BAB 3

METODE PENELITIAN

Dalam penelitian ini, penulis menggunakan *Software* PNET Lab yang di import pada VMWare *Workstation* untuk membuat simulasi jaringan. PNET Lab menggunakan *image router* dan perangkat lainnya yang dijalankan secara *virtual*isasi namun tidak merubah dan mengurangi fitur seperti *Device* aslinya.

3.1 ALAT YANG DIGUNAKAN

3.1.1 PERANGKAT KERAS (HARDWARE)

Penelitian ini akan menggunakan peangkat keras beupa satu buah laptop dengan spesifikasi seperti pada tabel 3.1.

	- ···· ·· - ···· ······ - ············
CPU	Intel i7-11700F @2.50GHz (16 CPUs) ~2.50GHz
RAM	64 GB
Storage	1 TB
OS	Windows 10

Tabel 3.1 Spesifikasi Perangkat Keras

3.1.2 PERANGKAT LUNAK (SOFTWARE)

Perangkat lunak digunakan sebagai penunjang guna mengumpulkan datadata yang akan dianalisa. Perangkat yang digunakan pada penelitian ini seperti yang terlihat pada tabel 3.2.

		<u> </u>	
No	Software	Versi	Fungsi
1	VMWare Workstation	16.2.3	Virtual Machine
2	PNETLab	4.2.10	Pembuatan Topologi
3	Wireshark	3.6.7	Pengambilan Data
4	D-ITG	2.8.1	Membangkitkan trafik

Tabel 3.2 Spesifikasi Perangkat Lunak

3.1.3 SPESIFIKASI DEVICE PADA SIMULASI

Penelitian ini menggunakan perangkat jaringan yang digunakan pada simulasi seperti pada tabel 3.3:

No	Perangkat	Keterangan
1	VPC	Perangkat default di
1	vi e	Pnetlab
2	Fortigate	FortiOS 7.0.1
		L3-
3	Router Cisco	ADVENTERPRISEK9-
		M-15.4-2T
		L2-
4	Switch	ADVENTERPRISEK9-
		M-15.2-20150703

Tabel 3.3 Spesifikasi Device pada Simulasi

3.2 ALUR PENELITIAN

Pada penelitian ini melakukan beberapa tahapan seperti pada diagram alur pada gambar 3.1.



Gambar 3.1 Diagram Alur Penelitian

Tahapan pada penelitian ini dilakukan dengan mengacu pada diagram alur pada Gambar 3.1. Tahap pertama yaitu mempersiapkan perangkat baik berupa perangkat keras maupun perangkat lunak. Perangkat keras berupa PC dengan OS Windows 10 dengan CPU Intel i7-11700F @2.50GHz (16 CPUs) ~2.50GHz dan RAM sebesar 64 GB dengan kapasitas penyimpanan setidaknya 30 GB. Adapun perangkat lunak yaitu VMWare *Workstation*, PNETLab, *Wireshark* dan D-ITG. Berikutnya melakukan proses instalasi *Software* yang telah disiapkan tersebut. Berikutnya melakukan uji coba pada *Software* yang telah diinstall. Uji coba dilakukan dengan menghubungkan dua buah VPC pada PNETLab (*peer-to-peer*) kemudian mengkonfigurasikan IP dan melakukan ping pada masing-masing VPC. Apabila proses ping berhasil maka *Software* dapat digunakan untuk tahapan berikutnya. Tahapan selanjutnya membuat topologi jaringan dimana sebuah VPC akan terhubung pada sebuah switch yang menghubungkan pada dua buah *router* fortigate yang mana masing-masing *router* akan terhubung pada jaringan *internet* yang berbeda. *Router* pertama digunakan sebagai *router* utama sedangkan *router* lainnya digunakan sebagai *router backup*. Kemudian masing-masing perangkat dikonfigurasi dimana pada *router* backup.

Tahap berikutnya yaitu mengambil data-data berdasarkan scenario yang akan dilakukan. D-ITG digunakan untuk membangkitan trafik pada jaringan dan *Wireshark* digunakan untuk merekam *traffic* pada jaringan. Data-data yang diambil tersebut akan dianalisa berdasarkan pada parameter uji yaitu QoS dan *time response failover* dengan menggunakan standarisasi TIPHON.



3.3 TOPOLOGI JARINGAN

Gambar 3.2 Topologi Jaringan

Gambar 3.2 adalah topologi yang akan digunakan pada penelitian ini dimana jaringan pada HQ (sebelah kiri) akan dihubungkan pada jaringan *Branch* (sebelah kanan) melalui *public Network* dengan dua buah *link* koneksi yang berbeda. *Router* Utama pada *headquarter* dan pada *branch* akan melalui *link* MPLS sedangkan *router backup* akan melalui *link* koneksi *internet. Router* SD-WAN pada masing-masing cabang akan diberi *virtual* IP yang sama namun dengan nilai *priority* yang berbeda. Pada *router* utama akan diberi nilai *priority* sebesar 255 sedangkan pada *router backup* akan diberi nilai *priority* 100.

Device	Interface	Ip address	Priority	Gateway
	Port1 192.168.1.1/24			
<i>Router</i> Utama HQ	Vrip	192.168.1.100/24	255	
	Port2	11.11.11.2/24		
	Port1	192.168.1.10/24		
Router Backup HQ	Vrip	192.168.1.100/24	100	
	Port2	172.33.20.2/24		
Doutor Litomo	Port2	192.168.100.1/24		
Rouler Olama	Vrip	192.168.100.100/24	255	
Dranch	Port1	14.14.14.2/24		
Doutor Dackup	Port2	192.168.100.2/24		
Rouler Buckup	Vrip	192.168.100.100/24	100	
Diditch	Port1	172.33.25.2/24		
D1	fe0/0	11.11.11.1/24		
K1	fe0/1	12.12.12.1/24		
20	fe0/0	12.12.12.2/24		
RZ	fe0/1	13.13.13.1/24		
20	fe0/0	13.13.13.2/24		
КЭ	fe0/1	200.20.10.1/24		
	fe0/0	172.33.20.1/24		
R4	fe0/1	172.33.21.1/24		
	fe0/2	172.33.22.1/24		
DE	fe0/0	172.33.21.2/24		
C7	fe0/1	172.33.23.1/24		
DC	fe0/0	172.33.22.2/24		
KO	fe0/1	172.33.24.1/24		
	fe0/0	172.33.24.2/24		
R7	fe0/1	172.33.23.2/24		
	fe0/2	100.10.10.1/24		
VPC1	eth0	192.168.1.3		192.168.1.100
VPC2	eth0	192.168.100.3		192.168.100.100

Tabel 3.4 Alokasi *Ip address* pada Topologi Jaringan

Tabel 3.3 merupakan alokasi IP dan nilai *priority* yang akan diberikan pada masing-masing *router* dan VPC.

3.4 KONFIGURASI SD-WAN

Konfigurasi SD-WAN dilakukan pada fortigate baik pada *router* utama maupun *router backup* sehingga jaringan local dapat terhubung ke jaringan publik. Adapun urutan konfigurasinya yaitu:

🕞 Router-Backup	-	≣ ଦ				
🖚 Dashboard	>	Edit Interface				
🕂 Network	~		A b 1 (+4)			
Interfaces	☆	Name 🛄 L	AN (port1)			
DNS		Alias LA				
Packet Capture		Type P	nysical interface			
SD-WAN				÷.		
Static Routes			N	•		
Policy Routes		Address				
RIP		Addressing mode		Manual DHCF	Auto-managed	by FortiIPAM
OSPF		IP/Netmask		192.168.100.2/2	255.255.255.0	
BGP		Create address ob	ject matching subnet 🖸			
Routing Objects		Secondary IP addr	ess a			
Multicast						
🛓 Policy & Objects	>	Administrative Ac	cess			
Security Profiles	>	IPv4	Speed Test	HTTPS		PING
🖵 VPN	>		FMG-Access	SSH 🔽		SNMP
● User &	,		□ FTM	🗌 RADIU	S Accounting	Connection ()
Authentication		Receive LLDP 🜖	Use VDOM Setting	Enable Disable		
System 1	<u> </u>	Transmit LLDP 🚯	Use VDOM Setting	Enable Disable		
	> v7.0.1				ОК	Cancel

1. Menentukan Role *Port* pada fortigate pada menu *Network > Interface*

Gambar 3.3 Role pada Interface Port1

Gambar 3.3 menunjukkan *interface port*1 pada fortigate yang berfungsi sebagai *port* LAN dimana IP yang digunakan adalah 192.168.100.2 dengan subnet mask 255.255.255.0.

Router-Backup	~	≣ વ				
Dashboard	>	Edit Interface				
Network	~		MAND (port2)			
Interfaces	☆	Name				
DNS		Alias	WAN2			
Packet Capture		Туре	Physical Interface			
SD-WAN		VRFID 🚯	0			
Static Routes		Role 🟮	WAN	•		
Policy Routes		Estimated bandwidth 🤅	0		kbps Upstr	eam
	— I		0		kbps Dowr	istream
RIP						
OSPF		Address				
BGP		Addressing mode	Manual DHCP A	uto-managed by For	tilpam	
Routing Objects		IP/Netmask	100.10.10.2/255.255	5.255.0		
Multicast		Secondary IP address (
Policy & Objects	>					
Security Profiles	>	Administrative Access				
III VPN	>	IPv4	Speed Test	HTTPS		HTTP
User & Authentication	>) PING) SNMP	FMG-Access FTM		SSH RADIUS Accounting
🗢 System	1 > •		Connection ()			
	> v7.0.1	-			ОК	Cancel

Gambar 3.4 Role pada Interface Port2

Gambar 3.4 menunjukkan *interface port*2 pada fortigate dengan role sebagai *interface* WAN yang terhubung ke jaringan public. Adapun IP yang digunakan pada *interface* ini adalah 100.10.10.2 dengan subnetmask 255.255.255.0

Menentukan SD-WAN Zone dan SD-WAN member pada menu Network > SD-WAN

🕞 Router-Backup 🔹	≡ Q.				>_ 0 - L
🙆 Dashboard 🔹 🔸	Edit SD-WAN Zone				
	Edit SD-WAN Zone Name Interface members	SD-WAN2 WAN2 (port2)	×		Additional Information Additional Information API Preview References Edit in CLI Solvean Setup Guides Creating the SD-WAN Interface C MPLS (SIP and Backup) + DIA (Cloud A) SD-WAN Traffic Shaping and QoS with Per Packet Distribution and Tunnel Age Documentation Online Help C Video Tutorials C
A Security Profiles Security Profiles					
⊒ VPN >			ОК	Cancel	
▲ User & > Authentication					
🕸 System 🚺 🗴 🖣					
🔆 Security Fabric 💦 🔪					

Gambar 3.5 Konfigurasi SD-WAN Zone

Gambar 3.5 menunjukkan konfigurasi SD-WAN Zone dengan nama zona adalah SD-WAN2 dengan *interface* member *port*2 sebagai *interface* yang terhubung pada jaringan public.

🕞 Router-Backup 🔹	≡ Q.	>_ 🚱 - 1
🙆 Dashboard 🔹 🔸	Edit SD-WAN Member	
 Network Interfaces DNS Packet Capture SD-WAN Static Routes Policy Routes RIP OSPF BGP Routing Objects Multicast	Interface WAN2 (port2) SD-WAN Zone SD-WAN2 Gateway 100.10.1.1 Cost 0 Status Contemporation Disabled	Additional Information Additional Information API Preview Edit in CLI SD-WAN Setup Guides Creating the SD-WAN Interface MPLS (SIP and Backup) + DIA (Cloud A SD-WAN Traffic Shaping and QoS with Per Packet Distribution and Tunnel Ag Documentation Online Help C Video Tutorials C
Policy & Objects >		
Security Profiles >	I	
묘 VPN >	OK Cance	l
Luser & Authentication System Security Fabric > FailerTINET v7.0.1		

Gambar 3.6 Konfigurasi SD-WAN Member

Gambar 3.6 menunjukkan konfigurasi SD-WAN Member dimana *interface* yang digunakan adalah *port*2 dengan SD-WAN zone adalah SD-WAN2 yang telah dibuat sebelumnya. Adapun alamat gateway yang digunakan adalah *interface router* dari jaringan public yang terkoneksi ke *port*2 *router* fortigate.

3.	Melakukan	konfigurasi	static route	pada menu	Network >	Static Routes
----	-----------	-------------	--------------	-----------	-----------	---------------

🕞 Router-Backup		≡ Q		
🙆 Dashboard	>	Edit Static Route		
Network	~ I	Destination 6	Subpot Internet Service	A
Interfaces		Destination		
DNS		Interface	@ SD WAN2	
Packet Capture		interface	*	
SD-WAN		Comments	Write a comment	55
Static Routes	☆	Status	Enabled ODisabled	
Policy Routes				
RIP				
OSPF				
BGP				
Routing Objects				
Multicast				
💄 Policy & Objects	>			
Security Profiles	`			
D VPN	>			OK Cancel
User & Authentication	>			
🌣 System	<u>1</u> > "			
🔆 Security Fabric	>			
FURTINET	v7.0.1			

Gambar 3.7 Konfigurasi Static Routes pada SD-WAN

Gambar 3.7 menunjukkan konfigurasi static route dengan *interface* yang digunakan adalah SD-WAN Zone yang telah dikonfigurasi sebelumnya. Adapun destinasinya dibiarkan 0.0.0/0.0.0.0.

٩∎	а контег-раскир		= ~			
Ð	Dashboard	>	Edit Policy			
÷	Network	>				
B	Policy & Objects	~	Name 🚯	LAN-WAN2		
	Firewall Policy	☆	Incoming Interface	🖮 LAN (port1)	•	
	IPv4 DoS Policy		Outgoing Interface	SD-WAN2	•	
	Addresses		Source	🗉 all	×	
	Internet Service Database		Destination	+ I all	×	
	Services			+		
	Schedules		Schedule	Lo always	•	
	Virtual IPs		Service	ALL +	×	
	IP Pools		Action	✓ ACCEPT Ø DENY		
	Protocol Options					
	Traffic Shaping		Inspection Mode	Flow-based Proxy-based		
۵	Security Profiles	>				
	VPN	>	Firewall / Network O	ptions		
•	User &		NAT			
Ť	Authentication	Ý I	IP Pool Configuration	Use Outgoing Interface Add	ress	Use Dynamic IP Pool
۵	System	1 >	Preserve Source Port			
*	Security Fabric	> ~	Passive Health Check			
	F	v7.0.1				ОК

4. Mengatur firewall policy pada menu Policy & Objects > Firewall Policy

Gambar 3.8 Firewall Policy

Gambar 3.8 menunjukkan konfigurasi firewall policy yang digunakan dimana incoming *interface* adalah *interface* yang digunakan sebagai jaringan local yaitu *port*1. Outgoing *interface* adalah *interface* yang akan meneruskan komunikasi data pada jaringan public, yaitu SD-WAN Zone yang telah dibuat sebelumnya.

3.5 KONFIGURASI VRRP

Konfigurasi VRRP dilakukan pada masing-masing *router* pada *Headquarter* dan Branch. Konfigurasi VRRP ini dilakukan untuk menentukan *link* koneksi utama dan *link* koneksi cadangan.

Router Utama HQ config system interface edit port1 config vrrp edit 20

set vrip 192.168.1.100
set priority 255
next
end
next
end
Router Backup HQ
config system interface
edit <i>port</i> 1
config vrrp
edit 20
set vrip 192.168.1.100
set <i>priority</i> 100
next
end
next
end
Router Utama branch
config system interface
edit <i>port</i> 1
config vrrp
edit 10
set vrip 192.168.100.100
set priority 255
next
end
next
end
Router Backup branch
config system interface
edit <i>port</i> 1
config vrrp

```
edit 10
set vrip 192.168.100.100
set priority 100
next
end
next
end
```

Gambar 3.9 Konfigurasi VRRP

Pada gambar 3.9 menunjukkan konfigurasi *protocol* VRRP yang digunakan pada penelitian ini. Pada jaringan lokal di *headquarter*, *router* utama dan *router backup* menggunakan *virtual* ID 20 dengan *virtual* IP 192.168.1.100. Sedangkan pada jaringan local di branch, *router* utama dan *router backup* menggunakan *virtual router* ID 10 dengan *virtual router* IP yaitu 192.168.100.100. Adapun *router* dengan nilai *priority* sebesar 255 akan menjadi *Router* Utama dan *router* dengan nilai *priority* 100 akan menjadi *router backup*.

3.6 SKENARIO PENGUJIAN DAN PENGAMBILAN DATA

Penelitian ini melakukan 4 (empat) buah scenario dengan besar beban *traffic* yang berbeda-beda yaitu sebesar 10 Mbps, 25 Mbps, 50 Mbps dan 100 Mbps dengan waktu pengamatan 60 detik. Pengujian protokol VRRP dilakukan dengan memutuskan koneksi *router* utama sehingga seolah-olah tengah mengalami kendala. Pemutusan koneksi *router* utama dilakukan pada detik 20 waktu pengamatan untuk diamati apakah terjadi peralihan *link* koneksi dari *router* utama ke *router backup*. Lalu *router* utama akan diaktifkan kembali pada detik 40 waktu pengamatan untuk mengetahui apakah ada peralihan dari *router backup* ke *router* utama. Data yang dihimpun kemudian diolah untuk dianalisa berdasarkan parameter-parameter uji yang telah ditentukan. Adapun pengujian akan dilakukan sebanyak 5 kali pada masing-masing beban trafik seperti pada tabel 3.5.

Beban Trafik	Pengujiam
10 Mbps	5 Kali Pengujian
25 Mbps	5 Kali Pengujian

Tabel 3.5 Skenario Penelitian

Beban Trafik	Pengujiam
50 Mbps	5 Kali Pengujian
100 Mbps	5 Kali Pengujian