Available *online*at : http://bit.ly/InfoTekJar

InfoTekJar :Jurnal Nasional InformatikadanTeknologiJaringan

ISSN (Print) 2540-7597|ISSN (Online) 2540-7600

Desain *Virtual Private Network* (VPN) Berbasis *Open Shortest Path First* (OSPF)

Hari Antoni Musril

Program Studi Pendidikan Teknik Informatika dan Komputer Institut Agama Islam Negeri (IAIN) Bukittinggi, Kampus II IAIN Bukittinggi Jl. Gurun Aur Kubang Putih Kab. Agam, 26181, Sumatera Barat, Indonesia

KEYWORDS

VPN, OSPF, AAA server, router

CORRESPONDENCE

Phone: +628126769772

E-mail: kum_ayik@yahoo.co.id

A B S T R A C T

Access to a local network that is limited to certain parties can be done from public networks by utilizing Virtual Private Network (VPN). Access is done through the internet by utilizing VPN. This allows users to utilize all local network resources that can be accessed without limitation of time and location. OSPF routing is needed to connect all routers in the network that using VPN. OSPF routing on VPN networks can connect several buildings to different locations with one network. This research produces a network scheme prototype that connects two locations separated by long distances, but can be connected both real and virtually.

ABSTRAK

Akses terhadap sebuah jaringan lokal yang bersifat terbatas untuk pihak tertentu dapat dilakukan dari jaringan publik dengan memanfaatkan *Virtual Private Network* (VPN). Akses tersebut dilakukan melalui internet dengan memanfaatkan VPN. Hal itu membuat pengguna bisa memanfaatkan semua *resources* jaringan lokal yang dapat diakses tanpa batasan waktu dan lokasi. OSPF *routing* diperlukan untuk menghubungkan semua *router* dalam jaringan yang menggunakan VPN. OSPF routing pada jaringan VPN bisa saling mengkoneksikan beberapa gedung di lokasi yang berbeda dengan satu jaringan. Penelitian ini menghasilkan prototipe skema jaringan yang menghubungkan dua lokasi yang dipisahkan oleh jarak yang jauh, namun dapat terhubung baik secara nyata maupun secara virtual.

PENDAHULUAN

Jaringan komputer adalah himpunan "interkoneksi" antara dua komputer *autonomous* atau lebih yang terhubung dengan media transmisi kabel atau tanpa kabel [1]. Jaringan komputer mampu menghubungkan berbagai perangkat (*device*) baik yang diam (*static*) maupun yang bergerak (*mobile*) seperti *smartphone*. Salah satu perkembanagan jaringan komputer adalah teknologi internet, yang mendukung proses komunikasi dan transmisi data secara *real time*. Sehingga dengan internet hilanglah pembatas informasi dari segi ruang dan waktu. Internet sebagai jaringan publik dapat memberikan akses informasi dengan cepat dan mudah, sehingga setiap *user* dimanapun berada dan kapanpun waktunya dapat mengakses informasi baik milik pribadi, swasta, maupun pemerintah. Kemudahan tersebut harus diikuti dengan kemampuan untuk tetap menjaga keamanan informasi. Akses dalam sebuah jaringan komputer harus diawasi dan dibatasi [2].

VPN adalah sebuah teknologi komunikasi yang memungkinkan dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal [3]. Koneksi VPN dalam bentuk *virtual* (maya) dan bersifat *private* (rahasia), sehingga hanya *user* tertentu saja yang bisa mengaksesnya. VPN sangat dibutuhkan bagi suatu organisasi baik swasta (organisasai bisnis) maupun pemerintah yang memiliki unit dan cakupan wilayah kerja yang luas serta jumlah *user* yang banyak. *User* yang terhubung ke dalam jaringan VPN perlu akun dan sandi untuk *login*.

VPN diaplikasikan pada jaringan yang memiliki banyak *router*. Komunikasinya diatur oleh protokol *routing*. *Routing* adalah proses memilih lintasan yang akan ditempuh oleh sebuah paket data pada suatu jaringan komputer [4]. [5] OSPF adalah suatu protokol routing Link State (LS) yang bersifat terbuka atau didukung berbagai perangkat jaringan. OSPF dapat digunakan untuk menentukan jalur terbaik dalam pengiriman paket data di dalam jaringan skala besar.

Penelitian ini membuat jaringan VPN yang berjalan dalam protokol *routing* OSPF. Skema jaringan yang digunakan mengacu pada prototipe jaringan di area kampus yang memiliki dua buah lokasi berbeda. Perancangan dan konfigurasi memanfaatkan software Cisco Packet Tracer. Hasil prototipe ini bisa diterapkan dalam kondisi sebenarnya.

DOI: https://doi.org/10.30743/infotekjar.v3i2.1055

LANDASAN TEORI

Virtual Private Network (VPN)

Menurut *Internet Engineering Task Force* (IETF) [6], VPN merupakan suatu bentuk *private* internet yang melalui *public network* (internet), dengan menekankan pada keamanan data dan akses global melalui internet. Prosedur enkripsi dilakukan terhadap data yang melalui VPN, sehingga keamanannya terjamin.

Prinsip Kerja VPN [7] :
- Komponen utamanya adalah VPN *server*.
- VPN *Client* akan mengirim pesan ke *server* VPN.
- Untuk proses *login*, VPN *server* memeriksa akun *client*.
- Komputer *client* dapat digunakan mengakses berbagai *resource* di VPN *server*.

Jenis VPN berdasarkan aksesnya yaitu [8] :
- *Remote Access*,
- dan *Site to Site*.

Manfaat jaringan VPN yaitu [7] :
- Untuk *remote access*,
- dan Menghemat keuangan.

AAA *Server*

Protokol AAA (*Authentication, Authorization, Accounting*) sebagai pengatur komunikasi antara *client* dengan domain yang sama, maupun antar *client* dengan domain yang berbeda [9]. Autentikasi merupakan tahapan mengenali siapa yang akan *login*. Otorisasi mengizinkan pengguna mengakses sumber daya sistem. *Accounting* merupakan proses pencatatan seluruh sumber daya yang digunakan dan besaran biayanya [10].

Open Shortest Path First (OSPF)

OSPF bekerja dengan landasan perutean hierarkis dengan membagi beberapa tingkatan jaringan. Tingkatan itu diaplikasikan dengan sistem pengelompokan area. Dengan menggunakan konsep perutean hierarki ini sistem penyebaran informasi dalam protokol OSPF menjadi lebih teratur dan tersegmentasi, sehingga tidak menyebar secara sembarangan [5].

METODE PENELITIAN

Pada tulisan ini metode penelitian yang digunakan adalah sebagai berikut :
1. Analisis. Berupa kegiatan kajian literatur. Literatur bersumber dari buku, jurnal ilmiah, dan penelitian yang membahas mengenai *Virtual Provate Network (VPN)* dan *Open Shortest Path First* (OSPF).
2. Desain. Di sini dilakukan proses perancangan topologi. Merancang jarinan fisik dan logika.
3. Pengembangan. Tahapan untuk konfigurasi prototipe. Alat yang diatur sesuai dengan topologi, antara lain router, PC, dan server.
4. Pengujian. Setelah prototipe jaringan selesai dikembangkan, setiap *device* dilakukan pengujian konektivitasnya dan pengujian VPN.

HASIL DAN PEMBAHASAN

Skema Jaringan

Skema jaringan pada desain *Virtual Private Network* (VPN) berbasis *Open Shortest Path First* (OSPF) seperti gambar berikut.

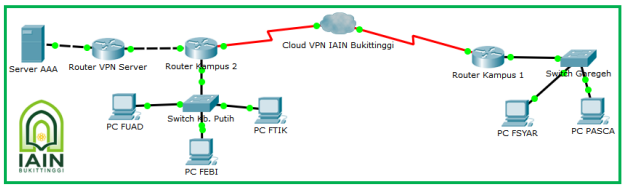

Figure 1. Skema jaringan untuk penelitian

Pengaturan OSPF dilakukan pada *router* VPN server, *router* Kampus 1, dan *router* kampus 2. Server AAA merupakan server yang digunakan untuk mengakses jaringan VPN. *Cloud* VPN IAIN Bukittinggi menjadi penghubung jaringan antara Kampus 1 dan Kampus 2. Tabel berikut ini adalah informasi mengenai alamat pada *port* aktif di masing-masing *router*.

Table 1. Konfigurasi Alamat Router

Router	Port : IP Address / Prefix		Clock Rate
VPN Server	Fa0/0	: 7.6.4.2/ 24	-
	Fa0/1	: 184.75.66.1 /24	-
Kampus I	Fa0/0	: 10.7.6.1 /24	-
	Se3/0	: -	56000
	Se3/0.101	: 35.18.40.1 /24	-
Kampus II	Fa1/0	: 192.168.1.1 /24	-
	Fa0/0	: 7.6.4.1 /24	-
	Se2/0	: 35.18.40.2 /24	56000

Konfigurasi *Router*

Pengaturan pada masing-masing *router* dilakukan melalui jendela CLI. Berikut ini merupakan konfigurasi di setiap *router*.

1. Konfigurasi di Router VPN Server : Konfigurasinya seperti berikut :

```
Router>enable
Router#configure terminal
Router(config)#hostname Router-VPN_Server
Router-VPN_Server(config)#aaa new-model
Router-VPN_Server(config)#aaa authentication login
VPNAUTH group radius local
Router-VPN_Server(config)#aaa authorization network
VPNAUTH local
Router-VPN_Server(config)#crypto isakmp policy 10
Router-VPN_Server(config-isakmp)#encr aes 256
Router-VPN_Server(config-isakmp)#authentication pre-
share
Router-VPN_Server(config-isakmp)#group 2
Router-VPN_Server(config-isakmp)#exit

Router-VPN_Server(config)#crypto isakmp client
configuration group myciscogroup
Router-VPN_Server(config-isakmp-group)#key
myciscogroup
Router-VPN_Server(config-isakmp-group)#pool
VPNCLIENTS
Router-VPN_Server(config-isakmp-group)#netmask
255.255.255.0
Router-VPN_Server(config-isakmp-group)#exit
```


DOI: https://doi.org/10.30743/infotekjar.v3i2.1055

Router-VPN_Server(config)#crypto ipsec transform-set 6 esp-3des esp-sha-hmac
Router-VPN_Server(config)#crypto dynamic-map mymap 10
Router-VPN_Server(config-crypto-map)#set transform-set 6
Router-VPN_Server(config-crypto-map)#reverse-route
Router-VPN_Server(config-crypto-map)#exit

Router-VPN_Server(config)#crypto map mymap client authentication list VPNAUTH
Router-VPN_Server(config)#crypto map mymap isakmp authorization list VPNAUTH
Router-VPN_Server(config)#crypto map mymap client configuration address respond
Router-VPN_Server(config)#crypto map mymap 10 ipsec-isakmp dynamic mymap

Router-VPN_Server(config)#ip ssh version 1
Router-VPN_Server(config)#spanning-tree mode pvst

Router-VPN_Server(config)#interface FastEthernet0/0
Router-VPN_Server(config-if)#ip address 7.6.4.2 255.255.255.0
Router-VPN_Server(config-if)#crypto map mymap
Router-VPN_Server(config-if)#no shutdown
Router-VPN_Server(config-if)#ip local pool VPNCLIENTS 201.1.100.100 201.1.100.150
Router-VPN_Server(config-if)#exit

Router-VPN_Server(config)#interface FastEthernet0/1
Router-VPN_Server(config-if)#ip address 184.75.66.1 255.255.255.0
Router-VPN_Server(config-if)#no shutdown
Router-VPN_Server(config-if)#exit

Router-VPN_Server(config)#ip route 201.1.100.0 255.255.255.0 7.6.4.1
Router-VPN_Server(config)#radius-server host 184.75.66.100 auth-port 1645 key myciscovpn

Router-VPN_Server(config)#router ospf 1
Router-VPN_Server(config-router)#network 7.6.4.0 0.0.0.255 area 0
Router-VPN_Server(config-router)#network 184.75.66.0 0.0.0.255 area 0
Router-VPN_Server(config-router)#exit

Router-VPN_Server(config)#exit
Router-VPN_Server#write memory

2. Konfigurasi di *Router* Kampus 1 : Pada *router* Kampus 1 konfigurasinya seperti berikut ini :
Router>enable
Router#configure terminal
Router(config)#hostname Router-KAMPUS_1
Router-KAMPUS_1(config)#ip ssh version 1
Router-KAMPUS_1(config)#spanning-tree mode pvst
Router-KAMPUS_1(config)#interface FastEthernet0/0
Router-KAMPUS_1(config-if)#ip address 10.7.6.1 255.255.255.0
Router-KAMPUS_1(config-if)#no shutdown
Router-KAMPUS_1(config-if)#exit

Router-KAMPUS_1(config)#interface se3/0
Router-KAMPUS_1(config-if)#encapsulation frame-relay ietf
Router-KAMPUS_1(config-if)#frame-relay LMI-type ansi
Router-KAMPUS_1(config-if)#clock rate 56000
Router-KAMPUS_1(config-if)#no shutdown
Router-KAMPUS_1(config-if)#exit

Router-KAMPUS_1(config)#interface se3/0.101 point-to-point
Router-KAMPUS_1(config-subif)#ip address 35.18.40.1 255.255.255.0
Router-KAMPUS_1(config-subif)#frame-relay interface-dlci 101
Router-KAMPUS_1(config-subif)#ip ospf network broadcast
Router-KAMPUS_1(config-subif)#no shutdown
Router-KAMPUS_1(config-subif)#exit

Router-KAMPUS_1(config)#router ospf 1
Router-KAMPUS_1(config-router)#network 35.18.40.0 0.0.0.255 area 0
Router-KAMPUS_1(config-router)#network 10.7.6.0 0.0.0.255 area 0
Router-KAMPUS_1(config-subif)#exit
1) Konfigurasi di Router Kampus 2 : Pada *router* Kampus 2 konfigurasinya seperti berikut ini :
Router>enable
Router#configure terminal
Router(config)#hostname Router-KAMPUS_2
Router-KAMPUS_2(config)#ip ssh version 1
Router-KAMPUS_2(config)#spanning-tree mode pvst
Router-KAMPUS_2(config)#interface FastEthernet1/0
Router-KAMPUS_2(config-if)#ip address 192.168.1.1 255.255.255.0
Router-KAMPUS_2(config-if)#no shutdown
Router-KAMPUS_2(config-if)#exit

Router-KAMPUS_2(config)#interface FastEthernet0/0
Router-KAMPUS_2(config-if)#ip address 7.6.4.1 255.255.255.0
Router-KAMPUS_2(config-if)#no shutdown
Router-KAMPUS_2(config-if)#exit

Router-KAMPUS_2(config)#interface se2/0
Router-KAMPUS_2(config-if)#encapsulation frame-relay ietf
Router-KAMPUS_2(config-if)#frame-relay LMI-type ansi
Router-KAMPUS_2(config-if)#clock rate 56000
Router-KAMPUS_2(config-if)#no shutdown
Router-KAMPUS_2(config-if)#exit

Router-KAMPUS_2(config)#interface se2/0 point-to-point
Router-KAMPUS_2(config-subif)#ip address 35.18.40.2 255.255.255.0
Router-KAMPUS_2(config-subif)#frame-relay interface-dlci 101
Router-KAMPUS_2(config-subif)#ip ospf network broadcast
Router-KAMPUS_2(config-subif)#no shutdown
Router-KAMPUS_2(config-subif)#exit

Router-KAMPUS_2(config)#router ospf 1
Router-KAMPUS_2(config-router)#network 35.18.40.0 0.0.0.255 area 0
Router-KAMPUS_2(config-router)#network 7.6.4.0 0.0.0.255 area 0
Router-KAMPUS_2(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router-KAMPUS_2(config-subif)#exit

3. Pengaturan *Cloud* VPN
Port Se1 pada *cloud* VPN IAIN Bukittinggi dihubungkan ke *router* Kampus 1, dan *port* Se0 nya dihubungkan ke *router* Kampus 2. Setelah itu dilakukan konfigurasi perangkat *frame relay* pada *cloud* VPN IAIN Bukittinggi tersebut. Seperti gambar berikut ini.

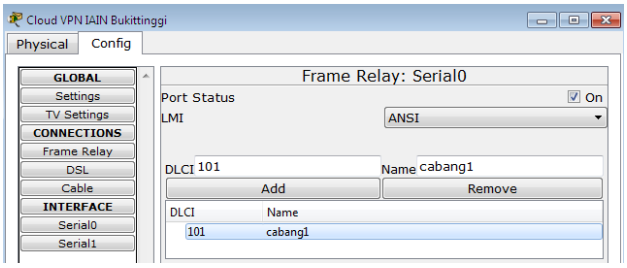

Figure 2. Konfigurasi serial0 di cloud VPN IAIN Bukittinggi

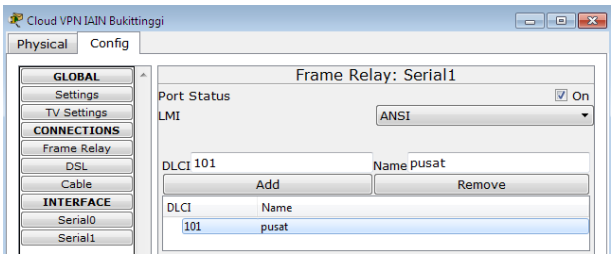

Figure 3. Konfigurasi serial1 di *cloud* VPN IAIN Bukittinggi

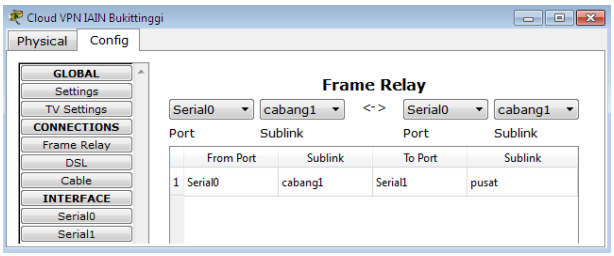

Figure 4. Konfigurasi *frame relay* di *cloud* VPN IAIN Bukittinggi

Konfigurasi *Server* AAA

Tahapan berikutnya adalah pengaturan pada *server* AAA. *Server* AAA akan melakukan proses autentikasi, otorisasi, dan akunting. AAA akan mengatur akses ke komputer dengan memeriksa *user* yang ingin tersambung. Berikut ini konfigurasi pada *server* AAA.

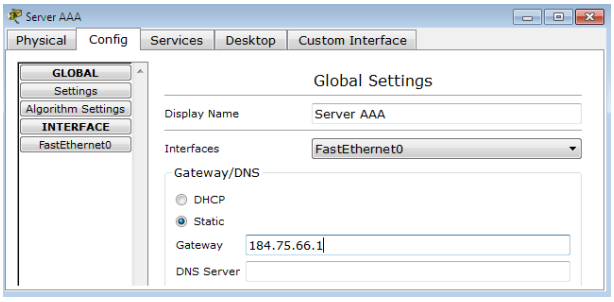

Figure 5. Konfigurasi *display name* dan IP *address server* AAA

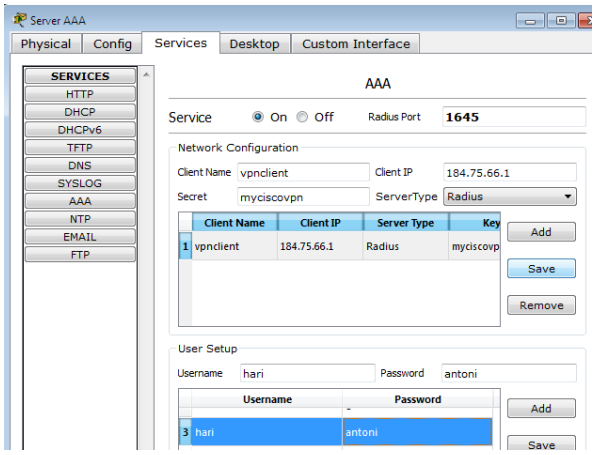

Figure 6. Konfigurasi *network* dan *username* di *server* AAA

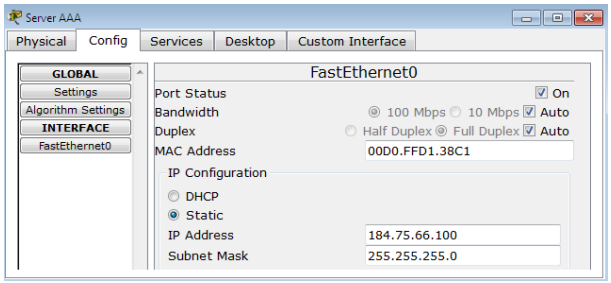

Figure 7. Konfigurasi alamat IP *server* AAA

Koneksi ke VPN *Server*

Setelah selesai melakukan semua konfigurasi, berikutnya adalah tahapan untuk menghubungkan komputer *client* ke jaringan VPN yang bekerja dalam *routing* OSPF. Gambar berikut ini merupakan tahapan koneksi pc FSYAR ke jaringan VPN.

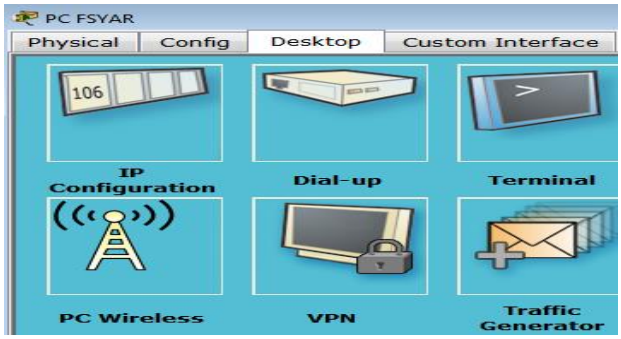

Figure 8. Proses awal koneksi VPN pada PC FSYAR

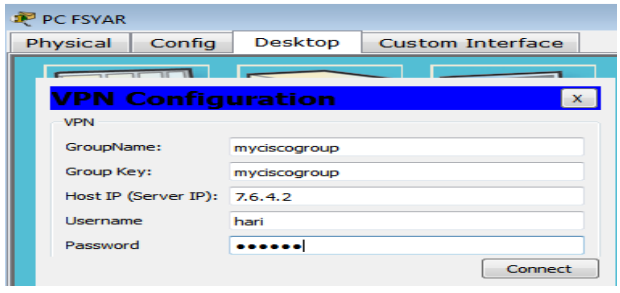

Figure 9. Proses *login* VPN ke *server* AAA dari PC FSYAR

DOI: https://doi.org/10.30743/infotekjar.v3i2.1055

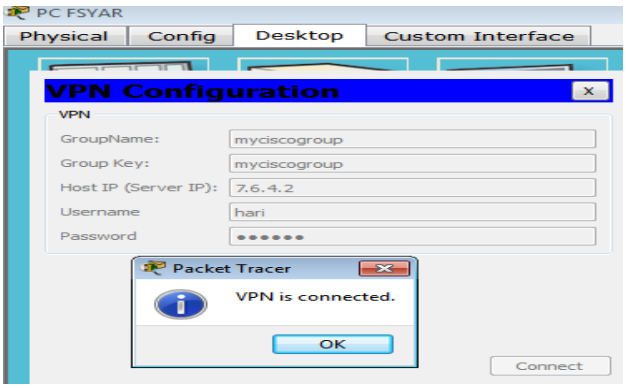

Figure 10. Proses *login* ke VPN berhasil

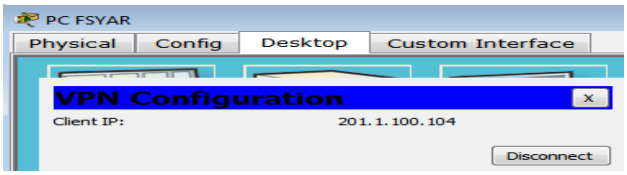

Figure 11. Alamat PC FSYAR pada saat *login* ke VPN

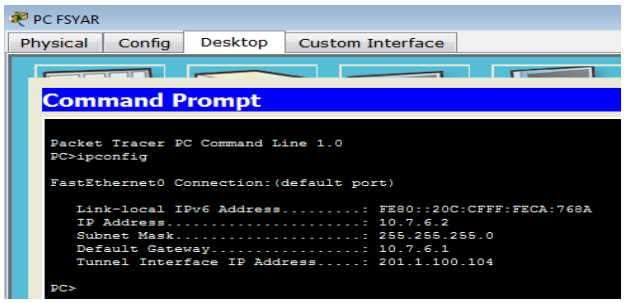

Figure 12. Informasi alamat IP pada PC FSYAR

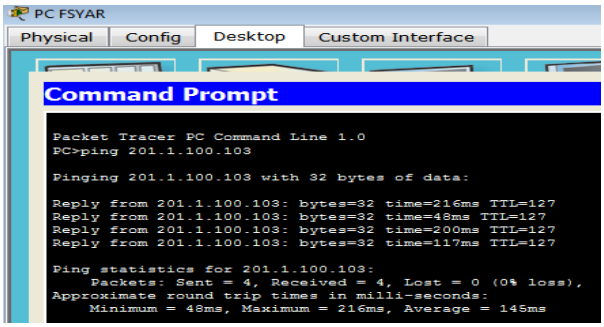

Figure 13. Uji koneksi ke komputer lain dalam jaringan VPN

Hasil Simulasi

Hasil desain VPN berbasis OSPF ini antara lain adalah :

1. Tabel *Routing:* diketahui dengan menulis perintah *show ip route ospf* pada setiap *router*. Berikut ini adalah hasilnya pada *router* kampus 2.

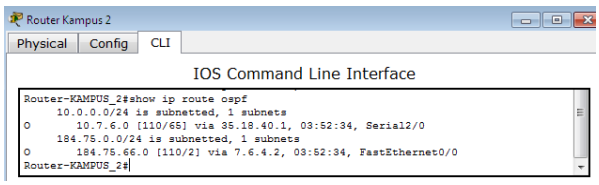

Figure 14. Tabel *routing* OSPF di *router* kampus 2

2. Tabel *Neighbor:* memuat informasi *router neighbor*. Gambar di bawah ini adalah tabel *neighbor* protokol OSPF di Kampus 2.

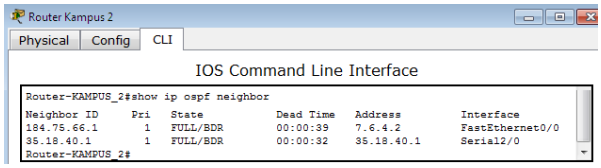

Figure 15. Tabel *neighbor* di *router* kampus 2

3. *Database Routing* : Untuk melihat database *routing* OSPF pada *router* menggunakan perintah *show ip ospf database*. *Router* kampus 2 memiliki database *routing* seperti berikut.

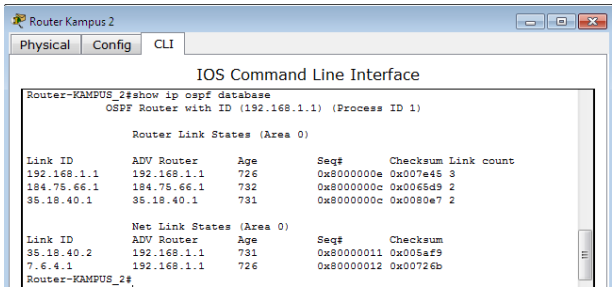

Figure 16. Database *Routing* OSPF di *Router* Kampus 2

4. Pengaturan IP *Protocol* : Untuk melihat pengaturan IP protokol dengan menggunakan perintah *do show ip protocol*. Gambar 17 di bawah adalah IP protokol di *router* Kampus 2.

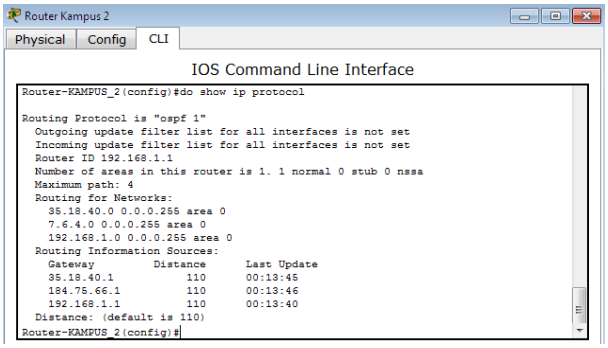

Figure 17. IP *Protocol* di *Router* Kampus 2

5. *Koneksi ke VPN* : Koneksi ke VPN dilakukan oleh PC user dengan mengambil menu VPN (lihat *gambar* 8). Kemudian input data *group name*, *group key*, server IP, *username*, dan *password* seperti terlihat pada *gambar* 9. Apabila ada data yang salah maka PC user tidak akan bisa untuk masuk ke VPN. *gambar* 10 merupakan PC user yang berhasil masuk ke VPN. Setelah PC user terhubung ke VPN maka PC tersebut akan mendapatkan *tunnel interface* IP *address* seperti nampak pada *gambar* 12. Setelah sebuah PC terhubung ke VPN maka PC tersebut dapat melakukan komunikasi dengan PC lain yang juga sudah terhubung ke VPN, seperti terlihat pada *gambar* 13. PC yang sedang terhubung dalam jaringan VPN tidak akan bisa mengakses alamat fisik dari PC lain.

KESIMPULAN

Kesimpulan yang dapat diambil adalah sebagai berikut :

1. VPN dapat membuat akses data dan informasi ke jaringan menjadi lebih aman karena adanya mekanisme *tunnel* VPN yang melakukan enkapsulasi dan enkripsi terhadap data dalam jaringan.
2. Adanya *username* dan *password* user pada saat login ke VPN akan memudahkan proses monitoring terhadap user.
3. Pemanfaatan jaringan publik (internet) untuk menerapkan VPN dapat menghemat anggaran, karena tidak dibutuhkan infrastruktur tambahan untuk implementasinya.
4. Secara keseluruhan jaringan VPN yang berjalan dalam *routing* OSPF mampu bekerja dengan baik, dimana terdapat beberapa *network* yang berbeda namun dapat saling terhubung dalam jaringan *private*.
5. *Routing* OSPF dapat menghubungkan semua perangkat dalam skema jaringan yang dirancang baik dalam kondisi sebenarnya maupun dalam kondisi *virtual* (maya).

REFERENSI

[1] H. A. Musril, "Simulasi Interkoneksi Antara Autonomous System (AS) Menggunakan Border Gateway Protocol (BGP)," *Jurnal Nasional Informatika dan Teknologi Jaringan (InfoTekJar)*, vol. 2, no. 1, pp. 1-9, 2017.

[2] H. A. Musril, "Extended Access List untuk Mengendalikan Trafik Jaringan," *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, vol. 2, no. 2, pp. 129-135, 2016.

[3] P. Oktivasari, and A. B. Utomo, "Analisa Virtual Private Network Menggunakan OpenVPN dan Point To Point Tunneling Protocol," *Jurnal Penelitian Komunikasi dan Opini Publik*, vol. 20, no. 2, pp. 185-202, 2016.

[4] H. A. Musril, "Simulasi Interkoneksi Antara Autonomous System (AS) Menggunakan Border Gateway Protocol (BGP)" *Jurnal Nasional Informatika dan Teknologi Jaringan (InfoTekjar)*, vol. 2, no. 1, pp. 1-9, 2017.

[5] H. A. Musril, "Penerapan Open Shortest Path First (OSPF) untuk Menentukan Jalur Terbaik dalam Jaringan," *Jurnal Elektro Telekomunikasi Terapan (JETT)*, vol. 4, no. 1, pp. 421-431, 2017.

[6] T. Mulyadin, M. Sholeh, and C. Iswahyudi, "Implementasi Routing Open Shortest Path First (OSPF) Melalui Tunnel Open VPN," *Jurnal JARKOM*, vol. 4, no. 1, pp. 62-70, 2016.

[7] T. D. Purwanto, "Perancangan Jaringan VPN Router Dengan Metode Link State Routing Protocols," *Seminar Nasional Inovasi dan Tren (SNIT)*, pp. A69-A74, 2014.

[8] C. Umam, E. Roza, and Irfan, "Perancangan Jaringan Keamanan Virtual Private Network (VPN) Site to Site," *Seminar Nasional TEKNOKA FT UHAMKA*, pp. 23-30, 2016.

[9] A. Masykuri, E. Utami, and Sudarmawan, "Implementasi VPN Server dalam Sistem Informasi Apotek (Studi Kasus Integrasi Sistem Informasi Apotek Santi Pontianak), "*Jurnal Ilmiah DASI*, vol. 17, no. 2, pp. 7-12, 2016.

[10] Y. Syafitri, "Mengamankan Pengiriman Data Dari Malware Berbasis VPN Menggunakan Router Cisco di Kampus DCC," *Jurnal Cendikia*, vol. 10, no. 1, pp. 10-14, 2014.

BIOGRAFI PENULIS

Hari Antoni Musril

Lahir di Padang, 7 September 1983. Menyelesaikan program S1 Sarjana Komputer (S.Kom) pada jurusan Sistem Komputer Universitas Putra Indonesia "YPTK" Padang tahun 2007. Menyelesaikan program S2 Magister Komputer (M.Kom) pada Universitas Putra Indonesia "YPTK" Padang tahun 2009. Saat ini sebagai dosen tetap pada program studi Pendidikan Teknik Informatika dan Komputer, yang berada dalam Fakultas Tarbiyah dan Ilmu Keguruan di Institut Agama Islam Negeri (IAIN) Bukittinggi.

DOI: https://doi.org/10.30743/infotekjar.v3i2.1055