ORACLE
Cloud Infrastructure

Virtual Cloud Network

Level 100

Rohit Rahi

March 2018

ORACLE

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Objectives

After completing this lesson, you should be able to:

- Describe key Virtual Cloud Network (VCN) concepts
- Manage your cloud network components, such as:
  - Subnets, Route Table, Security Lists, Private IP, Public IP
- Learn about various OCI connectivity options
  - Internet Gateway, NAT Gateway, Service Gateway, Local and Remote Peering
  - VPN, FastConnect

Virtual Cloud Network (VCN)

- A private network that you set up in the Oracle data centers, with firewall rules and specific types of communication gateways that you can choose to use
- A VCN covers a single, contiguous IPv4 CIDR block of your choice
- A VCN resides within a single region but can cross multiple Availability Domains

CIDR Basics

- CIDR (classless inter-domain routing) notation
  - xxx.xxx.xxx.xxx/n, where n is the number of bits used for subnet mask. E.g. /24 would be 255.255.255.0
  - 192.168.1.0/24 would equate to IP range: 192.168.1.0 – 192.168.1.255
    - 128 64 32 16 8 4 2 1 -> 2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0
    - 192 is represented as 1 1 0 0 0 0 0 0

192.168.1.0	11000000.10101000 .00000001.00000000
255.255.255.0	11111111. 11111111. 11111111 .00000000 → 192.168.1.0 – 192.168.1.255
AND	11000000.10101000.00000001.00000000

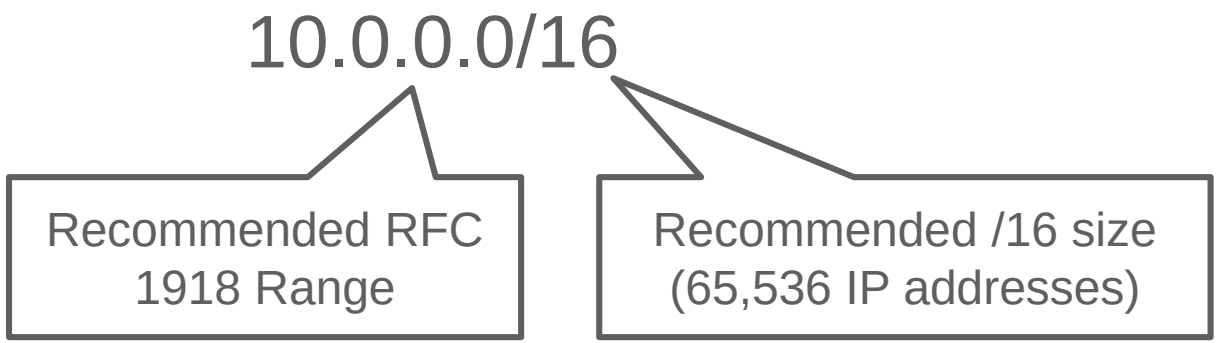
  - 192.168.1.0/27 would equate to IP range: 192.168.1.0 – 192.168.1.31
    - Now network divided in 8 subnets with 32 hosts each due to /27 mask (255.255.255.224)

192.168.1.0	11000000.10101000 .00000001.00000000
255.255.255.224	11111111. 11111111. 11111111 .11100000
AND	11000000.10101000.00000001.00000000

    - Subnets – 2 x 2 x 2 = 8. Hosts – 2 x 2 x 2 x 2 x 2 = 32
    - Subnetworks – 192.168.1.0/27, 192.168.1.32/27, 192.168.1.64/27…

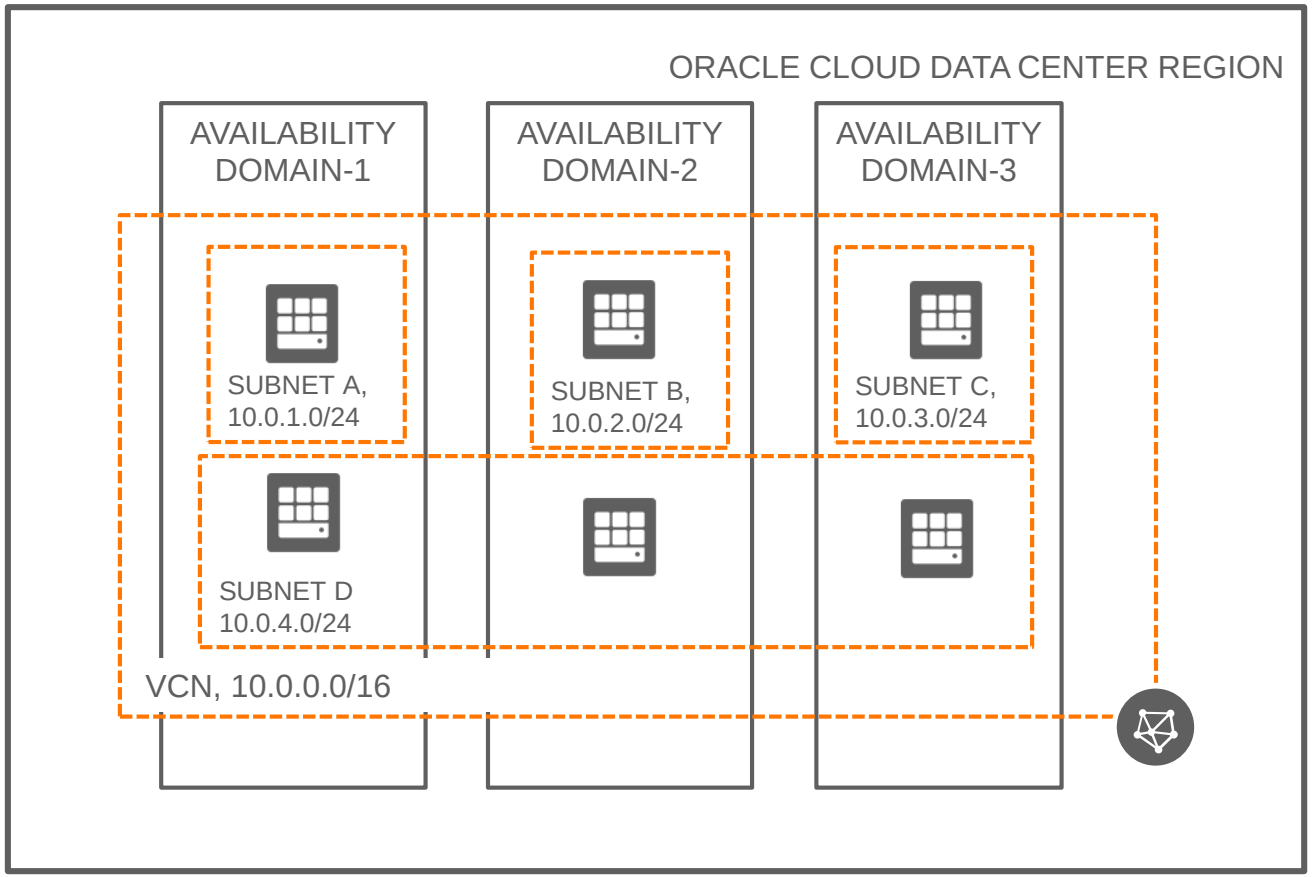
IP address range for your VCN

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

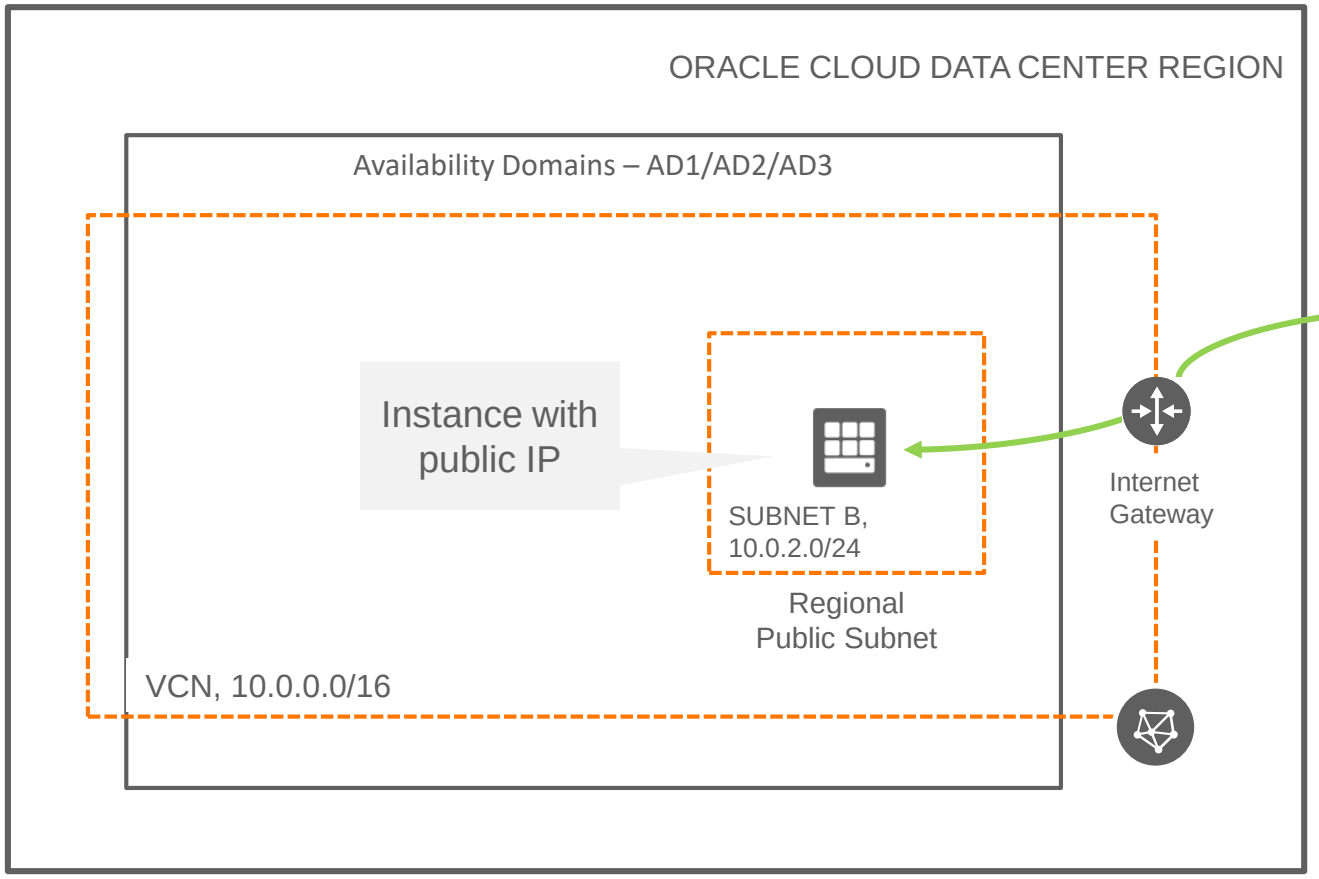
Subnet



Each VCN network is subdivided into subnets

- Each subnet can be a AD specific or can be a **Regional Subnet (recommended)**
- Regional Subnet spans all three ADs in a multi-AD region
- AD specific subnets is contained within a single AD in a multi-AD region
- Each subnet has a contiguous range of IPs, described in CIDR notation. Subnet IP ranges cannot overlap
- Instances are placed in subnets and can live across
- Instances draw their internal IP address and network configuration from their subnet
- Subnets can be designated as either
  - **Private** (instances contain private IP addresses assigned to vNICs)
  - **Public** (contain both private and public IP addresses assigned to vNICs)

Internet Gateway

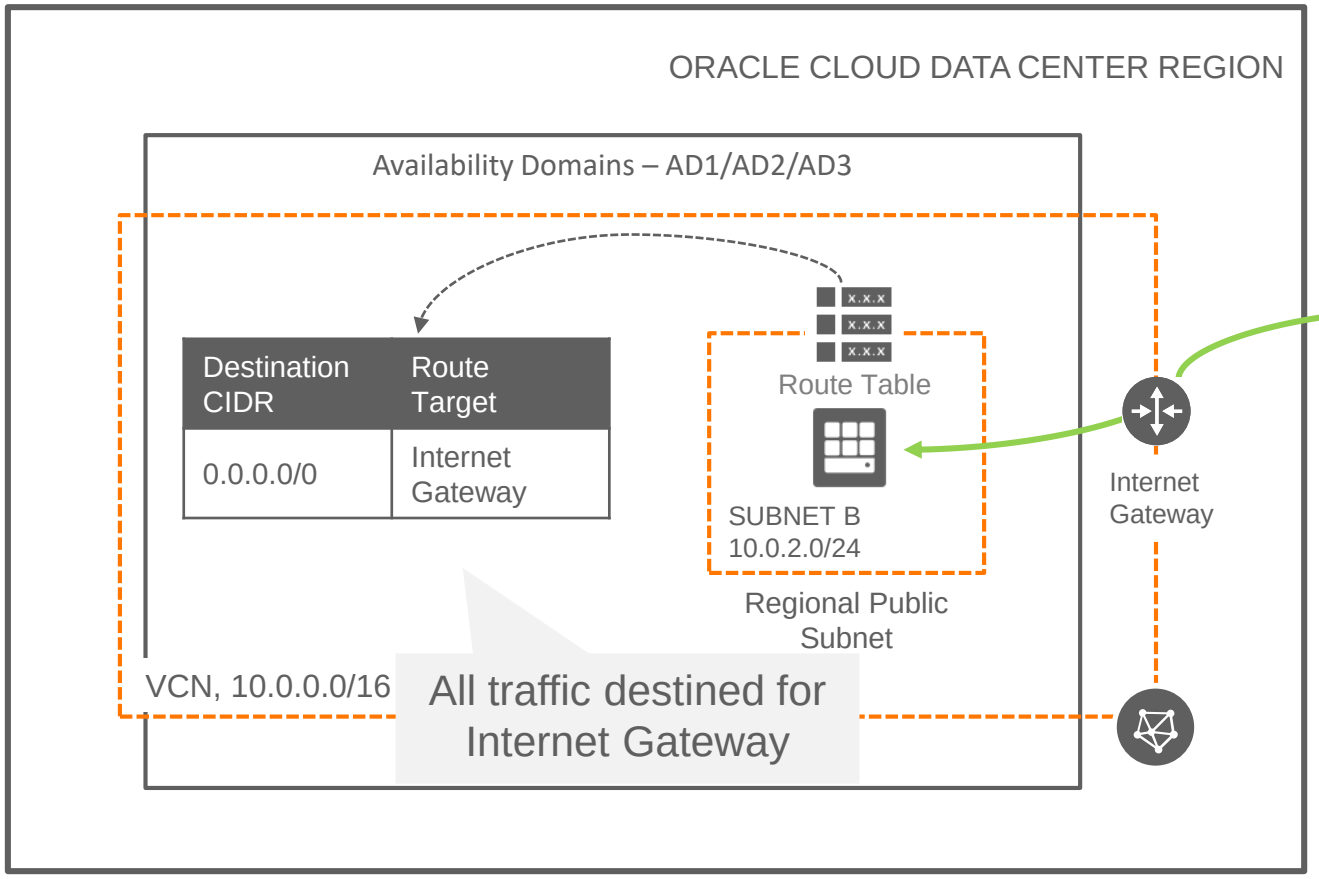


Internet gateway provides a path for network traffic between your VCN and the internet

You can have only one internet gateway for a VCN

After creating an internet gateway, you must add a route for the gateway in the VCN's Route Table to enable traffic flow

Route Table

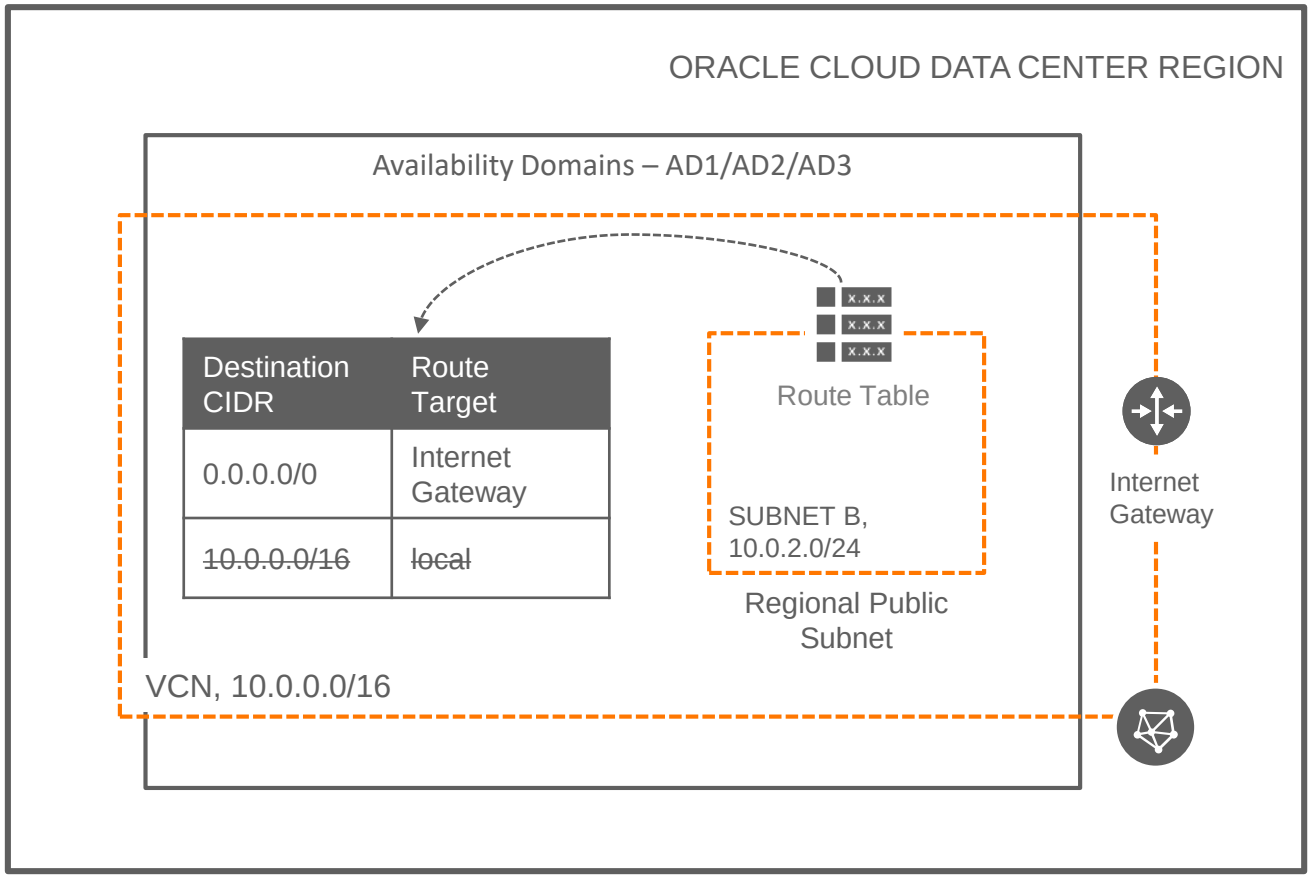


Route Table is used to send traffic out of the VCN

Consists of a set of route rules; each rule specifies

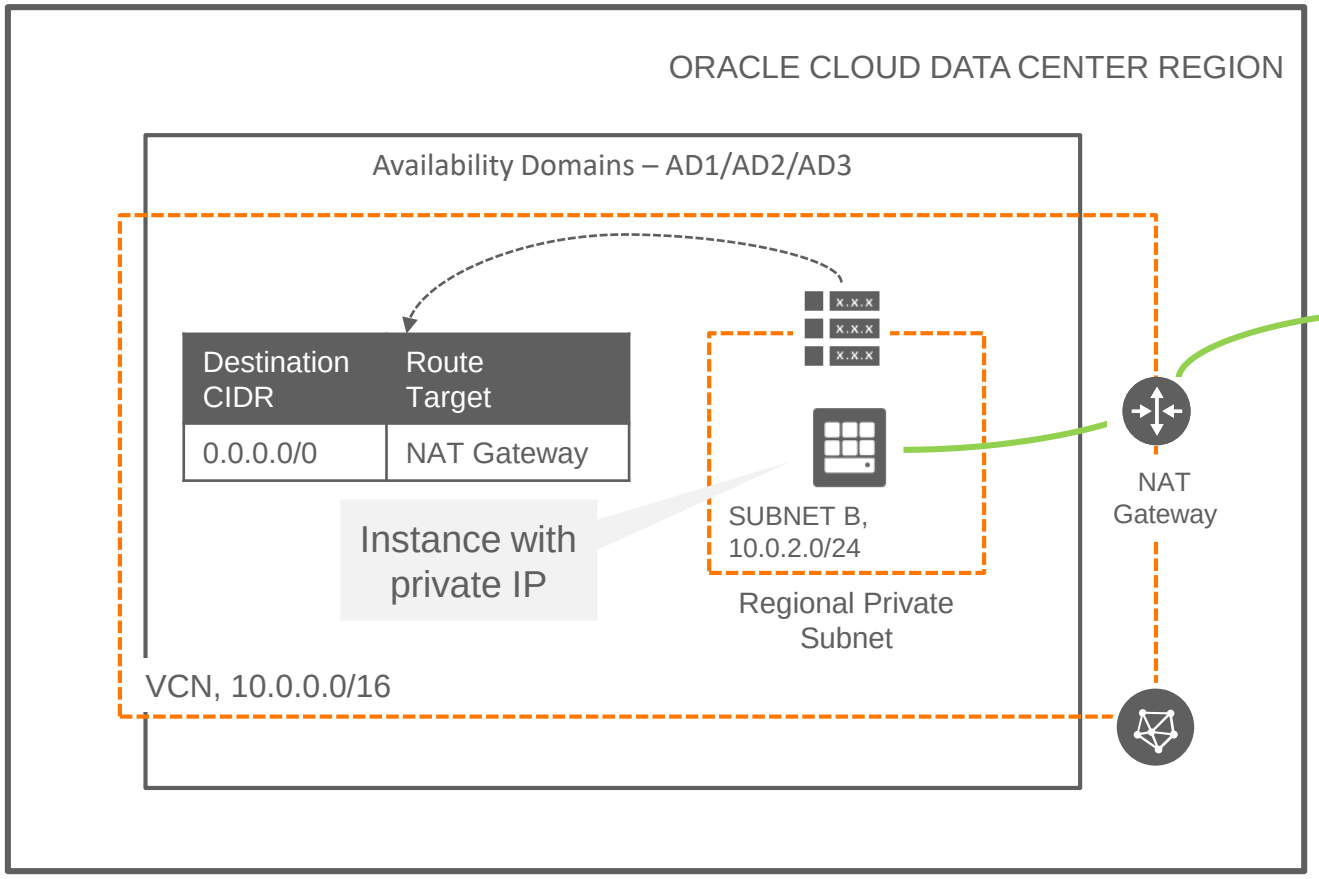
- Destination CIDR block
- Route Target (the next hop) for the traffic that matches that CIDR

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
- When you add an internet gateway, NAT gateway, service gateway, dynamic routing gateway or a peering connection, you must update the route table for any subnet that uses these gateways or connections

NAT Gateway

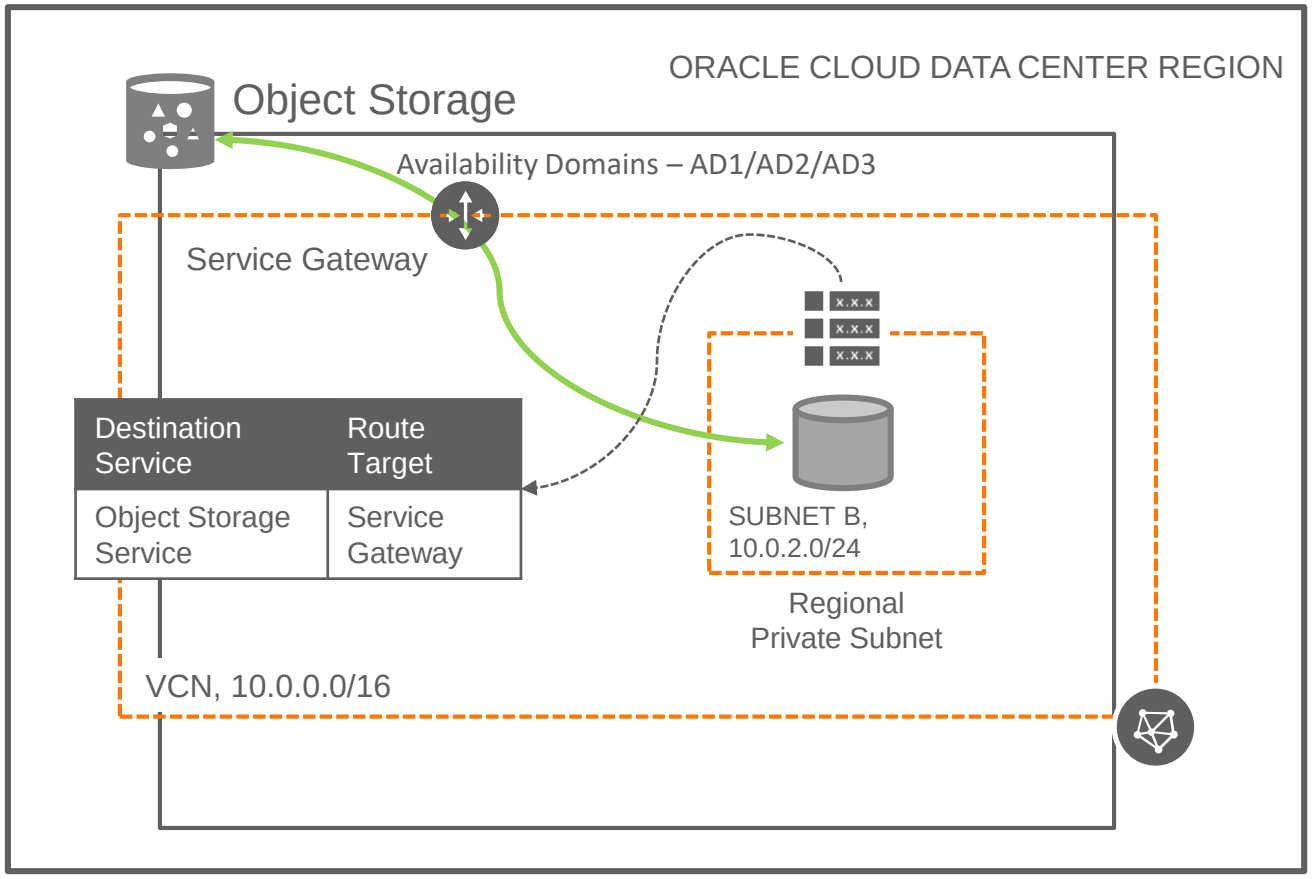


NAT gateway gives an entire private network access to the internet without assigning each host a public IP address

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

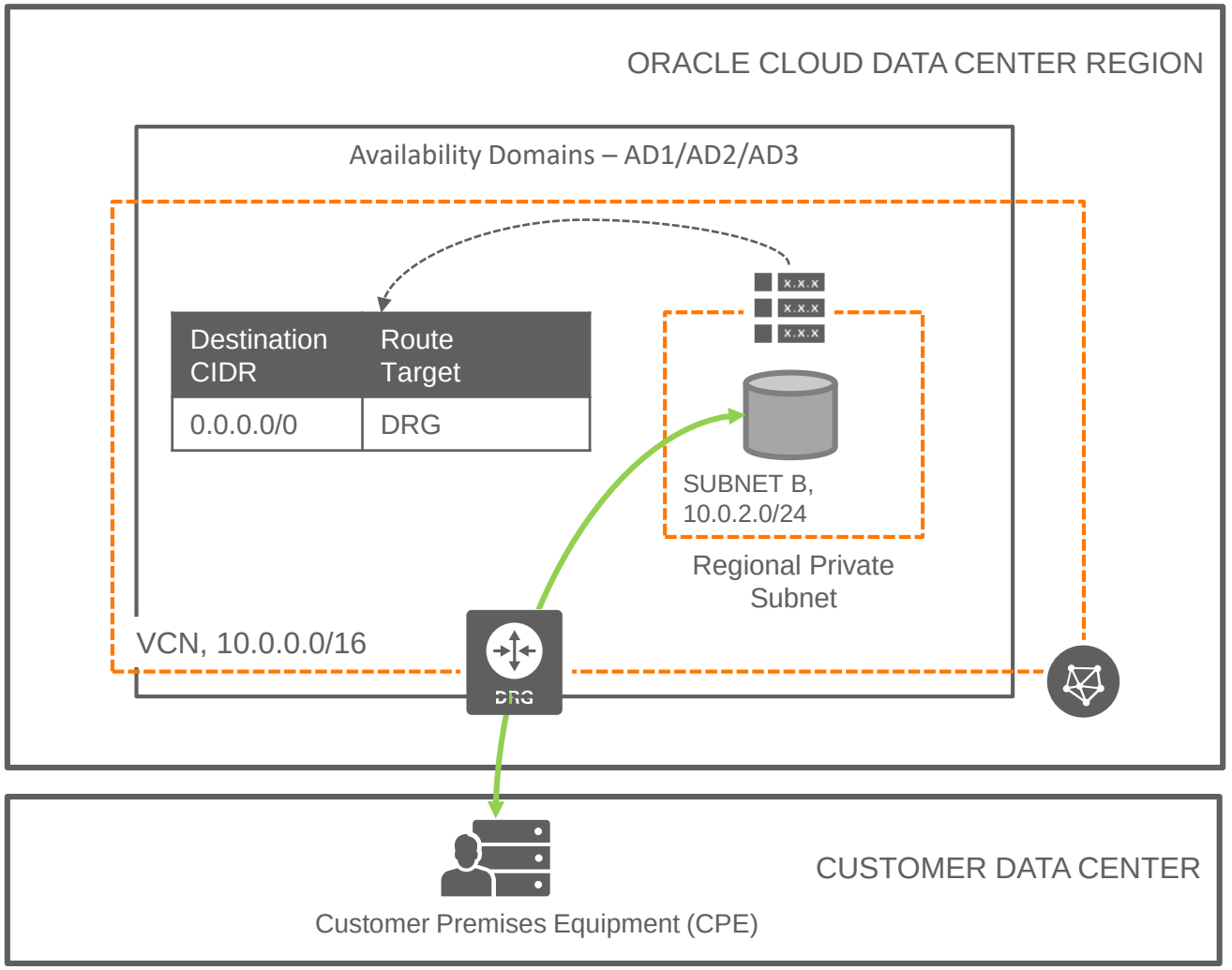


Service gateway lets resources in VCN access public OCI services such as Object Storage, but without using an internet or NAT gateway

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

Use case: back up DB Systems in VCN to Object Storage)

Dynamic Routing Gateway



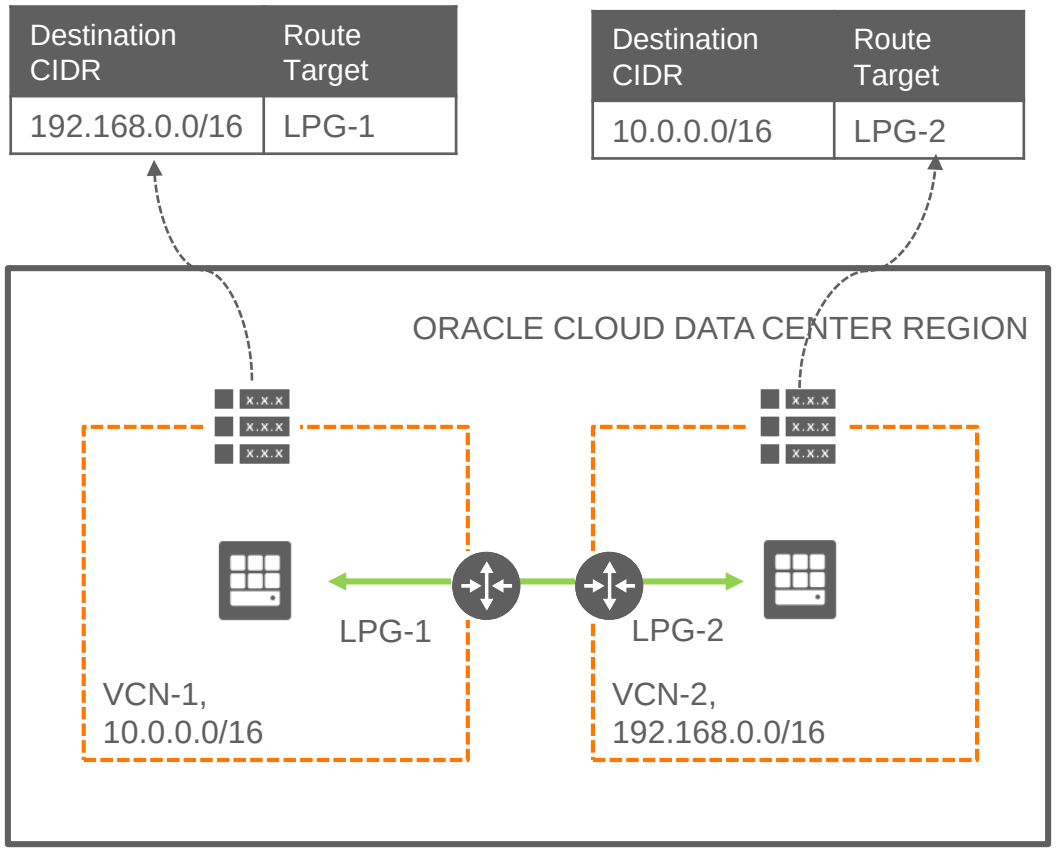
A virtual router that provides a path for private traffic between your VCN and destinations other than the internet

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

Local Peering



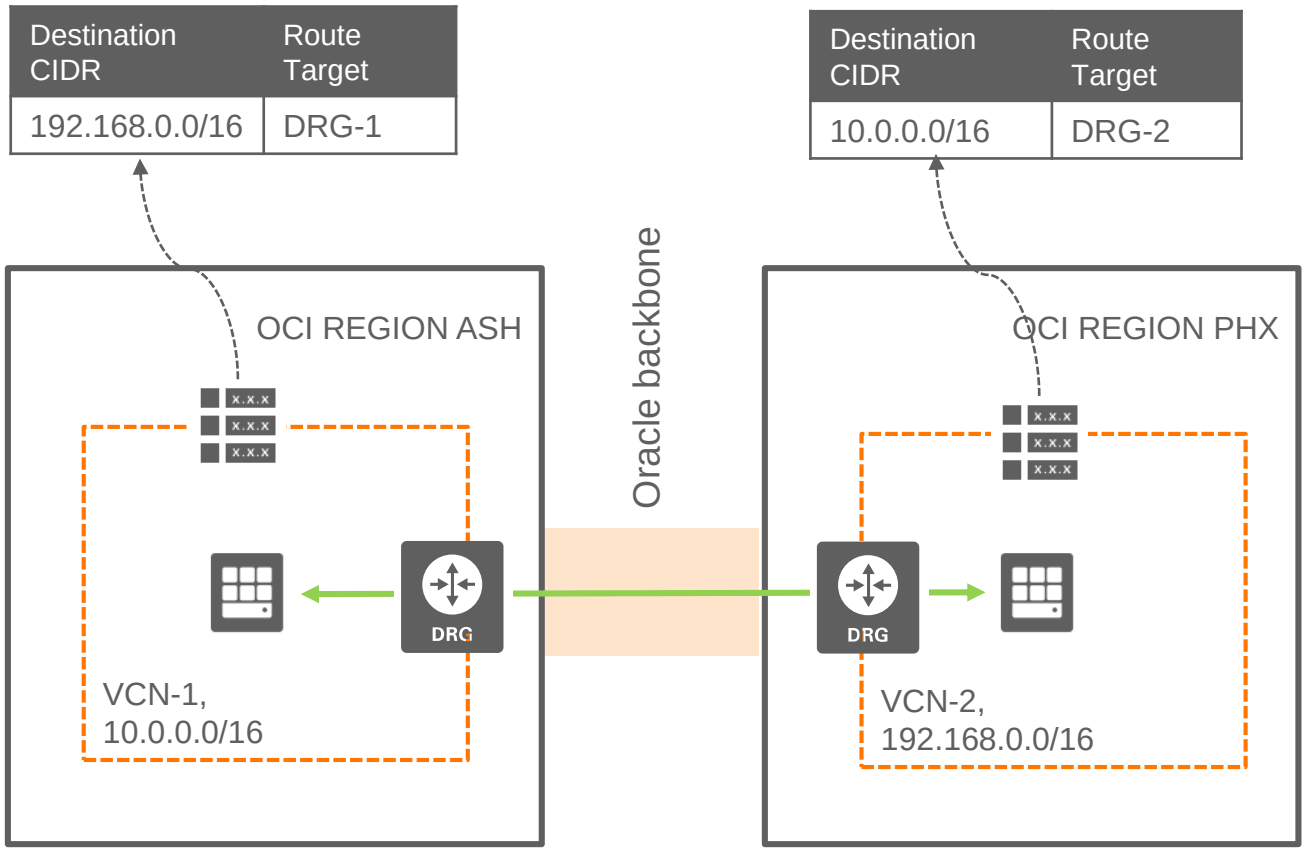
VCN peering is the process of connecting multiple VCNs

Local VCN peering is the process of connecting two VCNs in the **same region** so that their resources can communicate using private IP addresses

A local peering gateway (LPG) is a component on a VCN for routing traffic to a locally peered VCN

The two VCNs in the peering relationship shouldn't have overlapping CIDRs

Remote Peering



Remote VCN peering is the process of connecting two VCNs in **different regions** so that their resources can communicate using private IP addresses

Requires a remote peering connection (RPC) to be created on the DRGs. RPC's job is to act as a connection point for a remotely peered VCN

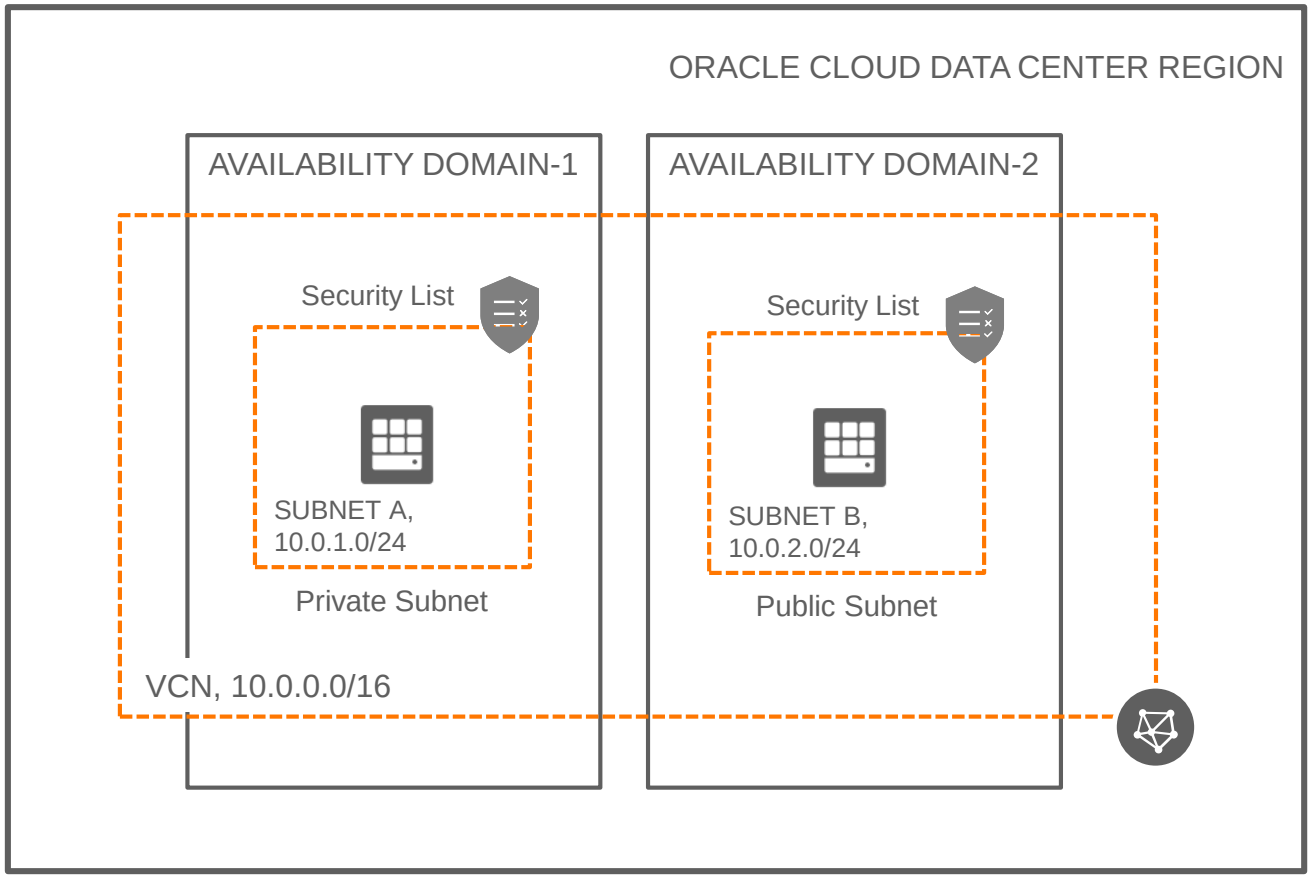
GA for ASH-PHX and LHR-FRA regions (available through Oracle support for other combinations)

The two VCNs in the peering relationship must not have overlapping CIDRs

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)

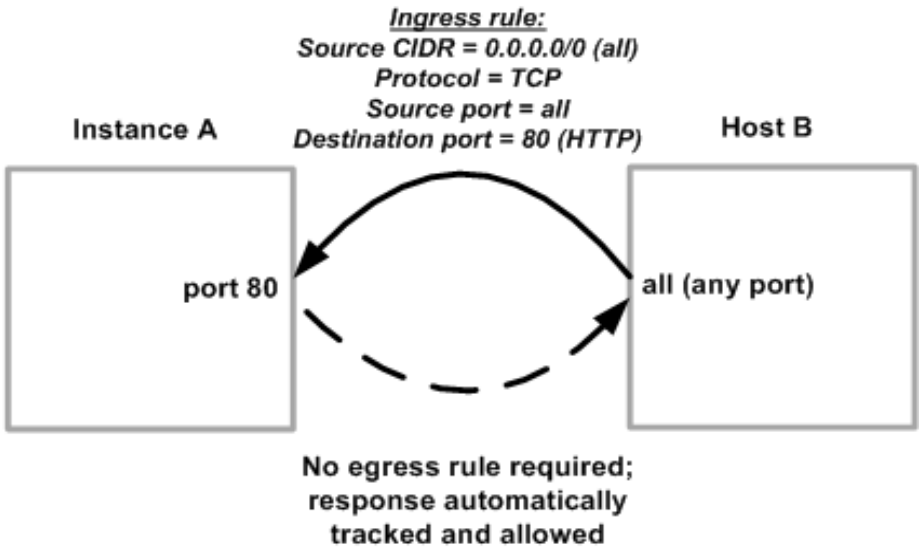
Security Lists



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

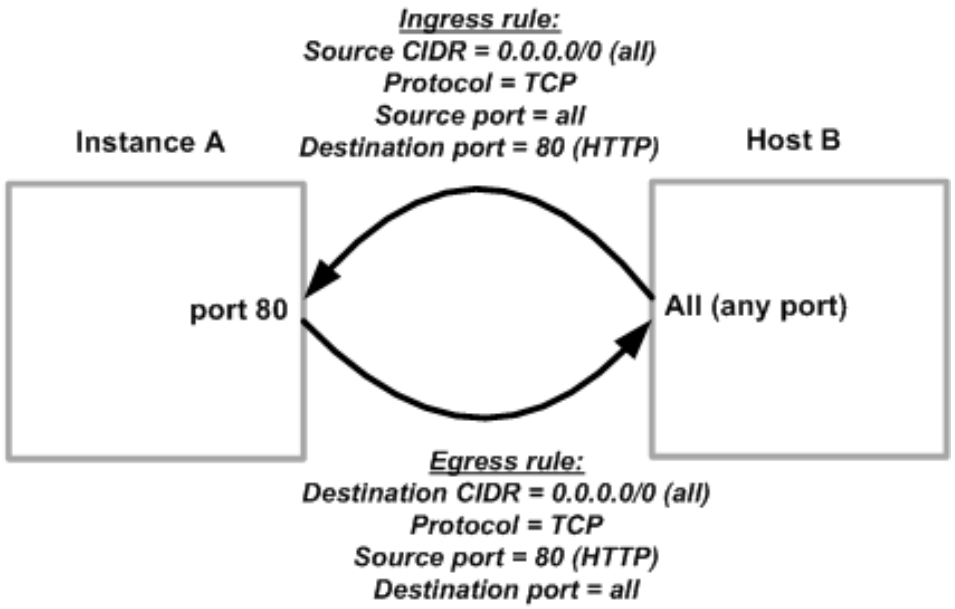
Stateful Security Rules



- 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

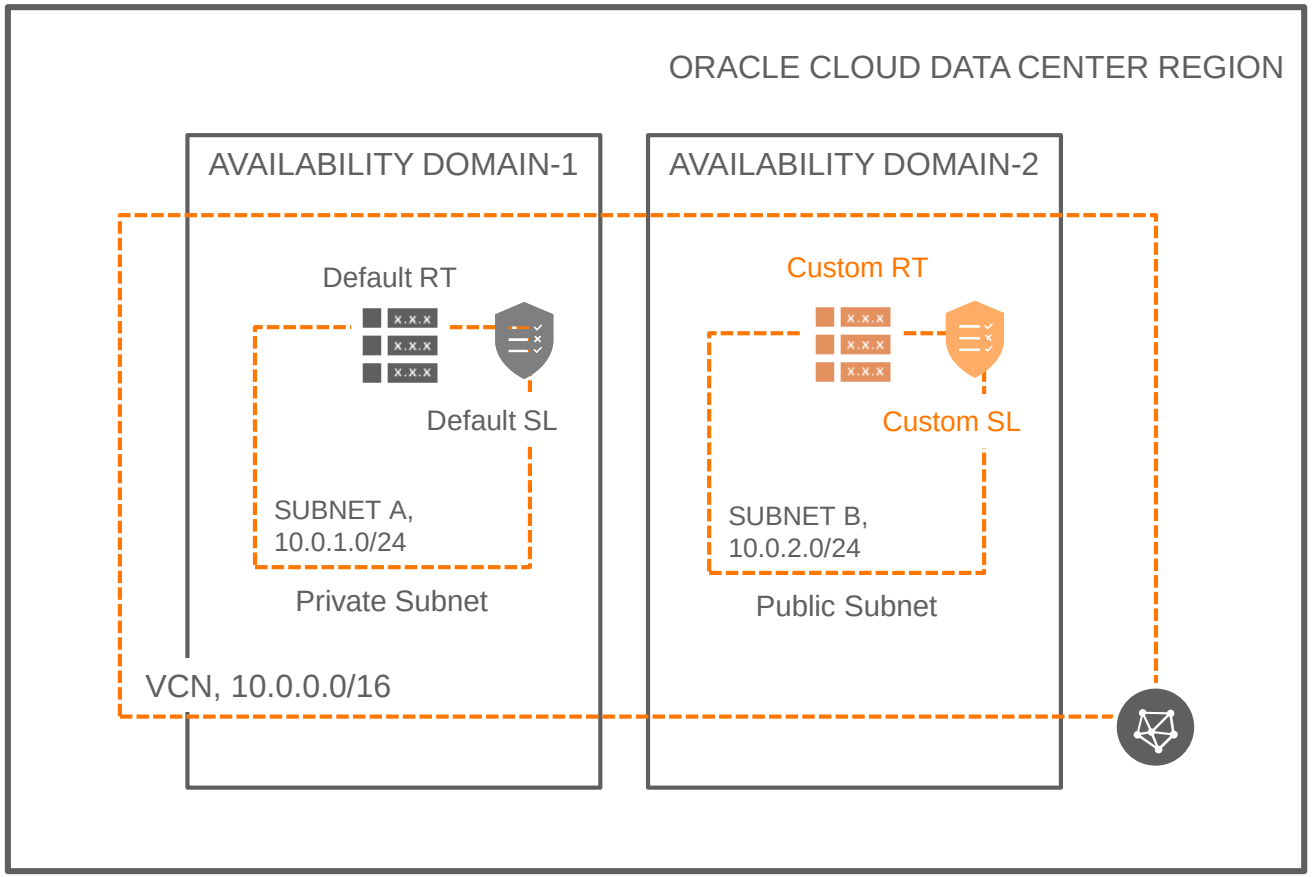
Hosts in this group are reachable from the internet on Port 80

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)

Default VCN components



Your VCN automatically comes with some default components

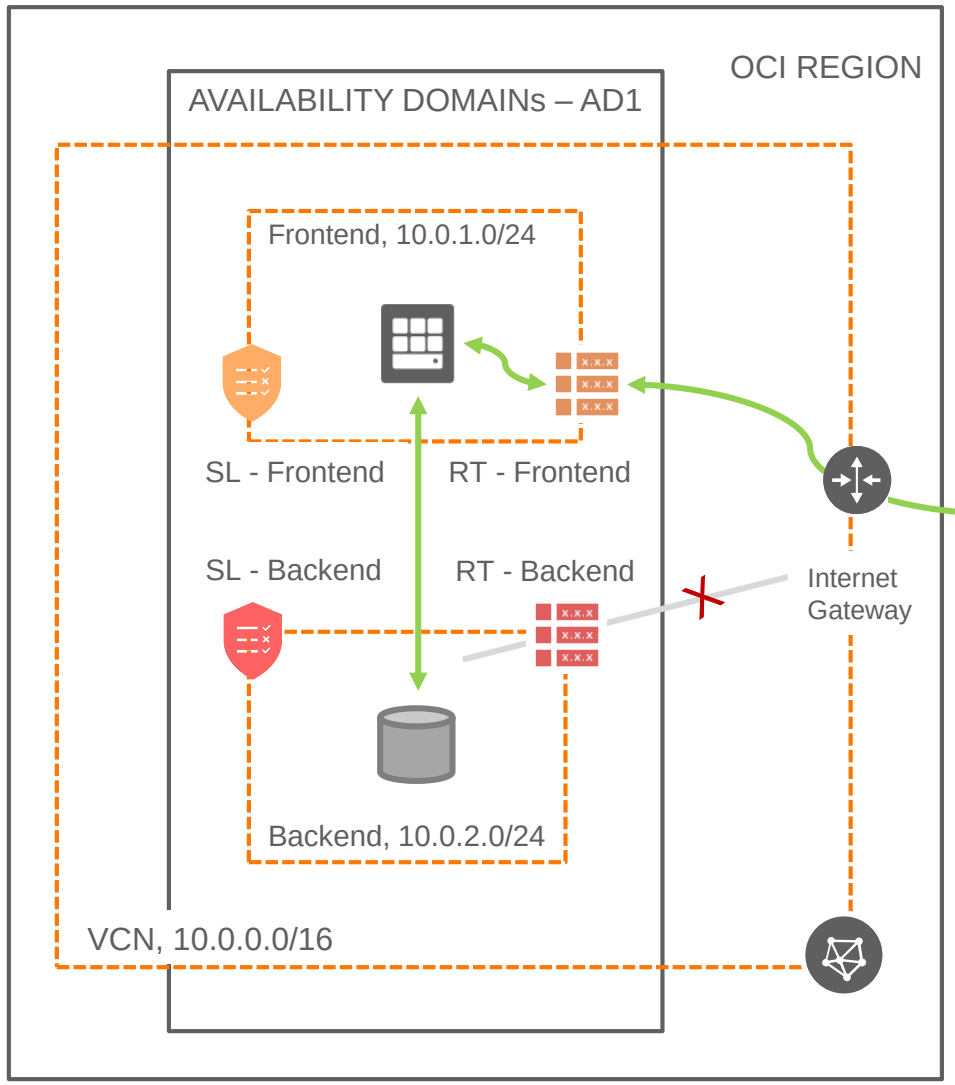
- Default Route Table
- Default Security List
- Default set of DHCP options

You can't delete these default components; however, you can change their contents (e.g. individual route rules). And you can create more of each kind of component in your cloud network (e.g. additional route tables).

VCN Review

- Subnets can have one Route Table and multiple (5*) Security Lists associated to it
- Route table defines what can be routed out of VCN
- Private subnets are recommended to have individual route tables to control the flow of traffic outside of VCN
- All hosts within a VCN can route to all other hosts in a VCN (no route table required)
- Security Lists manage connectivity north-south (incoming/outgoing VCN traffic) and east-west (internal VCN traffic between multiple subnets)
- OCI follows a white-list model (you must manually specify white listed traffic flows); By default, things are locked down
- Instances cannot communicate with other instances in the same Subnet, until you permit them to!

VCN Review



Destination CIDR	Route Target
0.0.0.0/0	Internet Gateway

	Type	CIDR	Protocol	Source Port	Dest Port
Stateful	Ingress	0.0.0.0/0	TCP	All	80
Stateful	Egress	10.0.2.0/24	TCP	All	1521

Destination CIDR	Route Target
0.0.0.0/0	NAT/ Service gateway /DRG

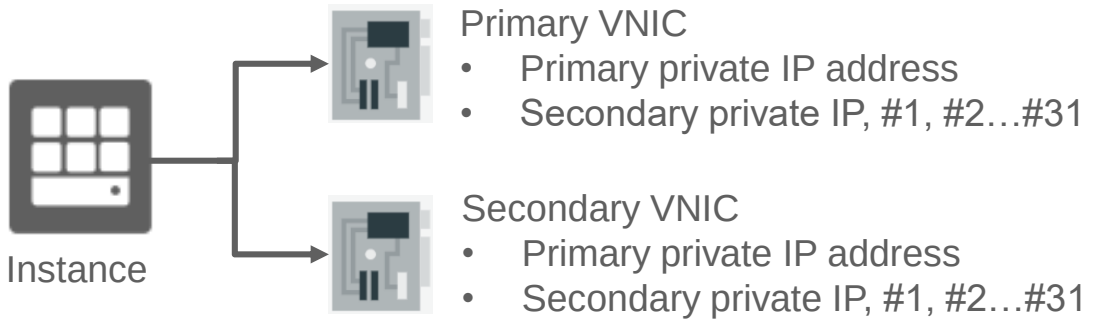
	Type	CIDR	Protocol	Source Port	Dest Port
Stateful	Ingress	10.0.1.0/24	TCP	All	1521
~~Stateful~~	~~Egress~~		~~All~~	~~All~~	

Internal DNS

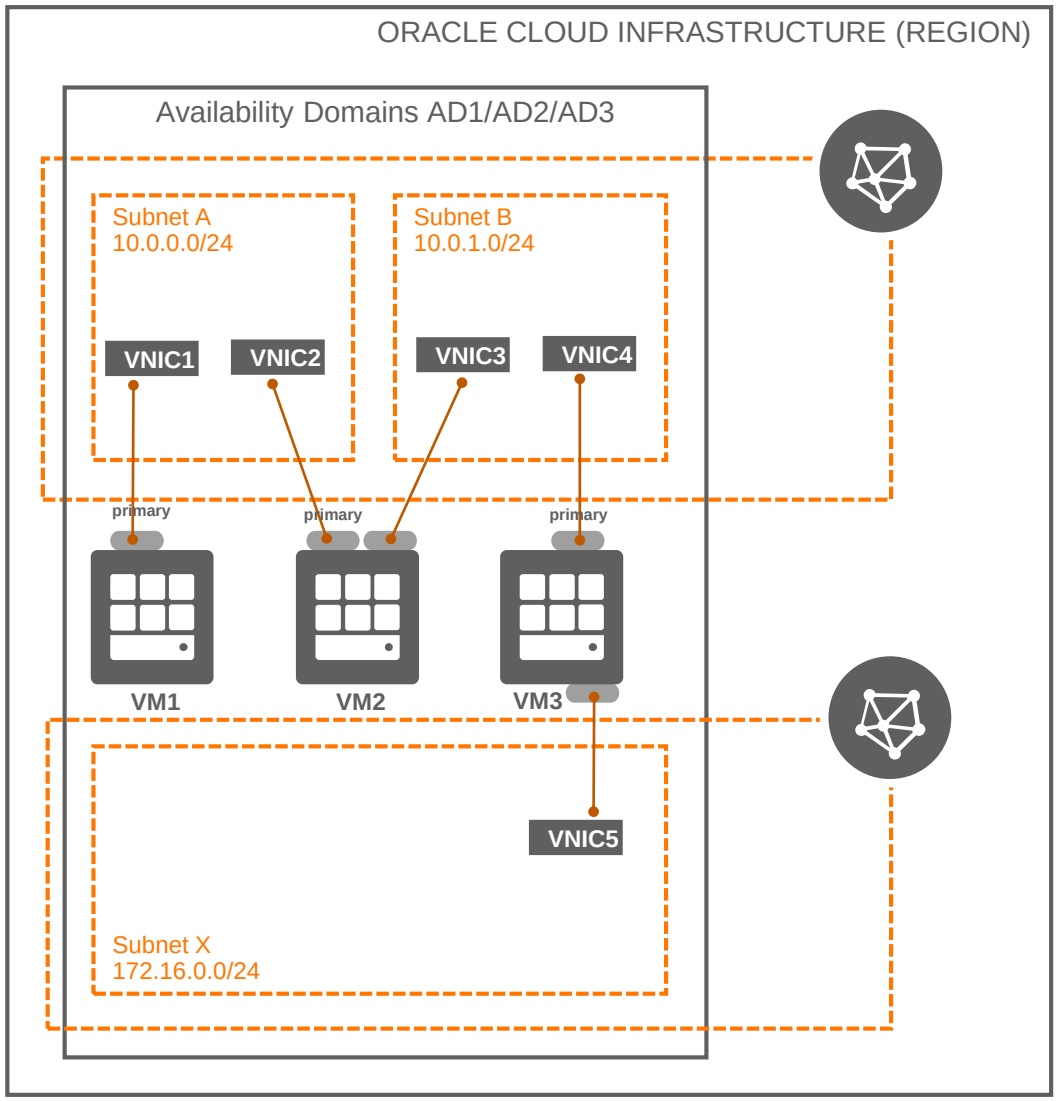
- The VCN Private Domain Name System (DNS) enables instances to use hostnames instead of IP addresses to talk to each other
- Options:
  - Internet and VCN Resolver: default choice for new VCNs
  - Custom Resolver: lets instances resolve the hostnames of hosts in your on-premises network through IPsec 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 (additional VNICs called secondary VNICs)
- Each VNIC has one primary private IP; can have additional private IPs called secondary private IPs

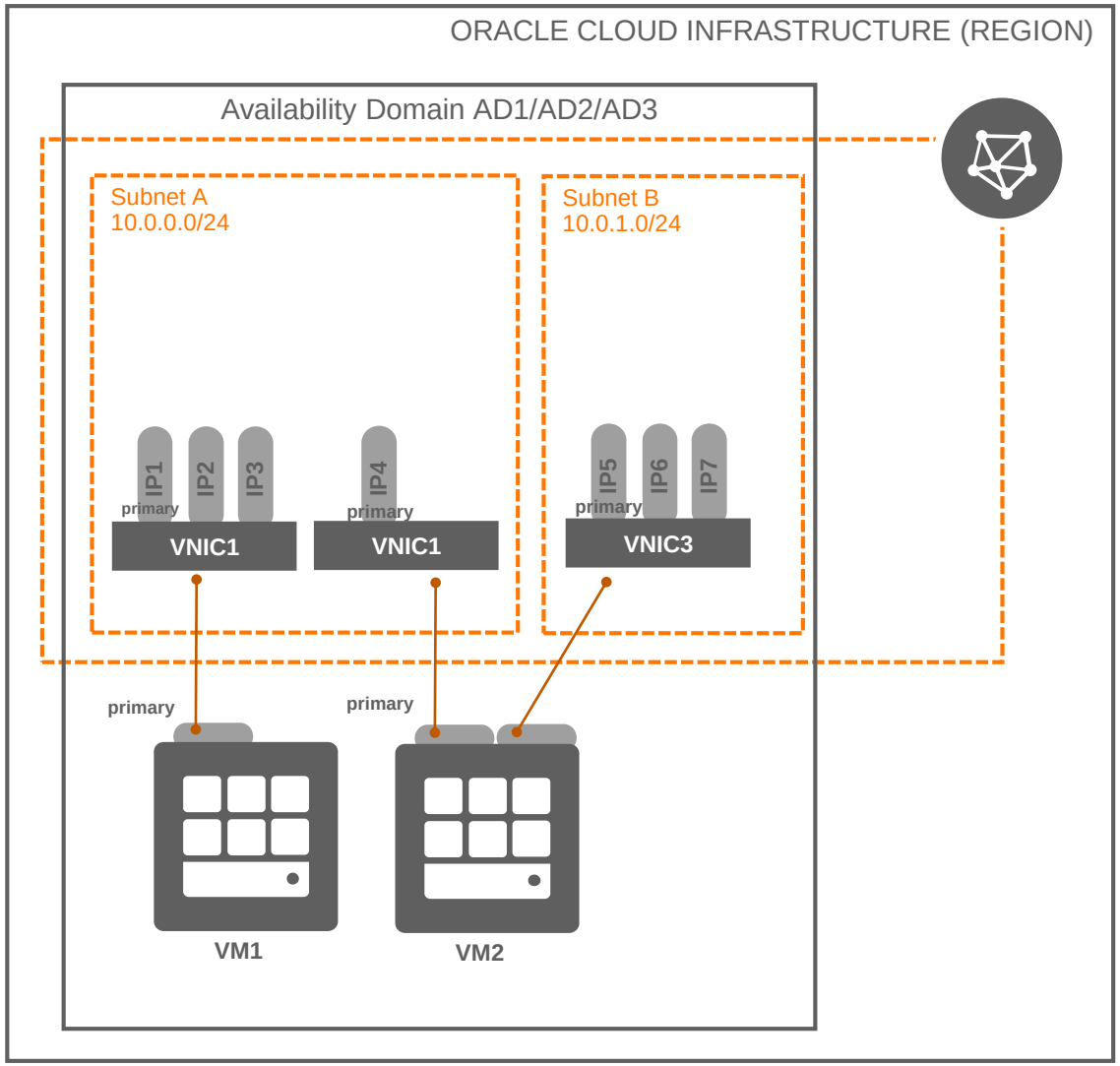


Multiple VNICs on virtual machines



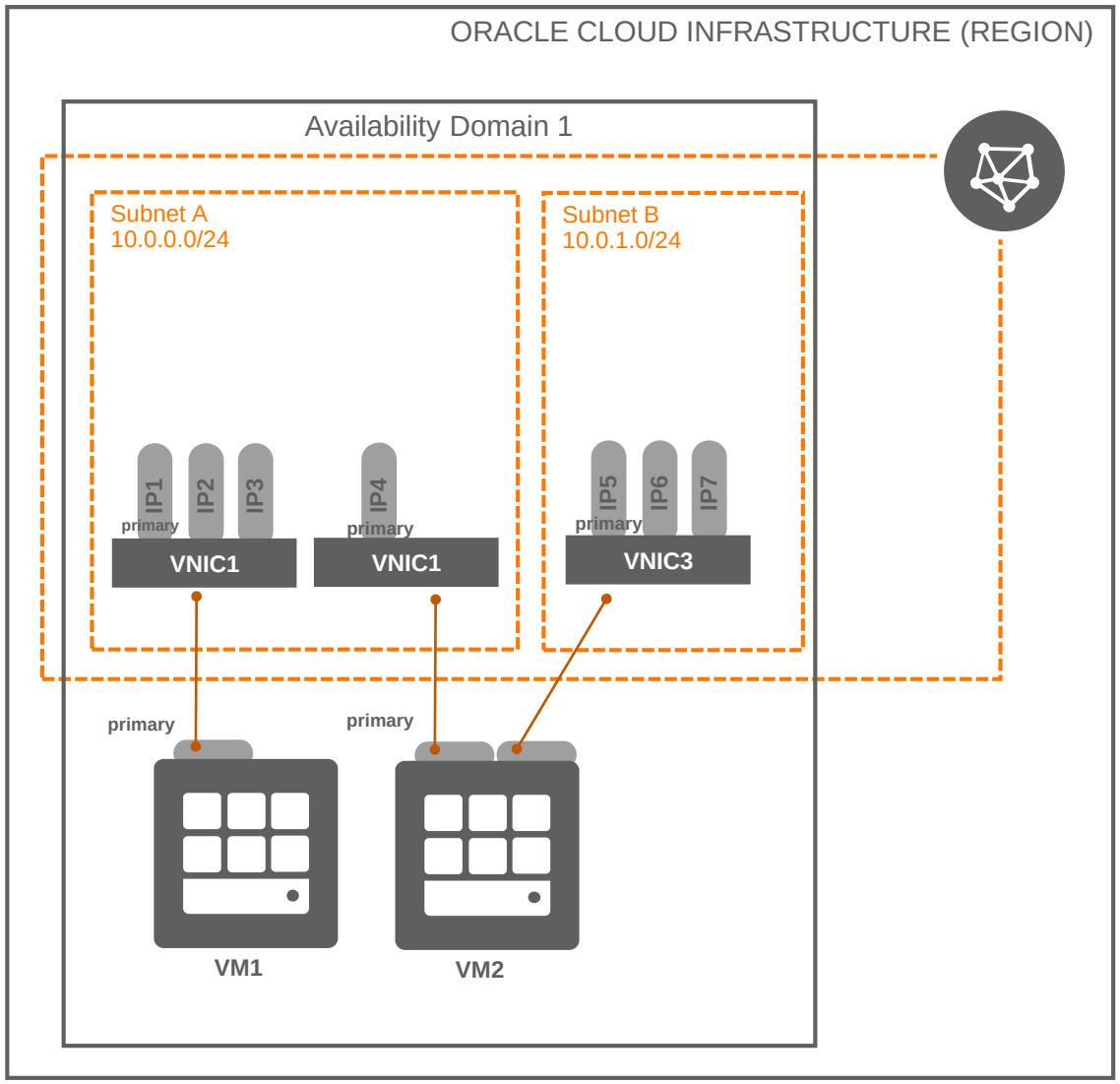
- Every VM has one primary VNIC created at launch, and a corresponding Ethernet device on the instance with the IP address configuration of the primary VNIC
- When a secondary VNIC is added, new Ethernet device is added and is recognized by the instance OS
  - VM1 - single VNIC instance
  - VM2 - connected 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

Secondary IP addresses on VNICs



- Every VNIC is assigned a primary private IP address when it is created, which is configured automatically on the corresponding Ethernet device in the instance OS
- Every VNIC can have additional private IPs called Secondary private IPs (max of 31)
- Secondary private IP assigned only after the instance is launched (or the secondary VNIC is created/attached)
- 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 the corresponding Ethernet device

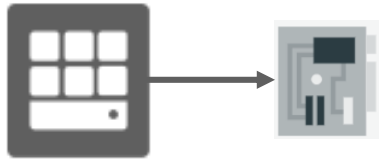
Secondary IP addresses on VNICs



- Possible to move a secondary private IP from a VNIC on one instance to a VNIC on another instance if both VNICs belong to the same subnet (use case: instance failover)
- The instances can be in same or different Availability Domains if we use Regional subnets

Public IP

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



Instance

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)

Public IP

- Public IP types: Ephemeral and Reserved
  - Ephemeral: temporary and existing for the lifetime of the instance
  - Reserved: Persistent and existing beyond the lifetime of the instance it's assigned to (can be unassigned and then reassigned to another instance)
  - Ephemeral IP can be assigned to primary private IP only (hence, only 1 per VNIC v/s a max 32 for Reserved IP)
- No charge for using Public IP, including when the Reserved public IP addresses are unassociated

Virtual Cloud Network Demo

VCN Pricing

- Data Transfer charges apply at the published rates below

	Metric	Pay as You Go	Monthly Flex
Outbound Data Transfer - First 10 TB / Month	GB/month	Free	Free
Outbound Data Transfer - Over 10 TB / Month	GB/Month	$0.0085	$0.0085
Inbound Data Transfer	GB/Month	Free	Free

- No charge for data transfer between Availability Domains within a region

Summary

- Key Virtual Cloud Network (VCN) concepts
  - Subnets, Route Table, Security Lists, Private IP, Public IP
- OCI connectivity options
  - Internet Gateway, NAT Gateway, Service Gateway, Local and Remote Peering
  - VPN, FastConnect (next module)

ORACLE®
Cloud Infrastructure

cloud.oracle.com/iaas

cloud.oracle.com/tryit