JUTIK : Jurnal Teknologi Informasi dan Komputer
Oktober-2025, Vol. 11, No.2, Hal 150-163
ISSN(P): 2442-241X; ISSN(E): 2528-5211

IMPLEMENTASI VPN DIATAS *ROUTING* OSPF DALAM MEMBANGUN SIMULASI JARINGAN MAN

Nezza Anggraini Yolandari[1*], Delvita Aulia Artika[2], Bunga Dwi Febrianti[3], Dedy Kiswanto[4]
Universitas Negeri Medan, Medan, Sumatera Utara, Indonesia[1]
Email*:nezzaanggraini0@gmail.com
Universitas Negeri Medan, Medan, Sumatera Utara, Indonesia[2]
Email: delvitaartika@gmail.com
Universitas Negeri Medan, Medan, Sumatera Utara, Indonesia[3]
Email: bungadwifebrianti@gmail.com
Universitas Negeri Medan, Medan, Sumatera Utara, Indonesia[4]
Email: dedykiswanto@unimed.ac.id

ABSTRAK

Penelitian ini bertujuan untuk membandingkan efektivitas protokol *Virtual Private Network* (VPN) *Ipsec* dan *GRE tunnel* dalam membangun koneksi *VPN site-to-site* pada jaringan *Metropolitan Area Network* (MAN) yang dioptimalkan dengan *routing Open Shortest Path First* (OSPF). Dengan menggunakan perangkat lunak *Cisco packet tracer*, simulasi dilakukan dengan melibatkan tujuh *router* sebagai representasi dari lokasi yang berbeda, dihubungkan melalui koneksi VPN. Hasil simulasi menunjukkan bahwa meskipun *Ipsec* menawarkan keamanan yang signifikan melalui enkripsi data, keterbatasan dalam pengiriman *multicast* menimbulkan tantangan dalam komunikasi OSPF. Sebaliknya, *GRE tunnel* mendukung pengiriman *rute multicast* yang diperlukan untuk OSPF, menjadikannya pilihan yang lebih efisien dalam konteks ini. Penelitian ini memberikan wawasan tentang kelebihan dan kekurangan masing-masing protokol untuk pengimplementasian jaringan yang aman dan efisien.
Kata kunci: VPN *site-to-site, Routing* OSPF, Jaringan MAN, *Ipsec* VPN, GRE *Tunnel,* Cisco Packet Traser

ABSTRACT

This study aims to compare the effectiveness of the Virtual Private Network (VPN) Ipsec and GRE tunnel protocols in establishing site-to-site VPN connections on a Metropolitan Area Network (MAN) optimized with Open Shortest Path First (OSPF) routing. Using Cisco packet tracer software, simulations were conducted involving seven routers as representations of different locations, connected via VPN connections. The simulation results show that although Ipsec offers significant security through data encryption, its limitations in multicast delivery pose challenges in OSPF communications. In contrast, GRE tunnel supports multicast route delivery required for OSPF, making it a more efficient choice in this context. This study provides insight into the advantages and disadvantages of each protocol for implementing a secure and efficient network.
Keywords: Site-to-Site VPN, OSPF Routing, MAN Network, Ipsec VPN, GRE tunnel, Cisco packet tracer

Submitted: 14 April 2025
Accepted: 15 September 2025
Published: 10 Oktober 2025

1. PENDAHULUAN

Perkembangan teknologi jaringan komputer saat ini menuntut sistem komunikasi yang aman, handal, dan efisien, terutama dalam skala jaringan berskala luas seperti *Metropolitan Area Network* (MAN). Jaringan *Metropolitan Area Network* (MAN) merupakan jaringan yang mencakup area geografis yang lebih luas dibandingkan dengan Local Area *Network* (LAN) tetapi lebih kecil dari *Wide Area Network* (WAN) [1].

Salah satu solusi untuk membangun jaringan yang aman antar lokasi berbeda adalah dengan menerapkan *Virtual Private Network* (VPN). *Virtual Private Network* (VPN) merupakan solusi yang digunakan untuk menghubungkan jaringan di berbagai lokasi secara aman melalui internet. VPN ini bekerja dengan meng*enkripsi* data yang dikirimkan antar cabang, sehingga memastikan integritas dan kerahasiaan informasi [4], [6].

Dalam mendukung efisiensi komunikasi jaringan, protokol *routing* dinamis seperti *Open Shortest Path First* (OSPF) turut berperan dalam mengoptimalkan jalur komunikasi antar perangkat jaringan, sehingga lalu lintas data dapat diarahkan melalui rute tercepat dan terbaik. OSPF adalah protokol *routing* yang hanya dapat berjalan di jaringan internal yang masih memiliki hal pengelolaan jaringan. OSPF juga merupakan protokol perutean standar terbuka, artinya tidak ada vendor yang membuatnya. OSPF menggunakan *routing* link-state yang berfokus pada efisiensi prosesor, kebutuhan memori, dan konsumsi *bandwidth*.[5].

Protokol *routing* OSPF digunakan untuk memastikan komunikasi antar jaringan berjalan secara optimal. Simulasi yang dilakukan menunjukkan bahwa kombinasi VPN dan OSPF dapat mengoptimalkan konektivitas antar cabang dengan latensi minimal serta meningkatkan efisiensi dalam pengelolaan lalu lintas data. Penggunaan metode ini juga memungkinkan pengujian performa dan keandalan koneksi dalam skenario jaringan yang lebih luas [3], [9], [12].

Implementasi VPN dalam jaringan MAN disimulasikan menggunakan perangkat lunak *Cisco packet tracer*. Dua jenis protokol VPN, yaitu *Ipsec* dan *GRE tunnel*, digunakan dalam simulasi untuk mengamankan komunikasi antar site. Kedua protokol tersebut dianalisis dari segi fungsi, kelebihan, dan efektivitasnya dalam membangun jaringan yang aman. Selain itu, protokol OSPF dirancang untuk mengoptimalkan proses *routing* yang mendukung komunikasi data antar site secara dinamis dan efisien.

Penelitian ini bertujuan untuk mengimplementasi VPN dan membandingkan efektivitas dari protokol *Ipsec* dan *GRE tunnel* dalam membangun koneksi VPN pada jaringan MAN berbasis OSPF.

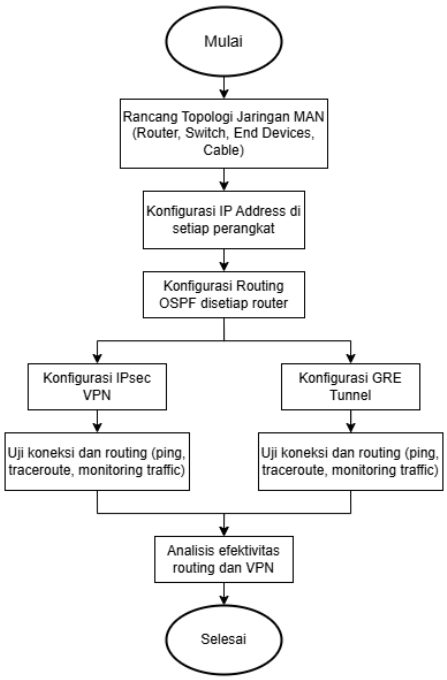
2 METODE

Metode Pengumpulan Data

Penelitian ini menggunakan metode eksperimen kuantitatif untuk menganalisis perbandingan efektivitas protokol VPN *Ipsec* dan *GRE tunnel* dalam membangun koneksi *VPN site-to-site* pada jaringan *Metropolitan Area Network* (MAN) dengan *routing Open Shortest Path First* (OSPF).

Penelitian dimulai dengan merancang topologi jaringan menggunakan perangkat lunak *Cisco packet tracer*. Simulasi melibatkan tujuh buah router yang mewakili lokasi berbeda (site), yang dihubungkan dan membentuk koneksi *VPN site-to-site*. Pada masing-masing site juga terdapat beberapa perangkat jaringan tambahan seperti switch dan *end-device* (PC). Dalam proses ini, peneliti mengimplementasikan dua protokol VPN yaitu *Ipsec* dan *GRE tunnel*.

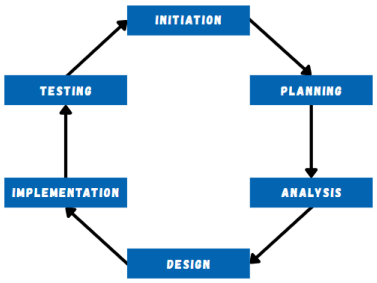
Data dikumpulkan secara deskriptif kuantitatif berdasarkan hasil simulasi dari setiap skenario. Hasil simulasi kemudian dibandingkan untuk mengetahui kelebihan dan kekurangan masing-masing protokol dalam mendukung komunikasi jaringan antar site.



Gambar 1. Alur Membangun Sistem VPN

Metode Pengembangan Jaringan

Metode pengembangan jaringan pada penelitian ini menggunakan model *Network Development Life Cycle* (NDLC), yang terdiri dari beberapa tahapan berikut:



Gambar 2. Metode Pengembangan Jaringan

a. *Initiation*
Mengidentifikasi kebutuhan keamanan komunikasi antar site pada jaringan MAN. Tahap ini melibatkan analisis awal dengan meninjau studi pustaka terkait VPN, *Ipsec*, *GRE tunnel*, dan OSPF.

b. *Planning*
Menyusun rencana topologi jaringan, jenis protokol yang akan digunakan (*Ipsec*, *GRE*, dan OSPF), serta perangkat lunak pendukung yaitu *Cisco packet tracer*.

c. *Analysis*
Melakukan analisis terhadap kebutuhan konfigurasi perangkat, skema *routing*, dan pemilihan protokol VPN yang sesuai dengan kebutuhan jaringan serta parameter pengujian efektivitas.

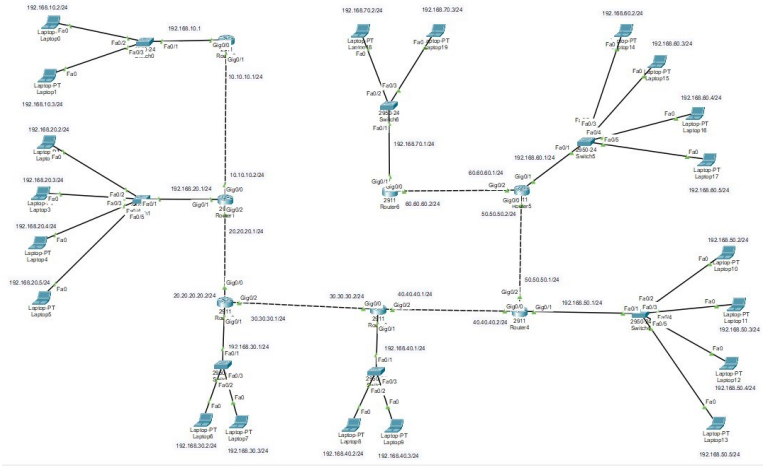
d. *Design*
Merancang topologi jaringan pada *Cisco packet tracer* dan desain konfigurasi VPN dengan *Ipsec* dan *GRE* serta *routing* OSPF pada masing-masing router.

e. *Implementation*
Melakukan konfigurasi jaringan secara langsung pada simulasi, termasuk pengaturan IP address, *routing* OSPF, dan protokol VPN yaitu *Ipsec* dan *GRE tunnel*.

f. *Testing*
Menguji hasil konfigurasi dengan melakukan ping antar perangkat, trace route, dan pemantauan tabel *routing* OSPF. Analisis hasil dilakukan dengan membandingkan performa kedua jenis protokol VPN dari segi dukungan protokol VPN (*Ipsec* dan *GRE tunnel*) terhadap *routing* OSPF dan kemudahannya dalam proses troubleshooting.

3. HASIL DAN PEMBAHASAN

Topologi Jaringan MAN



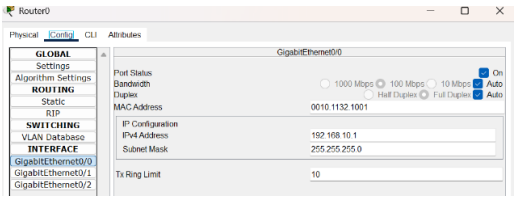
Gambar 3. Simulasi Jaringan MAN

Topologi jaringan MAN (*Metropolitan Area Network*) yang ditampilkan terdiri dari 7 router yang saling terhubung. Setiap router mewakili lokasi yang berbeda dan memiliki koneksi ke beberapa PC. Komunikasi antar-router dilakukan melalui koneksi *Ethernet*.

Saling berkomunikasi melalui koneksi antar router menggunakan *Ipsec* VPN dan *GRE tunnel*.

Konfigurasi IP Address

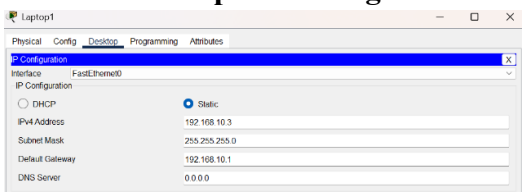
Internet *Protoco*l atau IP merupakan sebuah protokol yang dirancang yang berfungsi sebagai komunikasi data pada sebuah jaringan internet. IP ini terdiri dari sekumpulan beberapa jenis protokol jaringan yang dimana masing-masing protokol memiliki tanggung jawab atas bagian dari komunikasi data[13].Untuk mengkonfigurasi ip *address* pada ketujuh *router* dapat dilakukan melalui *config* di setiap *router*. Lalu masukkan ip address dan *subnet* mask pada setiap *port Gigabitethernet* yang terhubung pada *router*. Dan aktifkan *port* menjadi *on* agar *router* dalam jaringan bisa terhubung.



Gambar 4. Contoh konfigurasi IP Address pada router

Selain itu PC juga harus di konfigurasi agar dapat berkomunikasi di dalam jaringan. Konfigurasi IP dapat dilakukan dengan memberikan ip address, *subnet*mask dan juga ip gatewaynya yang dilakukan dengan Langkah:

PC > Desktop> IP configuration



Gambar 5. Contoh konfigurasi IP Address pada PC

Setelah melakukan konfigurasi ip address pada setiap Router dan Pc di setiap jaringan LAN maka harus di uji semua perangkat sudah dapat berkomunikasi dalam jaringan dengan melakukan ping antar PC atau ping antar Router atau ping antar PC dan Router. Berikut adalah rancangan IP Address :

- Router 0

- PC 1 :192.168.10.2/24
- PC 2 :192.168.10.3/24
- Gig0/0 :192.168.10.1
- Gig0/1 :10.10.10.1/24

- Router 1

- PC 1:192.168.20.2/24
- PC 2: 192.168.20.3/24
- PC 3: 192.168.20.4/24
- PC 4: 192.168.20.5/24
- Gig0/0: 10.10.10.2/24
- Gig0/1: 192.168.20.124
- Gig0/2: 20.20.20.1/24

- Router 2

- PC 1: 192.168.30.2/24

- PC 2: 192.168.30.3/24
- Gig0/0: 20.20.20.2/24
- Gig0/1: 192.168.30.1/24
- Gig0/2: 30.30.30.1/24

- Router 3

- PC 1: 192.168.40.2/24
- PC 2: 192.168.40.3/24
- Gig0/0: 30.30.30.2/24
- Gig0/1: 192.168.40.1/24
- Gig0/2: 40.40.40.1/24

- Router 4

- PC 1: 192.168.50.2/24
- PC 2: 192.168.50.3/24
- PC 3: 192.168.50.4/24
- PC 4: 192.168.50.5/24
- Gig0/0: 40.40.40.2/24
- Gig0/1: 192.168.50.1/24
- Gig0/2: 50.50.50.1/24

- Router 5

- PC 1: 192.168.60.2/24
- PC 2: 192.168.60.3/24
- PC 3: 192.168.60.4/24
- PC 4: 192.168.60.5/24
- Gig0/0: 50.50.50.2/24
- Gig0/1: 192.168.60.1/24
- Gig0/2: 60.60.60.1/24

- Router 6

- PC 1: 192.168.70.2/24
- PC 2: 192.168.70.3/24
- Gig0/0: 60.60.60.2/24
- Gig0/1: 192.168.70.1/24

***Routing* OSPF (*Open Shortest Path First*)**

Open Shortest Path First (OSPF) adalah protokol *routing* dinamis yang digunakan untuk menentukan jalur optimal dalam jaringan. OSPF memungkinkan pembaruan rute secara otomatis berdasarkan kondisi jaringan, sehingga lebih efisien dibandingkan metode *routing* statis [2], [11].

Dengan OSPF, setiap perangkat dalam jaringan dapat bertukar informasi rute secara otomatis, sehingga meningkatkan keandalan dan efisiensi lalu lintas data. Implementasi ini juga mendukung penyesuaian *rute* berdasarkan perubahan kondisi jaringan, sehingga memastikan komunikasi yang optimal antar *node* dalam jaringan MAN [7].

Dalam perangkat cisco, konfigurasi OSPF dapat dilakukan melalui *Command* Line *Interface* (CLI) pada setiap router. Berikut adalah langkah konfigurasi *routing* OSPF, Masuk ke mode konfigurasi :

Router> enable

Router# configure terminal

Perintah enable berfungsi untuk masuk ke mode privilege dan perintah configure terminal berfungsi untuk masuk ke mode konfigurasi global. Aktifkan *Routing* OSPF:

Router(config)# router ospf [process-id]

Process-id adalah nomor proses OSPF (1-65535), nilai ini tidak harus sama antar router dan berfungsi untuk membedakan proses OSPF secara internal. Tentukan *network* yang akan di*routing* dengan menjalankan perintah :

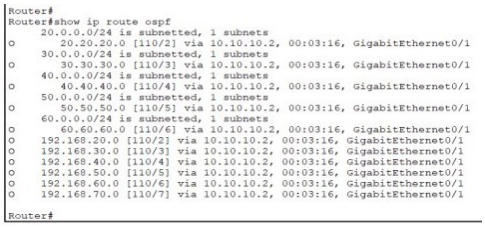
Router(config-router)# *network* [ip-*network*] [*Wildcard-mask*] area [area-id]

IP *network* yang dimasukkan hanya *network* yang terhubung langsung dan ingin di*routing* ospf. *Wildcard-mask* adalah kebalikan dari *subnet* mask yang digunakan untuk

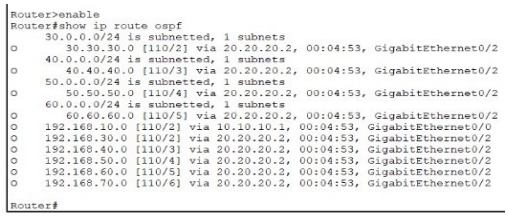
mencocokan IP router. Sedangkan area-id menentukan area OSPF sebagai backbone yang wajib ada. Setelah semua router dikonfigurasi, jalankan perintah :

Router# show ip route ospf

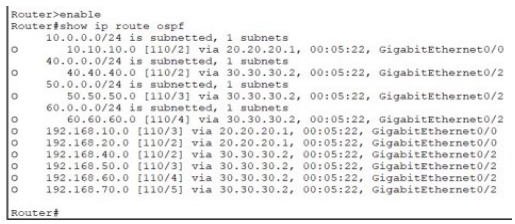
Perintah ini berfungsi untuk menampilkan rute (jalur) jaringan yang didapat dari Protokol *routing* OSPF (O). *Output* akan menampilkan daftar yang memuat *network* tujuan, *administrative distance* ospf, *cost* (biaya), *next hop* IP (alamat router tetangga), durasi sejak rute OSPF tersebut diterima, dan *Interface* keluar yang digunakan untuk menuju jaringan tersebut.



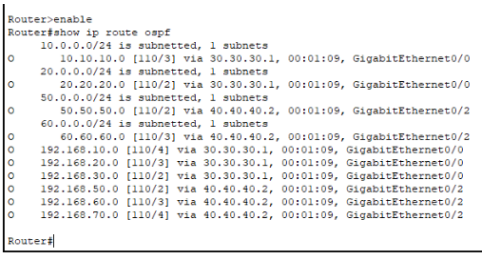
Gambar 6. OSPF Router 0



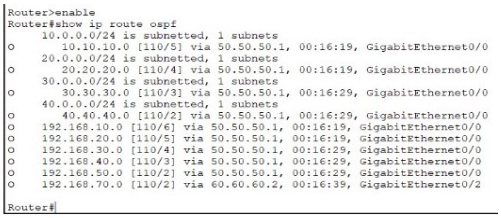
Gambar 7. OSPF Router 1



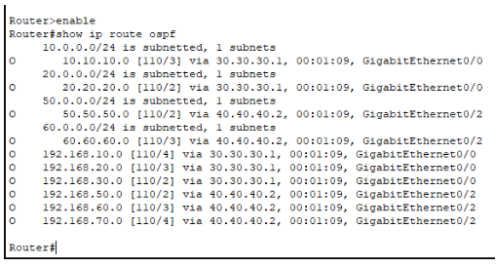
Gambar 8. OSPF Router 2



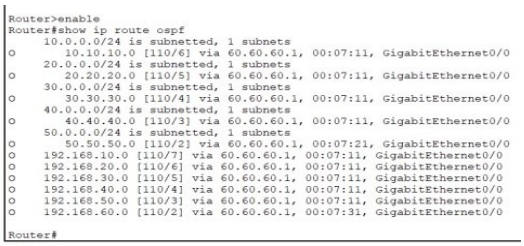
Gambar 9. OSPF Router 3



Gambar 10. OSPF Router 4



Gambar 11. OSPF Router 5



Gambar 12. OSPF Router

Konfigurasi *VPN site-to-site*

Protokol *Ipsec* (*Internet Protocol Security*)

Dalam perangkat cisco, konfigurasi *Ipsec* VPN dapat dilakukan melalui *Command* Line *Interface* (CLI). *Ipsec* VPN di konfigurasi pada 2 router yang tidak terhubung

langsung, yaitu Router 0 dan Router 6. Berikut adalah langkah konfigurasi *Ipsec* VPN antara dua router, Masuk ke mode konfigurasi :

Router> enable
Router# configure terminal

IKE Phase 1 *(Internet Key Exchange)* adalah tahap pertama dalam pembentukan koneksi VPN *Ipsec*. Konfigurasi ISAKMP (*Internet Security Association and Key Management Protokol*) :

Router(config)# *crypto* isakmp policy 10
Router(config-isakmp)# encryption aes 256
authentication pre-share
group 5

Membuat atau memilih kebijakan ISAKMP dengan prioritas nomor 10. Metode *enskripsi* yang digunakan *Advanced Encryption Standard* (AES) dengan panjang kunci 256 bit. Metode *autentikasi* yang digunakan Pre-share key, yaitu kata sandi yang sama dikedua router. Menggunakan *Diffie-Helman* (DH) Group 5 untuk mengatur performa *kriptografi*. Selanjutnya tentukan pre-shared key:

Router(config)# *crypto* isakmp key [sandi] address [IP router tujuan]

Mengatur kunci bersama (pre-shared key) yang digunakan dalam IKE Phase 1 saat membentuk *tunnel Ipsec* VPN antar 2 router. Konfigurasi Transform Set:

Router(config)# *crypto ipsec transform-set* [namaTS] esp-aes 256 esp-sha-hmac

Masuk ke IKE Phase 2, membuat *transform-set* dalam konfigurasi *Ipsec* VPN, yaitu kumpulan metode yang digunakan untuk melindungi data saat sudah berada dalam *tunnel* VPN. Membuat Access Control List:

Router(config)# access-list 100 permit ip [*network* local] [wildcard-*network* local]
[*network* remote] [wildcard-*network* remote]

Access Control List (ACL) bertipe extended (100-199) yang mengizinkan lalu lintas IP antara 2 jaringan yaitu local dan remote dengan mengizinkan semua jenis protokol IP. Konfigurasi *Crypto map* :

***crypto map* [namaCM] 10 *ipsec*-isakmp**
set peer [IP router tujuan]
set pfs group5
set security-association lifetime seconds 86400
set *transform-set* [namaTS]
match address 100

Membuat dan mengedit *crypto map* dengan angka prioritas 10. Menentukan IP yang dijadikan target untuk membangun *tunnel* VPN. Mengaktifkan *Perfect Forward Secrecy* (PFS) untuk meningkatkan keamanan dengan group 5. Menentukan masa berlaku SA (*Security Associatio*n) dalam 24 jam. Menggunakan *enskripsi* sesuai dengan transform set yang telah dibangun. Dan menentukan *traffic* jaringan melalui *tunnel Ipsec* VPN dengan nomor ACL sesuai konfigurasi sebelumnya. Terapkan *Crypto map* ke *Interface* :

Router(config)# *Interface* [router local]
Router(config-if)# *crypto map* [namaCM]

Mode konfigurasi *Interface* jaringan sesuai dengan nama *Interface* yang digunakan. Dan menerapkan *crypto map* yang sebelumnya dikonfigurasi ke *Interface* tersebut. Berarti semua *traffic* yang lewat *Interface* tersebut akan diperiksa dan dicocok dengan ACL, perlu di*enkripsi* atau tidak. Verifikasi konfigurasi VPN :

Router# show *crypto* isakmp sa

Perintah untuk menampilkan status koneksi ISAKMP (IKE Phase 1) antara router local dan router tujuan. *Output* memuat destination (ip router tujuan), port, state (status koneksi jika QM_IDLE berarti phase 1 sukses), Conn-id (ID koneksi), slot, dan status VPN.

Router# show *crypto ipsec* sa

Perintah untuk menampilkan status IKE phase 2 yaitu *Ipsec tunnel* yang aktif dan mengamankan lalu lintas (*traffic*) data yang lewat di dalamnya. *Output* akan menampilkan statistic data yang dikirim dan diterima melalui *tunnel*.

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.10.10.1      60.60.60.2      QM_IDLE           1076    0 ACTIVE

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0x61958A2C(1637190188)
         transform: esp-aes 256 esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 2008, flow_id: FPGA:1, crypto map: IPSEC-MAP
         sa timing: remaining key lifetime (k/sec): (4525504/86256)
         IV size: 16 bytes
         replay detection support: N
         Status: ACTIVE

      outbound ah sas:

      outbound pcp sas:

 Router#

Router#show crypto ipsec sa

interface: GigabitEthernet0/0
    Crypto map tag: IPSEC-MAP, local addr 60.60.60.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.70.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   current_peer 10.10.10.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 60.60.60.2, remote crypto endpt.:10.10.10.1
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
     current outbound spi: 0x61958A2C(1637190188)

     inbound esp sas:
      spi: 0x643CD829(1681709097)
        transform: esp-aes 256 esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2007, flow_id: FPGA:1, crypto map: IPSEC-MAP
        sa timing: remaining key lifetime (k/sec): (4525504/86256)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE
```

Gambar 13. *Ipsec* VPN Router 6

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
60.60.60.2      10.10.10.1      QM_IDLE           1086    0 ACTIVE

 Router#show crypto ipsec sa

 interface: GigabitEthernet0/1
     Crypto map tag: IPSEC-MAP, local addr 10.10.10.1

    protected vrf: (none)
    local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
    remote  ident (addr/mask/prot/port): (192.168.70.0/255.255.255.0/0/0)
    current_peer 60.60.60.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 0
    #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

      local crypto endpt.: 10.10.10.1, remote crypto endpt.:60.60.60.2
      path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
      current outbound spi: 0x643CD829(1681709097)

      inbound esp sas:
       spi: 0x61958A2C(1637190188)
         transform: esp-aes 256 esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 2007, flow_id: FPGA:1, crypto map: IPSEC-MAP
         sa timing: remaining key lifetime (k/sec): (4525504/86305)
         IV size: 16 bytes
         replay detection support: N
         Status: ACTIVE

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0x643CD829(1681709097)
         transform: esp-aes 256 esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 2008, flow_id: FPGA:1, crypto map: IPSEC-MAP
         sa timing: remaining key lifetime (k/sec): (4525504/86305)
         IV size: 16 bytes
         replay detection support: N
         Status: ACTIVE

      outbound ah sas:

      outbound pcp sas:

 Router#
```

Gambar 14. *Ipsec* VPN Router 0

Protokol *GRE* (*Generic Routing Encapsulation*) *Tunnel*

Protokol *GRE tunnel* ini dibangun di atas jaringan publik antar LAN yang tidak saling terhubung. Ini membuat komputer di LAN 0 bisa "berpura-pura" terhubung langsung satu sama lain dengan komputer di LAN 6. Untuk melakukan Protokol ini dapat dilakukan dengan mengkonfigurasi *GRE tunnel* pada kedua router yang ingin dibangun. Masuk mode konfigurasi pada router

Router> enable

Router# configure terminal

Kemudian defenisikan *Interface* virtual yang disebut *Tunnel*0 (ini berarti *tunnel* virtual pertama yang dibuat di router).

***Interface Tunnel*0**

Selanjutnya memberikan ip untuk *Interface tunnel* nya agar dapat berkomunikasi antar *tunnel*. Saat memberikan ip tidak boleh memberikan ip address yang sama dan *subnet* nya juga harus beda dengan *Interface* yang lain karna router yang sama ini akan menyebabkan konflik.

Ip address (ip *tunnel*0) (*subnet*mask *tunnel*0)

Menentukan *Interface* fisik dan ip address yang digunakan router untuk mengirim *traffic GRE tunnel* keluar dengan :

***Tunnel* souce (nama *Interface*)**

Dengan ini maka router akan membangun *GRE tunnel* lewat *Interface* yang disebutkan di *tunnel* source. Dengan kata lain nama *Interface* ini merupakan titik awal dari *GRE tunnel*. Selanjutnya memasukkan ip public router tujaun sebagai *tunnel* destination. Dengan kata lain *tunnel* destination ini adalah ujung atau router tujuan dari *tunnel*.

***Tunnel* destination (ip public router tujuan)**

Router# Show *Interface tunnel*0

Perintah ini digunakan untuk melihat apakah *GRE tunnel* yang dibangun telah aktif dan berjalan ditandai dengan *Tunnel*0 is up, line Protokol is up (connected). Yang selain itu juga memberikan informasi lain berupa ip addres *tunnel*, ip asal *tunnel*, dan ip tujuan *tunnel*

```
Router>
Router>enable
Router#show interface tunnel0
Tunnel0 is up, line protocol is up (connected)
  Hardware is Tunnel
  Internet address is 192.168.100.1/30
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.10.10.1 (GigabitEthernet0/1), destination 60.60.60.2
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
      0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

Gambar 15. *GRE tunnel* Router 0

```
Router#show interface tunnel0
Tunnel0 is up, line protocol is up (connected)
  Hardware is Tunnel
  Internet address is 192.168.80.2/30
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 60.60.60.2 (GigabitEthernet0/0), destination 10.10.10.1
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
      0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

Gambar 16. *GRE tunnel* Router 6

Analisis Protokol VPN

***Ipsec* (*Internet Protocol Security*)**

Protokol *IPSEC* adalah prokol yang memiliki tujuan utama untuk mengamankan komunikasi antar perangkat dalam sebuah jaringan. protokol *Ipsec* untuk melindungi komunikasi internet pada level IP dengan meng*enkripsi* dan memverifikasi paket IP sehingga lebih terjaga keamanannya [8]. Protokol ini bekerja dengan meng*enkripsi* dan meng*autentikasi* setiap paket data agar tisak bisa dilihat, diubah dan disadap olek pihak lain. Namun keterbatasan *IPSEC* adalah hanya bisa mengirimkan *unicast traffic* yaitu komunikasi dari satu perangkat ke satu perangkat lain ini artinya protokol *routing* OSPF yang menggunakan *multicast* tidak bisa langsung berjalan di atas *IPSEC*. Selain itu dalam melakukan troubleshooting lebih rumit karena data yang ter*enkripsi*, sehingga tidak bisa

melihat isi paket nya secara langsung dan juga terdapat dua fase (ISAKMP/IKE dan *Ipsec* SA) sehingga harus memiliki pemahaman dalam melakukan fase negosiasi tentang cara berkomunikasi yang aman.untuk melihat bahwa *IPSEC* tidak mendukung komunikasi *multicast* dapat dengan perintah:

Router# Show *crypto ipsec* sa

Ketika menjalankan perintah ini dapat dilihat bahwa IP local satu dan IP remote satu (point to point) yang artinya, komunikasi ini hanya terjadi antar dua IP saja, bukan antar banyak host seperti pada *multicast*.

proses *enkripsi* data yang membuat isi paket tidak bisa langsung dilihat atau diuji dengan tools sederhana seperti ping atau debug. Selain itu adanya dua fase negosiasi yang sensitif sehingga kedua sisi harus memiliki pengaturan yang benar-benar sama, mulai dari algoritma *enkripsi*, metode *autentikasi*, hingga daftar akses (ACL) dan tidak ada nya pesan error yang jelas ketika satu parameter saja tidaak sesuai membuat nya lebih sulit di atasi ketika terjadi masalah. Namun untuk melakukan *trouble shooting* di *IPSEC* dapat dilakukan dengan perintah:

Router#Show *crypto* isakmp sa

***GRE* (*Generic Routing Encapsulation*)**

Generic Routing Encapsulation (*GRE*) adalah Protokol *tunnel*ling yang dikembangkan oleh cisco untuk mengenkapsulasi berbagai Protokol layer 3 di dalam koneksi point-to point. Dalam implementasi, *GRE tunnel* digunakan untuk membangun komunikasi virtual antar-router di Lokasi berbeda.[10]

Protokol *GRE tunnel* itu fleksibel dan sederhana. Ditambah *GRE tunnel multicast* dan mendukung OSPF karena dapat membawa protokol apa saja. Sehingga ini menjadi alasan utama mengapa *GRE tunnel* sangat cocok untuk jaringan yang butuh *routing* dinamis. Selain itu dalam *GRE tunnel* untuk *trouble shooting* kesalahan juga lebih mudah. Namun *GRE tunnel* juga memiliki kekurangan yaitu dalam protokol *GRE tunnel* suatu paket data akan di bungkus atau di enkapsulasi ke dalam paket baru tetapi *GRE tunnel* hanya membungkusnya dalam IP baru tetapi isi paket nya tetap terlihat (tidak di*enkripsi*) lalu di kirim ke jaringan lalu router penerima akan membuka bungkus *GRE* lalu meneruskannnya ke pemiliki asli paket tersebut. Sehingga data protokol *GRE tunnel* ini tidak aman dalam jaringan karena paket yang dikirimkan berupa *plain text* yang dapat dilihat siapa saja. Untuk mengecek apakah *GRE tunnel* benar mendukung OSPF dapat dilakukan dengan perintah :

Router# Show ip ospf neighbor

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/DR         00:00:30    10.10.10.2      GigabitEthernet0/1
6.6.6.6           0   FULL/  -        00:00:32    10.1.1.2        Tunnel0
```

Gambar 17. Neighbor OSPF *GRE tunnel*

Ketika menjalankan perintah tersebut maka akan menampilkan tetangga ospf dari router tersebut yang berjalan via *tunnel*. Ini berarti *routing* OSPF berjalan di atas protokol *GRE tunnel*.

karena *GRE* tidak memakai *enkripsi* atau *kriptografi*, sehingga memmbuat troubleshooting jadi lebih cepat. Untuk melihat masalah-masalah yang terjadi pada protokol *GRE tunnel* dapat dilakukan dengan perintah:

Router# Show *Interface Tunnel*0

Ketika menjalankan perintah ini dapat dilihat beberapa informasi tentang *GRE tunnel* tersebut salah satu nya adalah apakah *GRE tunnel* sudah aktif atau belum. Semua komponen *GRE tunnel* dipaparkan dengan jelas sehingga ketika ada masalah dapat dengan mudah di ketahui.

4. KESIMPULAN DAN SARAN

Penelitian ini memberikan wawasan mendalam mengenai implementasi VPN dengan protokol OSPF dalam jaringan *Metropolitan Area Network* (MAN). Hasil simulasi menunjukkan bahwa kombinasi antara VPN menggunakan protokol *Ipsec* dan *GRE tunnel*, serta penerapan OSPF sebagai protokol *routing* dinamis, dapat secara signifikan meningkatkan keamanan dan efisiensi komunikasi antar lokasi. Meskipun *Ipsec* menyediakan *enkripsi* yang kuat untuk melindungi data, namun memiliki keterbatasan dalam mendukung *traffic multicast*, yang merupakan syarat penting untuk operasi OSPF. Sebaliknya, *GRE tunnel* lebih efektif dalam mendukung OSPF untuk komunikasi di jaringan MAN, memberikan performa konektivitas yang lebih optimal dibandingkan *Ipsec*. Penelitian ini menekankan pentingnya pemilihan protokol yang tepat dalam membangun infrastruktur jaringan yang aman dan handal, serta memberikan referensi praktis bagi pengembangan jaringan berbasis kebutuhan spesifik di masa mendatang.

5. DAFTAR PUSTAKA

[1] Ariyadi, T. & Roy J. (2024). Perancangan Jaringan Lan Di Sekolah Menggunakan *Cisco packet tracer* Dan Protokol *Routing* Ospf. *Jurnal Ilmiah Teknik dan Ilmu Komputer*, 242 – 248.

[2] Aulia, R., Risko L. & Haida D. (2024). Analisis *Routing* Loop dalam *Open Shortest Path First* (OSPF) *Routing* Menggunakan Teknik Spanning Tree di Jaringan Multi Area. *Jurnal Ilmu Komputer*, 158-168.

[3] Firdausi, A. & Hamam W. W. (2020). Simulasi dan Analisa QoS dalam Jaringan VPN Site to Site Berbasis *Ipsec* dengan *Routing* Dynamic. *Jurnal Telekomunikasi dan Komputer*, 49-56.

[4] Forbacha, S. C. & Mbuya J. A. A. (2023). Design and Implementation of a Secure *Virtual Private Network* Over an Open *Network* (Internet). *American Journal of Technology*, 1-36.

[5] Gultom, A. S ., 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), 1-2*

[6] Juliansyah, J. & Yuma A. (2023). Optimalisasi Kinerja Jaringan Vpn Dengan Metode Dmvpn. *Jurnal Indonesia: Manajemen Informatika dan Komunikasi*, 1788-1798.

[7] Musril, H. A. (2019). Desain *Virtual Private Network* (VPN) Berbasis *Open Shortest Path First* (OSPF). *Jurnal Nasional Informatika dan teknologi jaringan*, 187-192.

[8] Prayitno, H. & Irwan A. S. (2025). Implementasi Jaringan *VPN site-to-site* Dan Protokol Ospf Menggunakan Cisco Di Sekolah Bina Bangsa. *Jurnal Informatika dan Teknik Elektro Terapan*, 196-202.

[9] Said, M. A., Setyorini & Erwid M. J. (2022). Analysis of *Ipsec* Implementation on Dynamic Multipoint VPN Protokol Using *Routing* Border Gateway Protokol. *Building of Informatics, Technology and Science (BITS)*, 595−605.

[10] Setianto, M. A. & Yuli F. (2023). Implementasi *GRE* Over *Ipsec Tunnel* VPN Menggunakan Fortigate. *Jurnal Politeknik Caltex Riau,* 212-223.

[11] Thaenchaikun, C. & Komsan K. (2025). A Comparative Study of OSPF Metrics in *Routing* Algorithms for Dynamic Path Selection in *Network* Security. *Journal of Scientific and Technological Reports*, 1-17.

[12] Wicaksana, P., Febri H. & Aulia F. H. (2021). Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan *Ipsec* Sebagai Keamanan Jaringan. *Jurnal KomtekInfo*, 169-175.

[13] Wiranata, A. B., Apriana, G. A., & Almantara, I. P. S. (2024). Review Perbandingan Kinerja Named Data *Network* Dan Ip Based *Network*ing. *Jurnal Teknologi Informasi dan Komputer*, *10*(1).