

Virtual Private Network Tunneling Dengan Protokol IP in IP Melalui Jaringan Internet

Felix Wuryo Handono^{1,*}, Sumarna², Hafis Nurdin³

¹ Manajemen Informatika; AMIK Bina Sarana Informatika; Jl. RS. Fatmawati No. 24 Jakarta, 021-3100413; felix@bsi.ac.id

² Sistem Informasi; STMIK Nusa Mandiri; Jl. Damai No. 8, Warung Jati Barat (Margasatwa) Jakarta, 021-78839513; sumarna2008@gmail.com.

³ Sistem Informasi; STMIK Nusa Mandiri; Jl. Damai No. 8, Warung Jati Barat (Margasatwa) Jakarta, 021-78839513; haviezt.rnr@gmail.com

*Korespondensi: e-mail: felix@bsi.ac.id

Diterima: 10 Oktober 2017; Review: 15 oktober 2017; Disetujui: 21 Oktober 2017

Cara sitasi: Handono FW, Sumarna, Nurdin. H. 2017. VPN Tunneling Dengan Protokol IPIP Melalui Jaringan Internet. *Informatics For Educators and Professionals*. 2 (1): 61 – 70.

Abstrak: Internet menghubungkan jaringan komputer secara global dengan standar TCP/IP. Untuk dapat terhubung secara lokal melalui internet disebut *tunneling*. Dengan teknik *tunneling* melalui internet dapat menghubungkan secara *private* dengan tetap dapat menikmati koneksi ke area. Teknik yang dikenal dengan nama *tunneling* ini menghubungkan dua atau lebih jaringan LAN melalui jalur internet. IP in IP (IPIP) merupakan salah satu *protocol* dari beberapa *protocol tunneling* yang bekerja dengan mengenkapsulasi paket data dari satu IP ke IP yang lain.

Kata Kunci: *Internet, tunneling, IPIP*

Abstract: *The Internet connects the network of computers globally with standard TCP/IP. To be connected locally via the internet is called tunneling. With tunneling techniques through the internet can connect privately while still able to enjoy connections to the internet. This technique known as tunneling which connects two or more LAN networks through the internet. IP in IP (IPIP) is one of the protocols of several tunneling protocols that work by encapsulating data packets from one IP to another.*

Key Word: *Internet, tunneling IPIP*

1. Pendahuluan

Terhubung kedalam jaringan internet menjadi hal umum yang dibutuhkan bagi masyarakat modern saat ini. Tidak hanya masyarakat secara personal, kebutuhan komunikasi melalui jaringan internet juga dibutuhkan bagi institusi, perusahaan dan juga lainnya dengan tetap dapat terhubung secara private pada jaringan LAN.

Jaringan LAN adalah Komputer dan perangkat jaringan yang terhubung dalam jaringan komunikasi atau transimi.[Tanenbaum, 2003]

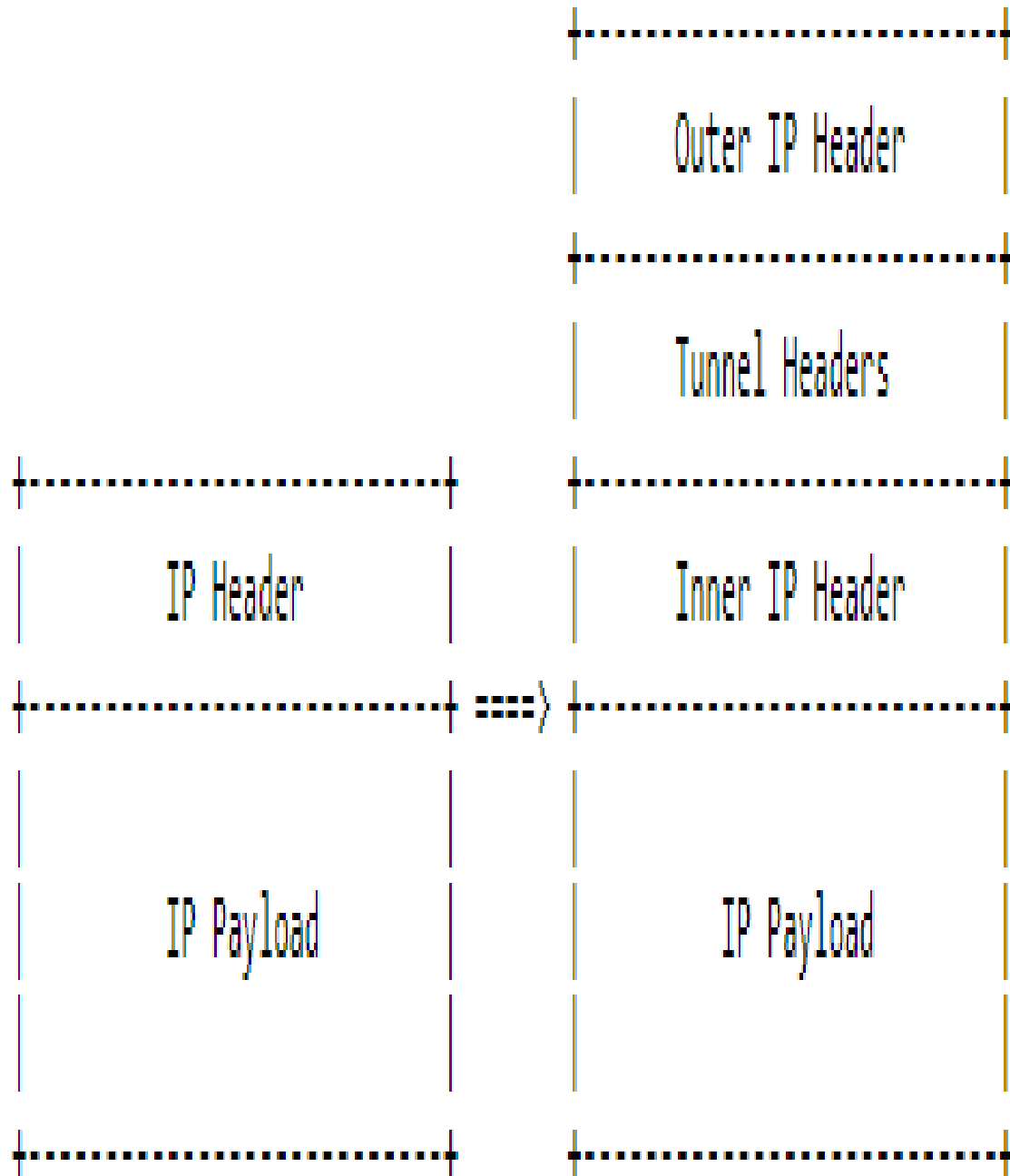
Pertumbuhan jumlah badan, institusi maupun perusahaan yang sama yang berkembang dan berekspansi ke luar wilayah membutuhkan jaringan komunikasi yang tetap dapat terhubung secara private dengan LAN. Perkembangan teknologi, terutama pada perangkat lunak komputer (dalam bentuk sistem operasi dan aplikasi), memungkinkan adanya konfigurasi dari suatu jaringan komputer secara virtual (virtualisasi). VLAN merupakan salah satu solusi yang diberikan untuk hal tersebut.[Pratama, 2015]

Tunnel adalah mekanisme yang digunakan untuk mengirimkan protokol asing ke jaringan yang biasanya tidak mendukungnya. Protokol *tunneling* memungkinkan Anda untuk menggunakan, misalnya IP untuk mengirim protokol lain di bagian "data" dari datagram IP. Kebanyakan protokol *tunneling* beroperasi pada layer 4, yang berarti protokol tersebut

diimplementasikan sebagai protokol yang menggantikan sesuatu seperti TCP atau UDP [Charlie Schluting, 2006].

VPN (*Virtual Private Network*) merupakan sebuah sambungan komunikasi yang bersifat pribadi dan dilakukan secara virtual [Supriyono et al., 2013].

IP in IP (IPIP) Tunnel adalah satu dari sekian protocol tunneling yang dapat digunakan dalam IPV4. IPIP adalah protokol yang mengenkapsulasi sebuah paket IP didalam paket IP lainnya.



Sumber: (Simpson, 1995)

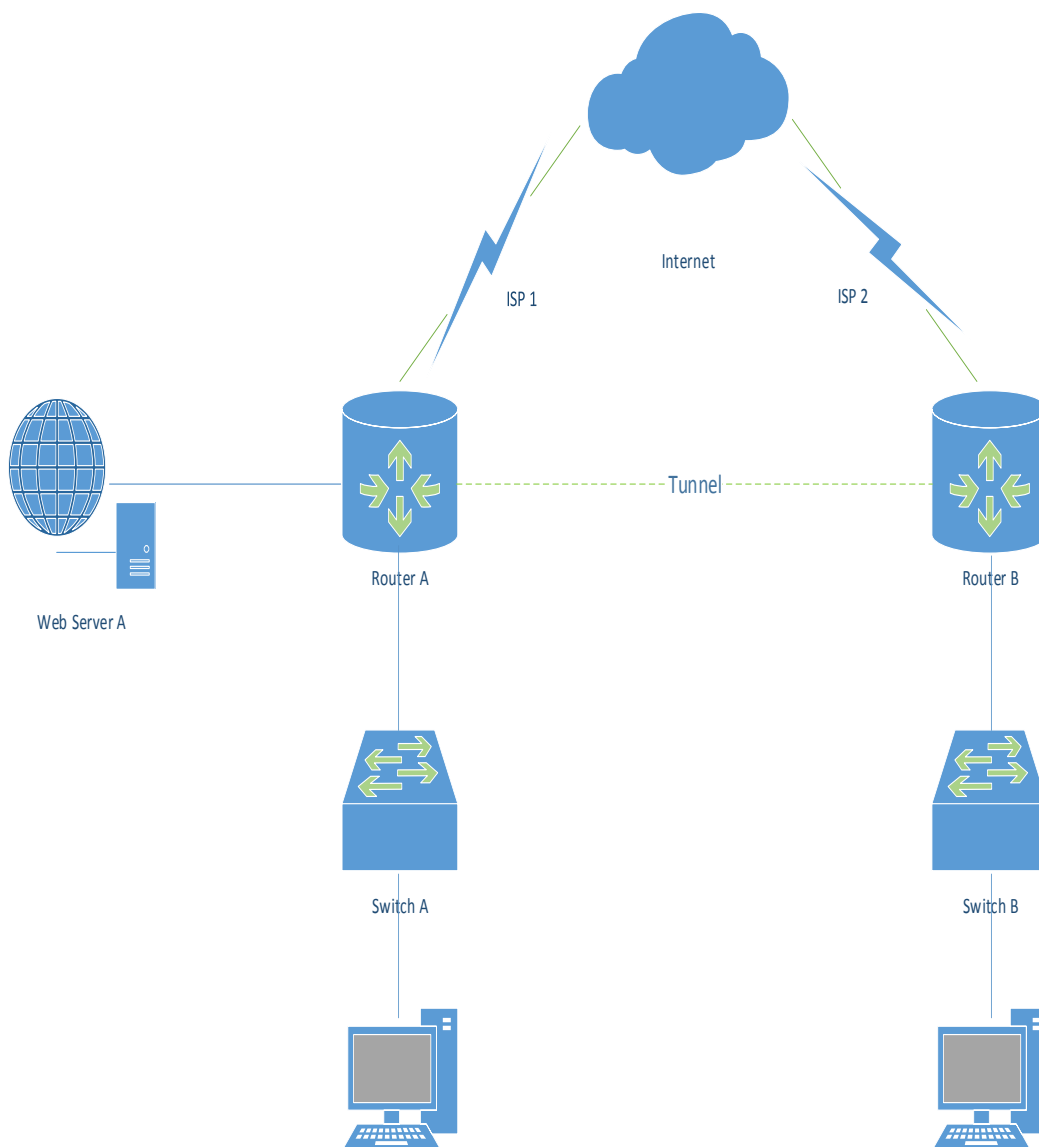
Gambar 1. IP in IP Encapsulation

Untuk mengenkapsulasi paket IP dalam Paket IP, *Header* terluar ditambahkan alamat sumber, IP masuk *tunnel* dan IP Tujuan, IP keluar *tunnel*.

Tunneling pada penelitian ini adalah sebagai salah satu cara yang digunakan untuk dapat terhubung secara LAN dengan memanfaatkan jalur internet dengan membuat kanal tersendiri yang terhubung lewat pengalamanan IP secara virtual dan melakukan enkapsulasi terhadap paket IP tersebut.

2. Metode Penelitian

Metode yang digunakan dalam penelitian ini diantaranya studi literatur, desain penelitian, implementasi dan pengujian. Studi literatur, dilakukan dengan mencari data dan informasi melalui sumber-sumber tulisan berupa jurnal, buku atau sumber lainnya yang berkaitan dengan penelitian. Desain penelitian, dengan membuat desain konfigurasi perangkat berdasar informasi umum tentang perangkat dan koneksi yang digunakan.



Sumber: Hasil Penelitian (2017)

Gambar 2. Topologi Jaringan

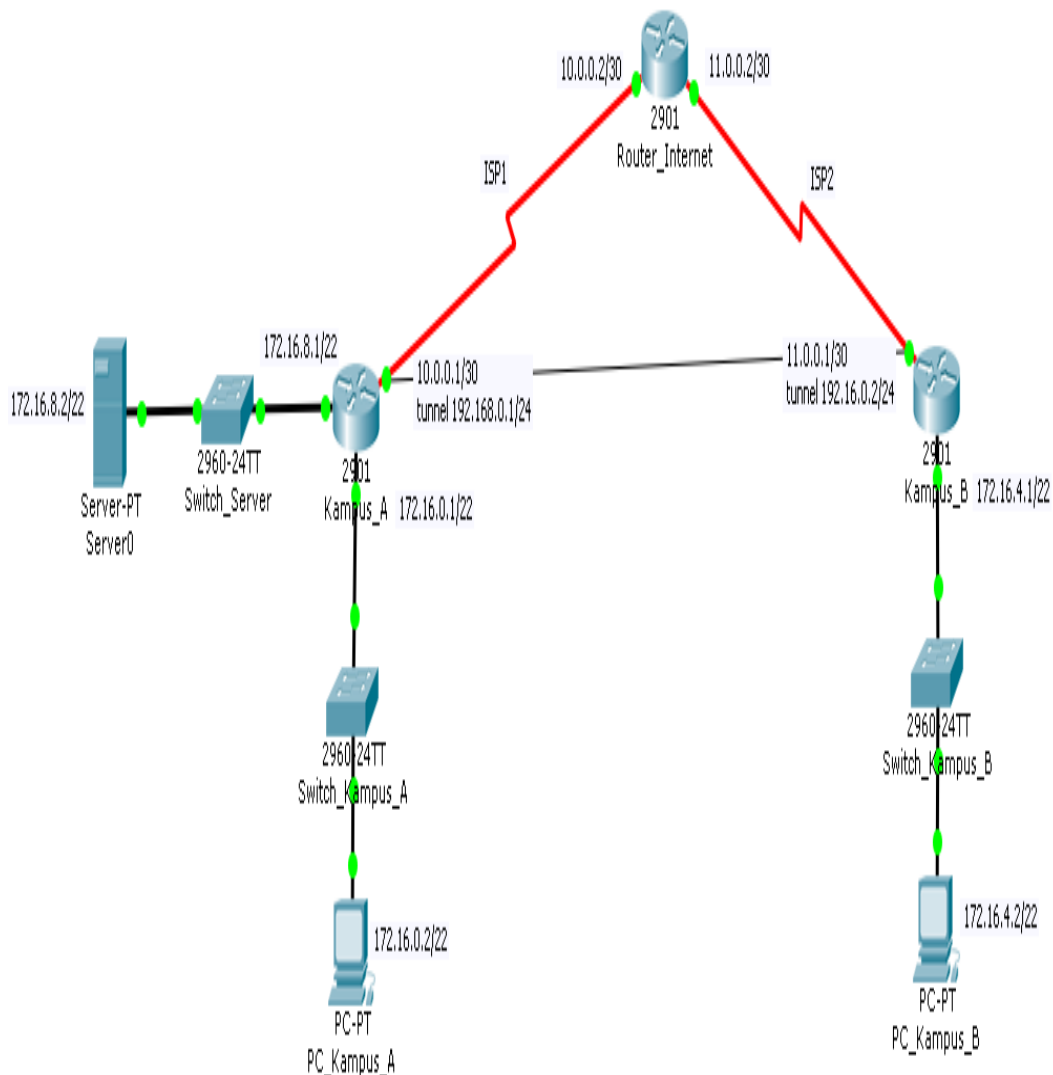
Tahapan implementasi kegiatan yang dilakukan yaitu melakukan konfigurasi virtual menggunakan *packet tracer* sebagai simulator implementasi *VPN Tunneling* menggunakan *protocol IPIP*. Dilanjutkan dengan tahap pengujian, pada tahap pengujian proses dilakukan dengan penelusuran paket IP melalui *VPN Tunneling*, kemudian melakukan analisa apakah paket berhasil dikirim dengan melalui jalur yang dibuat.

3. Hasil dan Pembahasan

Penelitian menggunakan aplikasi *Packet Tracer 7.0* sebagai perangkat *simulator VPN Tunneling* dengan *protocol IPIP*. Berikut tahapan percobaan yang dilakukan:

3.1. Perancangan Jaringan

Berikut adalah skema jaringan simulasi implementasi *VPN Tunneling* dengan *protocol IPIP*:



Sumber: Olahan Penelitian (2017)

Gambar 3. Skema Jaringan Simulasi Implementasi *VPN Tunneling* dengan *Protokol IPIP*

Berikut adalah tabel *IP Address* yang digunakan:

Tabel 1. *IP Address*

No	Interface	IP Address	Subnet Mask	Gateway
1 PC A				
	Fa0/0	172.16.0.2	255.255.252.0	172.16.0.1
2 PC B				
	Fa0/0	172.16.4.2	255.255.252.0	172.16.4.1
3 Server				
	Fa0	172.16.8.2	255.255.252.0	172.16.8.1
4 Router_Kampus_A				
	Gig0/0	172.16.0.1	255.255.252.0	
	Gig0/1	172.16.8.1	255.255.252.0	
	Se0/0/0	10.0.0.1	255.255.255.252	
5 Router_Kampus_B				
	Gig0/0	172.16.0.1	255.255.252.0	
	Se0/0/0	11.0.0.1	255.255.255.252	
6 Router_Internet				
	Se0/0/0	10.0.0.2	255.255.255.252	
	Se0/0/0	11.0.0.2	255.255.255.252	

Sumber: Hasil Pengolahan Data (2017)

Instalasi Router pada Router Kampus A dan B menggunakan dua model *protocol routing*. Routing pertama menggunakan Routing RIP untuk menghubungkan jaringan LAN (*Local Area Network*) yang terdapat dimasing-masing kampus ke Jaringan Internet yang disimulasikan dengan Router_Internet, sementara Routing yang digunakan untuk menghubungkan jaringan LAN antar kampus melalui *VPN Tunnel* menggunakan Routing EIGRP. Pemilihan Routing atas dasar pemilihan tipe routing yang diprioritaskan oleh Cisco Router sendiri agar akses antar LAN melalui tunnel menjadi prioritas utama dan bukan melalui IP Publik yang disimulasikan dengan Router_Internet.

Berikut konfigurasi routing Router RIP Version 2 pada Router Kampus A:

```
router rip
version 2
network 10.0.0.0
network 172.16.0.0
```

Berikut konfigurasi VPN Tunnel pada Router Kampus A:

```
interface Tunnel1
ip address 192.168.0.1 255.255.255.0
mtu 1476
tunnel source Serial0/0/0
tunnel destination 11.0.0.1
```

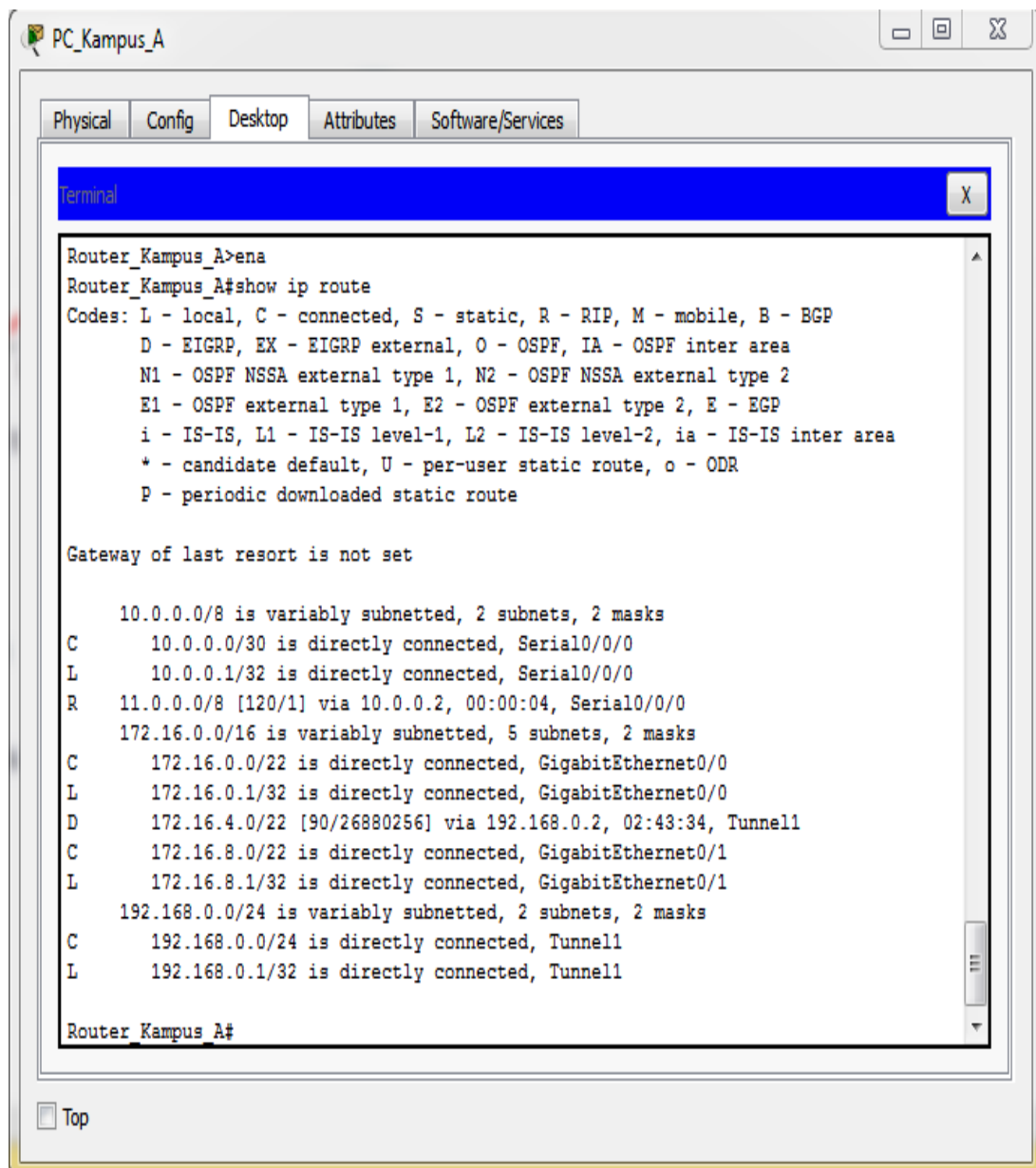
Konfigurasi VPN Tunnel menggunakan Interface Serial0/0/0, IP Address 11.0.0.1

Berikut konfigurasi routing Router EIGRP pada Router Kampus A:

```
router eigrp 1
network 172.16.0.0
network 192.168.0.0
```

Routing EIGRP menghubungkan network 172.16.0.0 dengan network 192.168.0.0, hal ini diperlukan karena VPN Tunnel menggunakan Protokol IPIP tidak dapat langsung terhubung ke perangkat interface namun menggunakan IP Penghubung.

Berikut adalah hasil konfigurasi routing Router Kampus A:



```

PC_Kampus_A
Physical Config Desktop Attributes Software/Services
Terminal
Router_Kampus_A>ena
Router_Kampus_A#show ip route
Codes: L - local, 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, E - EGP
       i - IS-IS, 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

 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.0.0.0/30 is directly connected, Serial0/0/0
L    10.0.0.1/32 is directly connected, Serial0/0/0
R    11.0.0.0/8 [120/1] via 10.0.0.2, 00:00:04, Serial0/0/0
 172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C    172.16.0.0/22 is directly connected, GigabitEthernet0/0
L    172.16.0.1/32 is directly connected, GigabitEthernet0/0
D    172.16.4.0/22 [90/26880256] via 192.168.0.2, 02:43:34, Tunnel1
C    172.16.8.0/22 is directly connected, GigabitEthernet0/1
L    172.16.8.1/32 is directly connected, GigabitEthernet0/1
 192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.0.0/24 is directly connected, Tunnel1
L    192.168.0.1/32 is directly connected, Tunnel1

Router_Kampus_A#
  
```

Sumber: Hasil Penelitian (2017)

Gambar 4. Hasil Konfigurasi Routing Router Kampus A

Berikut konfigurasi routing Router RIP Version 2 pada Router Kampus B:

```
router rip
version 2
network 11.0.0.0
network 172.16.4.0
```

Berikut konfigurasi VPN Tunnel pada Router Kampus A:

```
interface Tunnel1
ip address 192.168.0.2 255.255.255.0
mtu 1476
tunnel source Serial0/0/0
tunnel destination 10.0.0.1
```

Konfigurasi VPN Tunnel menggunakan Interface Serial0/0/0, IP Address 10.0.0.1

Berikut konfigurasi routing Router EIGRP pada Router Kampus A:

```
router eigrp 1
network 172.16.8.0
network 192.168.0.0
```

Routing EIGRP menghubungkan network 172.16.8.0 dengan network 192.168.0.0, hal ini diperlukan karena VPN Tunnel menggunakan Protokol IPIP tidak dapat langsung terhubung ke perangkat interface namun menggunakan IP Penghubung.

Berikut adalah hasil konfigurasi routing Router Kampus B:

```

Router_Kampus_B>ena
Router_Kampus_B#show ip route
Codes: L - local, 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, E - EGP
       i - IS-IS, 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    10.0.0.0/8 [120/1] via 11.0.0.2, 00:00:23, Serial0/0/0
     11.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C     11.0.0.0/30 is directly connected, Serial0/0/0
L     11.0.0.1/32 is directly connected, Serial0/0/0
     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
D     172.16.0.0/22 [90/26880256] via 192.168.0.1, 02:47:38, Tunnell
C     172.16.4.0/22 is directly connected, GigabitEthernet0/0
L     172.16.4.1/32 is directly connected, GigabitEthernet0/0
D     172.16.8.0/22 [90/26880256] via 192.168.0.1, 02:47:38, Tunnell
     192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.0.0/24 is directly connected, Tunnell
L     192.168.0.2/32 is directly connected, Tunnell

Router_Kampus_B#

```

Sumber: Olahan Penelitian (2017)

Gambar 5. Hasil Konfigurasi Routing Router Kampus B

3.2. Hasil Pengujian

Pengujian tetap menggunakan aplikasi *Packet Tracer 7.0* dengan melakukan *tracing* dari kedua sisi LAN yakni LAN Kampus A dan LAN Kampus B.

Berikut hasil pengujiannya:

Pengujian dari PC A Ke Router Internet

PC>tracert 10.0.0.2

Tracing route to 10.0.0.2 over a maximum of 30 hops:

```

1  1 ms  0 ms  0 ms  172.16.0.1
2  0 ms  1 ms  0 ms  10.0.0.2

```

Trace complete.

Pengujian berhasil dimana akses ke Router Internet melalui Gateway Router Kampus A dengan IP Address 172.16.0.1.

Pengujian dari PC B Ke Router Internet

PC>tracert 11.0.0.2

Tracing route to 11.0.0.2 over a maximum of 30 hops:

1	0 ms	0 ms	0 ms	172.16.4.1
2	0 ms	1 ms	0 ms	11.0.0.2

Trace complete.

Pengujian berhasil dimana akses ke Router Internet melalui Gateway Router Kampus B dengan IP Address 172.16.4.1.

Pengujian dari PC A Ke PC B

PC>tracert 172.16.4.2

Tracing route to 172.16.4.2 over a maximum of 30 hops:

1	0 ms	0 ms	0 ms	172.16.0.1
2	2 ms	2 ms	2 ms	192.168.0.2
3	2 ms	1 ms	2 ms	172.16.4.2

Trace complete.

Pengujian berhasil dimana akses dari PC A ke PC B melalui VPN Tunnel dengan IP Penghubung 192.168.0.2.

Pengujian dari PC B ke PC A

PC>tracert 172.16.0.2

Tracing route to 172.16.0.2 over a maximum of 30 hops:

1	0 ms	0 ms	0 ms	172.16.4.1
2	2 ms	2 ms	2 ms	192.168.0.1
3	2 ms	2 ms	1 ms	172.16.0.2

Trace complete.

Pengujian berhasil dimana akses dari PC B ke PC A melalui VPN Tunnel dengan IP Penghubung 192.168.0.1.

Pengujian dari PC B ke Server Kampus A

PC>tracert 172.16.8.2

Tracing route to 172.16.8.2 over a maximum of 30 hops:

1	0 ms	0 ms	0 ms	172.16.4.1
2	2 ms	2 ms	2 ms	192.168.0.1
3	2 ms	1 ms	2 ms	172.16.8.2

Trace complete.

4. Kesimpulan

Setelah melakukan serangkaian pengujian diatas, maka dapat disimpulkan bahwa konfigurasi VPN Tunneling dengan menggunakan protocol IPIP dapat menghubungkan 2(dua) jaringan Lan melalui Jaringan Publik, Lokal server dapat diakses private melalui jalur tunnel. Hal ini bermanfaat dalam efisiensi belanja internet karena dapat menjalankan 2(dua) koneksi LAN dan Internet sekaligus hanya dengan berlangganan internet saja dengan IP Publik statis.

Referensi

- Charlie Schluting. 2006. Networking 101: Understanding Multicast Routing. Enterp. Netw. Planet.
- Pratama IPAE. 2015. Handbook Jaringan Komputer. 762 p.
- Supriyono H, Widhaya JA, Supardi A. 2013. Penerapan Jaringan VPN Untuk Keamanan Komunikasi Data Bagi PT. Mega Tirta Alami. Jarkom 16: 88–101.
- Tanenbaum AS. 2003. Computer Networks. World Wide Web Internet Web Inf. Syst. 52: 349–351.