ISSN : 2338-4018

PERBANDINGAN PERFORMANSI JARINGAN VIRTUAL PRIVATE NETWORK METODE POINT TO POINT TUNNELING PROTOCOL (PPTP) DENGAN METODE INTERNET PROTOCOL SECURITY

Irwan Nugroho (irwannugroho5@gmail.com)
Bebas Widada (bbswdd@yahoo.com)
Kustanto (kustanto@sinus.ac.id)

ABSTRAK

Teknologi Virtual Private Network (VPN) sangat berperan besar dalam dunia komunikasi sekarang ini, dikarenakan VPN mampu membuat jaringan local dengan menggunakan fasilitas public. Karena dengan VPN perusahaan bisa menjalin suatu koneksi data yang mudah dan aman. Tujuan penelitian ini untuk untuk membandingkan performasi tunneling jaringan Virtual Private Network metode Point to Point Tunneling Protocol (PPTP) dan metode Internet Protocol Security (IPsec) yang dapat membantu para pakar jaringan untuk menyesuaikan tunneling mana yang sesuai dengan kondisi lapangan karena dengan penelitian ini dapat terlihat perbadingan performansi dari sisi waktu transmisi, delay, bandwidth, jitter serta troughput saat proses transmisi data. Performansi dan arsitektur VPN yang seperti apa yang terbaik. Hasil penelitian ini dapat disimpulkan bahwa jaringan VPN dengan koneksi internet disisi server dan client yang berbeda berpengaruh besar dalam kestabilan suatu jaringan yang menggunakan jaringan public. Koneksi internet yang lebih besar di sisi server akan membuat jaringan VPN lebih stabil dan tidak banyak timbul perbedaan pada PPTP maupun IPSec dan pada performansi IPSec dengan server yang lebih besar membuatnya lebih baik dibandingkan dengan PPTP.

Keyword :PPTP, IPSEC, Performansi jaringan virtual private network.

I. PENDAHULUAN

Banyak perusahaan besar yang sudah mempunyai anak cabang di berbagai daerah. Untuk menjalin koneksi dan menjaga keamanan data ketika melakukan suatu pengiriman data dibuatlah jaringan VPN sebagai solusi dalam pengiriman serta melindungi data penting perusahaan saat melakukan *transmisi* data.

Tujuan penelitiian ini untuk membandingkan performansi *tunneling* jaringan *Virtual Private Network* metode *Point to Point Tunneling Protocol* (PPTP) dan metode *Internet Protocol Security* (IPsec).

II. METODE PENELITIAN

Dalam melakukan penelitian ini, penulis menggunakan beberapa metode pengumpulan data yang meliputi:

1. Metode Wawancara
   Pengumpulan data melalui wawancara langsung dengan nara sumber yang ahli jaringan VPN.
2. Metode Pustaka
   Penulis mengumpulkan data dengan cara membaca literatur, jurnal, *browsing* internet dan bacaan-bacaan yang ada kaitannya dengan masalah yang akan diteliti sebagai bahan referensi tertulis.
3. Metode Eksperimen
   Eksperimen yang dilakukan penulis adalah mengumpulkan data mengenai kebutuhan sistem, merancang sistem dan membangun arsitektur jaringan *tunneling* VPN kemudian mengimplementasikan teknologi *site-to-site VPN*.

Dalam perancangan jaringan VPN ini penulis menggunakan

- Router seri RB751U-2HnD mikrotik operation system.
- Penggunaan winbox sebagai media konfigurasi mikrotik jaringan VPN baik PPTP maupun IPSec dengan koneksi internet menggunakan Telkom speedy 512 kbps.
- Penggunaan *software* FileZilla, *Bandwidth* Meter Pro dan Wireshark.

Skenario pengujian :

Dalam pengujiaannya dari sisi client di install *software Bandwidth* Meter Pro, wireshark dan filezilla. Dengan cara mengakses *server* menggunakan FileZilla client dan pada saat melakukan aktifitas *transmisi* data dimonitoring dengan *Bandwidth*

Meter Pro dan Wireshark untuk dibandingkan dalam hal *bandwidth, delay, jitter* dan *troughput* dari masing-masing *tunneling*.

III. TINJAUAN PUSTAKA

3.1 JARINGAN KOMPUTER

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagi sumber daya, berkomunikasi dan dapat mengakses informasi. Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan. Pihak yang meminta atau menerima layanan disebut *client* dan yang memberikan atau mengirim layanan disebut peladen atau *server*. Desain ini disebut dengan *system client-server*. [1]

Media *transmisi* merupakan jalur yang digunakan untuk dapat melakukan perpindahan data, baik berupa kabel maupun tanpa kabel. [2]

Dalam pemilihan media *transmisi* perlu pertimbangkan aspek-aspek sebagai berikut:

1. *Resistance*:ketahanan terhadap pengaruh *Electrical Magentic Interface* (EMI). Data yang dialirkan melalui kabel akan berupa gelombang elektro magnetik, sehingga apabila terdapat gelombang elektro magnetik lain di sekitar kabel dapat mengganggu atau merusak data yang berjalan di dalam kabel.
2. *Bandwidth* : jumlah frekuensi yang dapat diakomodasi oleh media *transmisi*. Dengan media yang dapat mengakomodasi jumlah frekuensi lebih banyak, jumlah data yang dikirim atau diterima akan lebih banyak dan dengan waktu pengiriman yang lebih cepat.
3. *Attenuation* : luas jangkauan yang dapat diberikan oleh media *transimsi*. Luas jangkau ini dikarenakan adanya hambatan yang dimiliki media *transmisi* itu sendiri.
4. *Cost* : dana yang dimiliki dan biaya yang harus dikeluarkan untuk instalasi jaringan tetap harus dibandingkan dengan kebutuhan yang ada. [2]

3.2 VIRTUAL *PRIVATE* NETWORK (VPN)

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi jaringan yang memungkinkan untuk dapat terkoneksi ke jaringan *public* dan menggunakannya untuk dapat bergabung dengan jaringan lokal. Dengan cara tersebut maka akan di dapatkan hak dan pengaturan yang sama seperti halnya berada didalam LAN itu sendiri, walaupaun sebenarnya menggunakan jaringan milik *public*.

VPN dapat dibentuk dengan menggunakan teknologi *tunneling* dan *enkripsi*. Koneksi VPN juga dapat terjadi pada semua layer pada *protocol* OSI (*Open System Interconnection*), sehingga komunikasi dengan VPN dapat digunakan untuk berbagai keperluan. [3]

Virtual Private Network merupakan perpaduan dari teknologi *tunneling* dengan teknologi *enkripsi*.

1. Teknologi *Tunneling*.
   Teknologi *tunneling* adalah teknologi yang bertugas untuk menangani dan menyediakan koneksi *point-to-point* dari sumber ke tujuannya. Disebut tunnel karena koneksi point-to-point tersebut sebenarnya terbentuk dengan melintasi jaringa umum, namun koneksi tersbut tidak mempedulikan paket-paket data milik orang lain yang sama-sama melintasi jaringan umum tersebut, tetapi koneksi tersebut hanya melayani transportasi data dari pembuatnya. Hal ini sama dengan seperti penggunaan jalur busway yang pada dasarnya menggunakan jalan raya, tetapi dia membuat jalur sendiri untuk dapat dilalui bus khusus. [4]
2. Teknologi *enkripsi*.
   Setiap orang ketika ingin menyampaikan pesan secara pribadi, maka orang tersebut harus menyembunyikannya dari orang yang tidak diinginkan. Maka, pesan tersebut akan dimasukkan ke dalam amplop agar tidak dapat dibaca langsung oleh orang lain.Untuk dapat menambah kerahasiaan surat tersebut agar tetap tidak mudah terbaca walaupun amplopnya terbuka, maka harus ada mekanisme tertentu agar isi dari pesan tersebut tidak dapat dengan mudah dipahami oleh orang yang tidak diinginkan. Mekanisme tersebut dapat disebut dengan *enkripsi*. *Enkripsi* merupakan proses atau mekanisme untuk mengamankan informasi dengan cara membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetehuan atau alat khusus. Sedangkan dekripsi merupakan algoritma atau cara yang dapat digunakan untuk membaca informasi yang telah dienkripsi untuk dapat dibaca kembali. [4]

3.3 *POINT TO POINT TUNNELING PROTOCOL* (PPTP)

PPTP merupakan *protocol* jaringan yang memungkinkan pengamanan *transfer* data dari remote *client* ke *server* pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP. Teknologi jaringan PPTP merupakan pengembangan dari *remote access Point-to-Point protocol* yang dikeluarkan oleh *Internet Engineering Task Force* (IETF). PPTP merupakan *protocol* jaringan yang merubah paket PPP menjadi IP datagram agar dapat di*transmisi*kan melalui intenet. PPTP juga dapat digunakan pada jaringan *private* LAN-to-LAN.[4]

3.4 *INTERNET PROTOCOL SECURITY* (IPSEC)

IPSec merupakan *tunneling protocol* yang bekerja pada layer 3. IPSec menyediakan layanan sekuritas pada IP layer dengan mengizinkan system untuk memilih *protocol* keamanan yang diperlukan, algoritma apa yang akan digunakan pada layanan, dan menempatkan kunci kriptografi yang diperlukan untuk menyediakan layanan yang diminta. IPSec bekerja dengan tiga cara yaitu: *Network-to-network, Host-to-network dan Host-to-host.* [5]

3.5 PARAMETER JARINGAN KOMPUTER

Dalam Jaringan komputer, semisal jaringan LAN (*Local Area Network*) dikatakan jaringan tersebut handal atau memiliki reability yang besar ada beberapa parameter untuk menyatakan suatu jaringan komputer seperti itu.[1]

Parameter itu antara lain:

- *Bandwitdh*
  Bandwidth adalah luas atau lebar cakupan frekuensi yang digunakan oleh sinyal dalam medium *transmisi*. Dalam kerangka ini, *bandwidth* dapat diartikan sebagai perbedaan antara komponen sinyal frekuensi tinggi dan sinyal frekuensi rendah. frekuensi sinyal diukur dalam satuan Hertz.. Berikut adalah rumus dari *bandwidth*: *bandwidth* = jumlah bit / waktu. [6]
- *Delay* dan *Jitter*
  Delay dan *jitter* merupakan satu satuan yang hampir sama. *Delay* merupakan keterlambatan dalam waktu *transmisi* data dari pengirim dan penerima, satuan dari *delay* adalah *second* atau detik. Misalnya keterlambatan waktu pengiriman sebesar 3ms, jadi ada jeda waktu di pihak penerima dalam peneriamaan data yang dikirim selama 3 milidetik. Sedangkan jiter merupakan variasi dari *delay* atau selisih antara *delay* pertama dengan *delay* selanjutnya. [6]
- *Throughput*
  Throughput merupakan *bandwidth* aktual yang terukur pada suatu ukuran waktu tertentu dalam suatu hari menggunakan rute internet yang spesifik ketika sedang men-*download* suatu file. Sedangkan throughput walau pun memiliki satuan dan rumus yang sama dengan *bandwidth*, tetapi *throughput* lebih pada menggambarkan *bandwidth* yang sebenarnya pada suatu waktu tertentu dan pada kondisi dan jaringan internet tertentu yang digunakan untuk *download* suatu *file* dengan ukuran tertentu. Berikut adalah formula pembanding *throughput* dengan *bandwidth*:
  waktu terbaik = ukuran *file*/*bandwidth*
  waktu typical = ukuran *file* / *throughput*
  Jika dengan hanya mengunakan *bandwidth* sebagai patokan, seseorang menganggap seharusnya file yang akan di*download*nya yang berukuran 64 kb seharusnya bisa di-*download* dalam waktu sekedip mata atau satu detik, tetapi setelah diukur ternyata memerlukan waktu 4 detik. Jadi jika ukuran file yang di*download* adalah 64 kb, sedangkan waktu *download*nya adalah 4 detik, maka *bandwidth* yang sebenarnya atau bisa kita sebut sebagai *throughput* adalah 64 kb / 4 detik = 16 kbps. [6]

IV. HASIL DAN PEMBAHASAAN

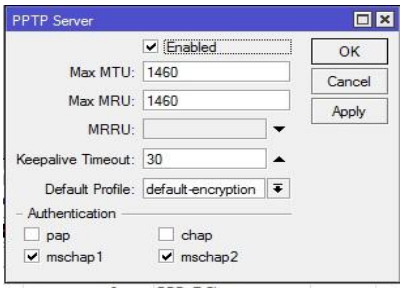
4.1 KONFIGURASI *TUNNELING* VPN

Untuk mengimplentasikan teknologi VPN, masing-masing *tunneling* metode PPTP dan IPSec diperlukan konfigurasi disetiap metodenya yang disesuaikan dengan kondisi lapangan tempat pengujian *tunneling*. Berikut ini konfigurasi *tunneling* metode PPTP dan metode IPSec.

A. KONFIGURASI PPTP

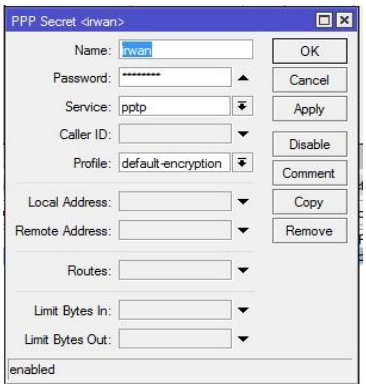
- Konfigurasi server PPTP

1. Masuk mikrotik melalui winbox aktifkan *PPTP server* melalui PPP-PPTPserver.



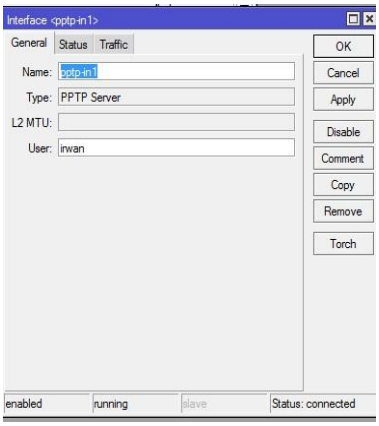
Gambar 1. Enable PPTP server

2. Kemudian pilih menu PPP secret untuk membuat user client



Gambar 2. PPP secret

3. Setelah selesai pilih tab interface dan buat PPTP server.



Gambar 3. interface PPTPserver

4. Tekan OK dan konfigurasi selesai.

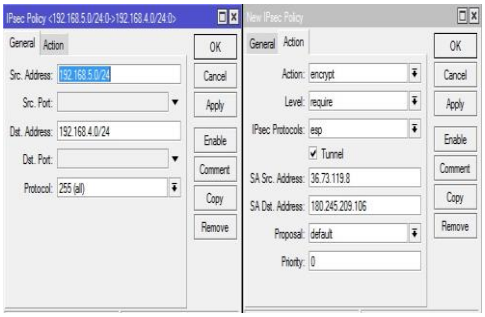
- Konfigurasi client PPTP

1. Buka control panel, kemudian *network and sharing Center*
2. Buat koneksi *client* VPN PPTP pilih *set up a new connection or network*
3. Pilih *connect to workplace*
4. Pilih *No, create a new connention*
5. Pilih *use my Internet connention (VPN)*
6 Masukkan *ip server* ganti vpn *connection* dengan nama pptp
7. Buat user yang sama saat kita buat pada pptp server
8. Pilih connect dan kita sudah dapat terhubung dengan pptp

B. KONFIGURASI IPSEC

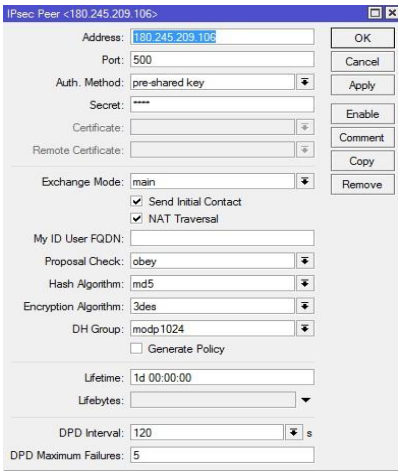
Konfigurasi pada *server* dan client IPSec pada dasarnya sama tinggal tinggal kita menukarkan ip pada saat konfigurasinya.

1. Buat *ip address* dengan konfigurasi
   - *Ip address* pada server
     Ip public : 36.73.119.8
     Ether 1 : 192.168.1.1/24
     Ether 2 (*ip private*): 192.168.5.1/24
   - *Ip address* pada client
     Ip public: 180.245.209.106
     Ether 1: 192.168.3.1/24
     Ether 2(*ip private*): 192.168.4.1/24
2. Setelah terkoneksi dengan internet kemudian kita setting ipsec police pada *server activekan tunnel* dan masukkan *ip public* speedy seperti gambar,sebaliknya jg disisi *client*.



Gambar 4. konfigurasi IPsec Police

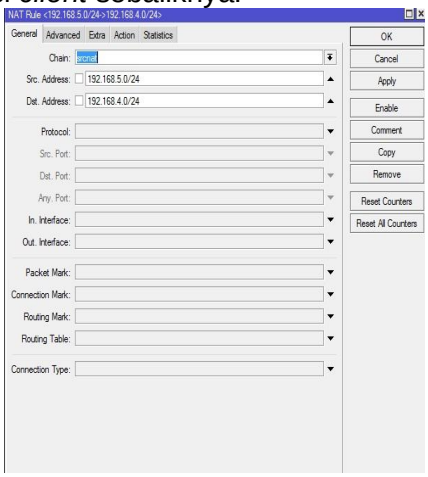
3. Setelah ok, setting ipsec peer dengan *address* di isi ip *public* tujuan,sebaliknya juga client. *Secret* kita isi sebagai kunci hubungan *server* dan client yang di isi sama semisal “test”



Gambar 5. konfigurasi IPsec Peer

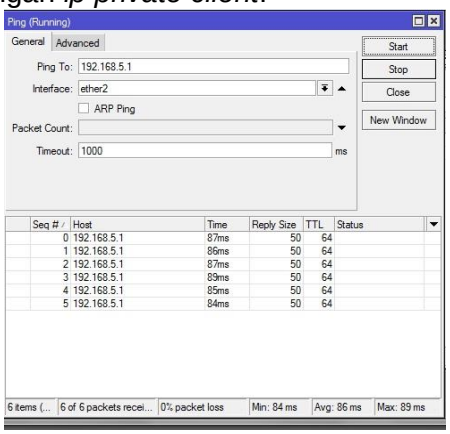
4. Setelah selesai pilih tab proposal dan biarkan default baik *server* maupun *client*

5. Setelah selesai tutup dan buka *ip* firewall nat, masukkan *ip private* dan tujuan *ip private*,dengan action : *accept*. Begitu pula di sisi *client* sebaliknya.



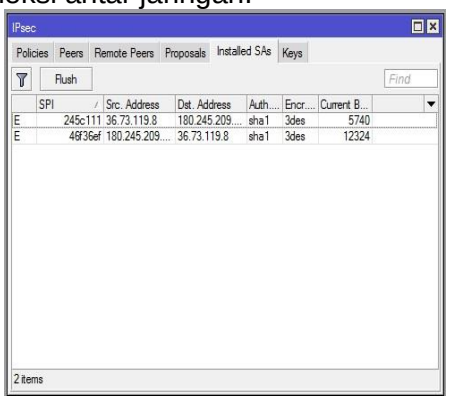
Gambar 6. Konfigurasi Nat Rule

6. Setelah selesai semua konfigurasi *reboot router* baik *server* maupun *client*.
7. Setelah selesai ping *ip private server* dengan *ip private client*.



Gambar 7. Pengujian IPsec

8. Jika IPsec berjalan ketika ping terjadi pada *installed SAs IPsec* akan muncul koneksi antar jaringan.



Gambar 8. Installed SAs IPSec

4.2 PENGUJIAN *TUNNELING* VPN

Pengujian dilakukan dengan men*download* 3 *file* yang berbeda baik dengan PPTP maupun IPSec. Langkah pengujian *system tunneling*:

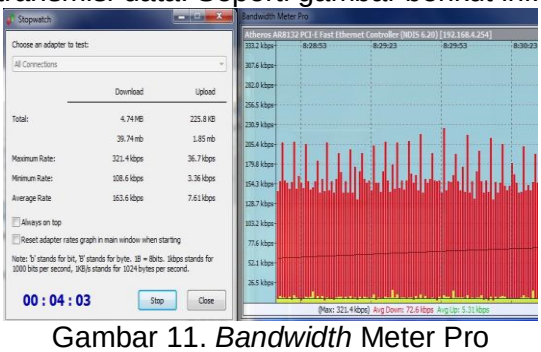
1. Pada client baik PPTP maupun IPSec setelah terkoneksi, buka *software* FileZilla dan login sesuai dengan *username* dan *password*.
   - Pada PPTP lihat *ip address* server,masukkan *ip address* kedalam host kemudian *username* dan *password*.

Gambar 9. Login FileZilla PPTP

   - Pada IPSec masukkan *ip private* dari server, *username* dan *password*.

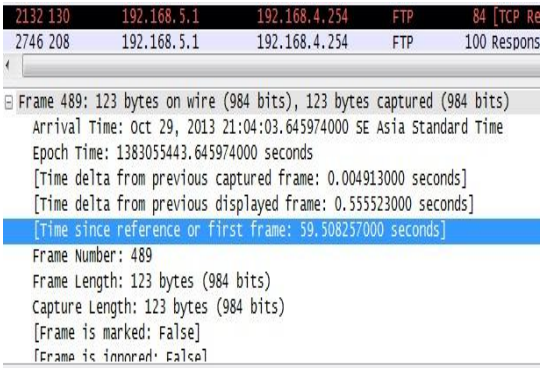
Gambar 10. Login FileZilla IPSec

2. Setelah terkoneksi *download* file dari *server* baik PPTP maupun IPSec.
3. Jalankan *Bandwidth* Meter Pro untuk mengukur *bandwidth* ketika proses *transmisi* data. Seperti gambar berikut ini:



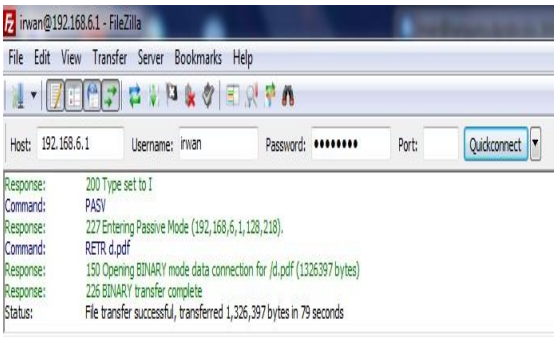
Gambar 11. *Bandwidth* Meter Pro

4. Jalankan wireshark untuk merekam kinerjaVPN dari masing-masing *tunneling*, baik PPTP maupun IPsec pada saat *trasmisi* data.



Gambar 12. Hasil *delay* pada wireshark saat *transmisi* data

5. Lama waktu *transmisi* data dapat dilihat dari FileZilla setelah selesai proses *transmisi* data.



Gambar 13. Waktu *transmisi* data

4.3 HASIL PENGUJIAN

Hasil pengujian tunneling dengan PPTP dan IPSec dari proses transmisi data dilakukan dengan koneksi internet yang sama baik metode tunneling PPTP maupun IPSec.

Hipotesa sebelum dalam melakukan pengujian performansi ini sebagai berikut :

1. Apa berpengaruh koneksi yang lebih besar di client dibandingkan pada server dalam proses transmisi data di jaringan VPN.
2. Berapa besar bandwidth yang dibutuhkan untuk melakukan transmisi pada tiap metodenya.
3. Metode mana yang lebih cepat dalam melakukan proses transmisi.
4. Keterlambatan transmisi atau delay pada masing-masing metode.

Pengujian dilakukan 2 kali dengan koneksi internet yang berbeda baik disisi server maupun client kedua metode. Adapun hasil pengujian sebagai berikut ini:

❖ **PENGUJIAN PERTAMA**

Pengujian pertama dengan menggunakan arsitektur sebagai berikut :

- Koneksi server 1: 512 kbps Telkom speedy
- Koneksi client 1: 384 kbps Telkom speedy
- Pengujian dilakukan pada pukul 22.00 WIB
- Kondisi cuaca cerah

a) *Download file*: ii.ppt *size* : 1.12 MB (1183744 Bytes)

Tabel 1. Tabel pengujian pertama file ii.ppt

No	Pengukuran	Software	Hasil IPSec	Hasil PPTP
1	Lama transmisi	FileZilla	72 second	99 second
2	Bandwidth	Bandwidth Meter Pro	138,3 kbps	98,5 kbps
3	Troughput	FileZilla	16,4 kbps	11,9 kbps
4	Delay	Wireshark	0.102038 second	0.759932 second
5	Jitter	Wireshark	0 second	0 second

b) *Download file* : d.pdf *size* : 1.26 MB(1326397 Bytes)

Tabel 2. Tabel pengujian pertama file d.pdf

No	Pengukuran	Software	Hasil IPSec	Hasil PPTP
1	Lama transmisi	FileZilla	80 second	96 second
2	Bandwidth	Bandwidth Meter Pro	160,6 kbps	122 kbps
3	Troughput	FileZilla	16,5 kbps	13,8 kbps
4	Delay	Wireshark	0.164702 second	2.876338 second
5	Jitter	Wireshark	1.102939 second	2.116406 second

c) *Download file* : driver-canon-pixma-ip1000.exe *size*: 6.33 MB (6638080 Bytes)

Tabel 3. Tabel pengujian pertama file driver-canon-pixma-ip1000.exe

No	Pengukuran	Software	Hasil IPSec	Hasil PPTP
1	Lama transmisi	FileZilla	486 second	690 second
2	Bandwidth	Bandwidth Meter Pro	175,7 kbps	156,2 kbps
3	Troughput	FileZilla	13,6 kbps	9,6 kbps
4	Delay	Wireshark	1.204977 second	2.462215 second
5	Jitter	Wireshark	1.040275 second	0.414123 second

Rasio performansi dari hasil percobaan 1

Tabel 4. Tabel rasio performasi pengujian pertama

Metode	FILE	Rumus rasio	Lama Transmisi	Bandwidth rata-rata	Troughput	Delay	Jitter
PPTP	A	PPTP/PPTP	1	1	1	1	0
IPSEC	A	IPSEC/PPTP	0.72	1.4	1.3	0.1	0
PPTP	B	PPTP/PPTP	1	1	1	1	1
IPSEC	B	IPSEC/PPTP	0.83	1.3	1.1	0.05	0.5
PPTP	C	PPTP/PPTP	1	1	1	1	1
IPSEC	C	IPSEC/PPTP	0.70	1.1	1.4	0.4	0.7

Dari hasil percobaan 1 diatas dapat disimpulkan sebagai berikut :

- Koneksi kedua metode berjalan tanpa terputus setiap melakukan transmisi data.
- Lama transmisi IPSEC <1 dapat diartikan semakin cepat dalam melakukan proses transmisi data dibandingkan PPTP.
- Bandwidth IPSEC >1 dapat diartikan bandwidth yang diperlukan dalam proses transmisi lebih besar dibandingkan dengan PPTP
- Troughput IPSEC >1 dapat diartikan troughput atau bandwidth yang sebenarnya lebih besar dibandingkan PPTP
- Delay IPSEC <1 dapat diartikan delay atau keterlambatan dalam proses transmisi lebih kecil dibandingkan dengan PPTP
- Jitter IPSEC <1 dapat diartikan jitter atau selisih delay antar transmisi lebih kecil dibandingkan PPTP.

❖ **PENGUJIAN KEDUA**

Pengujian kedua dilakukan sebagai pembanding percobaan pertama, apakah arsitektur dengan koneksi internet pada server lebih kecil dibandingkan koneksi internet pada client berpengaruh pada performansi dari masing-masing arsitektur..

Pengujian kedua ini menggunakan arsitektur sebagai berikut :

- Koneksi server 2 : 384 kbps Telkom speedy
- Koneksi client 2: 780 kbps Smartlink
- Pengujian dilakukan pukul 11.00-13.00 WIB
- Kondisi cuaca cerah

a. Download file : googletalk-setup.exe ukuran file : 1,61 MB (1606064 Bytes)

Tabel 5. Tabel pengujian kedua file googletalk-setup.exe

Metode	Percobaan	Waktu	Lama Transmisi (second)	Bandwidth rata-rata (kbps)	Troughput (kbps)	Delay (second)	Jitter (second)
PPTP	1	11.20	90	320,9	17,8	0.910786	0
	2	11.46	88	328,3	18,3	0.840563	0.070223
	3	12.39	88	325,9	18,3	0.997776	0.157213
Metode	**Percobaan**	**Waktu**	**Lama Transmisi (second)**	**Bandwidth rata-rata (kbps)**	**Troughput (kbps)**	**Delay (second)**	**Jitter (second)**
IPSEC	1	12.20	107	143,0	15,1	103.562166	0
	2	12.26	89	166,9	18,1	86.456224	17.105942
	3	12.58	94	145,4	17,2	93.721307	7.265083

Rasio performansi dari hasil percobaan :

Tabel 6. Tabel performansi tabel 5

Metode	Rumus rasio	Lama Transmisi	Bandwidth rata-rata	Troughput	Delay	Jitter
PPTP	PPTP/PPTP	1	1	1	1	0
PPTP	PPTP/PPTP	1	1	1	1	1
PPTP	PPTP/PPTP	1	1	1	1	1
IPSEC	IPSEC/PPTP	1.1	0.4	0.8	113.7	0
IPSEC	IPSEC/PPTP	1.01	0.5	0.9	102.8	243.5
IPSEC	IPSEC/PPTP	1.06	0.4	0.9	93.9	46.2

b. Download file : pknkelasxiurut.rar ukuran file : 3,31 MB (3312017 Bytes)

Tabel 7. Tabel pengujian kedua file pknkelasxiurut.rar

Metode	Percobaan	Waktu	Lama Transmisi (second)	Bandwidth rata-rata (kbps)	Troughput (kbps)	Delay (second)	Jitter (second)
PPTP	1	11.27	174	330,8	19,0	1.042377	0
	2	11.58	177	330,4	18,7	2.645663	1.603286
	3	12.44	190	299,5	17,4	10.543172	7.897509
Metode	**Percobaan**	**Waktu**	**Lama Transmisi (second)**	**Bandwidth rata-rata (kbps)**	**Troughput (kbps)**	**Delay (second)**	**Jitter (second)**
IPSEC	1	12.22	185	165,3	17.9	185.067208	0
	2	12.32	181	173,6	18,3	181.385412	3.681796
	3	12.55	173	164,4	19,1	173.339933	8.045479

Rasio performansi dari hasil percobaan :

Tabel 8. Tabel rasio performansi tabel 7

Metode	Rumus rasio	Lama Transmisi	Bandwidth rata-rata	Troughput	Delay	Jitter
PPTP	PPTP/PPTP	1	1	1	1	0
PPTP	PPTP/PPTP	1	1	1	1	1
PPTP	PPTP/PPTP	1	1	1	1	1
IPSEC	IPSEC/PPTP	1.06	0.4	0.9	177.5	0
IPSEC	IPSEC/PPTP	1.02	0.5	0.9	68.5	2.2
IPSEC	IPSEC/PPTP	0.9	0.5	1.09	16.4	1.01

c. Download file : if-Iknow.mp3 ukuran file : 2,07 MB (2074577 Bytes)

Tabel 9. Tabel pengujian kedua file if-iknow.mp3

Metode	Percobaan	Waktu	Lama Transmisi (second)	Bandwidth rata-rata (kbps)	Troughput (kbps)	Delay (second)	Jitter (second)
PPTP	1	11.43	108	336,0	19,1	1.076674	0
	2	11.53	113	303,0	18,3	1.039134	0.03754
	3	12.37	115	315,7	18	1.093421	0.054287
Metode	Percobaan	Waktu	Lama Transmisi (second)	Bandwidth rata-rata (kbps)	Troughput (kbps)	Delay (second)	Jitter (second)
IPSEC	1	12.16	120	161,0	17,2	119.464185	0
	2	12.28	112	170,7	18,5	111.245451	8.218734
	3	12.52	118	151,4	17,5	117.940575	6.695124

Rasio performansi dari hasil percobaan:

Tabel 10. Tabel rasio performansi tabel 9

Metode	Rumus rasio	Lama Transmisi	Bandwidth rata-rata	Troughput	Delay	Jitter
PPTP	PPTP/PPTP	1	1	1	1	0
PPTP	PPTP/PPTP	1	1	1	1	1
PPTP	PPTP/PPTP	1	1	1	1	1
IPSEC	IPSEC/PPTP	1.1	0.4	0.9	111.5	0
IPSEC	IPSEC/PPTP	0.9	0.5	1.01	107.9	218.9
IPSEC	IPSEC/PPTP	1.02	0.4	0.9	108.1	123.3

Dari hasil percobaan 2 diatas dapat disimpulkan sebagai berikut :

- Koneksi PPTP sering terputus ketika transmisi data, sedangkan IPSEC tidak pernah terputus.
- Lama transmisi IPSEC >1 dapat diartikan semakin lama dalam melakukan proses transmisi data dibandingkan PPTP.
- Bandwidth IPSEC <1 dapat diartikan bandwidth yang diperlukan dalam proses transmisi lebih kecil dibandingkan dengan PPTP
- Troughput IPSEC <1 dapat diartikan troughput atau bandwidth yang sebenarnya lebih kecil dibandingkan PPTP
- Delay IPSEC >1 dapat diartikan delay atau keterlambatan dalam proses transmisi lebih besar dibandingkan dengan PPTP
- Jitter IPSEC >1 dapat diartikan jitter atau selisih delay antar transmisi lebih besar dibandingkan PPTP.

V. PENUTUP

5.1 KESIMPULAN

Dari hasil percobaan yang telah dilakukan pada tunneling PPTP dan IPsec baik percobaan 1 dan percobaan 2 dapat disimpulkan sebagai berikut:

1. Pada percobaan 1 tidak pernah mengalami masalah dalam proses transmisi data dari server, sedangkan pada percobaan 2 sering terputus ketika melakukan proses transmisi data terutama pada PPTP.
2. Pada percobaan 1 yang dengan koneksi internet pada client 384 kbps bandwidth yang dihasilkan bisa mencapai maksimal,akan tetapi dengan percobaan 2 client koneksi 780 kbps, bandwidth maksimal yang dihasilkan tidak bisa mencapai koneksi internet dan tidak bisa melebihi server.
   Jadi : koneksi server pada VPN sangat berpengaruh besar dalam proses transmisi,akan tetapi sebesar apapun koneksi di sisi client tidak bisa melebih server saat proses transmisi data.
3. Bandwidth rata-rata pada percobaan 1, PPTP membutuhkan 132,06 kbps lebih kecil dibandingkan IPSec151,7 kbps, pada percobaan 2 PPTP membutuhkan bandwidth rata-rata 321.16 kbps sedangkan IPSec hanya 160.18 kbps.
   Jadi : perbedaan koneksi internet yang dipakai pada client dan server sangat berpengaruh pada bandwidth yang dibutuhkan dalam proses transmisi data, akan lebih stabil bandwidth VPN dengan koneksi internet server lebih besar dari client.
4. Waktu yang diperlukan dalam melakukan transmisi pada percobaan 1

PPTP selalu lebih lama dibandingkan dengan IPSec, pada percobaan 2 waktu yang diperlukan hampir sama pada kedua metode.
Jadi : waktu yang diperlukan dalam proses transmisi VPN lebih baik dan stabil pada client yang koneksi dibawah server.

5. Delay atau keterlambatan transmisi data pada percobaan 1 PPTP lebih besar dibandingkan IPSec, tapi pada percobaan 2 IPSec lebih besar dibandingkan PPTP.
Jadi : delay pada IPSec percobaan kedua menunjukkan ketidakstabilan suatu koneksi karena begitu besar perbedaan dibandingkan PPTP, lebih stabil pada percobaan 1.

Jadi dapat disimpulkan bahwa jaringan VPN dengan koneksi internet disisi server dan client yang berbeda berpengaruh besar dalam kestabilan suatu jaringan yang menggunakan jaringan public. Koneksi internet yang lebih besar di sisi server akan membuat jaringan VPN lebih stabil dan tidak banyak timbul perbedaan pada PPTP maupun IPSec dan pada performansi IPSec dengan server yang lebih besar membuatnya lebih baik dibandingkan dengan PPTP.

5.2 SARAN

Dari hasil penelitian ini, penulis berharap dapat dijadikan suatu patokan untuk lebih mengembangkan performansi jaringan VPN. Masih banyak yang perlu dianalisa dalam jaringan VPN khusunya metode PPTP dengan IPSec, baik dari sisi keamanan kedua metode, banyaknya client yang melakukan proses transmisi data, dan lain sebagainya yang mempengaruhi performansi jaringan VPN.

DAFTAR PUSTAKA

[1] Oscar Rachman. ***Router Teknologi Konsep Konfigurasi dan Trobleshooting***. Informatika. Bandung. 2012.

[2] Rully Charitas. ***Mengenal Komputer for Beginner***. Andi Publisher. Jogjakarta. 2012.

[3] Deris Setiawan dan Diah Palupi Rini. ***Optimasi Interkoneksi VPN Dengan Menggunakan Hardware Based dan Lix Sebagai Alternatif Jaringan WAN***. Makasar. 2009.

[4] Rendra Towidjojo. ***Mikrotik Kung Fu Kitab 2***. Jasakom. Jakarta. 2013.

[5] Bambang Ardiansyah. ***Jurnal Keamanan Jaringan Komputer Implementasi IPSec pada VPN. Universitas Sriwijaya*****.** 2008

[6] Redaksi***. Jurnal Ilmiah dan Informatika*** vol 1 no 1. Komputa. Jakarta. 2012.