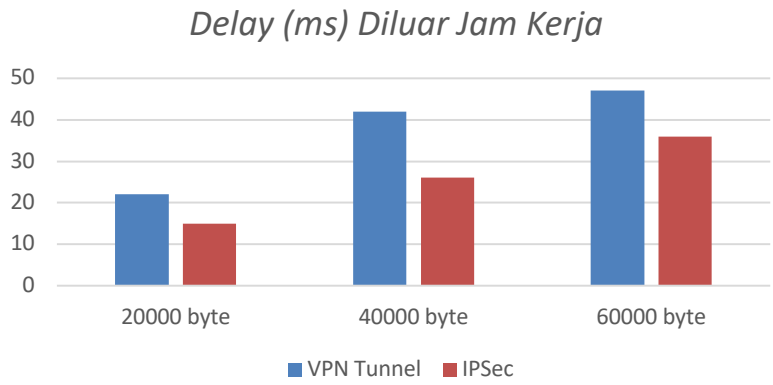
Gambar 5. Packet Loss pada jam kerja

Berdasarkan gambar 5 pada tahap pertama dengan ukuran paket 20000 byte/s kedua VPN sama-sama memiliki persentase kehilangan paket sebesar 0% dengan kata lain, paket yang berhasil diterima memiliki persentase 100%. Sedangkan untuk tahap kedua dengan ukuran paket sebesar 40000 byte/s VPN *Tunnel* memiliki persentase kehilangan sebesar 2%, sedangkan IPSec memiliki persentase 0%. Untuk tahap ketiga dengan ukuran paket 60000 byte/s VPN *Tunnel* memiliki persentase kehilangan paket 31%, sedangkan IPSec memiliki persentase 0%.



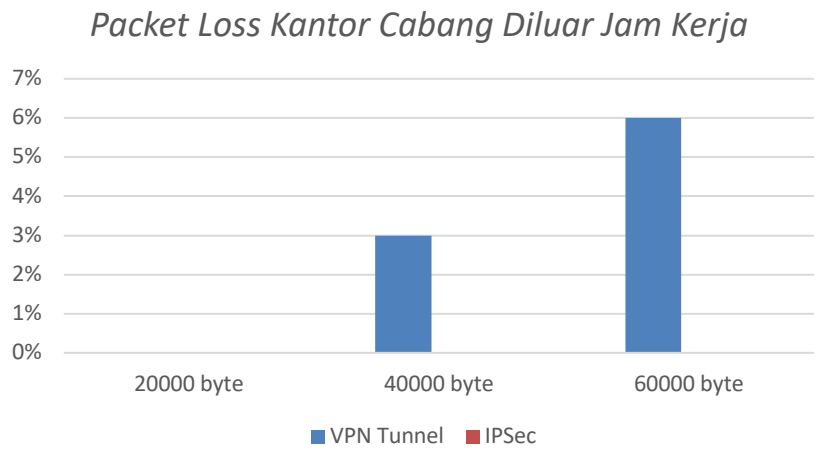
Gambar 6. Throughput diluar jam kerja

Berdasarkan gambar 6 dapat dilihat pada uji coba tahap pertama dengan ukuran paket 20000 byte/s kedua VPN memiliki nilai persentase *throughput* yang sama yaiu 100%. Sedangkan untuk tahap yang kedua dengan ukuran paket 40000 byte/s IPSec lebih unggul dengan persentase 100% sedangkan *Tunnel* dengan persentase 95%. Sedangkan untuk tahap ketiga 60000 byte/s IPSec lebih unggul dengan persentase 100% sedangkan *Tunnel* 94%.



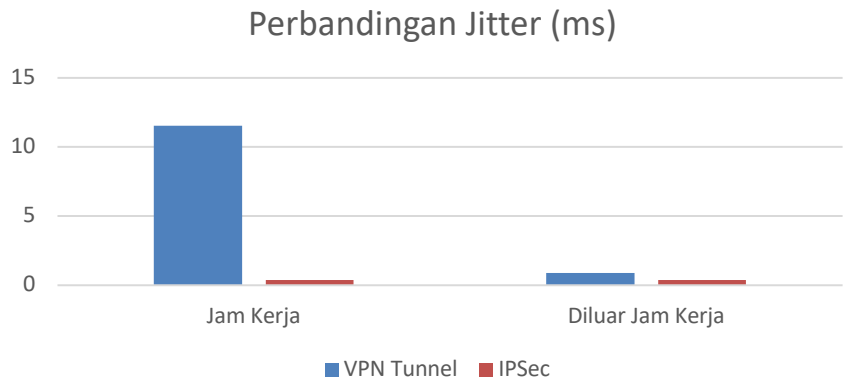
Gambar 7. Delay diluar jam kerja

Berdasarkan gambar 7 dapat dilihat pada uji coba tahap pertama dengan ukuran paket 20000 byte/s VPN *Tunnel* memiliki waktu *delay* yang lebih lama selama 22 ms, sedangkan IPSec memiliki waktu selama 15 ms. Sedangkan untuk tahap yang kedua dengan ukuran paket 40000 byte/s VPN *Tunnel* memiliki waktu *delay* yang lebih lama selama 42 ms, sedangkan IPSec memiliki waktu *delay* selama 26 ms. Sedangkan untuk tahap ketiga dengan ukutan paket 60000 byte/s VPN *Tunnel* memiliki waktu *delay* yang lebih lama selama 47 ms, sedangkan IPSec memiliki waktu *delay* selama 36 ms.



Gambar 8. Packet Loss diluar jam kerja

Berdasarkan gambar 8 pada tahap pertama dengan ukuran paket 20000 byte/skedua VPN sama-sama memiliki persentase kehilangan paket sebesar 0% dengan kata lain, paket yang berhasil diterima memiliki persentase 100%. Sedangkan untuk tahap kedua dengan ukuran paket sebesar 40000 byte/s VPN *Tunnel* memiliki persentase kehilangan sebesar 3%, sedangkan IPSec memiliki persentase 0%. Untuk tahap ketiga dengan ukuran paket 60000 byte/s VPN *Tunnel* memiliki persentase kehilangan paket 6%, sedangkan IPSec memiliki persentase 0%.

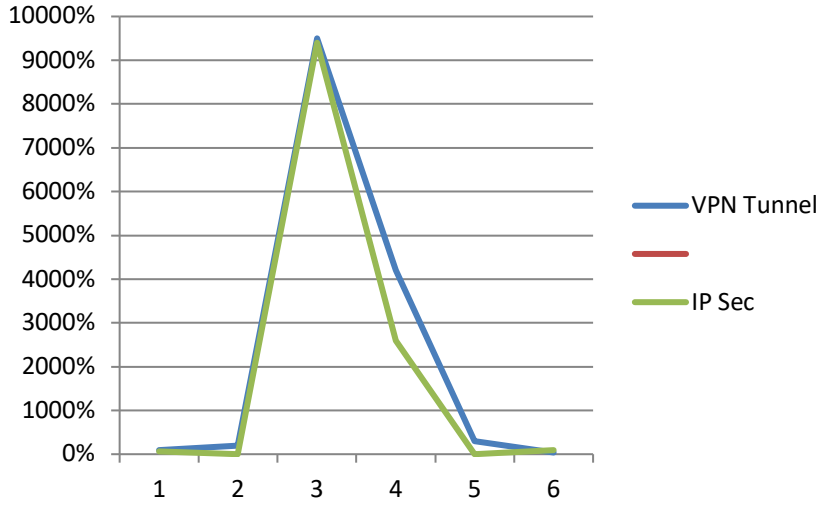


Gambar 9. Perbandingan Jitter

Berdasarkan gambar 9 dapat dilihat bahwa pada jam kerja IPSec memiliki waktu *jitter* yang lebih cepat selama 0,393 ms, sedangkan VPN *Tunnel* memiliki waktu *jitter* yang lebih lama selama 11,558 ms. Untuk diluar jam kerja IPSec juga memiliki waktu yang lebih cepat selama 0,383 ms , sedangkan VPN *Tunnel* memiliki waktu selama 0,909 ms. Dapat ditarik kesimpulan secara peforma berdasarkan *jitter* IPSec memiliki kinerja yang lebih cepat dibandingkan VPN *Tunnel*, baik.

B. Pembahasan

Perbandingan yang telah dilakukan dengan metode Quality of Service (QoS) pada gambar 10 terlihat bahwa IPSec memiliki tingkat keamanan yang lebih tinggi dibandingkan dengan VPN *Tunnel* dengan jalur komunikasi dilengkapi dengan kriptografi.



Gambar 10. Perbandingan antara VPN Tunnel dan IP Sec

IV. KESIMPULAN

Dari hasil perbandingan data yang telah dipaparkan, maka VPN *Tunnel* memiliki konsep yang lebih sederhana dibandingkan dengan IPSec karena dapat menghubungkan *server* dan *client* secara *remoteaccess* yang hanya membutuhkan 1 *router* saja yang terhubung pada sisi *server*. IPSec memiliki tingkat keamanan yang lebih tinggi dibandingkan dengan VPN *Tunnel* dengan jalur komunikasi dilengkapi dengan kriptografi. IPSec yang berjalan pada L2TP memiliki tingkat kinerja yang lebih baik dibandingkan VPN *Tunnel* berdasarkan hasil yang telah di dapatkan, karena konsep yang mengharuskan *router* terkoneksi secara *point-to-point* dengan kata lain, tidak bisa dimasuki oleh jaringan lain selain kedua *router* tersebut yang telah di daftarkan secara *point-to-point* dari sisi *client* maupun *server.*

REFERENSI

[1] Wijaya, Hendar. 2011. Belajar Sendiri Cisco DSL Router, ASA Firewall, dan VPN. Jakarta, Elex Media Komputindo.

[2] Triyono, Joko, K, Rr. Yuliana Rachmawati, dan Irnawan, Fahmi Dhimas. (2014). *Analisis Perbandingan Kinerja Jaringan VPN Berbasis Mikrotik Menggunakan Protokol PPTP dan L2TP Sebagai Media Transfer Data.* Jurnal Jarkom. Vol.1. No.2.2 Januari 2014.ISSN:2338.6312

[3] Madjid, Nurkholis. Perbandingan SSL (Secure Socket Layer) dan IPSec (Internet Protocol Security) Pada VPN (Virtual Private Network). Program studi Teknik Informatika. Institut Teknologi Bandung: Bandung

[4] Guritno, S, Sudaryono, dan Raharja, U. 2011. Theory and Application of IT Research. Yogyakarta, Andi.

[5] Boedi P, Dessyanto. PERBANDINGAN KINERJA IP SEC DAN SSL. Jurnal Informatika dan Teknologi Informasi.2010; Vol (7): 23-32.

[6] Yanto. Analisis Qos (Afrianto, Irawan. dan Setiawan, Eko Budi. 2011. *Kajian Virtual Private Network (VPN).Sebagai Sistem Pengaman Data Pada Jaringan Komputer.* Majalah Ilmiah UNIKOM. Vol 12 No.1. Agustus. 2011. Universitas Komputer Indonesia

[7] Frankel, Sheila. 2005. *Guide to IPSec VPN*. National Institute of Standard Technologi. United State Departement of Commerce

[8] Frankel, Sheila. 2001. *Demystifying the IPSec Puzzle.* British Library Catalouging in Publication Data: Boston-London

[9] Seta, Henki Bayu, Ridwan, Muhammad, dan Wati, Theresia. 2015. *Perbandingan Virtual Private Network Protokol Menggunakan Point-to-Point Tunnel Protocol dan OpenVPN.* Konferensi NasionalSistem & Informatika.Universitas Pembangunan Nasional "Veteran": Jakarta

[10] Riadi, Muchlisin. 2018. *Fungsi dan Jenis Protokol VPN (Virtual Private Network).* https://www.kajianpustaka.com/2018/01/fungsi-jenis-dan-protokol-vpn-virtualprivate-network.html

[11] Quality Of Service Pada Jaringan Internet (Studi Kasus: Fakultas Teknik Universitas Tanjungpura)". Universitas Tanjungpura, Pontianak. 2013.

UCAPAN TERIMA KASIH

Terima kasih kepada program studi Teknik Informatika dan Teknik Komputer Universitas Bina Darma serta Staf Laboratorium Cisco-UBD yang telah membantu dan berpartisipasi dalam penelitian ini. Terima kasih juga disampaikan kepada Tim Editor jurnal Inovtek Seri Infomatika. Semoga mendapat berkah dari Allah Tuhan Yang Maha Esa atas karunia-NYA dan tak yang tak terlupakan istri dan anak-anak tercinta.