Jurnal Politeknik Caltex Riau
Terbit Online pada laman https://jurnal.pcr.ac.id/index.php/jkt/
| **e- ISSN: 2460-5255 (Online) | p- ISSN: 2443-4159 (Print) |**

Implementasi GRE Over IPSec Tunnel VPN Menggunakan Fortigate

Maruf Alfiando Setianto[1], Yuli Fitrisia*[2]

[1,2]Teknik Rekayasa Komputer, Politeknik Caltex Riau, Pekanbaru, Indonesia
[1]*maruf.setianto@alumni.pcr.ac.id*, [2*]*uli@pcr.ac.id*
**Corresponding Author*

Diserahkan: 03 Agustus 2023 Diterima: 13 November 2023 Diterbitkan: 22 Desember 2023

ABSTRAK

VPN adalah sebuah teknologi komunikasi yang menggunakan jaringan private (pribadi) yang dapat terhubung ke sebuah jaringan publik. Dengan cara tersebut, maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada didalam jaringan local walaupun sebenarnya menggunakan jaringan publik. Pada penelitian ini, protocol yang digunakan adalah protokol GRE over IPSec. GRE adalah protokol enkapsulasi yang secara default tidak mendukung keamanan enkripsi. Maka untuk menambahkan lapisan enkripsi di GRE Tunnel digunakanlah IPSec dan protokol enkripsi IKEv2. Oleh karena itu, diimplementasikanlah kombinasi antara GRE dan IPSec pada Fortigate yang memungkinkan pengguna untuk membuat jalur tuneling aman antara dua jaringan yang berbeda. Seluruh lalu lintas data yang melewati jalur tuneling akan dienkripsi menggunakan protokol IPSec. Selain keamanan, performa jaringan juga menjadi hal yang penting dalam membangun jaringan GRE over IPSec yang efektif dan efisien. Penggunaan protokol keamanan seperti IPSec dapat mempengaruhi performa jaringan karena proses enkripsi dan dekripsi data dapat memakan waktu dan sumber daya yang signifikan. Setelah berhasil membangun VPN tunnel GRE Over IPSec, kemudian jaringan tersebut diuji. Hasil pengujian terhadap GRE Over IPSec tunnel VPN dengan protokol IKEv2 sudah berjalan dengan baik dan paket yang melalui tunnel tersebut sudah terenkripsi dengan aman. Selain itu, juga dilakukan pengujian terhadap performa jaringan GRE over IPSec pada Fortigate untuk mengukur delay dan throughput paket yang dikirim. Pengujian dilakukan melalui dua proses pengujian yaitu upload dan download dengan berbagai jenis paket data seperti teks, gambar, suara dan video. Berdasarkan hasil pengujian, delay berada pada nilai <150 ms dan throughput berada pada nilai >100 bps. Berdasarkan, standar yang dikeluarkan oleh THIPON, delay dan throughput termasuk kedalam kategori "sangat bagus".

Kata kunci: *Fortigate, GRE, IPSec, VPN Tunnel*

ABSTRACT

VPN is a communication technology that uses a private network that can be connected to a public network. In this way, it will get the same rights and settings as if you were on a local network, even though you are actually using a public network. In this study, the protocol used was the GRE over IPSec protocol. GRE is an encapsulation protocol that by default does not support encryption security. So, to add an encryption layer in the GRE Tunnel, IPSec and the IKEv2 encryption protocol are used. Therefore, a combination of GRE and IPSec is implemented in Fortigate which allows users to create a secure tuning path between two different networks. All data traffic passing through the tuning line will be encrypted using the IPSec protocol. Apart from security, network performance is also important in building an effective and efficient GRE over IPSec network. The use of security protocols such as

IPSec can affect network performance because the process of encrypting and decrypting data can take significant time and resources. After successfully building a GRE Over IPSec VPN tunnel, the network is then tested. The test results for the GRE Over IPSec VPN tunnel with the IKEv2 protocol are running well and packets passing through the tunnel are securely encrypted. Apart from that, testing was also carried out on the performance of the GRE over IPSec network on Fortigate to measure the delay and throughput of packets sent. Testing is carried out through two testing processes, namely uploading and downloading with various types of data packages such as text, images, voice and video. Based on the test results, delay is <150 ms and throughput is >100 bps. Based on the standards issued by THIPON, delay and throughput are included in the "very good" category.

Keywords: *Fortigate, GRE, IPSec, VPN Tunnel*

1. PENDAHULUAN

VPN adalah sebuah teknologi komunikasi yang menggunakan jaringan private (pribadi) yang dapat terhubung ke sebuah jaringan publik. Sampai saat ini, ada banyak sekali perusahaan yang melakukan akses langsung ke internet untuk kepentingan pekerjaan. Masalah yang sering dihadapi adalah tidak mempunyai dukungan yang baik terhadap keamanan pada jaringan publik atau internet sehingga komunikasi antar jaringan dapat diserang atau dimanipulasi oleh pihak yang tidak bertanggung jawab[1]. Solusinya adalah dengan menerapkan teknologi VPN yang muncul untuk mengatasi persoalan tersebut. Sebuah perusahaan jaringan yang menggunakan infrastruktur IP untuk berhubungan langsung dengan instansi melakukan pengalamatan IP secara private sekaligus melakukan pengamanan terhadap transmisi paket data.

Untuk membangun sebuah VPN memerlukan enkapsulasi untuk menghubungkan antara dua node jaringan. Hal ini dapat dilakukan dengan menggunakan protokol GRE. Generic Routing Encapsulation (GRE) adalah protokol enkapsulasi yang secara default tidak mendukung keamanan enkripsi. Membuat *tunnel* GRE *point to point* tanpa enkripsi sangat berisiko karena data sensitif dapat dengan mudah diekstraksi dari *tunnel* dan dilihat oleh orang lain[2]. Maka untuk menambahkan lapisan enkripsi di GRE *tunnel* dapat dilakukan dengan dukungan IPSec dan protokol enkripsi IKEv2. GRE Over IPSec memiliki kelebihan seperti, menghubungkan subnet yang tidak continue, penggunaan sumber daya yang rendah, mendukung pesan unicast, multicast, dan broadcast, dapat mengenkapsulasi semua jenis protokol layer 3. IPSec dirancang untuk menyediakan keamanan berbasis kriptografi yang mendefinisikan beberapa standar keamanan untuk melakukan enkripsi, autentikasi dan integritas data pada internetwork layer. IPsec melakukan enkripsi terhadap bagian data pada lapisan yang sama dengan protokol header pada paket IP dan bagian protokol distribusi kunci secara otomatis (IKEv2).

Selain keamanan, performa jaringan juga menjadi hal yang penting dalam membangun jaringan GRE over IPSec yang efektif dan efisien. Penggunaan protokol keamanan seperti IPSec dapat mempengaruhi performa jaringan karena proses enkripsi dan dekripsi data dapat memakan waktu dan sumber daya yang signifikan. Pengukuran performa jaringan pada GRE over IPSec yang akan dibangun sangat diperlukan untuk memastikan bahwa jaringan berjalan dengan baik dan optimal, serta dapat memberikan kecepatan dan kinerja yang memadai untuk kebutuhan komunikasi antar jaringan. Dalam pengukuran performa jaringan, beberapa faktor yang perlu diperhatikan antara lain Delay dan Throughput.

Oleh karena itu, untuk menyelesaikan penelitian ini dibutuhkan perangkat yang mengimplementasikan GRE over IPSec VPN *Tunnel*, yaitu perangkat Fortigate. Dalam hal ini, perangkat Fortigate dapat digunakan karena selain sebagai VPN Gateway yang dapat menerapkan GRE over IPSec, juga berfungsi sebagai firewall, router, dan gateway bagi jaringan LAN, sehingga dapat menjamin keamanan jaringan secara keseluruhan.

2. TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Referensi [3] berdasarkan segi aspek keamanan VPN harus diperhatikan karena serangan pada komunikasi jaringan VPN dapat masuk dengan mudah tanpa adanya keamanan. Solusinya, dibutuhkan sebuah keamanan firewall atau filtering pada protokol EoIP. Hasil penelitian ini dapat mengamankan koneksi pada protokol EoIP karena jalur data dialirkan pada jalur *tunneling* sehingga tidak melewati routing di internet, tetapi dalam aspek keamanan EoIP tidak memberlakukan keamanan enkripsi.

Referensi [4] solusi VPN dapat digunakan pada infrastruktur jaringan nirkabel untuk mengamankan transmisi antara klien nirkabel dan jaringan perusahaan kabel. Karena *tunneling* melibatkan pengemasan ulang data lalu lintas ke dalam bentuk yang berbeda, mungkin dengan enkripsi sebagai standar. Penggunaan ketiga adalah untuk menyembunyikan sifat lalu lintas yang dijalankan melalui *tunnel*. Generik Routing Encapsulation (GRE) protokol tunneling memberikan pendekatan generik sederhana untuk mengangkut paket satu protokol melalui protokol lain dengan cara enkapsulasi.

Referensi [5] berdasarkan hasil pengujian yang telah dilakukan, protokol IPSec lebih optimal dibandingkan dengan protokol SSL karena memiliki nilai throughput lebih tinggi pada protokol IPSec dibandingkan nilai throughput pada protokol SSL. Selain itu IPSec sangat cocok untuk digunakan pada komunikasi antar gateway.

Referensi [6] berdasarkan hasil pengujian yang telah dilakukan, pengujian ini diterapkan pada penggunaan MPEG4 dan Codec MJPEG CCTV IP dengan membandingkan performansi protokol IPSec dan SSL. Hasil penelitian menunjukkan bahwa protokol IPSec memiliki kualitas performansi yang lebih baik dibandingkan protokol SSL.

Referensi [7] pada penelitian ini, membandingkan kinerja GRE *tunnel* dengan PPPoE *tunnel* dari segi Quality Of Service (QOS) fokus pada delay dan throughput. Pengujian menggunakan perangkat mikrotik routerboard yang saling terhubung melalui konfigurasi GRE *tunnel* dan PPPoE *tunnel*. Dalam pengujian, client melakukan download file pada server dummies berukuran 100 MB, 300 MB, dan 500 MB dengan berekstensi rar dan exe. Pengujian dilakukan sebanyak tiga kali, dijumlahkan dan diambil nilai rata- rata. Hasil pengujian disajikan dalam bentuk tabel dan grafik. Dari hasil pengujian, PPPoE tunnel lebih unggul dibandingkan dengan GRE tunnel terhadap parameter Quality Of Service (QOS) khususnya delay dan throughput.

Referensi [8] berdasarkan pengujian terhadap keamanan IPSec Site-to-Site VPN dengan protokol IKEv2 sudah berjalan dengan baik yang didukung oleh protokol ESP dan SPI. Sedangkan hasil pengukuran kinerja throughput pada layanan Audio dan Video termasuk dalam kategori “Sangat Buruk” menurut TIPHON dan hasil pengukuran throughput pada layanan FTP termasuk dalam kategori “Buruk” menurut TIPHON. Kemudian, hasil pengukuran delay pada layanan Audio, Video dan FTP termasuk dalam kategori “Sangat Bagus” menurut TIPHON. Sedangkan, hasil pengukuran packet loss pada layanan Audio, Video dan FTP sebesar 0 % yang termasuk dalam kategori “Sangat Bagus” menurut TIPHON.

Referensi [9] hasil dari penelitian dengan dual link jaringan FO lebih bagus dibanding dengan modem GSM, dengan nilai rata – rata FO yaitu packet loss 1%, delay FO 0,105 s, dan latency dual link sangat bagus. Namun disisi lain jaringan GSM mampu membackup ketika jaringan FO down, sehingga meminimalisir terjadinya downtime.

Referensi [10] penelitian ini mensimulasikan jaringan site to site IPsec VPN menggunakan simulator EVE-NG untuk menjalankan dua algoritma enkripsi keamanan jaringan point to point, yaitu IPSec dengan algoritma enkripsi default AES (Advanced Encryption Standard) dan IPSec (Internet Protocol Security) dengan algoritma enkripsi Blowfish dalam mengenkripsi trafik data yang dikirim melalui jaringan publik. Uji upload file sebesar 900 Megabyte dari komputer 2 dan

komputer 3 ke FTP (File Transfer Protocol) Server dengan throughput 3,51 MBps dengan algoritma enkripsi AES; dan throughput 3,81 MBps dengan algoritma enkripsi Blowfish.

Referensi [11] penelitian ini bertujuan untuk membangun VPN (Virtual Private Network) berbasis IPSec. Penelitian dilakukan pada jaringan Wide Area Network menggunakan dua buah perangkat FortiGate sebagai firewall dangan gateway yang saling terhubung dan membentuk *tunnel* sebagai jalur khusus yang menghubungkan jaringan private antar kampus secara aman.

2.2 Landasan Teori

2.2.1 VPN

Referensi [8],[12] VPN (Virtual Private Network) merupakan sebuah teknologi komunikasi yang memungkinkan pengguna terhubung ke jaringan publik dan memanfaatkannya untuk bergabung dengan jaringan lokal. Dengan cara ini, pengguna memperoleh akses dan hak yang setara dengan yang ada di dalam jaringan lokal, meskipun sebenarnya menggunakan infrastruktur jaringan publik. Teknologi VPN menyediakan tiga fungsi utama, yaitu:

i) Confidentially (kerahasiaan)
ii) Data Integrity (Keutuhan Data)
iii) Origin Authentication (Autentikasi Sumber)

2.2.2 GRE (Generic Routing Encapsulation)

Referensi [9] Generik Routing Encapsulation (GRE) tunneling adalah sebuah metode yang sederhana namun efektif untuk mengangkut paket data dari satu protokol melalui protokol lain dengan menggunakan enkapsulasi. GRE berfungsi sebagai protokol pembawa yang dapat digunakan untuk berbagai protokol penumpang. Saat melakukan enkapsulasi, GRE menyimpan paket data asli yang akan disampaikan ke jaringan tujuan dalam sebuah paket IP luar. Setelah mencapai titik akhir tunnel, proses enkapsulasi GRE dihapus, dan muatan (payload) dari paket data tersebut diteruskan langsung ke tujuan yang dituju.

2.2.3 IPSec (IP Security)

Referensi [10] IPSec (IP Security) adalah sebuah protokol yang digunakan untuk mengamankan transmisi datagram dalam jaringan berbasis TCP/IP. IPSec menyediakan layanan keamanan pada lapisan IP dengan memberikan fleksibilitas bagi sistem untuk memilih protokol keamanan yang sesuai, menentukan algoritma yang digunakan, dan menyimpan kunci kriptografi yang diperlukan untuk layanan yang diminta. Penggunaan IPSec dapat melindungi jalur komunikasi antara sepasang host, antara sepasang security gateway, atau antara gateway keamanan dan host (dalam hal ini, security gateway merujuk pada perangkat intermediate yang menerapkan IPSec, seperti router dan firewall).

2.2.4 Fortigate (61E)

Referensi [13],[14] Fortigate sebagai perangkat yang menjamin keamanan jaringan secara keseluruhan sekaligus berfungsi sebagai gateway dan router bagi jaringan LAN sehingga tidak dibutuhkan lagi router ataupun perangkat tambahan load balancing bila ada lebih dari satu koneksi WAN.

Satu perbedaan yang utama, memungkinkan sistem Fortigate mendeteksi dan mengeliminir secara real time ancaman yang terintegrasi, bahkan dalam skala kompleks, tanpa menurunkan kinerja jaringan, sementara serangkaian proses manajemen, analisa, database dan solusi perlindungan endpoint bekerja meningkatkan penyebaran fleksibilitas dan memberikan dampak yang nyata dalam mengurangi biaya operasional manajemen keamanan jaringan.

2.2.5 QoS (Quality of Services)

Referensi [1] Quality of service (QoS) mengacu pada teknologi apa pun yang mengelola lalu lintas data untuk mengurangi packet loss (kehilangan paket), latency, delay, dan jitter pada jaringan. QoS mengontrol dan mengelola sumber daya jaringan dengan menetapkan prioritas untuk tipe data tertentu

pada jaringan. Untuk melihat kualitas layanan Throughput dan Delay dapat menggunakan standarisasi yang dikeluarkan oleh TIPHON seperti pada Tabel 1 dan Tabel 2.

Tabel 1 Kategori Throughtput menurut TIPHON

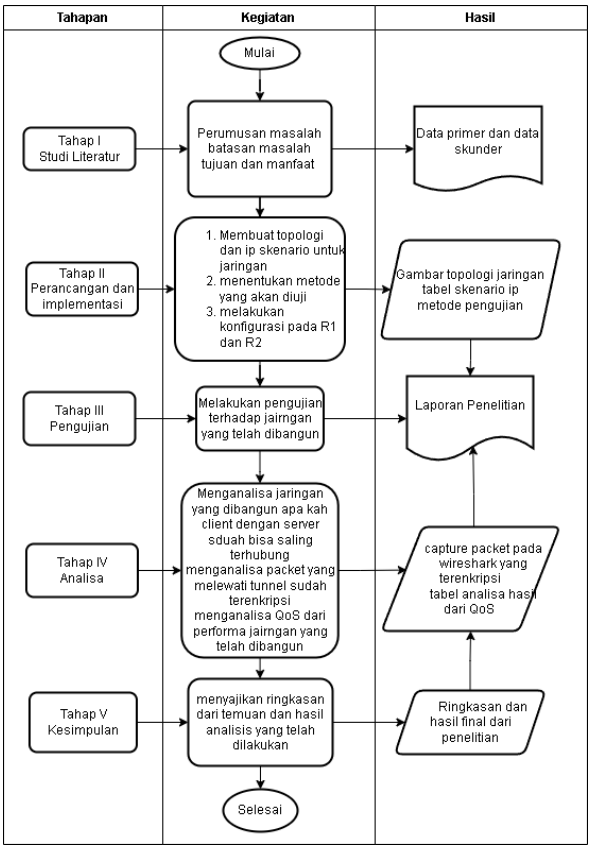
Kategori Troughput	Troughput (bps)	Indeks
Sangat Bagus	100	4
Bagus	75	3
Sedang	50	2
Jelek	<25	1

Tabel 2 Kategori Delay menurut TIPHON

Kategori Degredasi	Delay (ms)	Indeks
Sangat Bagus	<150 ms	4
Bagus	150 ms s/d 300 ms	3
Sedang	300 ms s/d 450 ms	2
Jelek	> 450 ms	1

3. METODE PENELITIAN

Pada metode penelitian dapat dilihat pada gambar 1. Proses metodologi penelitian ini adalah merupakan langkah demi langkah dalam penyusunan penelitian mulai dari perancangan judul, identifikasi masalah, perancangan dan implementasi, pengujian dan Analisa serta kesimpulan.



Gambar 1 Tahapan Penelitian

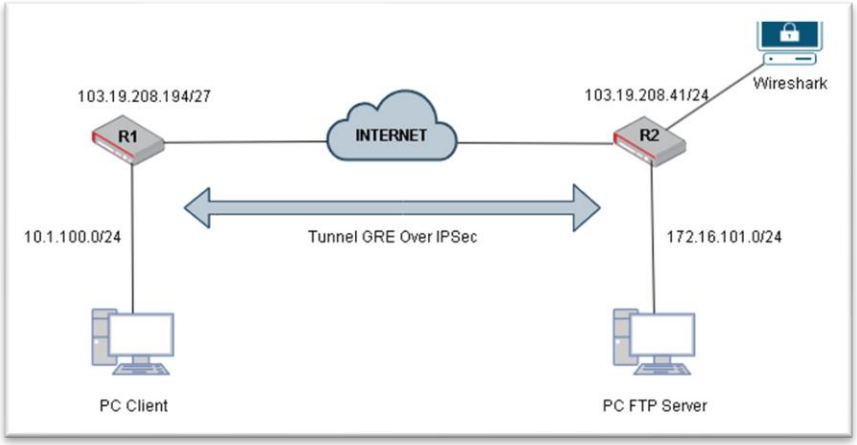
3.1 Tahap Studi Literatur

Pada tahap ini dilakukan studi literatur dengan membaca sumber-sumber pustaka yang berasal dari jurnal, web page dan sebagainya untuk identifikasi masalah, tujuan dan manfaat penelitian. Berdasarkan hasil studi litaratur dirumuskan beberapa permasalahan yaitu:

i) Apakah protokol GRE dengan IPSec bisa mengamankan packet yang melalui jaringan tunnel VPN tersebut.
ii) Skema topologi harus sesuai dengan skema dari GRE Over IPSec.
iii) Packet yang melalui tunnel harus terenkripsi dengan aman.

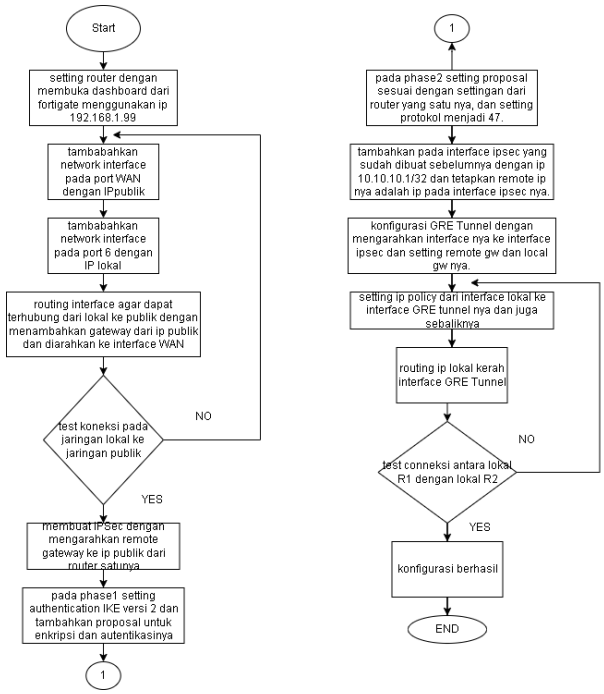
3.2 Tahap Perancangan dan Implementasi

Rancangan topologi pada Gambar 2 menjelaskan terdapat 2 router Fortigate 61E terhubung ke jaringan publik (internet), PC Client dan PC-FTP Server terhubung ke perangkat Fortigate sebagai jaringan LAN. Kemudian di R1 dan R2 yang membentuk suatu Tunnel VPN GRE Over IPSec dan memiliki network tunnel yaitu 10.10.10.0/24. PC-2 menyediakan layanan berupa FTP server menggunakan sistem operasi windows dengan Internet Information Services sebagai service FTP nya. Sedangkan PC-1 sebagai Client yang mengakses layanan FTP ke PC-2. Kemudian pada R2 akan dilakukan *capture* packet yang melintas melalui *tunnel* dengan menggunakan fitur yang tersedia dari fortigate.



Gambar 2 Topologi GRE Over IPSec Tunnel VPN

Pada Gambar 3 menjelaskan tahapan konfigurasi untuk membangun jaringan VPN Tunnel GRE Over IPSec. Tahapan ini berdasarkan topologi pada Gambar 2.



Gambar 3 Flowchart konfigurasi

3.3 Tahap Pengujian

Pada Tahap ini dilakukan pengujian terhadap jaringan VPN yang telah dibangun. Pengujian proses enkripsi IPSec menggunakan protokol enkripsi IKEv2 dilakukan dengan menggunakan aplikasi Wireshark, untuk menangkap paket yang sudah dienkripsi dengan protokol ESP sehingga memastikan paket yang dikirim dari asal ke tujuan melawati GRE Over IPSec tersebut terenkripsi. Pengujian layanan FTP pada jaringan GRE over IPSec dengan melakukan pengambilan data dari server dan client. Untuk pengujian PC-2 merupakan server dengan sistem operasi windows yang menyediakan berupa data seperti layanan pengiriman file (FTP) yang sering dipakai untuk pengambilan data tersebut. Pengujian ini akan dilihat dari seberapa banyak pemakaian bandwidth yang mengakses layanan tersebut dari beberapa client untuk menentukan delay dan throughput pada jaringan GRE Over IPSec tersebut. Hasil pengujian dilakukan dengan menggunakan tools Wireshark, dimana tools ini dipergunakan sebagai network analyzer paket data yang berjalan melewati suatu jaringan. Pengujian dilakukan dengan dua skenario, pengujian upload data dan pengujian download data.

3.4 Tahap Analisa

Adapun Analisa yang dilakukan yaitu analisa packet melalui tunnel GRE Over IPSec VPN. Analisa akan dilakukan dengan membaca data yang tertangkap pada aplikasi wireshark. Kemudian Analisa yang kedua akan dilakukan dengan mengukur performa dari jaringan dengan parameter delay dan throughput

3.5 Tahap Kesimpulan

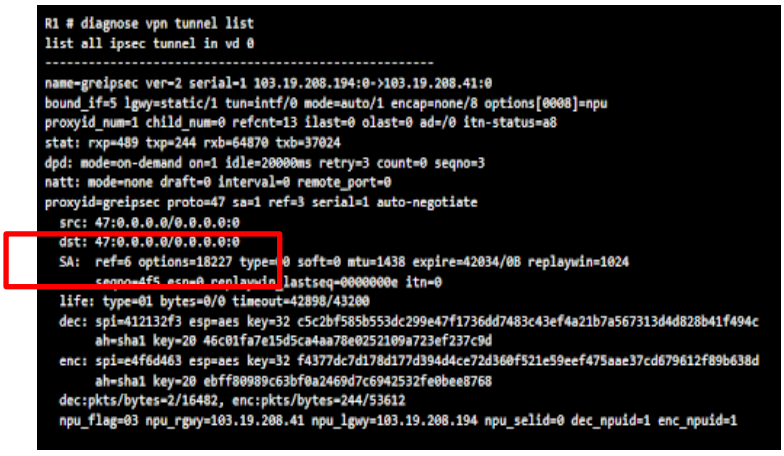
Pada tahap Kesimpulan menyajikan ringkasan dari temuan dan hasil analisis yang telah dilakukan pada penelitian. Pada tahap ini menyajikan ringkasan tujuan, temuan utama serta saran untuk penelitian berikutnya.

4. HASIL

4.1 Tahap Pengujian

4.1.1 VPN Tunnel List

Gambar 4 menampilkan verifikasi VPN Tunnel sudah berjalan, dengan menjalankan perintah untuk verifikasi GRE Over IPSec pada perangkat Fortigate. Dapat dilihat nama dari VPN adalah “greipsec”. Nama tersebut dibuat sebagai nama interface IPSec. Kemudian dilihat dari asal dan tujuannya sudah berjalan melalui protocol 47. Protokol 47 adalah protocol untuk GRE. Sehingga dapat disimpulkan bahwa VPN sudah melalui protocol GRE Over IPSec.

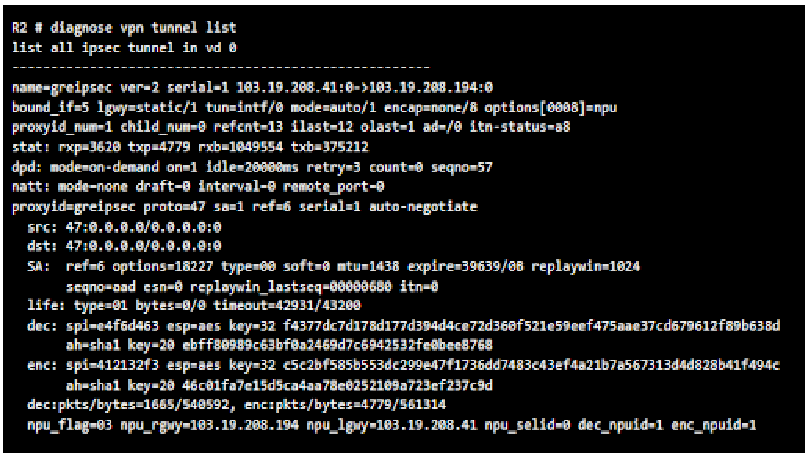


Gambar 4 Diagnosa List VPN Tunnel

4.1.2 VPN IKE Gateway List

Gambar 5 menampilkan untuk memverifikasi protocol IKEv2 yang sudah berjalan. Pada R1 protocol IKEv2 yang berjalan dengan direction initiator, yang berarti perangkat yang terhubung ke gateway tersebut akan bertindak sebagai inisiatif dalam membangun koneksi VPN. Setelah itu mengirimkan

permintaan koneksi ke perangkat peer untuk membentuk koneksi yang aman. Hal ini juga dilakukan pada R2 untuk memverifikasi protocol IKEv2 yang sudah berjalan dengan direction Responder. Responder adalah perangkat yang menerima permintaan koneksi VPN dari perangkat initiator yang bertindak sebagai pengirim. Permintaan koneksi ini diterima melalui protokol Internet Key Exchange (IKE) yang digunakan untuk membangun koneksi VPN dan membentuk koneksi yang aman antara kedua perangkat.



Gambar 5 Diagnosa VPN IKEv2 gateway list pada R1

4.1.3 Capture Packet ICMP dengan WireShark

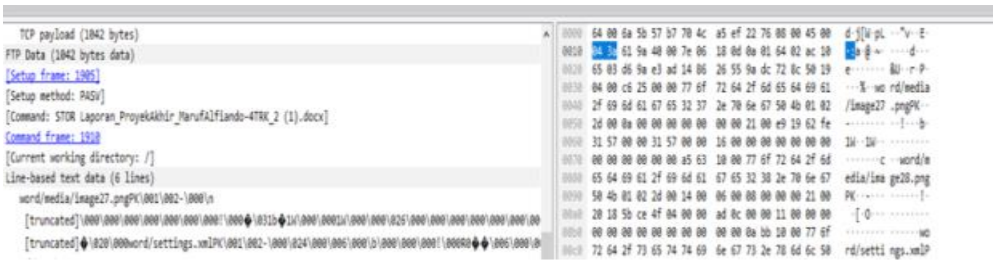
Gambar 6 adalah capture paket ICMP di Wireshark. Semua capture paket yang ada di Wireshark sudah dienkripsi menjadi paket dengan protokol ESP (Encapsulating Security Payload), dimana protokol ESP berfungsi untuk menjaga kepastian data, autentifikasi sumber data, dan proteksi gangguan terhadap data. Protokol ESP dibuat dengan mengenkripsi pada paket IP dan membuat paket IP lain yang mengandung header IP asli dan header ESP.

Gambar 6 Capture Packet ICMP yang dienkripsi di *Wireshark*

4.2 Hasil Pengujian dan Analisa

4.2.1 Pengujian Enkripsi IPSec (IKEv2)

Gambar 7 menampilkan data yang berhasil dikirim menggunakan FTP sudah terenkripsi dengan baik. Dapat dilihat line-based text data sudah tidak dapat terbaca lagi. Ini menandakan bahwa packet yang dikirim sudah dienkripsi dengan protokol IKEv2. Ketika protokol IKEv2 dienkripsi, informasi di dalam header dan payload akan diubah sehingga tidak dapat dibaca dengan mudah tanpa dekripsi.

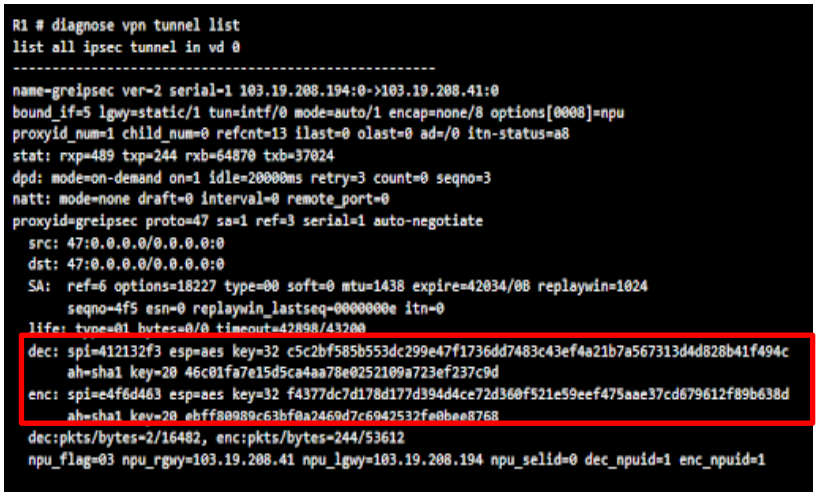


Gambar 7 Capture packet FTP yang terenkripsi

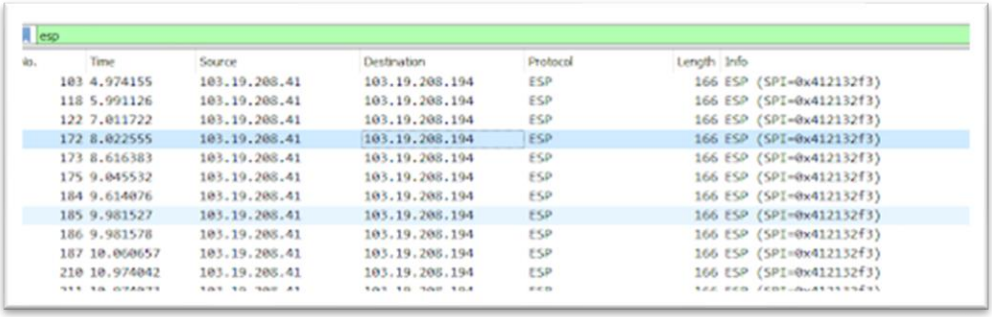
4.2.2 Analisa protokol IPSec dengan ESP

Gambar 8 menampilkan kunci decrypt dari SPI local gateway dan kunci encrypt dari SPI remote gateway. Kemudian kunci tersebut bisa diupload pada wireshark untuk dapat menganalisa protokol data yang ditransmisikan dalam paket tersebut. Gambar 9 adalah hasil capture ESP yang merupakan salah

satu komponen utama dari IPSec. Dari gambar ini tercatat nilai SPI yang sama dengan SPI decrypt pada Gambar 8. Pada Gambar 8 terdapat kunci decrypt dan kunci autentikasi. Kunci yang diupload harus sesuai dengan nilai SPI yang ada pada Gambar 8. Begitujuga hasil capture ESP dari PC1 ke PC2 yang merupakan salah satu komponen utama dari IPSec. Dari gambar ini tercatat nilai SPI yang sama dengan SPI encrypt pada Gambar 8. Pada Gambar 8 terdapat kunci enkripsi dan kunci autentikasi. Kedua kunci ini harus sesuai saat memasangkannya.

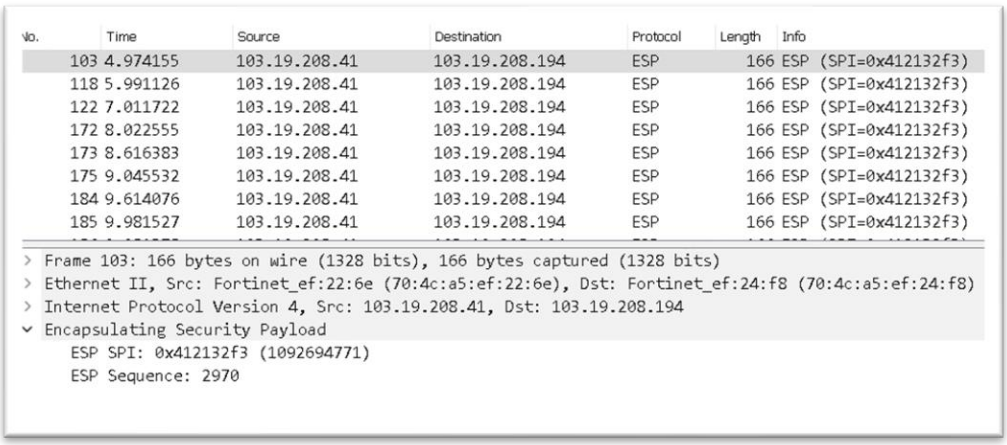


Gambar 8 Diagnosa dari VPN Tunnel list

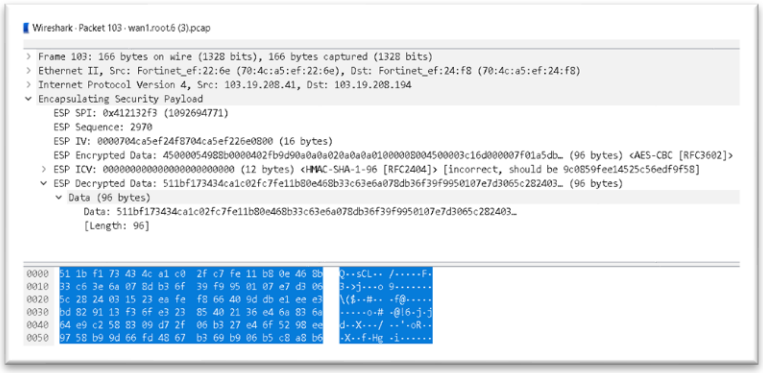


Gambar 9 Capture packet ESP dari PC2 ke PC1

Pada Gambar 10 terlihat packet sebelum dilakukan decrypt. Gambar 10 terlihat hasil decrypt dari packet yang terenkripsi. Pada gambar ini data yang sudah didekripsi masih berbentuk nilai hexa. Walaupun telah ditambahkan kunci dekripsi, filepun masih tidak terbaca. Hal ini berarti bahwa paket masih terenkapsulasi dengan protokol GRE.



Gambar 10 Sebelum paket didecrypt



Gambar 11 Hasil setelah didecrypt

4.2.3 Pengujian Performa QoS pada Jaringan IPSec

Tabel 3 merupakan hasil pengujian performa QoS untuk Delay (ms) dan Throughput (mbps) pada saat proses upload. Sedangkan Tabel 4 merupakan saat proses download.

Tabel 3 Hasil Pengujian Upload

No	TEKS		GAMBAR		SUARA		VIDEO	
	D	T	D	T	D	T	D	T
1	0.174	46	0.775	10	0.183	43	0.404	19
2	0.159	49	8.739	0.916	1.035	7.7	0.602	13
3	0.158	50	2.665	3	0.819	10	0.975	8
4	1.833	4.4	2.074	4	0.663	12	0.716	11
5	2.55	3.1	2.099	4	0.676	11	0.874	9
Rata-rata	**0.974**	**30.5**	**3.27**	**4.38**	**0.675**	**16.74**	**0.714**	**12**

Tabel 4 Hasil Pengujian Downlaod

No	TEKS		GAMBAR		SUARA		VIDEO	
	D	T	D	T	D	T	D	T
1	0.442	18	0.16	50	0.204	39	0.465	17
2	0.137	58	0.169	47	0.286	27	0.521	15
3	0.146	54	0.166	48	0.197	40	0.479	16
4	0.155	51	0.158	50	0.204	39	0.343	23
5	0.187	42	0.152	52	0.215	37	0.511	15
Rata-rata	**0.213**	**44.6**	**0.161**	**49.4**	**0.221**	**36.4**	**0.481**	**17.2**

Keterangan:
D : Delay
T : Throughput

4.2.4 Analisa Performa QoS pada Jaringan IPSec

Dari hasil pengujian yang telah dilakukan terhadap performa jaringan GRE over IPSec pada Fortigate dengan menggunakan berbagai jenis data seperti teks, gambar, suara, dan video. Pada Tabel 4-11 dapat disimpulkan bahwa secara umum jaringan ini menunjukkan performa yang baik dengan rata-rata throughput sebesar 30,5 Mbps untuk pengujian upload teks, 4,38 Mbps untuk pengujian upload gambar, 16,74 Mbps untuk pengujian upload suara, dan 12 Mbps untuk pengujian upload video. Sedangkan untuk pengujian download, rata-rata throughput sebesar 44,6 Mbps untuk pengujian download teks, 49,4 Mbps untuk pengujian download gambar, 36,4 Mbps untuk pengujian download suara, dan 17,2 Mbps untuk pengujian download video. Semua percobaan dalam pengujian menunjukkan bahwa jaringan dalam kondisi stabil dan dapat diandalkan. Namun, pada pengujian upload gambar terdapat satu percobaan yang memiliki delay yang cukup tinggi yaitu sebesar 8,739 ms, hal ini dapat disebabkan oleh kondisi jaringan yang buruk atau masalah lain yang tidak terkait dengan jaringan GRE over IPSec.

Dengan performa yang baik dan stabil, jaringan GRE over IPSec pada Fortigate dapat menjadi pilihan yang tepat untuk diimplementasikan pada lingkungan jaringan perusahaan yang membutuhkan koneksi jaringan yang aman dan andal untuk mengirimkan berbagai jenis data yang berbeda. Namun, harus selalu diingat bahwa hasil pengujian hanya mencerminkan kondisi saat pengujian dilakukan, dan kinerja jaringan dapat berubah seiring waktu serta faktor-faktor tertentu yang dapat mempengaruhinya seperti jumlah pengguna dan kondisi jaringan yang berubah.

5. SIMPULAN DAN SARAN

5.1 Kesimpulan

Adapun kesimpulan yang dapat diambil pada penelitian ini adalah: i) Pengujian terhadap keamanan GRE Over IPSec VPN dengan protokol IKEv2 sudah berjalan dengan baik. Data yang dikirimkan antara server dan client melalui jalur VPN tunnel tersebut telah dienkripsi menggunakan teknologi IPSec. ii) Penggunaan protokol IKEv2 sebagai protokol kunci kriptografi yang digunakan dalam pembangunan jalur VPN tunnel tersebut juga memastikan bahwa koneksi antara server dan client dapat didirikan dengan aman. iii) Untuk melihat paket yang melalui jaringan GRE Over IPSec dilakukan proses decrypt pada wireshark, dengan memberikan kunci enkripsi dan hasilnya paket yang didecrypt masih berbentuk hexa yang berarti paket masih belum bisa terbaca. iv) Berdasarkan standarisasi pengukuran Delay menurut TIPHON, hasil pengujian pada percobaan upload dan download Teks, Gambar, Suara dan Video termasuk dalam kategori “sangat bagus”. Berdasarkan standarisasi pengukuran Throughput menurut TIPHON, hasil pengujian pada percobaan upload dan download Teks, Gambar, Suara dan Video termasuk kategori “sangat bagus”.

5.2 Saran

Berikut beberapa saran setelah melakukan penelitian terhadap GRE Over IPSec Tunnel VPN: i) Melakukan perbandingan pengiriman data yang aman pada jaringan public melalui VPN IPSec over GRE. ii) Karena pengujian throughput dan delay baru menggunakan layanan FTP pada jaringan, tingkat akurasi QoS nya masih kecil maka perlu percobaan baru dengan layanan yang lebih besar untuk meningkatkan akurasi dari penilaian kinerja pada jaringan. iii) Untuk melihat seberapa efisien jaringan GRE Over IPSec pengujian juga dapat dilakukan dengan skenario kondisi jaringan yang berbeda-beda, misalnya seperti menggunakan jaringan dengan sinyal yang buruk atau bervariasi dan menggunakan jaringan yang padat dengan pengguna lain atau di lokasi yang sama dengan jaringan lain.

DAFTAR PUSTAKA

[1] H. Kuswanto, "Implementasi Jaringan Virtual Private Network (VPN) Menggunakan Protokol EoIP," J. Komput. dan Inform. Univ. Bina Sarana Inform., vol. 19 No 1, 2017, [Online]. Available: https://ejournal.bsi.ac.id/ejurnal/index.php/paradigma/article/view/1491.

[2] B. A. Wicaksono and W. Sulistyo, "Rancang Bangun Interkoneksi Jaringan Lokal Berbasis VPN Menggunakan Metode GRE Tunnel dan IPSec.: Studi Kasus CV. Candra Perkasa," Universitas Kristen Satya Wacana, 2019.

[3] G. Ajiardiawan, "Analisis Pengaruh Sistem Keamanan IPSec dan SSL pada Implementasi Virtual Private Network (VPN) di Layanan CCTV IP," Universitas Telkom, 2010.

[4] M. R. Effendi, E. A. Z. Hamidi, and A. Saepulloh, "Implementasi GRE Tunneling Menggunakan Open vSwitch Pada Jaringan Kampus," J. Telekomun. Elektron. Komputasi dan Kontrol, vol. 3 No 2, 2017, https://doi.org/10.15575/telka.v3n2.103-111

[5] D. B. P, "Perbandingan Kinerja IP Sec dan SSL," J. Inform. dan Teknol. Inf., vol. 7 No 1, 2010, [Online]. Available: http://jurnal.upnyk.ac.id/index.php/telematika/article/view/411.

[6] A. A. Sukmandhani, "QoS (Quality of Services)," 2020. https://onlinelearning.binus.ac.id/computer-science/post/qos-quality-of-services.

[7] I. Warman and A. Hanafi, "Analisa Perbandingan Kinerja Generic Routing Encapsulation (GRE) Tunnel dengan Point to Point Protocol Over Ethernet (PPPoE) Tunnel Mikrotik RouterOS," J. Tek. Inform., vol. 7 No 1, 2019, https://doi.org/10.21063/jtif.2019.V7.1.

[8] W. Dinata, "Implementasi IPSec Site-To-Site VPN Menggunakan Cisco ASA," Politeknik Caltex Riau, 2021.

[9] W. Agustina and M. Rifqi, "Implementasi Dual Link IPVPN dan GSM Berbasis IPSec pada Fortigate 50 E," J. Rekayasa Sist. dan Teknol. Inf., vol. 4 No 2, 2020, https://doi.org/10.29207/resti.v4i2.1465.

[10] I. K. Rahman, D. I. Mulyana, and Y. Akbar, "Optimasi IPSec Site to Site VPN Mikrotik menggunakan Algoritme Enkripsi Blowfish," J. Ilm. Komput., vol. 19 No 1, 2023, [Online]. Available: http://ojs.stmik-banjarbaru.ac.id/index.php/progresif/article/view/1092.

[11] H. Suryantoro, A. Sopian, and D. Dartono, "Penerapan Teknologi Fortigate dalam Pembangunan Jaringan VPN-IP Berbasis IPSec," J. Elektro dan Inform. Swadharma, vol. 1 No 1, 2021, [Online]. Available: https://ejurnal.swadharma.ac.id/index.php/jeis/article/view/64. https://doi.org/10.56486/jeis.vol1no1.64.

[12] Wibowo, A., Zul, M. I. ., Fadly Ridha, M. A. ., & Zain, M. M. . (2020). Sistem Terintegrasi untuk Mendeteksi Perubahan Lingkungan dengan Algoritma Frame Difference dan Dynamic - Adaptive Template Matching menggunakan Raspberry Pi dan Virtual Private Network (VPN). Jurnal Komputer Terapan, 6(2), 129-147. https://doi.org/10.35143/jkt.v6i2.3598

[13] S. S. Kardono, "Arsitektur E-Kios di Surabaya," J. Komunikasi, Media dan Inform., vol. 5 No 1, 2016. https://doi.org/10.31504/komunika.v5i1.637.

[14] Riduan, A., & Sadikin, N. (2021). Perancangan Firewall Menggunakan Fortigate Di PT Swadharma Duta Data. Jurnal Maklumatika, 8(1), 90-98. Retrieved from https://maklumatika.i-tech.ac.id/index.php/maklumatika/article/view/122.