ANALISIS IMPLEMENTASI VPN IPSEC DI ATAS ROUTING DINAMIS PROTOKOL OSPF MENGGUNAKAN CISCO

Desni Paramitha Purba[1], Leni Karmila Daulay[2], Yusmita Imelda[3], Dedy Kiswanto[4]
desnypurba9@mhs.unimed.ac.id[1], lenikarmila.4231250006@mhs.unimed.ac.id[2],
yusmita.423125002@mhs.unimed.ac.id[3], dedykiswanto@unimed.ac.id[4]
Universitas Negeri Medan

ABSTRAK

Kebutuhan akan jaringan yang aman dan efisien semakin meningkat, terutama untuk organisasi yang memiliki banyak lokasi operasional. Teknologi Virtual Private Network (VPN) dengan protokol IPsec menjadi solusi dalam menjamin keamanan komunikasi data melalui jaringan publik. Di sisi lain, protokol routing dinamis seperti OSPF (Open Shortest Path First) memberikan efisiensi dalam pengaturan jalur komunikasi di jaringan. Penelitian ini bertujuan untuk menganalisis implementasi VPN IPsec di atas protokol routing OSPF menggunakan perangkat Cisco. Metode yang digunakan adalah berupa simulasi jaringan melalui Cisco Packet Tracer. Topologi jaringan yang dibangun terdiri dari tiga router Cisco yang saling terhubung, di mana VPN IPsec dikonfigurasi antara dua router yang mewakili site berbeda, dan OSPF digunakan sebagai protokol routing antar router. Hasil simulasi menunjukkan bahwa konfigurasi VPN IPsec tidak mengganggu fungsi kinerja OSPF, dan konektivitas antar perangkat tetap berjalan stabil. VPN IPsec terbukti mampu memberikan enkripsi data yang efektif tanpa mengurangi performa routing. Dengan demikian, kombinasi OSPF dan VPN IPsec layak diterapkan pada jaringan yang membutuhkan keamanan dan efisiensi/ kestabilan koneksi tinggi.

Kata Kunci: VPN, IPsec, OSPF, Cisco, Simulasi Jaringan, Keamanan Data, Enkripsi, Packet Tracer.

PENDAHULUAN

Virtual Private Network (VPN) adalah teknologi yang memungkinkan terbentuknya sebuah jaringan data pribadi atau private pada jaringan publik dengan menerapkan otentikasi dan enkripsi sehingga hanya pihak tertentu yang dapat mengakses jaringan tersebut. (Hadi & Irwan, 2025). Dengan diterapkannya VPN pada sistem jaringan ini maka dapat memungkinkan kedua router (router kiri dan router kanan) dapat berkomunikasi secara aman pada semua jaringan publik dengan baik sehingga jaringan publik dapat beroperasi sebagai satu atau beberapa tautan komunikasi pribadi. Seperti masalah yang kita lihat, ada beberapa yang ditemui diantaranya, komunikasi antar PC masih belum optimal. Pengiriman data dari router kiri ke router kanan atau sebaliknya masih belum terenkripsi yang dimana masalah ini dapat mengakibatkan data dapat dilihat atau bahkan di ambil oleh orang yang tidak berkepentingan sehingga perlu penerapan VPN di sistem jaringan ini. Serta menambahkan protokol OSPF (Open Shortest Path First).

IPsec (Internet Protocol Security) merupakan protokol yang menyediakan keamanan komunikasi melalui otentikasi dan enkripsi pada layer IP. Dengan menggunakan IPsec, organisasi dapat membangun koneksi yang terenkripsi antara dua jaringan, memastikan kerahasiaan dan integritas data yang ditransmisikan. Sementara itu, dalam pengelolaan jalur komunikasi di dalam jaringan, protokol routing dinamis seperti OSPF memberikan efisiensi tinggi karena kemampuannya dalam menyesuaikan rute secara otomatis berdasarkan kondisi jaringan terkini.

Routing merupakan proses untuk meneruskan paket yang dikirim dan digunakan untuk memilih jalur dari sebuah jaringan. Jenis dari routing ada beragam, ada yang statis dan dinamis. Sedangkan routing OSPF itu sendiri merupakan salah satu dari jenis routing

yang tersedia, masuk dalam kategori routing dinamis. Open Shortest Path First (OSPF) adalah sebuah routing protokol yang dipergunakan untuk merutekan paket data yang akan dikirimkan dari sebuah komputer ke komputer lain dalam jaringan komputer (Hadi & Irwan, 2020).

Cisco sebagai perangkat jaringan telah mengintegrasikan kedua teknologi ini dalam perangkatnya, memungkinkan pengguna untuk mengimplementasikan VPN IPsec dan OSPF secara bersamaan. Oleh karena itu, artikel ini mengangkat studi mengenai bagaimana implementasi VPN IPsec dapat dilakukan di atas routing OSPF menggunakan perangkat Cisco, serta mengevaluasi kinerja dan manfaatnya.

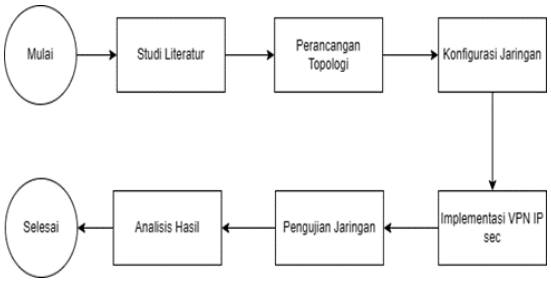
Dalam era digital, kebutuhan akan jaringan yang aman, fleksibel, dan dapat diandalkan menjadi tantangan utama dalam pengembangan infrastruktur jaringan modern, terutama untuk perusahaan atau institusi yang memiliki banyak lokasi operasional. Penggunaan jaringan publik seperti internet membuka risiko kebocoran data, sehingga dibutuhkan metode pengamanan seperti Virtual Private Network (VPN) yang didukung oleh protokol keamanan IPsec.

Disisi lain, pengaturan lalu lintas jaringan secara efisien memerlukan protokol routing dinamis. OSPF merupakan protokol yang mampu secara otomatis menyesuaikan rute berdasarkan kombinasi jaringan terkini. Kombinasi VPN IPsec dan OSPF memberikan solusi yang ideal untuk komunikasi data aman atar site.

Penelitian ini bertujuan untuk menganalisis bagaimana VPN IPsec dapat diimplementasikan di atas OSPF menggunakan perangkat Cisco, serta mengevaluasi pengaruhnya terhadap performa jaringan.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan eksperimental berbasis simulasi jaringan pada Cisco Packet Tracer.



Gambar 1. Alur Penelitian

Ada beberapa tahapan yang harus dilakukan yaitu:

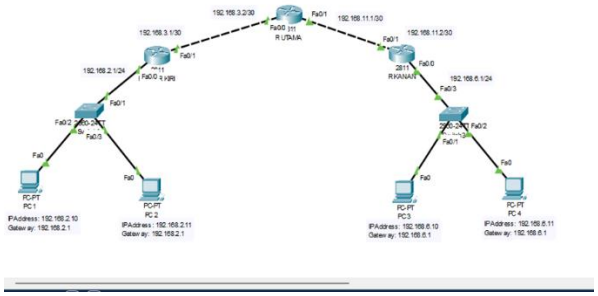
1. Studi Literatur

Penelitian dimulai dengan studi literatur terhadap sepuluh jurnal ilmiah yang membahas implementasi VPN IPsec, routing OSPF, dan simulasi jaringan menggunakan perangkat Cisco. Jurnal-jurnal ini dijadikan dasar dalam membangun simulasi dan interpretasi hasil. Tujuan dari tahap ini adalah memperkuat landasan teori dan metodologi dalam membangun simulasi.

2. Perancangan Topologi Jaringan

Perancangan dilakukan dengan membangun topologi jaringan terdiri atas tiga router (2811): (Router Kiri, Router Tengah/Utama, dan Router Kanan), dua switch, dan 4 (empat) PC. Dua site jaringan direpresentasikan masing-masing dengan satu router Cisco, dihubungkan melalui jaringan publik (internet), serta masing-masing site memiliki beberapa PC sebagai endpoint. Routing tengah fungsinya menjadi penghubung kedua site melalui jaringan publik. Protokol routing OSPF digunakan untuk memastikan jalur komunikasi antar router, dan tunnel VPN IPsec dikonfigurasikan antara Router Kiri dan

Router Kanan. Masing-masing router memiliki segmentasi jaringan lokal yang terhubung ke switch dan PC. Berikut adalah gambar topologinya:



Gambar 2. Topologi Jaringan VPN IPsec di atas OSPF dengan Switch dan PC

Router Kiri dan Router Kanan mewakili dua site yang dihubungkan melalui Router Tengah/Utama sebagai jalur publik. OSPF digunakan untuk routing dinamis, sedangkan tunnel VPN IPsec dibentuk antara Router Kiri dan Router Kanan.

3. Konfigurasi Jaringan

Tahap konfigurasi dimulai dari penentuan alamat IP pada masing-masing antarmuka di setiap router. Setelah semua perangkat saling terkoneksi secara fisik, konfigurasi OSPF diterapkan pada ketiga router dengan mengaktifkan proses OSPF dan menentukan network yang termasuk dalam Area 0. Berikut konfigurasi dilakukan secara bertahap:

❖ Menentukan IP address setiap antarmuka pada ketiga router sesuai topologi.IP address diberikan sesuai segmentasi.

- Router Kiri: IP: 192.168.2.1 pada Fa0/0 ke switch IP: 192.168.3.1 pada Fa0/1 ke R UTAMA
- Router Utama: IP: 192.168.3.2 pada Fa0/0 ke R KIRI IP: 192.168.11.1 pada Fa0/1 ke R KANAN
- Router Kanan: IP: 192.168.11.2 pada Fa0/1 ke R UTAMA IP: 192.168.6.1 pada Fa0/0 ke switch

❖ Mengaktifkan protokol routing OSPF pada seluruh router.

- Router KIRI: Router ini terhubung ke:
  LAN 192.168.2.0/24
  R UTAMA: 192.168.3.0/30
  Konfigurasinya:
  enable
  conf t
  router ospf 1
  network 192.168.2.0 0.0.0.255
  area 0
  network 192.168.3.0 0.0.0.3
  area 0
- Router UTAMA: Router ini terhubung ke:
  R KIRI: 192.168.3.0/30
  R KANAN: 192.168.11.0/30
  Konfigurasinya:
  enable
  conf t
  router ospf 1
  network 192.168.3.0 0.0.0.3 area 0
  network 192.168.11.0 0.0.0.3 area 0

- Router KANAN: Router ini terhubung ke:
  LAN 192.168.6.0/24
  R UTAMA: 192.168.11.0/30
  Konfigurasinya:
  enable
  conf trouter ospf
  network 192.168.6.0 0.0.0.255 area 0
  network 192.168.11.0 0.0.0.3 area 0
  Selanjutnya, konfigurasi VPN IPsec dilakukan secara bertahap mulai dari:

1. Membuataccess-list.
   - access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.6.0 0.0.0.255 (di R1)
   - access-list 100 permit ip 192.168.6.0 0.0.0.255 192.168.2.0 0.0.0.255 (di R3)
2. Membuat kebijakan ISAKMP (Phase 1):
   crypto isakmp policy 10
   encryption aes
   hash sha
   authentication pre-share
   group 2
   lifetime 86400
3. Menambahkan kunci bersama:
   - crypto isakmp key vpn123 address 192.168.11.2 (di R1)
   - crypto isakmp key vpn123 address 192.168.3.1 (di R3)
4. Membuat transform-set (Phase 2):
   crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
5. Membuat dan menempelkan crypto map:
   Crypto map & Transform-set: crypto map VPN-MAP 10 ipsec-isakmp
   set peer <IP-Public-Remote>
   set transform-set VPN-SET
   match address 100
   interface Fa0/1
   crypto map VPN-MAP

HASIL DAN PEMBAHASAN

Topologi jaringan yang digunakan terdiri dari tiga buah router Cisco (Router Tengah, Router Kiri, dan Router Kanan). Router Tengah berfungsi sebagai penghubung utama antar site, sementara Router Kiri dan Router Kanan mewakili dua jaringan yang berbeda. Untuk memastikan semua jaringan saling terhubung, dilakukan konfigurasi routing dinamis OSPF pada ketiga router. Langkah ini diulang pada Router Kiri dan Kanan sesuai dengan IP yang digunakan. Setelah konfigurasi, dilakukan uji konektivitas menggunakan perintah ping antar router dan PC untuk memastikan bahwa semua jalur komunikasi telah terbentuk dengan baik.

Sebelum penerapan VPN IPsec, konektivitas antar jaringan lokal (192.168.2.0/24 dan 192.168.6.0/24) telah berjalan dengan baik melalui protokol OSPF. Pengujian konektivitas menggunakan perintah ping menunjukkan tidak ada paket yang hilang (0% packet loss), yang menandakan bahwa rute OSPF sudah dikonfigurasi dengan benar dan stabil.

Namun, data yang dikirimkan antar site masih dalam bentuk plaintext, artinya seluruh informasi dapat dengan mudah disadap pihak ketiga saat melintas di jalur publik. Ini menjadi celah keamanan serius pada jaringan.

A. Implementasi Jaringan

Dalam tahapan untuk implementasi jaringan ini dilakukan beberapa konfigurasi pada perangkat yang ada di sistem jaringan yang ada yaitu dengan menerapkan beberapa konfigurasi.Ada beberapa tahapan yaitu:

1. Konfigurasi router utama (R2)

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
ip address 192.168.3.2 255.255.255.0
Router(config-if)#ip address 192.168.3.2 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
ip address 192.168.11.1 255.255.255.0
Router(config-if)#ip address 192.168.11.1 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface                    FastEthernet0/0
Router(config-if)#
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet changed state to up

2. Konfigurasi router kanan (R3)

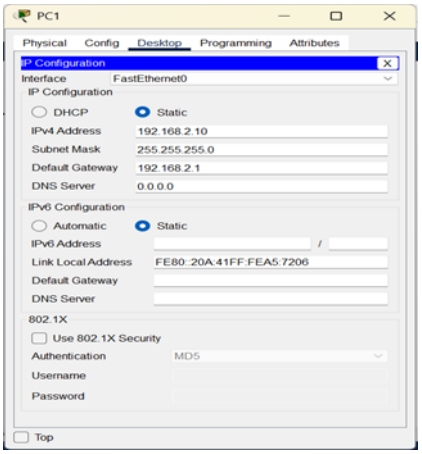
```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED:Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN:
Line protocol on Interface FastEthernet0/0, changed state to up
ip address 192.168.11.2 255.255.255.0
Router(config-if)#ip
address 192.168.11.2 255.255.255.0
Router(config-if)#
Router(config-if)#exit
```

Router(config)#interface FastEthernet0/1
Router(config-if)#ipaddress 192.168.6.1 255.255.255.0
Router(config-if)#ip
address 192.168.6.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED:Interface
FastEthernet0/1, changed state to up

3. Konfigurasi router Kiri (R3)

Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#ipaddress 192.168.3.1 255.255.255.0
Router(config-if)#ipaddress 192.168.3.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED:interface FastEthernet0/0, changed state to up %LINEPROTO-5-UPDOW
Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED:Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN:Line protocol on Interface FastEthernet0/1, changed state to up
ip address 192.168.2.1 255.255.255.0
Router(config-if)#ipaddress 192.168.2.1 255.255.255.0
Router(config-if)#

4. Konfigurasi PC/Server



Gambar 3. Konfigurasi salah satu PC

B. Pengujian Jaringan Awal

Dalam penerapannya dan juga tahapan selanjutnya adalah sebelum implementasi VPN IPsec, konfigurasi routing OSPF pada semua router terhubung dan dapat bertukar informasi routing secara dinamis, memungkinkan PC1 dan PC3, P2 dan PC4 saling

melakukan ping tanpa kendala. Namun demikian, data yang dikirim antar jaringan belum melalui proses enkripsi sehingga masih dalam bentuk plaintext.

1. Konfigurasi OSPF Pada Semua Router Dan Hasil Pingnya:

- Router Kiri (R1)

Konfigurasinya:

```
R.KIRI >enable
R.KIRI#
R.KIRI(config)#router ospf 1
R.KIRI(config-router)#network 192.168.2.0 0.0.0.255 area 0
R.KIRI(config-router)#network 192.168.3.0 0.0.0.3 area 0
R.KIRI(config-router)#
R.KIRI(config-router)#exit
R.KIRI(config)#end
R.KIRI#
%SYS-5-CONFIG_I: Configured from console by console
R.KIRI#wr
Building configuration...
[OK]
R.KIRI#
```

❖ Hasil Ping R1-R2:

```
R.KIRI#
R.KIRI#ping 192.168.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/10 ms
```

❖ Pastikan ospf sudah muncul: show ip route ospf

```
R.KIRI>enable
R.KIRI#show ip route ospf
O 192.168.6.0 [110/3] via 192.168.3.2, 00:43:10, FastEthernet0/1
O 192.168.11.0 [110/2] via 192.168.3.2, 00:45:27, FastEthernet0/1
```

❖ Router Utama (R2)

Konfigurasinya:

```
R.UTAMA(config)#router ospf 1
R.UTAMA(config-router)# network 192.168.3.0 0.0.0.3 area 0
R.UTAMA(config-router)# network 192.168.11.0 0.0.0.3 area 0
R.UTAMA(config-router)#
R.UTAMA(config-router)#end
R.UTAMA#
%SYS-5-CONFIG_I: Configured from console by console
R.UTAMA#wr
Building configuration...
[OK]
```

❖ Hasil ping R2-R3:

```
R.UTAMA#
R.UTAMA#ping 192.168.11.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.11.2, timeout is 2 seconds:
!!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/12 ms
R.UTAMA#

❖ Pastikan Ospf Sudah Muncul: Show Ip Route Ospf
R.UTAMA>enable
R.UTAMA# show ip route ospf
O 192.168.2.0 [110/2] via 192.168.3.1, 00:42:56, FastEthernet0/0
O 192.168.6.0 [110/2] via 192.168.11.2, 00:41:01, FastEthernet0/1

❖ Router Kanan (R3)
R.KANAN(config)#router ospf 1
R.KANAN(config-router)#network 192.168.6.0 0.0.0.255 area 0
R.KANAN(config-router)#network 192.168.11.0 0.0.0.3 area 0
R.KANAN(config-router)#
R.KANAN(config-router)#end
R.KANAN#
%SYS-5-CONFIG_I: Configured from console by console
R.KANAN#wr
Building configuration...
[OK]
R.KANAN#

❖ Hasil ping R1-R3:
R.KANAN>enable
R.KANAN#ping 192.168.6.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.6.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/12/40 ms
R.KANAN#

❖ Pastikan Ospf Sudah Muncul: Show Ip Route Ospf:
R.KANAN#show ip route ospf
O 192.168.2.0 [110/3] via 192.168.11.1, 00:38:06, FastEthernet0/1
O 192.168.3.0 [110/2] via 192.168.11.1, 00:38:06, FastEthernet0/1

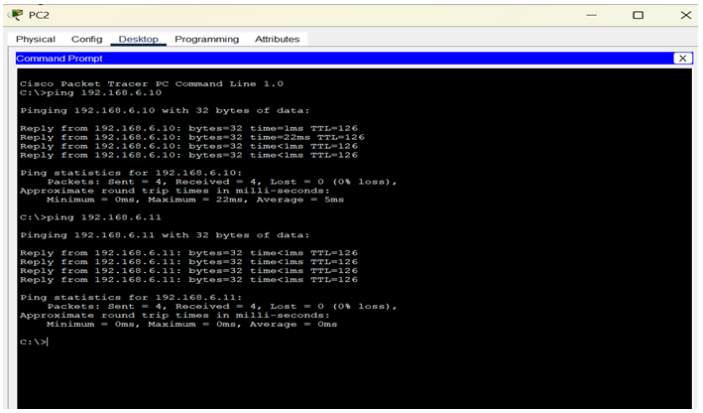
2. Selanjutnya, Konfigurasi VPN Ipsec Dilakukan Secara Bertahap Mulai Dari:

❖ Router Kiri (R1)
R.KIRI>enable
R.KIRI#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R.KIRI(config)#access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.6.0 0.0.0.255
R.KIRI(config)#
R.KIRI(config)#crypto isakmp policy 10
R.KIRI(config-isakmp)# encryption aes
R.KIRI(config-isakmp)# hash sha
R.KIRI(config-isakmp)# authentication pre-share
R.KIRI(config-isakmp)# group 2
R.KIRI(config-isakmp)# lifetime 86400
R.KIRI(config-isakmp)#crypto isakmp key vpn123 address 192.168.11.2
R.KIRI(config)#
R.KIRI(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R.KIRI(config)#crypto map VPN-MAP 10 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R.KIRI(config-crypto-map)# set peer 192.168.11.2
R.KIRI(config-crypto-map)# set transform-set VPN-SET
R.KIRI(config-crypto-map)# match address 100
R.KIRI(config-crypto-map)#
R.KIRI(config-crypto-map)#interface fa0/1
R.KIRI(config-if)# crypto map VPN-MAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R.KIRI(config-if)#end
R.KIRI#
%SYS-5-CONFIG_I: Configured from console by console
R.KIRI#wr
Building configuration...
[OK]
R.KIRI#

❖ Router Kanan (R1)

R.KANAN>enable
R.KANAN#conf
Enter configuration commands, one per line. End with CNTL/Z.
R.KANAN(config)#access-list 100 permit ip 192.168.6.0 0.0.0.255 192.168.2.0 0.0.0.255
R.KANAN(config)#crypto isakmp policy 10
R.KANAN(config-isakmp)# encryption aes
R.KANAN(config-isakmp)# hash sha
R.KANAN(config-isakmp)# authentication pre-share
R.KANAN(config-isakmp)# group 2
R.KANAN(config-isakmp)# lifetime 86400
R.KANAN(config-isakmp)#
R.KANAN(config-isakmp)#crypto isakmp key vpn123 address 192.168.3.1
R.KANAN(config)#crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
R.KANAN(config)#crypto map VPN-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R.KANAN(config-crypto-map)#set peer 192.168.3.1
R.KANAN(config-crypto-map)# set transform-set VPN-SET
R.KANAN(config-crypto-map)# match address 100
R.KANAN(config-crypto-map)#
R.KANAN(config-crypto-map)#interface fa0/1
R.KANAN(config-if)# crypto map VPN-MAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R.KANAN(config-if)#
R.KANAN(config-if)#end
R.KANAN#
%SYS-5-CONFIG_I: Configured from console by console
R.KANAN#
Building configuration...
[OK]
R.KANAN#



Gambar 4. Hasil ping antar PC sebelum VPN aktif

❖ Router Kiri(R1)

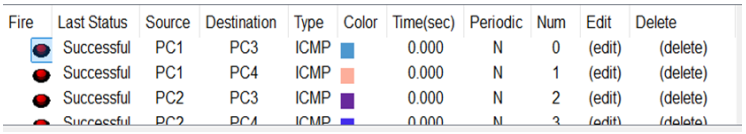
R.KIRI>enable
R.KIRI#
R.KIRI#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id slot status
192.168.11.2 192.168.3.1 QM_IDLE 1093 0 ACTIVE
IPv6 Crypto ISAKMP SA
R.KIRI#show crypto ipsec sa
interface: FastEthernet0/1
Crypto map tag: VPN-MAP, local addr 192.168.3.1
protected vrf: (none)
localident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
remoteident (addr/mask/prot/port): (192.168.6.0/255.255.255.0/0/0)
current_peer 192.168.11.2 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 15, #pkts encrypt: 15, #pkts digest: 0
#pkts decaps: 13, #pkts decrypt: 13, #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.: 192.168.3.1, remotecrypto endpt.:192.168.11.2
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
current outbound spi: 0x4C347619(1278506521)
inbound esp sas:
spi: 0x1B08A298(453550744)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2001, flow_id: FPGA:1, crypto map: VPN-MAP
sa timing: remaining key lifetime (k/sec): (4525504/3286)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE
inbound ah sas:
inbound pcp sas:
outbound esp sas:

spi: 0x4C347619(1278506521)
transform: esp-aes esp-sha-hmac,
in use settings ={Tunnel, }
conn id: 2002, flow_id: FPGA:1, crypto map: VPN-MAP
sa timing: remaining key lifetime (k/sec): (4525504/3286)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE
outbound ah sas:
outbound pcp sas:

❖ Router Kanan(R3)

R.KANAN>enable
R.KANAN#
R.KANAN#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id slot status
192.168.3.1 192.168.11.2 QM_IDLE 1020 0 ACTIVE
IPv6 Crypto ISAKMP SA
R.KANAN#show crypto ipsec sa
interface: FastEthernet0/1
Crypto map tag: VPN-MAP, local addr 192.168.11.2
protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.6.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current_peer 192.168.3.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 13, #pkts encrypt: 13, #pkts digest: 0
#pkts decaps: 15, #pkts decrypt: 15, #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.: 192.168.11.2, remote crypto endpt.:192.168.3.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
current outbound spi: 0x1B08A298(453550744)
inbound esp sas:
spi: 0x4C347619(1278506521)
transform: esp-aes esp-sha-hmac,
in use settings ={Tunnel, }
conn id: 2001, flow_id: FPGA:1, crypto map: VPN-MAP
sa timing: remaining key lifetime (k/sec): (4525504/3014)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x1B08A298(453550744)
transform: esp-aes esp-sha-hmac,

in use settings ={Tunnel, }
conn id: 2002, flow_id: FPGA:1, crypto map: VPN-MAP
sa timing: remaining key lifetime (k/sec): (4525504/3014)
IV size: 16 bytes
replay detection support: N
Status: ACTIVE
outbound ah sas:
outbound pcp sas:
R.KANAN#



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1	PC3	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC1	PC4	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC2	PC3	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC2	PC4	ICMP		0.000	N	3	(edit)	(delete)

Gambar 5. Hasil ping setelah uji koneksi dan validasi VPN

C. Hasil Koneksi

1. Sebelum Implementasi VPN IPsec

Pada kondisi awal sebelum implementasi VPN, seluruh perangkat baik router maupun PC dapat saling terhubung menggunakan routing dinamis OSPF. Komunikasi antar jaringan 192.168.2.0/24 (Site Kiri) dan 192.168.6.0/24 (Site Kanan) berjalan lancar menggunakan perintah ping. Namun, data yang dikirimkan melalui jaringan publik belum dienkripsi, sehingga masih berisiko untuk disadap oleh pihak ketiga.

Tanpa VPN, informasi penting bisa dikirim secara plaintext (pesan asli) dan rawan disadap, khususnya ketika melewati jaringan publik. Dengan VPN IPsec, dapat membuat jalur aman seolah-olah site kiri dan site kanan berada dalam satu LAN.

Setelah routing OSPF berhasil, selanjutnya dilakukan konfigurasi tunnel VPN IPsec antara Router Kiri dan Router Kanan. Tujuannya adalah untuk mengenkripsi data yang lewat jalur publik (antara Router Kiri dan Router Kanan via Router Tengah).

2. Setelah Implementasi VPN IPsec

Setelah konfigurasi VPN IPsec diterapkan antara Router KIRI dan Router KANAN, tunnel VPN berhasil terbentuk. Trafik antar jaringan lokal kedua site kini melalui tunnel terenkripsi. Hasil uji konektivitas menggunakan ping tetap berhasil, menunjukkan bahwa konektivitas tetap stabil dan proses enkripsi tidak mengganggu komunikasi antar jaringan.

Berikut Tabel Ringkasan Kondisi Sebelum dan Sesudah Implementasi VPN IPsec:

Aspek	Sebelum VPN Ipsec	Sesudah VPN Ipsec
Konektivitas	Stabil, komunitas antar site berjalan normal	Stabil, komunikasi tetap berjalan tanpa gangguan
Keamanan data	Data dikirim dalam bentuk plaintext (rawan disadap)	Data dienkripsi, aman dari penyadapan
Validasi Tunnel	Tidak ada tunnel VPN	Tunnel aktif, status ISAKMP: QM_IDLE
Statistik Enkripsi	Tidak ada paket terenkripsi	Ada paket terenkripsi dan terdekripsi
Routing OSPF	Berfungsi normal	Tetap berfungsi normal, tidak terganggu
Performa Jaringan	Optimal, tanpa delay	Optimal, tidak ada penurunan performa yang signifikan

D. Stabilitas dan Keamanan

Implementasi VPN IPsec tidak mempengaruhi kestabilan protokol routing OSPF. Semua router tetap dapat bertukar informasi routing, memperbarui tabel rute secara dinamis, dan memastikan jalur komunikasi antar site berjalan normal. Keamanan data meningkat signifikan melalui penggunaan protokol ESP (Encapsulating Security Payload), yang mengenkripsi payload data dan melindungi integritas paket. Selain itu, penggunaan

metode autentikasi berbasis pre-shared key memastikan hanya perangkat terpercaya yang dapat membentuk tunnel VPN, menghindari serangan "man-in-the-middle". Monitoring tunnel menunjukkan semua trafik antar site telah terenkripsi, menjaga kerahasiaan dan integritas data sepenuhnya.

Catatan tambahan:

- Beban CPU router tetap dalam batas normal setelah penerapan VPN.
- Overhead enkripsi-dekripsi dalam simulasi skala kecil ini tidak mempengaruhi performa jaringan secara signifikan.

E. Validasi dan Monitoring

Validasi dilakukan menggunakan perintah show pada router yang terlibat:

“show crypto isakmp sa”: Menampilkan status tunnel Phase 1 (ISAKMP). Status "QM_IDLE" menandakan bahwa tunnel aktif dan stabil.

“show crypto ipsec sa”: Menampilkan statistik enkripsi/dekripsi. Terdapat paket encrypted dan decrypted yang menunjukkan bahwa data telah berhasil dienkripsi saat melewati tunnel.

Hasil pengujian ping setelah VPN aktif menunjukkan konektivitas tetap stabil, tanpa adanya delay signifikan atau packet loss, membuktikan bahwa implementasi IPsec tidak menurunkan performa jaringan.

KESIMPULAN

Berdasarkan hasil simulasi dan analisis terhadap implementasi VPN IPsec di atas routing protokol OSPF menggunakan perangkat Cisco, dapat disimpulkan bahwa penggabungan antara protokol routing dinamis dan teknologi keamanan jaringan memberikan hasil yang optimal dalam hal konektivitas dan proteksi data.

Protokol OSPF berhasil mengatur jalur komunikasi antar router secara otomatis dan efisien, sementara VPN IPsec menjamin bahwa setiap paket data yang dikirim antar jaringan terenkripsi dan tidak dapat diakses oleh pihak yang tidak berwenang. Melalui simulasi di Cisco Packet Tracer, terlihat bahwa seluruh perangkat jaringan dapat saling terhubung dengan baik, baik sebelum maupun sesudah konfigurasi IPsec diterapkan.

Hal ini membuktikan bahwa IPsec dapat berjalan tanpa mengganggu kinerja OSPF sebagai pengatur rute. Implementasi ini sangat cocok digunakan dalam jaringan yang memiliki lebih dari satu lokasi atau cabang, seperti pada perusahaan atau lembaga pendidikan, yang memerlukan komunikasi data yang aman dan andal. Dengan demikian, penerapan VPN IPsec di atas OSPF terbukti menjadi solusi tepat dalam membangun jaringan yang aman.

DAFTAR PUSTAKA

Afrianto, D., Et Al. (2023). Perbandingan Kinerja Tunneling Vpn Ipsec Dan Vpn Ssl Pada Jaringan Komputer. Jurnal Teknologi Dan Sistem Informasi, 12(2), 123-130.

Ariyadi, T., & Jordi, R. (2024). Perancangan Jaringan Lan Di Sekolah Menggunakan Cisco Packet Tracer Dan Protocol Routing Ospf. Storage: Jurnal Ilmiah Teknik Dan Ilmu Komputer, 3(4), 242-248.

Ayub, M., Maulana, A., & Fauzi, A. (2021). Penerapan Firewall Dan Protokol Ipsec/L2tp Sebagai Solusi Keamanan Akses Jaringan Publik. Computer Science (Co-Science), 1(2), 81-90.

Damanik, H. A., Anggraeni, M., & Nusantari, F. A. A. (2023). Konsep Dan Penerapan Switching Dan Routing Implementasi Jaringan Komputer Berbasis Cisco. Mega Press Nusantara.

Dzikrullah Suratin, M., & Gunawan, E. (2024). Analisis Kinerja Routing Protokol Ospf Dengan Frrouting (Frr). Jurnal Teknik Informatika (J-Tifa), 7(2), 18-27.

Firdausi, A., & Wardani, H. W. (2020). Simulasi Dan Analisa Qos Dalam Jaringan Vpn Site To Site Berbasis Ipsec Dengan Routing Dynamic. Incomtech: Jurnal Telekomunikasi Dan

Komputer, 10(2), 49-56.
Fitrian, H. P., Nurani, A. A., Mulhakim, I., Maesaroh, N., & Raharja, P. (2025). Analisis Manajemen Trafik Jaringan Pada Virtual Private Network (Vpn) Menggunakan Protokol Pptp, L2tp/Ipsec, Dan Open Vpn. Jati (Jurnal Mahasiswa Teknik Informatika), 9(2), 2310-2314.
Oktavian, B. D., & Sobari, I. A. (2022). Implementasi Jaringan Terpusat Menggunakan Ospf Dan Vpn Dengan Failover Link Di Pt. Advantage Scm. Jurnal Teknik Mesin, Industri, Elektro Dan Informatika, 1(3), 69-88.
Ramdhani, A. I., & Anwar, S. (2024). Rancang Bangun Infrastruktur Jaringan Dengan Metodelogi Nat Dynamic Dan Routing Open Shortest Path First. Jupiter: Journal Of Computer & Information Technology, 5(2), 70-79.
Syahputra, R., Kurnia, R., & Ferdian, R. (2020). Analysis Of Fhrp Design And Implementation In Ripv2 And Ospf Routing Protocols. Jurnal Resti (Rekayasa Sistem Dan Teknologi Informasi), 4(1), 102-108.