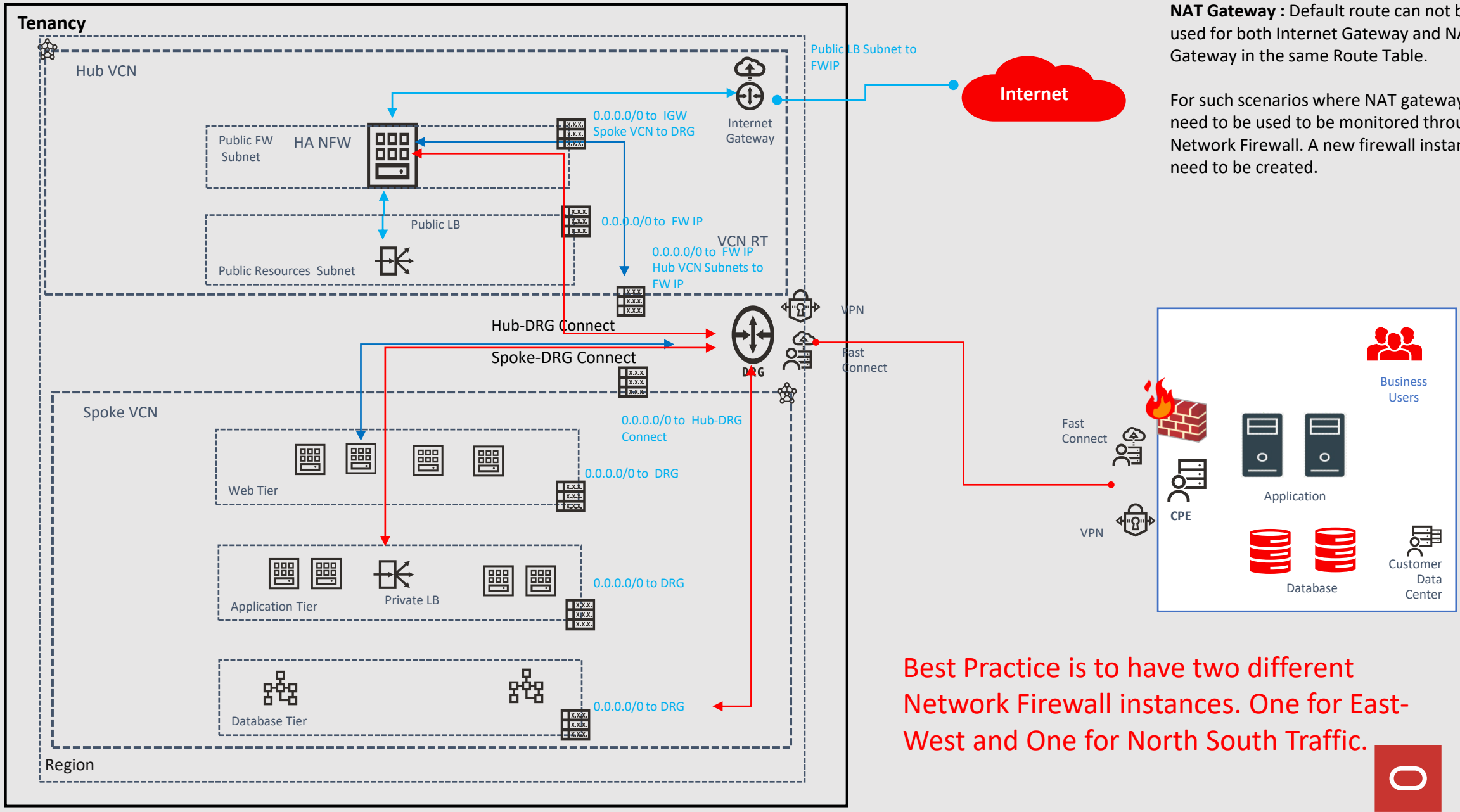
OCI Network Firewall Routing

Sachin Sharma
OCI Networking Specialist

Hub and spoke architecture having OCI Network firewall in HUB to monitor North-South and East-West Traffic



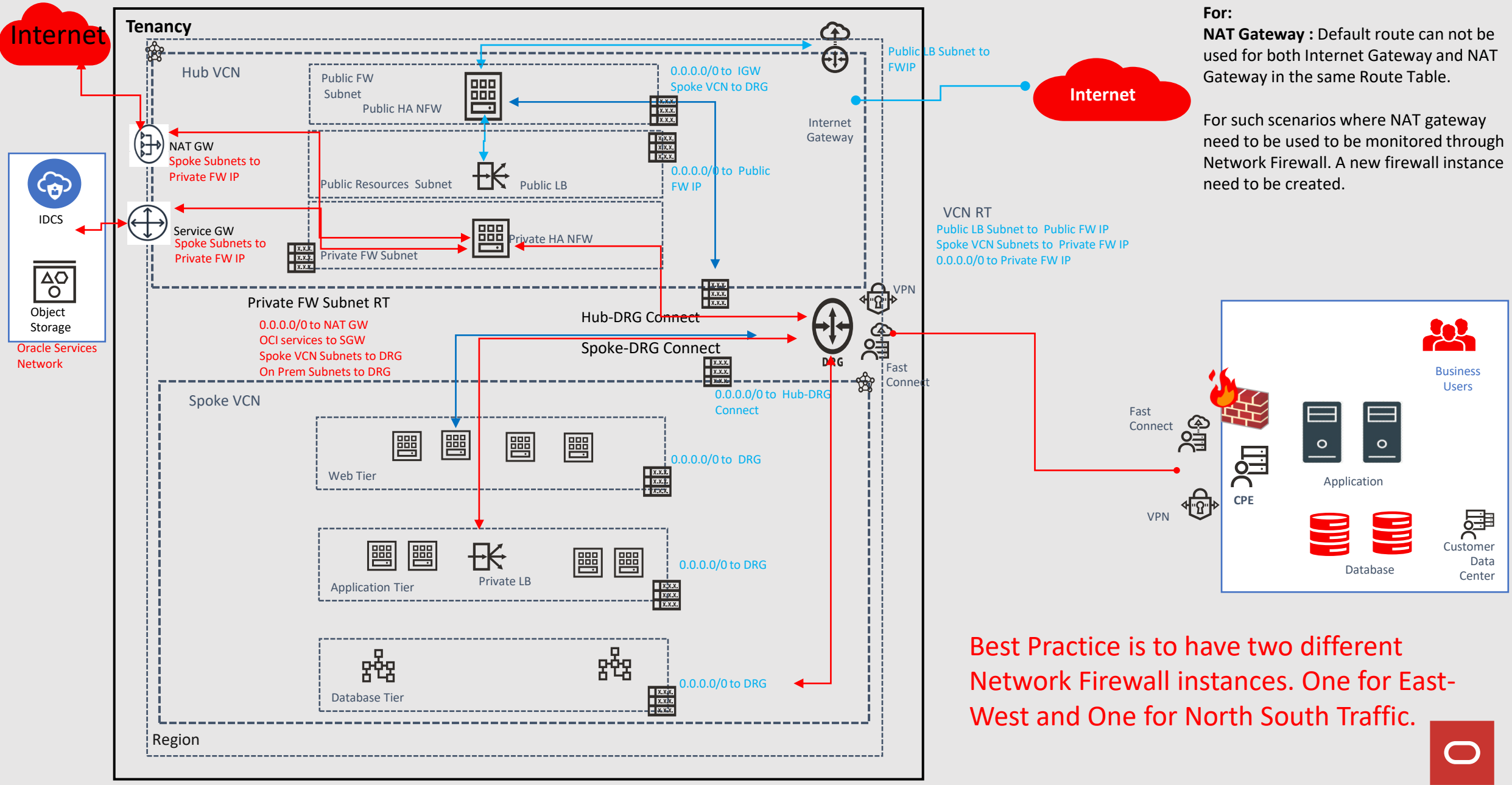
For:

NAT Gateway : Default route can not be used for both Internet Gateway and NAT Gateway in the same Route Table.

For such scenarios where NAT gateway need to be used to be monitored through Network Firewall. A new firewall instance need to be created.

Best Practice is to have two different Network Firewall instances. One for East-West and One for North South Traffic.

Hub and spoke architecture having one Network Firewall for Internet Traffic and one for within VCNs and Subnets and On prem Network.



For:

NAT Gateway : Default route can not be used for both Internet Gateway and NAT Gateway in the same Route Table.

For such scenarios where NAT gateway need to be used to be monitored through Network Firewall. A new firewall instance need to be created.

Best Practice is to have two different Network Firewall instances. One for East-West and One for North South Traffic.

Network Firewall routing for both North-South and East-West Traffic

Gateways/Subnets	RT
IGW	Public resources Subnet to Firewall IP/Hub VCN address range to Firewall IP
Public LB Subnet	Spoke VCN Subnets to Firewall IP
Spoke Subnets	0.0.0.0/0 to DRG
Hub-DRG Attachment	VCN-Route Table:0.0.0.0/0 to Firewall IP. On Prem Network to Firewall IP
Spoke DRG Attachment	0.0.0.0 Next HOP to HUB-DRG Attachment
Network Firewall Subnet	0.0.0.0/0 to IGW Spoke VCN to DRG

Network Firewall routing for Internet Traffic and for within VCNs and Subnets & OP

GATEWAYS/SUBNETS	RT
IGW	Public resources Subnet to Public Firewall IP
Public LB Subnet	Spoke VCN Subnets to Public Firewall IP
Spoke Subnets	0.0.0.0/0 to DRG
Hub-DRG Attachment	VCN-Route Table: 0.0.0.0/0 to Private Firewall IP. Public Load Balancer Subnet to Public Firewall IP. Spoke Subnets to Private Firewall IP. On Prem Subnets to Private Firewall IP
Spoke DRG Attachment	0.0.0.0 Next HOP to HUB-DRG Attachment
Public Network Firewall Subnet	0.0.0.0/0 to IGW Spoke VCN to DRG
Private Network Firewall Subnet	0.0.0.0/0 to Nat GW OCI services to SGW Spoke Subnets to DRG. On prem Subnets to DRG
SGW RT	Spoke Subnets to Private Network Firewall IP
NATGW RT	Spoke Subnets to Private Network Firewall IP