

# 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

# ABSTRACT

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.

## 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

		0	-
Router	Port : IP	Address / Prefix	Clock Rate
VPN Server	Fa0/0	: 7.6.4.2/24	-
	Fa0/1	: 184.75.66.1 /24	-
	Fa0/0	: 10.7.6.1 /24	-
Kampus I	Se3/0	:-	56000
	Se3/0.10	1 : 35.18.40.1 /24	-
	Fa1/0	: 192.168.1.1 /24	-
Kampus II	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 preshare 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

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)#reverse-route

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 ipsecisakmp 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* 

 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-topoint 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)#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)#no shutdown

Router-KAMPUS\_2(config)#router ospf 1Router-KAMPUS\_2(config-router)#network35.18.40.00.0.0.255 area 07.6.4.0Router-KAMPUS\_2(config-router)#network7.6.4.00.0.0.255 area 0192.168.1.0Router-KAMPUS\_2(config-router)#network192.168.1.00.0.0.255 area 0Router-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

a						
4	Cloud VPN IAIN Bukitt	ing	igi			
	Physical Config					
ſ_		_				
	GLOBAL	^		Frame Re	elay: Serial1	
	Settings		Port Status			🗹 On
	TV Settings		LMI		ANSI	-
	CONNECTIONS					
	Frame Relay					
	DSL		DLCI 101		Name pusat	
	Cable			Add	Remove	
	INTERFACE		DLCI	Name	<u>^</u>	]
	Serial0		101	pusat		
	Serial1		101	pusu		

Figure 3. Konfigurasi serial1 di cloud VPN IAIN Bukittinggi

P Cloud VPN IAIN Bukit	tinggi					
Physical Config						
GLOBAL Settings TV Settings CONNECTIONS Frame Relay	*	Po	erial0 ▼ Ca rt Su	Frame abang1 • <	e Relay <-> Serial0 Port	▼ cabang1 ▼ Sublink
DSL			From Port	Sublink	To Port	Sublink
Cable		1	Serial0	cabang1	Serial1	pusat
Serial0 Serial1						

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.

💐 Server AAA		- • •
Physical Config	Services Desktop Custom Interface	
GLOBAL ^	Global Settings	
Algorithm Settings	Display Name Server AAA	
FastEthernet0	Interfaces FastEthernet0	•
	Gateway/DNS	
	O DHCP	
	<ul> <li>Static</li> </ul>	
	Gateway 184.75.66.1	
	DNS Server	

Figure 5. Konfigurasi display name dan IP address server AAA

SERVICES       AAA         DHCP       Service       On       Off       Radus Port       1645         DHCPv6       Network       Configuration       Clent IP       184.75.66.1         SYSLOG       AAA       Servertype       Radius         NTP       EMAIL       Clent Name       Clent IP       ServerType       Key         PTP       User Setup       User Setup       Server Type       Key       A         User Setup       Username       Password       antoni       A	Physical	Config	Servi	ces	Desktop	Custom	Interface		
DHCP     Service     On     Off     Radus Port     1645       DHCPv6     Network     Configuration       DNS     Client Name     vpnclient     Client IP     184.75.66.1       SYSLOG     Servet     myciscovpn     ServerType     Key       AAA     A     Servet     Invision     Servet Type     Key       MTP     Client Name     Client IP     Server Type     Key       EMAIL     1     vpnclient     184.75.66.1     Radius     Myciscorp       FTP     User Setup     Username     Password     antoni	SERV	ICES	A				AAA		
TFTP     Network Configuration       DNS     Clent Name vpnclient       SYSLOG     Servet myciscovpn       NTP     Ediant Name       EMAIL     Client Name       FTP     Client Name       User Setup     Servet myciscovp       User Setup     Usermame       Usermame     Password       Antic     Password	DH	CP Pv6	Ser	vice	٥ (	n 🔘 Off	Radius Port	1645	
DNS         SYSLOG         AAA         NTP         EMAIL         FTP         User Setup         User Setup         User Setup         User Maria         Password         Antoni         Usermame         Password         Antoni	TF	TP	C N	etwork	Configura	tion			
SISLUG AAA NTP EMAIL FTP User Setup User Setup User Setup User Setup User Setup User Setup User Setup User Setup User Antoni User Antoni AAA	DN	IS	d	ient Nar	vpnclie	nt	Client IP	184.75.66.	1
NTP     Client Name     Client IP     Server Type     Key       EMAIL     I     vpndient     184.75.66.1     Radius     mydiscorp       FTP     User Setup     S       User Setup     Username     Password     antoni       Username     Password     A	AA	A	Se	ecret	mycisco	ovpn	ServerType	Radius	
EMAIL FTP User Setup User Setup Usermame hari Vsermame Password Antoni	ТИ	rp )		Clie	nt Name	Client IP	Server Type	Key	
User Setup User Setup Usermane hari Password antoni	EM4		1	vpncli	ent	184.75.66.1	Radius	myciscovp	Add
User Setup User Setup Username hari Password antoni Username Password A		<u> </u>							Save
User Setup Username hari Password antoni Username Password A									Remove
Username hari Password antoni Username Password A			-U	ser Set	up				
Username Password A			Us	sername	hari		Password	antoni	
					Userna	me -	Passwor	d	Add
3 hari antoni			3	hari		ai	ntoni		

Figure 6. Konfigurasi network dan username di server AAA

🐙 Server AAA	4				
Physical	Config	Services	Desktop	Custom Interface	9
GLO	BAL			FastEtherne	t0
Setti	ngs	Port Stat	us		🗹 On
Algorithm Settings		Bandwidt	n	10	0 Mbps 🗇 10 Mbps 🗹 Auto
INTER	INTERFACE			🔿 Half Duplex 🖲 Full Duplex 🗹 Auto	
FastEthe	ernet0	MAC Add	ess	00D0.FFD1.38C1	
		IP Conf	iguration		
		O DHC			
		Stat	Static		
		IP Addr	ess	184.75.66.100	
		Subnet	Mask	255.2	55.255.0
1					,

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

🔊 PC FSYAR		
Physical Config	Desktop	Custom Interface
VPN Config	uration	x
VPN		
GroupName:	myciscogroup	
Group Key:	myciscogroup	
Host IP (Server IP):	7.6.4.2	
Username	hari	
Password	•••••	
		Connect

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



Figure 10. Proses login ke VPN berhasil

🐙 Ро	C FSYAR			
Phy	vsical	Config	Desktop	Custom Interface
	VPN (	Configu	uration	x
C	lient IP:		201	1.100.104
				Disconnect
F	igure 11	. Alamat F	PC FSYAR pa	da saat <i>login</i> ke VPN



Figure 12. Informasi alamat IP pada PC FSYAR

R PC FSYAR
Physical Config Desktop Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0 PC>ping 201.1.100.103
Pinging 201.1.100.103 with 32 bytes of data:
Reply from 201.1.100.103: bytes=32 time=216ms TTL=127 Reply from 201.1.100.103: bytes=32 time=49ms TTL=127 Reply from 201.1.100.103: bytes=32 time=20ms TTL=127 Reply from 201.1.100.103: bytes=32 time=117ms TTL=127
<pre>Ping statistics for 201.1.100.103:</pre>

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.

Router Kampus 2	- • •
Physical Config CLI	
IOS Command Line Interface	
Router-KAMPUS_2%show ip route ospf 10.0.0.0/24 is subnetted, 1 subnets 0 10.7.6.0 [110/65] via 35.18.40.1, 03:52:34, Serial2/0 184.75.0.0/24 is subnetted, 1 subnets	E
0 184.75.66.0 [110/2] via 7.6.4.2, 03:52:34, FastEthernet0/0 Router-KAMPUS_2#	-

Figure 14. Tabel routing OSPF di router kampus 2

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

Router Kampus 2					
Physical Con	ifig C	U			
		IOS Co	mmand Lino	Intorfaco	
Router-KAMPUS	2#show	in canf neigh		Interface	
Router-KAMPUS Neighbor ID	2‡show Pri	ip ospf neigh State	bor Dead Time	Address	Interface
Router-KAMPUS Neighbor ID 184.75.66.1	_2#show Pri 1	ip ospf neigh State FULL/BDR	bor Dead Time 00:00:39	Address 7.6.4.2	Interface FastEthernet0/0
Router-KAMPUS Neighbor ID 184.75.66.1 35.18.40.1	2#show Pri 1 1	ip ospf neigh State FULL/BDR FULL/BDR	bor Dead Time 00:00:39 00:00:32	Address 7.6.4.2 35.18.40.1	Interface FastEthernet0/0 Serial2/0

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.

						×
Physical C	Config CLI					
		IOS Comm	and Line Inter	face		
Router-KAMP	US_2#show ip	ospf database	68 1 1) (Process	TD 1)		
	0077 104041		00.11.1) (21000222	10 17		
	Router I	ink States (Ar	ea ()			
Link ID	ADV Rout	er Age	Seq#	Checksum Link	count	
192.168.1.1	192.168.	1.1 726	0x8000000e	0x007e45 3		
184.75.66.1	184.75.6	6.1 732	0x8000000c	0x0065d9 2		
35.18.40.1	35.18.40	.1 731	0x800000c	0x0080e7 2		
	Net Link	States (Area	0)			_
Link ID	ADV Rout	er Age	Seq#	Checksum		
35.18.40.2	192.168.	1.1 731	0x80000011	0x005af9		=
7.6.4.1	192.168.	1.1 726	0x80000012	0x00726b		
Router-KAMP	US_2#					

Figure 16. Database Routing OSPF di Router Kampus 2

 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.

🤻 Router Ka	mpus 2				- • •
Physical	Config	CLI			
IOS Command Line Interface					
Router-KAMPUS_2(config) # do show ip protocol					
Peuting Protocol is Torof 1					
Outraing Protocol is "ospi 1"					
Incoming update filter list for all interfaces is not set					
Bouter ID 192 168 1 1					
Number of areas in this router is 1, 1 normal 0 stub 0 nssa					
Maximum path: 4					
Routing for Networks:					
35.18.40.0 0.0.0.255 area 0					
7.6.4.0 0.0.255 area 0					
192.168.1.0 0.0.0.255 area 0					
Routing Information Sources:					
Gate	way	Dist	ance	Last Update	
35.1	8.40.1		110	00:13:45	
184.	75.66.1		110	00:13:46	
192.	168.1.1		110	00:13:40	=
Distance: (default is 110)					
Router-K	AMPUS_2 (co	onfig)#			*

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

- 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.