ORACLE

Oracle Cloud Infrastructure Onboarding

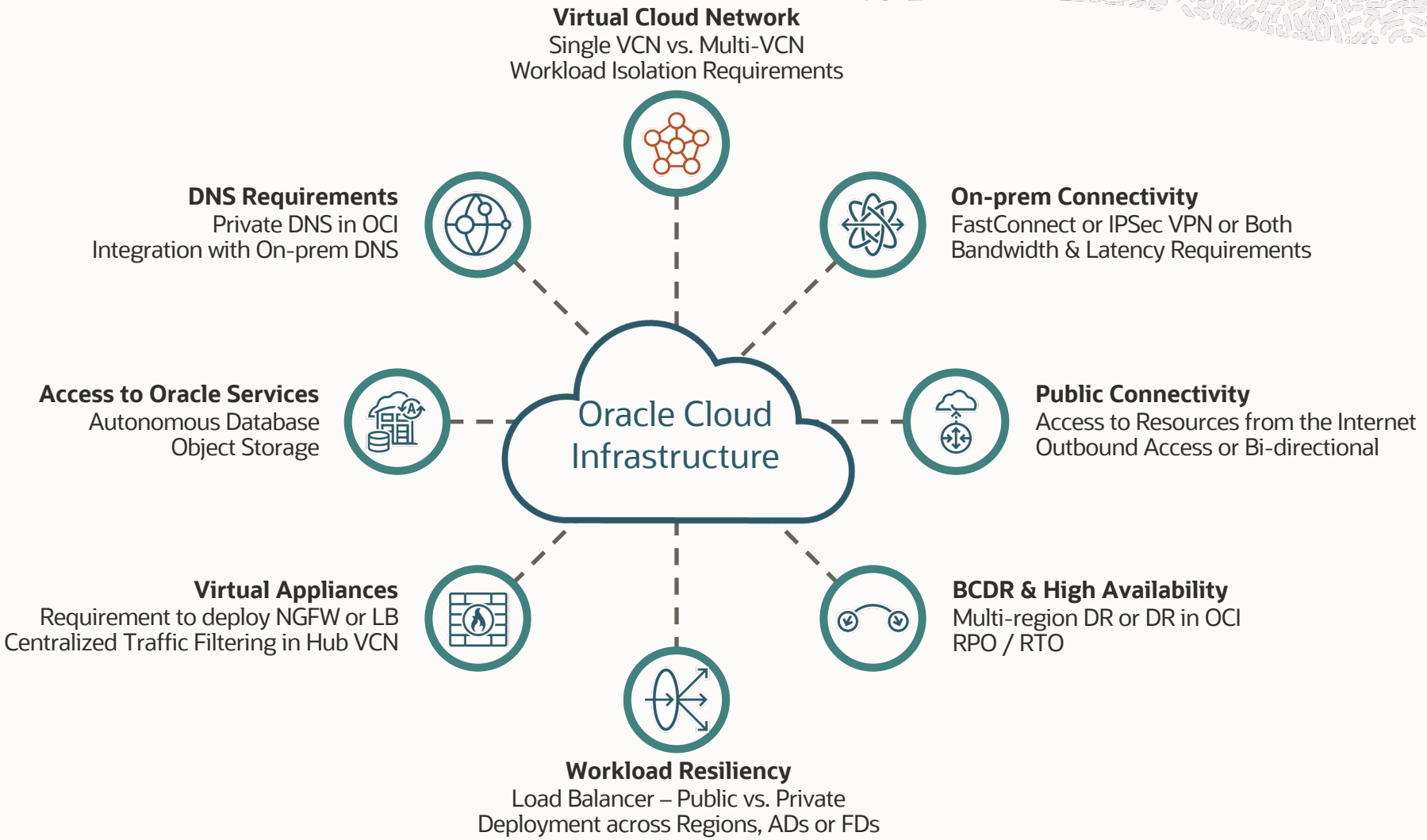
Cloud Networking Workshop

Agenda

- Introduction
- Architecting Cloud Networking for Workloads in OCI
- Cloud Network Architecture
- Virtual Cloud Network Specifications
- Workload Communication Requirements
- Workload Connectivity Requirements
- Workload Resiliency Requirements
- DNS Requirements

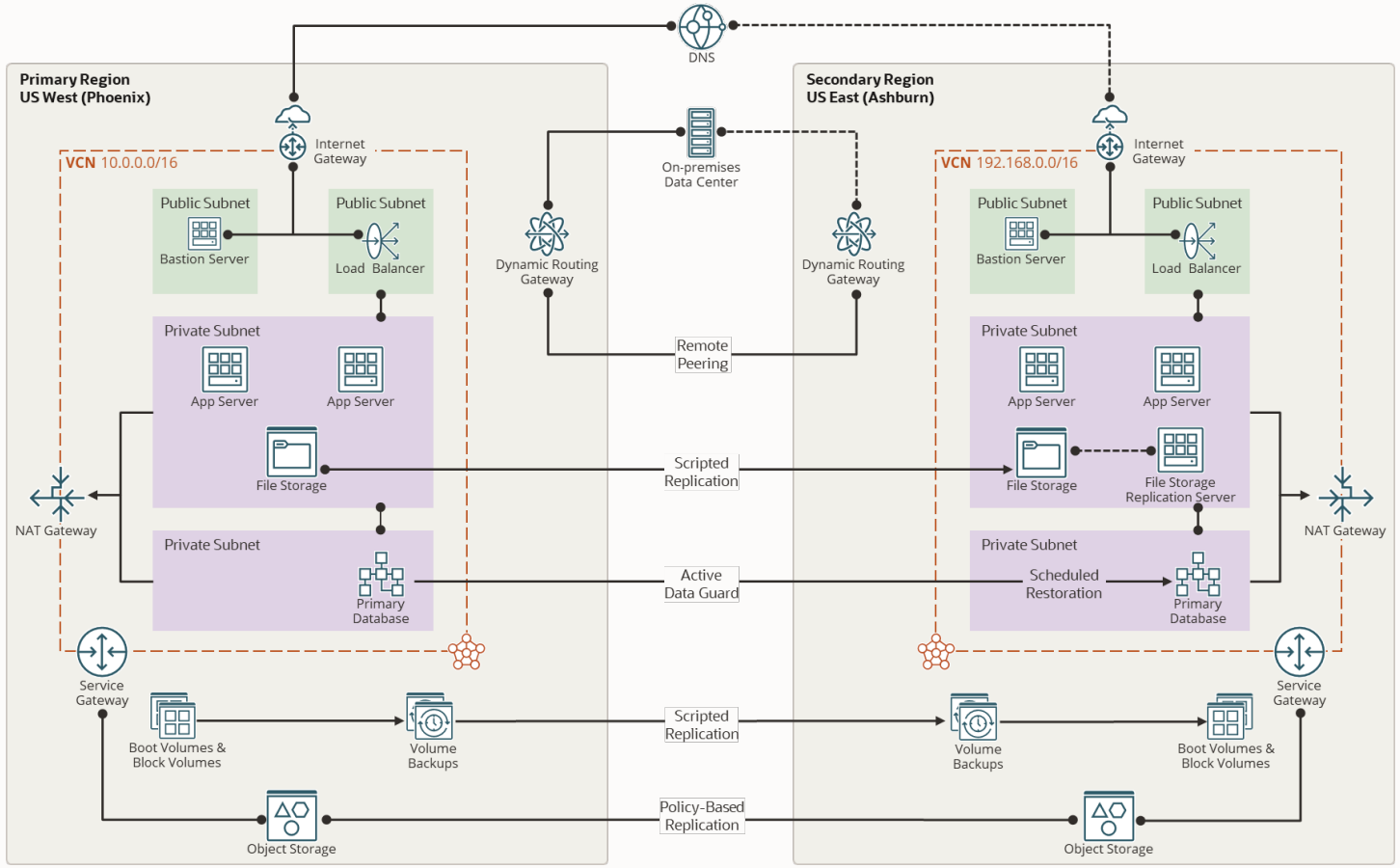
Architecting Cloud Networking for Workloads in OCI

Key Design Decisions



Architecting Cloud Networking for Workloads in OCI

Creating a Final Picture for your Networking & Connectivity



Virtual Cloud Network(s)

- Network Topology – Single VCN vs. Hub-Spoke
- Communication – Internet, Oracle Services

Security

- Network Security Groups & Security Lists

Connectivity

- Hybrid Cloud & Multi-cloud Architecture

DNS

- Private DNS
- Traffic Management

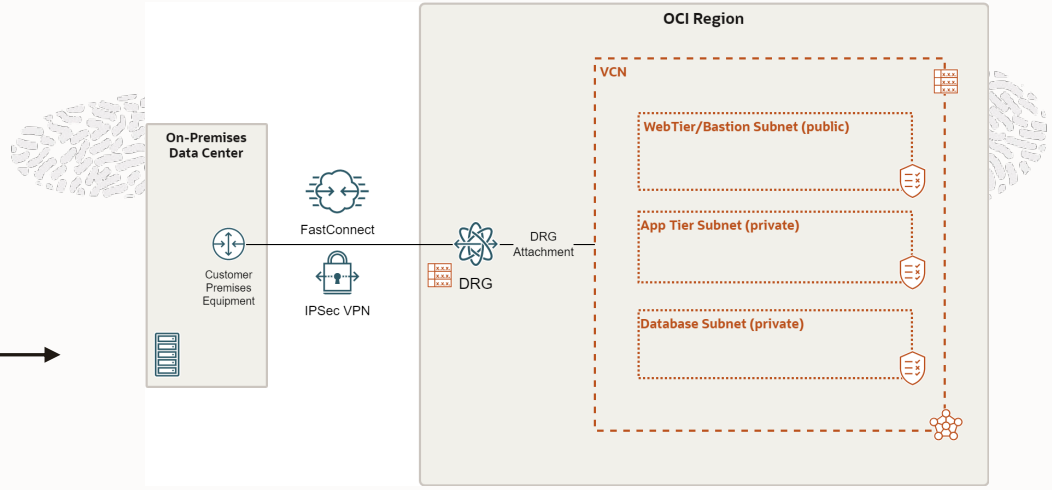
Monitoring

- Metrics
- Logging

Cloud Network Architecture

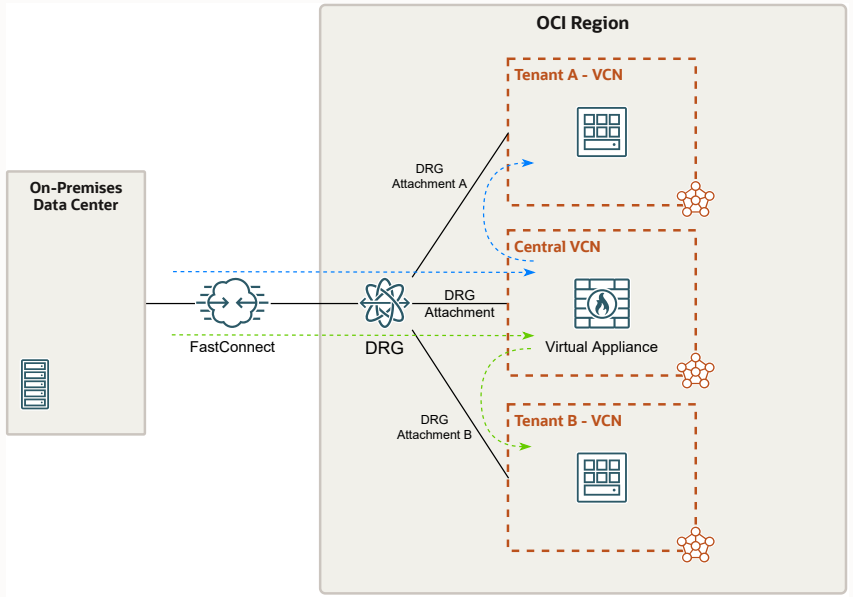
Design Decision: Virtual Cloud Network Topology

- Is the purpose just PoC or quick test ?
- No requirement to put a firewall between on-premise and OCI or between VCNs
- No or limited plans to expand with several VCNs



Single network architecture

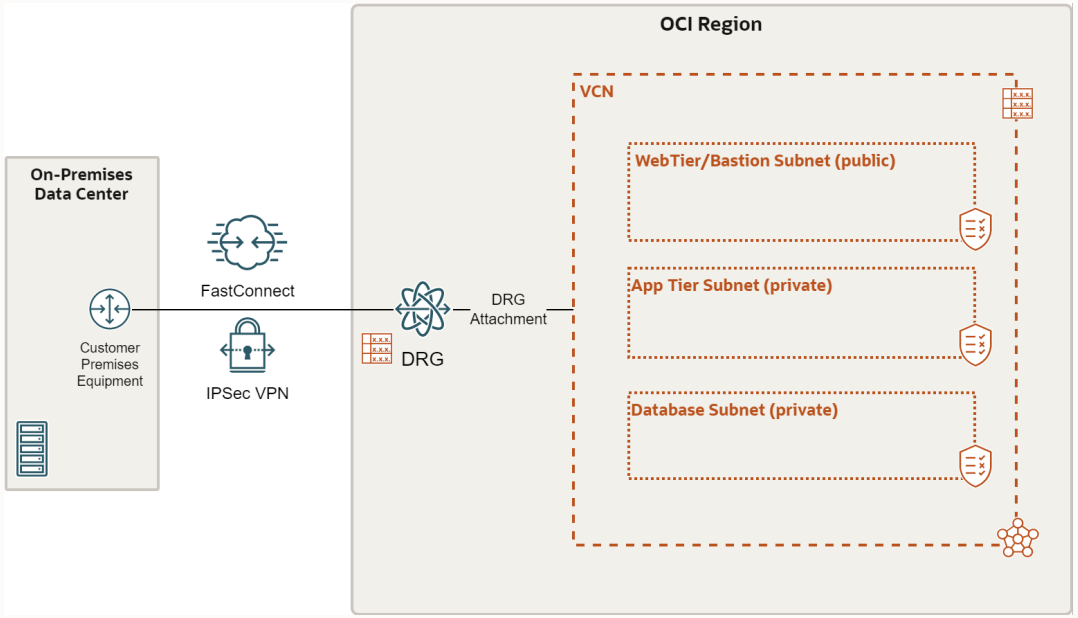
- Might your deployment get expanded in the future ?
- Will the deployment span several VCNs ?
- Do you have/might get requirement to implement firewall software between on-premise and OCI or between VCNs?
- Do you need to separate VCNs due to regulations ?
- Will you host customers with VCNs separation ?
- Separation of production, test and development environment



Hub/spoke network architecture – this is our recommended option
This picture shows different tenancies, but can be same

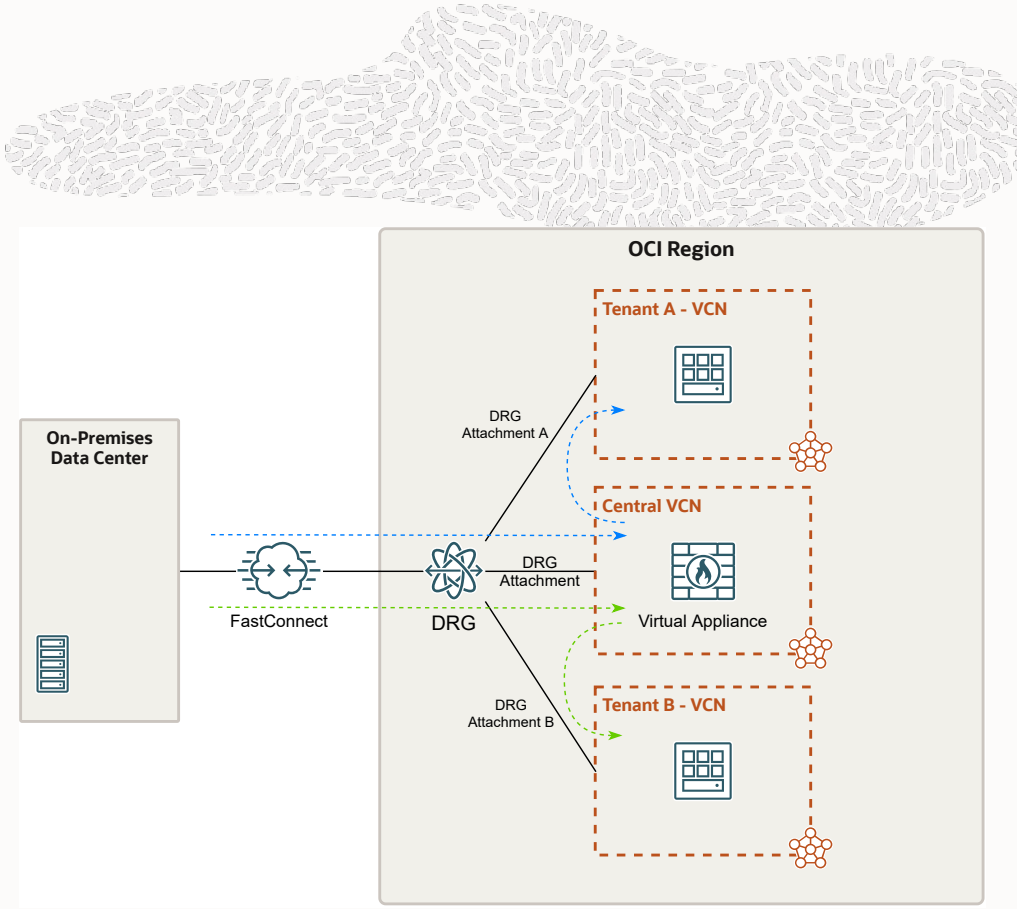
Cloud Network Architecture

Single VCN vs. Hub-Spoke Topology



Single network topology

- Quick deployment



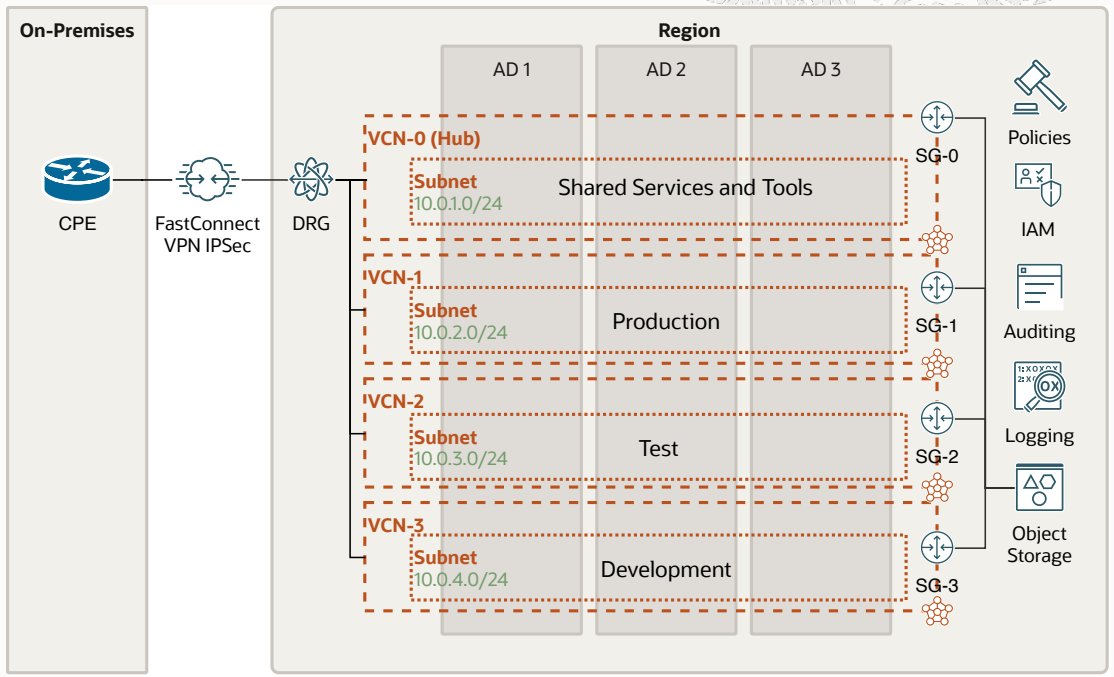
Hub & Spoke network topology

- Flexible solution
- Transit routing capable with firewall in hub VCN
- Recommended as standard deployments

Virtual Cloud Network Specifications

Design Decision: IP Addressing & Workload Accessibility

- Maximize the use of Availability Domains for HA design
- In a region with one AD, use Fault Domains
- Use regional subnets which spans all Availability Domains in a region
- Separate VCNs for different workloads



- Size your VCNs/subnets so expansion can happen
- Choose IP address range that don't overlap with on-premise or other networks customer might connect to
- Maximum 65000 IP within a VCN

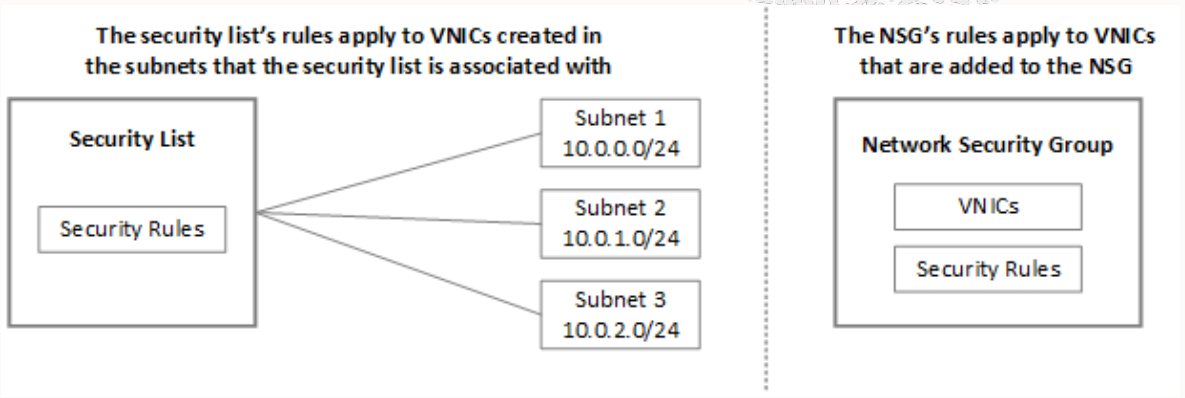
VCN Size	Netmask	Subnet Size	IPs/Subnet	Total Subnets	Total IPs
Small	/24	/27	29	8	232
Medium	/20	/24	253	16	4,048
Large	/18	/22	1,021	16	16,336
Extra Large	/16	/20	4,093	16	65,488

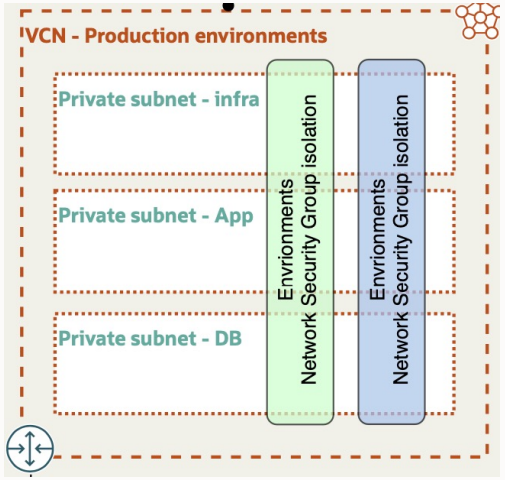
Example of combinations of VCN size, subnet size and usable IPs

Virtual Cloud Network Specifications

Design Decision: IP Addressing & Workload Accessibility

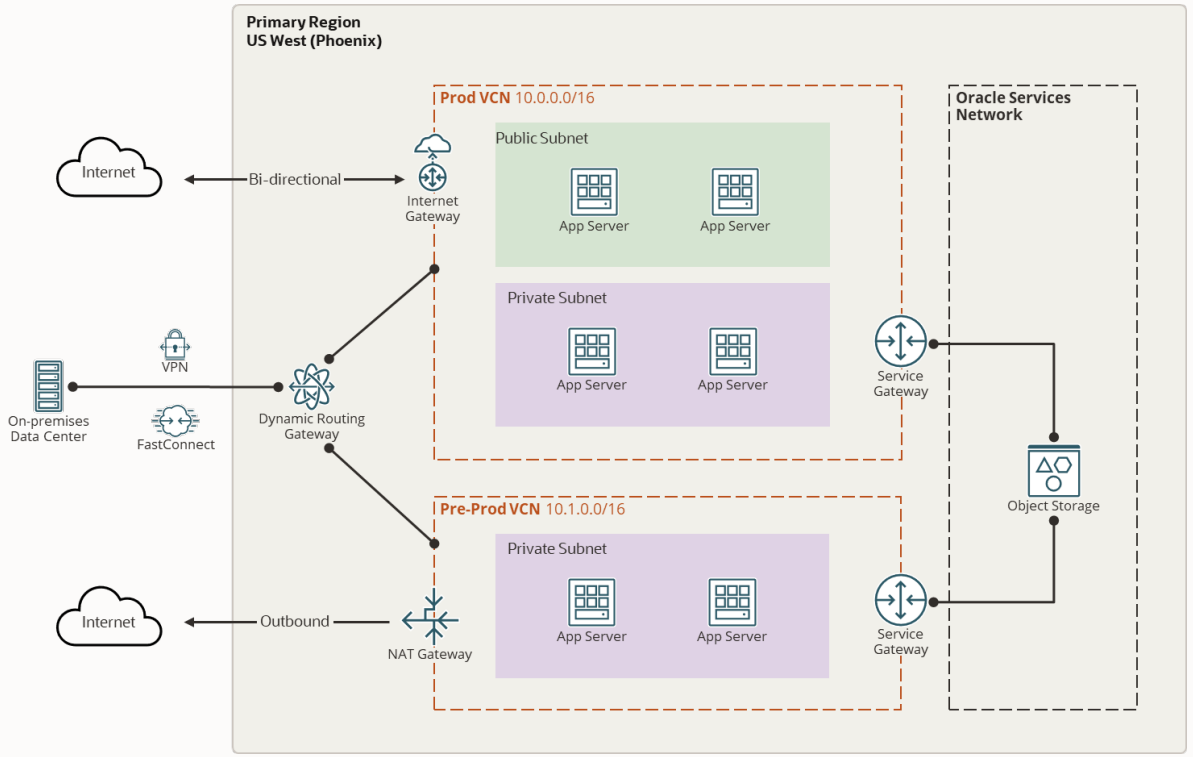
- Use **Security Lists** and/or **Network Security Groups** to control access to your resources in both private and public subnets.
- Security Lists are applied at subnet level
- You can use NSGs to define a set of ingress and egress rules that apply to specific VNICs.
- Oracle recommend using NSGs rather than security lists because NSGs enable you to separate VCN's subnet architecture from the security requirements of your application
- Private subnets are recommended to have individual route tables to control the flow of traffic to other VCNs or on-premises





Workload Communication Requirements

Design Decision: OCI Communication Gateways

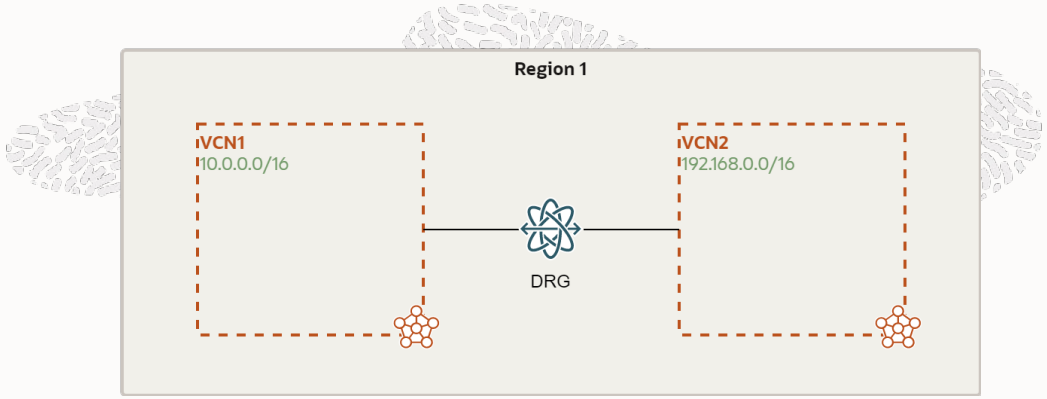


Feature	Gateway to use	Comments
Traffic in and out of OCI. Can be initiated from OCI or internet	**Internet Gateway**	Need to have a public subnet and a resource with public IP
Resources in OCI access internet securely	**NAT Gateway**	Use private subnet, cannot receive internet traffic initiated from internet
Access to Object Storage or other Service in Oracle Service Network (OS management Service, Oracle Linux Yum Service etc…)	**Service Gateway**	List of services is long https://www.oracle.com/cloud/networking/service-gateway/service-gateway-supported-services
Connection between OCI and on-premise and between VCNs.	**Dynamic Routing Gateway**	This is a virtual router that connect VCNs and on-premise locations together. Central connection point. Also between regions and different tenancies

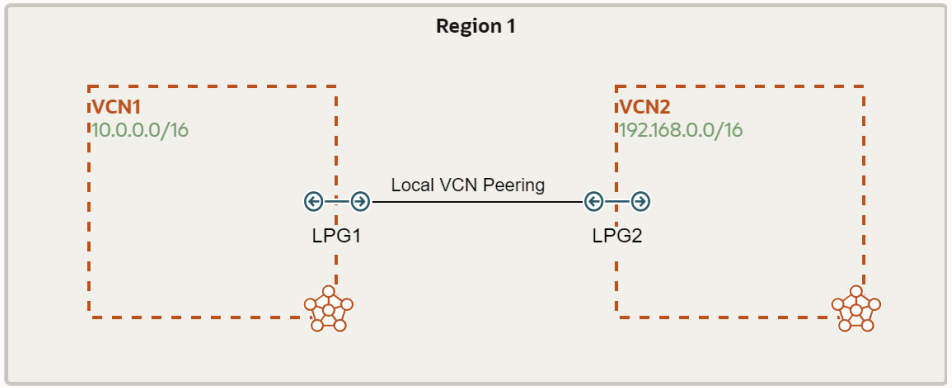
Workload Communication Requirements

Inter-VCN Connectivity

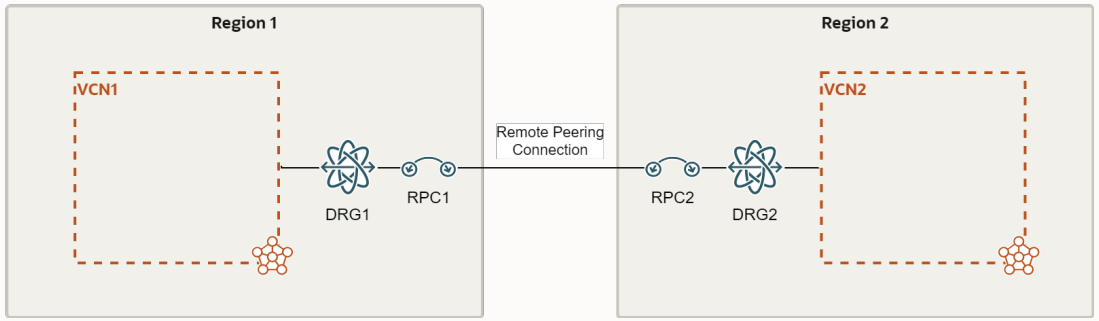
How to communicate between VCNs in OCI



DRG – Attach VCNs in same region



LPG – Local Peering Gateway



DRG – Attach VCNs between regions

- Connect two VCNs together either within same tenancy or different tenancies
- Need to be in the same region
- Max 10 LPGs per VCN

- Connect two VCNs together either within same tenancy or different tenancies
- Preferred method
- One DRG can connect up to 300 VCNs'
- Connect VCNs within same region or between regions

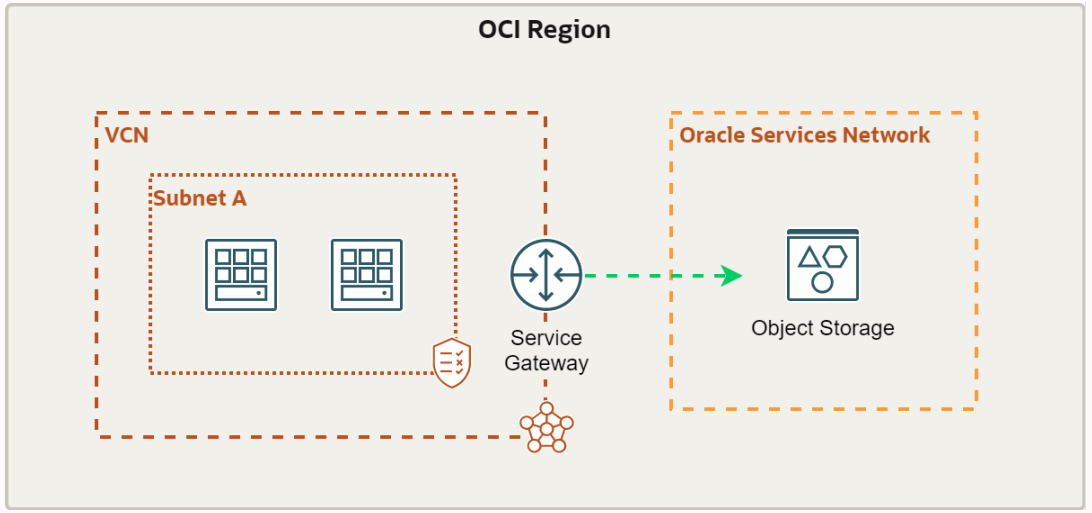
Workload Communication Requirements

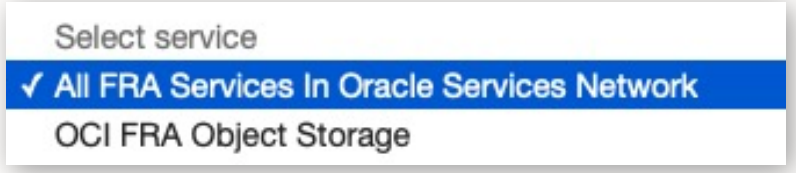
Accessing Oracle Services Network

- Oracle Services Network is a conceptual network in Oracle Cloud Infrastructure that is reserved for Oracle services.
- These services have public IP addresses that you typically reach over the internet. However, you can access the Oracle Services Network without the traffic going over the internet, by using a **Service Gateway** from within a VCN

- When adding a route to Oracle Service Network, you need to decide if the network shall be able to use all Services or just access to Object Storage.

- Object Storage is normally used for backup purposes, e.g Oracle DB backups



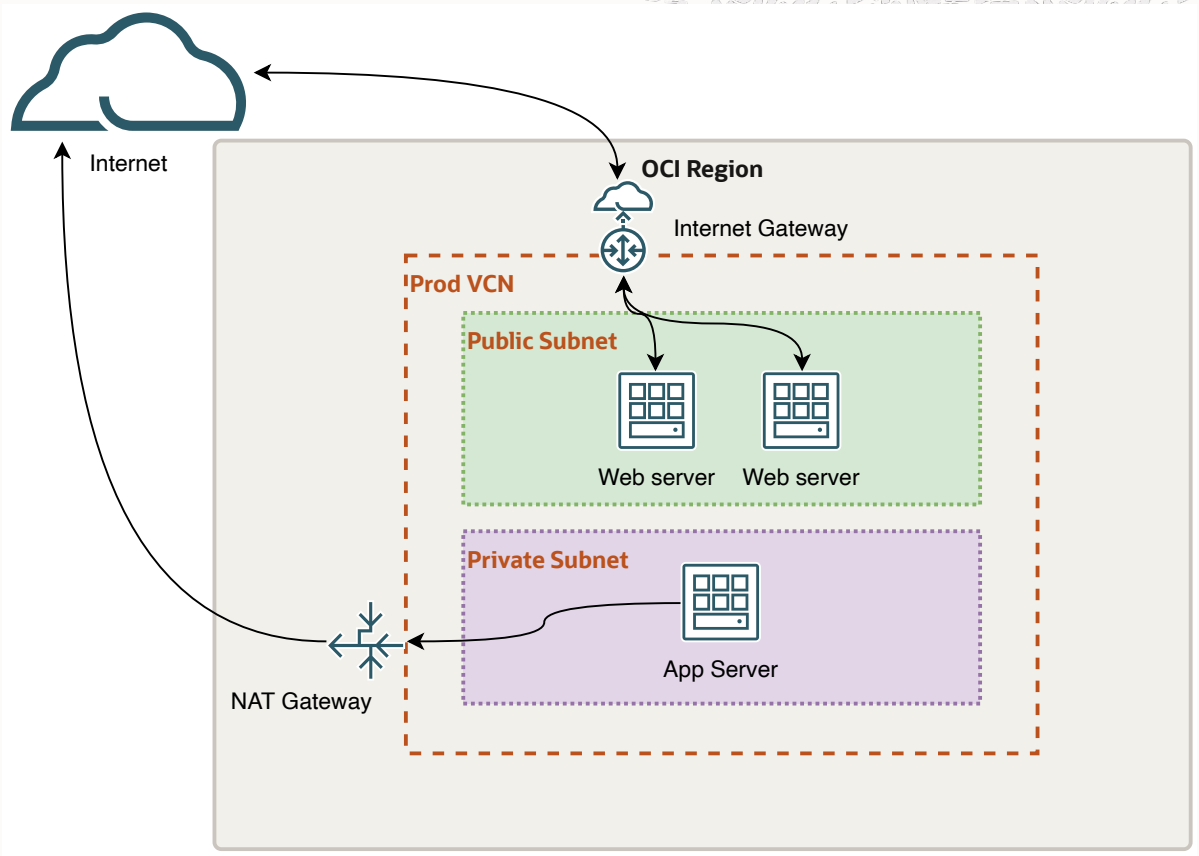


Workload Communication Requirements

Internet Connectivity

- **Internet Gateway** is used for allowing incoming traffic to OCI from internet. Need to use a public subnet and resurces that shall receive the traffic needs to have a public IP address

- **NAT Gateway** is used for instances that needs to reach internet securely, from a private subnet. Can be OS updates. Cannot initiate traffic from internet through NAT Gateway.

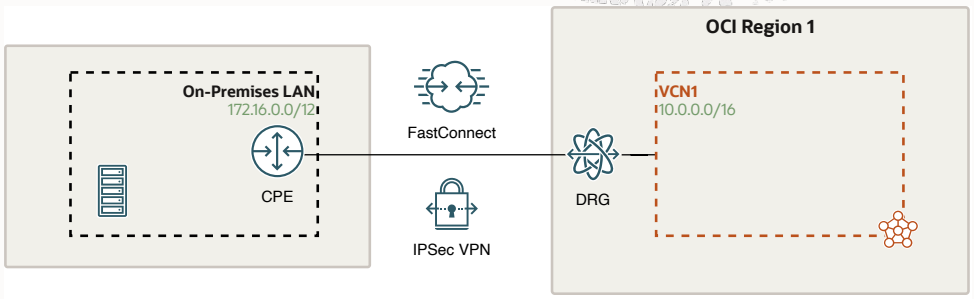


Workload Connectivity Requirements

Design Decision: Hybrid Cloud & Multi-cloud Architecture

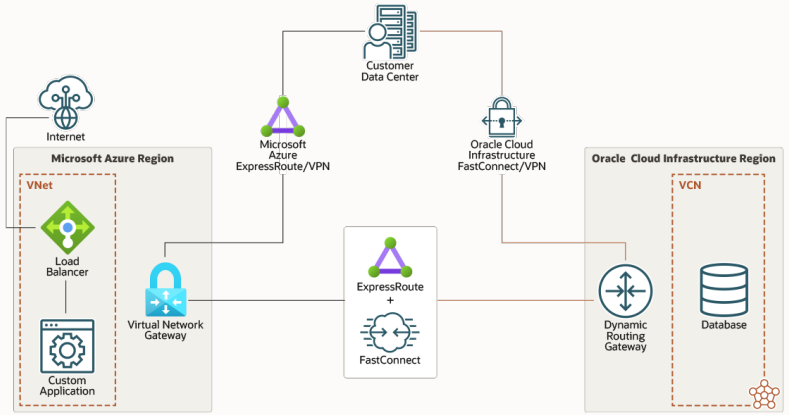
- Site-to-site VPN
  - uses normally internet as carrier (can use FastConnect as well)
  - bandwidth/latency can vary
  - can have, and recommended to use redundant tunnels

- FastConnect
  - uses dedicated connection
  - fixed bandwidth/latency
  - can have, and recommended to use redundant connections



Example : Connecting On-premise DC to OCI with IPSec or FastConnect

- Evaluate bandwidth requirements for the connection
- Latency are important for good user experience (for response times)
- Oracle and Micorsoft Azure has integrations points in different locations around the world to make it easy to integrate but also with very short latency which makes it possible to have solution that spans between the clouds. FastConnect/ExpressRoute is used in this scenario
- Possible to use FastConnect as primary and Site-to-Site VPN as backup connection
- Possible to connect to other clouds with both Site-to-Site VPN and FastConnect

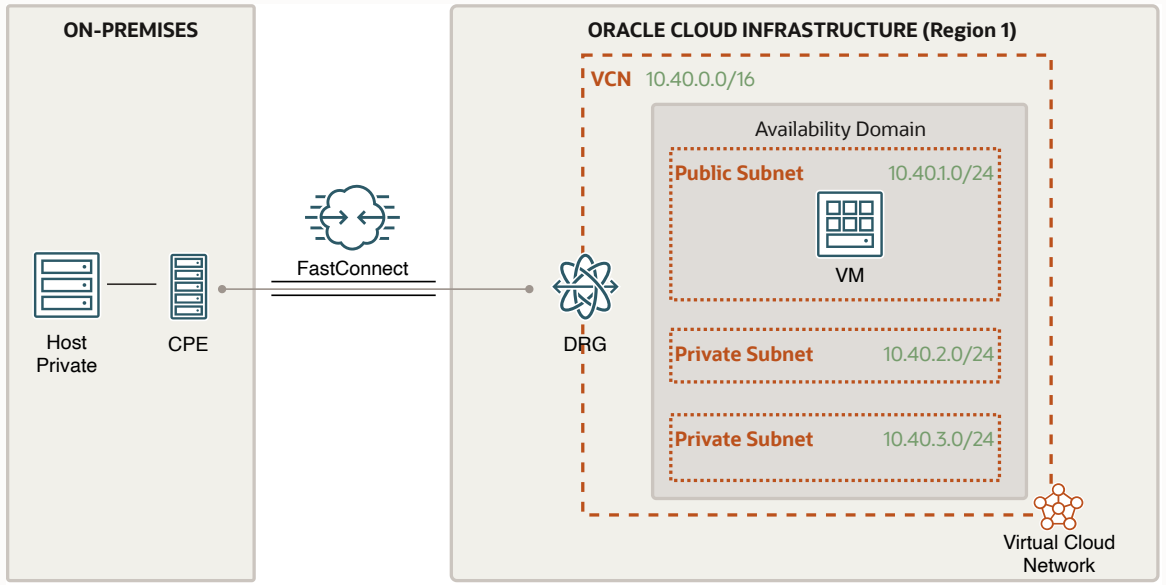


Example : DB in OCI and Application/Load balancer in Azure

Workload Connectivity Requirements

Connectivity to On-premises Networks – FastConnect

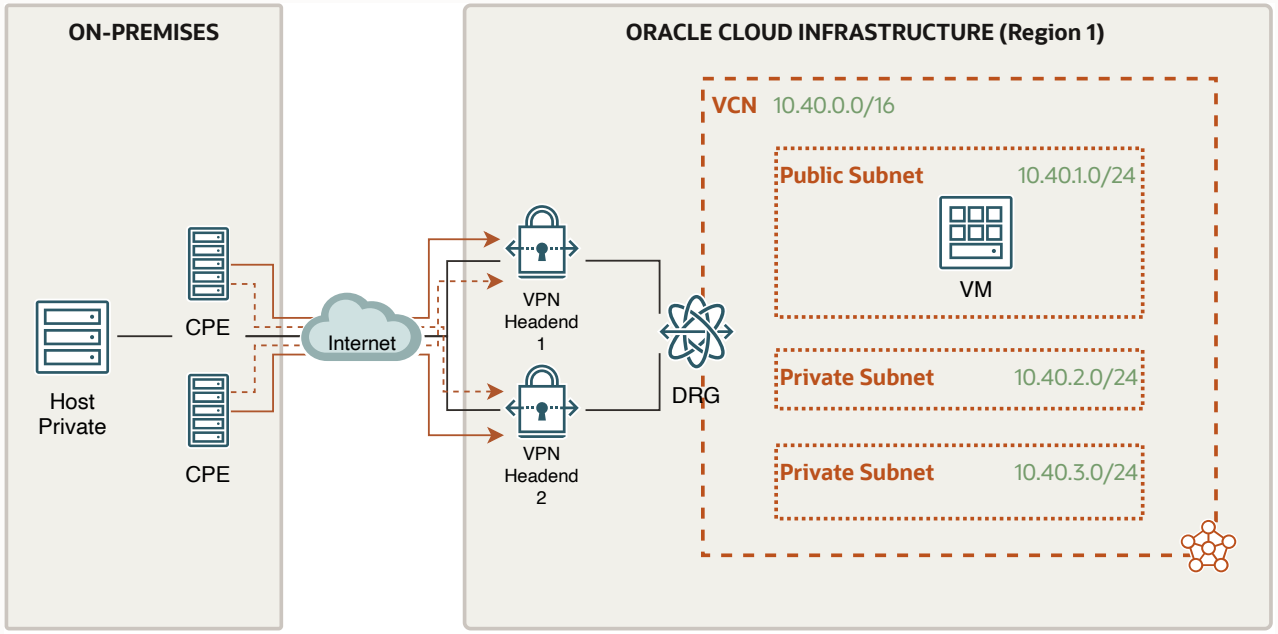
- When a dedicated connection between on-premise and OCI are needed. Traffic does not go over public internet
- Can be public peering – if need direct access to Oracle Service Network only or want to use IPSec VPN on top of FastConnect for encryption of traffic
- Private peering is normally what customer use Connect to private resources in OCI (VCNs)
- Can also be a combination of both above
- Connection speed is : 1Gbps, 10Gbps, 100Gbps
- Recommended to use 2x for redundancy



Workload Connectivity Requirements

Connectivity to On-premises Networks – Site-to-Site VPN

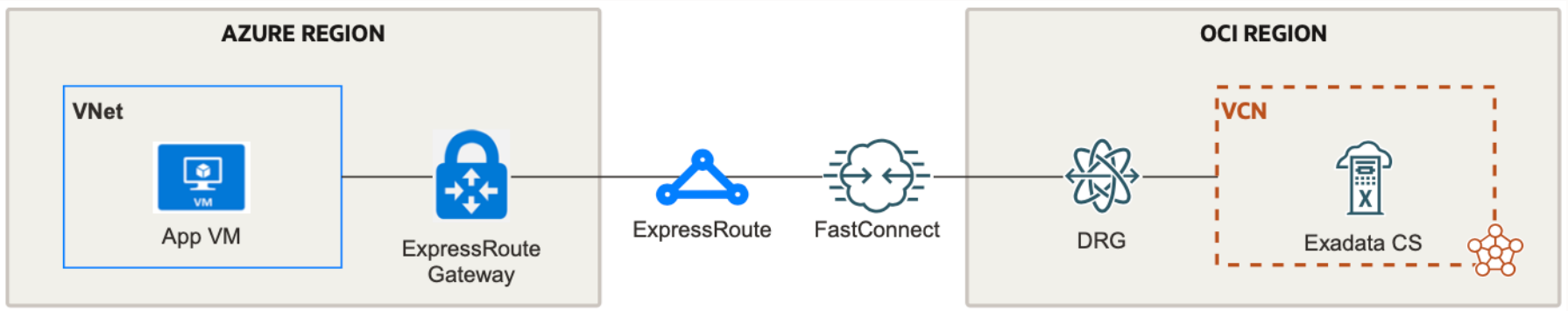
- Connects on-premise DC to OCI via an encrypted link (IPSec)
- Can also be used for connecting OCI to other CSPs
- Site-to-site VPN uses the internet as carrier (performance may vary depending on internet traffic) and encrypt the traffic with IPSec protocol suite
- Can be an alternative to FastConnect if bandwidth fluctuation does not cause issue
- Cannot scale to the same bandwith as FastConnect
- Can be used as a backup for FastConnect.
- The service is a no cost and is built into our cloud tooling to make is easy to setup



Site-to-Site VPN with redundant Customer-Premises Devices

Workload Connectivity Requirements

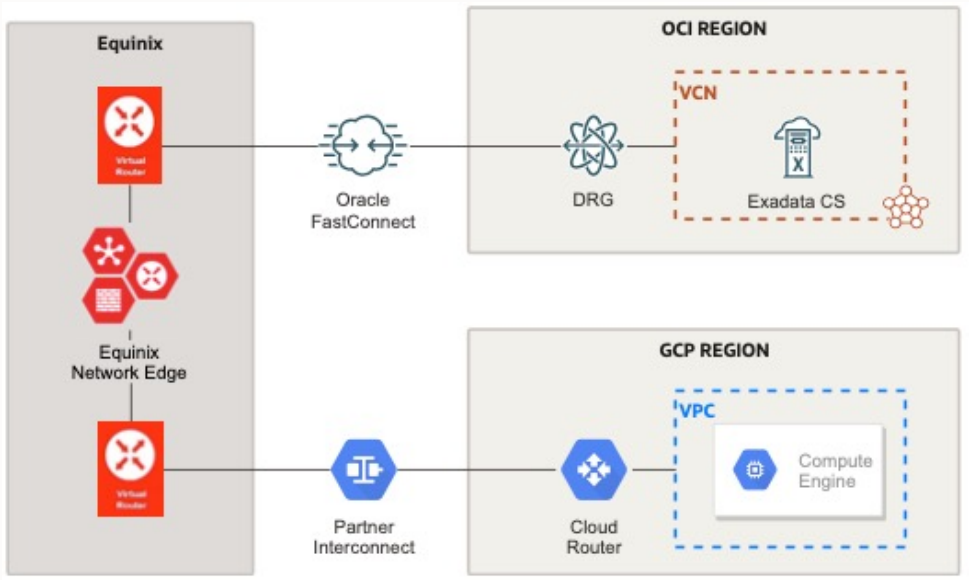
Connectivity to Other Public Clouds – OCI-Azure Interconnect



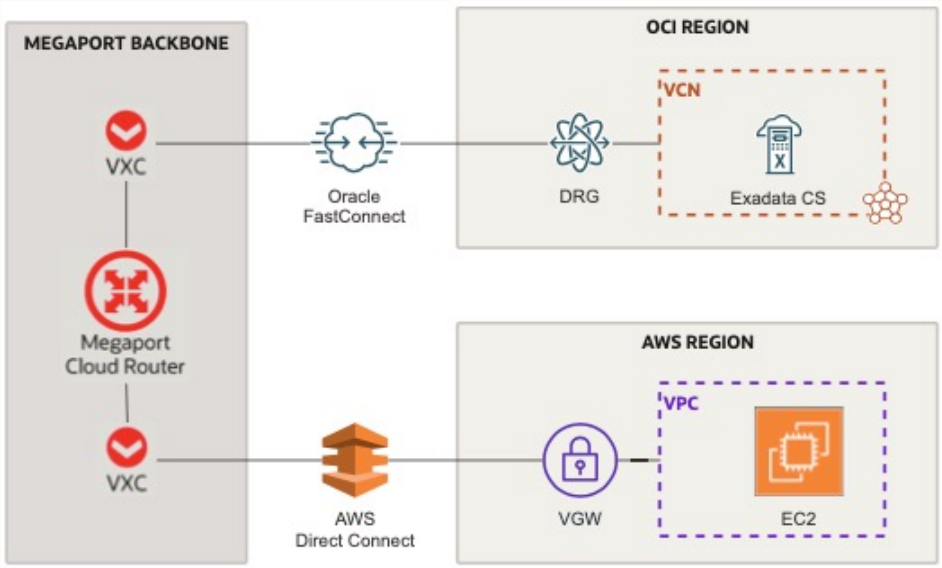
- Microsoft and Oracle have a partnership with pre-integration of Azure with OCI in several regions
- Only need to enable access between the clouds by enable it from both sites/console using FastConnect and ExpressRoute
- No network service provider in between
- Only need to set up 1x Virtual Circuit since it has built-in redundancy (different from standard FastConnect)
- No cost for traffic between Azure – OCI
- Low latency
- Not all regions have this capability, can use Network Service provider in other regions
- https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/azure.htm

Workload Connectivity Requirements

Connectivity to Other Public Clouds – AWS & GCP



Connection OCI - GCP



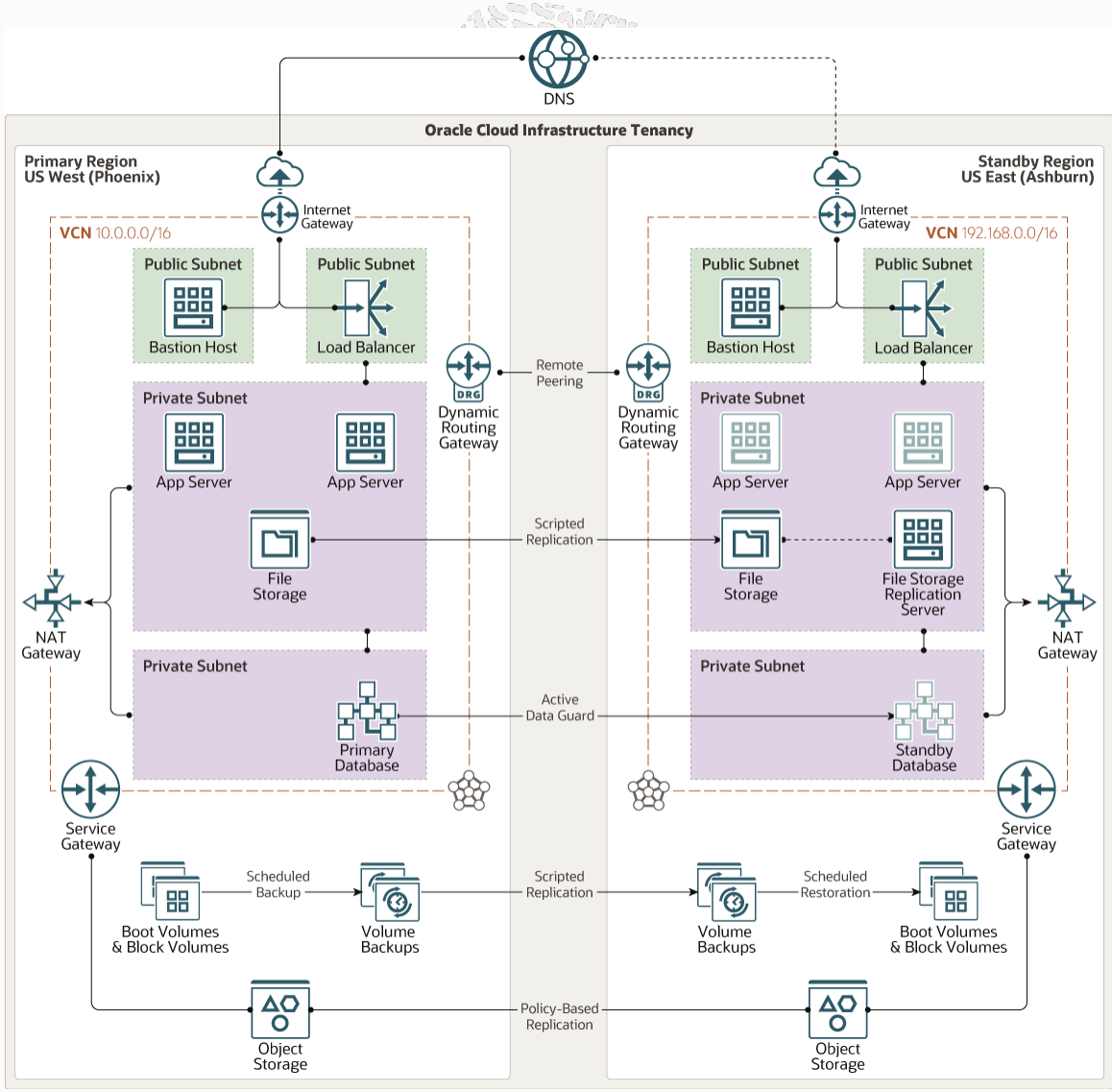
Connection OCI - AWS

- Connections to other cloud from OCI is quick and easy to establish through our FastConnect partners
- In the above pictures we show two of our largest connectivity partners, Equinix and Megaport

Workload Resiliency Requirements

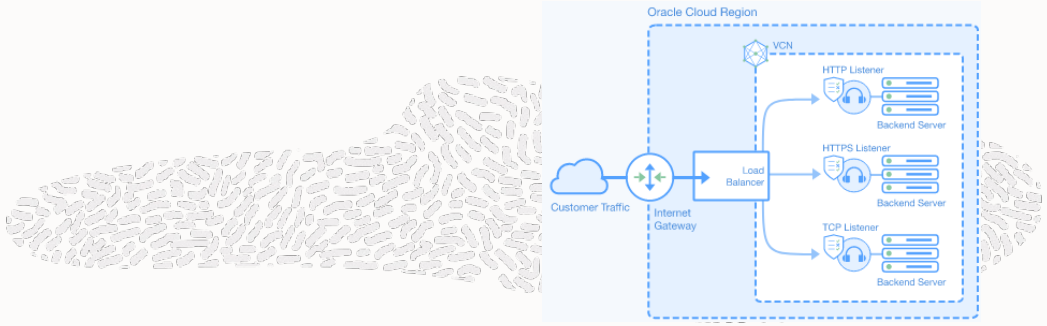
Design Decision: Multi-region Deployment

- If need to have resiliency from a complete region outage, consider multi-region deployment
- Cross regional replication for block volume/object storage
- Data Guard replication for database
- Setup same set of resources in second region
- Remote peering between DRGs to enable traffic between different regions utilizing OCI network backbone
- Replicate data and necessary content that needs to be used for running the solution, to secondary region



Workload Resiliency Requirements

Design Decision: Load Balancing



A Load Balancer distribute traffic to several backend servers

Web browser

Normal IP traffic between applications

Layer 4/7, TCP/HTTP layer

Flexible Load Balancer

Layer 4, TCP/UDP, transport layer

Network Load Balancer

Public Load Balancer
Public IP and accessible from internet

Private Load Balancer
Private IP and accessible from within VCN

Public Load Balancer
Public IP and accessible from internet

Private Load Balancer
Private IP and accessible from within VCN

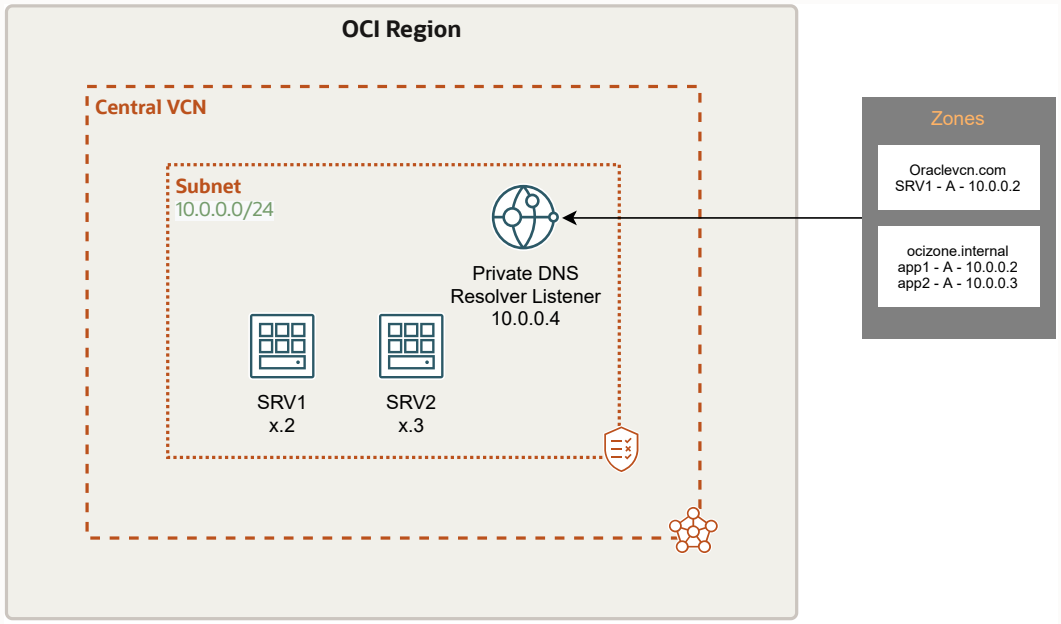
- Can terminate SSL traffic on load balancer or pass it through to backend
- Standard Load balancer for public facing web servers
- Directly apply WAF (Web application Firewall) protection onto Flexible Load Balancer
- Flexible shape will use between Min and Max bandwidth depending on traffic, lower cost if less traffic

- Non-proxy, pass through load balancing
- High throughput and ultra low latency
- Optimized for long-running connections (days or months)
- A connection always goes to same backend server – good for DB
- Scales up and down automatically based on client traffic, no bandwidth config needed
- No SSL termination

DNS Requirements

Design Decision: Public vs. Private DNS

- **Public DNS Zones** hold the trusted DNS records that will reside on Oracle Cloud Infrastructure's nameservers. You can create public zones with publicly available domain names – reachable on internet (need to register with a DNS registrar).
- **Private DNS zones** contain domain names that resolve DNS queries for private IP addresses within a VCN
- You can create private zones to define your own domain name for private address resolution
- Can also combine VCNs for private DNS resolution over several VCNs



Private DNS for name resolution within OCI

Questions?

ORACLE