ORACLE

Oracle Cloud Infrastructure

Virtual Cloud Networking Basics

Sebastian Solbach
sebastian.solbach@oracle.com

November 2019

Our mission is to help people see data in new ways, discover insights, unlock endless possibilites.

Agenda

- Virtual Cloud Network (VCN) concepts
- Manage your cloud network components
  - Subnets, Route Table, Security Lists, Private IP, Public IP
  - Internet Gateway, NAT Gateway, Service Gateway
- OCI connectivity options
  - VPN, FastConnect
  - DRG, Local and Remote Peering
- Service Network Patterns

Virtual Cloud Network (VCN)

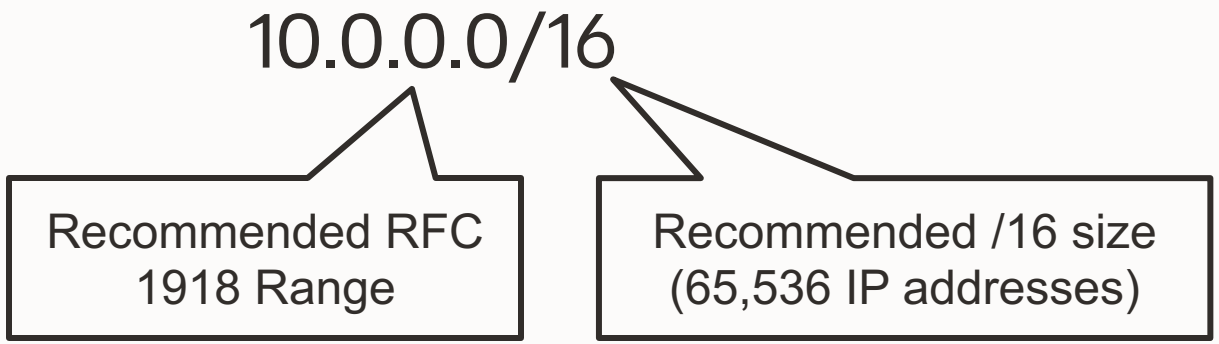
- Private network in the Oracle data centers, with
  - Firewall Rules
  - Communication Gateways

- A VCN covers a single, contiguous IPv4 CIDR block

- A VCN resides within a single region but can cross multiple Availability Domains

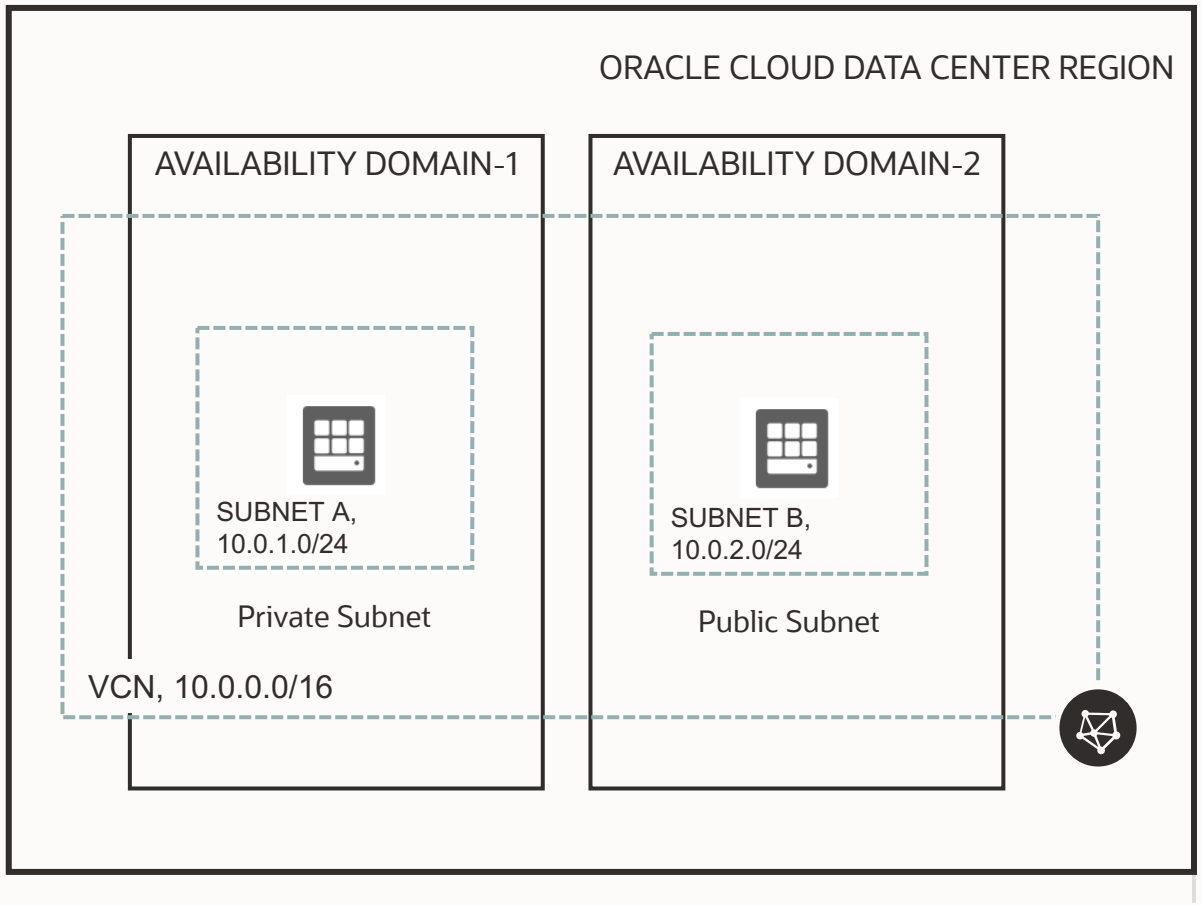
IP address range for your VCN

Avoid IP ranges that overlap with other on-premises or other cloud networks



- Use private IP address ranges specified in RFC 1918 (10.0.0.0/8, 172.16/12, 192.168/16)
- Allowable OCI VCN size range is from /16 to /30
- VCN reserves the first two IP addresses and the last one in each subnet's CIDR

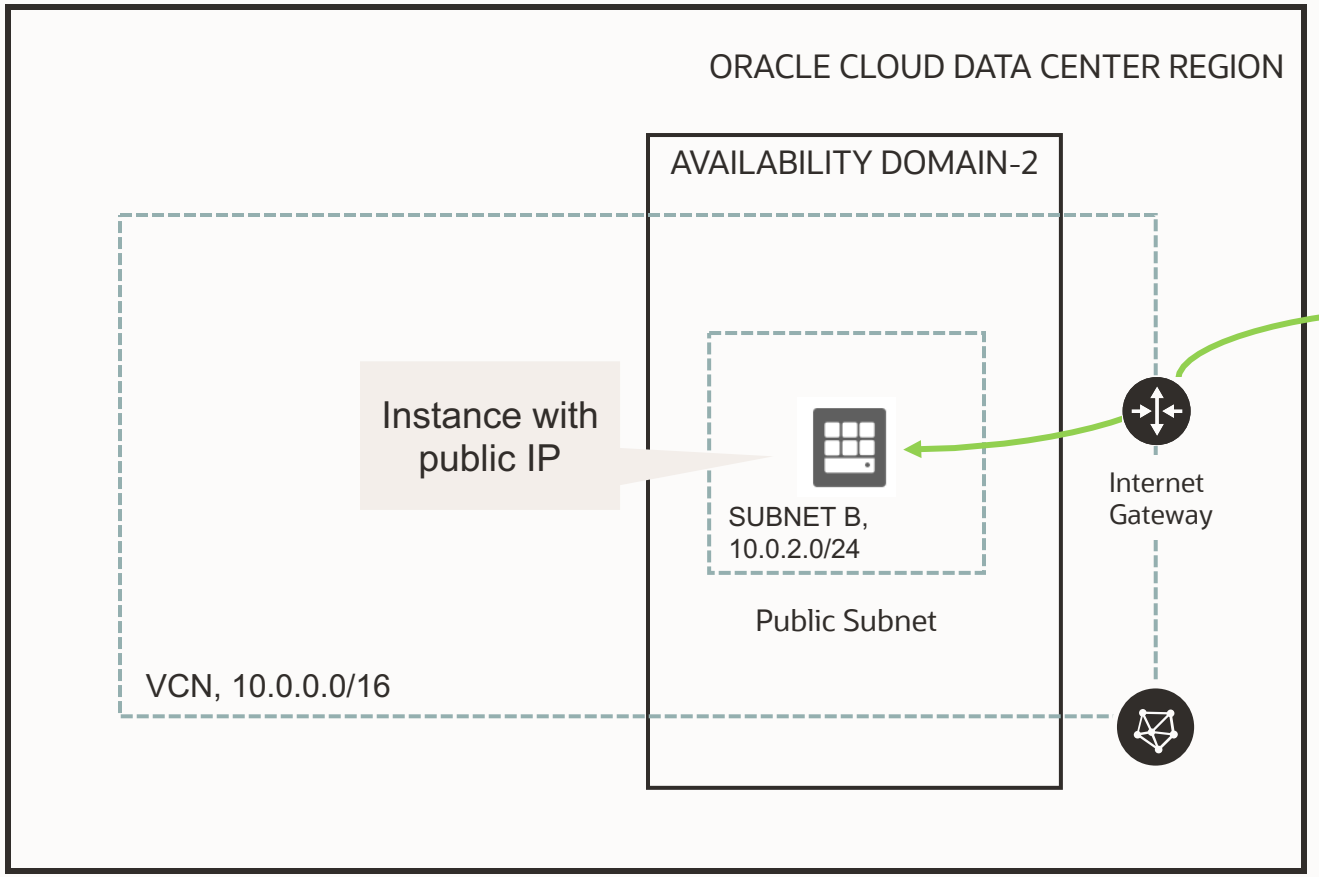
Subnet



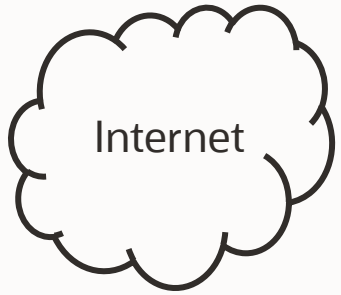
Each VCN subdivided into subnets:

- Contiguous range of IPs (CIDR)
- AD Local or Regional Subnets
- Subnet IP ranges cannot overlap
- Instances are placed in subnets
- Instances draw internal IP address and network configuration from their subnet
- Subnets can be designated as either
  - **Private** (vNICs with private IP)
  - **Public** (vNICs with both private & public IP)

Internet Gateway



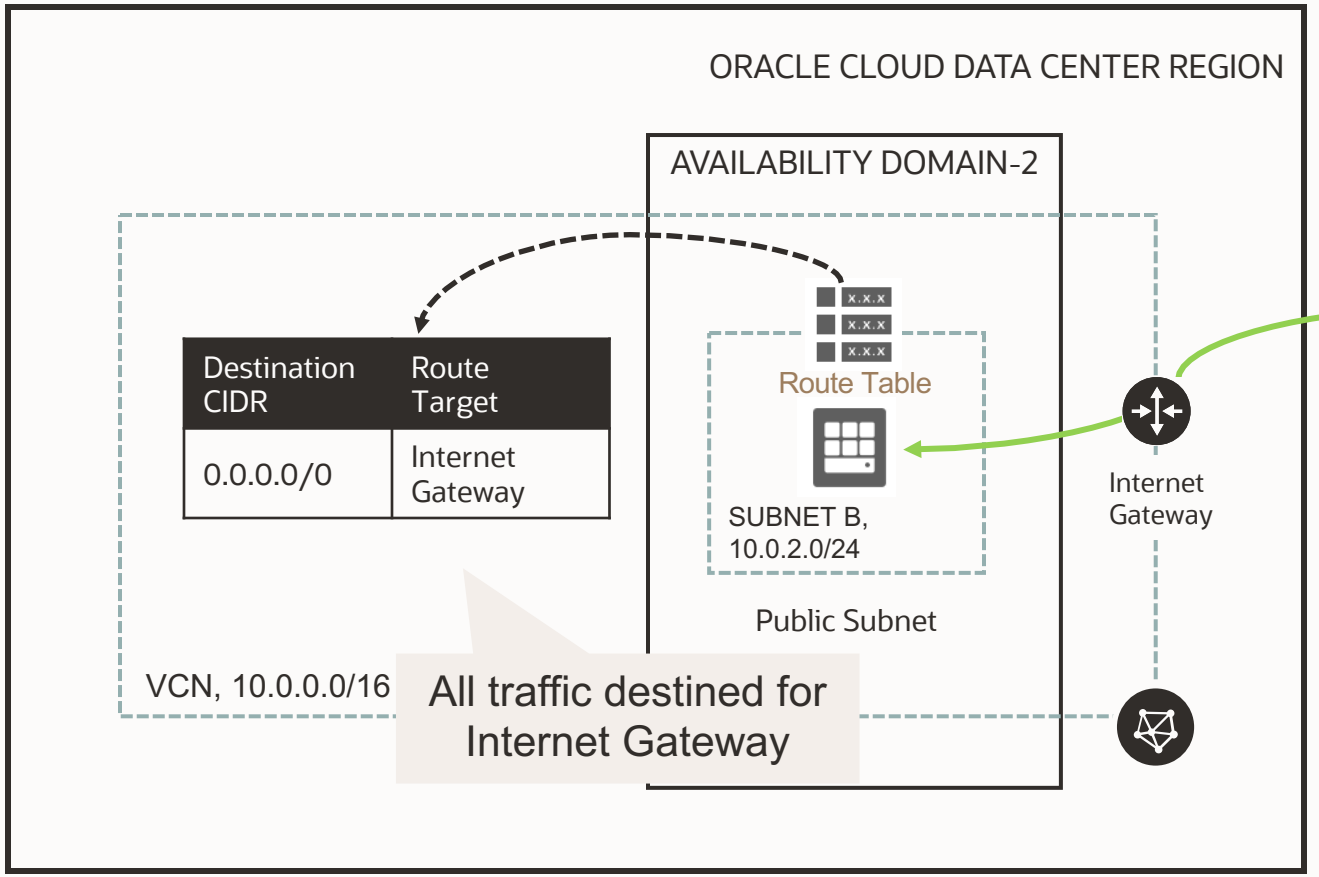
Internet Gateway provides a path for network traffic between your VCN and the internet



Only one internet gateway for a VCN

- Don’t forget to add a route for the gateway in the VCN's Route Table

Route Table

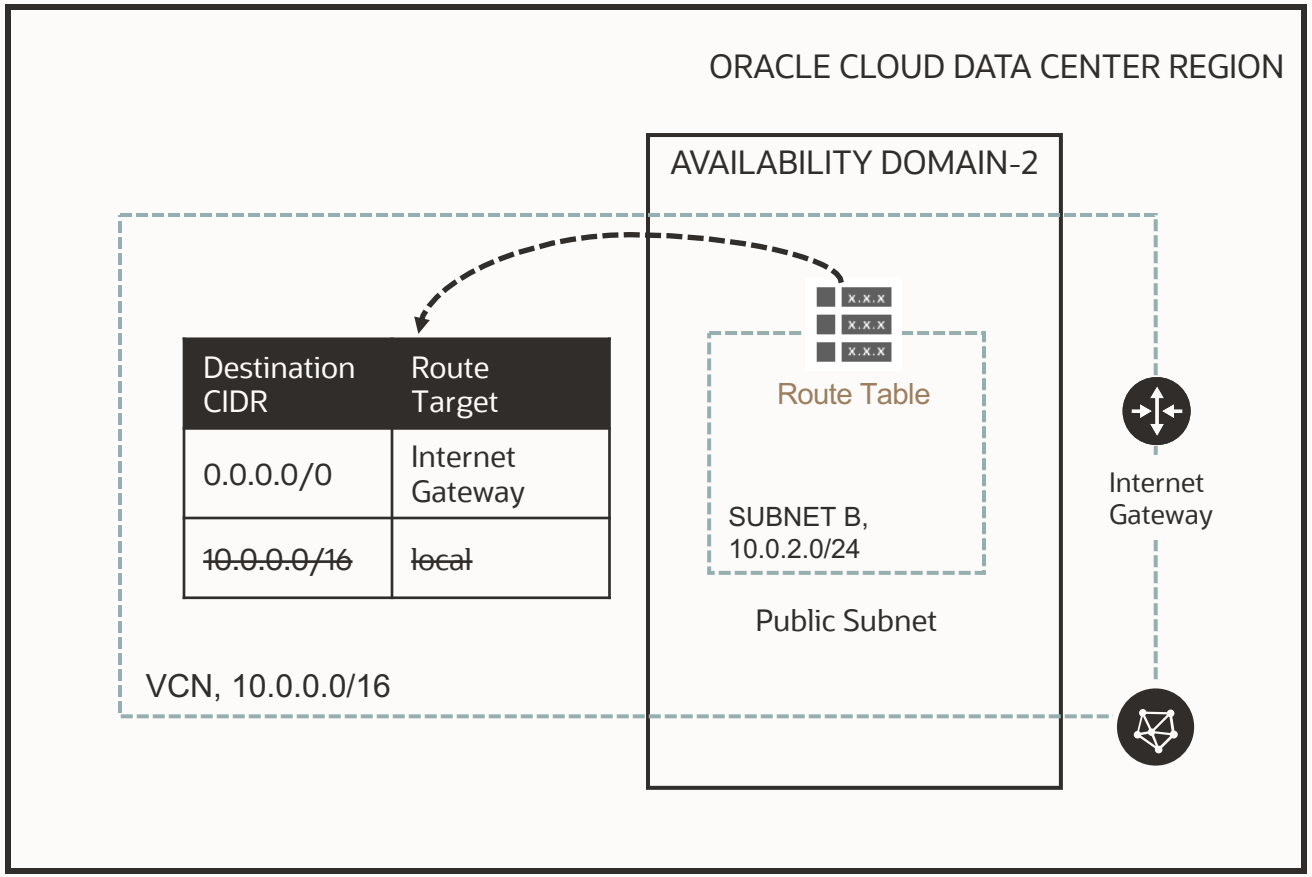


Route Table is used to send traffic out of the VCN

Consists of a set of route rules:

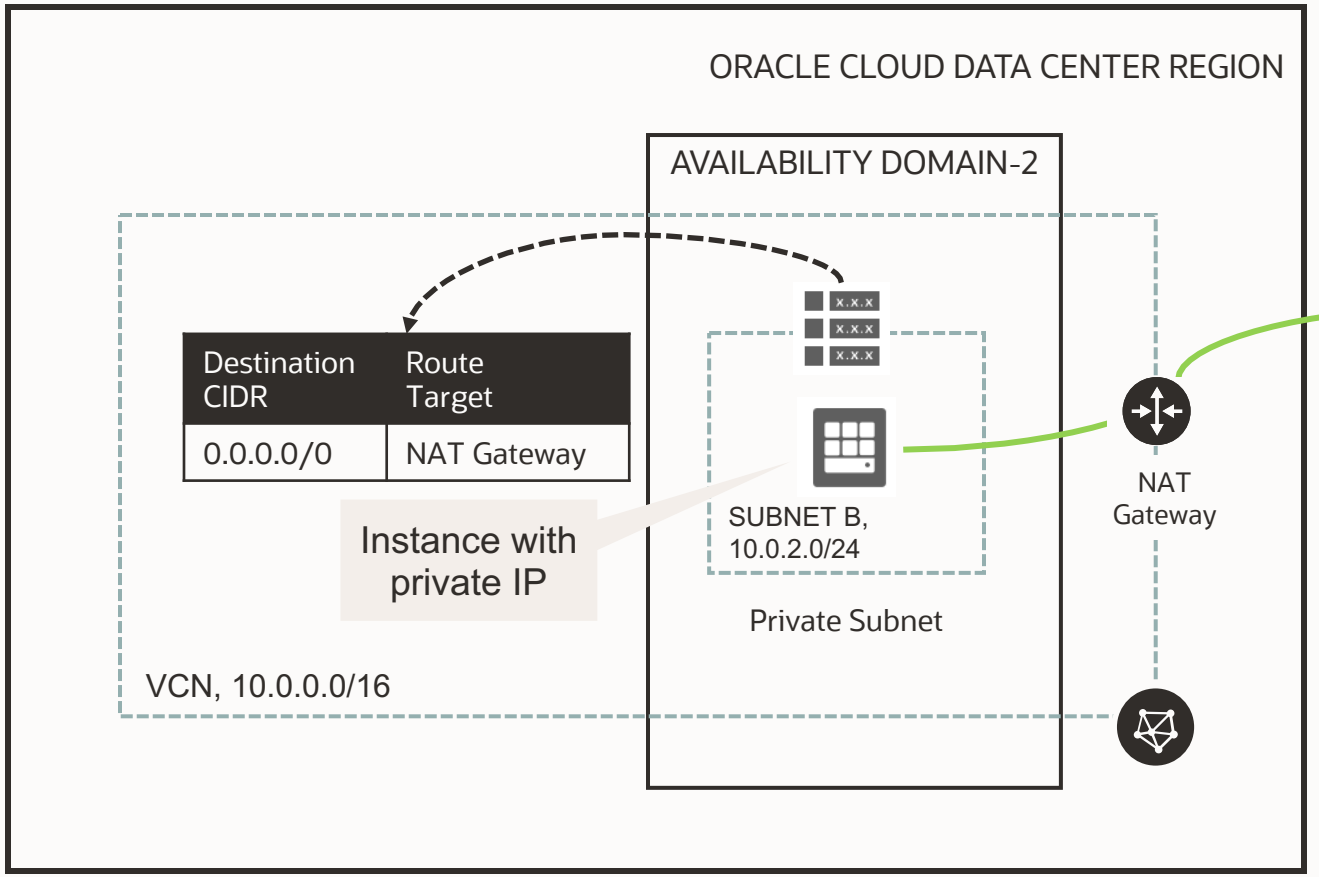
- Destination CIDR block
- Route Target (the next hop) for the traffic that matches that CIDR

Route Table



- Each subnet uses a single route table specified at time of subnet creation, but can be edited later
- Route table is used only if the destination IP address is **not** within the VCN's CIDR block
- No route rules are required in order to enable traffic within the VCN itself
- Update Route table for
  - internet gateway
  - NAT gateway
  - service gateway
  - dynamic routing gateway
  - peering connection
  - ...

NAT Gateway

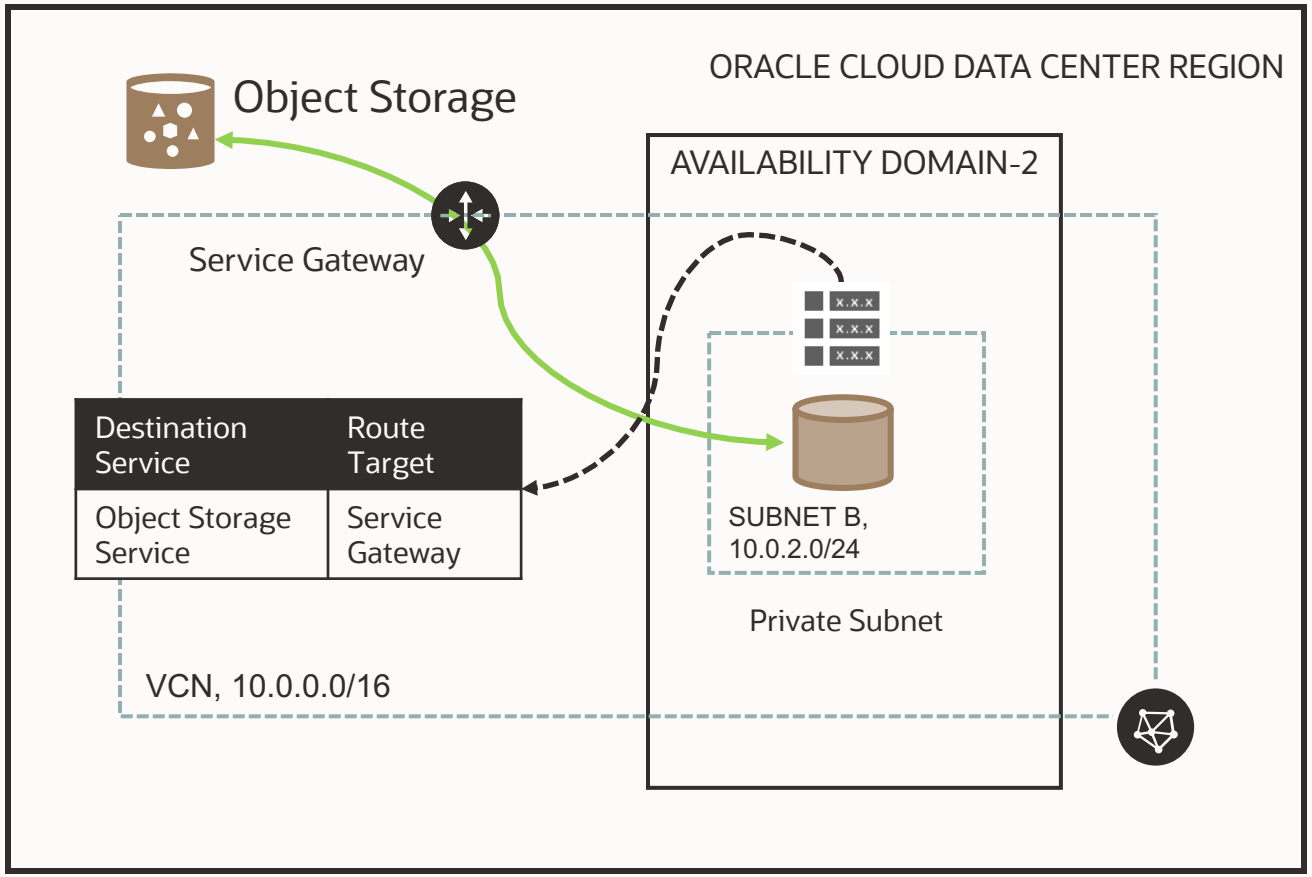


NAT gateway gives an entire private network access to the internet without assigning each host a public IP address

Hosts can initiate outbound connections to the internet and receive responses, but not receive inbound connections initiated from the internet. (Use case: updates, patches)

You can have more than one NAT gateway on a VCN, though a given subnet can route traffic to only a single NAT gateway

Service Gateway

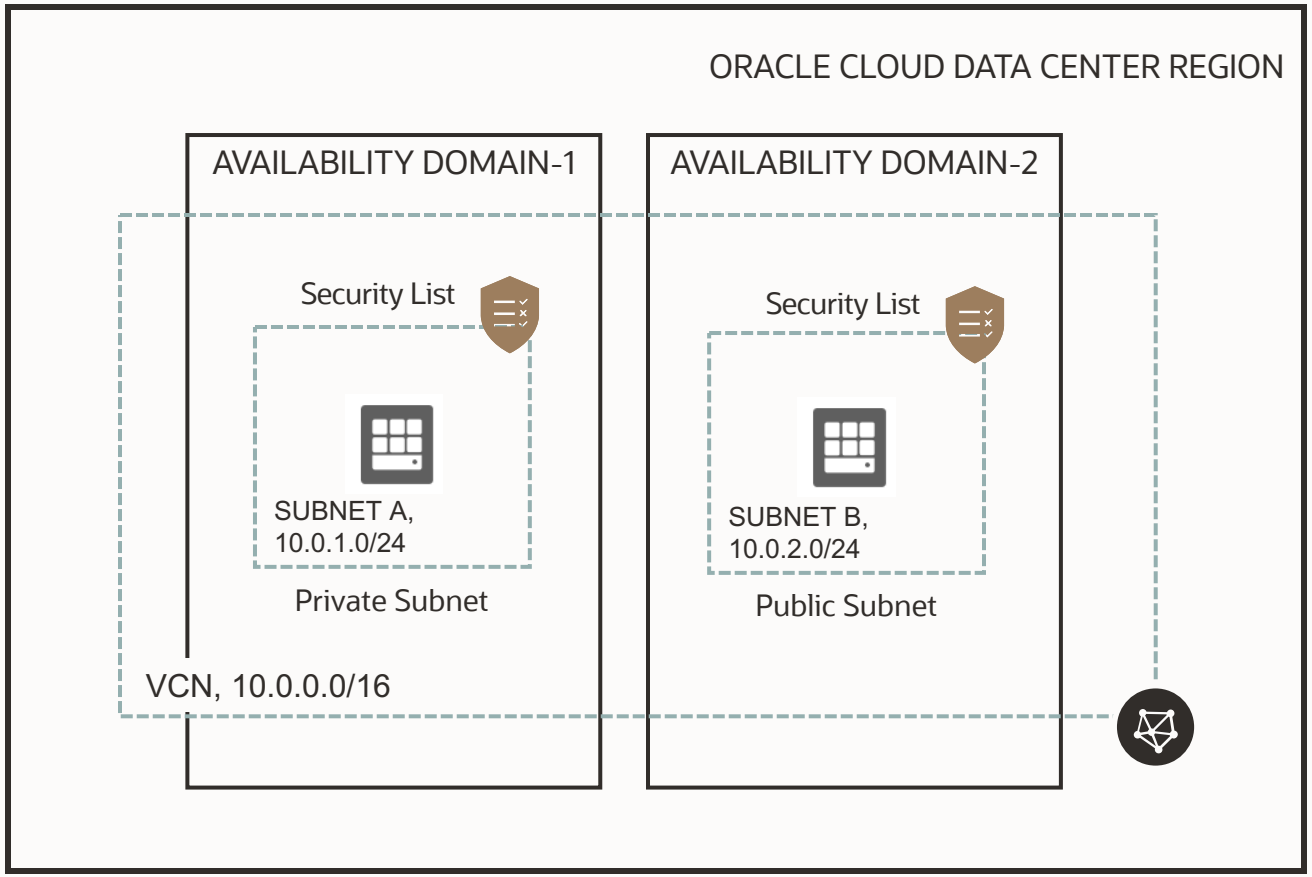


Service gateway lets resources in VCN access public OCI services such as Object Storage

Any traffic from VCN that is destined for one of the supported OCI public services uses the instance's private IP address for routing, travels over OCI network fabric, and never traverses the internet

- Back up DB Systems in VCN to Object Storage
- Access to Autonomous Database

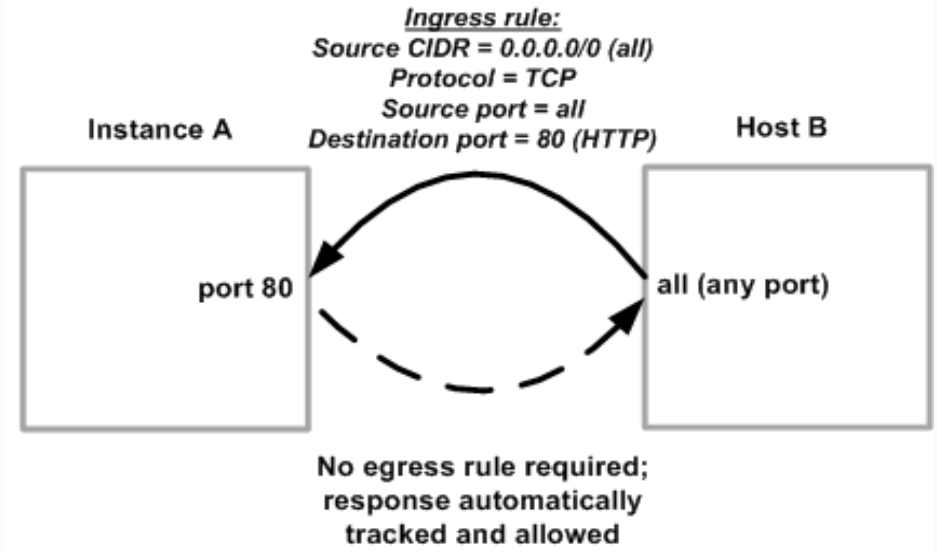
Security Lists / Network Security Groups (NSGs)



A common set of firewall rules associated with a subnet and applied to all instances launched inside the subnet

- Security lists provide ingress and egress rules that specify the types of traffic allowed in and out of the instances
- Security lists apply to a given instance whether it's talking with another instance in the VCN or a host outside the VCN
- You can choose whether a given rule is stateful or stateless

Stateful Security Rules

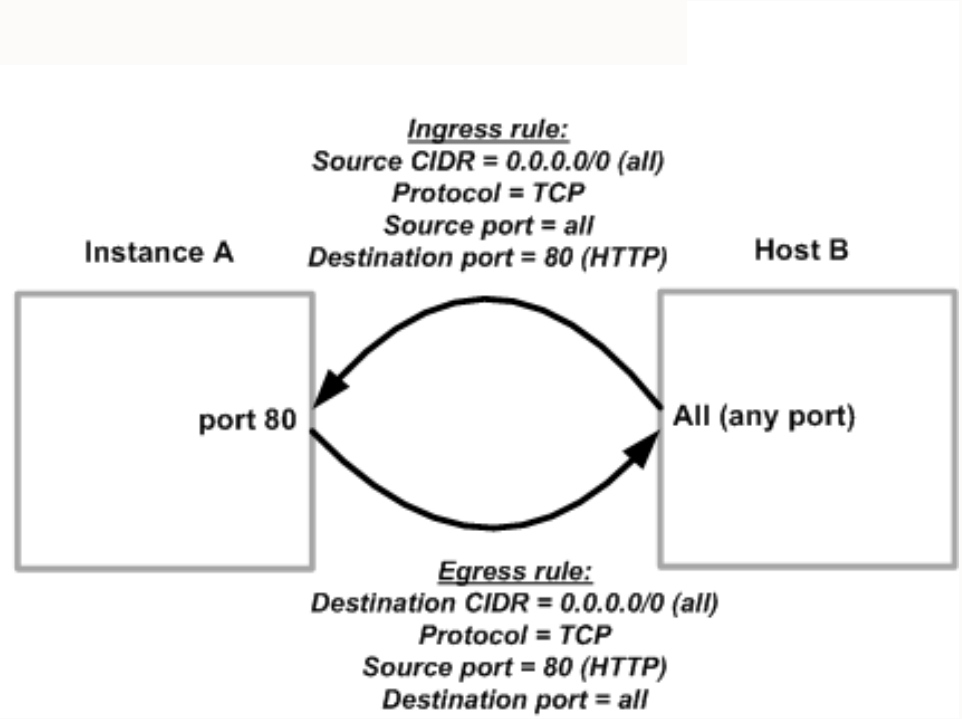


- Connection Tracking: when an instance receives traffic matching the stateful ingress rule, the response is tracked and automatically allowed regardless of any egress rules; similarly for sending traffic from the host
- Default Security List rules are stateful

SOURCE TYPE	SOURCE CIDR	IP PROTOCOL	SOURCE PORT RANGE *(OPTIONAL)*	DESTINATION PORT RANGE *(OPTIONAL)*
CIDR	0.0.0.0/0	TCP	All	80
	Specified IP addresses: 0.0.0.0-255.255.255.255 (4,294,967,296 IP addresses)	*(more information)*	Examples: 80, 20-22 or All *(more information)*	Examples: 80, 20-22 or All *(more information)*

Hosts in this group are reachable from the internet on Port 80

Stateless Security Rules



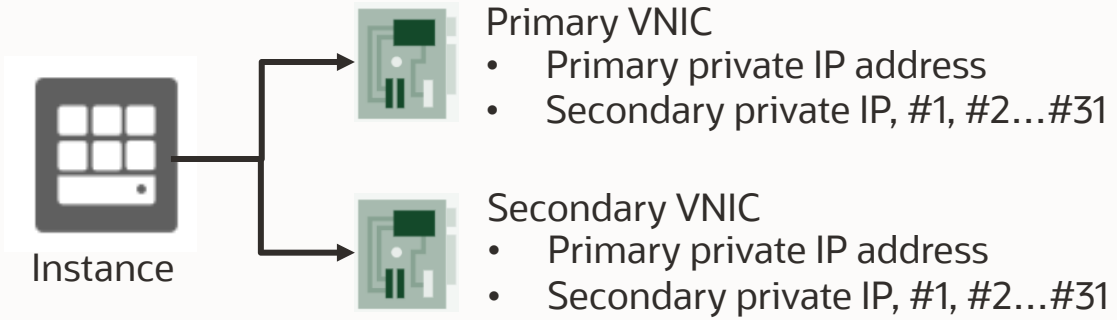
- With stateless rules, response traffic is not automatically allowed
- To allow the response traffic for a stateless ingress rule, you must create a corresponding stateless egress rule
- If you add a stateless rule to a security list, that indicates that you do NOT want to use connection tracking for any traffic that matches that rule
- Stateless rules are better for scenarios with large numbers of connections (Load Balancing, Big Data)

Internal DNS

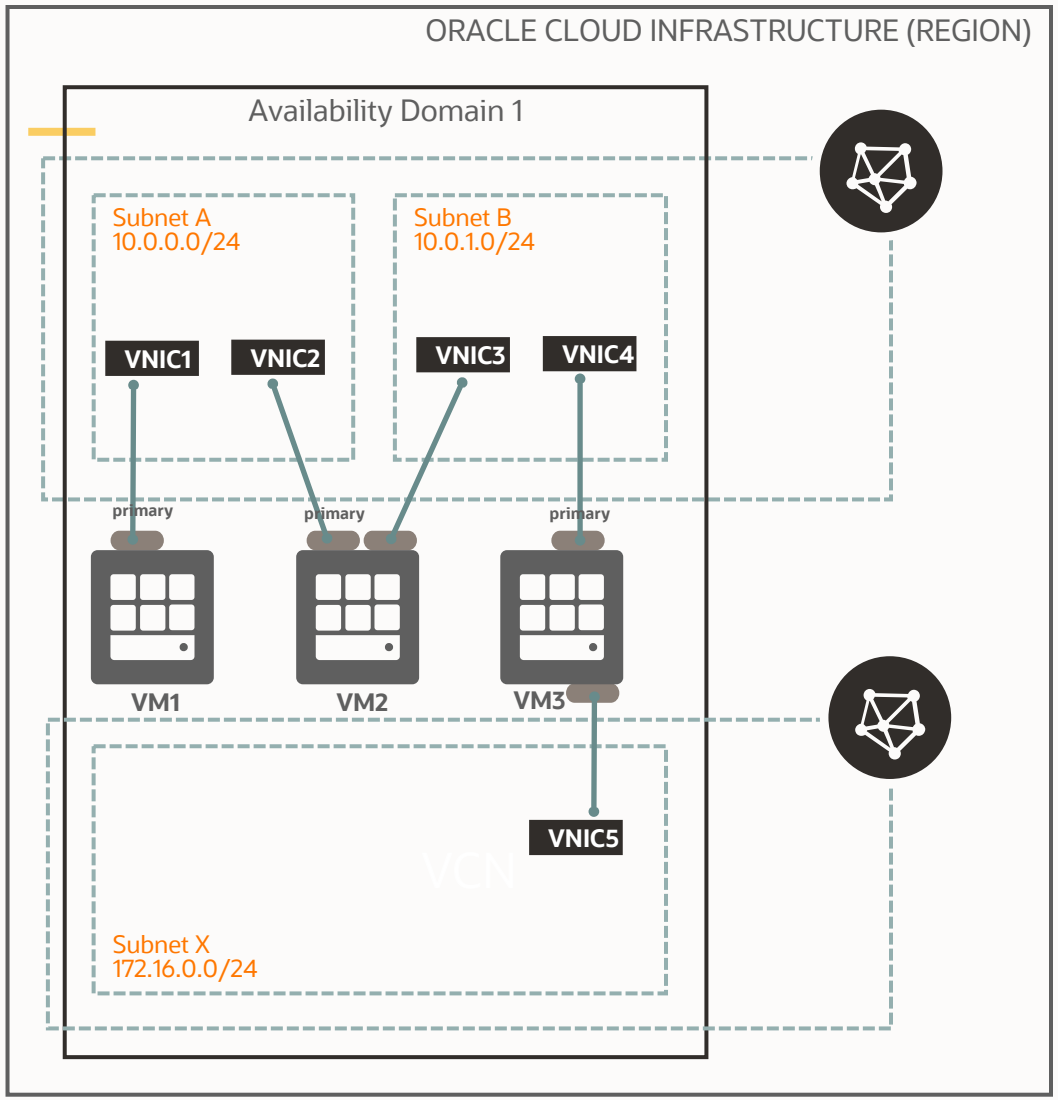
- The VCN Private Domain Name System (DNS) enables instances to use hostnames instead of IP addresses to talk to each other
- Options:
  - Internet and VCN Resolver: default choice for new VCNs
  - Custom Resolver: lets instances resolve the hostnames of hosts in your on-premises network through IPsec VPN/FastConnect
- Optionally specify a DNS label when creating VCN/subnets/instances
  - VCN: <VCN DNS label>.oraclevcn.com
  - Subnet: <subnet DNS label>.<VCN DNS label>.oraclevcn.com
  - Instance FQDN: <hostname>.<subnet DNS label>.<VCN DNS label>.oraclevcn.com
- Instance FQDN resolves to the instance's Private IP address
- No automatic creation of FQDN for Public IP addresses (e.g. cannot SSH using <hostname>.<subnet DNS label>.<VCN DNS label>.oraclevcn.com)

Private IP

- Each instance has at least one primary private IP address
- A private IP can have an optional public IP assigned to it
- Instances ≥ 2 VNICs (secondary VNICs)
- Each VNIC has one primary private IP



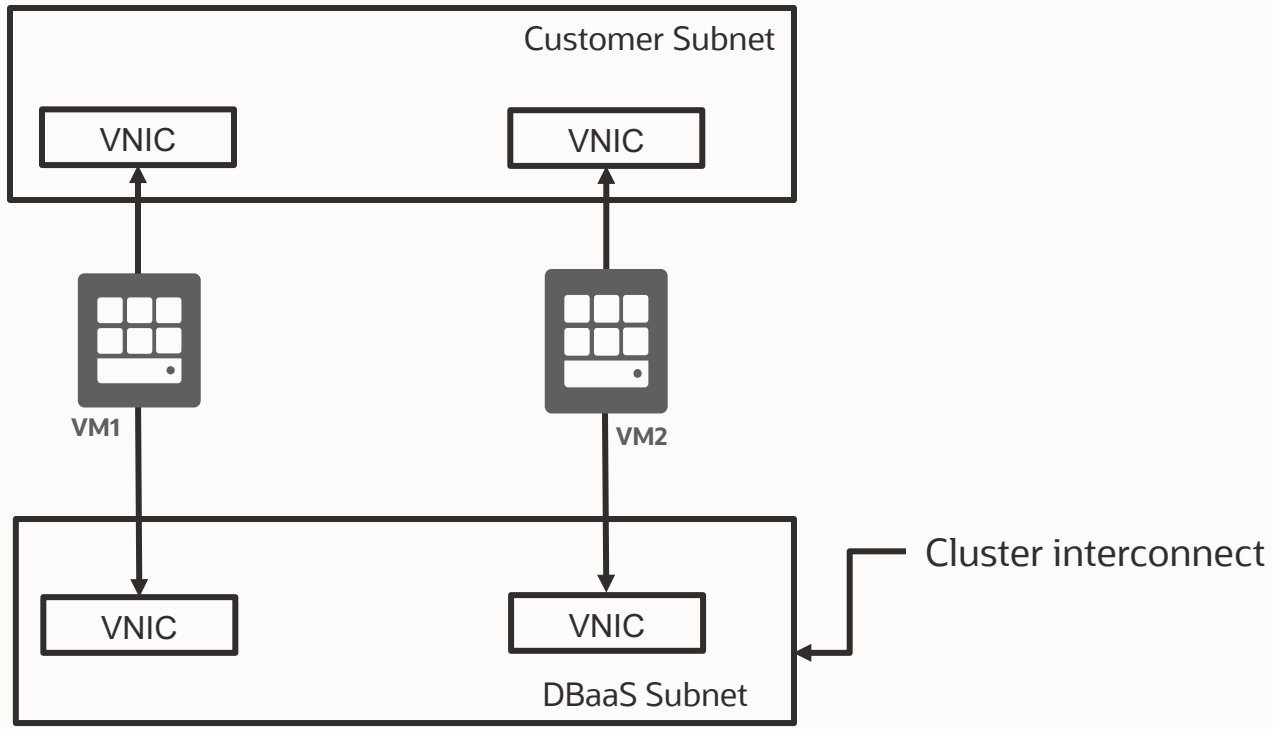
Multiple VNICs on virtual machines



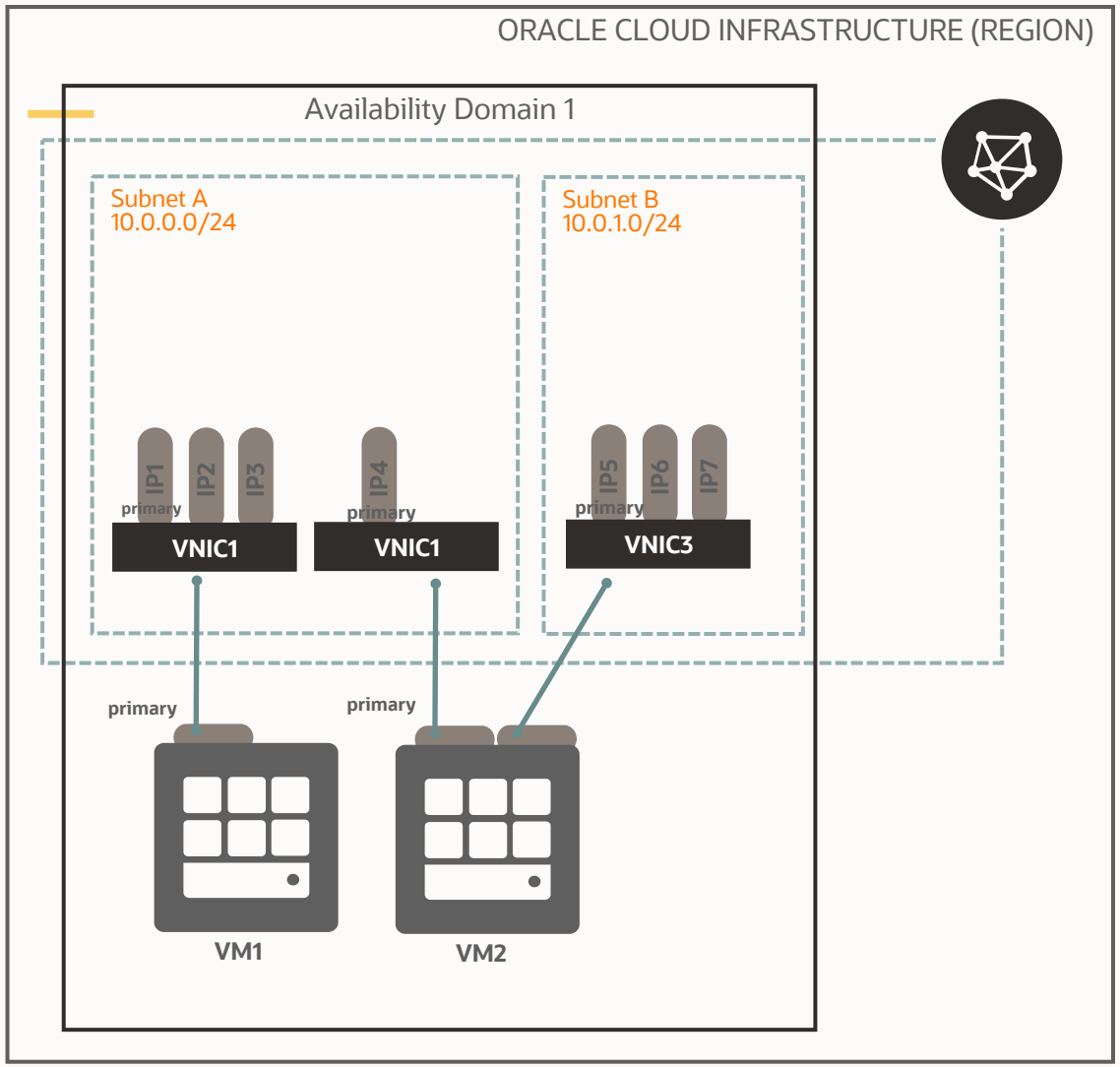
- Every VM has one primary VNIC created at launch, and a corresponding Ethernet device on the instance with the IP address configuration of the primary VNIC
- When a secondary VNIC is added, new Ethernet device is added and is recognized by the instance OS
  - VM1 - single VNIC instance
  - VM2 - connected to two VNICs from two subnets within the same VCN. Used for virtual appliance scenarios
  - VM3 - connected to two VNICs from two subnets from separate VCNs. Used to connect instances to a separate management network for isolated access

Multiple VNICs with DB RAC VM

- VM DB 2 –node RAC instances use multiple VNICs
  - Client subnet
  - Cluster Subnet – DBaaS Service Owned VCN



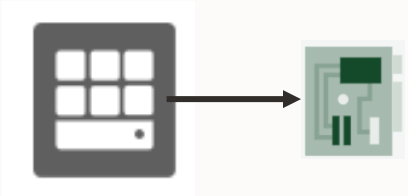
Secondary IP addresses on VNICs



- Every VNIC
  - Primary private IP on creation
  - Additonal private (secondary) IPs (max 31)
- Secondary private IP assigned only after instance launch
- Two step process to use secondary IP addresses
  - Assign a secondary private IP address to VNIC using console/API/SDK
  - Update the instance OS to configure an additional IP address on corresponding Ethernet device
- Possible to move secondary private IP from a VNIC on one instance to a VNIC on another instance
- Used for SCAN and VIP with RAC deployment on Exadata and 2-node VM RAC

Public IP

- Public IP is an IPv4 address reachable from internet; assigned to a private IP object on the resource (Instance, load balancer). Ephemeral or Reserved.
- Possible to assign a given resource multiple public IPs across one or more VNICs



Primary VNIC
- Primary Private IP address, Public IP address
- Secondary Private IP #1, Public IP address
- Secondary Private IP #2, Public IP address
- …

- Public IP assigned to
  - Instance (not recommended in most cases)
  - OCI Public Load Balancer (Oracle provided; you cannot choose/edit)
  - NAT Gateway (Oracle provided; you cannot view/choose/edit)
  - DRG – IPsec tunnels (Oracle provided; you cannot choose/edit)
  - Autonomous Data Warehouse (Oracle provided; you cannot view/choose/edit)
  - Autonomous Transaction Processing (Oracle provided; you cannot view/choose/edit)
  - OKE cluster master and worker nodes (Oracle provided; you cannot choose/edit)

Putting it together with OCI ExaCS

- OCI Exadata DomU connected to 2 customer subnets
  - Client (vnic1)
  - Backup (vnic2)
- Primary Private IP – Host IP (vnic1), Backup IP (vnic2)
- Secondary Private IPs – VIP (vnic1), SCAN IP (vnic1)
- Create additional Application VIPs (example: Golden Gate)
- Use internal VCN DNS to resolve private IPs
  - Host name
  - VIP name
  - SCAN name (RR-DNS)
- Secondary IP failover
  - VIP and SCAN IP failover

- Deploy in Private Subnet
  - Service Gateway for object store backups
  - NAT gateway for Yum repos access
  - DG with remote peering
- Deploy in Public Subnet
  - Host IP mapped to Public IP
- Route Table for NAT Gateway or Service Gateway access
- Security lists for
  - Egress to Object store
  - Ingress on TCP/1521 from VCN clients or on-premise applications

On-Prem Connectivity

Connectivity options

Public Internet

- Internet Gateway/ NAT Gateway
- Reserved and Ephemeral IPs
- Internet Data out Pricing (first 10TB free)

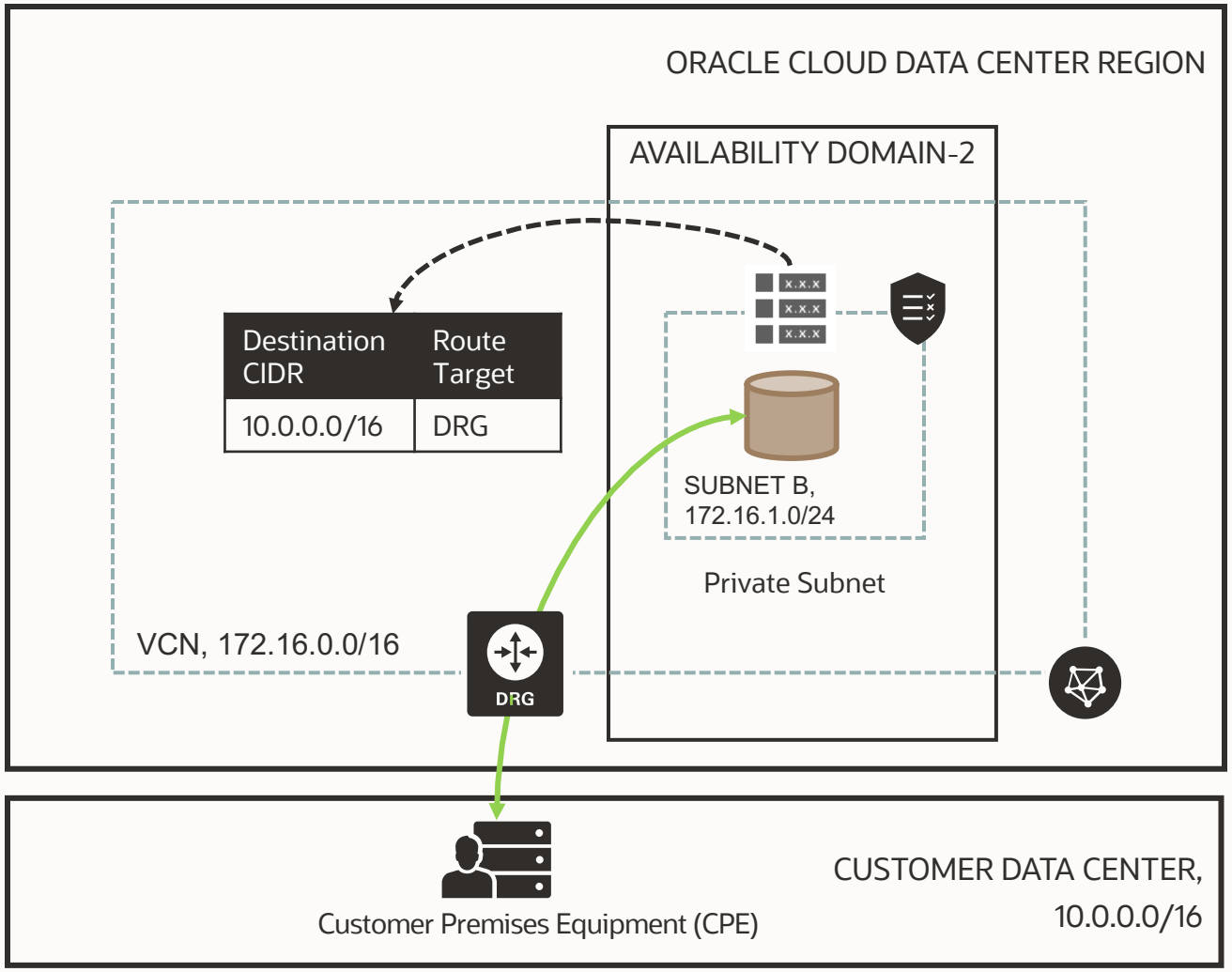
VPN

- IPsec authentication and encryption
- Two main options
  - OCI managed VPN Service (free)
  - Software VPN (running on OCI Compute)

FastConnect

- Private Connection
- Separate from the internet
- Consistent network experience
- Port speeds of 1 Gbps and10 Gbps
- SLA

Dynamic Routing Gateway



A virtual router that provides a path for private traffic between your VCN and destinations other than the internet

You can use it to establish a connection with your on-premises network via IPsec VPN or FastConnect (private, dedicated connectivity)

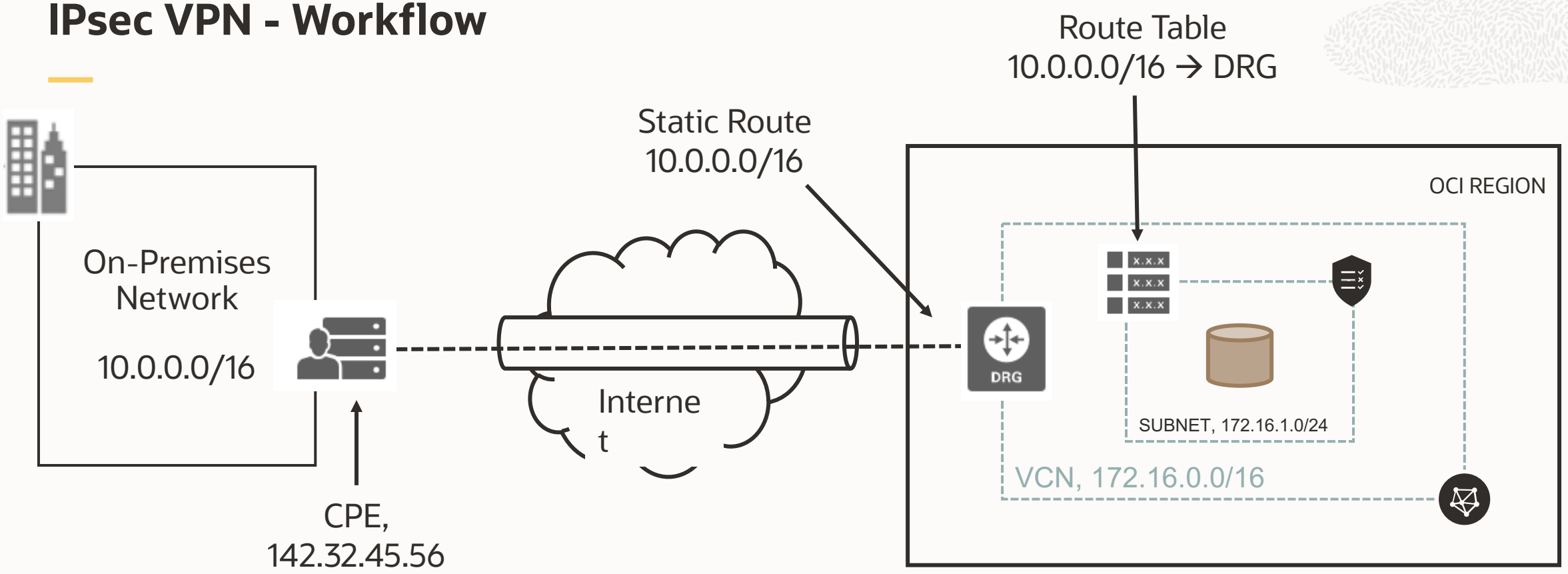
After attaching a DRG, you must add a route for the DRG in the VCN's route table to enable traffic flow

DRG is a standalone object. You must attach it to a VCN. VCN and DRG have a 1:1 relationship

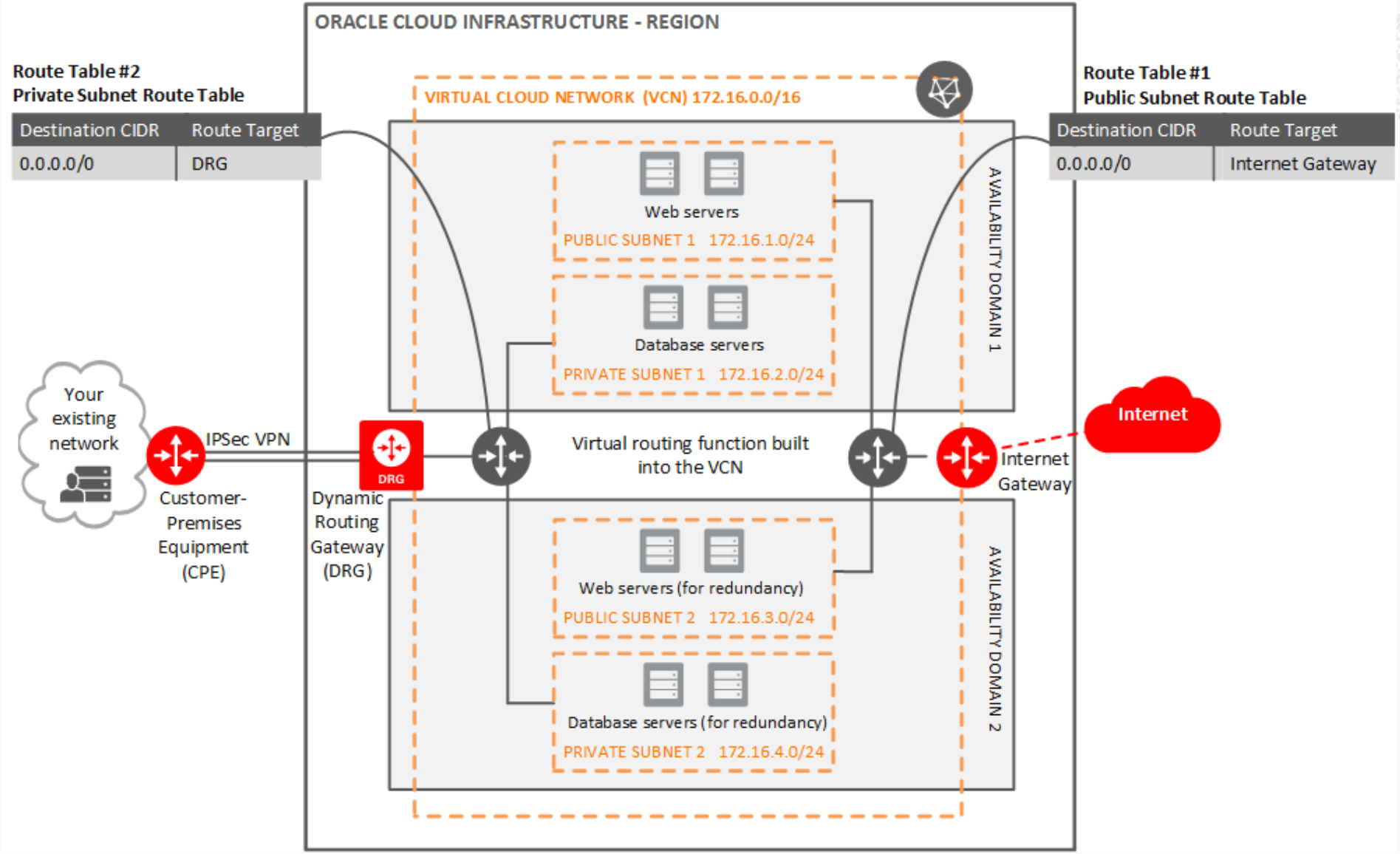
OCI VPN Overview

- OCI VPN securely connects on-premises network to OCI VCN through an IPsec VPN connection
- VPN can help ensure a business that its networks provide secure remote connectivity
- Bandwidth is dependent on the customer's access to the Internet and general Internal congestion (Typically less than 250 Mbps – but your mileage may vary)
- VPN Service is offered for free
- Customer Proof of Concepts usually start as a VPN and then morph into FastConnect designs
- OCI provisions redundant VPN tunnels located on physically and logically isolated tunnel endpoints

IPsec VPN - Workflow



Public & Private Subnets with VPN

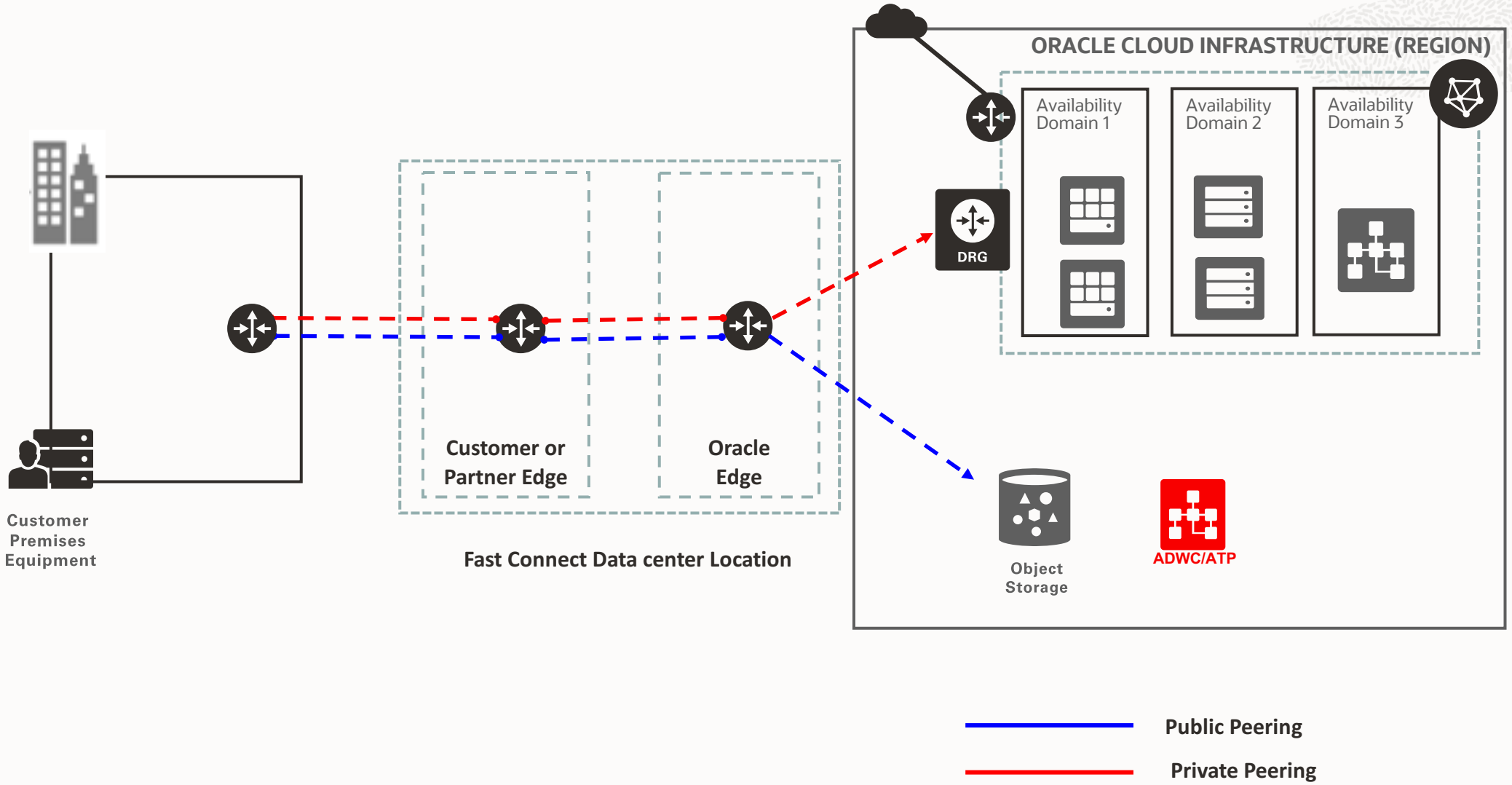


FastConnect

FastConnect provides a dedicated and private connection with higher bandwidth options, and a more reliable and consistent networking experience when compared to internet-based connections

- Connect to OCI directly or via pre-integrated Network Partners
- Port speeds of 1 Gbps and 10 Gbps increments
- Extend remote datacenters into Oracle ("**Private peering**") or connect to Public resources **("Public peering")**
- No charges for inbound/outbound data transfer
- Uses BGP protocol

FastConnect Use Cases



VCN Peering

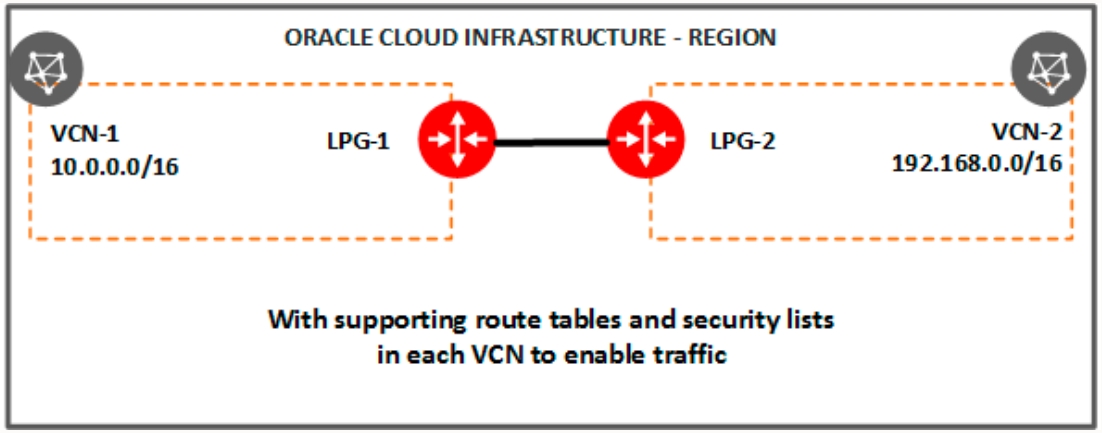
- Enables connectivity between the resources in different VCNs
- Does not require public IPs or NAT to enable connectivity
- Traffic never leaves the Oracle Network
- Over other options such as connecting over the internet, VCN Peering offers
  - Faster connectivity
  - Higher security
- Types of VCN Peering available
  - Local Peering (In-region)
  - Remote Peering (Cross-region)

Local VCN Peering – connecting VCNs in the same region

- Connecting two VCNs within a region to allow direct communication via. private IPs
- VCNs should not have overlapping IP addresses
- Local Peering VCNs can be either in the same or different tenancies (cross-tenancy peering)

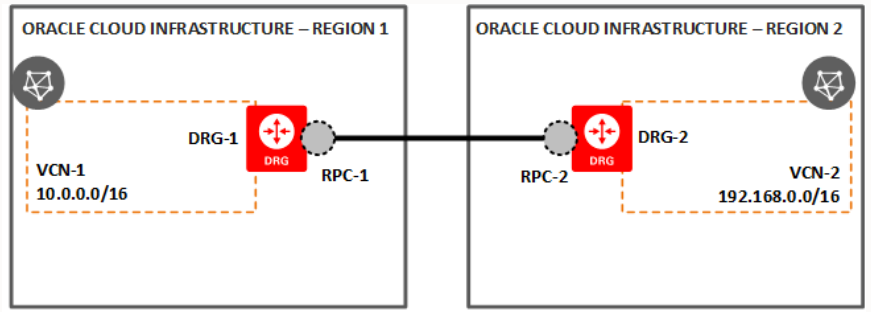
Local Peering Gateway (LPG)

- Like Internet Gateway, LPG is a component on the VCN
- LPGs of two VCNs are connected to make a peering relationship
- Enable the data plane to learn about instances in peered VCNs



Remote VCN Peering – connecting VCNs in the different region

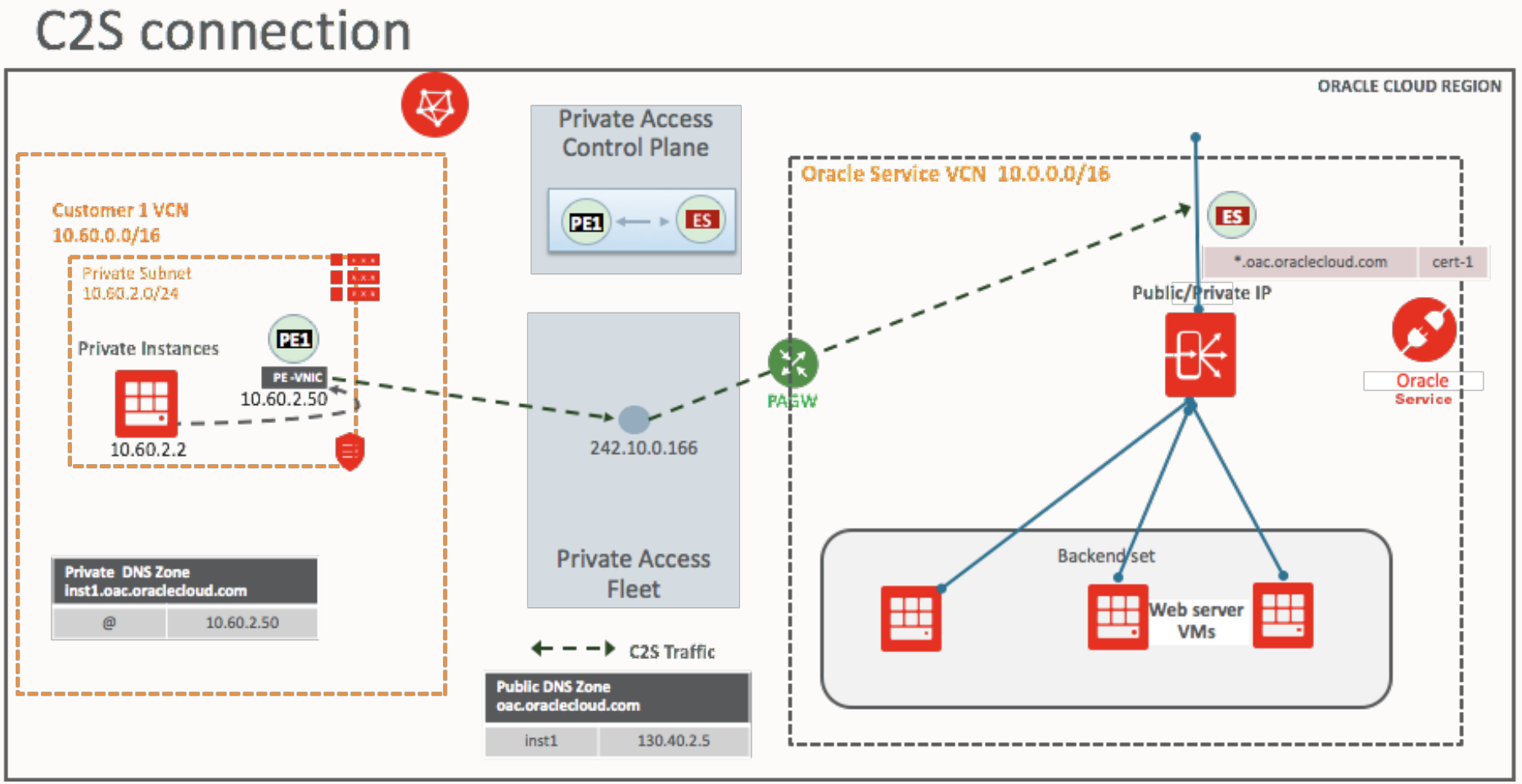
- Traffic flows between regions through the OCI backbone network
- The two VCNs in the peering relationship must not have overlapping CIDRs
- Requires a DRG to set up the Remote Peering connection; vNIC of one VCN instance forwards traffic to its DRG, which forwards traffic to peer DRG in other region over backbone
- **Remote Peering Connection**
  - Like Virtual Circuits, the Remote Peering Connection is a component of DRG
  - RPCs of two DRGs from two regions are connected to create a peering relationship



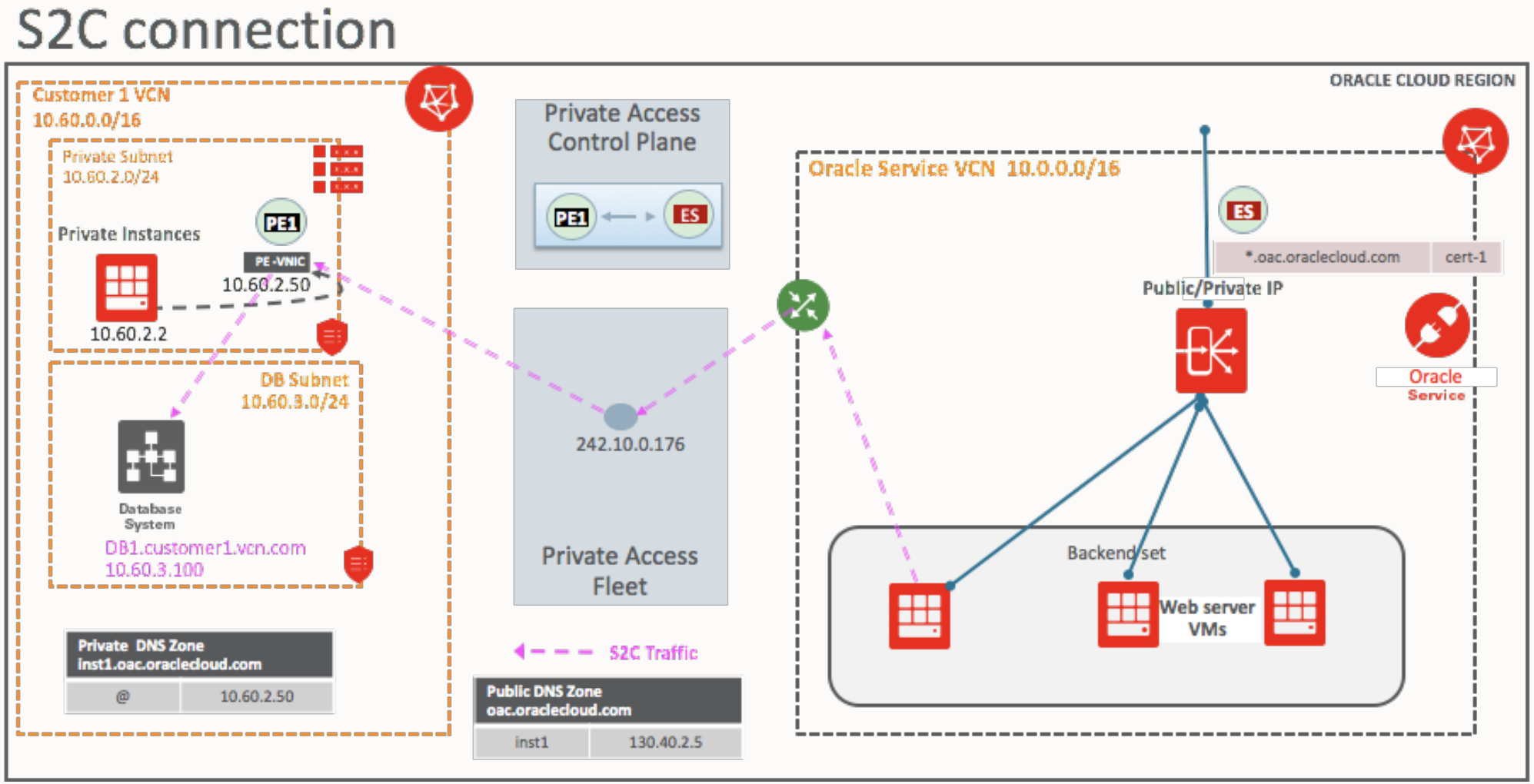
Summary of OCI network connectivity options

Scenario	Solution
Let instances connect to the Internet, and receive connections from it	Internet Gateway
Let instances reach the Internet without receiving connections from it	NAT Gateway
Let VCN hosts privately connect to object storage, bypassing the internet	Service Gateway
Make an OCI extend an on-premise network, with easy connectivity in both directions	IPsec VPN FastConnect
Privately connect two VCNs in a region	Local Peering Gateway
Privately connect two VCNs in different regions	Remote Peering Connection (DRG)

Private Endpoints – Client to Service (CY19Q4)

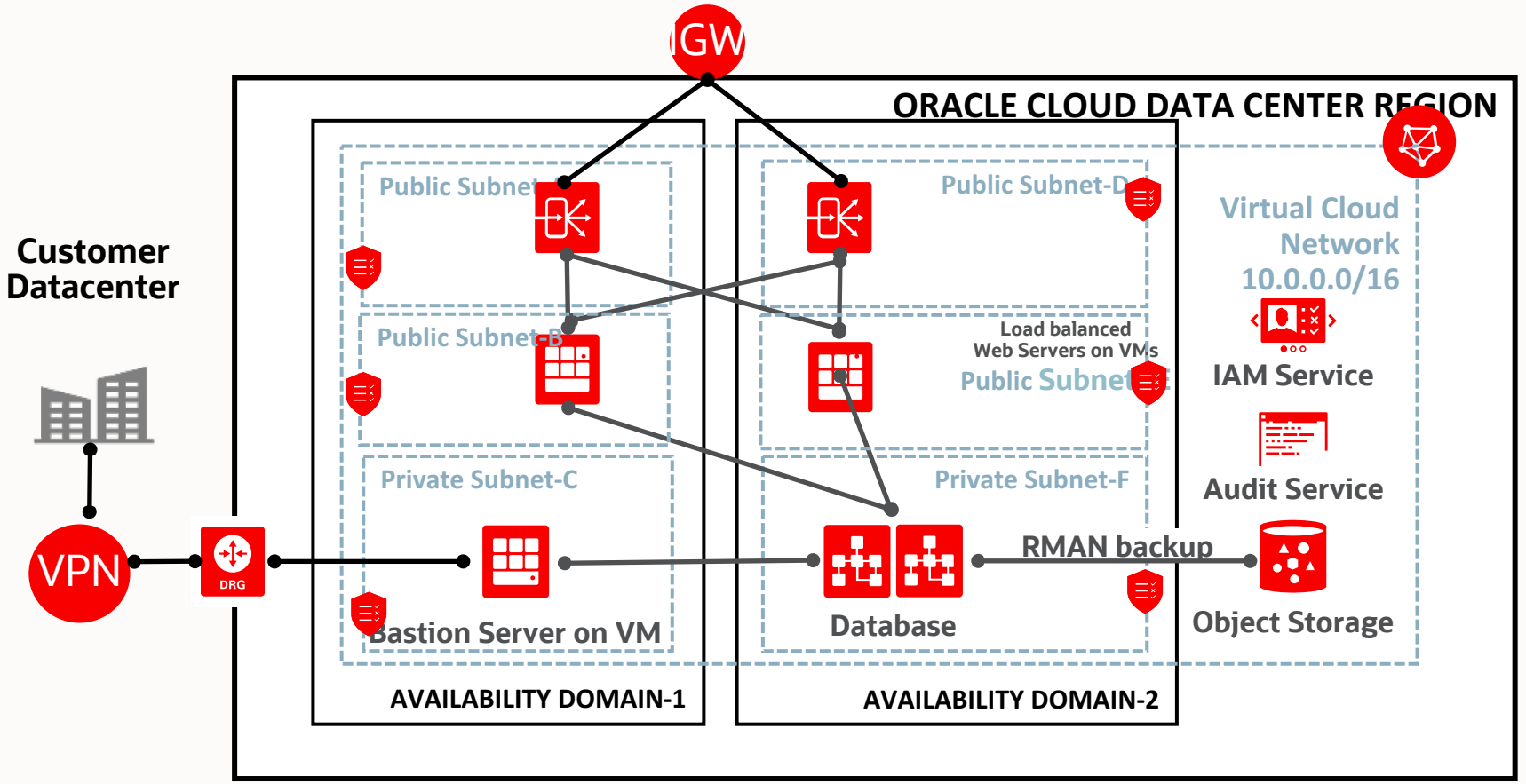


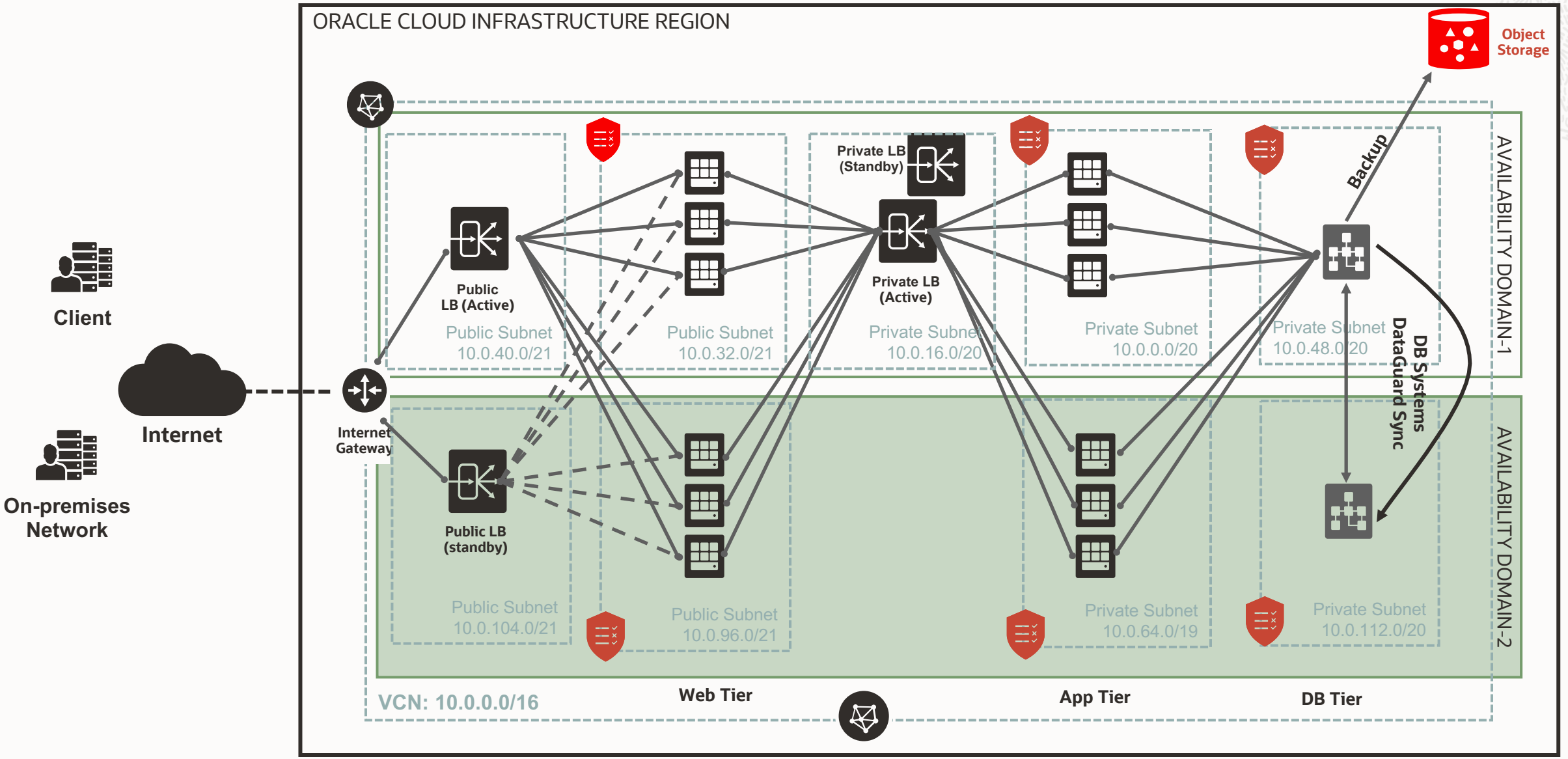
Private Endpoints – Service to Client (CY20Q4)



Customer deployment Patterns

Example: Oracle Customer Architecture




ORACLE CLOUD INFRASTRUCTURE REGION
Object Storage
Backup
Client
Internet
On-premises Network
Internet Gateway
Public LB (Active)
Public LB (standby)
Private LB (Standby)
Private LB (Active)
Public Subnet 10.0.40.0/21
Public Subnet 10.0.32.0/21
Public Subnet 10.0.104.0/21
Public Subnet 10.0.96.0/21
Private Subnet 10.0.16.0/20
Private Subnet 10.0.0.0/20
Private Subnet 10.0.64.0/19
Private Subnet 10.0.48.0/20
Private Subnet 10.0.112.0/20
DB Systems DataGuard Sync
AVAILABILITY DOMAIN-1
AVAILABILITY DOMAIN-2
VCN: 10.0.0.0/16
Web Tier
App Tier
DB Tier

ORACLE