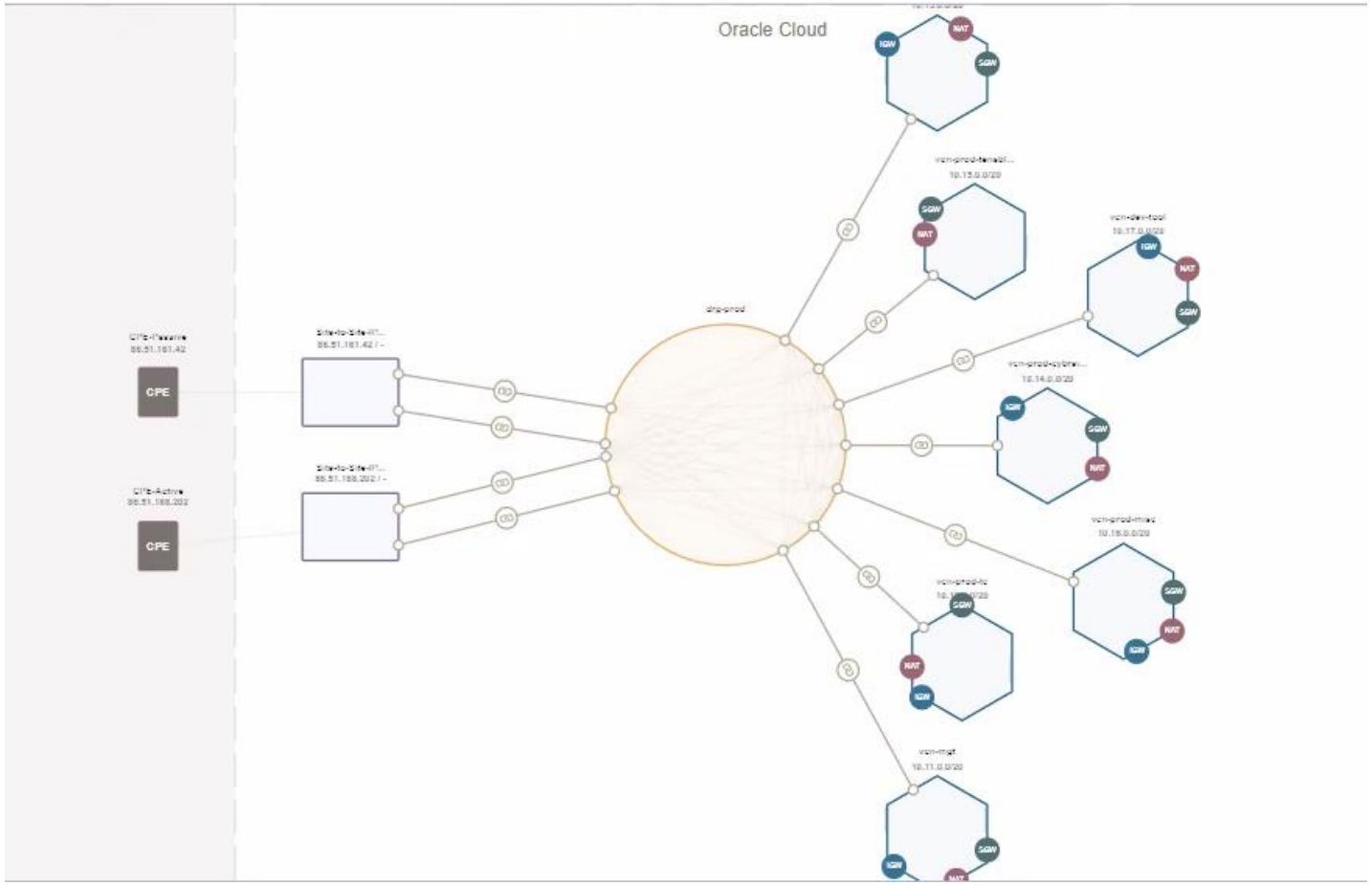
Implementation guide for Network Firewall in a Multi-VCNs deployment - Two different approaches

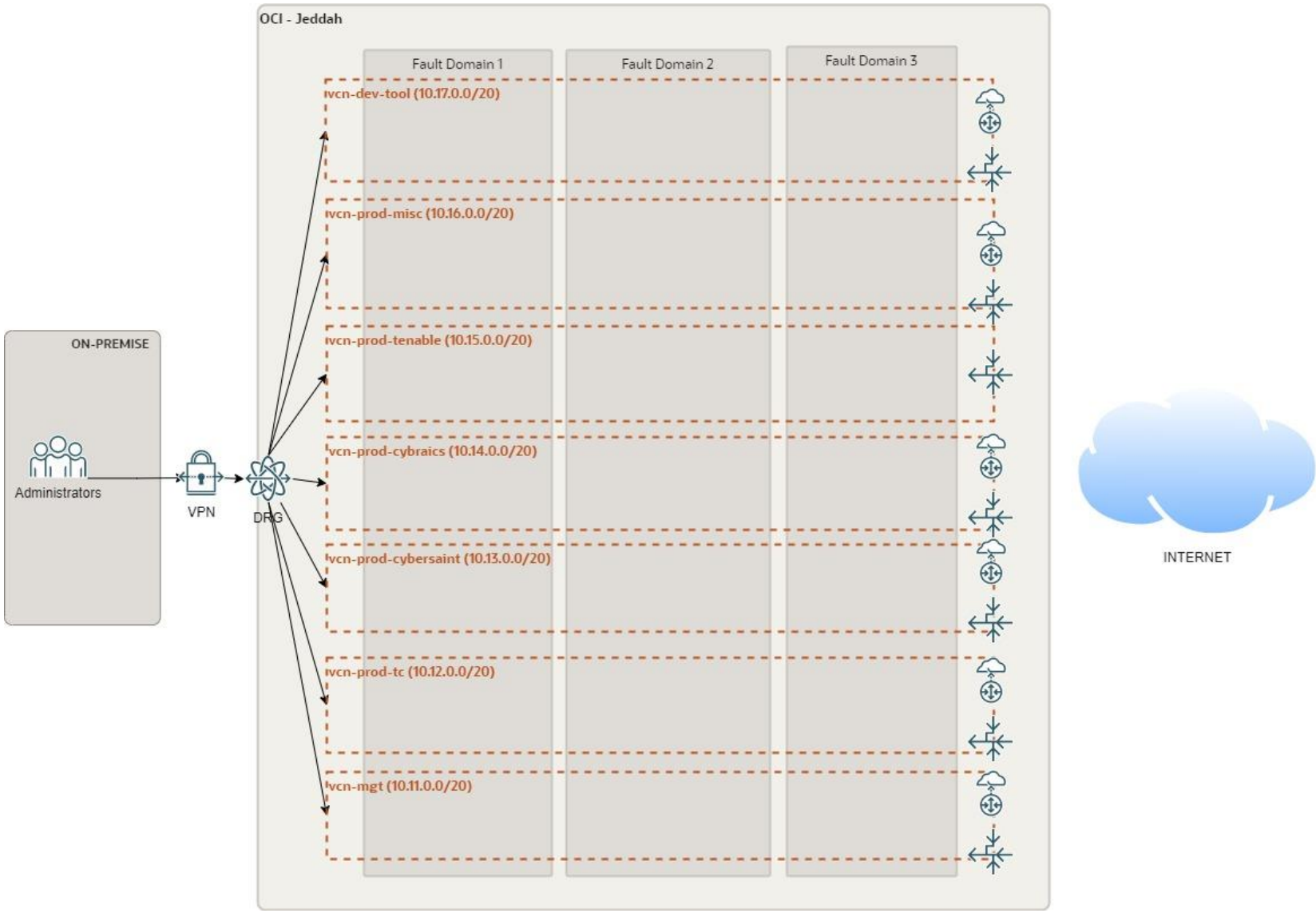
Antonio Gámir
OCI Networking Specialist

Starting point

The implementation rigth now it is a simple implementation for six VCNs and each workload is on its own VCN and all traffic from Internet comes from different Internet Gateways one in each VCNs

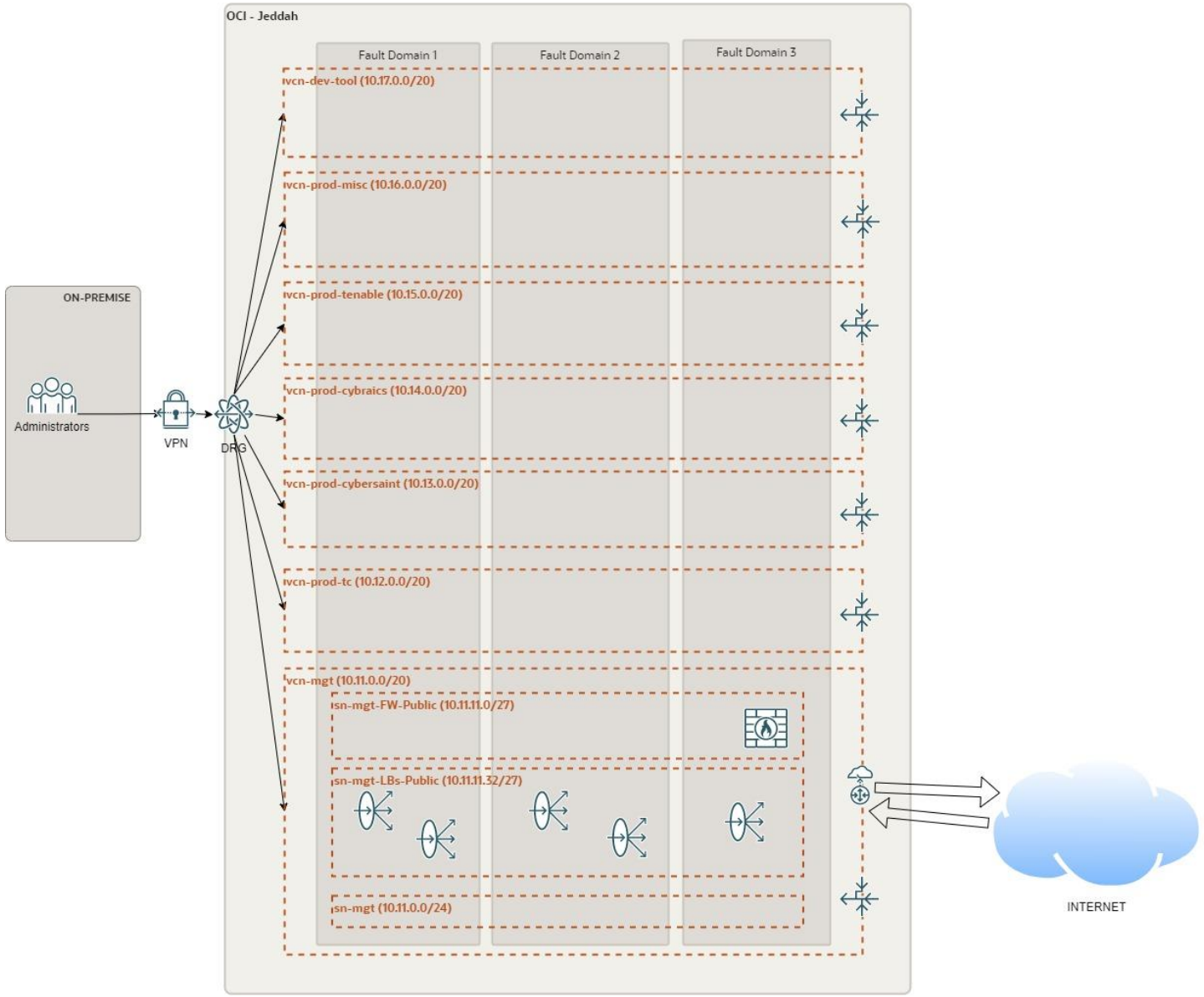


Starting point



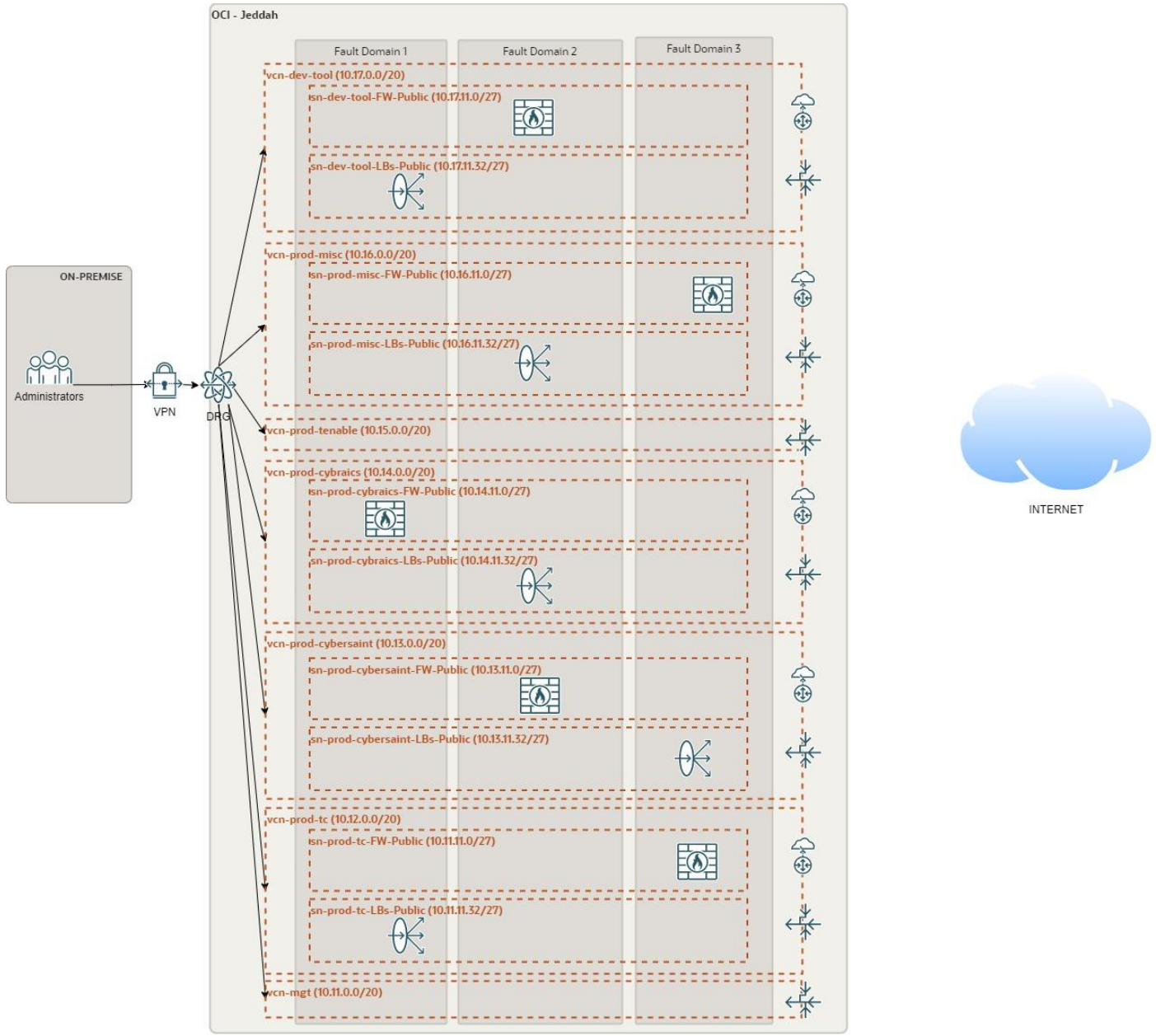
Hub and Spoke with one Network Firewall

Basic Approach



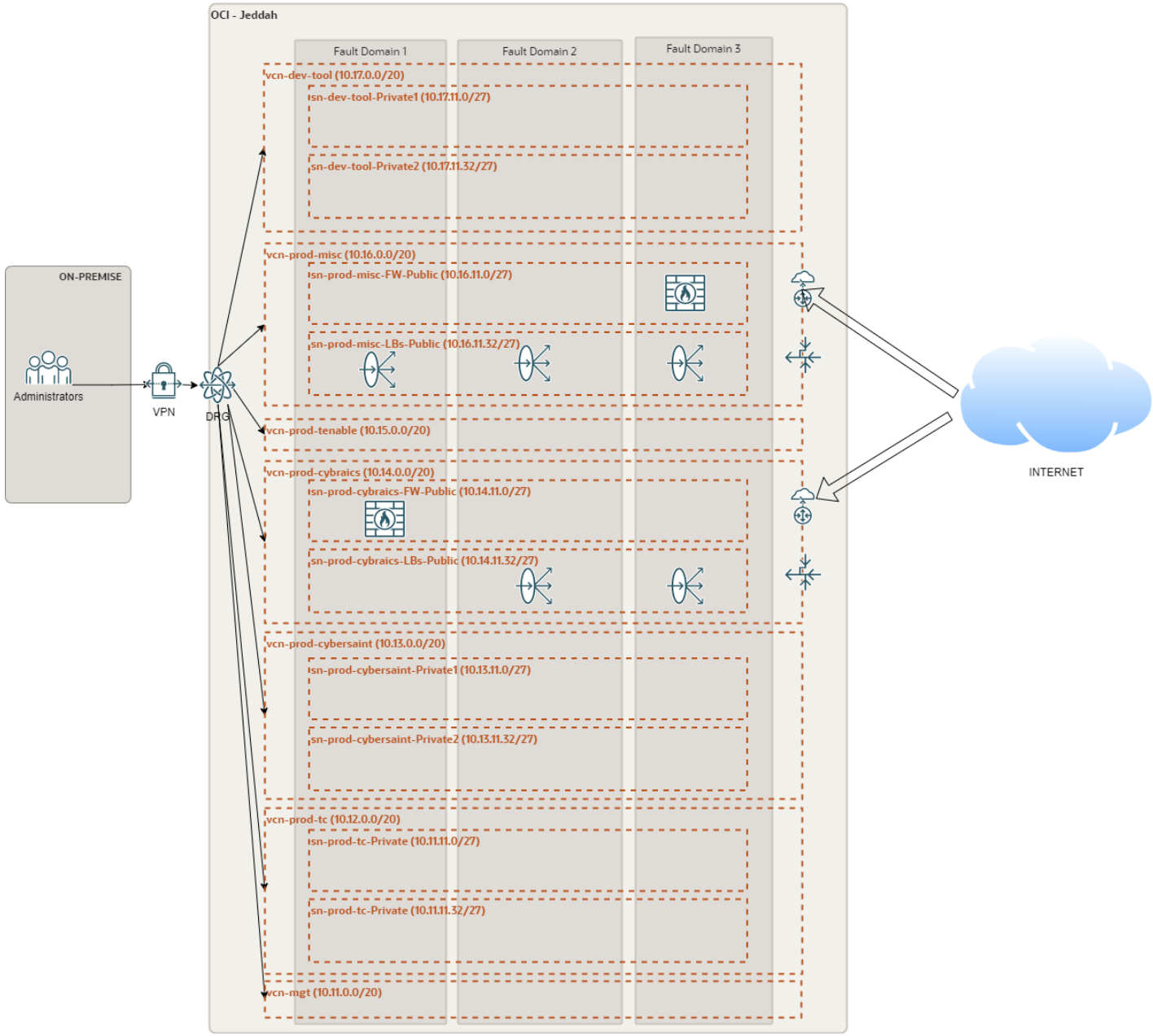
One Network Firewall per each Workload

Optimum Approach



Two Network Firewalls, One for Cybraics and another for the rest

Hybrid Approach



Basic Approach

Plan to achieve

Hub and Spoke with one Network Firewall

1.- Creates New two Subnets for DMZ for MGMT VCN
2.- Creates one Network Firewall Policy
3.- Create Network Firewall
4.- Change new routing
    a.- New RT (Internet Gateway Routing trough NFW IP)
    b.- DMZ FW Subnet RT
        1.- All traffic for Public Subnet to Internet Gateway
        2.- Traffic to Workloads to DRG
    c.- DMZ LB Subnet RT
        1.- All traffic to NFW IP address
        2.- Traffic to Workloads to DRG
5.- Create new LBs in the new Subnets
6.- Review all RT and SL to send traffic back to DRG
7.- Remove all unnecessary resources

Comments: All red entries will be downtime at the time to implement. The downtime will be for the complete environment.
We also change to join all public traffic in one Network Firewall and it will impact on the network performance.

Optimum Approach

Plan to achieve

One Network Firewall per each Workload

1.- Creates New Subnet(s) for DMZ in each Workload VCN
(We need one for FW and one for LB)
2.- Creates one Network Firewall Policy per each workload
3.- Create Network Firewall per each workload
4.- Change new routing in each DMZ VCN
    a.- New RT (Internet Gateway Routing trough NFW IP)
    b.- DMZ FW Subnet RT
        1.- All traffic for Public Subnet to Internet Gateway
        2.- Traffic to Workloads to DRG
    c.- DMZ LB Subnet RT
        1.- All traffic to NFW IP address
        2.- Traffic to Workloads to DRG
5.- Review all RT and SL to send traffic back to DRG
6.- Remove all unnecessary resources

Comments: This approach will have less impact on the implementation because the downtime will be workload by workload. So it can be done gradually. Performance for the network traffic will be higher than Basic option