BAB 3
METODE PENELITIAN

Dalam penelitian ini, penulis menggunakan *Software* PNET Lab yang di im*port* 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.

Tabel 3.1 Spesifikasi Perangkat Keras

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

3.1.2 PERANGKAT LUNAK (*SOFTWARE*)

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

Tabel 3.2 Spesifikasi Perangkat Lunak

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

3.1.3 SPESIFIKASI *DEVICE* PADA SIMULASI

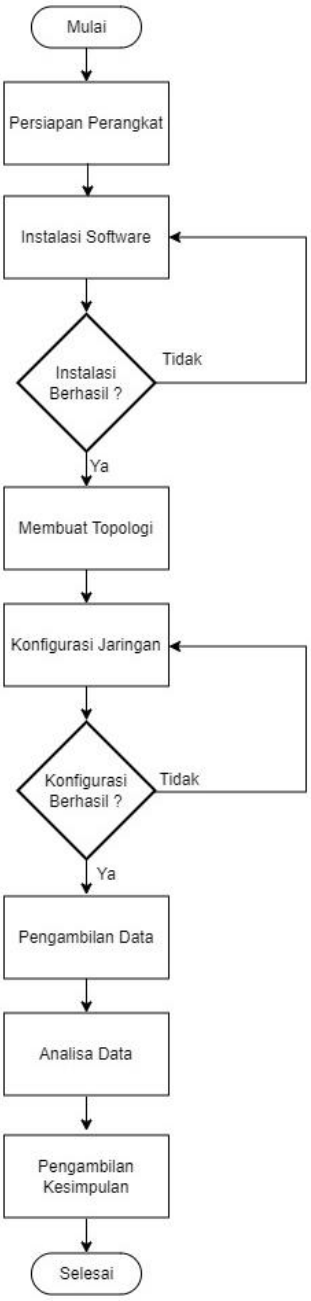
Penelitian ini menggunakan perangkat jaringan yang digunakan pada simulasi seperti pada tabel 3.3:

Tabel 3.3 Spesifikasi *Device* pada Simulasi

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

3.2 ALUR PENELITIAN

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



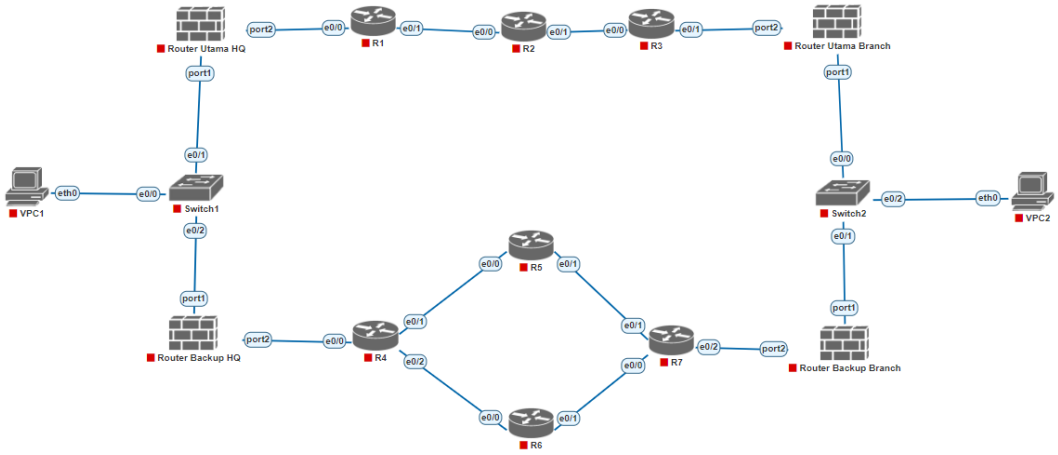
Gambar 3.1 Diagram Alur Penelitian

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* utama diberikan nilai *priority* yang lebih tinggi dari nilai *priority* 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.

Tabel 3.4 Alokasi *Ip address* pada Topologi Jaringan

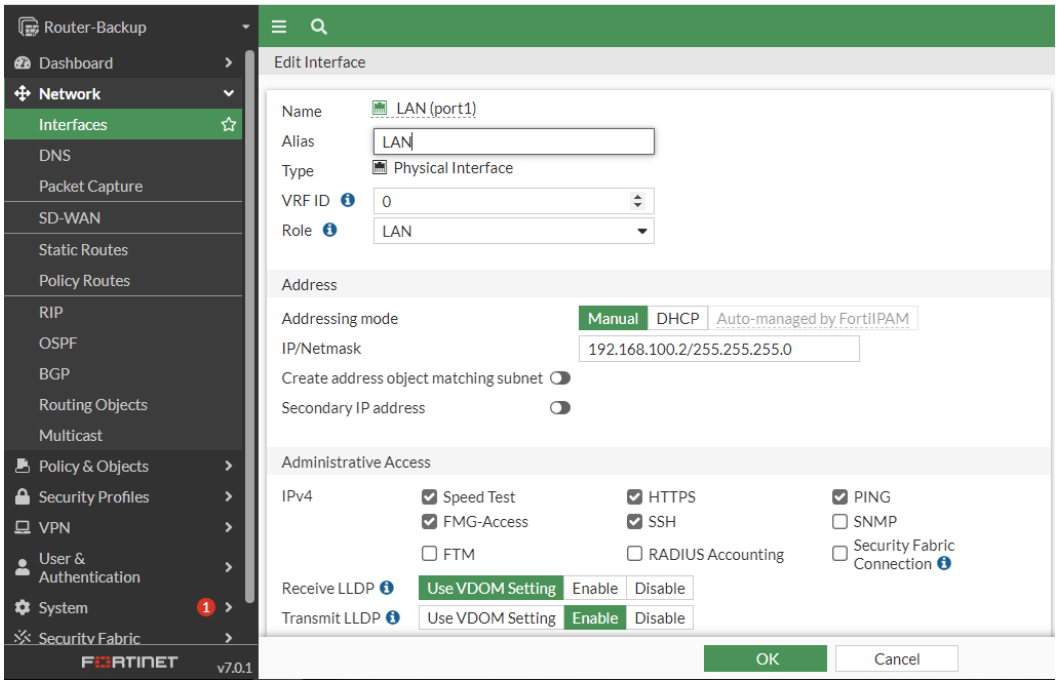
Device	*Interface*	*Ip address*	*Priority*	*Gateway*
Router Utama HQ	*Port*1	192.168.1.1/24		
	Vrip	192.168.1.100/24	255	
	*Port*2	11.11.11.2/24		
Router Backup HQ	*Port*1	192.168.1.10/24		
	Vrip	192.168.1.100/24	100	
	*Port*2	172.33.20.2/24		
Router Utama Branch	*Port*2	192.168.100.1/24		
	Vrip	192.168.100.100/24	255	
	*Port*1	14.14.14.2/24		
Router Backup Branch	*Port*2	192.168.100.2/24		
	Vrip	192.168.100.100/24	100	
	*Port*1	172.33.25.2/24		
R1	fe0/0	11.11.11.1/24		
	fe0/1	12.12.12.1/24		
R2	fe0/0	12.12.12.2/24		
	fe0/1	13.13.13.1/24		
R3	fe0/0	13.13.13.2/24		
	fe0/1	200.20.10.1/24		
R4	fe0/0	172.33.20.1/24		
	fe0/1	172.33.21.1/24		
	fe0/2	172.33.22.1/24		
R5	fe0/0	172.33.21.2/24		
	fe0/1	172.33.23.1/24		
R6	fe0/0	172.33.22.2/24		
	fe0/1	172.33.24.1/24		
R7	fe0/0	172.33.24.2/24		
	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 3.3 merupakan alokasi IP dan nilai *priority* yang akan diberikan pada masing-masing *router* dan VPC.

3.4 KONFIGURASI SD-WAN

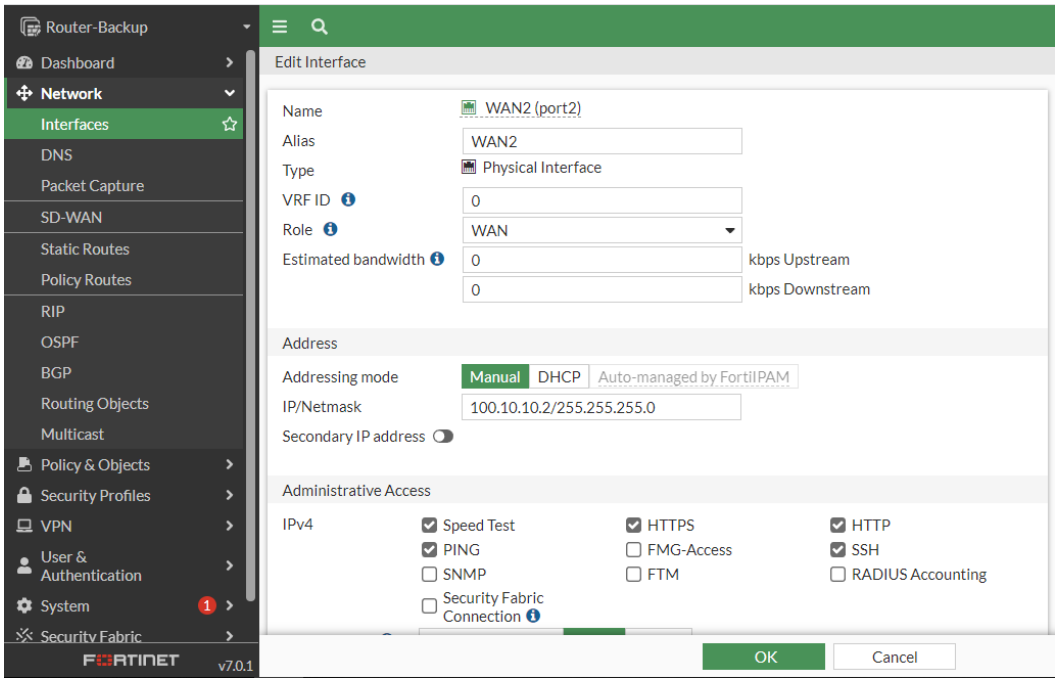
Konfigurasi SD-WAN dilakukan pada fortigate baik pada *router* utama maupun *router backup* sehingga jaringan local dapat terhubung ke jaringan publik. Adapun urutan konfigurasinya yaitu:

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



Gambar 3.3 Role pada *Interface Port*1

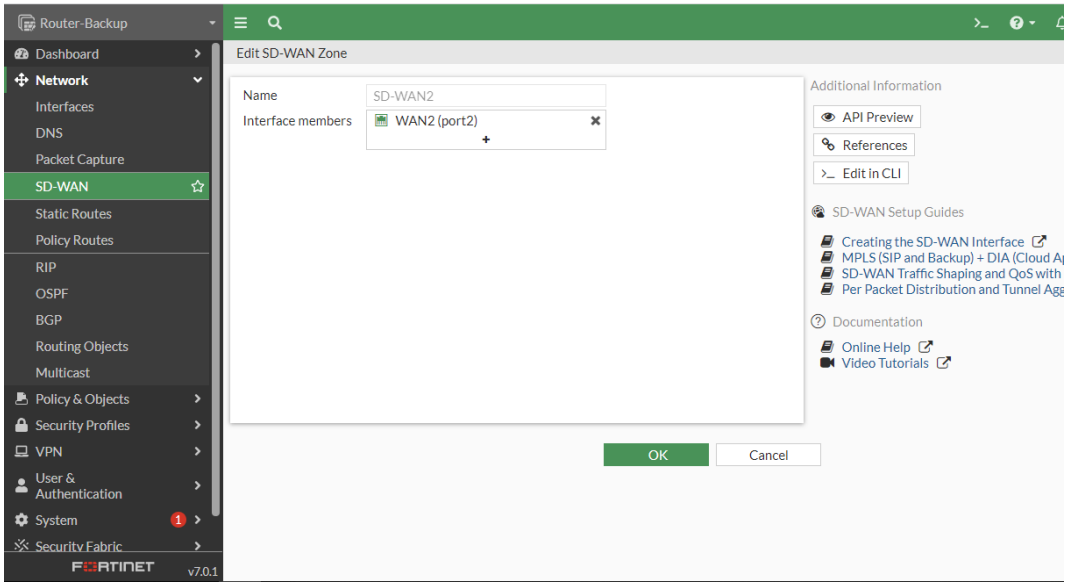
Gambar 3.3 menunjukkan *interface port*1 pada fortigate yang berfungsi sebagai *port* LAN dimana IP yang digunakan adalah 192.168.100.2 dengan subnet mask 255.255.255.0.



Gambar 3.4 Role pada *Interface Port*2

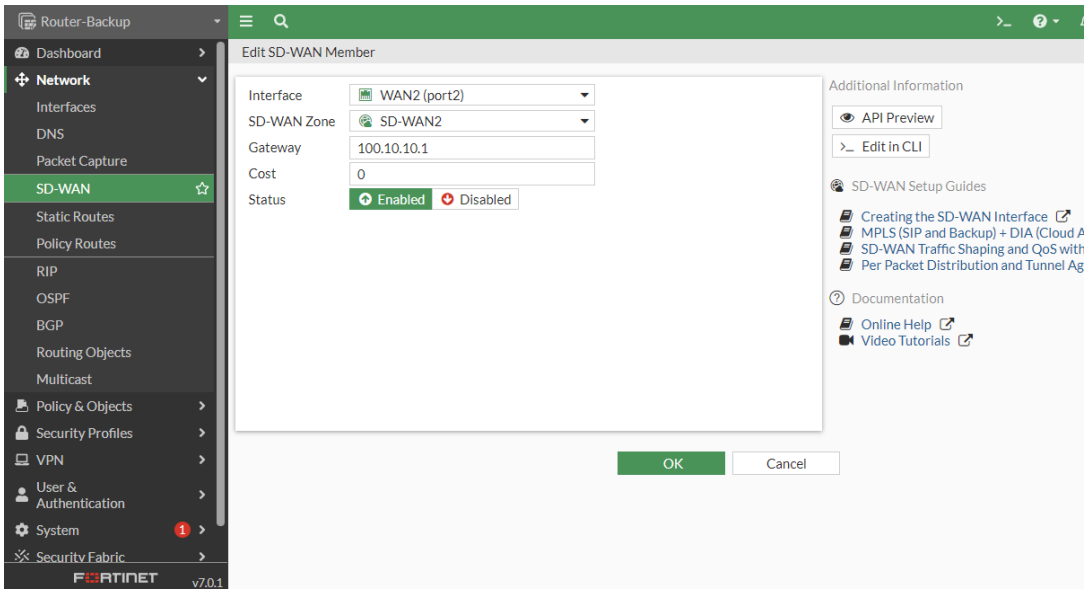
Gambar 3.4 menunjukkan *interface port2* pada fortigate dengan role sebagai *interface* WAN yang terhubung ke jaringan public. Adapun IP yang digunakan pada *interface* ini adalah 100.10.10.2 dengan subnetmask 255.255.255.0

2. Menentukan SD-WAN Zone dan SD-WAN member pada menu *Network* > SD-WAN



Gambar 3.5 Konfigurasi SD-WAN Zone

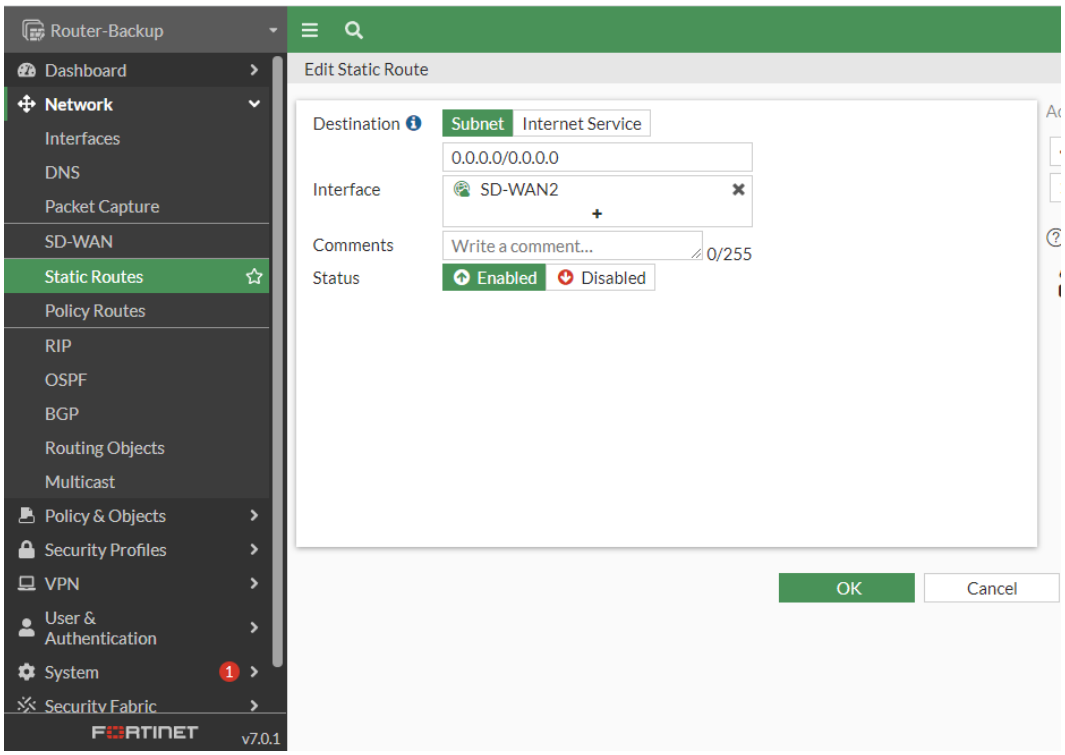
Gambar 3.5 menunjukkan konfigurasi SD-WAN Zone dengan nama zona adalah SD-WAN2 dengan *interface* member *port2* sebagai *interface* yang terhubung pada jaringan public.



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.

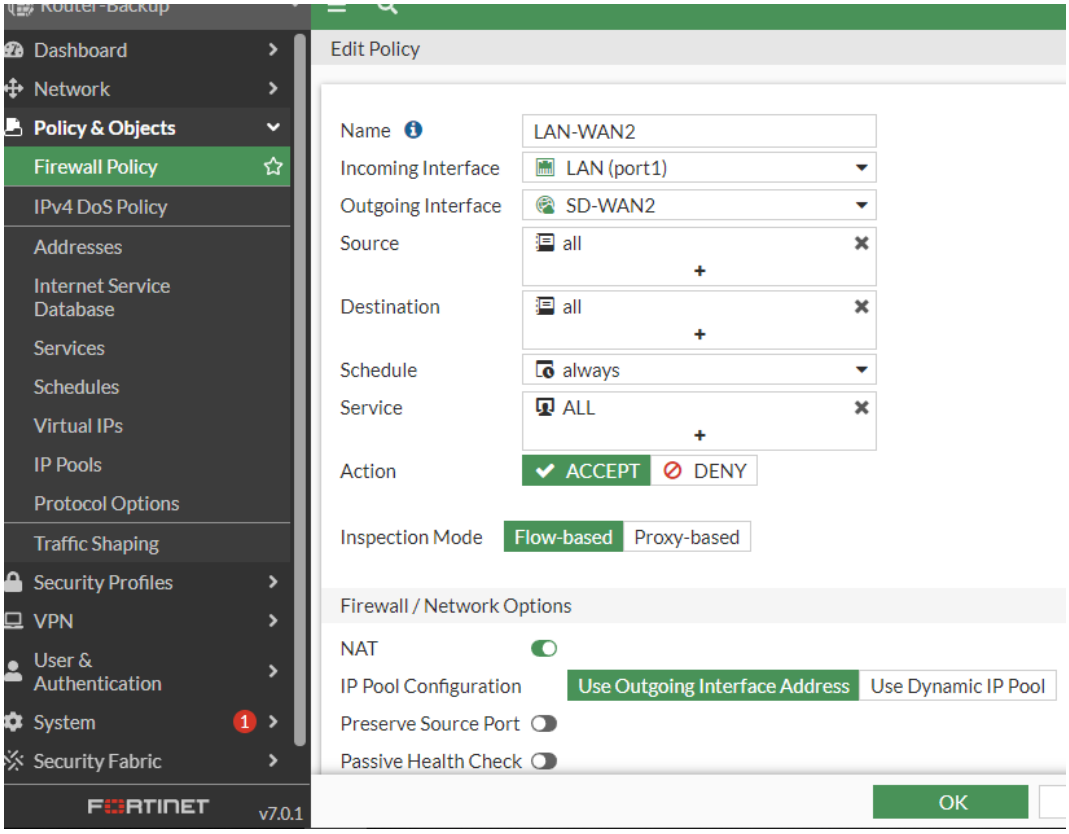
3. Melakukan konfigurasi static route pada menu *Network* > Static Routes



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 0.0.0.0/0.0.0.0.

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 *port*1 config vrrp edit 20

set vrip 192.168.1.100 set *priority* 255 next end next end
Router Backup HQ
config system *interface* edit *port*1 config vrrp edit 20 set vrip 192.168.1.100 set *priority* 100 next end next end
Router Utama branch
config system *interface* edit *port*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 *port*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.

Tabel 3.5 Skenario Penelitian

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

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