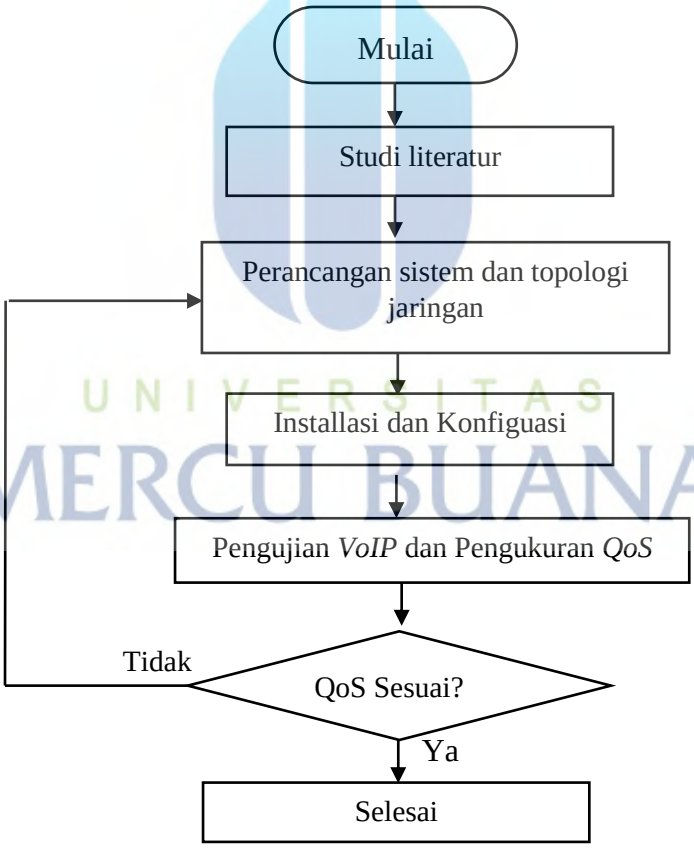
BAB III
METODOLOGI PENELITIAN

3.1 Perancangan Sistem

Pada bab ini akan dibahas tentang tahapan-tahapan yang dilakukan pada pengerjaan tugas akhir ini. Seperti yang terlihat pada gambar 3.1 berikut

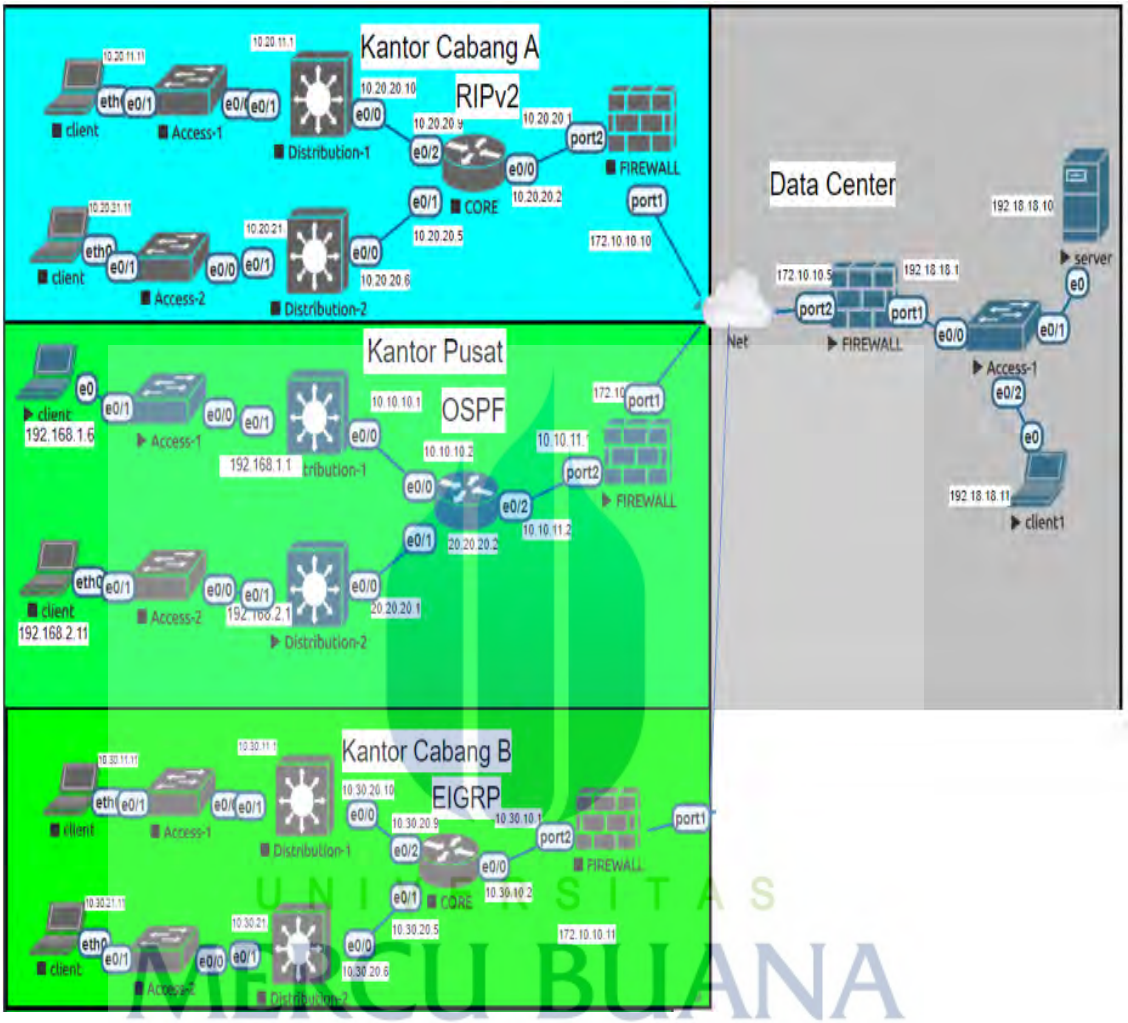


Gambar 3.1 Kerangka Penelitian

Pada pengerjaan simulasi dan analisa *QoS* dalam jaringan *virtual private network (VPN) site to site berbasis IPSec* dengan *routing OSPF*, *RIP* dan *EIGRP*. meliputi beberapa tahapan,diantaranya:

1. study literatur yang meliputi pengumpulan referensi dari jurnal dan penelitian yang telah dilakukan sebelumnya.
2. Perancangan sistem dan topologi jaringan. Dalam tahapan ini dilakukan design topologi jaringan yang akan digunakan dan perangkat apa saja yang akan digunakan dalam melakukan simulasi
3. Installasi *device* yaitu melakukan installasi semua perangkat termasuk *virual machine* yang akan di gunakan untuk simulasi dan analasis. Meliputi
4. Konfigurasi *device*. Setelah dilakukan installasi maka selanjutnya akan dilakukan konfigurasi pada masing-masing *device*.
5. Pengujian konfigurasi Apabila konfigurasi sudah dilakukan maka dapat dilanjutkan untuk pengujian *VoIP*, apabila VoIP sudah berhasil melakukan panggilan maka dapat dilanjutkan ke tahap selanjutnya namun apabila belum berhasil maka perlu di cek kembali pada design dan konfigurasinya.
6. Pengambilan dan Analisis Data *QoS*. Pada tahapan ini akan dilakukan pengukuran *QoS* dan analisisnya.

3.2 Topologi Jaringan dan Alokasi *IP address*



Gambar 3.2 Topologi Jaringan

Gambar diatas adalah model topologi yang akan di konfigurasi pada aplikasi simulator *Eve-NG*. *Eve-NG* adalah *emulator* berbasis web. Pada sisi server *DC (Data Center*) terdiri dari server asterisk yang akan digunakan sebagai server *VoIP*. Pada kantor pusat, kantor dan kantor cabang A, akan menggunakan routing yang berbeda sebagai perbandingan dan analisa. perangkat terdiri terdiri dari firewall, core switch, distribution switch, access switch dan klien linux. Topologi yang digunakan adalah star sehingga semua site dapat saling berkomunikasi satu sama lain dengan tunnel *VPN* berbasis *IPSec* melalui *data center*. Table dibawah ini merupakan alokasi *ip address*

Tabel 3.1 alokasi IP Address

Nama Site	IP Address	keterangan
Kantor Pusat	10.10.10.0/30	*Core* ke *distribution* 2
	20.20.20.0/30	*Core* ke *distribution* 1
	10.10.11.0/30	*Core* ke *Firewall*
	100.100.100.10	*Loopback*
	192.168.1.0/24 dan 192.168.2.0/24	klien
	172.10.10.1	*IPSec*
Kantor Cabang A	10.20.20.4/30	*Core* ke *distribution 2*
	10.20.20.8/30	*Core* ke *distribution 1*
	10.20.20.0/30	*Core* ke *Firewall*
	10.20.11.11/24 dan 10.20.21.11/24	klien
	172.10.10.10	*IPSec*
Data center	192.18.18.0/24	Server
	172.10.10.5	*IPSec*
Kantor Cabang B	10.30.10.4/30	*Core* ke *distribution* 2
	10.30.10.8/30	*Core* ke *distribution* 1
	10.30.10.0/30	*Core* ke *Firewall*
	10.30.11.11/24 dan 10.20.21.11/24	klien
	172.10.10.11	*IPSec*

3.3 Detail Perangkat

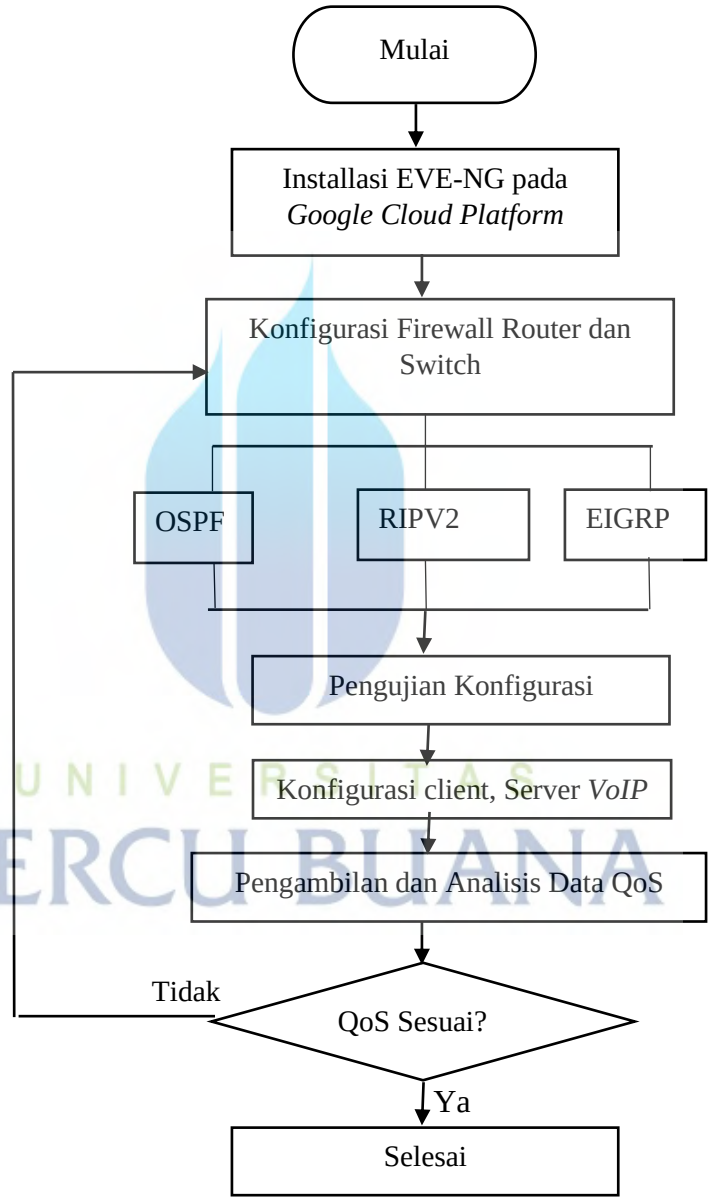
Adapun detail perangkat yang akan digunakan pada simulasi ini adalah seperti pada table berikut:

Table 3.2 Detail perangkat

Perangkat	Jumlah	Fungsi
Fortigate	4	Digunakan untuk membentuk *tunnel VPN* antar site dengan *IPSec*
Cisco Core switch	2	*Core layer* merupakan *backbone* yang menyediakan koneksi kecepatan tinggi (gigabit atau yang lebih tinggi). Core menjadi jalur Layer 3, bagi Layer core menyediakan scalability dan reliability.
Cisco Distribution switch	4	Distribution Layer disebut juga layer workgroup yang menerapkan titik kumunikasi antara layer akses dan layer inti.fungsi utama layer distribusi adalah menyediakan *routing*, filtering dan untuk menentukan cara terbaik untuk menangani permintaan layanan dalam jaringan.
Cisco access switch	5	Layer access menyediakan akses network bagi pengguna
Server *Asterisk*	1	Digunakan sebagai server *VoIP* untuk pengujian terhadap konfigurasi yang sudah dilakukan
Twinkle softphone	3	Digunakan untuk klien *VoIP*. Sehingga antara klien dan klien dapat melakukan panggilan.

3.4 Konfigurasi Sistem dan Simulasi

Pada tahap ini dilakukan proses simulasi, dan konfigurasi dari sistem yang akan dibuat. Berikut ini adalah *flowchart* dalam installasi sampai dengan pengukuran *QoS*.



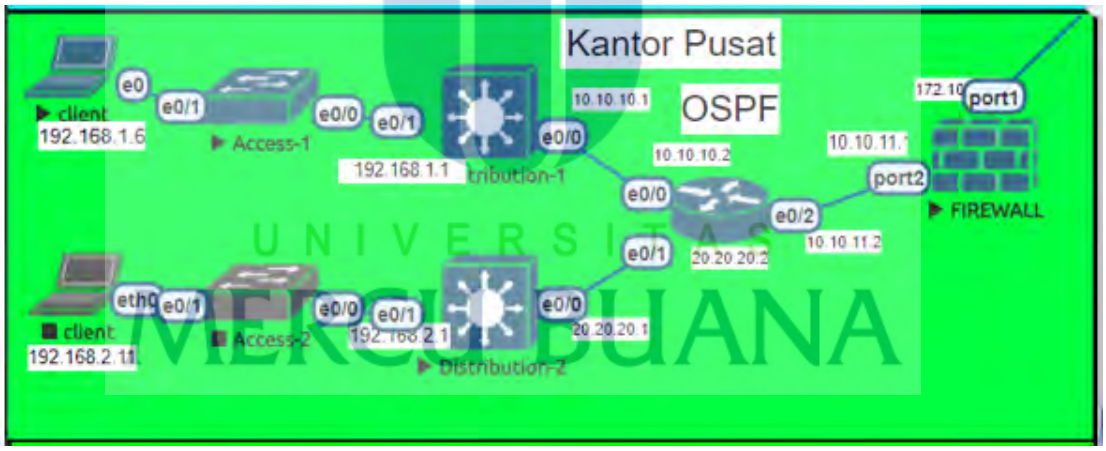
Gambar 3.3 *Flowchart* pengerjaan

3.4.1 Installasi EVE-NG pada *Google Cloud Platform*

EVE-NG adalah emulator yang akan digunakan melakukan simulasi. Pada tugas akhir ini penulis menginstall *EVE-NG pada google cloud platform. Google Cloud Platform* merupakan sebuah produk layanan *Cloud Computing* dari Google, Sehingga tidak diperlukan resource pada PC atau laptop.

3.4.2 Konfigurasi *OSPF*

konfigurasi dengan *routing OSPF* akan digunakan pada *Firewall*, *core switch* dan *distribution switch* di kantor Pusat. Koneksi ke arah server akan menggunakan *VPN tunnel* dengan *IPSec* 172.10.10.1. sedangkan IP yang digunakan pada klien adalah segment 192.168.1.0/24 dan 192.168.2.0/24. Dari *distribution switch* ke *access switch* akan menggunakan konfigurasi layer 2 dengan vlan 20. Gambar merupakan topologi yang digunakan pada kantor pusat.



Gambar 3.4 Topologi Kantor pusat

Berikut ini merupakan konfigurasi *OSPF* di *core switch*, disisi distribution switch konfigurasi nya sama hanya ip address dan network saja yang berbeda.

Core-HO(config)# interface Loopback0

Core-HO(config-if)#ip address 100.100.100.10 255.255.255.255

Core-HO(config)#interface Ethernet0/0

Core-HO(config-if)#ip address 10.10.10.2 255.255.255.252

Core-HO(config)# interface Ethernet0/1

Core-HO(config-if)# ip address 20.20.20.2 255.255.255.252

Core-HO(config)# interface Ethernet0/2

Core-HO(config-if)#ip address 10.10.11.2 255.255.255.252

Core-HO(config)#router ospf 100

Core-HO(config -router)# router-id 100.100.100.10

Core-HO(config -router)# network 10.10.10.0 0.0.0.3 area 0

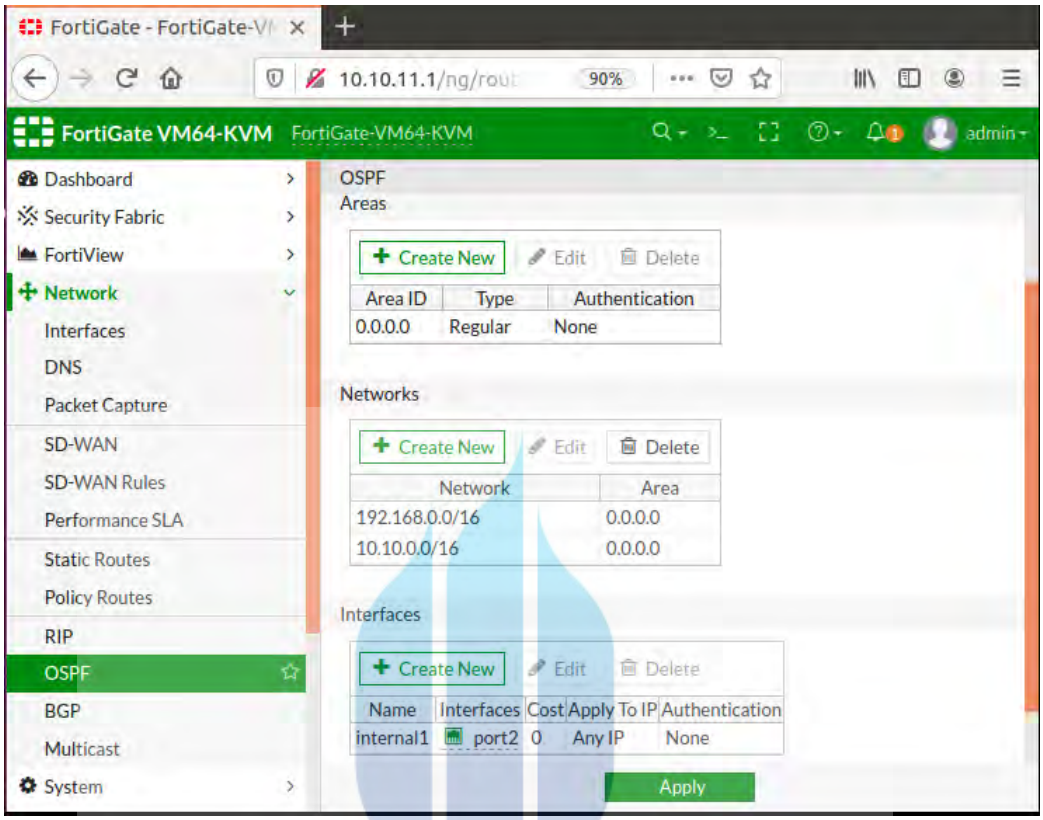
Core-HO(config -router)#network 10.10.11.0 0.0.0.3 area 0

Core-HO(config -router)#network 20.20.20.0 0.0.0.3 area 0

Core-HO(config -router)#network 100.100.100.10 0.0.0.0 area 0

Core-HO(config -router)#neighbor 200.200.200.1

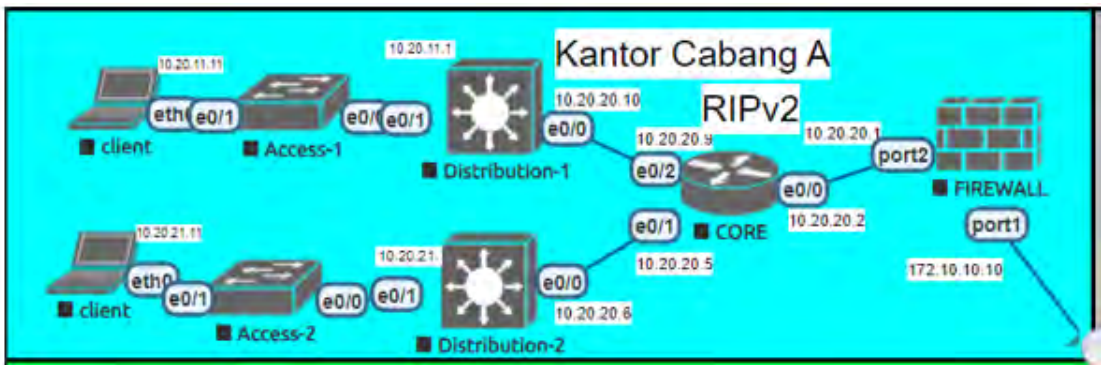
Disisi firewall fortigate konfigurasi *OSPF* dilakukan dengan cara akses *fortigate* melalui GUI kemudian pada menu network pilih *OSPF* dan masukan network 192.168.0.0/16 sebagai klien dan network ke arah router seperti pada gambar dibawah ini.



Gambar 3.5 konfigurasi OSPF

3.4.3 Konfigurasi *RIPv2*

konfigurasi dengan *routing RIPv2* akan digunakan pada *Firewall, core switch dan distribution switch* di kantor Cabang A. Koneksi ke arah server akan menggunakan *VPN tunnel* dengan *IPSec* 172.10.10.10. sedangkan IP yang digunakan pada client adalah segment 10.20.10.0/24 dan 10.20.11.0/24. Dari *distribution switch* ke *access switch* akan menggunakan konfigurasi layer 2 dengan vlan 20 Gambar merupakan topologi yang digunakan pada kantor cabang



Gambar 3.6 Topologi Kantor Cabang A

Berikut ini merupakan konfigurasi *RIPv2* di *core switch*, untuk melakukan konfigurasi dapat dilakukan dengan melakukan SSH ke core switch. disisi distribution switch konfigurasinya sama hanya ip address nya saja yang berbeda.

Core-Cab-A(config)#interface Ethernet0/0

Core-Cab-A(config-if)# ip address 10.20.20.2 255.255.255.252

Core-Cab-A(config)#interface Ethernet0/1

Core-Cab-A(config-if)#ip address 10.20.20.5 255.255.255.252

Core-Cab-A(config)#interface Ethernet0/2

Core-Cab-A(config-if)# ip address 10.20.20.9 255.255.255.252

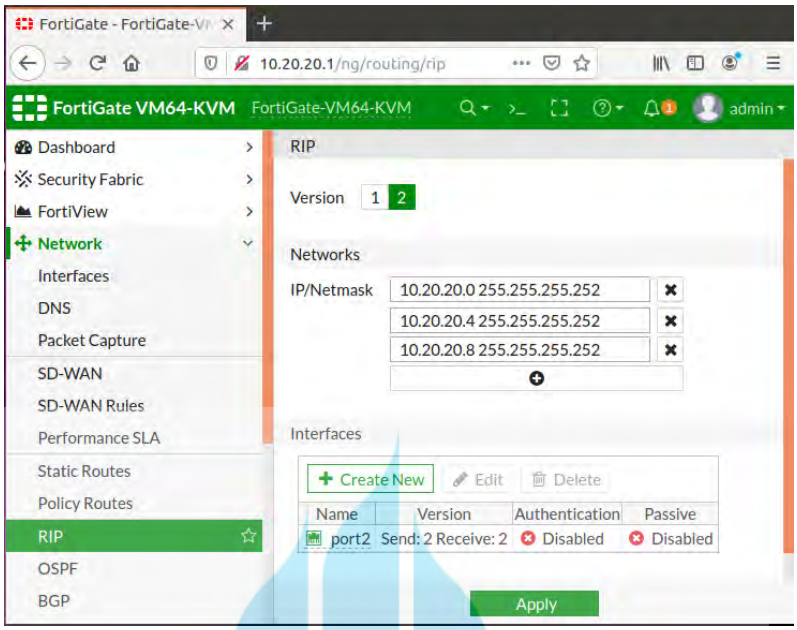
Core-Cab-A(config)#router rip

Core-Cab-A(config-router)# version 2

Core-Cab-A(config-router)# network 10.0.0.0

Core-Cab-A(config-router)#no auto-summary

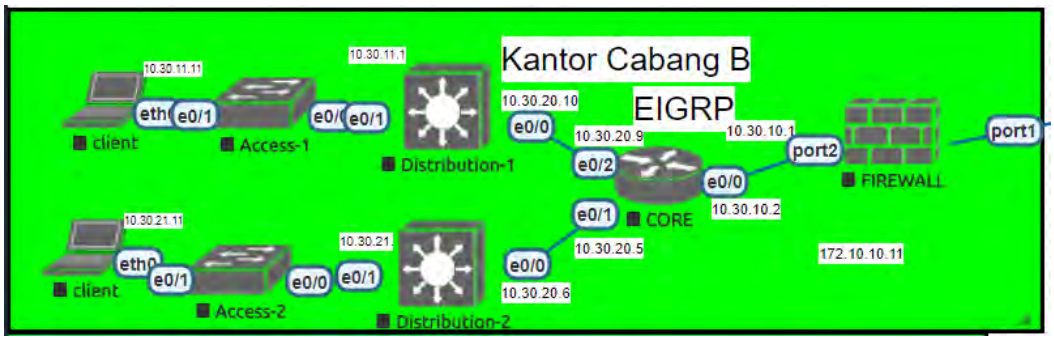
Disisi firewall fortigate konfigurasi *rip* dilakukan dengan cara akses *fortigate* melalui GUI kemudian pada menu network pilih *RIP* dan masukan network 192.168.0.0/16 sebagai klien dan network kea rah router seperti pada gambar dibawah ini.



Gambar 3.7 Konfigurasi RIP

3.4.4 Konfigurasi *EIGRP*

konfigurasi dengan *routing EIGRP* akan digunakan pada, *core switch dan distribution switch* di kantor Cabang B. Pada firewall akan dikonfigurasi static route ke arah core. Karena pada *EIGRP* hanya bisa dikonfigurasi pada perangkat cisco Koneksi ke arah server akan menggunakan *VPN tunnel* dengan *IPSec* 172.10.10.11. sedangkan IP yang digunakan pada client adalah segment 10.30.10.0/24 dan 10.30.11.0/24. Dari *distribution switch* ke *access switch* akan menggunakan konfigurasi layer 2 dengan vlan 20 Gambar merupakan topologi yang digunakan pada kantor cabang B.



Gambar 3.8 Topologi kantor cabang B

Berikut ini merupakan konfigurasi *EIGRP* di *core switch*, untuk melakukan konfigurasi dapat dilakukan dengan melakukan SSH ke core switch. disisi distribution switch konfigurasinya sama hanya ip address nya saja yang berbeda.

Core-Cab-B(config)#interface Ethernet0/0

Core-Cab-B(config-if)# ip address 10.20.20.2 255.255.255.252

Core-Cab-B(config)#interface Ethernet0/1

Core-Cab-B(config-if)#ip address 10.20.20.5 255.255.255.252

Core-Cab-B(config)#interface Ethernet0/2

Core-Cab-B(config-if)# ip address 10.20.20.9 255.255.255.252

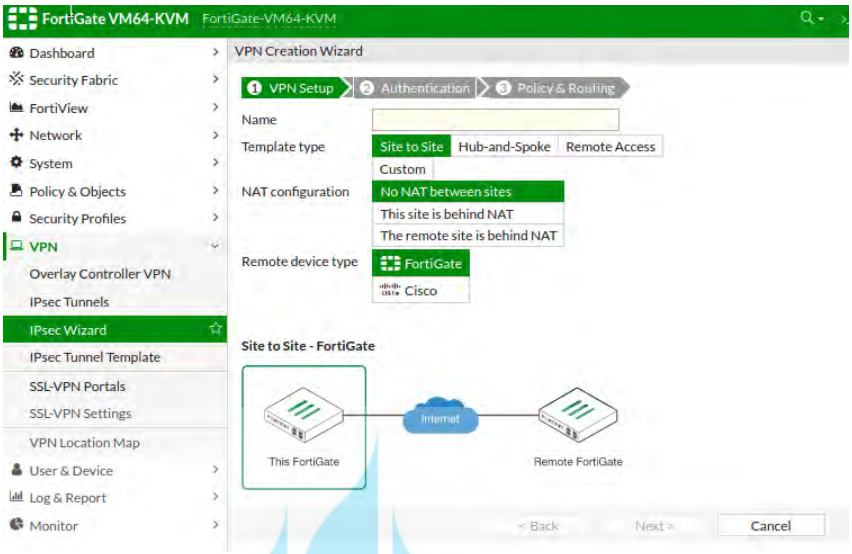
Core-Cab-B(config)#router eigrp 1

Core-Cab-B(config-router)# network 10.0.0.0

3.4.5 Konfigurasi *VPN IPSec*

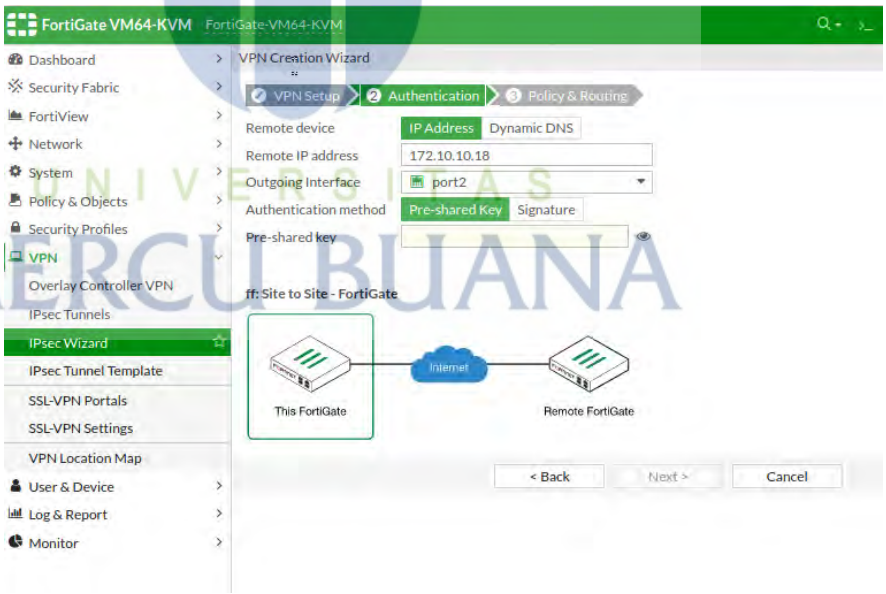
IPSec VPN akan dikonfigurasi pada *firewall* fortigate di semua *site*. Tujuannya agar dari kantor pusat, kantor cabang A dan kantor cabang B dapat terhubung ke Server atau data center. Untuk IP yang digunakan pada simulasi ini adalah IP dummy. Berikut tahapan-tahapan dalam konfigurasi *VPN IP-Sec* di fortigate.

1. Hal pertama dilakukan adalah dengan *login* melalui *GUI fortigate*. Pada menu pilih *VPN* lalu pilih *IP-Sec tunnels dan create new*.



Gambar 3.9 menu *create IPSec tunnels*

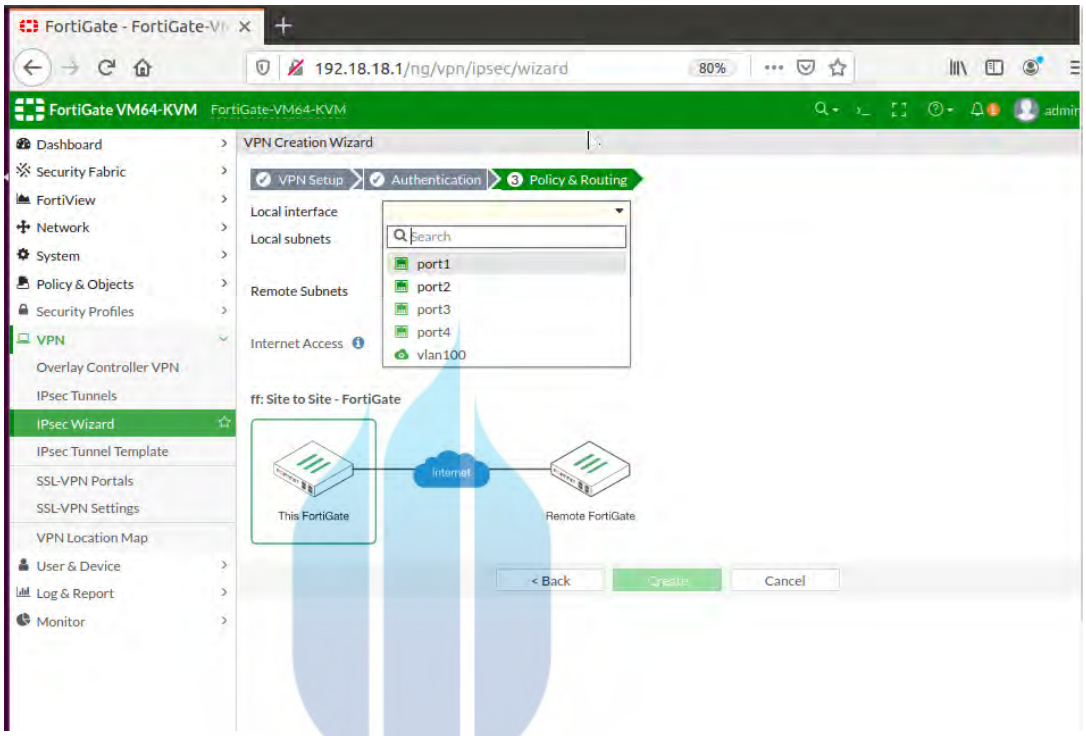
2. Masukan nama *to kantor pusat* kemudian pilih next, kemudian masukan remote IP address yang merupakan IPsec disisi kantor pusat, masukkan preshared key atau password. Password disisi data center dan disisi kantor pusat adalah sama.



Gambar 3.10 *Authetication IPSec VPN*

3. Pada tahap akhir, masukkan interface lokal yang akan diizinkan untuk diakses dari kantor pusat yaitu vlan 100 dengan *IP address* segmen 192.18.18.0/24 yang

merupakan segmen server di data center. Pada remote subnets masukkan ip address yang boleh diakses dari data center. Lalu pilih *create*.



Gambar 3.11 *Policy* dan *Routing* IPSec VPN

4. Setelah konfigurasi disisi data center selesai maka selanjutnya perlu membuat konfigurasi yang sama dikantor pusat namun dengan IP yang berbeda

3.4.6. Konfigurasi *Asterisk* dan *Twinkle*

Asterisk akan digunakan sebagai *server VoIP* untuk pengujian terhadap *QoS* pada *routing OSPF RIPv2 dan EIGRP* yang sudah dilakukan. Sedangkan twinkle akan digunakan untuk klien *VoIP*. Sehingga antara klien dapat melakukan panggilan. konfigurasi server asterisk pada linux di data center menggunkan ip 192.18.18.10 kemudian klien di kantor pusat dengan nomor 7001, klien 7002 di klien data center dan klien di kantor cabang A dengan nomor 7003. Twinkle merupakan aplikasi yang digunakan disisi klien untuk dapat melakukan panggilan ke nomor yang dituju.

3.5 Metode Simulasi.

Pada simulasi Tugas Akhir ini menggunakan metode *tunnel VPN* untuk menghubungkan jaringan antar site dengan *routing protocol OSPF, RIPv2* dan *EIGRP*. Terdapat *asterik* sebagai server *VoIP*, 4 Firewall sebagai pembentuk tunnel VPN dengan *IPSec*. 2 core switch, 4 distribution switch sebagai backbone dan 4 akses switch sebagai penghubung ke client *VoIP* . Adapun mekanisme pengiriman packet *VoIP* dari server ke klien sebagai berikut:

1. Packet *VoIP* akan di kirimkan dari server *asterisk* menuju client *twinkle*
2. *Firewall data center* akan meneruskan *packet* ke firewall dikantor pusat dan cabang melalui *tunnel VPN* yang sudah terkoneksi atau *terestablish* sebelumnya.
3. *firewall dan core switch* akan menerima paket yang sudah masuk melalui firewall kemudian akan menuruskan ke distribution switch dengan *routing OSPF* pada kantor pusat, routing *RIPv2* pada kantor cabang A *dan EIGRP* pada kantor cabang B
4. setelah proses *routing* packet akan langsung diteruskan dengan akses switch dengan layer 2 tanpa ada routing kembali.
5. didalam akses switch paket akan disampaikan ke client twinkle
6. untuk mendapatkan hasil yang akurat maka pengujian dilakukan dengan memutar video disisi server, sehingga inputan yang dimasukkan memiliki nilai yang sama.

Gambar 3.12 input untuk pengujian