Jurnal Penelitian Teknologi Komputer
Vol. 9 No. 4, April 2025
ISSN : 21102135

IMPLEMENTASI GRE OVER IPSEC VPN DENGAN DYNAMIC ROUTING RIP PADA TOPOLOGI MESH DI GNS3

Azhara Amelia H[1], Sabrina Akva[2], Yohana Lorinez[3], Dedy Kiswanto[4]
Universitas Negeri Medan
E-mail: azharaamelia549@gmail.com[1],
sabrinaakva55110@gmail.com[2], lorinezyohana@gmail.com[3],
dedykiswanto@unimed.ac.id[4]

Abstrak

Penelitian ini mengeksplorasi implementasi Generic Routing Encapsulation (GRE) yang dipadukan dengan protokol keamanan Internet Protocol Security (IPSec), serta penggunaan protokol routing dinamis Routing Information Protocol versi 2 (RIP v2) pada topologi mesh virtual yang disimulasikan menggunakan perangkat lunak GNS3. Tujuan utama dari studi ini adalah untuk menganalisis efektivitas kombinasi teknologi tersebut dalam mendukung keamanan data dan efisiensi distribusi rute dalam lingkungan jaringan kompleks. Proses implementasi mencakup konfigurasi IP statis, pembangunan GRE tunnel, pengaktifan IPSec untuk enkripsi lalu lintas antar-router, serta aktivasi RIP v2 untuk mendistribusikan rute secara otomatis. Hasil simulasi menunjukkan bahwa jaringan dapat beroperasi dengan stabil, menunjukkan latensi rendah dan tanpa kehilangan paket, serta memiliki jalur routing yang optimal dan terenkripsi dengan baik. Dengan demikian, pendekatan ini dapat menjadi solusi potensial untuk membangun Virtual Private Network (VPN) yang aman dan scalable pada jaringan berskala menengah hingga besar.

Kata Kunci — GRE, IPSec, RIP v2, VPN, GNS3, Topologi Mesh, Routing Dinamis, Keamanan Jaringan.

1. PENDAHULUAN

Di era digital saat ini, jaringan komputer telah menjadi bagian yang tidak terpisahkan dari berbagai aktivitas organisasi, baik dalam lingkup pemerintahan, swasta, pendidikan, maupun sektor industri. Kebutuhan akan sistem komunikasi dan pertukaran data yang cepat, stabil, dan aman telah mendorong pengembangan berbagai teknologi jaringan, salah satunya adalah Virtual Private Network (VPN) (Musril, 2019).

VPN merupakan teknologi yang memungkinkan pengguna untuk mengakses jaringan internal secara aman dari jarak jauh. Salah satu metode VPN yang banyak digunakan adalah IPsec (Internet Protocol Security), yang bekerja dengan melakukan enkripsi dan autentikasi data antar perangkat jaringan sehingga keamanan informasi yang dikirimkan melalui jaringan publik dapat terjamin (Sumarna & Maulana, 2021).

VPN berbasis IPsec (Internet Protocol Security) merupakan salah satu metode yang paling umum digunakan untuk membangun koneksi aman melalui jaringan public (Laksamana et al., 2022). IPsec menyediakan mekanisme enkripsi dan autentikasi yang menjamin kerahasiaan, integritas, dan keaslian data saat melintasi jaringan yang tidak terpercaya. Teknologi ini sangat efektif untuk kebutuhan komunikasi antar cabang perusahaan yang tersebar di berbagai wilayah. Namun, keterbatasan IPsec dalam mendukung protokol routing dinamis menjadi hambatan dalam pengembangan jaringan yang fleksibel. Oleh karena itu, dibutuhkan metode tambahan seperti Generic Routing Encapsulation (GRE) yang dapat mengenkapsulasi berbagai protokol layer 3 dan memungkinkan penggunaan routing dinamis di atas IPsec. Dengan demikian, kombinasi GRE over IPsec menjadi solusi yang ideal untuk jaringan dengan kebutuhan routing dinamis (Firdausi & Wardani, 2020).

Untuk mengatasi keterbatasan tersebut, diterapkan metode tunneling tambahan yaitu Generic Routing Encapsulation (GRE). GRE merupakan protokol tunneling yang memungkinkan pembungkusan berbagai protokol layer 3 di dalam paket IP sehingga dapat

dikirim melalui jaringan yang tidak mendukung protokol-protokol tersebut secara langsung. Dengan kata lain, GRE membuka peluang untuk menggunakan dynamic routing di atas IPsec. Penggabungan GRE dan IPsec (GRE over IPsec) menciptakan solusi yang ideal karena menghadirkan fleksibilitas dalam pengaturan routing sekaligus tetap mempertahankan aspek keamanan dari IPsec (Arifin et al., 2021).

Salah satu protokol routing dinamis yang banyak digunakan dalam jaringan berskala kecil hingga menengah adalah Routing Information Protocol (RIP). RIP merupakan protokol routing berbasis algoritma distance vector yang menentukan jalur terbaik berdasarkan jumlah perangkat jaringan yang harus dilewati untuk mencapai tujuan (Gultom et al., 2021). Meskipun saat ini telah hadir protokol yang lebih kompleks seperti OSPF dan EIGRP, RIP tetap relevan digunakan karena kemudahan implementasinya dan cocok untuk topologi jaringan yang tidak terlalu kompleks, termasuk topologi mesh yang memiliki banyak jalur redundan antar node (Jati et al., 2018).

Topologi mesh sendiri merupakan salah satu topologi jaringan yang menawarkan keunggulan dalam hal keandalan dan toleransi terhadap kegagalan jalur. Dalam topologi ini, setiap node dapat terhubung langsung dengan node lainnya, sehingga jika terjadi kerusakan pada salah satu jalur, data dapat dialihkan ke jalur alternatif yang tersedia (Alvionita & Nurwasito, 2019). Hal ini sangat sesuai dengan prinsip kerja dynamic routing yang akan terus memperbarui tabel routing berdasarkan kondisi terkini jaringan. Kombinasi topologi mesh, GRE over IPsec, dan dynamic routing RIP menjadi konfigurasi yang menjanjikan untuk membangun jaringan yang aman, dinamis (Arianti et al., 2024).

Selain itu, karakteristik dari topologi mesh yang mendukung banyak koneksi langsung antar node menjadikannya sangat mendukung mekanisme dynamic routing. Dalam skenario jaringan dinamis yang menggunakan protokol seperti RIP, setiap perubahan kondisi jaringan seperti penambahan atau pemutusan koneksi akan langsung diperbarui dalam tabel routing. Hal ini membuat mesh sangat responsif terhadap kondisi jaringan terkini. Lebih lanjut, topologi ini juga meningkatkan performa dalam hal distribusi trafik karena beban dapat didistribusikan melalui berbagai jalur yang tersedia, sehingga mengurangi potensi bottleneck pada jalur komunikasi tertentu (Sholikhin et al., 2020).

Untuk mendukung perancangan dan pengujian sistem jaringan tersebut, diperlukan media simulasi yang memungkinkan konfigurasi jaringan secara virtual namun realistis. Salah satu platform yang sering digunakan adalah GNS3 (Graphical Network Simulator 3), yang dapat mensimulasikan berbagai perangkat jaringan nyata seperti router, switch, dan firewall. GNS3 memberikan fleksibilitas tinggi dalam pengujian skenario jaringan termasuk VPN, GRE, dan routing dinamis, tanpa memerlukan perangkat fisik secara langsung (Nurdiansyah et al., 2020).

Penelitian ini bertujuan untuk mengimplementasikan dan menganalisis konfigurasi GRE over IPsec VPN dengan dynamic routing RIP pada topologi mesh yang disimulasikan menggunakan GNS3. Dengan melakukan pengujian ini, diharapkan dapat diketahui bagaimana performa protokol RIP dalam mendistribusikan rute secara dinamis pada jaringan mesh, serta sejauh mana kombinasi GRE dan IPsec dapat mendukung stabilitas dan keamanan komunikasi jaringan antar site. Selain itu, penelitian ini juga ingin membuktikan bahwa GNS3 sebagai media simulasi dapat memberikan hasil yang representatif untuk keperluan perencanaan jaringan di dunia nyata.

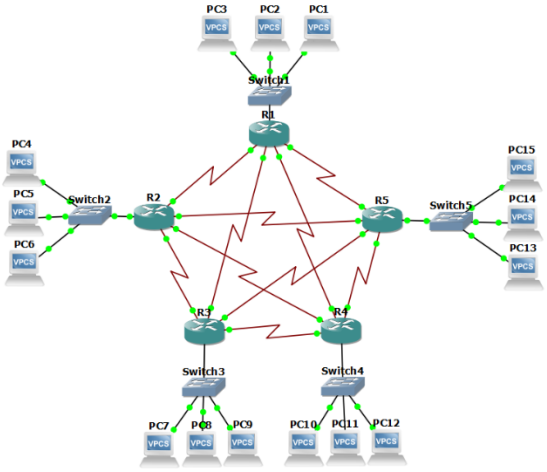
2. METODE PENELITIAN

Penelitian ini dilakukan untuk menganalisis dan menguji penerapan jaringan yang menggunakan perangkat berupa 5 router, 5 switch, dan 15 PC, dengan fokus pada implementasi tunnel GRE, enkripsi IPSec, serta protokol routing dinamis RIP v2 untuk memastikan kestabilan dan keamanan komunikasi jaringan.

Vol. 9 No. 4, April 2025
ISSN : 21102135

Desain Jaringan

Jaringan yang digunakan dalam penelitian ini dirancang dengan topologi mesh, di mana setiap router terhubung langsung dengan router lainnya. Dalam topologi ini digunakan 5 router yang saling terhubung, 5 switch yang menghubungkan router dengan perangkat PC, serta 15 PC. Setiap router dan perangkat dikonfigurasi dengan alamat IP statis pada interface yang menghubungkan mereka satu sama lain, menggunakan skema IP yang telah direncanakan.



Gambar 1. Topologi Mash

Pengaturan Dasar Jaringan

Langkah awal melibatkan konfigurasi dasar jaringan dengan penetapan alamat IP pada setiap interface router. Proses ini diikuti dengan pengujian konektivitas antar-router menggunakan perintah ping untuk memastikan bahwa semua router dapat saling terhubung tanpa adanya kehilangan paket dan waktu respons yang stabil.

```
R1#enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface Serial1/0
R1(config-if)#ip address 10.0.1.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#interface Serial1/1
R1(config-if)#ip address 10.0.2.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#interface Serial1/2
R1(config-if)#ip address 10.0.3.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#interface Serial1/3
R1(config-if)#ip address 10.0.4.1 255.255.255.252
R1(config-if)#no shutdown
R1(config-if)#interface FastEthernet0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#exit
R1#
*Mar  1 00:09:13.399: %SYS-5-CONFIG_I: Configured from console by console
R1#write memory
Building configuration...
[OK]
```

Gambar 2. Konfigurasi IP di Router

```
R1#ping 10.0.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/79/84 ms
R1#ping 10.0.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/80/84 ms
R1#ping 10.0.3.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/83/100 ms
R1#ping 10.0.4.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.4.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/80/84 ms
```

Gambar 3. Tes Konektivitas Router Melalui Ping

Konfigurasi Protokol Routing Dinamis RIP v2

Agar jaringan dapat mengelola rute secara otomatis, protokol routing dinamis RIP v2 diaktifkan pada setiap router. Proses ini melibatkan pengaturan RIP dan verifikasi informasi rute yang disebarkan antar-router. Tabel routing yang terdapat pada masing-masing router kemudian diperiksa dengan perintah show ip route untuk memastikan bahwa informasi rute yang diterima valid dan terbaru.

```
R1#enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 10.0.0.0
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.2.0
R1(config-router)#network 192.168.3.0
R1(config-router)#network 192.168.4.0
R1(config-router)#network 192.168.5.0
R1(config-router)#no auto-summary
R1(config-router)#exit
R1(config)#exit
R1#
*Mar  1 00:37:29.215: %SYS-5-CONFIG_I: Configured from console by console
R1#write memory
Building configuration...
[OK]
```

Gambar 4. Konfigurasi RIP di Router

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

R    192.168.4.0/24 [120/1] via 10.0.3.2, 00:00:25, Serial1/2
R    192.168.5.0/24 [120/1] via 10.0.4.2, 00:00:15, Serial1/3
     10.0.0.0/30 is subnetted, 9 subnets
R       10.0.10.0 [120/1] via 10.0.4.2, 00:00:15, Serial1/3
                  [120/1] via 10.0.3.2, 00:00:25, Serial1/2
R       10.0.8.0 [120/1] via 10.0.3.2, 00:00:25, Serial1/2
                 [120/1] via 10.0.2.2, 00:00:05, Serial1/1
C       10.0.2.0 is directly connected, Serial1/1
C       10.0.3.0 is directly connected, Serial1/2
C       10.0.1.0 is directly connected, Serial1/0
R       10.0.6.0 [120/1] via 10.0.3.2, 00:00:28, Serial1/2
                 [120/1] via 10.0.1.2, 00:00:10, Serial1/0
R       10.0.7.0 [120/1] via 10.0.4.2, 00:00:17, Serial1/3
                 [120/1] via 10.0.1.2, 00:00:10, Serial1/0
C       10.0.4.0 is directly connected, Serial1/3
R       10.0.5.0 [120/1] via 10.0.2.2, 00:00:07, Serial1/1
                 [120/1] via 10.0.1.2, 00:00:07, Serial1/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
R    192.168.2.0/24 [120/1] via 10.0.1.2, 00:00:09, Serial1/0
     192.168.100.0/30 is subnetted, 1 subnets
C       192.168.100.0 is directly connected, Tunnel0
R    192.168.3.0/24 [120/1] via 10.0.2.2, 00:00:11, Serial1/1
```

Gambar 5. Verifikasi RIP

Pembangunan Tunnel GRE

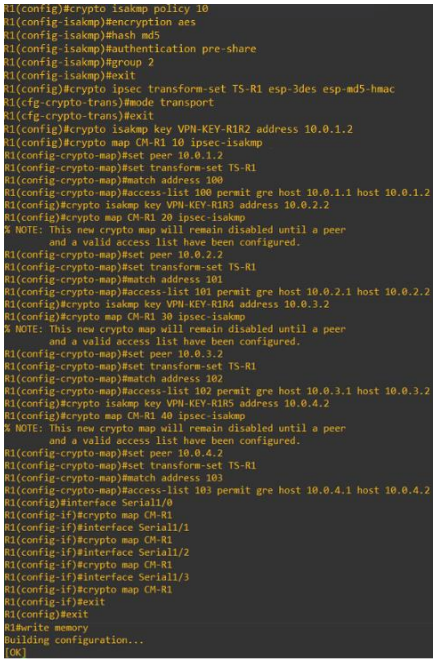
Untuk membangun komunikasi antar-router secara virtual, tunnel GRE dikonfigurasi antara pasangan router yang terlibat. Setiap tunnel diberikan alamat IP virtual yang dapat digunakan untuk komunikasi antar-router melalui jaringan publik. Pengujian dilakukan menggunakan perintah ping dan traceroute untuk memastikan kelancaran konektivitas antar-router melalui tunnel.

```
R1#enable
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface Tunnel0
R1(config-if)#description GRE to R2
R1(config-if)#ip address 192.168.100.1 255.255.255.252
R1(config-if)#tunnel source Serial1/0
R1(config-if)#tunnel destination 10.0.1.2
R1(config-if)#tunnel mode gre ip
R1(config-if)#no shutdown
R1(config-if)#interface Tunnel1
R1(config-if)#description GRE to R3
R1(config-if)#ip address 192.168.101.1 255.255.255.252
R1(config-if)#tunnel source Serial1/1
R1(config-if)#tunnel destination 10.0.2.2
R1(config-if)#tunnel mode gre ip
R1(config-if)#no shutdown
R1(config-if)#interface Tunnel2
R1(config-if)#description GRE to R4
R1(config-if)#ip address 192.168.102.1 255.255.255.252
R1(config-if)#tunnel source Serial1/2
R1(config-if)#tunnel destination 10.0.3.2
R1(config-if)#tunnel mode gre ip
R1(config-if)#no shutdown
R1(config-if)#interface Tunnel3
R1(config-if)#description GRE to R5
R1(config-if)#ip address 192.168.103.1 255.255.255.252
R1(config-if)#tunnel source Serial1/3
R1(config-if)#tunnel destination 10.0.4.2
R1(config-if)#tunnel mode gre ip
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#exit
```

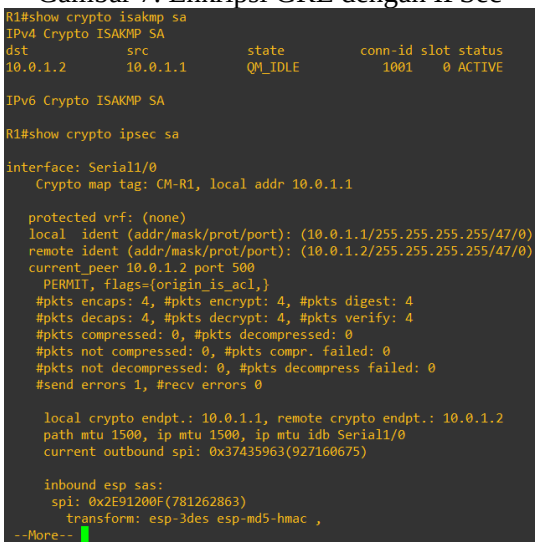
Gambar 6. Implementasi GRE Tunnel

Penerapan IPSec untuk Keamanan

Mengingat pentingnya keamanan data dalam jaringan, IPSec diterapkan pada tunnel GRE untuk mengenkripsi data yang melewati jalur komunikasi virtual. Pengujian keamanan dilakukan dengan menggunakan alat analisis jaringan seperti Wireshark untuk memverifikasi bahwa data yang melewati tunnel terenkripsi dengan benar dan tidak dapat dibaca tanpa kunci dekripsi yang tepat.



Gambar 7. Enkripsi GRE dengan IPSec



Gambar 8. Verifikasi IPSec

Pengujian Kinerja Jaringan

Setelah seluruh konfigurasi selesai, dilakukan serangkaian pengujian untuk memastikan kinerja jaringan secara keseluruhan. Pengujian latensi dilakukan dengan menggunakan perintah ping untuk mengukur waktu yang dibutuhkan paket data untuk mencapai tujuan.

Analisis Hasil

Semua hasil pengujian, baik konektivitas, keamanan, maupun kinerja jaringan, dianalisis untuk mengevaluasi sejauh mana konfigurasi yang diterapkan berhasil memenuhi tujuan penelitian. Hasil pengujian akan dibandingkan dengan standar yang diharapkan untuk memastikan bahwa sistem jaringan yang dibangun berfungsi dengan baik dan aman.

3. HASIL DAN PEMBAHASAN

Hasil Konfigurasi Jaringan

Jaringan yang digunakan terdiri dari 5 router, 5 switch, 15 perangkat PC. Konfigurasi jaringan dilakukan dengan menetapkan alamat IP statis pada setiap interface router sesuai dengan skema IP yang telah direncanakan, dengan pengaturan koneksi antar-router menggunakan koneksi point-to-point. Setelah konfigurasi jaringan selesai, pengujian konektivitas antar-router dilakukan menggunakan perintah ping, yang menunjukkan hasil bahwa semua router berhasil terhubung satu sama lain. Setiap router dapat saling ping ke router lainnya dengan hasil yang menunjukkan 0% packet loss dan waktu respons yang stabil.

Tabel 1: Hasil Pengujian Konektivitas Antar Router

Sumber Router	Tujuan Router	Hasil Ping	Waktu Rata-Rata	Status Koneksi
R1	R2	Sukses	80 ms	Terhubung
R1	R3	Sukses	79 ms	Terhubung
R1	R4	Sukses	97 ms	Terhubung
R1	R5	Sukses	89 ms	Terhubung
R2	R3	Sukses	120 ms	Terhubung
R2	R4	Sukses	78 ms	Terhubung
R2	R5	Sukses	80 ms	Terhubung
R3	R4	Sukses	94 ms	Terhubung
R3	R5	Sukses	120 ms	Terhubung
R4	R5	Sukses	80 ms	Terhubung

Hasil Implementasi Tunnel GRE

Konfigurasi tunnel GRE dibangun antara masing-masing router untuk menciptakan koneksi virtual yang memungkinkan paket data mengalir seolah-olah ada jalur fisik langsung, meskipun router-router tersebut terhubung melalui jaringan publik. Tunnel GRE berhasil dibangun di antara pasangan router yang terlibat, dengan setiap tunnel memiliki alamat IP virtual yang digunakan untuk komunikasi antar-router melalui jaringan publik. Pengujian konektivitas antar-router melalui tunnel GRE dilakukan dengan perintah ping, menghasilkan komunikasi yang berjalan lancar tanpa kehilangan paket.

Tabel 2: Status Tunnel GRE

Router	Tunnel	Status	Alamat IP Tunnel	MTU	Bandwidth
R1 - R2	Tunnel0	Up	192.168.100.1 - 192.168.100.2	1514 bytes	9 Kbit/sec
R1 - R3	Tunnel1	Up	192.168.101.1 - 192.168.101.2	1514 bytes	9 Kbit/sec
R1 - R4	Tunnel2	Up	192.168.102.1 - 192.168.102.2	1514 bytes	9 Kbit/sec
R1 - R5	Tunnel3	Up	192.168.103.1 - 192.168.103.2	1514 bytes	9 Kbit/sec
R2 - R3	Tunnel0	Up	192.168.104.1 - 192.168.104.2	1514 bytes	9 Kbit/sec
R2 - R4	Tunnel1	Up	192.168.105.1 - 192.168.105.2	1514 bytes	9 Kbit/sec
R2 - R5	Tunnel2	Up	192.168.106.1 - 192.168.106.2	1514 bytes	9 Kbit/sec
R3 - R4	Tunnel0	Up	192.168.107.1 - 192.168.107.2	1514 bytes	9 Kbit/sec
R3 - R5	Tunnel1	Up	192.168.108.1 - 192.168.108.2	1514 bytes	9 Kbit/sec
R4 - R5	Tunnel0	Up	192.168.109.1 -	1514 bytes	9 Kbit/sec

			192.168.109.2		

Hasil Implementasi IPSec untuk Keamanan Tunnel

Keamanan komunikasi melalui tunnel GRE menjadi aspek krusial, terutama dalam jaringan yang mengalirkan data sensitif. Oleh karena itu, IPSec diterapkan untuk mengenkripsi data yang melintasi tunnel GRE, dengan tujuan memastikan integritas dan kerahasiaan data. Setiap tunnel GRE dilengkapi dengan konfigurasi IPSec yang mengaktifkan enkripsi serta autentikasi guna melindungi data dari potensi penyadapan oleh pihak ketiga.

Tabel 3: Status IPSec Tunnel

Pasangan Router	Tunnel	Algoritma Enkripsi	Status Enkripsi
R1 - R2	Tunnel0	IKE: AES + MD5 IPSec: 3DES + MD5-HMAC	Aktif
R1 - R3	Tunnel1	IKE: AES + MD5 IPSec: 3DES + MD5-HMAC	Aktif
R1 - R4	Tunnel2	IKE: AES + MD5 IPSec: 3DES + MD5-HMAC	Aktif
R1 - R5	Tunnel3	IKE: AES + MD5 IPSec: 3DES + MD5-HMAC	Aktif
R2 - R3	Tunnel0	IKE: AES + MD5 IPSec: 3DES + MD5-HMAC	Aktif
R2 - R4	Tunnel1	IKE: AES + MD5 IPSec: 3DES + MD5-HMAC	Aktif
R2 - R5	Tunnel2	IKE: AES + MD5 IPSec: 3DES + MD5-HMAC	Aktif
R3 - R4	Tunnel0	IKE: AES + MD5 IPSec: 3DES + MD5-HMAC	Aktif
R3 - R5	Tunnel1	IKE: AES + MD5 IPSec: 3DES + MD5-HMAC	Aktif
R4 - R5	Tunnel0	IKE: AES + MD5 IPSec: 3DES + MD5-HMAC	Aktif

Hasil Implementasi Routing Dinamis dengan RIP

Protokol routing dinamis RIP v2 dikonfigurasi untuk memastikan jaringan dapat mengatur dan memperbarui rute secara otomatis, memungkinkan router-router dalam jaringan mendistribusikan informasi rute dan secara efektif menemukan jalur optimal untuk pengiriman data. Setelah mengaktifkan RIP pada setiap router, dilakukan verifikasi untuk memastikan bahwa informasi routing telah disebarkan dengan benar ke seluruh jaringan, dan semua router memperoleh rute yang diperlukan untuk mencapai tujuan melalui proses pertukaran informasi routing. Tabel routing yang diperoleh dapat diverifikasi menggunakan perintah show ip route, yang memastikan bahwa setiap router memiliki informasi rute yang terbaru dan valid, memungkinkan pemilihan jalur terbaik dalam pengiriman paket data.

Tabel 4: Tabel Routing pada Router 1

Jaringan Tujuan	Masker Subnet	Next Hop	Metode Routing
10.0.1.0	255.255.255.252	192.168.100.2	RIP
10.0.2.0	255.255.255.252	192.168.101.2	RIP
10.0.3.0	255.255.255.252	192.168.102.2	RIP
10.0.4.0	255.255.255.252	192.168.103.2	RIP
10.0.5.0	255.255.255.252	192.168.104.2	RIP
10.0.6.0	255.255.255.252	192.168.105.2	RIP
10.0.7.0	255.255.255.252	192.168.106.2	RIP
10.0.8.0	255.255.255.252	192.168.107.2	RIP
10.0.9.0	255.255.255.252	192.168.108.2	RIP

10.0.10.0	255.255.255.252	192.168.109.2	RIP

Hasil Pengujian Konektivitas dan Kinerja Jaringan

Pengujian lebih lanjut dilakukan untuk memastikan bahwa jaringan berfungsi dengan baik setelah konfigurasi selesai, dengan fokus pada konektivitas dan kinerja jaringan. Pengujian ini bertujuan untuk menilai apakah tunnel GRE dan IPSec beroperasi dengan efektif, menjaga stabilitas komunikasi antar-router dan perangkat lainnya. Tes latensi dilakukan menggunakan perintah ping untuk mengukur waktu yang dibutuhkan paket data untuk mencapai tujuan, dengan hasil rata-rata latensi antar-router sekitar 83 ms. Hasil ini menunjukkan bahwa komunikasi antar-router berlangsung cepat dan efisien meskipun adanya overhead akibat enkripsi IPSec yang sedikit meningkatkan waktu respons.

Tabel 5: Hasil Tes Ping (Latensi)

Sumber Router	Tujuan Router	Waktu (ms)	Paket Dikirim	Paket Diterima	Packet Loss
R1	R2	95 ms	5	5	0%
R1	R3	70 ms	5	5	0%
R1	R4	86 ms	5	5	0%
R1	R5	88 ms	5	5	0%
R2	R3	87 ms	5	5	0%
R2	R4	79 ms	5	5	0%
R2	R5	66 ms	5	5	0%
R3	R4	93 ms	5	5	0%
R3	R5	80 ms	5	5	0%
R4	R5	92 ms	5	5	0%

4. KESIMPULAN

Penelitian ini mengimplementasikan dan menguji jaringan dengan topologi mesh yang menggabungkan tunnel GRE, enkripsi IPSec, dan protokol routing dinamis RIP v2 pada lima router, lima switch, dan lima belas PC dalam lingkungan GNS3. Hasil penelitian menunjukkan bahwa konfigurasi jaringan berjalan dengan baik dan stabil, dengan semua router dapat terhubung satu sama lain tanpa kehilangan paket dan waktu respons yang stabil. Pengujian tunnel GRE membuktikan kemampuannya dalam membangun koneksi virtual antar-router, sementara penerapan IPSec memberikan lapisan enkripsi yang melindungi data yang mengalir melalui tunnel, memastikan kerahasiaan dan integritas data. Protokol RIP v2 berfungsi dengan baik dalam mendistribusikan informasi rute secara dinamis, memungkinkan setiap router memperbarui rutenya secara otomatis dan memilih jalur terbaik untuk pengiriman data. Pengujian kinerja jaringan menunjukkan bahwa meskipun ada sedikit penurunan latensi akibat enkripsi IPSec, komunikasi antar-router tetap berjalan efisien dan stabil, dengan latensi rata-rata sekitar 83 ms antara router-router yang terhubung. Secara keseluruhan, implementasi GRE over IPSec VPN dengan Dynamic Routing RIP pada topologi mesh di GNS3 terbukti efektif dalam memastikan kestabilan dan keamanan komunikasi jaringan, menjadikannya solusi yang layak untuk penerapan jaringan yang membutuhkan.

DAFTAR PUSTAKA

Alvionita, S., & Nurwasito, H. (2019). Analisis Kinerja Protokol Routing OSPF, RIP dan EIGRP Pada Topologi Jaringan Mesh (Vol. 3, Issue 8). http://j-ptiik.ub.ac.id

Arianti, B. D. D., Jamaluddin, J., & Kuswanto, H. (2024). Analisis penerapan RT-RW Net menggunakan Topologi Mesh-Wireless untuk meningkatkan pemahaman Administrasi Sistem Jaringan Siswa. Infotek: Jurnal Informatika Dan Teknologi, 7(1), 236–245. https://doi.org/10.29408/jit.v7i1.24809

Arifin, R. M., Dwi Wardhani, E., & Beta, S. (2021). Implementasi Tunnel GRE pada Jaringan Ring dan Mesh Perangkat Metro-E Nokia (Implementation of GRE Tunnel on Ring and Mesh Network Nokia Metro-E Devices). In Jurnal Nasional Teknik Elektro dan Teknologi Informasi | (Vol. 10, Issue 3).

Firdausi, A., & Wardani, H. W. (2020). Simulasi dan Analisa QoS dalam Jaringan VPN Site To Site Berbasis IPSec dengan Routing Dynamic. Jurnal Telekomunikasi Dan Komputer, 10(2), 49. https://doi.org/10.22441/incomtech.v10i2.8131

Gultom, S. A., Indriani, D. D., & Kiswanto, D. (2021). Konfigurasi dan Analisis Perbandingan Algoritma Dynamic Routing Link State dan Distance Vector Menggunakan Topologi Mesh dengan Simulator Cisco Packet Tracer. Journal of Informatics and Data Science (J-IDS, 1(1).

Jati, W. S., Nurwasito, H., & Data, M. (2018). Perbandingan Kinerja Protocol Routing Open Shortest Path First (OSPF) dan Routing Information Protocol (RIP) Menggunakan Simulator Cisco Packet Tracer (Vol. 2, Issue 8). http://j-ptiik.ub.ac.id

Laksamana, R., Naf'an, E., Praja, E., Mandala, W., Raya, J., Begalung, L., Xx, N., Lubuk Begalung, K., Padang, K., Barat, S., & Korespondensi, P. (2022). Protokol L2TP dan IPsec Sebagai Keamanan Jaringan Pada Dinas Kominfotik Sumatera Barat. 10(3), 162–171. https://doi.org/10.12928/jstie.v8i3.xxx

Musril, H. A. (2019). Desain Virtual Private Network (VPN) Berbasis Open Shortest Path First (OSPF). InfoTekJar (Jurnal Nasional Informatika Dan Teknologi Jaringan), 3(2), 83–88. https://doi.org/10.30743/infotekjar.v3i2.1055

Nurdiansyah, Y., Pratama, N., Putra, M. I., & Sya'roni, M. A. (2020). Analisis Perbandingan Metode Interior Gateway Protocol RIP Dengan OSPF Pada Jaringan MPLS-VPLS. In Informatics Journal (Vol. 5, Issue 2).

Sholikhin, A. R., Warisaji, T. T., & Cahyanto, T. A. (2020). Penerapan Wireless Distribution System (WDS) Mesh Untuk Optimasi Cakupan Area Wi-Fi di UM Jember. BIOS : Jurnal Teknologi Informasi Dan Rekayasa Komputer, 1(2), 61–69.

Sumarna, S., & Maulana, A. (2021). Implementasi Virtual Private Network Menggunakan L2TP/IPsec pada BBPK Jakarta. EXPERT: Jurnal Manajemen Sistem Informasi Dan Teknologi, 11(2), 90. https://doi.org/10.36448/expert.v11i2.1829