Optimasi Keamanan Jaringan Point to Point Menggunakan VPN IPSec dan GRE

Nana[1)], Dadang Iskandar Mulyana[2)],
[1,2]Teknik Informatika, STIKOM CKI Jakarta,
Jalan Raden Inten II, Duren Sawit, Jakarta Timur 13440
e-mail: *rifnrid@gmail.com, mahvin2012@gmail.com

Abstrak

Pada masa sekarang ini, dimana perkembangan teknologi dan informasi berkembang sangat cepat. Hal ini berdampak pada keamanan lalu lintas data di jaringan komputer sangat penting, terutama jika melibatkan data sensitif. Namun, keamanan data masih dianggap kurang penting dan kurang menarik perhatian pengguna komputer. Hal ini dikarenakan masih sulitnya penerapan keamanan data baik bagi pengguna komputer individu maupun perusahaan. Virtual Private Network (VPN), merupakan sebuah jaringan yang dibuat untuk melakukan transaksi data yang telah dienkripsi antara dua atau lebih pengguna jaringan yang resmi. Jaringan VPN seluruhnya menggunakan internet sehingga faktor keamanan menjadi sangat penting. Beberapa serangan yang mungkin terjadi di jaringan internet adalah Denial of Service (DoS) attack, sniffing, spoofing, session hijacking, dan masih banyak lagi. Peneliti mencoba mensimulasikan keamanan jaringan menggunakan simulator GNS3 untuk menjalankan dua metode untuk keamanan jaringan point to point yaitu dengan menggunakan VPN IPSec dan GRE yang berfungsi mengenkripsi tarfik data yang dikirim melalui jaringan publik. Pada saat dilakukan upload file sebesar 50 Megabyte dari komputer 2 dan komputer 3 ke FTP Server dengan throughput 0,878 Mbps dengan metode IPSec ping rata-rata 75ms; dan throughput 1,060 Mbps dengan metode GRE ping rata-rata 78ms; trafik masih normal tidak mengalami kendala pada jaringan atau request time out (RTO).

Kata kunci*—VPN, IPSec, GRE, Point to Point, GNS3.*

Abstract

At this time, where the development of technology and information is growing very fast. This has an impact on the security of data traffic on computer networks is very important, especially if it involves sensitive data. However, data security is still considered less important and attracts less attention from computer users. This is because it is still difficult to implement data security for both individual and corporate computer users. Virtual Private Network (VPN), is a network created to conduct encrypted data transactions between two or more authorized network users. VPN networks all use the internet so the security factor is very important. Some of the attacks that may occur on the internet network are Denial of Service (DoS) attacks, sniffing, spoofing, session hijacking, and many more. Researchers try to simulate network security using the GNS3 simulator to run two methods for point-to-point network security, namely by using IPSec VPN and GRE which functions to encrypt data traffic sent over public networks. At the time of uploading a file of 50 Megabytes from computer 2 and computer 3 to the FTP Server with a throughput of 0.878 Mbps with the IPSec method, the average ping is 75ms; and 1,060 Mbps throughput with the GRE method ping an average of 78ms; traffic is still normal, no problems on the network or request time out (RTO).

Keywords— *VPN, IPSec, GRE, Point to Point, GNS3.*

1. PENDAHULUAN

Karena teknologi jaringan Internet Protocol (IP) sekarang menjadi fenomena di seluruh dunia, layanan berbasis IP tumbuh dan beragam, termasuk *tunneling*. [1] *Tunneling* adalah solusi konektivitas antar jaringan lokal jarak jauh menggunakan jaringan publik untuk konektivitas. Namun, tunneling tidak memberikan pedoman untuk semua kondisi topologi jaringan saat menggunakan teknik tersebut. Dengan kata lain, tunneling hanya boleh digunakan berdasarkan pengalaman dan SOP. Ada berbagai merek peralatan untuk mendukung pembangunan *tunneling* di Indonesia. Salah satu merek yang digunakan adalah Cisco. Makalah ini berfokus pada *tunnel* yang dimiliki perangkat Cisco.

[2] Virtual Private Network (VPN), merupakan sebuah jaringan yang dibuat untuk melakukan transaksi data yang telah dienkripsi antara dua atau lebih pengguna jaringan yang memanfaatkan jaringan publik. Jaringan VPN seluruhnya menggunakan [3] internet sehingga faktor keamanan menjadi sangat penting. Dengan berkembangnya teknologi dan informsai yang sangat cepat pada saat ini menjadikan beberapa serangan yang mungkin terjadi di jaringan internet seperti [4] Denial of Service (DoS) attack, sniffing, spoofing, session hijacking.

Pada skala penyedia cloud saat ini, [5] gateway VPN perlu menyimpan informasi untuk sekitar satu juta tunnel internal. Kami berpendapat bahwa tidak ada perangkat komoditas tunggal yang dapat menangani banyak terowongan ini sambil memberikan kepadatan port yang cukup tinggi untuk terhubung ke ratusan pelanggan cloud di edge.

Salah satu tantangan yang diidentifikasi oleh International Telecommunication Union (ITU) dalam laporan mereka tentang [6] “The Internet of Things” adalah masalah privasi dan keamanan. Ketika kita mulai dikelilingi oleh benda-benda pintar yang bergerak, mengumpulkan informasi tentang kehidupan, perilaku, atau kebiasaan kita, akan ada kekhawatiran besar mengenai keamanan informasi itu, dengan implementasi vpn memberikan keamanan ke aplikasi IoT menggunakan solusi BITW IPSec.

Didapatkan bahwa layanan [7] PPTP memiliki kelemahan dalam hal kecepatan dan keamanan dibanding OpenVPN. Kelemahan PPTP ini diakibatkan tidak terdapatnya enkripsi yang baik pada pengiriman paket yang dilakukan sehingga bisa ditangkap dengan menggunakan aplikasi tertentu. L2TP adalah tunneling yang bekerja di layer 2, tetapi ia tidak memiliki pengamanan khusus sehingga biasanya ditambahkan sistem keamanan yang lebih baik, yaitu menggunakan IPSec.

1.1 Virtual Private Network

Virtual private network [8] (VPN) adalah teknologi komunikasi yang memungkinkan Anda terhubung ke jaringan publik dan menggunakannya untuk berpartisipasi dalam jaringan area lokal. Dengan cara ini Anda mendapatkan izin dan pengaturan yang sama dengan LAN itu sendiri, tetapi Anda sebenarnya menggunakan jaringan publik yang tidak memberikan dukungan keamanan yang memadai. Dari perspektif perusahaan, IP sekarang menjadi persyaratan mendasar untuk pertukaran data antar cabang atau dengan mitra perusahaan. VPN tampaknya menyelesaikan masalah ini. Jaringan perusahaan yang menghubungkan kantor cabang melalui pengalamatan pribadi dengan menggunakan infrastruktur IP untuk mengamankan transmisi paket data.

1.2 Internet Protocol Security (IPSec)

IPsec, kependekan dari IP Security, adalah protokol untuk mengamankan transmisi datagram dalam jaringan berbasis TCP/IP. [9] IPsec adalah Layer 2 dari Model Referensi DARPA (Lapisan Internet) dan mendefinisikan beberapa standar untuk enkripsi data dan integritas data. IPsec mengenkripsi data pada tingkat yang sama dengan protokol IP dan menggunakan teknologi tunneling untuk mengirimkan informasi secara aman melalui Internet atau intranet. IPsec didefinisikan oleh Internet Engineering Task Force [6] (IETF) dan diimplementasikan di banyak sistem operasi. Windows 2000 adalah sistem operasi Microsoft pertama yang mendukung IPsec. IPsec di implementasikan pada lapisan transport model

referensi OSI [8] dan melindungi IP dan protokol tingkat yang lebih tinggi menggunakan beberapa kebijakan keamanan yang dapat dikonfigurasi untuk memenuhi persyaratan keamanan pengguna atau jaringan. IPsec biasanya dimasukkan sebagai lapisan tambahan dalam tumpukan protokol TCP/IP [10], tunduk pada kebijakan keamanan yang diinstal pada setiap komputer dan skema enkripsi yang dapat dinegosiasikan antara pengirim dan penerima.

Kebijakan keamanan ini berisi kumpulan filter yang terkait dengan tindakan tertentu. Ketika alamat IP paket datagram IP, nomor port TCP dan UDP [10], atau protokol cocok dengan filter tertentu, tindakan terkait diterapkan ke paket IP tersebut. IPSec terutama menggunakan tiga protokol termasuk header otentikasi (AH), muatan keamanan yang dienkapsulasi (ESP) dan pertukaran kunci internet (IKE) untuk menawarkan fungsi enkripsi, [3] otentikasi, dan manajemen pertukaran kunci. IPSec menyediakan dua mode termasuk terowongan dan transportasi. Dalam mode Transport, [6] header IP asli tidak boleh diubah, dan informasi header IPSec dienkapsulasi antara header IP dan data dari pesan asli, yang sesuai dengan komunikasi antara host. Dalam mode Tunnel, pesan asli bersama dengan header IPSec, dan header IP baru cocok untuk komunikasi antara jaringan area lokal.

1.3 Generic Routing Encapsulation (GRE)

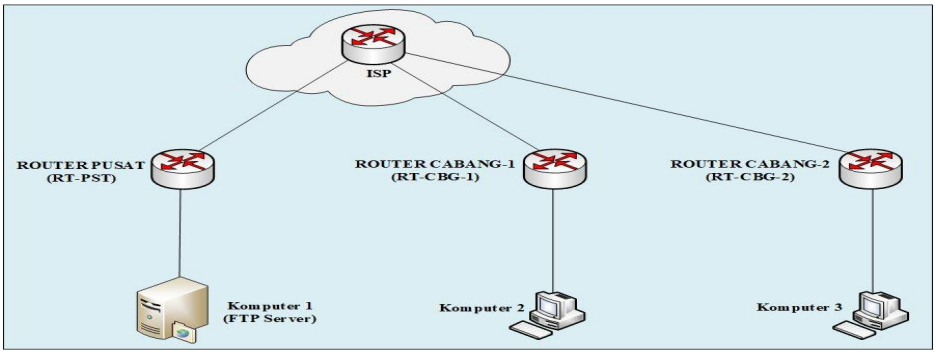
GRE adalah protokol yang menggunakan teknologi tunneling antar lapisan protokol. Terowongan adalah antarmuka virtual yang mendukung konektivitas point-to-point. Ini menyediakan saluran untuk transmisi paket data, merangkum protokol lain dengan protokol, dan merangkum dan membuka paket data di kedua ujung terowongan. [11] Paket dienkapsulasi dan didekapsulasi di kedua ujung terowongan. Ketika antarmuka sumber terowongan GRE menerima pesan data, pertama-tama ia mengenkapsulasi header dan ekor GRE dari paket data asli, kemudian menambahkan header IP baru dan mengirimkan paket data yang dienkapsulasi ke ujung terowongan yang lain.

Mengirim paket data dan mengirimkannya ke tujuannya. Teknologi GRE memiliki keunggulan mendukung multicast dan broadcast. GRE tunnel merupakan protokol tunneling yang dikembangkan oleh Cisco dan menyediakan encapsulasi untuk berbagai layer protokol jaringan pada jaringan point to point. [12] GRE tunnel dibangun antara router asal dan router tujuan sehingga paket yang di-forward melalui tunnel sebelumnya telah diencapsulasi oleh header yang baru (GRE header).

2. METODE PENELITIAN

3.

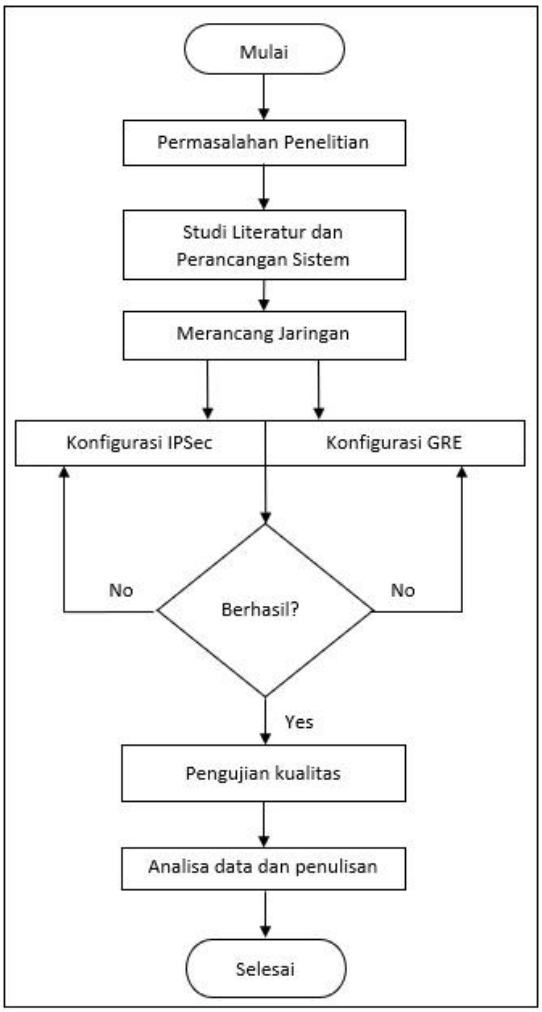
Perancangan metode penelitian dilakukan dengan langkah-langkah sebagai berikut. Observasi dilakukan untuk memperoleh data, yang dicari dengan referensi dan studi literatur berupa buku, jurnal, penelitian, karya ilmiah, artikel tentang perangkat Cisco yang digunakan, seperti Internet Protocol Security (IPSec) dan Generic Routing Encapsulation (GRE), serta mempelajari unjuk kerja protokol NAT, ACL, routing static dan routing dynamic BGP sebagai pendukung penelitian.



Gambar. 1 Topologi implementasi point to point (Olahan Data Sendiri dari Pengolahan Data)

2.3 Rancangan Pengujian

Tahapan ini melakukan perancangan sistem dan alur untuk jaringan point to point yang dibangun. Untuk perancangan ini, beberapa yang akan disusun adalah jalur topology jaringan WAN seperti pada gambar 1 di atas.



Gambar. 2 Diagram alir penelitian

Perancangan sistem kemudian dilakukan dengan menggunakan aplikasi GNS3 yang dapat dikonfigurasi seperti aslinya. Desain membutuhkan router Cisco, server FTP, dan komputer klien. Router Cisco bertanggung jawab untuk merutekan antarmuka tempat mereka terhubung dengan mengatur konfigurasi sesuai dengan desain yang dibuat. Komputer 1 bertanggung jawab untuk mengunggah file ke server FTP. Komputer 2 dan Komputer 3, di sisi lain, bertindak sebagai pengirim dan penerima dalam skenario teknologi jaringan. Komputer 3 (server FTP) bertanggung jawab untuk melayani komputer 1 dan komputer 2. Perangkat lunak Wireshark memungkinkan untuk melakukan akuisisi data dan analisis lalu lintas di server sesuai dengan skenario rekayasa jaringan yang telah dibuat.

Untuk menguji kualitas layanan serta mendapatkan rekomendasi saat yang tepat menggunakan teknik IPSec dan GRE, dilakukan skenario rekayasa jaringan, yaitu menggunakan topologi start, sebagai berikut.

1. Melakukan pembentukan topologi dan konfigurasi protokol sesuai perancangan seperti yang ditunjukkan pada gambar 1
2. Membuat layanan FTP Server pada jaringan pusat untuk dapat diakses oleh komputer 2 & 3.

3. Mengatur user password untuk akses Server FTP dari masing-masing komputer 2 & 3.
4. Melakukan pengaturan awal komputer 1 mengunggah file 50MB ke server FTP, Komputer 2 dan Komputer 3 menggunakan perangkat lunak TFGen untuk menjalankan skenario rekayasa lalu lintas, dan perangkat lunak Wireshark untuk menangkap lalu lintas masuk dari Komputer 1 ke server FTP.
5. Melakukan pengujian pada sisi router tempat IPSec dan GRE tunnel dipasang dengan melakukan ping dan tracing koneksi selama proses upload file dan traffic engineering. Perintah ping digunakan untuk menampilkan hasil run-time, dan jejak menunjukkan jalur yang diambil oleh komputer klien.

Berikut adalah pengaturan alamat IP yang digunakan untuk pengujian pada setiap masing-masing perangkat sebagai berikut:

Tabel 1. Pengaturan Alamat IP Router & PC

No	Nama Perangkat	Port	IP Address	Subnet	Gateway
1	ISP	Fastethernet 0/0	101.128.64.1	255.255.255.252	N/A
		Fastethernet 1/0	101.128.64.5	255.255.255.252	N/A
		Fastethernet 2/0	101.128.64.9	255.255.255.252	N/A
2	RT-PST	Fastethernet 0/0	101.128.64.2	255.255.255.252	101.128.64.1
		Fastethernet 1/0	192.168.10.1	255.255.255.0	N/A
		Tunnel 0	10.10.10.1	255.255.255.252	N/A
3	Komputer 1 (FTP Server)	Ethernet 0	192.168.10.10	255.255.255.0	192.168.10.1
4	RT-CBG-1	Fastethernet 0/0	101.128.64.6	255.255.255.252	101.128.64.5
		Fastethernet 1/0	192.168.20.1	255.255.255.0	N/A
5	Komputer 2	Ethernet 0	192.168.20.2	255.255.255.0	192.168.20.1
6	RT-CBG-2	Fastethernet 0/0	101.128.64.10	255.255.255.252	101.128.64.9
		Fastethernet 1/0	192.168.30.1	255.255.255.0	N/A
		Tunnel 0	10.10.10.2	255.255.255.252	N/A
7	Komputer 3	Ethernet 0	192.168.30.2	255.255.255.0	192.168.30.1

Alat-alat yang digunakan untuk mendukung penelitian ini meliputi mulai dari perangkat keras komputer dan Software simulator jaringan GNS3 untuk menjalankan perangkat jaringan secara virtual dan iOS Cisco Series 3600 yang digunakan, adapun peralatan sebagai berikut dapat dilihat pada tabel 2 dan 3.

Tabel. 2 Spesifikasi Perangkat Keras

No	Jenis Hardware	Spesifikasi	Jumlah
1	Laptop	Lenovo T440 14”	1
2	CPU	Intel Core i5 @ 1.90GHz - 2.49GHz	1
3	RAM	Samsung DDR3 8 Gigabyte	1
4	Storage / HDD	HGST 500 Gigabyte	1
5	Motherboard	Lenovo T440	1
6	Power Supply	Lenovo T440	1
7	Keyboard & Trackpad	Lenovo T440	1

Tabel. 3 Spesifikasi Perangkat Lunak

No	Spesifikasi	Jumlah	Keterangan
1	Windows 10 x64	1	Laptop yang digunakan untuk pengujian
	VMware	1	Untuk instalasi vm server GNS3, FTP Server & komputer klien
2	Windows 8	1	Sebagai Server FTP
3	Windows 7	2	Komputer 2 & 3
5	GNS3 version 2.1.21	1	Aplikasi simulator
6	GNS3 VM 2.1.21	1	VM Server GNS3
7	Cisco iOS 3600 Series	4	Router Cisco
8	Wireshark	1	Analisa trafik jaringan
9	Filezilla Server	1	Aplikasi FTP Server
10	WinSCP	2	FTP Client

3. HASIL DAN PEMBAHASAN

Penelitian ini diujicobakan untuk mengetahui proses dari terbentuknya sinkronisasi antar router pusat dengan router cabang baik yang menggunakan IPSec dan GRE, selanjutnya akan dilakukan *trace, ping,* unduh dan unggah data melalui FTP dari komputer 2 & 3 ke komputer 1 (FTP Server) secara topologi dari router cabang ke router pusat melewati ISP dan memiliki 2 hop untuk mencapai komputer 1 (FTP-Server), karena disini mengimplentasikan VPN IPSec dan GRE maka yang terjadi adalah antar router pusat dan cabang seakan terhubung langsung jadi hanya 1 hop melewati *tunnel*, seperti terlihat pada gambar 3 & 4 proses encryption dan encapsulation dari masing-masing aturan yang digunakan.

No.	Time	Source	Destination	Protocol	Length	Info
19063	724.824432	101.128.64.2	101.128.64.6	ISAKMP	214	Quick Mode
19064	724.856828	101.128.64.6	101.128.64.2	ISAKMP	214	Quick Mode
19065	724.867340	101.128.64.2	101.128.64.6	ISAKMP	94	Quick Mode
19242	793.251636	101.128.64.6	101.128.64.2	ISAKMP	110	Informational
291451	4183.048084	101.128.64.2	101.128.64.6	ISAKMP	214	Quick Mode
291452	4183.081085	101.128.64.6	101.128.64.2	ISAKMP	214	Quick Mode
291453	4183.104343	101.128.64.2	101.128.64.6	ISAKMP	94	Quick Mode
293464	4236.679779	101.128.64.6	101.128.64.2	ISAKMP	110	Informational

Gambar. 3 IPSec tunnel encryption (Sumber Olahan Data Sendiri dari Pengolahan Data)

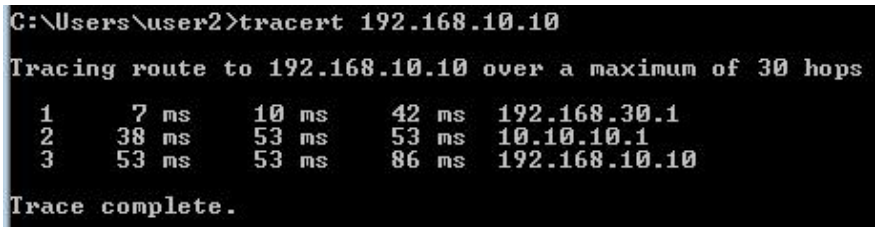
	Time	Source	Destination	Protocol	Length	Info
16	6.051287	101.128.64.2	101.128.64.10	GRE	70	Encapsulated Possible GRE keepalive packet
17	6.061644	101.128.64.2	101.128.64.10	GRE	42	Encapsulated Possible GRE keepalive packet
25	9.684515	101.128.64.10	101.128.64.2	GRE	70	Encapsulated Possible GRE keepalive packet
26	9.717010	101.128.64.10	101.128.64.2	GRE	42	Encapsulated Possible GRE keepalive packet

Gambar. 4 GRE tunnel encapsulation (Sumber Olahan Data Sendiri dari Pengolahan Data)

```
C:\Users\user1>tracert 192.168.10.10

Tracing route to 192.168.10.10 over a maximum of 30 hops

  1     8 ms    10 ms    10 ms  192.168.20.1
  2     *        *        *     Request timed out.
  3    87 ms    95 ms    63 ms  192.168.10.10

Trace complete.
```

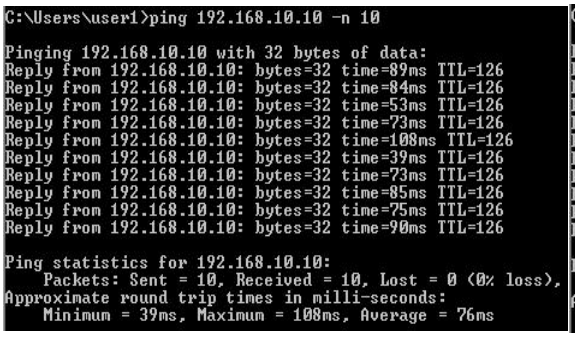
Gambar. 5 hasil *trace* komputer 2 (Sumber Olahan Data Sendiri dari Pengolahan Data)

Dapat terlihat dari hasil *trace* dari komputer 2 ke server ftp (gambar 5), pada hop pertama adalah ip gateway yang ada di router milik komputer 2 dan hop kedua adalah router pusat tapi disni tidak terlihat alamat ip berapa yang digunakan itu karena secara default IPSec tidak mengirimkan balik pesan trace yang dikirim oleh komputer 2.

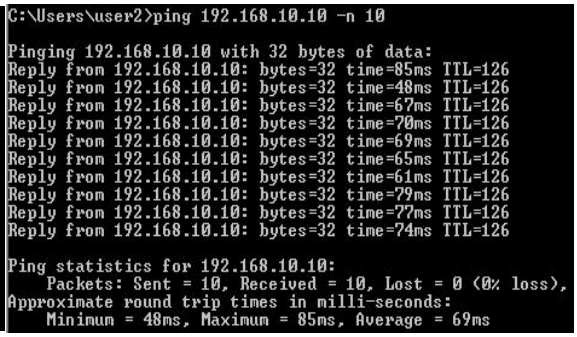


Gambar 6. Hasil *trace* komputer 3 (Sumber Olahan Data Sendiri dari Pengolahan Data)

Sementara terlihat dari hasil *trace* dari komputer 3 ke server ftp (gambar 6), pada hop pertama adalah ip gateway yang ada di router milik komputer 3 dan hop kedua adalah router pusat dan dapat terlihat ip yang digunakan adalah alamat ip yang ada pada antarmuka GRE tunnel.

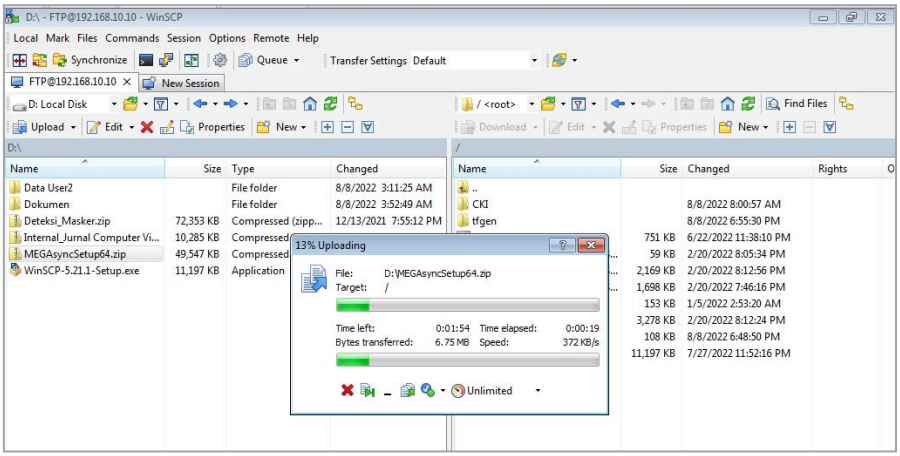


Gambar 7. Hasil *ping* komputer 2
Sumber: Gambar Olahan Data Sendiri dari Pengolahan Data

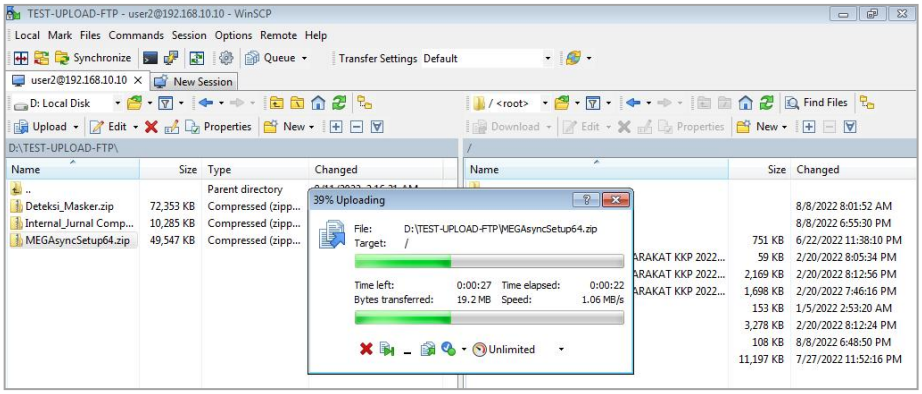


Gambar 8. Hasil *ping* komputer 3
Sumber: Gambar Olahan Data Sendiri dari Pengolahan Data

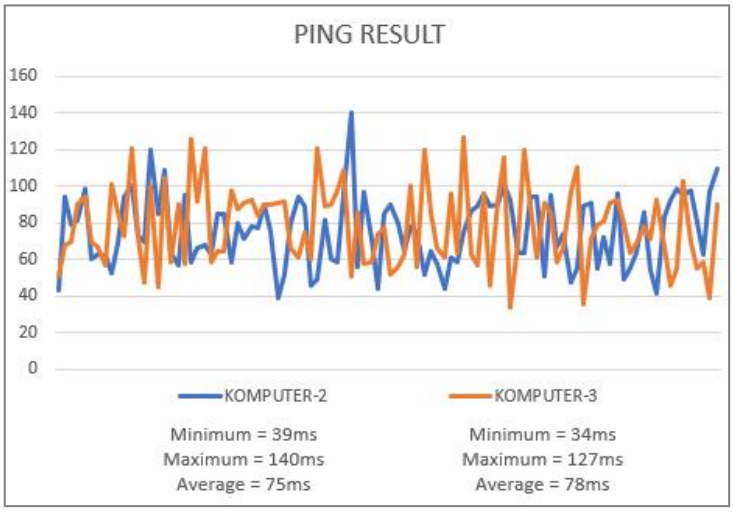
Dari hasil ping tanpa beban dari komputer 2 & 3 ke server ftp dapat terlihat berjalan normal dengan rata-rata 76 ms; untuk komputer 2 dan 69 ms; untuk hasil ping komputer 3 tanpa ada request time out (RTO) secara koneksi vpn tunnel antar router established.



Gambar 9. Test upload komputer 2 ke FTP Server (Sumber Olahan Data Sendiri dari Pengolahan Data)



Gambar 10. Test upload komputer 3 ke FTP Server (Sumber Olahan Data Sendiri dari Pengolahan Data)



Gambar 11. Ping komputer 2 & 3 ke FTP Server (Sumber Olahan Data Sendiri dari Pengolahan Data)

Pada pengujian saat dilakukan upload file sebesar 50 Megabyte terlihat pada gambar 9 & 10 dari komputer 2 dan komputer 3 ke FTP Server dengan througphut 0,878 Mbps pada komputer 2 dan 1,060 Mbps trafik masih normal dengan ping menggunakan beban rata-rata 75ms untuk komputer 2 dan 78ms untuk komputer 3 selama proses upload file tidak mengalami kendala pada jaringan atau request time out (RTO).

4. KESIMPULAN

Sehingga dari hasil penelitian dapat disimpulkan bahwa optimasi jaringan point to point menggunakan VPN IPSec dan GRE ini dapat dibangun dengan baik dan komunikasi pertuakaran data antar pusat dan cabang berjalan dengan lancar melalui dua metode yang berbeda. Selain itu, IPSec dan GRE memiliki perbedaan untuk mengamankan tarfik yang di lewatinya IPSec mengenkrispi IP router pada host yang dituju saat dilakukan trace. Sementara dari hari trace ip host dengan metode GRE dapat terlihat ip point to point yang digunakan untuk membangun *tunnel*. Pada saat dilakukan pengujian ping dengan beban rata-rata hasil yang di dapat 75ms untuk komputer 2 dan 78ms untuk komputer 3 selama proses upload file tidak mengalami kendala pada jaringan atau request time out (RTO).

5. SARAN

Menggunakan metode IPSec lebih kompleks secara penerapan konfigurasi untuk mengizinkan ip dengan segmen berapa saja yang akan di izinkan keluar masuk melalui IPSec, sementara untuk GRE lebih mudah untuk diterapakan baik di jaringan yang baru dibangun ataupun yang sudah banyak perkembangan segment.

DAFTAR PUSTAKA

[1] R. Muhammad Arifin, Eni Dwi Wardhani, and Samuel BETA, "Implementasi Tunnel GRE pada Jaringan Ring dan Mesh Perangkat Metro-E Nokia," *J. Nas. Tek. Elektro dan Teknol. Inf.*, vol. 10, no. 3, pp. 204–213, 2021, doi: 10.22146/jnteti.v10i3.1795.

[2] G. Wang, Y. Sun, Q. He, G. Xin, and B. Wang, "A content auditing method of IPsec VPN," *Proc. - 2018 IEEE 3rd Int. Conf. Data Sci. Cyberspace, DSC 2018*, pp. 634–639, 2018, doi: 10.1109/DSC.2018.00101.

[3] H. Gunleifsen, T. Kemmerich, and V. Gkioulos, "Dynamic setup of IPsec VPNs in service function chaining," *Comput. Networks*, vol. 160, pp. 77–91, 2019, doi: 10.1016/j.comnet.2019.05.015.

[4] Y. L. Aung, H. H. Tiang, H. Wijaya, M. Ochoa, and J. Zhou, "Scalable VPN-forwarded Honeypots: Dataset and Threat Intelligence Insights," *ACM Int. Conf. Proceeding Ser.*, vol. PartF16834, pp. 21–30, 2020, doi: 10.1145/3442144.3442146.

[5] 一种vpn网关支持数万连接，还有软硬件vpn网关实例, "Public Review for A Scalable VPN Gateway for Multi-Tenant Cloud Services Public review written by A Scalable VPN Gateway for Multi-Tenant Cloud Services," vol. 48, no. 1, pp. 49–55.

[6] M. Rao, J. Coleman, and T. Newe, "An FPGA based reconfigurable IPSec ESP core suitable for IoT applications," *Proc. Int. Conf. Sens. Technol. ICST*, pp. 1–5, 2016, doi: 10.1109/ICSensT.2016.7796269.

[7] S. Ikhwan and A. Amalina, "Analisis Jaringan VPN Menggunakan PPTP dan L2TP (Studi Kasus : Dinhubkominfo Kabupaten Banyumas)," *J. Infotel*, vol. 9, no. 3, pp. 265–270, 2017.

[8] Y. Shen, Q. F. Zhang, L. Di Ping, Y. F. Wang, and W. J. Li, "A multi-tunnel VPN concurrent system for new generation network based on user space," *Proc. 11th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. - 11th IEEE Int. Conf. Ubiquitous Comput. Commun. IUCC-2012*, pp. 1334–1341, 2012, doi: 10.1109/TrustCom.2012.41.

[9] Chaitanya and N. Roberts, "A Multilayer Application-Aware IPSec Mechanism for IP Multimedia Subsystem," *Int. J. Futur. Comput. Commun.*, vol. 3, no. 4, pp. 247–251, 2014, doi: 10.7763/ijfcc.2014.v3.305.

[10] I. Coonjah, P. C. Catherine, and K. M. S. Soyjaudah, "Design and Implementation of UDP Tunneling-based on OpenSSH VPN," *Proc. - IEEE 2018 Int. Conf. Adv. Comput. Commun. Control Networking, ICACCCN 2018*, no. 1, pp. 640–645, 2018, doi: 10.1109/ICACCCN.2018.8748849.

[11] J. Li and M. Zhou, "Research on VPN in experimental simulation environment based on GRE and IPSec," *ACM Int. Conf. Proceeding Ser.*, pp. 220–224, 2020, doi: 10.1145/3449301.3449338.

[12] B. Almási, G. Lencse, and S. Szilágyi, "Investigating the multipath extension of the GRE in UDP technology," *Comput. Commun.*, vol. 103, pp. 29–38, 2017, doi: 10.1016/j.comcom.2017.02.002.