



Oracle Cloud Infrastructure (OCI)

Networking Services

Jun 1, 2025

Agenda

OCI Networking Core Components

- Overview on VCN
- IP Management
- VCN Security
- Routing & Gateways
- Load Balancing
- Web Application Firewall (WAF)
- Network Firewall
- Domain Name System (DNS)

1

WAN Connectivity (OCI | On-prem | Multicloud)

- Dynamic Routing Gateway (DRG)
- Site-to-Site VPN
- Fast Connect
- Oracle Interconnect with Azure and GCP

2

Customer Onboarding

- Hub & Spoke Architecture
- Redundant Connectivity
- Multi-Region Communication
- DRCC

3

Tools to Troubleshoot Network Issues

- Network Visualizer
- Network Path Analyzer (NPA)
- Inter-Region Latency Dashboard
- VCN Flow Logs

4

OCI Network Core Components

Chapter Agenda

- 1 Overview on VCN
- 2 VCN Security
- 3 Routing & Gateways
- 4 Load Balancing
- 5 Web Application Firewall (WAF)
- 6 Network Firewall
- 7 Domain Name System (DNS)
- 8 IP Management



- **What is a Virtual Cloud Network (VCN) ?**

- **Each VCN is subdivided into Subnets**

- **To secure your resources within the VCN, use security rules:**

e.g.

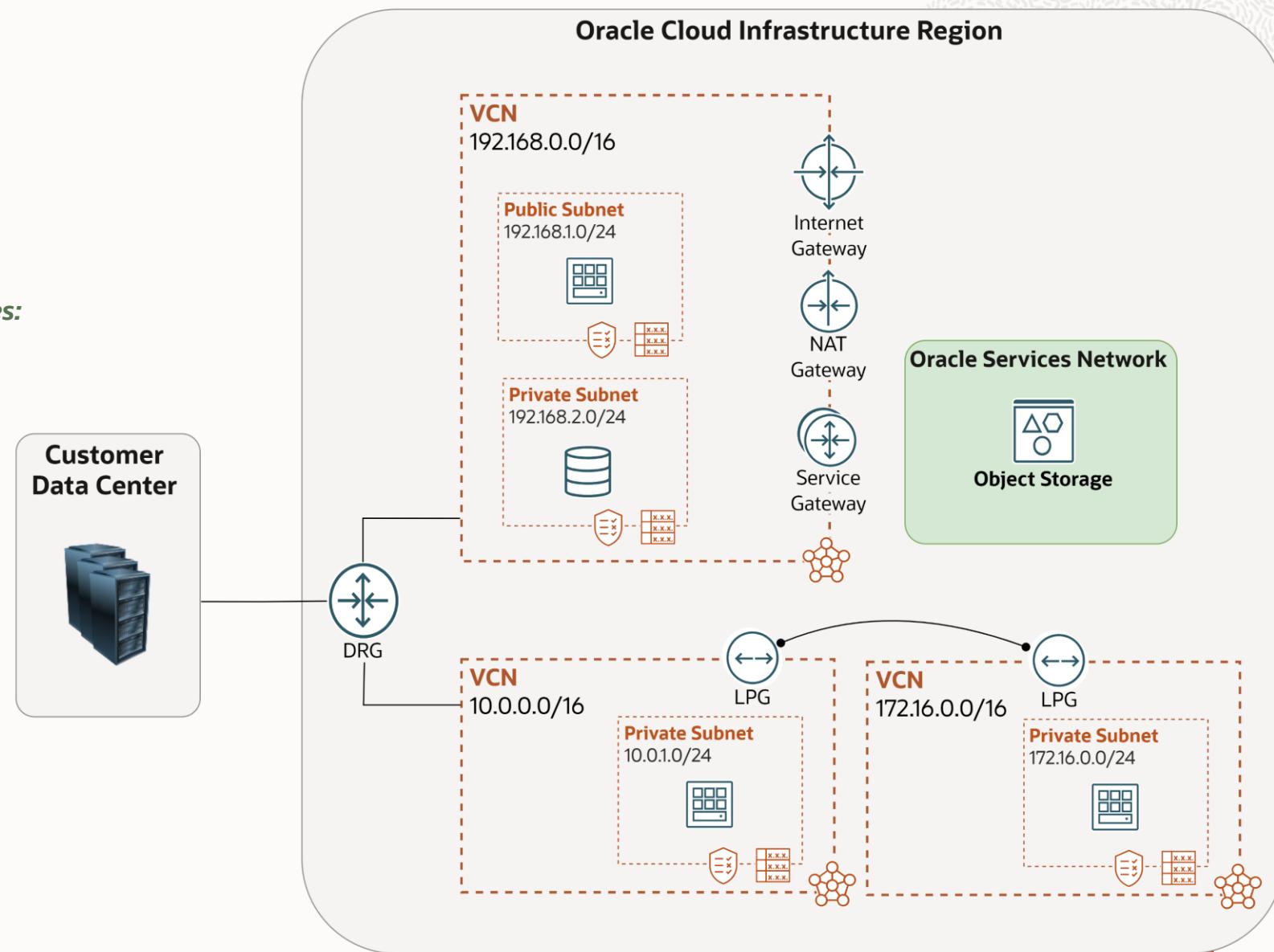
Allow inbound SSH traffic (port 22)

Allow inbound & outbound web traffic (port 80)

...

- **To route traffic out of the VCN, use Route Tables**

- **What are the Gateways types available in OCI ?**

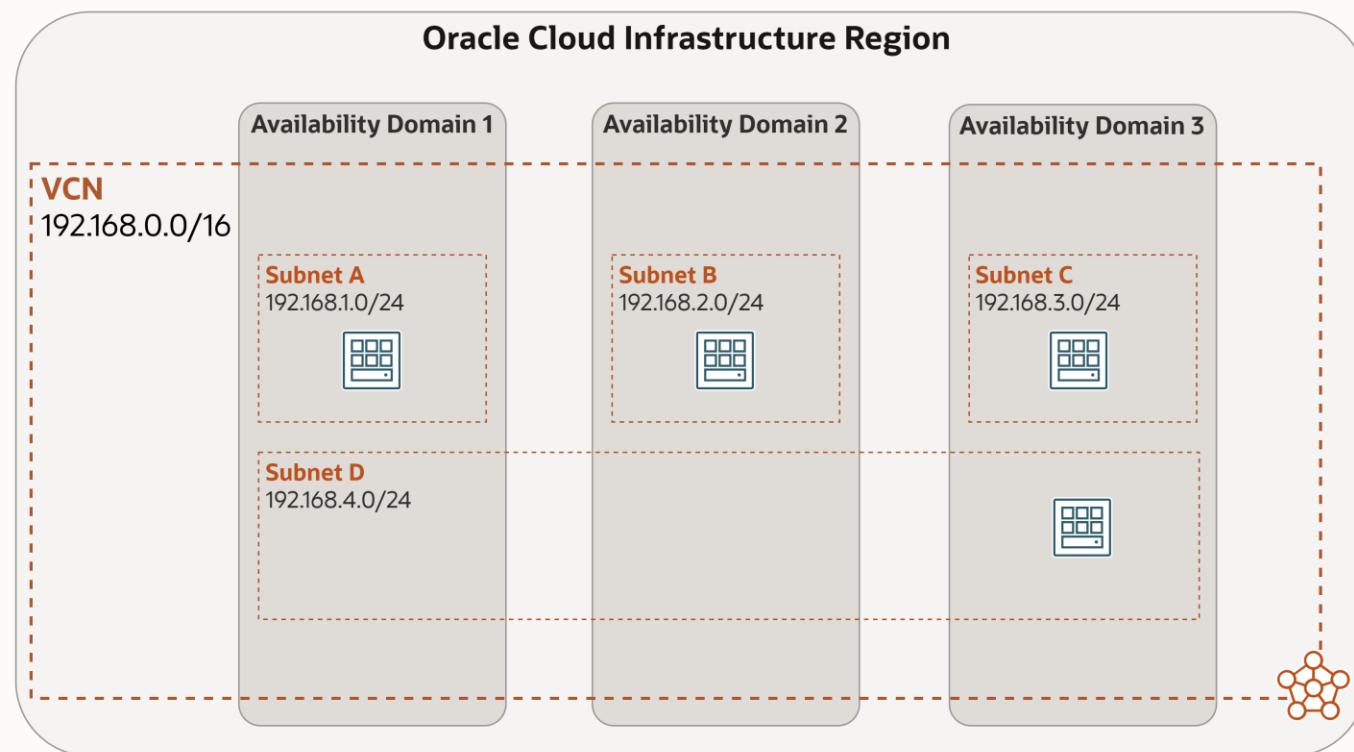


Virtual Cloud Network (VCN)

- 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 contiguous IPv4 CIDR blocks of your choice.
- A VCN resides within a single region.

Subnet

- Each VCN network is subdivided into subnets.
- Each subnet can be AD-specific or **Regional (recommended)**
 - AD specific subnet is contained within a single AD in a multi-AD region.
 - Regional subnet spans all three ADs 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 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).
- VNIC is a component that enables a compute instance to connect to a VCN. The VNIC determines how the instance connects with endpoints inside and outside the VCN.



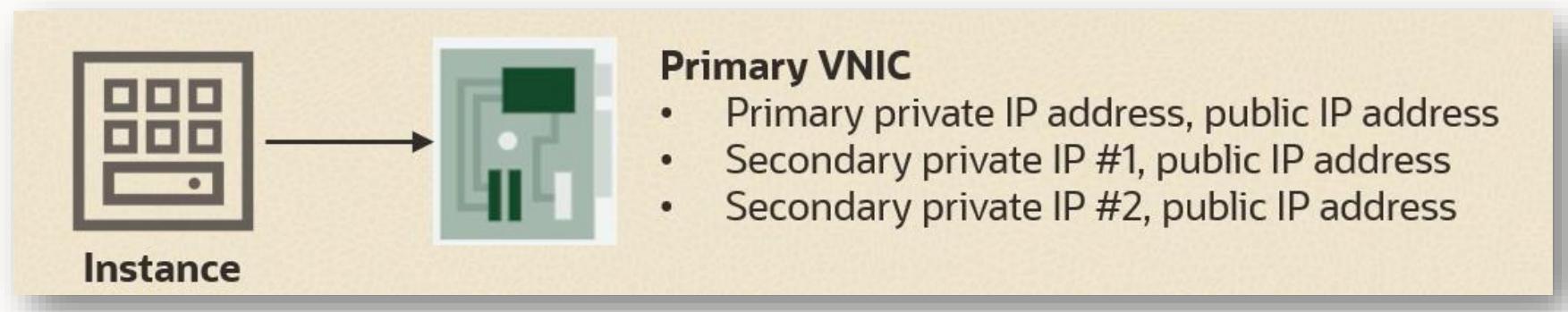
IP Management Agenda

- 1 OCI Virtual Network Interface Cards (VNICs)
- 2 Private IPv4 Addresses (Including Reserved Private IPs)
- 3 Public IP Addresses (Including Reserved Public IPs, BYOIP, IP Pools)
- 4 IPv6 on OCI
- 5 IP Address Insights
- 6 Bring Your Own ASN

OCI VNICs

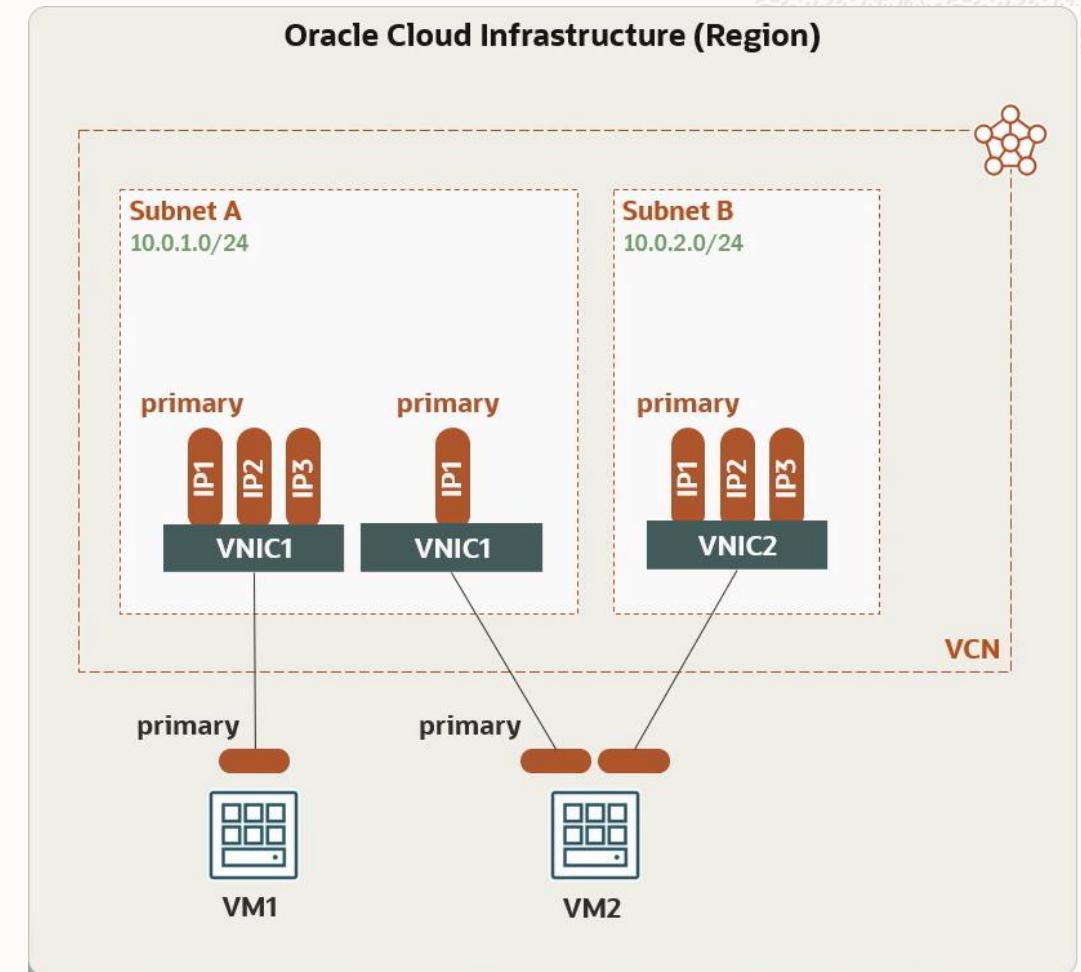
A Virtual Network Interface Card (VNIC) enables a compute instance to connect to a VCN and determines how the instance connects with endpoints inside and outside the VCN. Each VNIC resides in a subnet in a VCN and include these items:

- Up to 32 optional secondary IPv6 addresses.
- An optional public IPv4 address for each private IP, chosen by Oracle but assigned by you at your discretion.



OCI VNICs

- 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, a new Ethernet device is added and is recognized by the instance OS.



Private IPv4 Addresses

RFC 1918

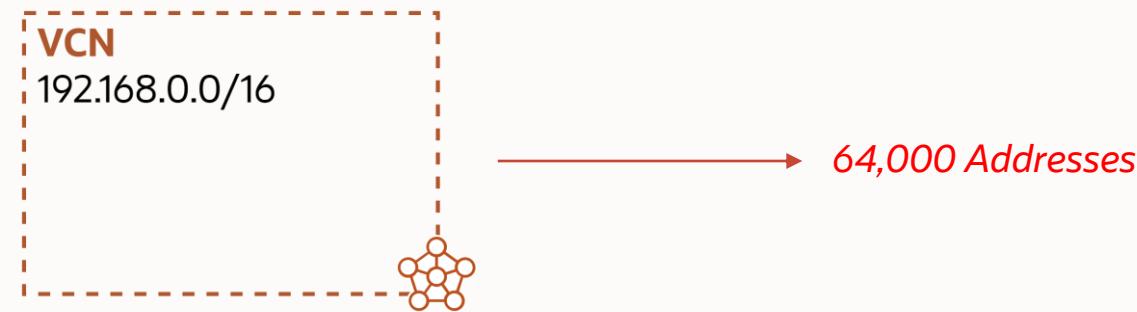
“Address Allocation for Private Internets”

RFC 1918 is a recommendation from the engineering task force for the IANA (Internet Assigned Numbers Authority) to reserve the following IPv4 address blocks for private use:

Class	RFC 1918 prefix	IP address range
A	10.0.0.0/8	10.0.0.0 – 10.255.255.255
B	172.16.0.0/12	172.16.0.0 – 172.31.255.255
C	192.168.0.0/16	192.168.0.0 – 192.168.255.255

Private IPv4 Addresses for Your VCN

- Allowable OCI VCN size range is from /16 through /30.



- A Private IP address enables communication with resources inside the VCN or with hosts in your on-premises network, but not with the hosts on the Internet.
- VCN reserves the first two IP addresses and the last one in each subnet's CIDR.

What Are Reserved Private IPs ?

- Static IPv4/IPv6 addresses you can take out of the dynamic pool inside a subnet.
- Remain assigned across reboots; can be re-attached to any VNIC in the same subnet.
- Avoids IP churn and simplifies DNS / firewall rules.

Reserved Private IPs – Key Use Cases

-  **Failover / HA** – Move the IP to a standby instance in seconds.
-  **Blue-Green Deployments** – Swap IP between versions with zero DNS change.
-  **Maintain Consistent IPs Across Lifecycle** – Reuse reserved IPs across replacements or re-creations of instances.
-  **Static IPs for Licensing or Compliance** – Some apps require fixed IPs for licensing, auditing, or compliance.
-  **Testing & DevOps Scenarios** – Use reserved IPs to test configurations before VM creation. Helpful in CI/CD pipelines, replicated environments, etc.
-  **Audit & Compliance** – Predictable IPs simplify security policies.

Reserved Private IPs – Feature Highlights

- Supports both IPv4 and IPv6 reserved addresses.
- Integrates with IP Address Insights for subnet-level visibility.
- Console, CLI, and Terraform support on day 1.

Reserving an IP

1. Navigate to Networking>Virtual Cloud Networks>VCN Name>Subnet Details>IPv4 addresses or IPv6 addresses.
2. Click **Add Reserved IP Address**, IPv4 or IPv6 and add a specific address.
3. Provide a name & description (and optionally hostname), then add reserved IPv4 or IPv6 address.
4. Attach the reserved IP to a VNIC in the same subnet.
5. You can reserve existing subnets private IPs to make sure it is not going to be reused in the future by other resources.

Reserving an IP console



AVAILABLE

web-tier-subnet1

Edit Move resource Add tags **Terminate** Create path analysis ▾

Details Tags

Subnet Information

OCID: ...h25eognq [Show](#) [Copy](#)
 IPv4 CIDR Block: 172.17.1.0/24
 IPv6 Prefix: -
 Virtual Router MAC Address: [REDACTED]
 Subnet Type: Regional
 Compartment: [REDACTED]
 DNS Domain Name: ...evcn.com [Show](#) [Copy](#)

Resources **IPv4 addresses**

View IP addresses of all resources in this subnet.

	Name	IP Address	State	Lifetime	Fully qualified domain name	Created	⋮
<input type="checkbox"/>	test	172.17.1.2	Available	Reserved	-	Tue, Apr 22, 2025, 16:57:34 UTC	⋮
<input type="checkbox"/>	PE_eu-amsterdam-1_eb4d2931-8538-4c39-8717-8e89ced72f51	172.17.1.229	Assigned	Ephemeral	pe-eu-amsterdam-1-eb4d2931-8538-4c39-8717-8e89ced72f51	Tue, Apr 22, 2025, 14:06:30 UTC	⋮
<input type="checkbox"/>	WebServer2_AppVCN2	172.17.1.196	Assigned	Ephemeral	webserver2-appvcn2	Mon, Jan 29, 2024, 18:37:39 UTC	⋮
<input type="checkbox"/>	WebServer1_AppVCN2	172.17.1.209	Assigned	Ephemeral	webserver1-appvcn2	Fri, Jan 19, 2024, 11:27:07 UTC	⋮

Add reserved IPv4 address Reserve IP address Remove IP address reservation

All Copyright © 2025, Oracle and/or its affiliates 0 selected Showing 4 items < 1 of 1 >

Reserving Existing Ephemeral in Bulk

- To reserve all IP addresses in bulk, select the **Name** checkbox, and click **Reserve IP address**. You can also select several IP addresses individually.

Resources

IPv4 addresses

View IP addresses of all resources in this subnet.

Add reserved IPv4 address Reserve IP address Remove IP address reservation

<input type="checkbox"/>	Name	IP Address	State	Lifetime	Fully qualified domain name	Created	⋮
<input type="checkbox"/>	test2	172.17.1.3	Available	Reserved	-	Tue, Apr 22, 2025, 17:05:50 UTC	⋮
<input type="checkbox"/>	test	172.17.1.2	Available	Reserved	-	Tue, Apr 22, 2025, 16:57:34 UTC	⋮
<input checked="" type="checkbox"/>	PE_eu-amsterdam-1_eb4d2931-8538-4c39-8717-8e89ced72f51	172.17.1.229	Assigned	Ephemeral	pe-eu-amsterdam-1-eb4d2931-8538-4c39-8717-8e89ced72f51	Tue, Apr 22, 2025, 14:06:30 UTC	⋮
<input checked="" type="checkbox"/>	WebServer2_AppVCN2	172.17.1.196	Assigned	Ephemeral	webserver2-appvcn2	Mon, Jan 29, 2024, 18:37:39 UTC	⋮
<input checked="" type="checkbox"/>	WebServer1_AppVCN2	172.17.1.209	Assigned	Ephemeral	webserver1-appvcn2	Fri, Jan 19, 2024, 11:27:07 UTC	⋮

3 selected Showing 5 items < 1 of 1 >

Security Lists (1)

Alarms

Logs

IP Address Insights

CIDR/prefix utilization

IPv4 Addresses

IPv6 Addresses

Filters

Lifetime

All

State

All

Tag filters add | clear

Reserved Private IPs – Best Practices

- Reserve IPs early in project design to avoid mid-stream renumbering.
- Periodically audit unused reserved IPs to free them for other teams.
- Remember: reservations are ****subnet-scoped****, not VCN-wide.
- Moving an IP briefly interrupts traffic—plan maintenance windows.

Public IPv4 Addresses

- Addresses that are reachable from the Internet.
- If a resource in your tenancy needs to be directly reachable from the Internet, it must have a public IP address.
- When you launch an instance in a public subnet, by default, the instance gets a public IP unless you say otherwise.
- There is **no charge** for using Public IPs, including when Reserved Public IP addresses are unassociated to a resource.



- ✓ *VM must be in a public subnet.*
- ✓ *VM must have a public IP address.*
- ✓ *VM's VCN must have an Internet Gateway.*
- ✓ *Public Subnet must have route tables and security lists configured accordingly.*

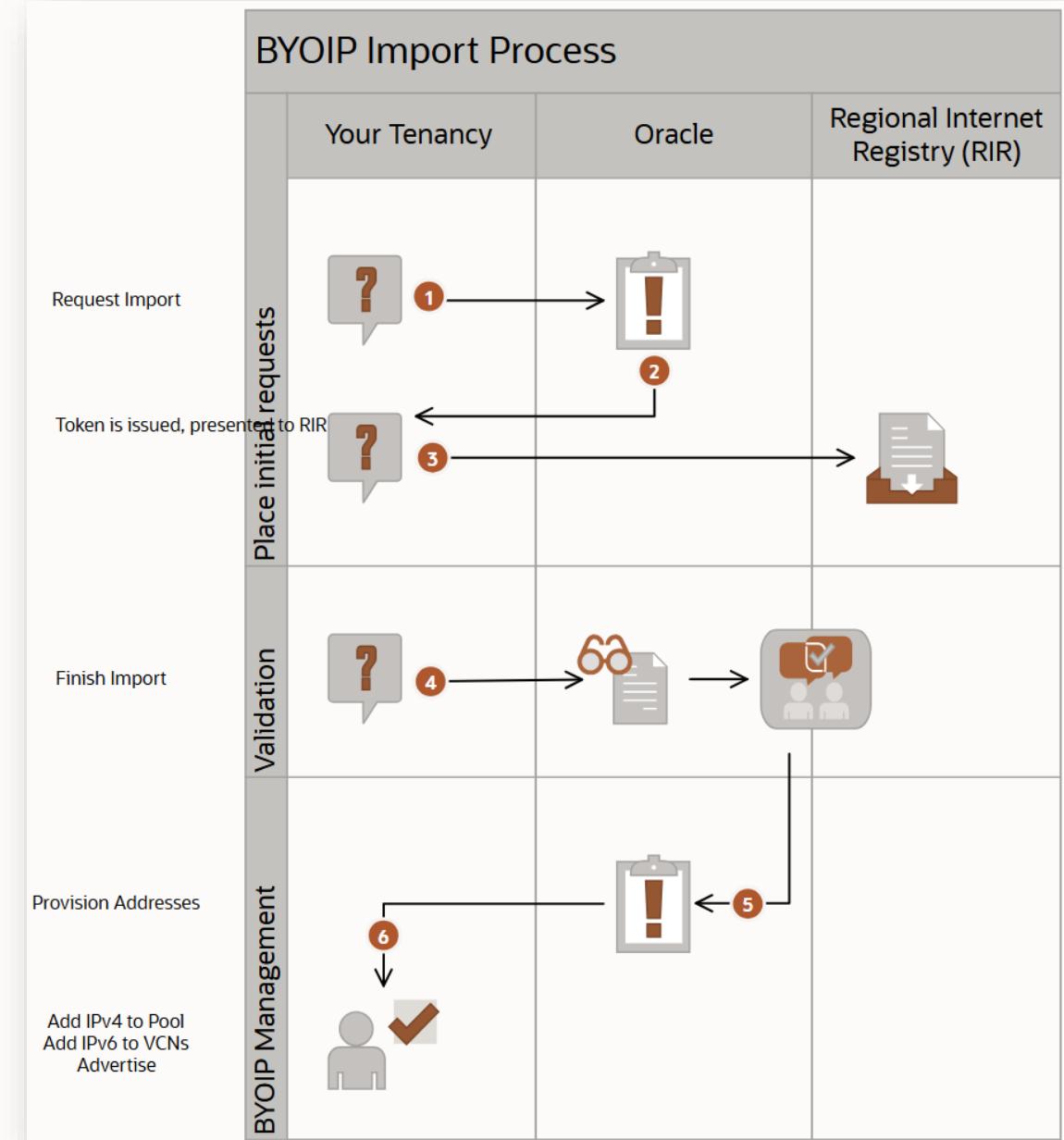
Types of Public IPs

- **Ephemeral:** A temporary public IP address that is assigned to resources for the lifetime of the resource. For example, once a VM instance with an ephemeral IP address is destroyed, the ephemeral public IP address is returned to the OCI IP pool for re-use by another device.
- **Reserved:** A persistent public IP address can be assigned, unassigned, and re-assigned to resources. For example, you can unassign the reserved public IP address and then reassign it to another instance whenever you want to.

Bring Your Own IP (BYOIP)

- Oracle allows you to Bring Your Own IP (BYOIP) address space to use with resources in OCI, in addition to using Oracle-owned addresses.
- Let you manage your IPv4 CIDR blocks and IPv6 prefixes to align with your existing security, management, and deployment policies and achieve:
 - **Solution continuity and hardcoded dependencies:** Your VCN is an extension of your public Internet presence, without needing to reinvent policies and management processes. If you have IP addresses hard-coded in devices or built architectural dependencies on specific IP addresses, using BYOIP you have a smooth migration to Oracle Cloud Infrastructure.
 - **IP pool management:** Some network administrators require the ability to summarize groups of IPv4 addresses into pools and to create resources for deployment such as load balancers, firewalls, or web servers. IP Pool management provides tools to manage reserved public IPv4 addresses. IPv6 does not use IP Pool management.
 - **IP reputation:** Some internet services rely on a contiguous IP address space (such as a full span of IP addresses from 1 through 255) and act as a trusted contact point between services such as major email service providers and mail delivery systems.

Bring Your Own IP (BYOIP)



Public IP Pools

- A public IP pool is a set of IPv4 CIDR blocks allocated to a tenancy; and they be all or part of a BYOIP CIDR block.
- Public IP CIDR blocks assigned to a pool are available only for your tenancy.
- Public IP pools are available as a source for IP allocation when launching a NAT gateway, load balancer, or compute instance.

IPv6 on OCI

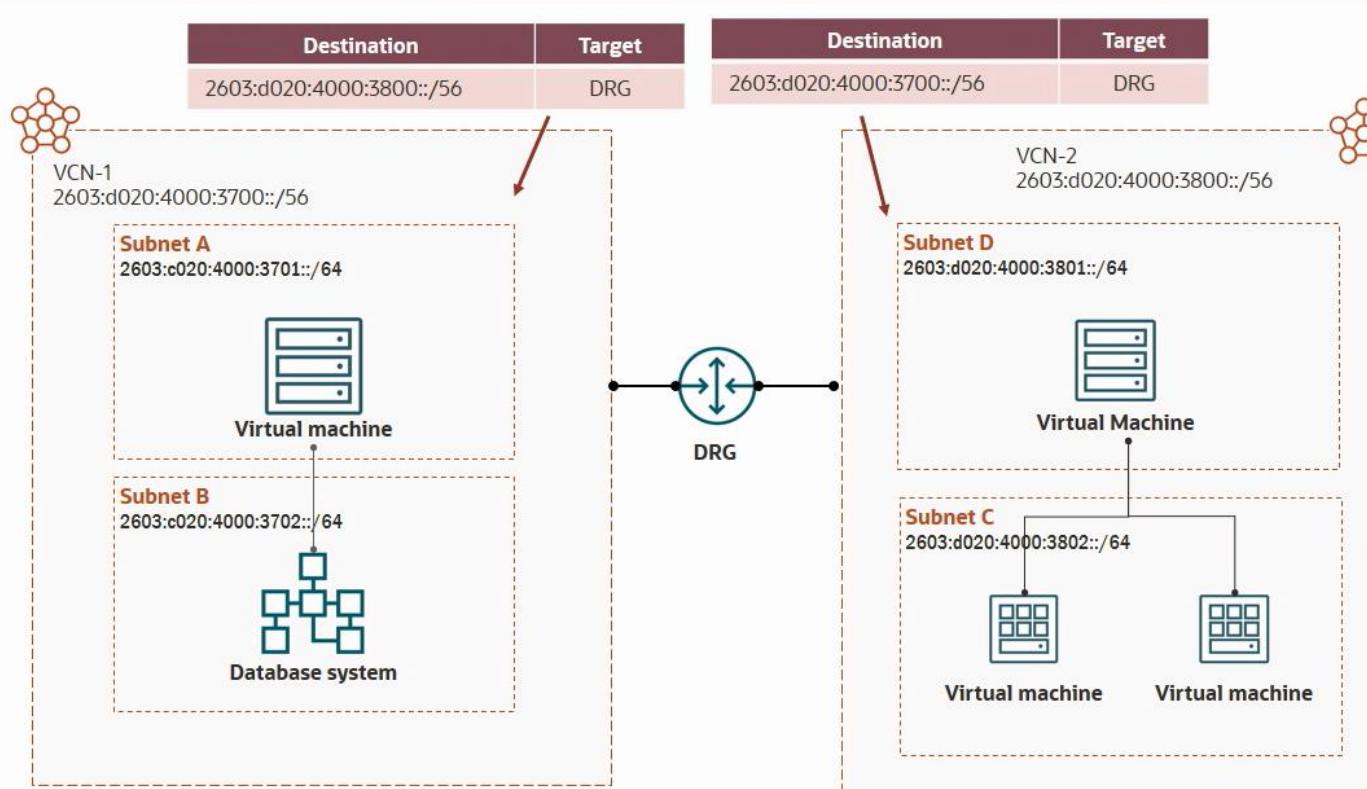
Supported Service	Features
Virtual Cloud Network (VCN)	Oracle-allocated Global Unicast Address (GUA) Prefix /56
	BYOIP IPv6 GUA Prefix /48 or larger
	Unique Local Address (ULA) Prefix /64 or larger
Subnet	/64 Prefix size
	Oracle-allocated IPv6 GUA, BYOIP IPv6 GUA, and/or ULA
Enabled Services	Compute instances
	Flexible LB
	Network load balancer (NLB)
	Network firewall (NFW)
	FastConnect
	VPN connect
	Dynamic Routing Gateway (DRG)
	Internet Gateway (IGW)

How to Route IPv6 to the Internet?

- OCI Internet gateways (IGW) support IPv6.
- An IPv6-enabled subnet can be a public or private subnet.
- A public IPv6 subnet with an IPv6 GUA prefix allocated can route directly to the Internet via the VCN Internet gateway (IGW).
- A private IPv6 subnet cannot route directly to the Internet even if it has an IPv6 GUA prefix allocated.

How to Route IPv6 Between VCNs and Regions?

- OCI local peering gateways (LPG) and dynamic routing gateways (DRG) support IPv6.
- Routing IPv6 between VCNs and regions is done in the same way as IPv4.



IP Address Insights

Monitors the utilization of IP addresses with hierarchical visibility.

Feature Capabilities:

- Gives you a consolidated view of IP addresses across tenancy/region.
- Correlate private IPv4 addresses with corresponding public IPv4 ones.
- Determine IP address utilization of your CIDRs.
- Create and manage alarms when IP utilization crosses a threshold.
- Find overlapping CIDRs and IP conflicts.
- Search for resources by IP address, name, or type.

IP Address Insights

ORACLE Cloud Cloud Classic >

Search resources, services, documentation, and Marketplace

Networking > IP management > IP Address Insights

IP management

IP Address Insights

IP address insights across your tenancy with hierarchical visibility into VCNs, subnets and individual resources, and ability to review IP conflicts, prefix utilization level, etc. centrally for ease of IP administration.

Overview

Reserved public IPs

BYOIP

Public IP pools

IP Address Insights

Filters [Restore default](#)

Search results [?](#)

Override search results and show all subnets and resources

Compartments (1/129)

[View](#)

Utilization greater than or equal to [?](#)

[View](#)

Resource	Resource Type	CIDR/Prefix/IP	Utilization i	Overlaps
> IMR_lhrVCN1	VCN	10.6.0.0/16	0.01%	-
> IMR_lhrVCN2	VCN	10.60.0.0/16	0.01%	-
ipam_vcn1	VCN	10.0.0.0/16	0.04%	⚠ 3 overlaps
nlbSubnet	Subnet	10.0.255.0/30	75%	-
Sub1	Subnet	10.0.1.0/27	40.63%	-
Resource1	Resource	10.0.1.14 (VNIC: ipam_vm10)	-	-
Resource2	Resource	10.0.1.20 (VNIC: ipam_vm4)	-	-

ipam_vcn1 overlaps

CIDR block/Prefix	VCN	Overlapping CIDR
10.0.0.0/16	noNat1_HubVCN	10.0.0.0/16
10.0.0.0/16	noNat3_mainVCN	10.0.0.0/16
10.0.0.0/16	noNat2_hubVCN	10.0.0.0/16

Showing 3 items < 1 of 1 >

IP Address Insights

Subnet level:

Networking > Virtual Cloud Networks > ipam_vcn1 > Subnet Details > CIDR/prefix utilization

Sub1

Available

S

[Edit](#) [Move resource](#) [Add tags](#) [Create path analysis ▾](#) [Terminate](#)

[Subnet Information](#) [Tags](#)

OCID: ...4nhvkq [Show](#) [Copy](#)
IPv4 CIDR Block: 10.0.1.0/27
IPv6 Prefix: —
Virtual Router MAC Address: 00:00:17:35:BF:BD
Subnet Type: Regional

Compartment: [\[REDACTED\]](#)
DNS Domain Name: sub1... [Show](#) [Copy](#)
Subnet Access: Public Subnet
DHCP Options: [Default DHCP Options for ipam_vcn1](#)
Route Table: [Default Route Table for ipam_vcn1](#)

CIDR/prefix utilization

Review the utilization level of the IPv4 CIDR block or IPv6 prefixes in this subnet, but you can set up an alarm only for IPv4 CIDR block at the desired threshold.

CIDR/prefix	Utilization	Address type
10.0.1.0/27	<div style="width: 40.63%;"></div> 40.63%	Private (IPv4)

[Security Lists \(1\)](#)
[Alarms](#)
[Logs](#)
[IPv6 Prefixes \(-\)](#)
[IP Address Insights](#)
[CIDR/prefix utilization](#)

Bring Your Own ASN (BYOASN)

- Autonomous System Number (ASN) is a unique number assigned to a network over the internet enabling different networks to exchange routing information with each other using the Border Gateway Protocol (BGP). ASN is also used for security policies to identify network traffic source, enabling you to filter traffic based on the originating network.
- Now you can bring your own ASN to OCI and use your existing ASN within the cloud environment.
- Currently supported for ARIN, RIPE and APNIC Regional Internet Registries (RIR) and is available across all OCI commercial regions.

BYOASN Key Capabilities

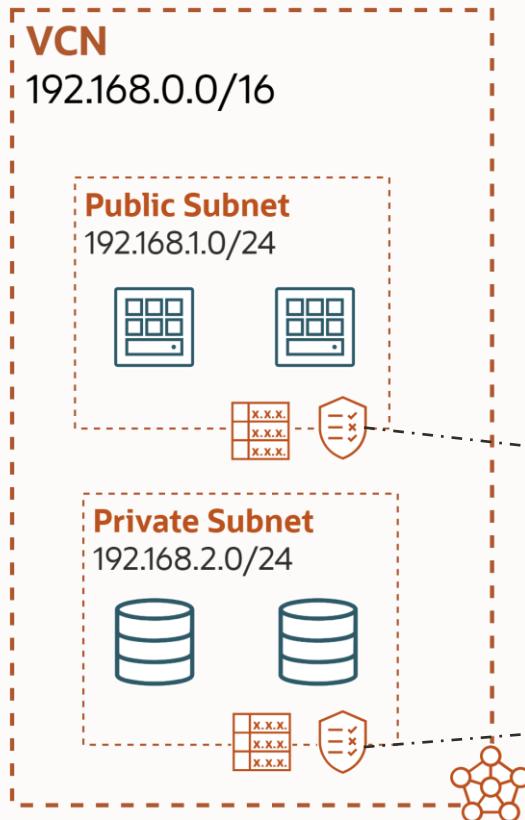
- No limit on the number of ASNs you can import into OCI.
- Import same ASN across multiple regions.
- You can prepend the ASN up to 20 times to influence the route preference, which can be used when setting up an active-standby or disaster recovery site.
- Support for both 2-byte and 4-byte ASN.
- Support for Console UI, CLI, API and Terraform.

VCN Security Agenda

- 1 Security Lists
- 2 Network Security Group (NSG)
- 3 Zero Trust Packet Routing (ZPR)
- 4 Bastion

Security Lists

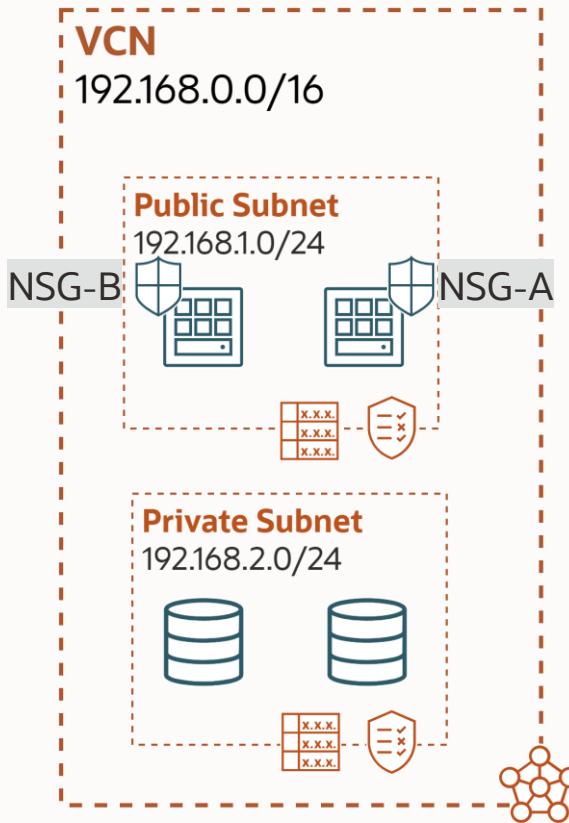
- A common set of firewall rules associated with a subnet and applied to all instances launched inside the subnet.
- Security list consists of rules that specify the types of traffic allowed in and out of the subnet.
- To use a given security list with a particular subnet, you associate the security list with the subnet either during subnet creation or later.
- Security list apply to a given instance whether it's talking with another instance in the VCN or a host outside the VCN.



	Direction	CIDR	Protocol	Source Port	Dest Port
Stateful	Ingress	0.0.0.0/0	TCP	All	80
Stateful	Egress	192.168.2.0/24	TCP	All	1521

	Direction	CIDR	Protocol	Source Port	Dest Port
Stateful	Ingress	192.168.1.0/24	TCP	All	1521

Network Security Group (NSG)



- A network security group (NSG) provides a virtual firewall for a set of cloud resources that all have the same security posture
- NSG consists of set of rules that apply only to a set of VNICs of your choice in a single VCN
- Currently, compute instances, load balancers and DB instances support NSG
- When writing rules for an NSG, you can specify an NSG as the source or destination. Contrast this with SL rules, where you specify a CIDR as the source or destination
- Oracle **recommends** using NSGs instead of SLs because NSGs let you separate the VCN's subnet architecture from your application security requirements

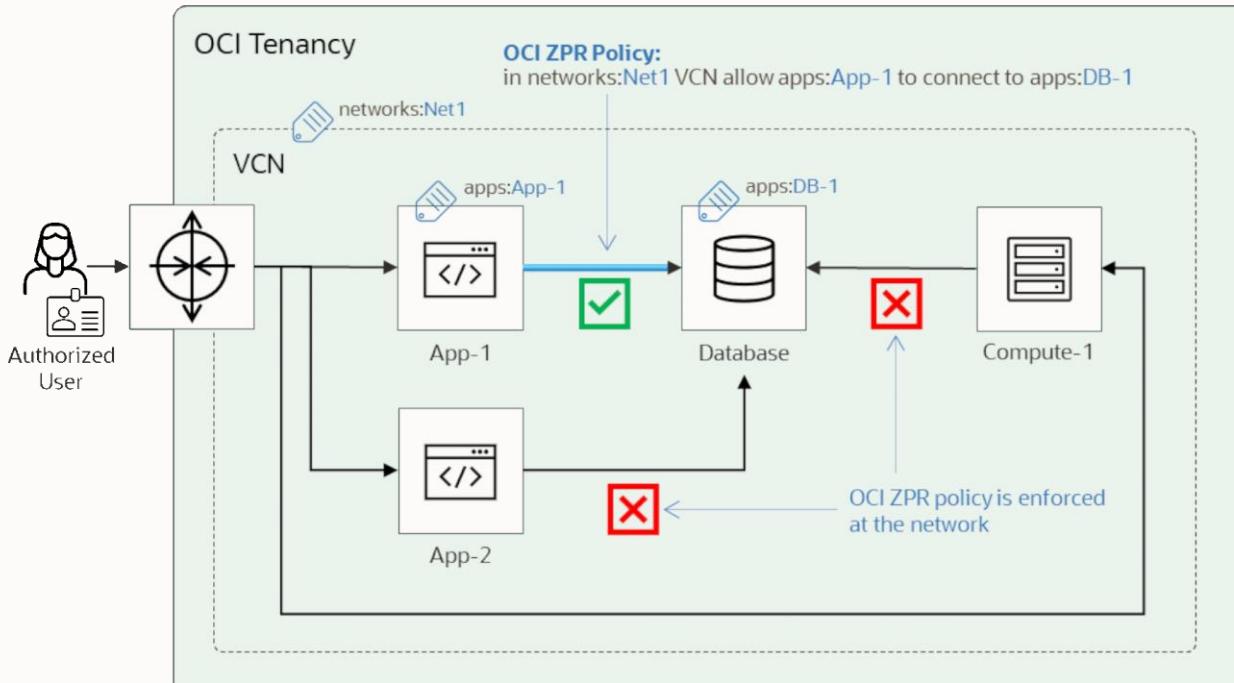
		Direction	CIDR	Protocol	Source Port	Dest Port
NSG-A	Stateful	Ingress	0.0.0.0/0	TCP	All	80
NSG-B	Stateful	Ingress	0.0.0.0/0	TCP	All	22

You can use SLs alone, NSGs alone, or both together.

Zero Trust Packet Routing (ZPR)

OCI ZPR provides internal and external threat protection from attackers, controlled with an additional network level security layer. It enables customers to define and enforce an intent-based, data-centric security policy, natively integrated with user and application attributes for resources within OCI and On-premises resources.

- **Simple, clear policies:** Protect your data with one easy-to-understand policy.
- **Data tagging for seamless protection:** Tag your sensitive data, and let the network enforce security policies automatically.
- **Future-proofed security:** Even if your network configuration changes, ZPR ensures data remains protected.
- **Provable security compliance:** Validate policies and prove they are working as intended.



Using ZPR with Other Security Methods

- ❑ Any VNIC or endpoint must have subnet security list rules that allow it to communicate.
- ❑ An NSG can add more rules on top of the security list rules for selected resources anywhere in a VCN.
- ❑ A **ZPR policy** can be layered on top of both security lists and NSG rules, or the ZPR policy can be in addition to a security list alone.



ZPR vs Security Rules

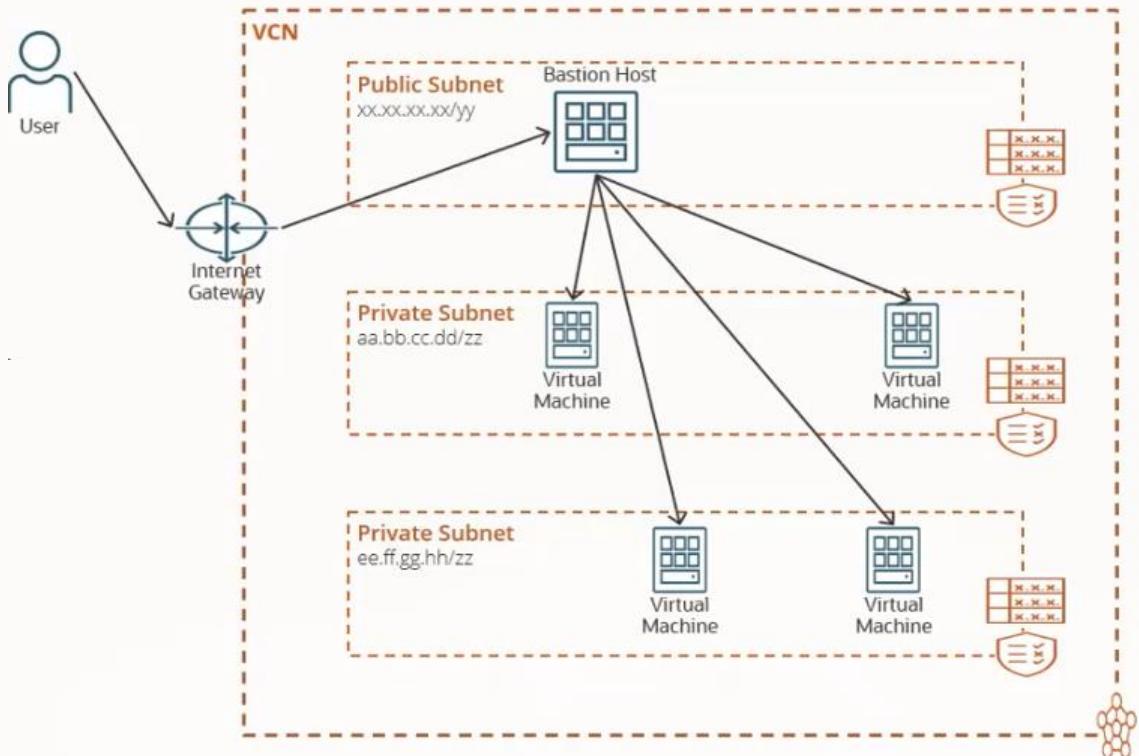
Security method	Applies to	Enable or disable	Limitations
Security list	All VNICs in a subnet or VCN	Not available	Maximum five security lists per subnet
Network security groups	Selected VNICs in a VCN	From the VNIC details page	Maximum five NSGs per VNIC
Zero Trust Packet Routing	Selected resources (VNICs and other resource types) in one or more VCNs	With a security attribute applied to the resource	Maximum three ZPR security attributes per resource

ZPR – Currently Supported OCI Resources

Service	Resource Types
<u>Compute</u>	instance instance configurations
<u>Database</u>	autonomous-databases cloud-autonomous-vmclusters cloud-vmclusters databases db-systems exadb-vm-clusters
<u>Networking</u>	vcns vnics PrivateEndpoint
<u>Network Load Balancer</u>	network load balancers

Bastion in the traditional way

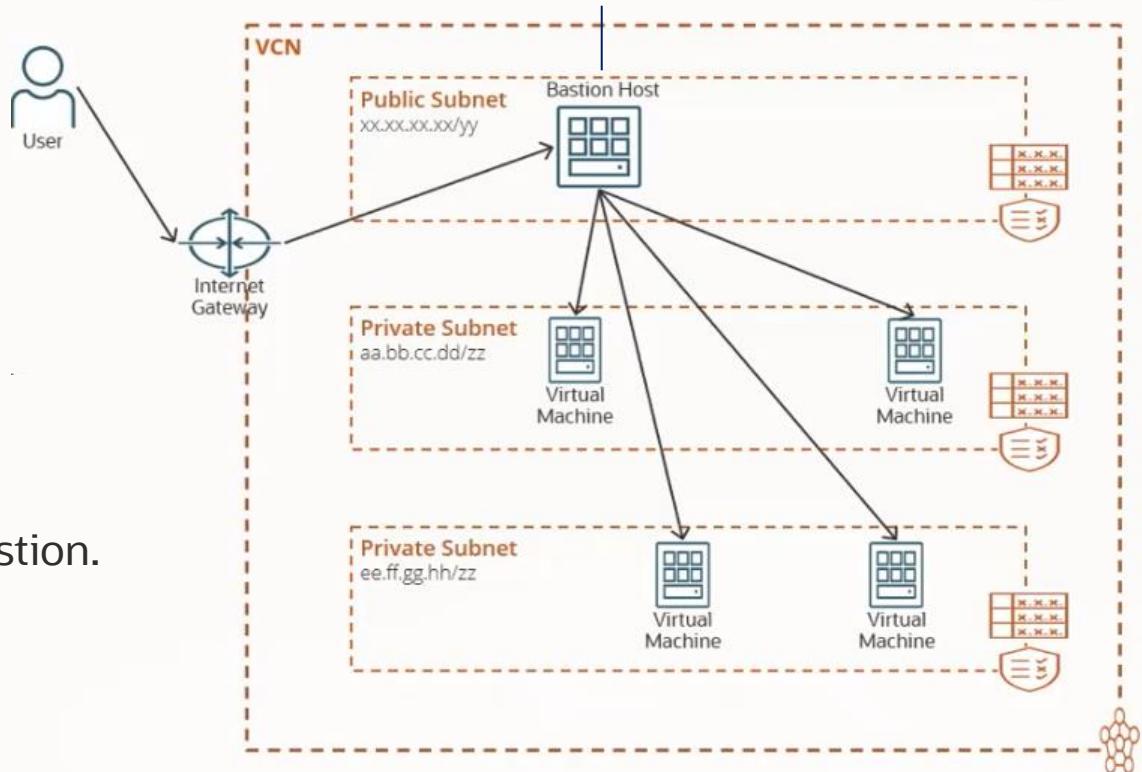
- A Bastion host is a special-purpose server or an instance that is used to configure to work against the attacks or threats. It is also known as the “Jump Box”.
- Bastion host basically provide an entry point into the private networks which are to be connected from external network securing from the attacks.
- While using Bastion service you must log in first to your Bastion host and then directed to the private instances.



Bastion in the traditional way

- Create a Public Subnet.
- Allocate public IP for bastion host.
- Compute management by OCI admin.
- Hardening of compute OS.
- SSH Keys management per user basis.
- Storing of SSH private keys for target compute in bastion.
- No session limit enforcement.
- Cost incurred to run the compute in OCI.

Linux VM acting as a bastion in OCI.

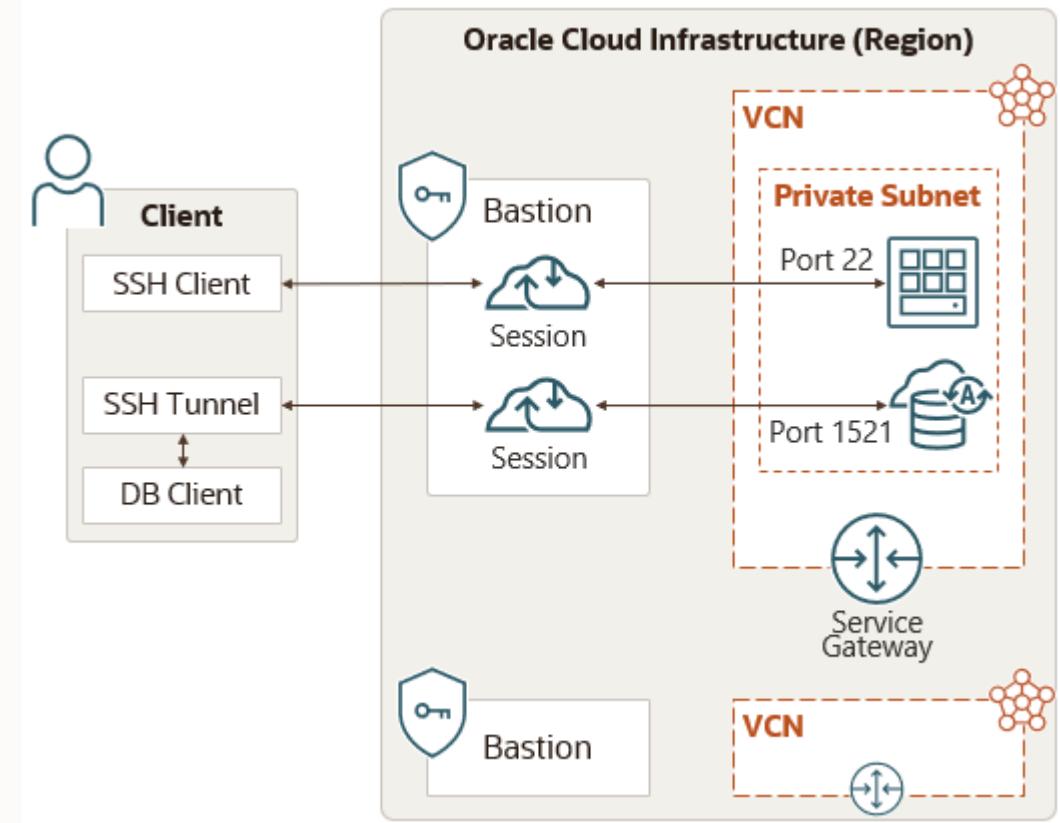


OCI Bastion

- OCI provided and managed service.
- There is no cost for using OCI Bastion.
- No public IP is needed, resulting in no surface attack area or zero-day vulnerabilities.
- Eliminate shared credentials, broad access limits, and other bad habits of using jump hosts.
- Restricted and time-limited access to target resources that don't have public endpoints.
- Targets can include resources like compute instances, DB systems, and Autonomous Database for Transaction Processing and Mixed Workloads databases.

OCI Bastion

- A bastion is associated with a single VCN. You cannot create a bastion in one VCN and then use it to access target resources in a different VCN.
- Bastion is a regional service. For example, bastion created in Frankfurt cannot be used to access resources in London.
- Bastion “Maximum session time-to-live (TTL)” is 3 hours and minimum is 30 minutes. The TTLs is configurable at the session level.
- Bastion is restricted with service limits per region per tenancy.
 - 5 bastions per region.
 - 20 active sessions per bastion.



Routing & Gateways Agenda

- 1 Route Tables
- 2 Per-Resource Routing
- 3 Key VCN Gateways (Internet Gateway, NAT Gateway, and Service Gateway)
- 4 Local VCN Peering
- 5 Remote VCN Peering

Route Table

Oracle Cloud Infrastructure Region

VCN

10.0.0.0/16

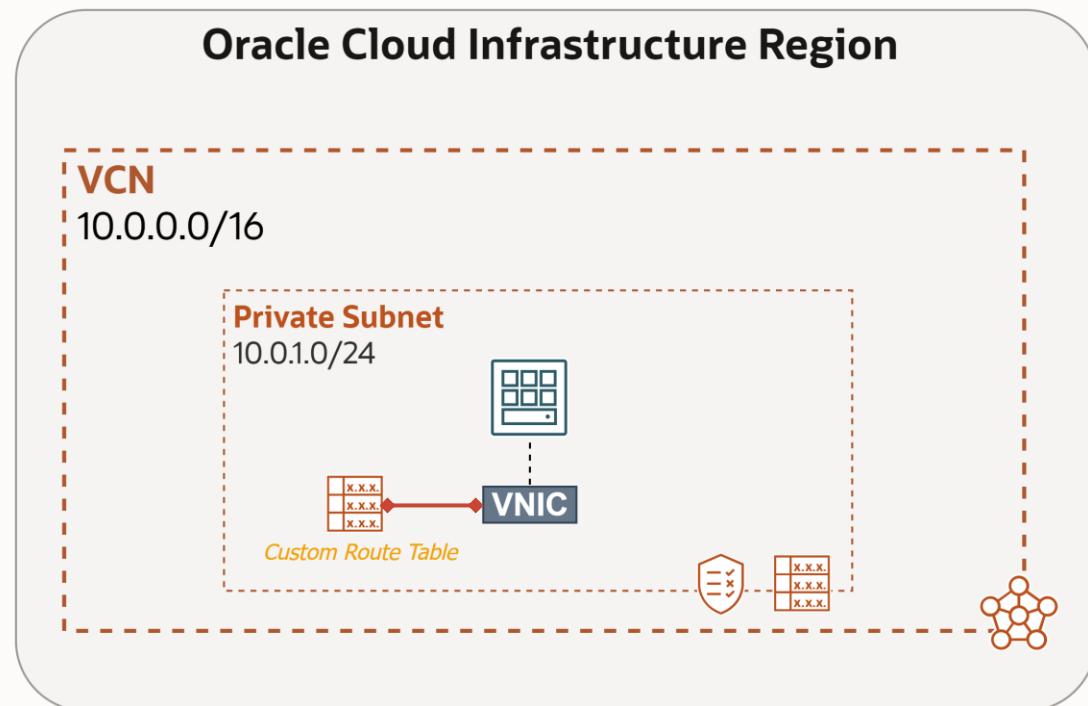
Private Subnet
10.0.1.0/24



Destination	Route Target
0.0.0.0	NAT Gateway
Object Storage	Service Gateway

- Associated with a Subnet.
- Used to send traffic out of the VCN.
- Consists of a set of route rules; each rule specifies the:
 - Destination CIDR block.
 - Route target (the next hop) for the traffic that matches the CIDR.
- No route rules are required to enable traffic within the VCN itself

Per-resource Routing



- Used to assign a custom VCN route table to one or more VNICS or to a particular IP addresses on a VNIC.
- This offers enhanced routing control tailored to each resource in a single subnet, in case they have different requirements, rather than relying solely on the subnet-level route table.
- Route Table selection process:
 1. VNIC IP address RT.
 2. VNIC RT.
 3. Subnet RT.

Internet Gateway

Oracle Cloud Infrastructure Region

VCN
10.0.0.0/16

Instance with
Public IP

Public Subnet
10.0.1.0/24

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.

Destination	Route Target
0.0.0.0/0	Internet Gateway

NAT Gateway

Oracle Cloud Infrastructure Region

VCN
10.0.0.0/16

Instance with
Private IP

Private Subnet
10.0.1.0/24



NAT
Gateway



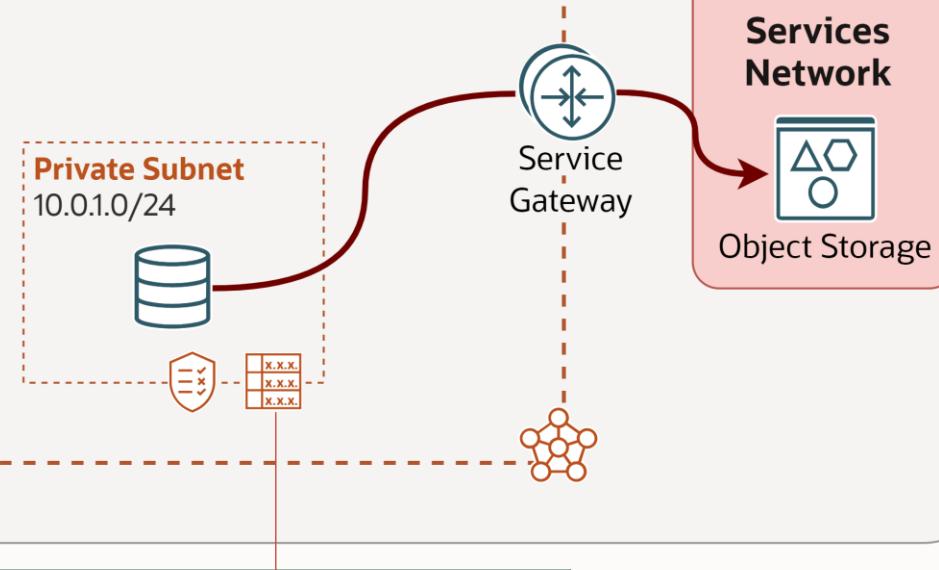
Destination	Route Target
0.0.0.0/0	NAT Gateway

- NAT Gateway gives a 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 cases: 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

Oracle Cloud Infrastructure Region

VCN
10.0.0.0/16



Destination	Route Target
Service CIDR Label	Service Gateway

- Service Gateway lets resources in VCN access public OCI services, exposed on the Oracle Services Network (OSN), such as Object Storage, but without using either 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).
- Service CIDR labels represent all the public CIDRs for a given Oracle service or a group of Oracle services. E.g.
 - OCI <region> Object Storage
 - All <region> Services

VCN Peering

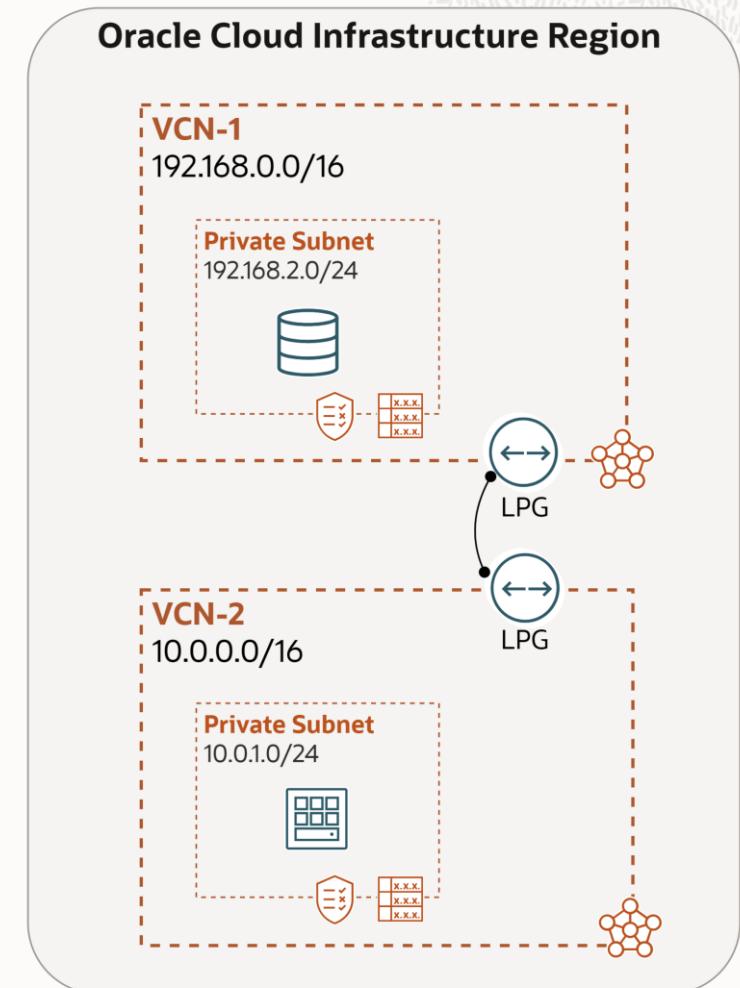
- A method to let VCNs communicate with each other.
- Does not require public IPs or NAT to enable connectivity.
- Traffic never leaves the Oracle Network.
- Over other options such as connecting over the internet, VCN Peering offers:
 - Faster connectivity.
 - Higher security.
- Types of VCN Peering available:
 - Local Peering (In-region): Enables communication between VCNs within the ***same*** OCI region.
 - Remote Peering (Cross-region): Enables communication between VCNs in ***different*** OCI regions.

Local VCN Peering – connecting VCNs in the same region

- Connecting two VCNs in the same region so that their resources can communicate using private IP addresses without routing the traffic over the internet or through your on-premises network.
- 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 the 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.

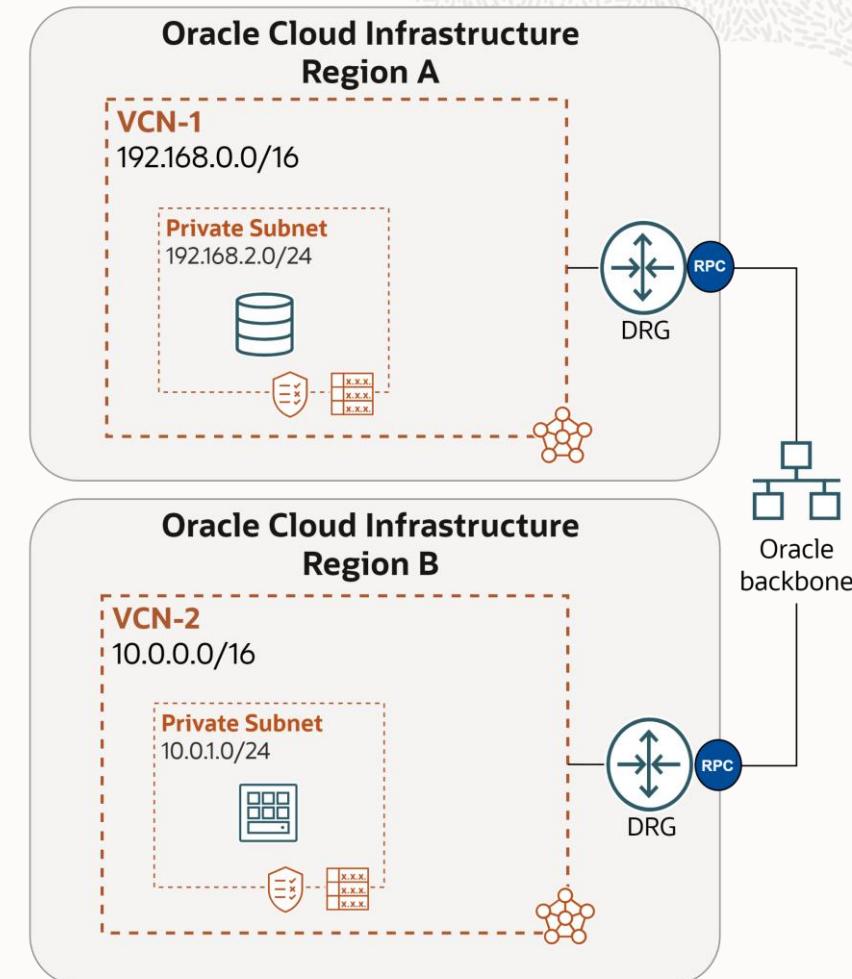


Remote VCN Peering – connecting VCNs in different regions

- 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.
- Enables features such as data replication across regions.

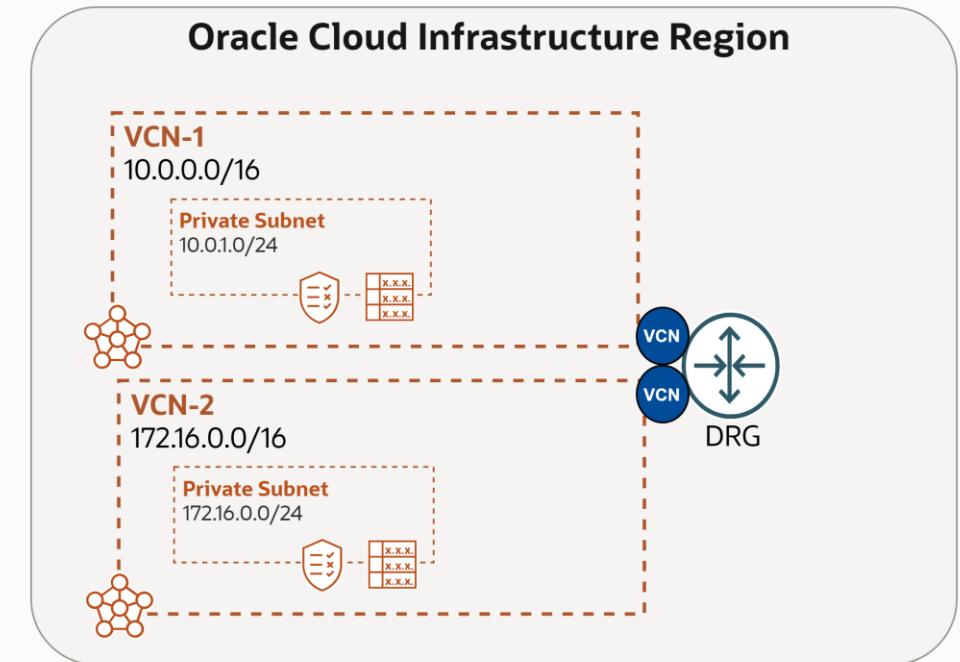
Remote Peering Connection (RPC)

- Like Virtual Circuits, the RPC is a component of DRG.
- RPCs of two DRGs from two regions are connected to create a peering relationship.



Local VCN Peering with DRG

- Oracle recommends using a Dynamic Routing Gateway (DRG) for local VCN peering instead of a Local Peering Gateway (LPG), as DRG offers greater scalability and simplifies the network design.
- Using LPG is **only** recommended in scenarios that require ultra-low latency or high bandwidth. If your use case does not have such requirements, leveraging DRG is preferred due to the flexibility it provides.



Load Balancing Agenda

1 Overview

- Definition & Benefits
- LB Types
- LB Components

2 Application Load Balancer (ALB) – Definition & Features

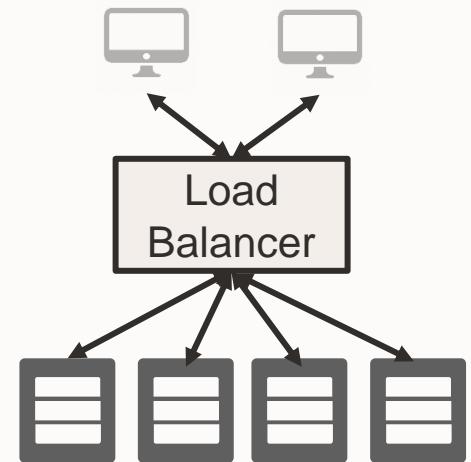
3 Network Load Balancer (NLB) – Definition & Features

Load Balancers – Definition & Benefits

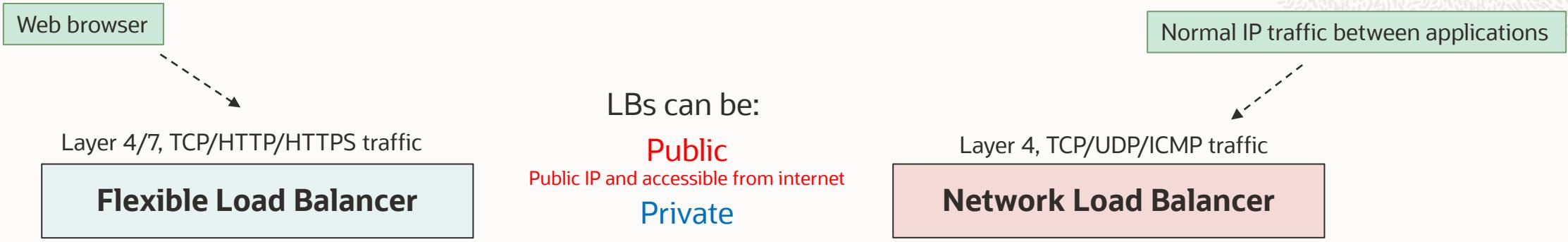
A load balancer sits between the clients and the backend servers.

Load Balancer Benefits:

- **Fault tolerance and HA:** using health check + LB algorithms, a LB can effectively route around a bad or overloaded backend.
- **Scalability:** LB maximizes throughput, minimizes response time, and avoids overload of any single resource.
- **Resource Utilization:** LB optimize resource utilization by evenly distributing traffic across healthy servers, ensuring no server is overloaded or idle, and enabling efficient scaling and task offloading.
- **Naming abstraction:** Name resolution can be delegated to the LB.



Load Balancer Types



- Standard Load balancer for public facing web servers.
- Acts as a reverse proxy.
- Can terminate SSL traffic on load balancer or pass it through to backend.
- Flexible shape will use between Min and Max bandwidth depending on traffic, lower cost if less traffic (10 Mbps – 8,000 Mbps).
- Directly apply WAF (Web application Firewall) protection onto Flexible Load Balancer.

- 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.
- Can preserve header information, like source & destination IP addresses.
- Free service.

Load Balancer Components

- **Listener** : Entity that checks for incoming traffic on the load balancer's IP address, listener should be configured for the type of traffic.

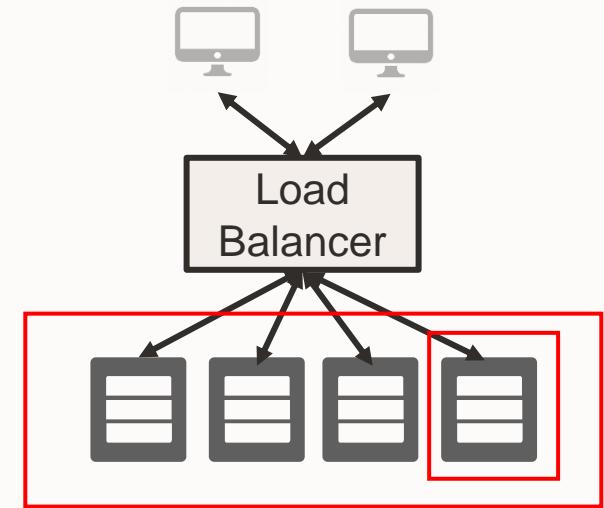
Specify the type of traffic your listener handles

HTTPS	<input checked="" type="checkbox"/>	HTTP	HTTP/2	TCP
-------	-------------------------------------	------	--------	-----

- **Load Balancing Policy**: Distribution algorithm of incoming traffic.

Weighted Round Robin	IP Hash	Least Connections
----------------------	---------	-------------------

- **Health Check**: What backends are currently healthy and available to accept requests?
- **Backend set**: A logical entity defined by a load balancing policy, a health check policy, and a list of backend servers.
- **Backend Server**: Application server responsible for generating content in reply to the incoming TCP or HTTP traffic.

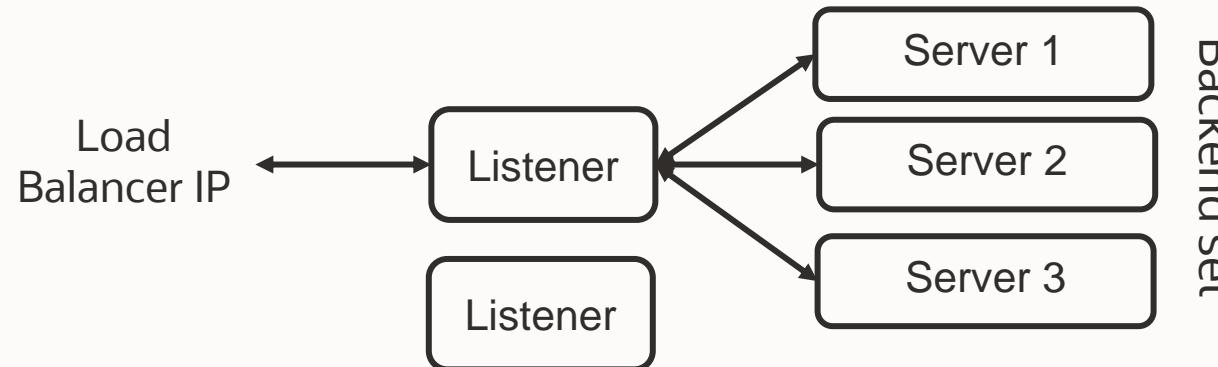


Health Check

- Health check is a test to confirm the availability of backend servers.
- Supports TCP-level, UDP-level, and HTTP-level health checks.
- Health API provides a 5-state health status (**ok, pending, incomplete, warning, critical**)
- Health status is updated **every three minutes**

Listeners

- A Load Balancer IP can have **up to 16 listeners** (port numbers). Each listener has a backend set that can have 1 to N backend servers



Backend Health Status

Level	Color	Description
Critical	Red	<p>Some or all reporting entities require immediate attention.</p> <p>The resource is not functioning or unexpected failure is imminent.</p>
Warning	Yellow	<p>Some reporting entities require attention.</p> <p>The resource is not functioning at peak efficiency or the resource is incomplete and requires further work.</p>
Incomplete	Yellow	<p>The load balancer does not have any backend sets configured or backend sets exist that contain no attached backend servers.</p>
Pending	Yellow	<p>The health status cannot be determined.</p> <p>The resource is not responding or is in transition and might resolve to another status over time.</p>
OK	Green	<p>No attention required.</p> <p>The resource is functioning as expected.</p>

Secure_LB_WAF_NGFW



ACTIVE

[Update shape](#) [Move resource](#) [Add tags](#) [Delete](#) [Create path analysis ▾](#)

[Details](#) [Tags](#)

Load balancer health

Overall health: ✓ OK

Backend sets health

Critical: ● 0
Warning: ● 0
Incomplete: ● 0
Pending: ● 0
OK: ● 2

Backend sets drain status

Drained: ● 0

Log Settings

[Learn more about load balancer logging.](#) To view logs click [here](#).

Error logs: Enabled
Access logs: Enabled
Request ID: Not enabled [Edit](#)

Load balancer information

Traffic between this load balancer and its backend servers is subject to the governing security lists and network security groups.

[Learn more about load balancers and security lists](#) ↗

OCID: ...afnacj2q [Show](#) [Copy](#)

Created: Fri, Jan 19, 2024, 11:21:40 UTC

Shape: Flexible

Min bandwidth: 10 Mbps

Max bandwidth: 20 Mbps

IP address: REDACTED.169.172 (public)

Virtual cloud network: [VCN1_Inter](#)

Subnet: [subnet2LB_pub](#)

Web application firewall: [webappfirewall20250123155026](#)

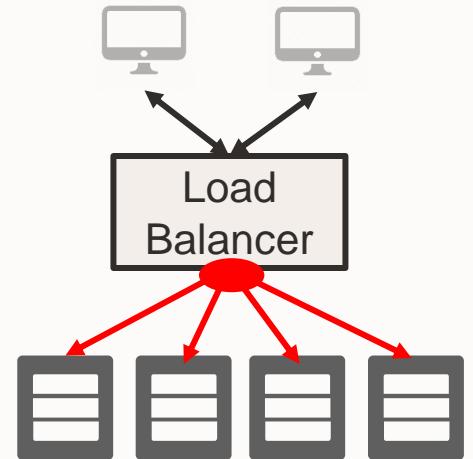
Network security groups: - [Edit](#)

Acceleration: -

Active load balancer delete protection: Not enabled [Edit](#)

Load Balancer Policies

- **Round Robin:** default policy, distributes incoming traffic sequentially to each server in a backend set. After each server has received a connection, the load balancer repeats the list in the same order.
- **IP Hash:** uses an incoming request's source IP address as a hashing key to route non-sticky traffic to the same backend server.
- **Least Connection:** routes incoming non-sticky request traffic to the backend server with the fewest active connections.
- Load balancer policy decisions apply differently to TCP load balancer, cookie-based session persistent HTTP requests (sticky requests), and non-sticky HTTP requests
 - A TCP load balancer considers policy and weight criteria.
 - An HTTP load balancer w/ cookie-based session persistence forwards requests using cookie's session info.
 - For non-sticky HTTP requests, the load balancer applies policy and weight criteria.



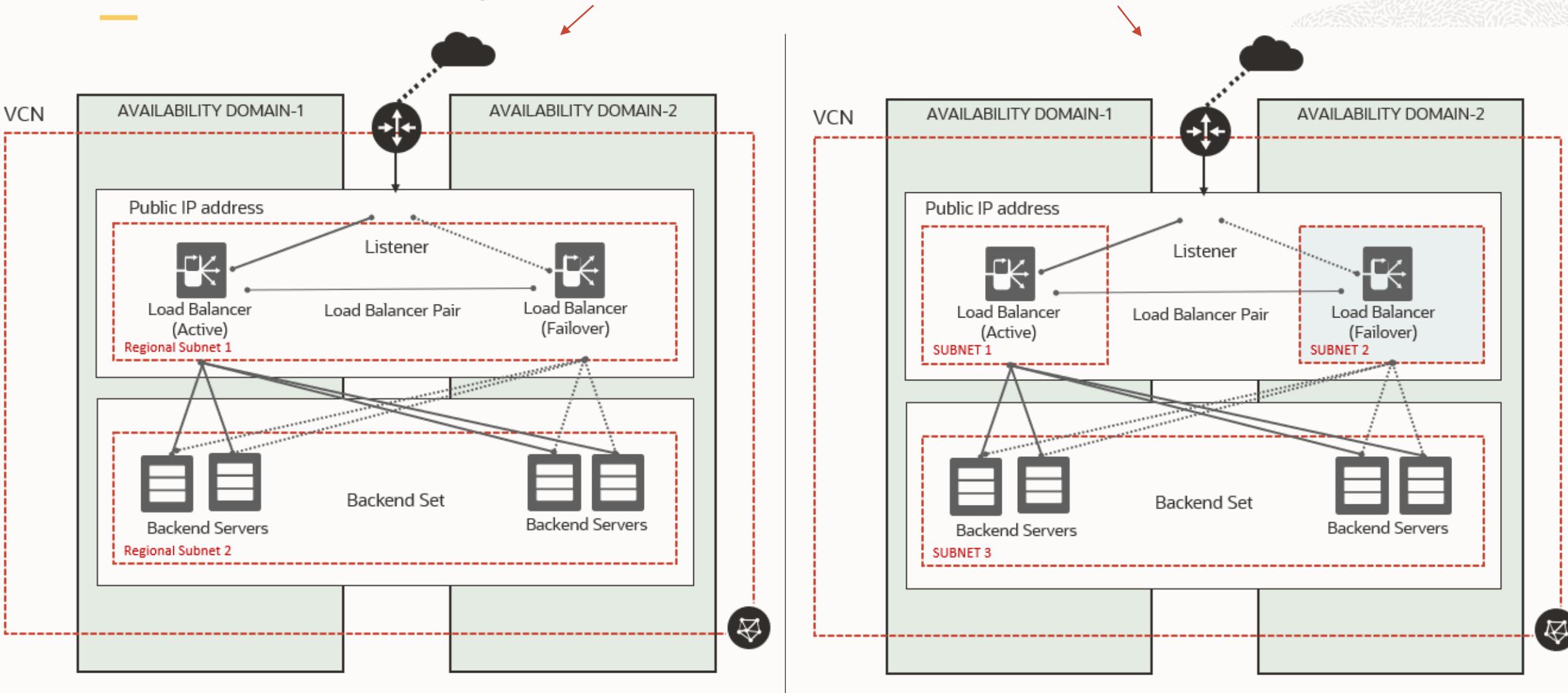
Flexible Load Balancer Bandwidth

Customer just defines the **minimum** and **maximum** bandwidth:

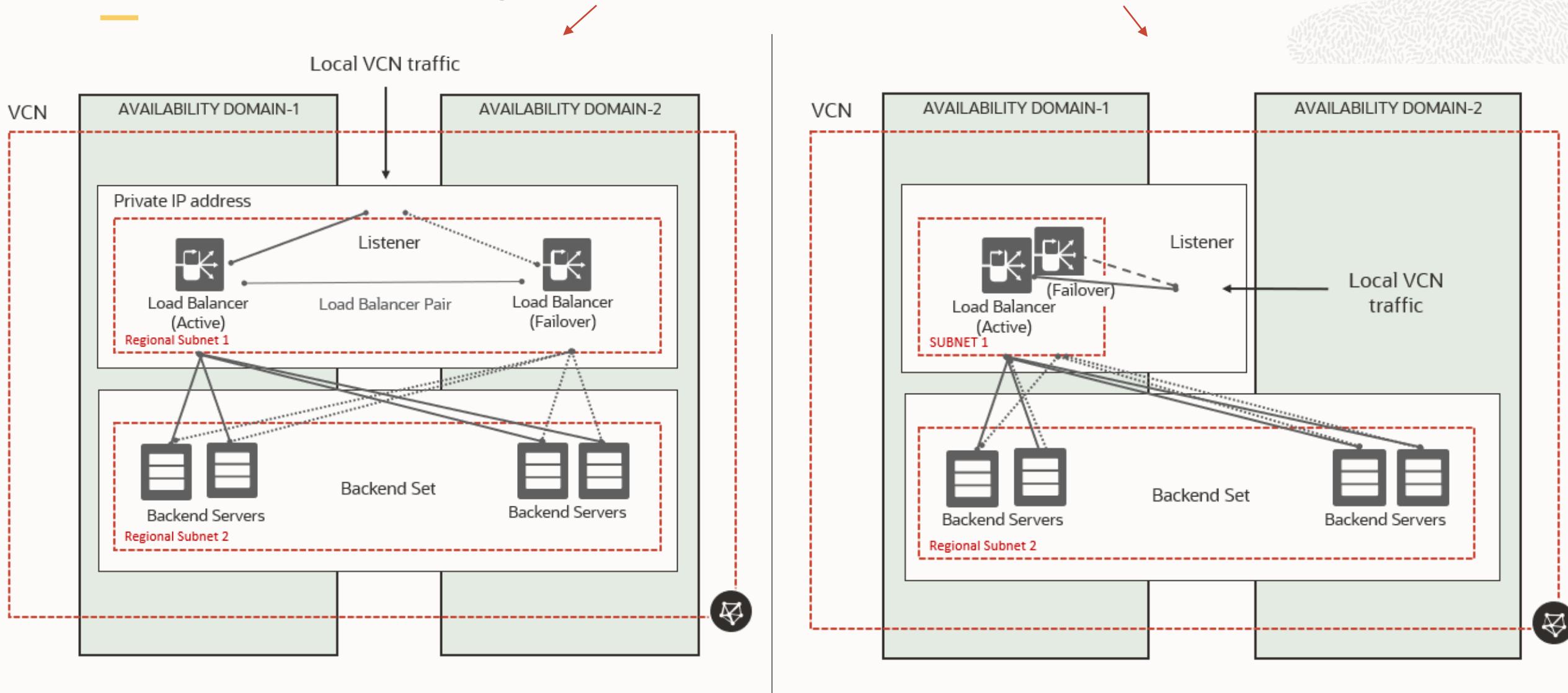
- Minimum bandwidth provides instant readiness for the load balancer.
- Maximum bandwidth allows control of maximum cost.
- Customer pays a minimal base cost for the load balancer and then pays a simple single rate.
- For the larger of the reserved bandwidth or the maximum bandwidth actually used each minute.
- The minimum customer can choose is 10 Mbps and the maximum is 8,000 Mbps.

The screenshot shows the Oracle Cloud Infrastructure (OCI) Create Load Balancer wizard. At the top, there's a navigation bar with icons for Cloud, a search bar, and location information (Saudi Arabia West (Jeddah)). Below the navigation bar, the title "Create load balancer" is displayed, along with a "Help" link. The main form has two sections: "Assign a public IP address" and "Bandwidth". The "Bandwidth" section is highlighted with a red border. It contains fields for "Choose a minimum bandwidth" (set to 10) and "Choose a maximum bandwidth" (set to 100). A note at the bottom states: "The maximum service limit is currently 4970 Mbps. For more bandwidth, request a service limit increase from the service limits page in the Console."

Public Load Balancer (Regional Subnets -Recommended- vs. AD Specific Subnets)



Private Load Balancer (Regional Subnets -Recommended- vs. AD Specific Subnets)



Request Routing

- Each HTTP request is evaluated against the rules.
- The rules are run in the order that is defined in the policy.
- Each rule has at least one condition and a backend set.
- If the HTTP request condition matches a rule, the request is forwarded to the backend set defined for the rule. The other rules in the policy are skipped and the request is not evaluated against them.

Create routing policy

Rule 1

Advanced controls Show

Name: rule_1

Condition type: Path (selected)

Conditions: When the following conditions are met...

Matching: If all match

Condition type: Path, Operator: Is, URL string: /w3/app

Action: Then perform the following action: Route to backend

Backend set: bs_lb_2025-0531-1552

Select a backend set where the traffic will be routed for the conditions

+ Another rule

Rule Sets

A rule set is a named set of rules associated with a load balancer and applied to one or more listeners on that load balancer.

- [Access control rules](#): Restrict access to application resources based on the source of the request.
- [Access method rules](#): Specify the permitted HTTP methods (GET, DELETE, ...etc.).
- [URL redirect rules](#): Route incoming HTTP requests to a different destination URL.
- [Request and response header rules](#): Which add, alter, or remove HTTP request or response headers.
- [HTTP header rules](#): Which specify the size of the HTTP header, enlarge header and whether period and underscore characters are permitted within the headers.
- [Max listener connection rules](#): Apply both a uniform maximum number of listener connections for all IP addresses, and also specify overrides to that uniform value for individual IP addresses you identify.

Resources Rule sets

Name	Number of rules
No items found.	

Metrics Smart check Logs (0) Backend sets (1) Routing policies (0) Rule sets (0) Listeners (1)

Create rule set

Cloud Search resources, services, documentation, and Marketplace

Create rule set

Name: HTTP_TO_HTTPS_REDIRECTION

Specify access control rules:

Specify access method rules:

Specify URL redirect rules:

Specify request header rules:

Specify response header rules:

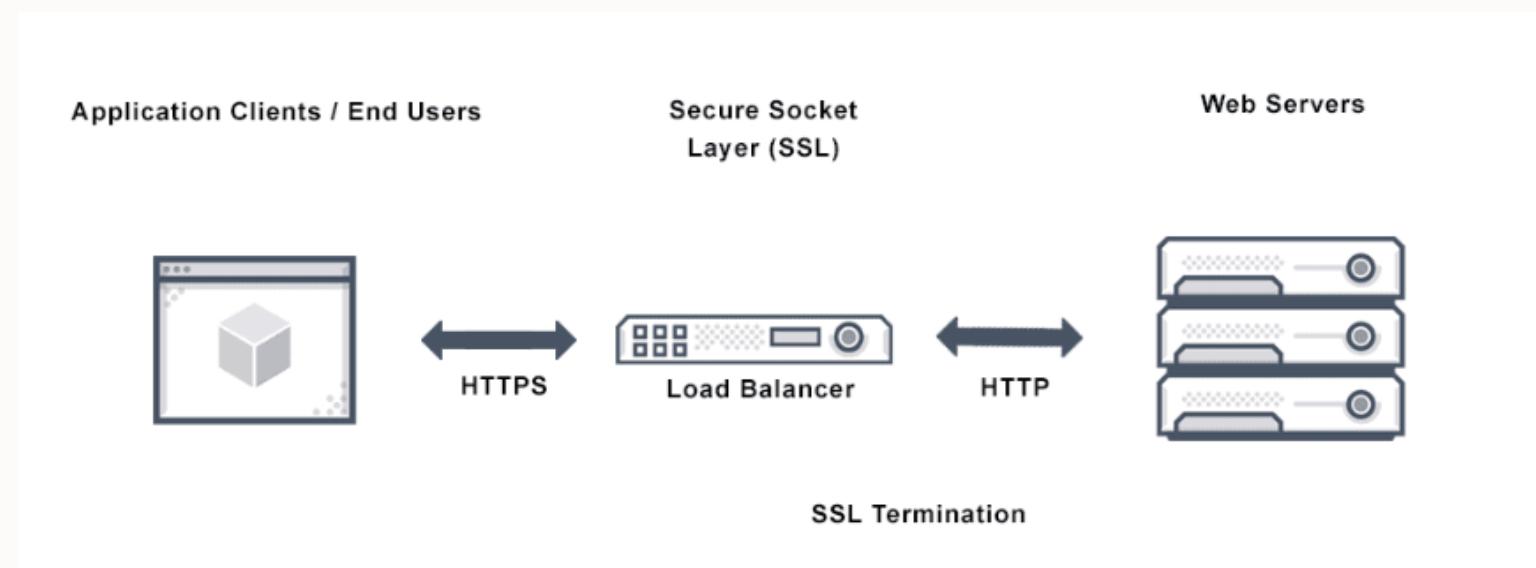
Specify HTTP header rules:

Specify max listener connection rules:

Submit Cancel

SSL Handling

- **Terminate SSL at the load balancer.** This configuration is *frontend SSL*. Your load balancer can accept encrypted traffic from a client. No encryption of traffic exists between the load balancer and the backend servers.
- **Implement SSL between the load balancer and your backend servers.** This configuration is *backend SSL*. Your load balancer does not accept encrypted traffic from client servers. Traffic between the load balancer and the backend servers is encrypted.
- **Implement point-to-point SSL.** Your load balancer can accept SSL encrypted traffic from clients and encrypts traffic to the backend servers.
 - To use SSL with your load balancer, you must add one or more certificate bundles to your system.
 - Oracle Cloud Infrastructure accepts x.509 type certificates in PEM format only.



Virtual Hostnames for Load Balancers

Cloud

Search resources, services, documentation, and Marketplace

✓ UAE Central (Abu Dhabi)



Create hostname

Name _____

first-application

Hostname

www.app1.com

Resources

Listeners

A large, solid red arrow pointing downwards, indicating the direction of flow or operation.

Metrics

Smart check

Logs (0)

Part A (a) (1)

Particulars (2)

Bullets (0)

Listeners (1)

Create listener									<input type="text"/> Search...	
Name	Protocol	Port	Cipher suite	Backend set	Routing policy	Path route set	Hostnames	Use SSL		
listener1	HTTP	80	—	be-set-1	—	—	first-application	No		
										Showing 1 item < 1 of 1 >

Session Persistence

Session persistence is a method to direct all requests originating from a single logical client to a single backend web server. Backend servers that use caching to improve performance, or to enable log-in sessions or shopping carts, can benefit from session persistence.

Application cookie stickiness

- The Load Balancer service activates application cookie session persistence (stickiness) when a backend server sends a *Set-Cookie* response header containing a recognized cookie name.
- The cookie name must match the name specified in the backend set configuration.

Load balancer cookie stickiness

- The load balancer inserts a cookie into the response. The parameters configured within the cookie enable session stickiness.
- This method is useful when you have applications and web backend services that can't generate their own cookies.

Logging

Load Balancers | Oracle Cloud Inf + Add

[Load-balancer-logs](#)

ORACLE Cloud Search for resources, services, and documentation Germany Central (Frankfurt) ...

Backend Sets Health

0	Critical
0	Warning
0	Incomplete
0	Pending
1	OK

Shape: Flexible
Min Bandwidth: 10 Mbps
Max Bandwidth: 100 Mbps
IP Address: 129.130.130.130 (Public)
Virtual Cloud Network: [w3](#)
Subnet: [lb_sub](#)
Network Security Groups: *None* [Edit](#)
Type: Load Balancer

Traffic between this load balancer and its backend servers is subject to the governing security lists and network security groups.

[Learn more about load balancers and security lists.](#)

Resources

[Metrics](#)
[Logs](#)
[Backend Sets \(1\)](#)
[Routing Policies \(1\)](#)
[Rule Sets \(0\)](#)
[Listeners \(1\)](#)

Logs

Category	Status	Log Name	Log Group	Enable Log	...
Access Logs	● Active	lb_w3_access	Default_Group	<input checked="" type="checkbox"/> Enabled	⋮
Error Logs	● Active	lb_w3_error	Default_Group	<input checked="" type="checkbox"/> Enabled	⋮

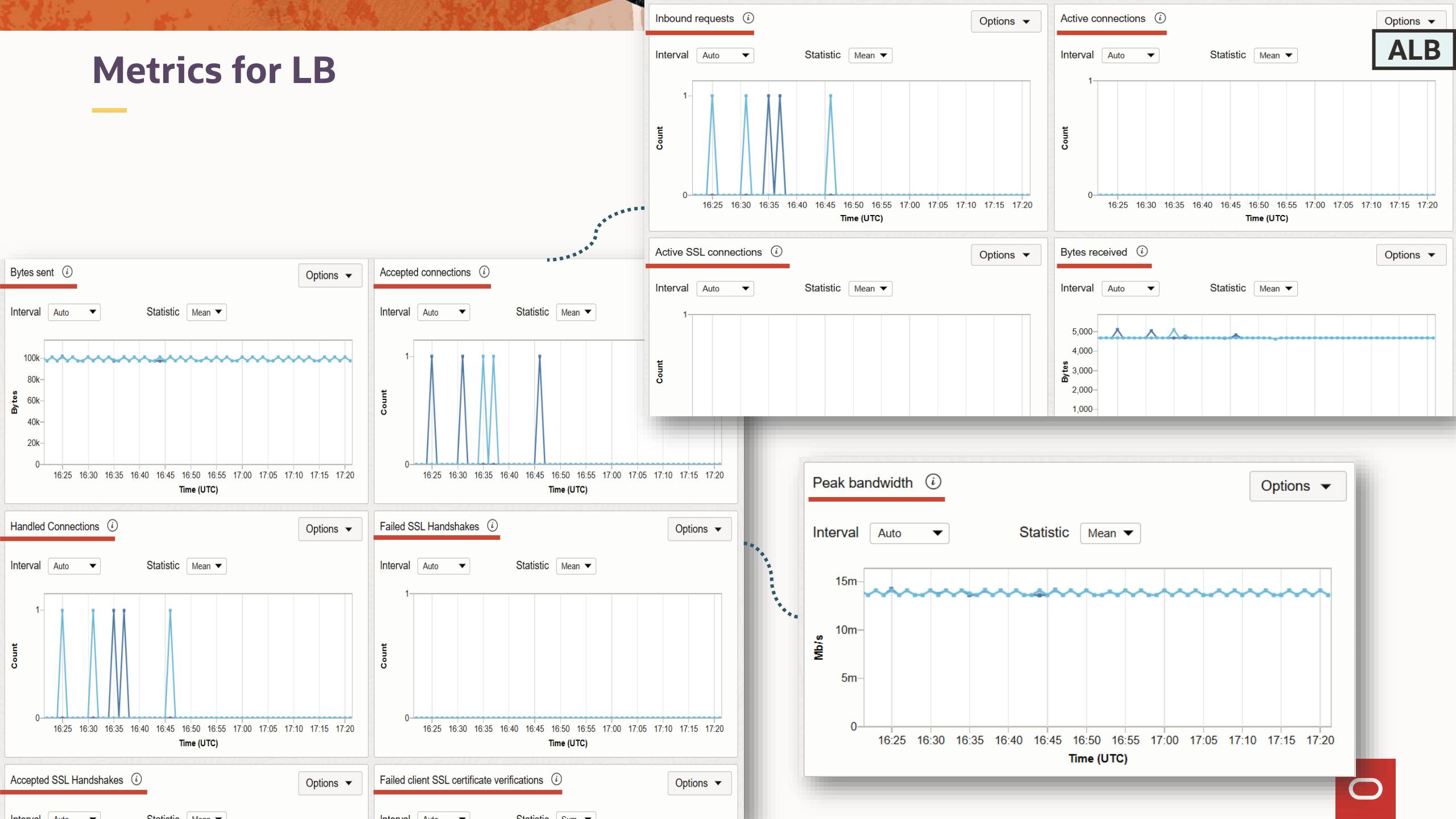
Showing 2 Items



Options

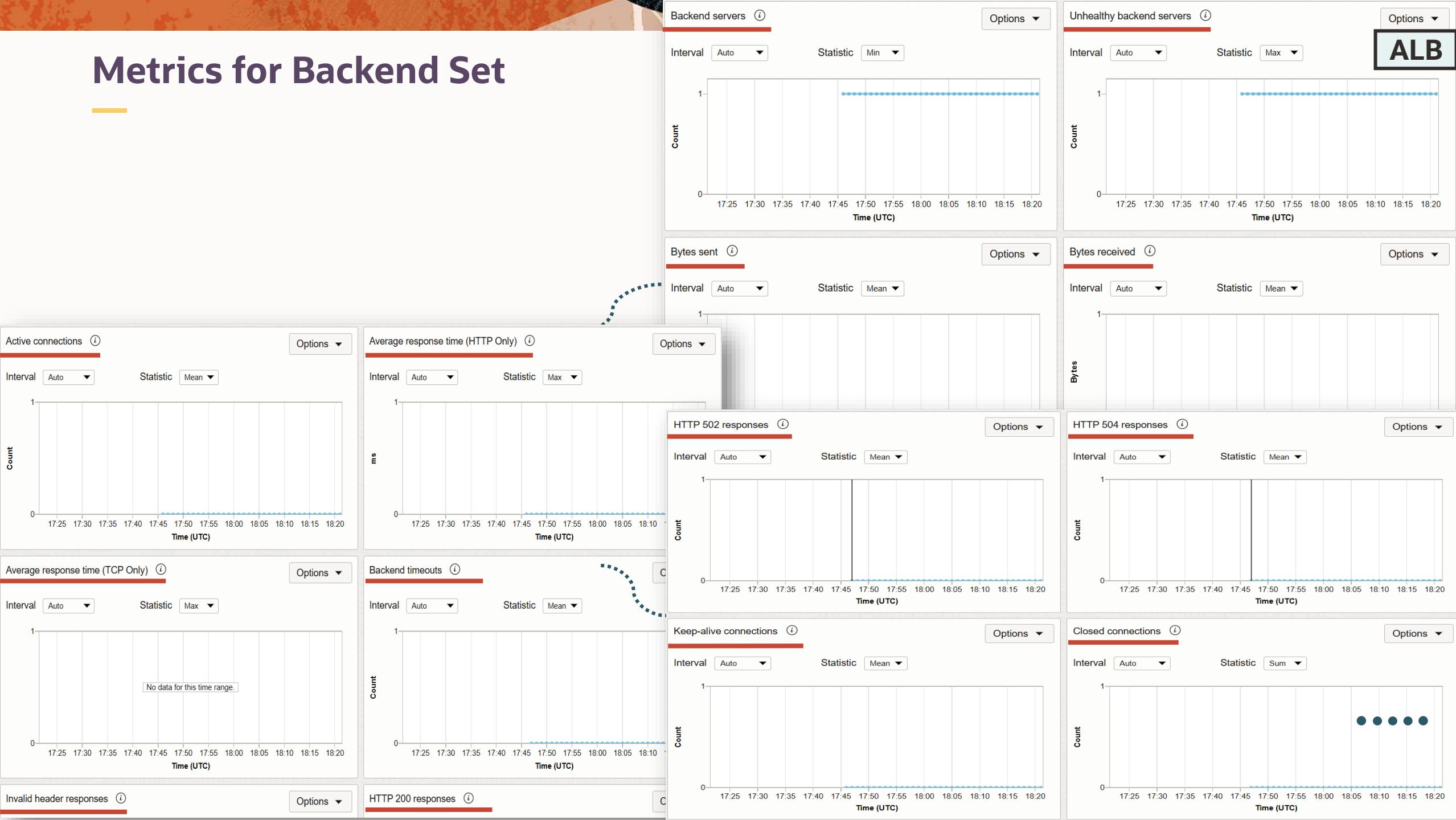
ALB

Metrics for LB



Metrics for Backend Set

ALB



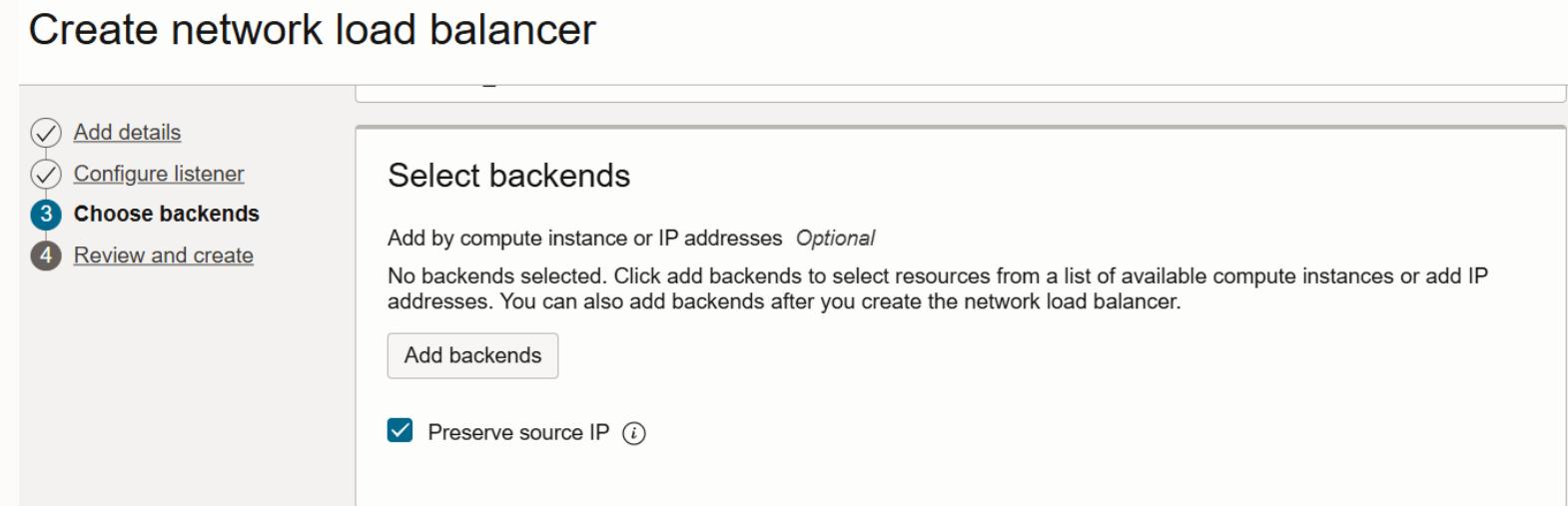
Network Load Balancer (Layer 4)

- The Network Load Balancer load balance **layer 3 and layer 4 (TCP/UDP/ICMP) workloads**
- It's designed to handle volatile traffic patterns and millions of flows, offering high throughput while maintaining **ultra-low latency**.
- Ideal load balancing solution for **latency-sensitive workloads** includes real-time streaming, VoIP, Internet of Things, HA scenarios and trading platforms.
- OCI Network Load Balancer can be public or private.
- **Symmetric Hashing** support for Active/Active configurations.
- Full NAT, Source/Destination Header (IP/Port) Preservation (Bump-in-the-wire), Source Header (IP/Port) Preservation.

NLB Backend Set Source Preservation

If you enable this option, the network load balancer preserves the source IP of the packet when it is forwarded to backend servers that are members of the configured backend set. Backend servers see the original source IP.

If source/destination preservation is enabled for the network load balancer (next slide). then this parameter cannot be disabled. The value is true by default. No network address translation (NAT) occurs on the source IP and port.



NLB Source/Destination Preservation

You can configure the network load balancer so that the original source and destination IP addresses and ports contained in the header of each incoming packet are preserved all the way to the backend server.

The network load balancer doesn't change packet characteristics. The source and destination IP header information is identical when viewed at the network load balancer or a backend server. No network address translation (NAT) occurs.

Create network load balancer

The screenshot shows the 'Create network load balancer' wizard in progress, specifically the 'Header preservation' step. The process is at step 1, 'Add details'. Under 'Choose visibility type', the 'Private' option is selected and highlighted with a red box. In the 'Header preservation' section, there are two checkboxes: one for 'Source/destination header (IP, port) preservation (network load balancer)' which is unchecked, and another for 'Source/destination header (IP, port) preservation (network load balancer)' which is checked and has a green arrow pointing to it. In the 'Symmetric hashing' section, there is an unchecked checkbox for 'Enable symmetric hashing'.

Choose visibility type

Public
You can use the assigned public IP address as a front end for incoming traffic.

Private
You can use the assigned private IP address as a front end for internal incoming VCN traffic.

Header preservation

Source/destination header (IP, port) preservation affects all backend sets in the network load balancer. Update your route table to use this feature.

Source/destination header (IP, port) preservation (network load balancer)
Preserve source/destination header (IP, port)

Source/destination header (IP, port) preservation (network load balancer)
Preserve source/destination header (IP, port)

Symmetric hashing

Network load balancer uses symmetric hashing to calculate the same hash for packets belonging to the same flow in both forward and return directions. The hash does not change when the source IP address:port value is exchanged with the destination IP address: port value. Enable symmetric hashing when you want to inspect both forward and return traffic with the same firewall appliance that is hosted as a backend on the network load balancer.

Enable symmetric hashing
Allows for NAT to be turned off for third party firewalls. If reverse traffic from backends is routed to the network load balancer using explicit route rules, ensure you add separate rules for both directions. Learn more about [route tables](#).

Network Load Balancer - Policies

5-Tuple Hash: Routes incoming traffic based on 5-Tuple (source IP and port, destination IP and port, protocol) Hash. This is the default network load balancer policy.

3-Tuple Hash: Routs incoming traffic based on 3-Tuple (source IP, destination IP, protocol) Hash.

2-Tuple Hash: Routs incoming traffic based on 2-Tuple (source IP Destination, destination IP) Hash.

ALB vs. NLB - Summary

OCI **Load Balancing service (ALB)** provides automated traffic distribution from one entry point to multiple servers reachable from your virtual cloud network (VCN) to load balance transport Layer 4 and Layer 7 (TCP and HTTP) traffic.

OCI Flexible **Network Load Balancing service (NLB)** provides automated traffic distribution from one entry point to multiple backend servers in your virtual cloud network (VCN). It operates at the connection level and load balances incoming client connections to healthy backend servers based on Layer 3/Layer 4 (IP protocol) data.

Web Application Firewall (WAF) Agenda

- 1 Overview
- 2 Access Controls
- 3 Protection Rules
- 4 Rate Limiting
- 5 Bot Management
- 6 Shared Responsibility Model

Increasing cyber attacks

<50%

of companies globally are sufficiently prepared for a cybersecurity attack, according to a report that surveyed 3,000 business leaders from 80 countries

Source: Eurasia Group, 2019

92%

of IT professionals surveyed feel that immaturity in their cloud security programs is creating a readiness gap

Source: Oracle and KPMG Cloud Threat Report, 2020



Exploit data

Steal personal data, usernames and passwords to get to more important data



Hold data ransom

Steal records, personal data, usernames and passwords and charge the organization to give it back



Steal infrastructure

Take control of an organization's compute, storage and network resources so not to pay for them



Deny service

Prevent web services from working to impact organization's reputation or bottom line

OCI Web Application Firewall (WAF)

OCI WAF protects against threats such as OWASP defined top-10 vulnerabilities. It can be used to limit access to the application based on geography or the signature of incoming requests, block unwanted bots.

OCI WAF protects your application infrastructure and workloads no matter where they reside: in OCI, on-premises, multi-cloud and anywhere in between.

Create WAF Policy

1 Basic Information
2 Access Control
3 Rate Limiting
4 Protections
5 Select Enforcement Point
6 Review and Create

Select Enforcement Point Optional
Use this to enforce web application firewall security on your load balancer.

ⓘ You can generate security logs for your firewalls after you create your WAF policy. Enabling security logs is highly recommended as it provides valuable insight into your WAF performance. See [Firewall Management](#) for more information.

Add Firewalls
Select ir-region application delivery resources to secure.
Load Balancer in [gopigopa \(root\)](#) ([Change Compartment](#))
mushooflexib
Ensure your load balancer can communicate with your origin.

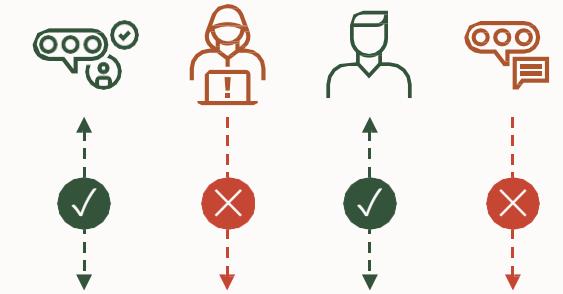
+ Additional Firewall

Previous Next Cancel

Customer benefits

- Layered defense and flexibility to enforce security at the edge closest to users as well as in-region closest to the application on flexible load balancers.
- WAF policies can be enforced on internet facing web applications, and/or (public/private) flexible load balancer instances.
- Protects internet facing and internal applications against both external and insider threats.
- Supports access rules, protection rules, rate limiting, and bot management*

OCI WAF Features



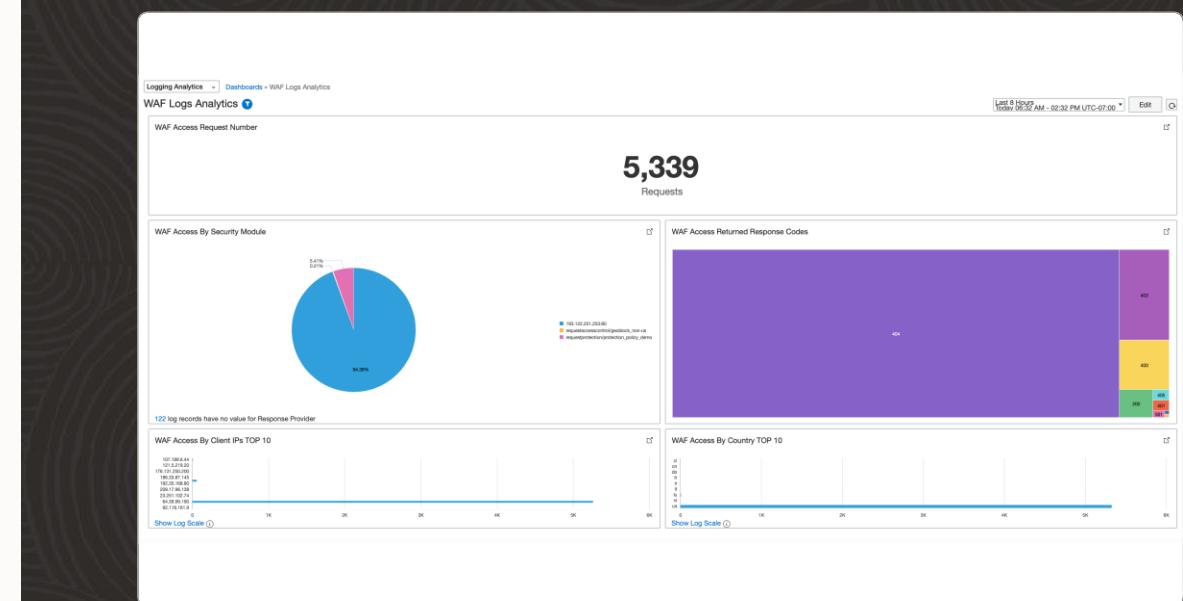
-  Access control
 - > Restrict or control access to critical web applications, data and service
-  Bot management
 - > Identifies whether requests are from a human or a machine. Controls or blocks non-human suspicious requests
-  Protection rules
 - > Hides the origin server
 - > Inspects traffic as it tries to access the server or as it leaves the server
-  Rate limit
 - > Provides protection against L7 DDOS
-  Customer applications

•———— Oracle Cloud Infrastructure ———•

Access controls

Use the access controls to restrict or control access to your critical web applications, data and services. Examples:

- Control access, based on HTTP header information. Block requests if the HTTP header contains specific names or values or allow traffic with proper HTTP regular expression.
- Control access based on URL address matching or partial matching or match proper URL regular expressions.
- Regional access control can be used to restrict users from certain geographies.



Protection rules

Use these rules to protect your critical web applications against malicious cyber-attacks from bad actors. Incoming requests are inspected to determine if it contains an attack payload as compared to industry-leading threat feeds.

- Supports over 250 rule sets as well as the Open Web Access Security Project (OWASP) rule sets.
- WAF will block and/or alert on the requests: SQL injection, cross-site scripting, HTML injection and many more.

Choose Protection Capabilities

Oracle provides protection capabilities that catch a variety of malicious traffic types, such as XSS attacks and SQL injection. These capabilities run when the specified request and response conditions are met.

Protection Capabilities

ⓘ Enable all capabilities tagged as **Recommended** for best practices.

Filter by Tags: OWASP, Recommended

Filter by Version: Latest

[Reset All Filters](#)

<input type="checkbox"/>	Key	Name	Description	Collaborative	Tags
<input type="checkbox"/>	944300	Java attack Attempt:Interesting keywords for possibly RCE on vulnerable classes and methods base64 encoded	Java attack Attempt: Interesting keywords for possibly RCE on vulnerable classes and methods base64 encoded	No	OWASP, OWASP-2017, CRS3, WASCTC, PCI, HTTP, A1, A1-2017, Java
<input type="checkbox"/>	944250	Java attack Attempt:SAP CRM Java vulnerability CVE-2018-2380	Java attack Attempt: SAP CRM Java vulnerability CVE-2018-2380	No	OWASP, OWASP-2017, CRS3, WASCTC, PCI, HTTP, A1, A1-2017, Java
<input type="checkbox"/>	944240	Java attack Attempt:Remote Command Execution: Java serialization	Java attack Attempt: Remote Command Execution: Java serialization	No	OWASP, OWASP-2017, CRS3, WASCTC, PCI, HTTP, A1, A1-2017, Java

Rate limit rules

Rate limiting rules based on URL request parameters and client IP to protect against layer 7 DDOS attacks.

- Allows inspection of HTTP request properties and limits the frequency of requests for each unique client IP address.

Add Rate Limiting Rule

Name

Conditions (Optional) [Show Advanced Controls](#)

When the following Conditions are met...

Condition Type	Operator	Value
Path	Is	<input type="text"/> X
Request Cookies		
Request Headers		
URL Query		
Country/Region		
Source IP Address		
Host		
Request Method		

+ Another Condition

Rate Limiting Configuration

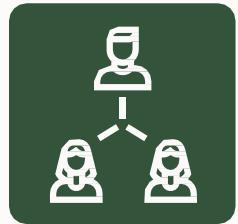
Requests Limit Period In Seconds Action Duration in Seconds Optional [X](#)

+ Another Rate Limiting [X](#)

[Add Rate Limiting Rule](#) [Cancel](#)

Bot management

Entity attributes and behavioral detection



Human interaction

Oracle WAF identifies normal usage patterns based on legitimate user behavior to the site.

The WAF will challenge with CAPTCHA or block requests when it detects abnormalities, or traffic exceeds defined interaction thresholds.



Device fingerprinting

Oracle WAF collects unique various characteristics about a device entity, generating a hashed signature. This hashed signature is then compared to other requests to determine the same signature is being leveraged across different contexts.

Shared responsibility model for OCI WAF



Responsibility	Oracle	Customer
Onboard/configure the WAF policy for the web application	No	Yes
Configure WAF onboarding dependencies (DNS, ingress rules, network)	No	Yes
Provide high availability (HA) for the WAF	Yes	No
Monitor for distributed denial of service (DDoS) attacks	Yes	No
Keep WAF infrastructure patched and up-to-date	Yes	No
Monitor data-plane logs for abnormal, undesired behavior	Yes	Yes
Construct new rules based on new vulnerabilities and mitigations	Yes	No
Review and accept new recommended rules	No	Yes
Tune the WAF's access rules and bot management strategies for your traffic	No	Yes

What's New in OCI WAF



- Include `\${http.request.id}` in custom responses for faster troubleshooting and correlation (Release Notes).
- Additional in-region protection rule sets and threat-intel feeds; easier tuning.
- HTTP Request Body Inspection—buffers and scans request bodies.

*All features supported on both Edge and Flexible Load Balancers.

Simplified Pricing – 2025



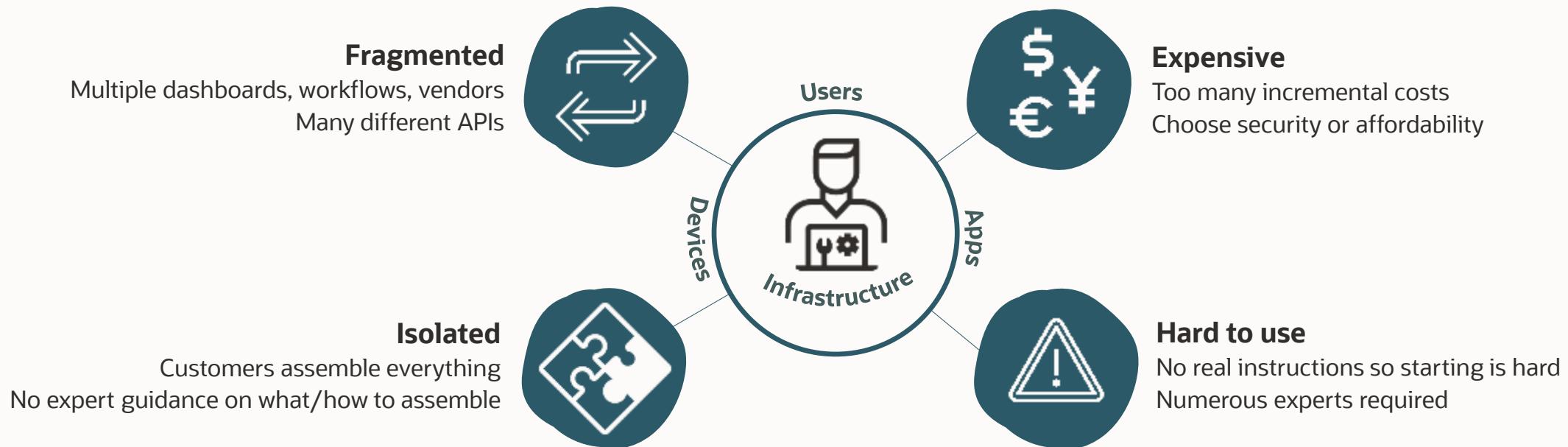
- First WAF instance + first 10 million requests/month are FREE for OCI commercial customers.
- After free tier: charged per WAF instance/month and per 1 million incoming requests.
- Pricing identical for Edge and In-region WAF; pay-as-you-go or commit models.

Network Firewall Agenda

- 1 Oracle's security principles
- 2 NFW Features & Benefits
- 3 OCI Network Firewall Versus Third-Party Firewall
- 4 Logging and Observability
- 5 NFW Deployment Topologies
- 6 Pricing

Fundamental challenges with cloud security today

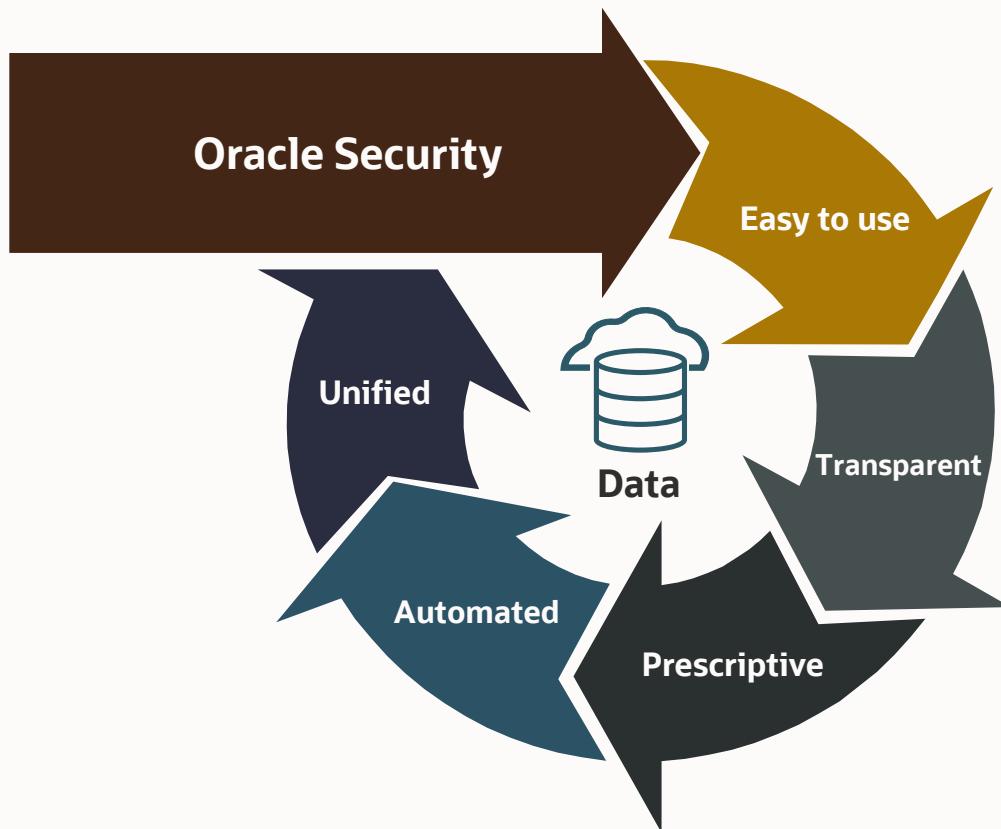
Organizations don't get breached because they don't have the tools.
They get breached because the tools are too complex.



Oracle believes there is a better way

Oracle's security principles

Core principles for enterprise cloud security



Simple:

'Always on' security posture.
Easy defaults for developing
and running apps

Prescriptive:

Policies to enforce security
posture, automated baseline
management

Integrated:

Unified Security and Identity
across IaaS, PaaS, and SaaS

No Compromise:

Included security eliminates the
cost/security tradeoff

Network Firewall Overview



**Next-Gen Network Firewall with
Advanced Threat Protection**

OCI Network Firewall is a cloud-native managed firewall service that is built using industry leading **Palo Alto Networks** next-generation firewall technology. It provides advanced threat protection capabilities including custom URL filtering, intrusion prevention and detection (IDS/IPS), and TLS inspection to help prevent malicious traffic and malware propagation.

Network Firewall Benefits



Next-Gen Network Firewall with Advanced Threat Protection

- **Cloud-native Solution** - Scalable cloud-native service, fully integrated with rich set of OCI platform capabilities, eliminating the need to manage additional third-party security infrastructure.
- **Advanced Threat Protection** – Industry leading threat protection to help monitor and block malware, spyware and vulnerability exploits.
- **Layered Defense** - Seamlessly integrates with Access Control Lists (ACLs), Network Security Groups (NSGs), and Web Application Firewalls (WAFs) to establish a Defense in Depth security strategy
- **Compliance** – Helps meet compliance requirements and stringent security needs of regulated environments.
- **Deep Integration with OCI** – Natively integrated with OCI platform including logging and metrics services.
- **Segment and Filter network traffic.**

OCI Network Firewall Versus Third-Party Firewall



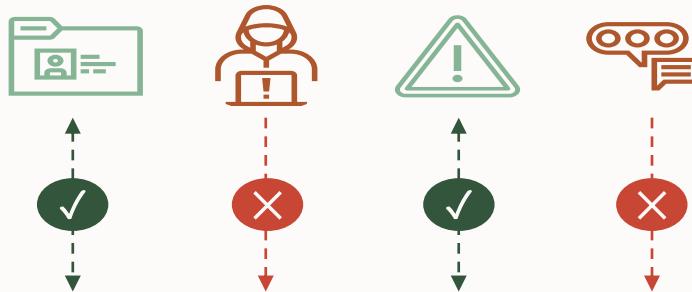
OCI Network Firewall

- Oracle-managed FWaaS
 - Simple deployment
 - Built in HA
 - Patch management and maintenance
 - Customer still responsible for policy
- Direct integration with OCI (Logging, Vaults, and so on)
- No requirement for specialized third-party skills and expertise

Third-Party Firewall

- Flexible deployment options:
 - BYOL
 - Choose your vendor
- Familiar interface and feature set for existing customers of a third-party vendor
- Support for more advanced features
- Integrate with existing tools

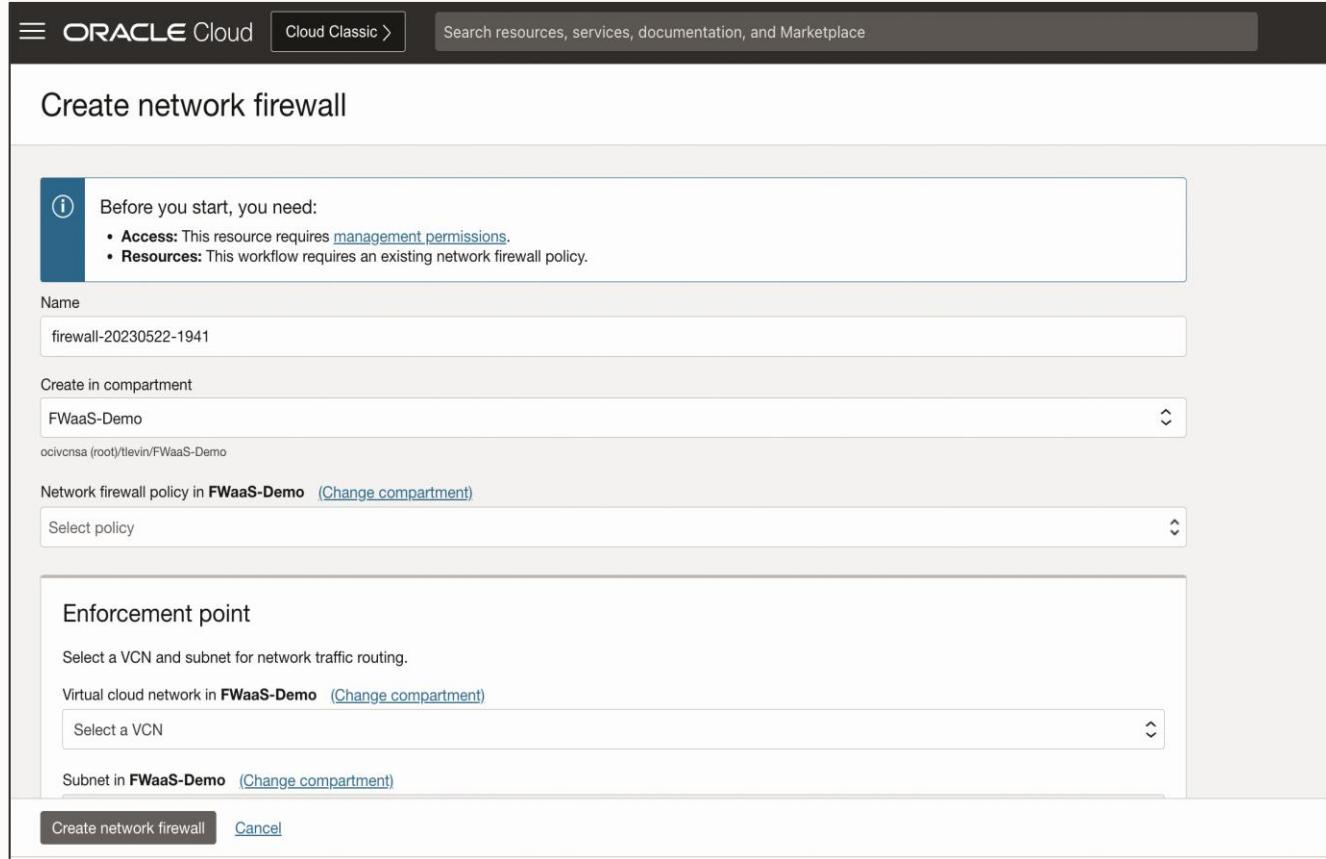
OCI Network Firewall features



- > Stateful filtering Allow or Deny rules based on 5-tuple information for both IPv4 and IPv6 traffic.
- > Industry-leading signature-based threat detection and prevention (IDS/IPS) engine to automatically stop known malware, spyware, C2 and vulnerability exploits.
- > Control inbound and outbound HTTP/S traffic to a specified list of FQDN including wild cards and custom URLs.
- > Secure inbound, outboud and lateral network/application traffic.
Can be enforced on OCI gateways as well as intra-vcn subnet traffic.

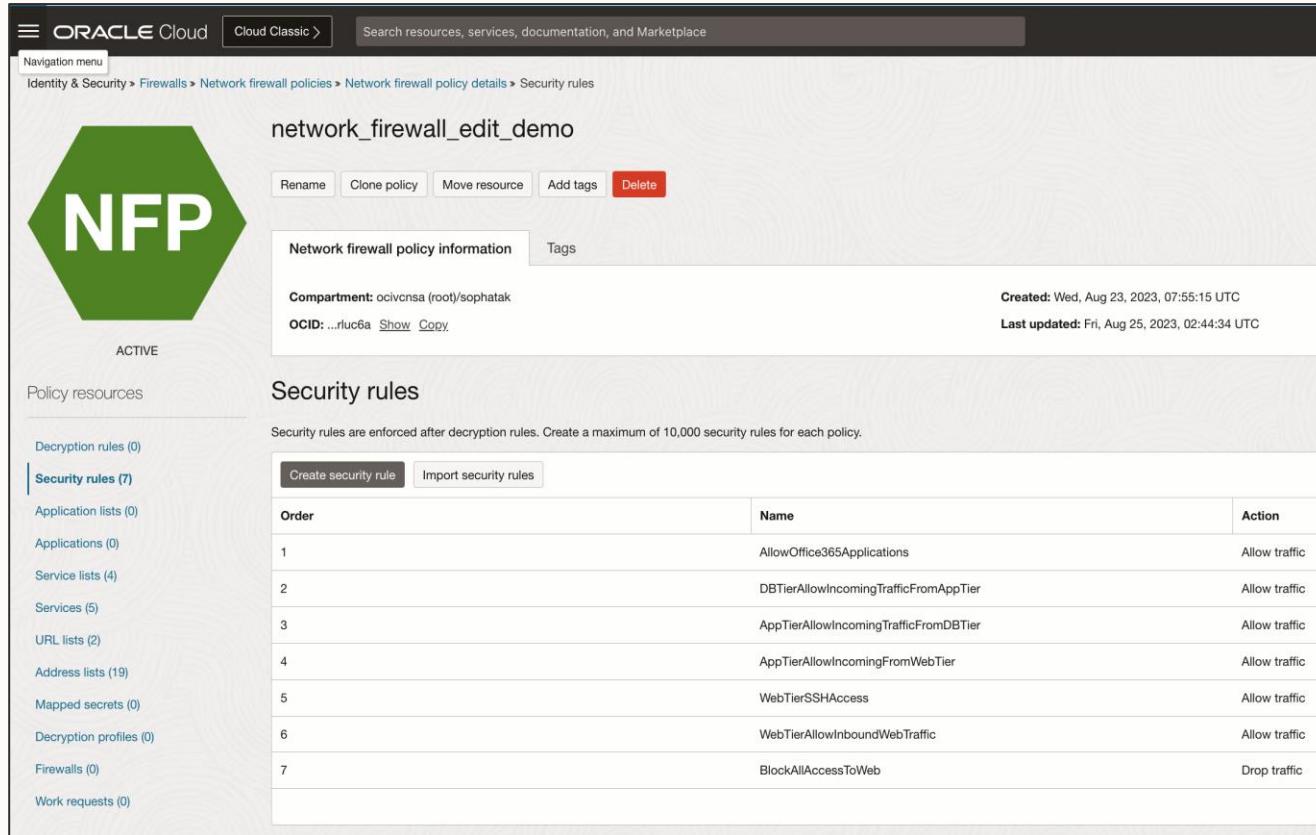
— Oracle Cloud Infrastructure —

Cloud Native Solution



- Best-of-breed Palo Alto network security with OCI-native experience.
- Scalable cloud service supporting 4 - 12.5 Gbps.
- Highly available in both multi-AD and mono-AD regions.
- Eliminates management of 3rd Party infrastructure.

Stateful Network Filtering



The screenshot shows the Oracle Cloud Identity & Security Firewall Policy Details page. The policy is named "network_firewall_edit_demo" and is marked as ACTIVE. It has 7 security rules defined:

Order	Name	Action
1	AllowOffice365Applications	Allow traffic
2	DBTierAllowIncomingTrafficFromAppTier	Allow traffic
3	AppTierAllowIncomingTrafficFromDBTier	Allow traffic
4	AppTierAllowIncomingFromWebTier	Allow traffic
5	WebTierSSHAcess	Allow traffic
6	WebTierAllowInboundWebTraffic	Allow traffic
7	BlockAllAccessToWeb	Drop traffic

- Enforce *Allow* or *Deny* stateful filtering rules based on 5-tuple information.
- Customer-defined priority order for rules across multiple virtual networks.
- Granular policy enforcement with traffic context-aware stateful firewall.
- Enterprise Scale with 10K Firewall Rules, 20K IP Addresses.

Difference between SL/NSG and Network Firewall features

SL/NSG

- Stateful and Stateless Rules for both IPv4 and IPv6 traffic:
 - CIDR Range or Service (Source IP and Destination IP)
 - Protocol
 - Source port
 - Destination port
- Access control list on Subnet and VNIC level.
- By default, all traffic is denied. Rules need to be created to allow the traffic.
- Deny rules can not be created.

Network Firewall

- Stateful filtering *Allow* or *Deny* rules based on 5-tuple information for both IPv4 and IPv6 traffic.
- Signature-based threat detection and prevention (IDS/IPS) engine.
- Control inbound and outbound HTTP/S traffic to a specified list of FQDN including wild cards and custom URLs.
- Decryption profiles for inbound and outbound HTTPS inspection.
- Policies manage traffic for intra-VCN and Inter-VCN centrally.



Custom URL and FQDN Filtering

The screenshot shows two main pages from the Oracle Cloud Infrastructure (OCI) console:

- Network firewall policy details:** A large green hexagonal icon labeled "NFP" is prominently displayed. The page title is "network_firewall_edit_demo". It shows basic policy information: Compartment: ocicnrsa (root)/sophatak, Created: Wed, Aug 23, 2023, 07:55:15, OCID: ...rluc6a, Last updated: Fri, Aug 25, 2023, 02:44. A sidebar lists policy resources like Decryption rules (0), Security rules (7), Application lists (0), Applications (0), Service lists (4), Services (5), and URL lists (2). The URL lists section shows two entries: "Office365URLs" (5 URLs) and "SkypeURLs" (2 URLs).
- Edit URL list:** This modal window is titled "Edit URL list". It contains instructions: "Create a list of URLs that you can allow or deny access to. A URL list can contain a maximum of 1,000 URLs." A "Name" field is populated with "Office365URLs". Below it, a text area lists URLs:

```
outlook.office.com
outlook.office365.com
smtp.office365.com
*.protection.outlook.com
*.mail.protection.outlook.com
```

A note at the bottom states: "Maximum 1,000 URLs. Each URL must be on its own line." At the bottom of the modal are "Save changes" and "Cancel" buttons.

- Use these rules to restrict traffic to a user specified list of fully qualified domain names (FQDN) including wild cards and custom URLs.
- Flexible enforcement for both inbound and outbound traffic.
- **SSL Inspection** - allows inspection of HTTPS (TLS 1.2 and 1.3) encrypted traffic. Natively integrated with highly secure OCI Vault.

Intrusion Detection and Prevention (IDPS)

Security rules		
Security rules are enforced after decryption rules. Create a maximum of 10,000 security rules for each policy.		
Create security rule		
Order	Name	Action
1	OBJ-STR-EICAR-BUCKET-A	Intrusion prevention
2	OBJ-STR-HELLOWORLD-BUCKET-B	Intrusion prevention
3	MANAGEMENT	Allow traffic

Security rule details	
Name: OBJ-STR-EICAR-BUCKET-A	Rule order: 1
Match condition	
Source addresses	<ul style="list-style-type: none">Any address
Destination addresses	<ul style="list-style-type: none">Any address
Applications	<ul style="list-style-type: none">Any application
Services	<ul style="list-style-type: none">Any service
URLs	<ul style="list-style-type: none">OBJ-STR-EICAR-BUCKET-A
Rule action	
Action: Intrusion prevention	

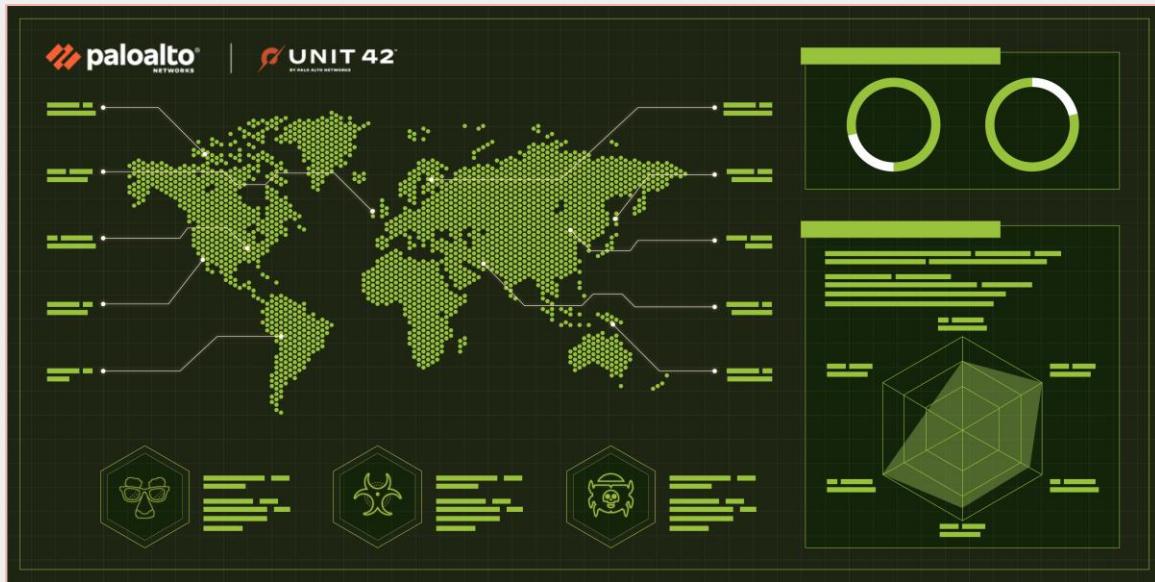
Security rule details	
Name: OBJ-STR-HELLOWORLD-BUCKET-B	Rule order: 2
Match condition	
Source addresses	<ul style="list-style-type: none">Any address
Destination addresses	<ul style="list-style-type: none">Any address
Applications	<ul style="list-style-type: none">Any application
Services	<ul style="list-style-type: none">Any service
URLs	<ul style="list-style-type: none">OBJ-STR-HELLOWORLD-BUCKET-B
Rule action	
Action: Intrusion prevention	

- Detect and block known exploits, malware, malicious URLs, spyware, command and control (C2) attacks.
- Palo Alto Networks security research team uses Advanced Threat Prevention powered by AI to equip the firewall with latest threat intelligence.
- Supports threat detection and prevention on encrypted traffic.

SSL Inspection

- Allows OCI Network Firewall to decrypt, inspect, and re-encrypt encrypted (HTTPS/TLS) traffic for deep packet inspection and threat detection.
- Forward Proxy SSL Inspection
 - Used for outbound traffic (e.g., from a VM to the internet).
 - The firewall acts as an intermediary to decrypt and inspect client-initiated HTTPS connections.
- Inbound SSL Inspection
 - Used for inbound traffic (e.g. from the internet to a public app).
 - The firewall terminates and re-encrypts traffic targeting internal services.

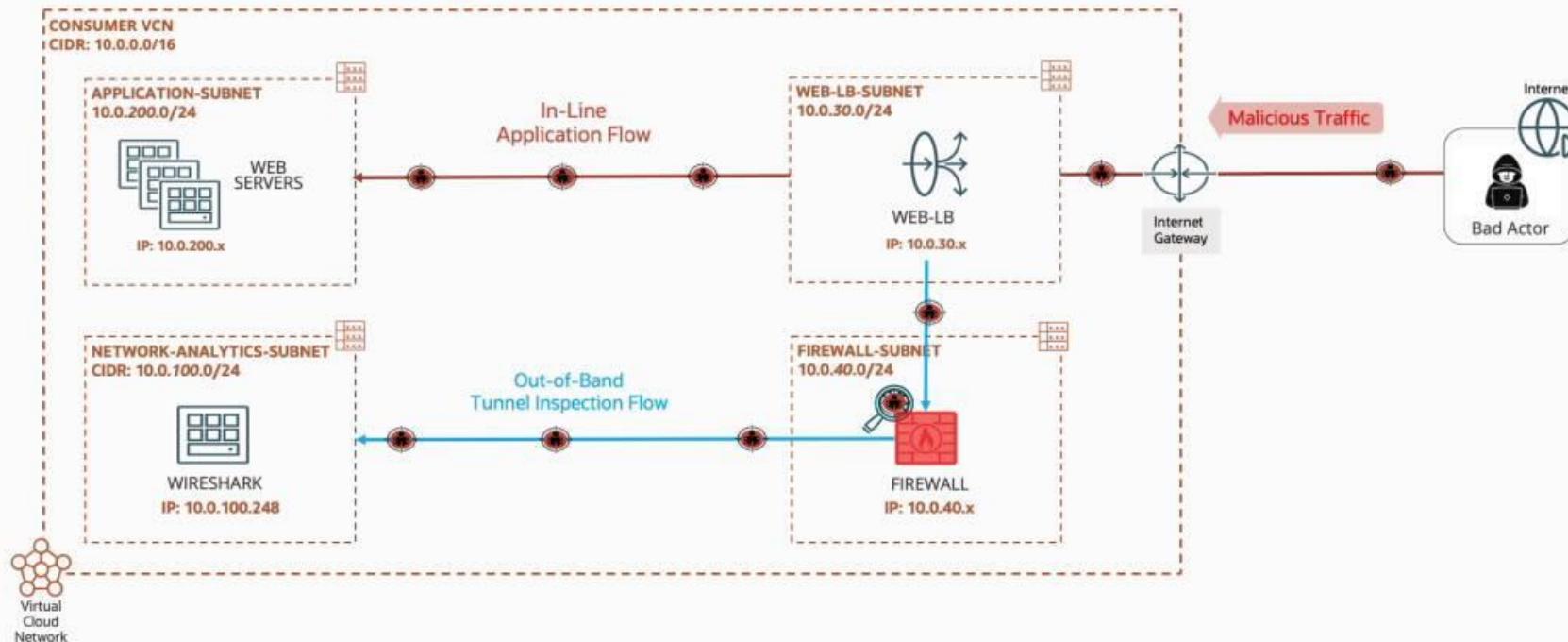
IDP and TLS/SSL encrypted traffic inspection



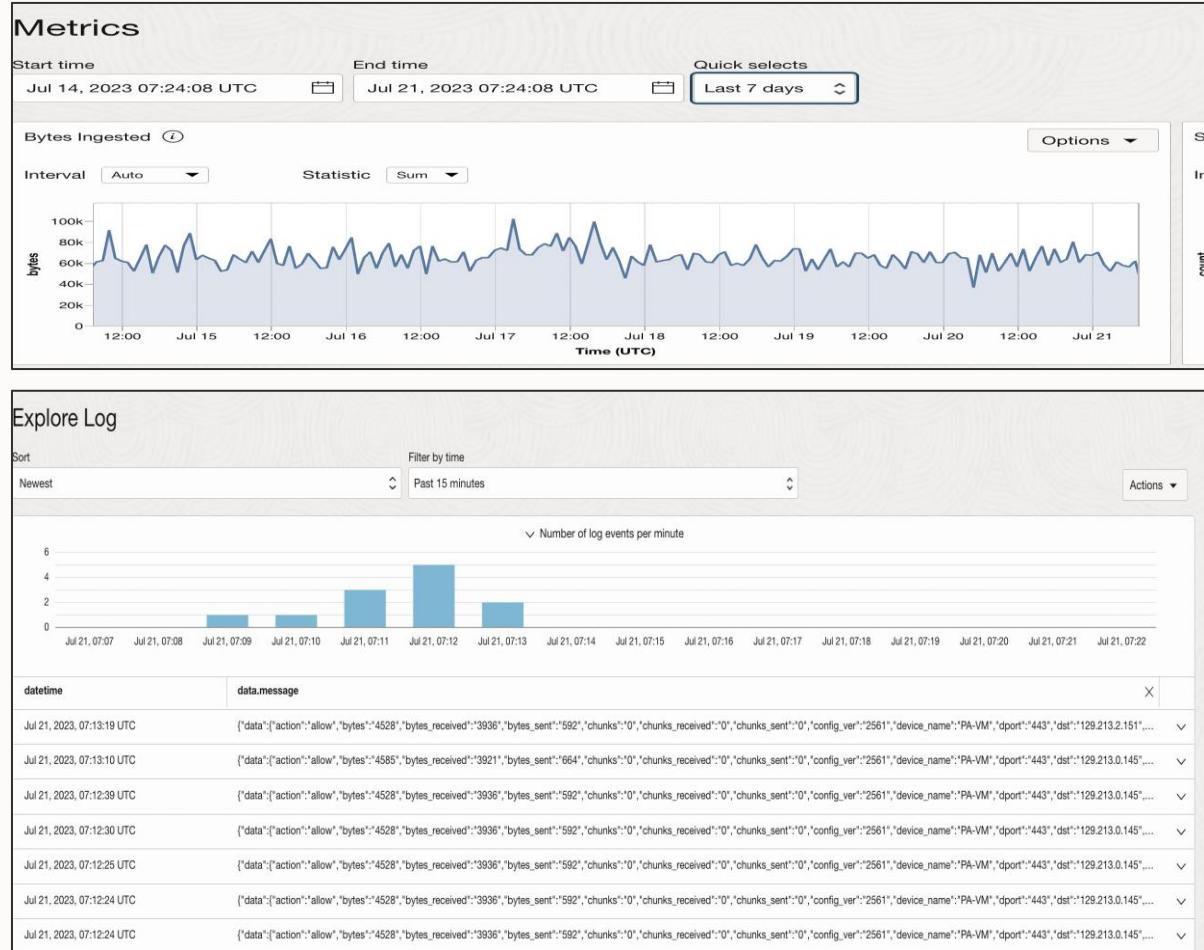
- Integrated IDS and IPS solution built with Palo Alto Networks' threat analysis engine and [Unit 42 - security research teams](#) that identify new threat signatures and detection mechanisms.
- Helps detect (IDS) and block (IPS) known exploits, malware, malicious URLs, spyware, command and control (C2) attacks.
- Use case: OCI Network firewall is to be able to apply Intrusion Detection and Prevention (IDS/IPS) controls to the traffic, including encrypted traffic over SSL/TLS secure channels and to do this, the NGFW must decrypt the SSL/TLS encrypted traffic.

VXLAN Traffic Inspection

- Provides threat detection and analysis capabilities by integrating tunnel inspection with OCI native virtual test access port (VTAP) service.
- This combination allows for comprehensive traffic analysis through a dedicated out-of-band channel. It enables the detection of malicious sources or destinations, identification of inappropriate crypto traffic, and spotting of SSH sessions targeting known command and control (C2) domains.



Logging, Monitoring, and Analytics

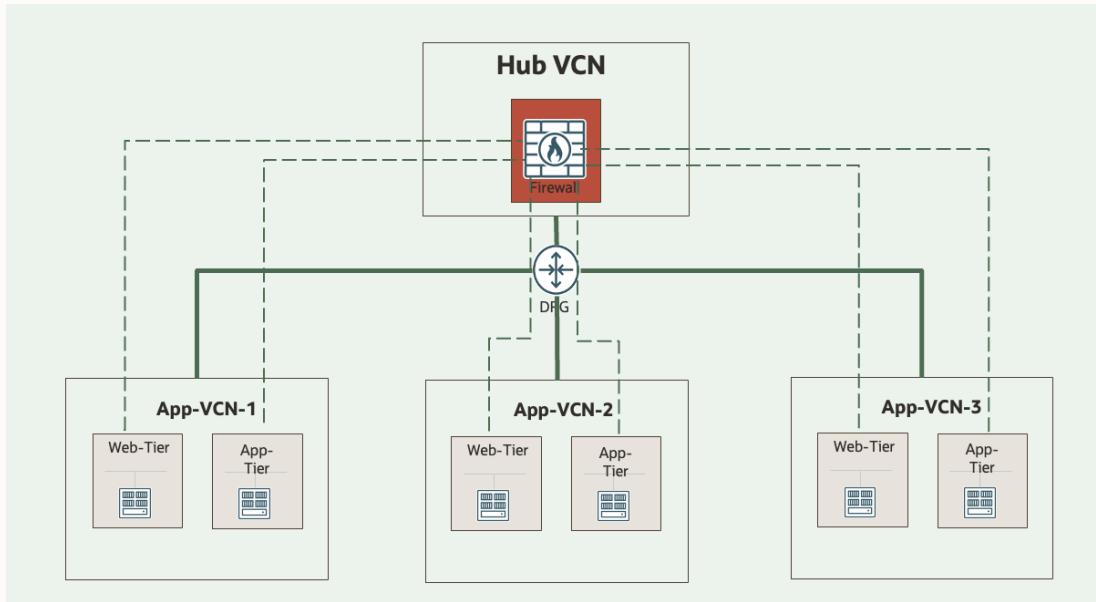


- Network Firewall metrics help monitor the health, capacity, and performance of firewall policies and resources.
- Alarms and Notifications can be configured to notify you when metrics meet alarm-specified triggers.
- Network Firewall logs (integrated with OCI logging) enable you to understand what rules and the countermeasures triggered by requests.
- Logging Analytics provides the *analytics*, making it simpler to explore the data, analyze patterns and out-liners, provide machine learning in the form of clustering and linking, create dashboards, provide topology drill-downs and much more.

OCI Network Firewall - Key Use Cases

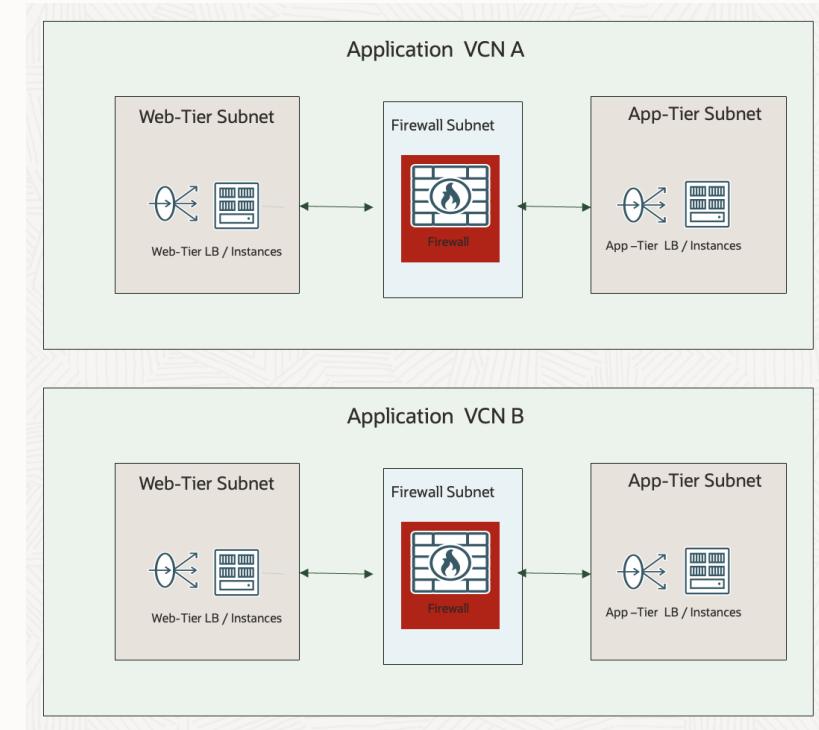
- Internet facing applications: Perimeter security
 - Protect against known vulnerabilities, until you have time to patch/update
 - For example: CVE-2017-5638 for Apache Struts
- Outbound: Protect against exfiltration
 - Allow Ubuntu servers to only do apt-get to *.canonical.com for updates
 - Allow only connections to payment gateway to *.amex.com
- East-West between VCNs or subnets: App Segmentation & Zero Trust
 - Block all threats from moving laterally between different trust domains
 - Allow only approved DB admins to only run SQL transactions against MySQL

Flexible Deployment Topologies



Centralized Deployment

- Network Firewall is deployed in a Hub VCN and connected to spoke VCNs through DRG.



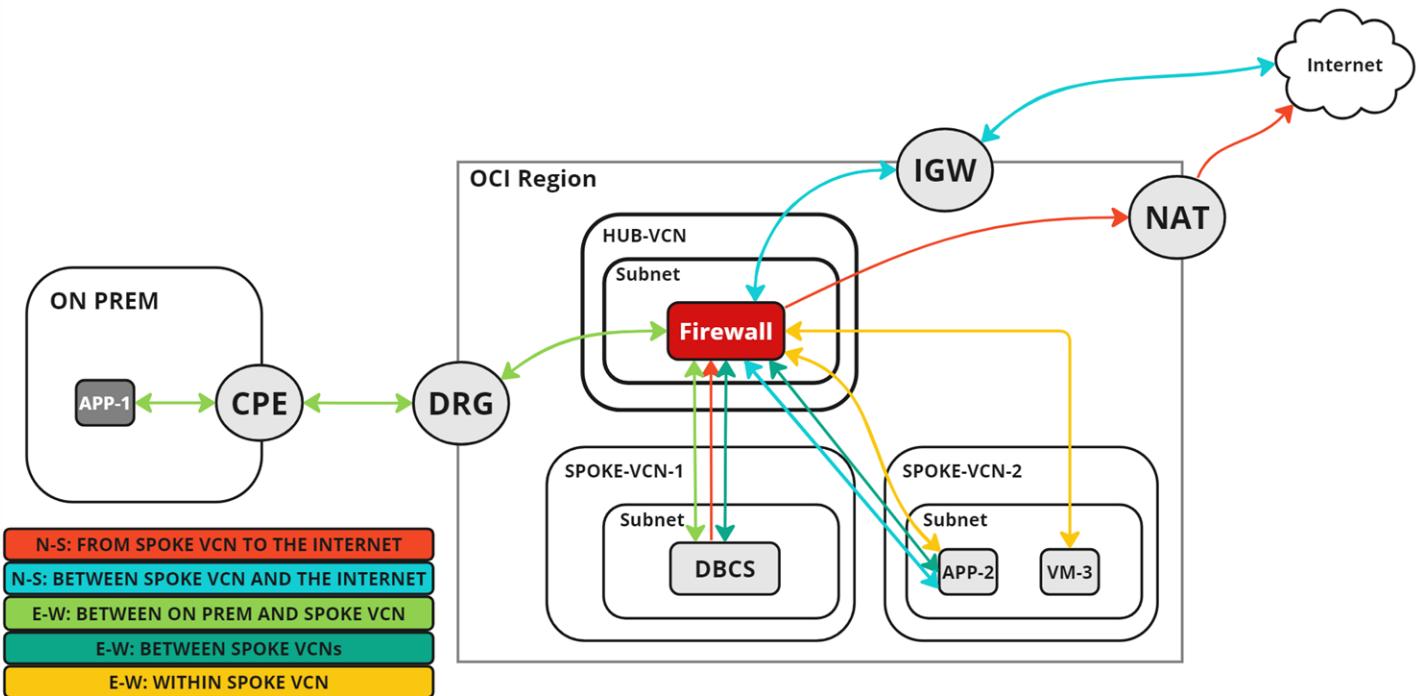
Distributed Deployment

- A dedicated Network Firewall deployed in each VCN.

Hub & Spoke Architecture

It is the most common due to the security and ease of management advantages it gives to organizations. In this scenario, all the communication traverse through a Central “Hub” network, where a Firewall inspect traffic before it reaches the Destination “Spoke” network where the actual workload resides. This provides enhanced security, improved management to your network environment as routing can be controlled between other networks using the hub, and higher scalability as customer can add new networks at any point of time to their existing hub.

- **North-South Traffic:**
 - Between Internet and OCI networks.
- **East-West Traffic:**
 - Between OCI Spoke networks.
 - Between OCI and on-premise networks.
 - Within the Spoke VCN.

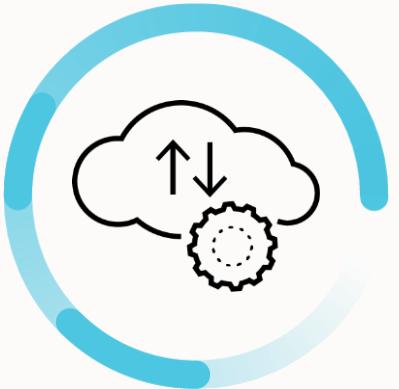


OCI Network Firewall Is...



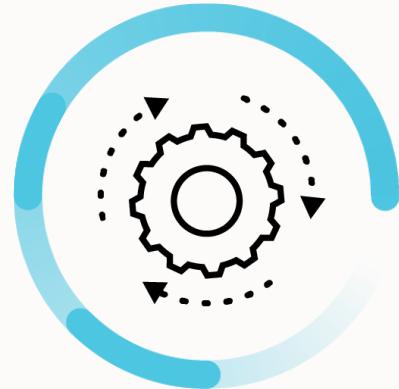
Best-in-class

Powered by Industry Leading Palo Alto Networks technology, best-in-class network security for all your apps



Cloud-Native

Deep integration with OCI platform and features, cloud-native form factor & deployment models



Automated

Easy integration into DevOps processes for automated deployment and scaling



Easy to Manage

Centralized management and Flexible Policy Enforcement



OCI Network Firewall and WAF – Better Together

- **OCI Network Firewall** helps secure network and application workloads. It enables policy-based visibility and control over applications, users and content including access control, SSL decryption, threat prevention, URL filtering and IDS/IPS capabilities.
- **OCI WAF** is primarily focused on the security of web applications and operates at the layer 7 (HTTP/S). It helps stop layer 7 attacks whether it's an attempt to exploit vulnerable code-level vulnerabilities such as SQL injection and other OWASP Top 10 vulnerabilities, or a layer 7 DDoS attack.
- **Layered Defense** - In most cases it's important to employ both technologies given the various potential points for intrusion across both networks and web applications.
- For e.g., in 3-tier architecture web-tier can be protected using WAF. But web tier to app tier and app tier to database tier communications are protected using Network Firewall.

Simple and Flexible pricing



- Network Firewall pricing is comprised of two components—Firewall Instance and Data Processing.
- The instances charge is based on the number of active firewall instances and the data processing covers the volume of traffic processed by the firewall instance.

SKU	Pay as you go rate
Oracle Cloud Infrastructure—Network Firewall Instance	\$2.75 Per Hour
Oracle Cloud Infrastructure— Network Firewall Data Processing	\$0.01 Per GB (10 TB Per Month free)

Domain Name System (DNS) Agenda

- 1 Introduction to DNS
- 2 Private DNS
- 3 Public DNS
- 4 Traffic Management Steering Policies

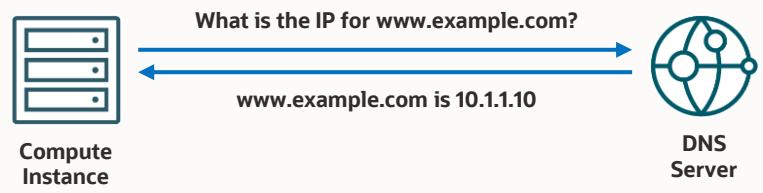
DNS:

“Domain Name System”

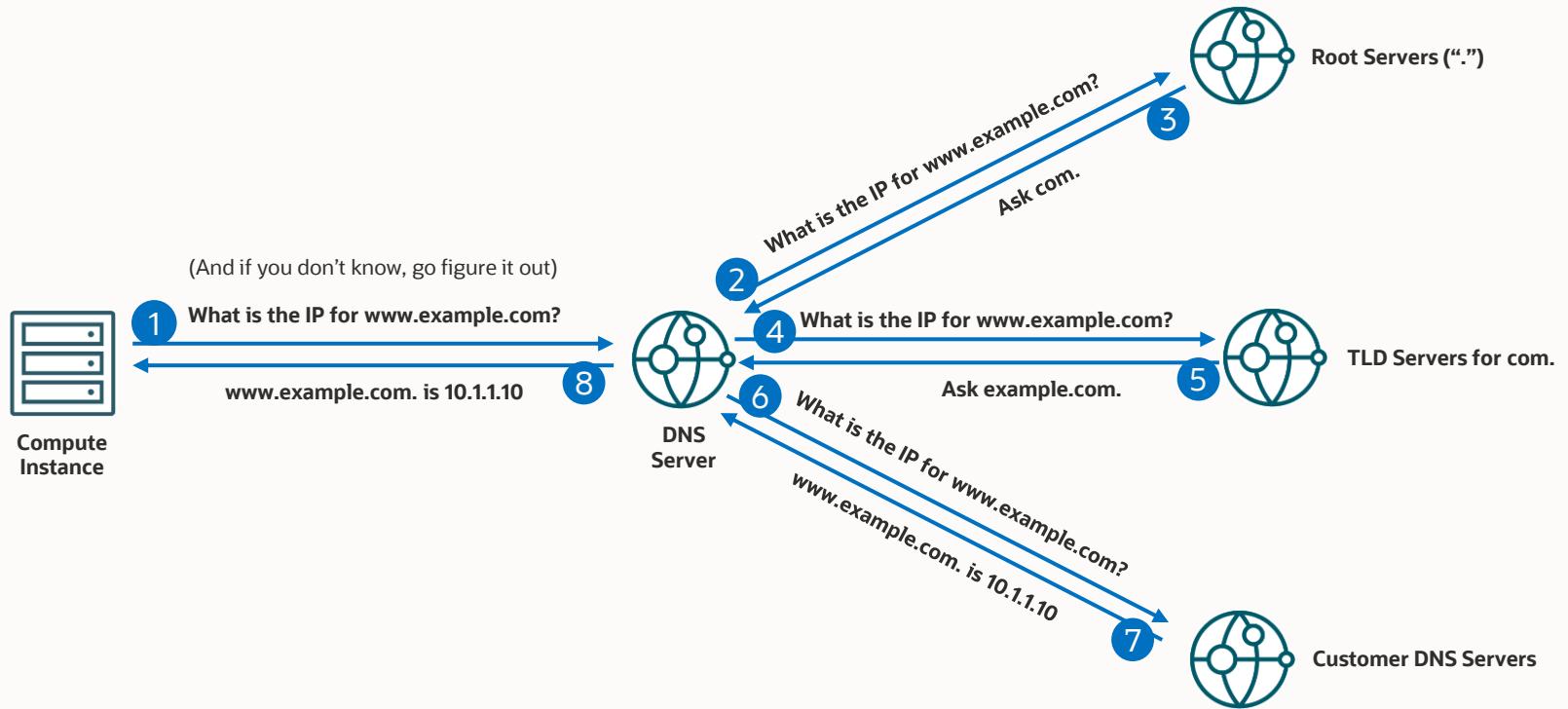
The hierarchical and decentralized naming system used to identify computers, services, and other resources reachable through the Internet or other Internet Protocol (IP) networks.

The resource records contained in the DNS associate domain names with other forms of information. These are most commonly used to map human-friendly domain names to the numerical IP addresses.

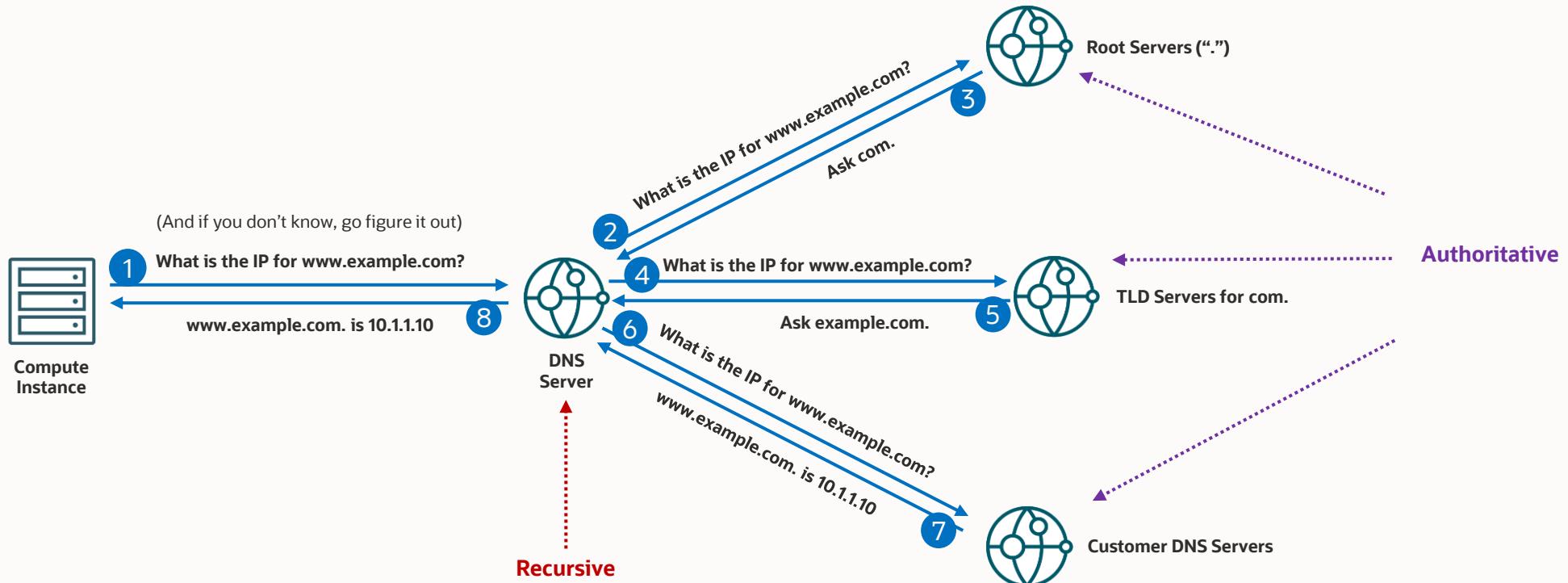
DNS Introduction



DNS Introduction



DNS Introduction

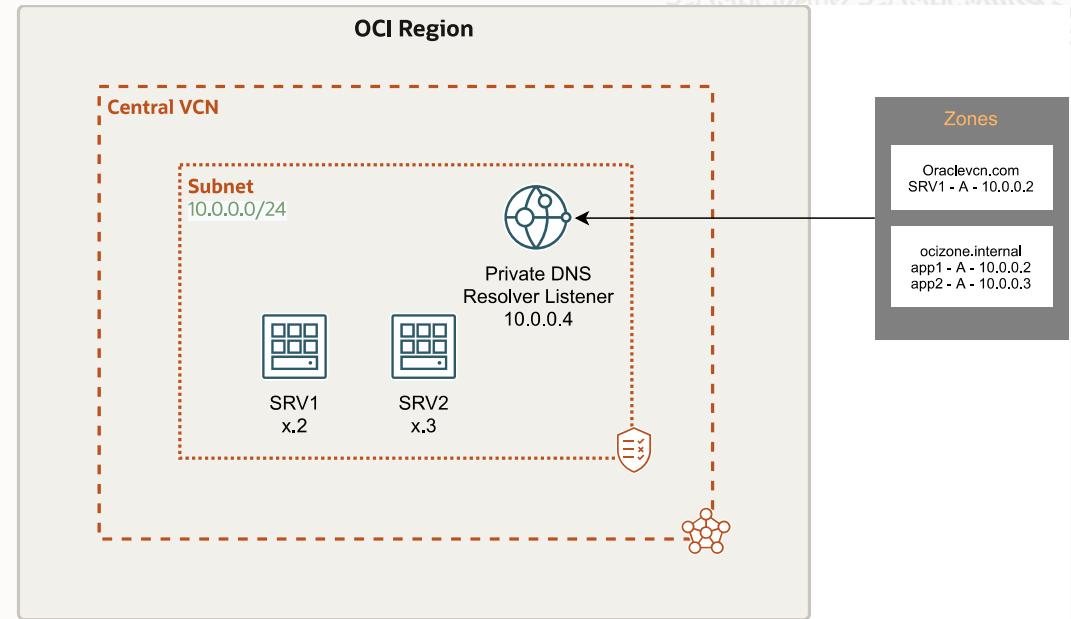


DNS Introduction – Common Resource Record Types

- **A** – An address record.
- **AAAA** – An IPv6 address record.
- **ALIAS** – Non-standard, used to redirect requests.
- **CNAME** – Canonical Name, refers client to use to another name.
- **MX** – Mail Exchanger, the mail servers for a domain.
- **NS** – Name servers, the name servers for domain or subdomain.
- **PTR** – Pointer, enables (reverse) resolution of IP addresses to names.
- **SOA** – Start of Authority, contains primary name server, responsible contacts, serial number.
- **TXT** – Contains text information, various uses including domain validation.

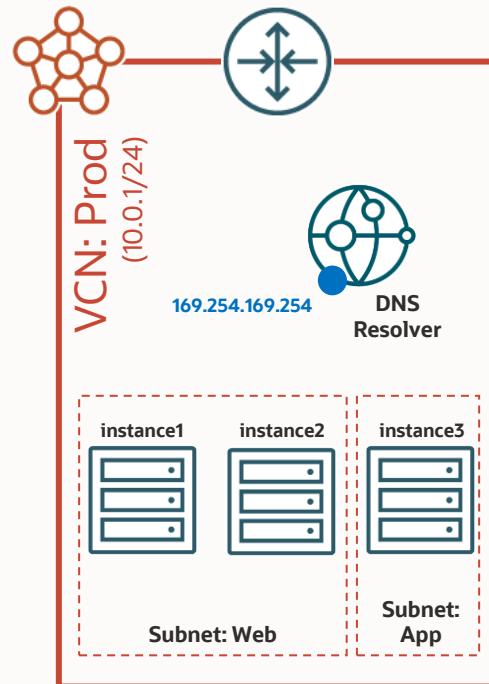
OCI Public & Private DNS

- **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

Virtual Cloud Network DNS

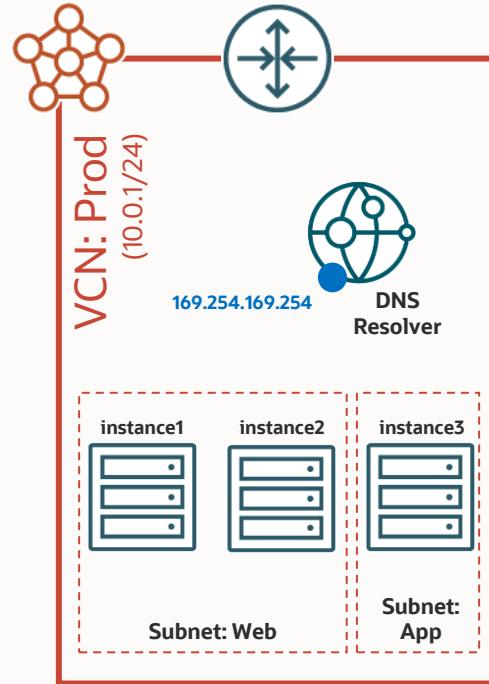


Example: `instance1.web.prod.oraclevcn.com`

● Default Endpoint

- Each VCN has one DNS Resolver.
 - *It is possible to create VCNs with DNS disabled.*
- Available at 169.254.169.254
- Resolves oraclevcn.com names **within** a VCN.
- Resolves DNS names **on the Internet**.

Private DNS

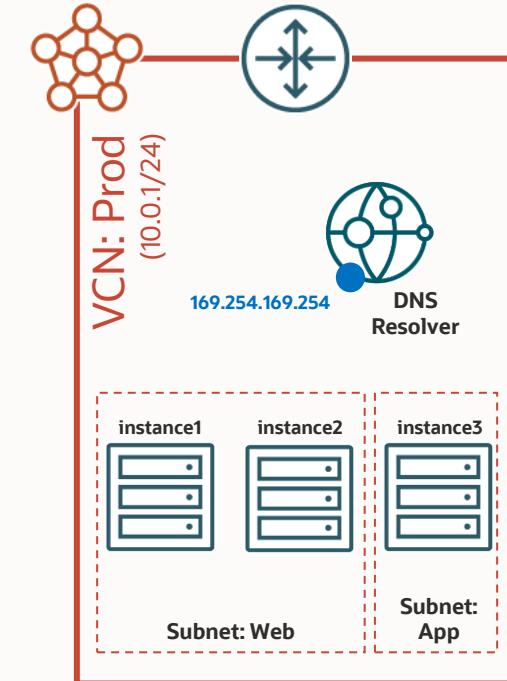


Example: instance1.web.prod.oraclevcn.com

● Default Endpoint

- Continuation of VCN DNS capabilities.
- Available at 169.254.169.254
- By default:
 - Resolves oraclevcn.com names within a VCN.
 - Resolves DNS names on the Internet.
- Adds support for:
 - Private Zones and Views.
 - Endpoints.
 - Rules.

Private DNS – Private Views

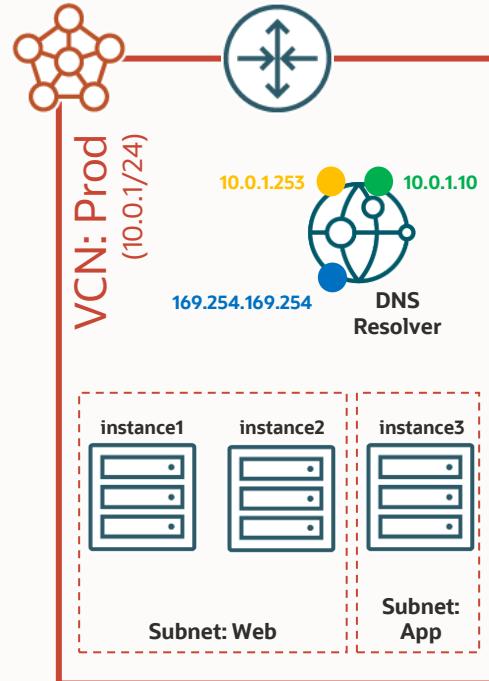


Example: `instance1.web.prod.oraclevcn.com`
`web-prod-1.oci.example.com`

● Default Endpoint

- Allows hosting of custom DNS zones.
- Create custom DNS records in custom zone.
 - Automatically-created DNS records still land in protected DNS zone for subnet in oraclevcn.com.
 - Not possible to assign custom zone to subnet.
- Custom zones can be shared by multiple VCNs.
 - In the same region.
- Private DNS hosts all data for zone.
 - Cannot delegate sub-zones.
 - Cannot be secondary to zone hosted by non-Private DNS server.
 - Cannot have non-Private DNS secondary server.

Private DNS – Endpoints

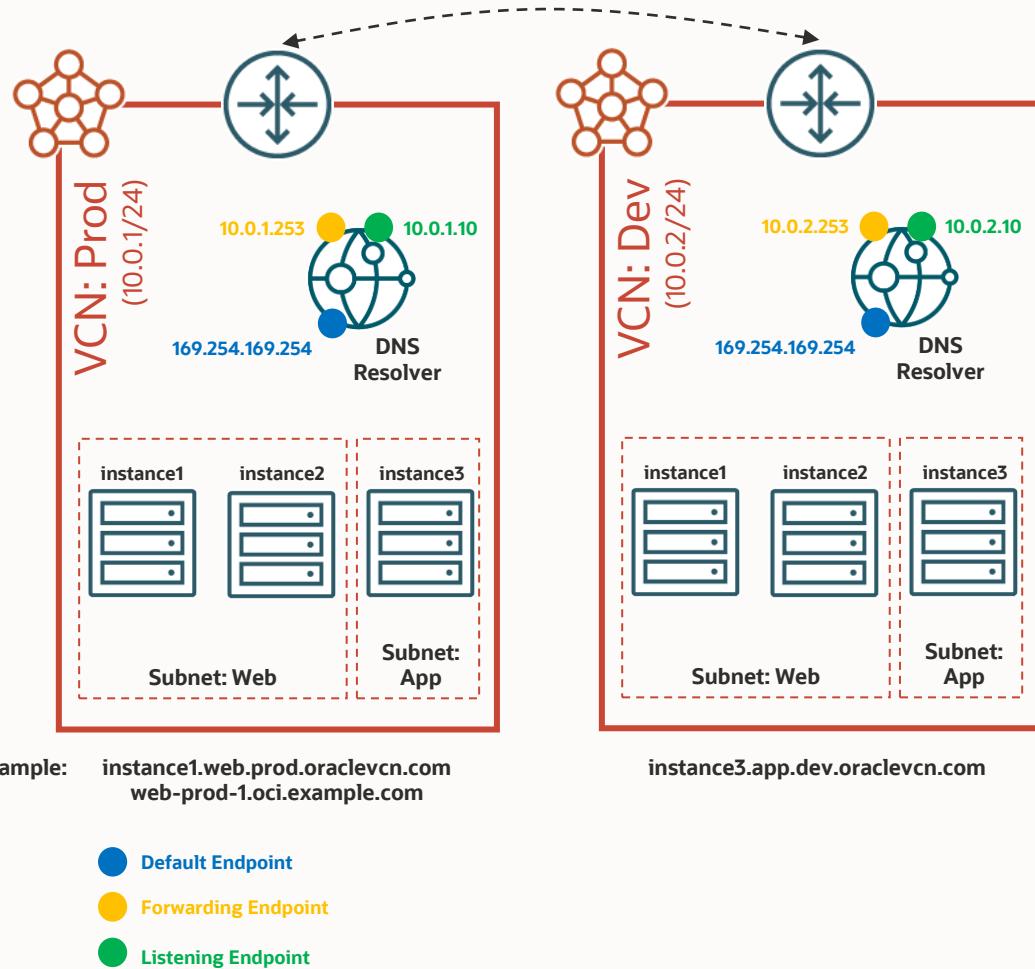


Example: `instance1.web.prod.oraclevcn.com`
`web-prod-1.oci.example.com`

- Default Endpoint
- Forwarding Endpoint
- Listening Endpoint

- Endpoints attach Private DNS resolvers to a subnet in a VCN.
- **Listening Endpoints** receive requests from clients and remote DNS servers.
- **Forwarding Endpoints** are used to send requests to remote DNS servers.
- There must be connectivity between the endpoint and relevant clients or servers.
 - Use DRGs for cross-VCN connectivity.
 - Be mindful of overlapping VCN CIDR ranges.
 - Traffic must be permitted by security lists.

Private DNS – Rules



- Directs requests to a remote DNS resolver.
 - Only used if resolver is not authoritative.
 - Remote DNS server could be **in another VCN or on-prem**.
- Up to 10 rules direct DNS zone to remote Servers.

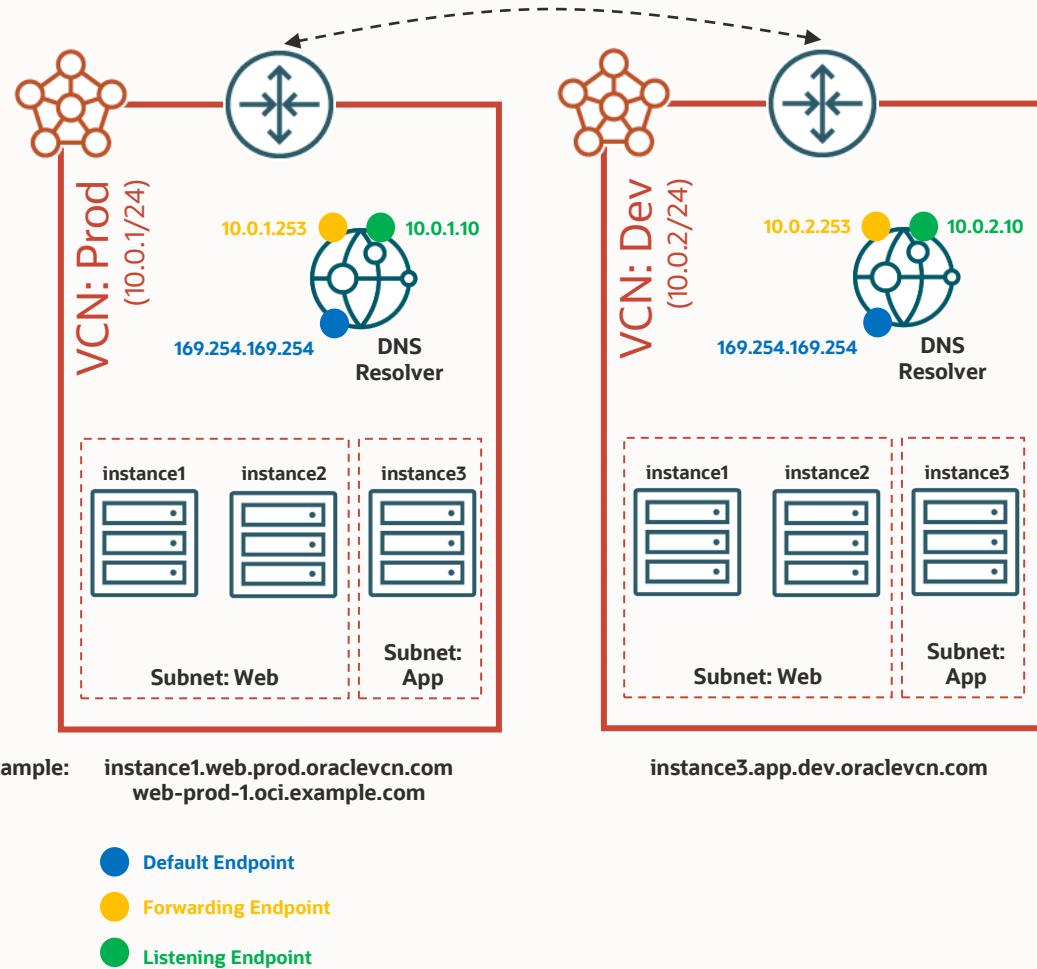
Rules in Prod VCN

Domains	Source (Forwarding Endpoint)	Destination (Listening Endpoint)
dev.oraclevcn.com	10.0.1.253	10.0.2.10

Rules in Dev VCN

Domains	Source (Forwarding Endpoint)	Destination (Listening Endpoint)
prod.oraclevcn.com, oci.example.com	10.0.2.253	10.0.1.10

Private DNS – Demo



1. Create `oci.example.com` Private View in Prod VCN.
2. Create `web-prod-1.oci.example.com` DNS record.
3. Create following DNS rules.

Rules in Prod VCN

Domains	Source (Forwarding Endpoint)	Destination (Listening Endpoint)
dev.oraclevcn.com	10.0.1.253	10.0.2.10

Rules in Dev VCN

Domains	Source (Forwarding Endpoint)	Destination (Listening Endpoint)
prod.oraclevcn.com, oci.example.com	10.0.2.253	10.0.1.10

Public DNS

```
$ dig NS test-at-oracle.com

; <>> DiG 9.10.6 <>> NS test-at-oracle.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56101
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 8

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;tim-at-oracle.com.      IN      NS

:: ANSWER SECTION:
test-at-oracle.com.    86358   IN      NS      ns3.p68.dns.oraclecloud.net.
test-at-oracle.com.    86358   IN      NS      ns4.p68.dns.oraclecloud.net.
test-at-oracle.com.    86358   IN      NS      ns1.p68.dns.oraclecloud.net.
test-at-oracle.com.    86358   IN      NS      ns2.p68.dns.oraclecloud.net.

;; ADDITIONAL SECTION:
ns2.p68.dns.oraclecloud.net. 1272 IN      A      108.59.162.68
ns4.p68.dns.oraclecloud.net. 432 IN      A      108.59.164.68
ns1.p68.dns.oraclecloud.net. 495 IN      A      108.59.161.68
ns3.p68.dns.oraclecloud.net. 933 IN      A      108.59.163.68
ns2.p68.dns.oraclecloud.net. 901 IN      AAAA   2600:2000:2220::68
ns1.p68.dns.oraclecloud.net. 537 IN      AAAA   2600:2000:2210::68
ns3.p68.dns.oraclecloud.net. 1682 IN     AAAA   2600:2000:2230::68

;; Query time: 62 msec
;; SERVER: 206.223.27.1#53(206.223.27.1)
;; WHEN: Thu Mar 24 14:34:03 PDT 2022
;; MSG SIZE  rcvd: 289
```

- Provides **Authoritative DNS** service functionality for public DNS zones.
- Served via anycast from OCI's global commercial regions.
- Supports import in standard BIND zone data format.
- OCI for Primary + Secondary DNS.
 - Hosting a customer's public DNS domains entirely in OCI.
- OCI for Secondary DNS
 - Provides fault tolerance for a customer's public DNS zones hosted on-prem or with other providers.

Public DNS – Traffic Management Steering Policies

- Provides intelligence DNS responses based on user-configured policies
 - **Failover:** Integrates with the OCI Health Checks service to direct clients towards a primary resource while healthy and then failing over to backup resources.
 - **Load Balancing:** Distributes load equally or using user-defined weighting across multiple resources. Uses OCI Health Checks to detect and remove failed resources from service.
 - **Geolocation Steering:** Directs users based on the user's source geography. For example, direct users in Europe to eu.customer.com.
 - **ASN Steering:** Directs users based on the user's source BGP ASN.
 - **IP Prefix Steering:** Directs users based on the user's source IP address.

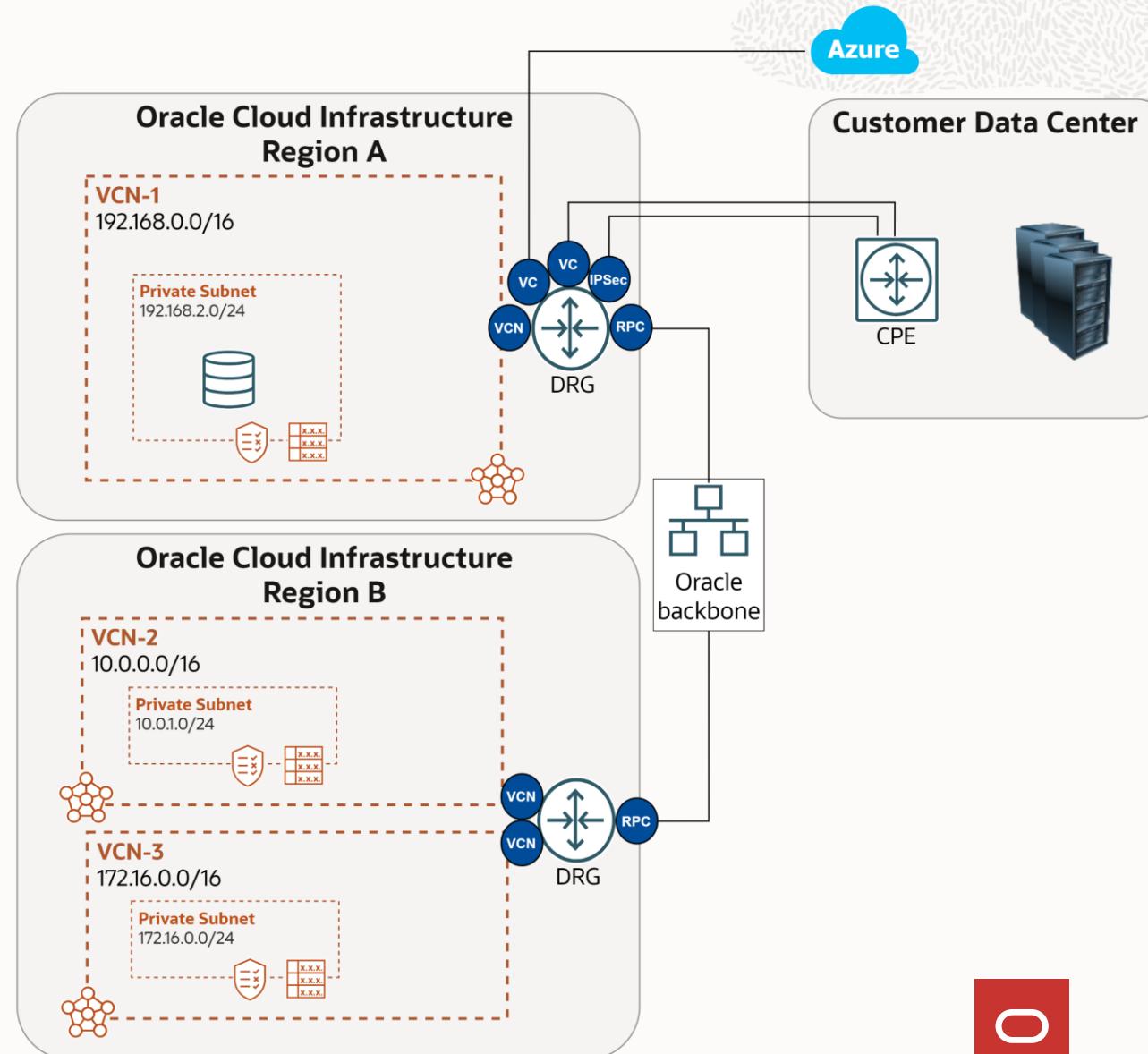
WAN Connectivity (OCI | On-prem | Multicloud)

Chapter Agenda

- 1 Dynamic Routing Gateway (DRG)**
- 2 Site-to-Site VPN**
- 3 FastConnect**
- 4 Oracle Interconnect with Azure and GCP**

Dynamic Routing Gateway (DRG)

- A virtual router that provides a path for private traffic between your VCN and destinations other than the internet.
- DRG is a standalone object. You must attach it to a VCN. VCN and DRG have n:1 relationship.
- 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.

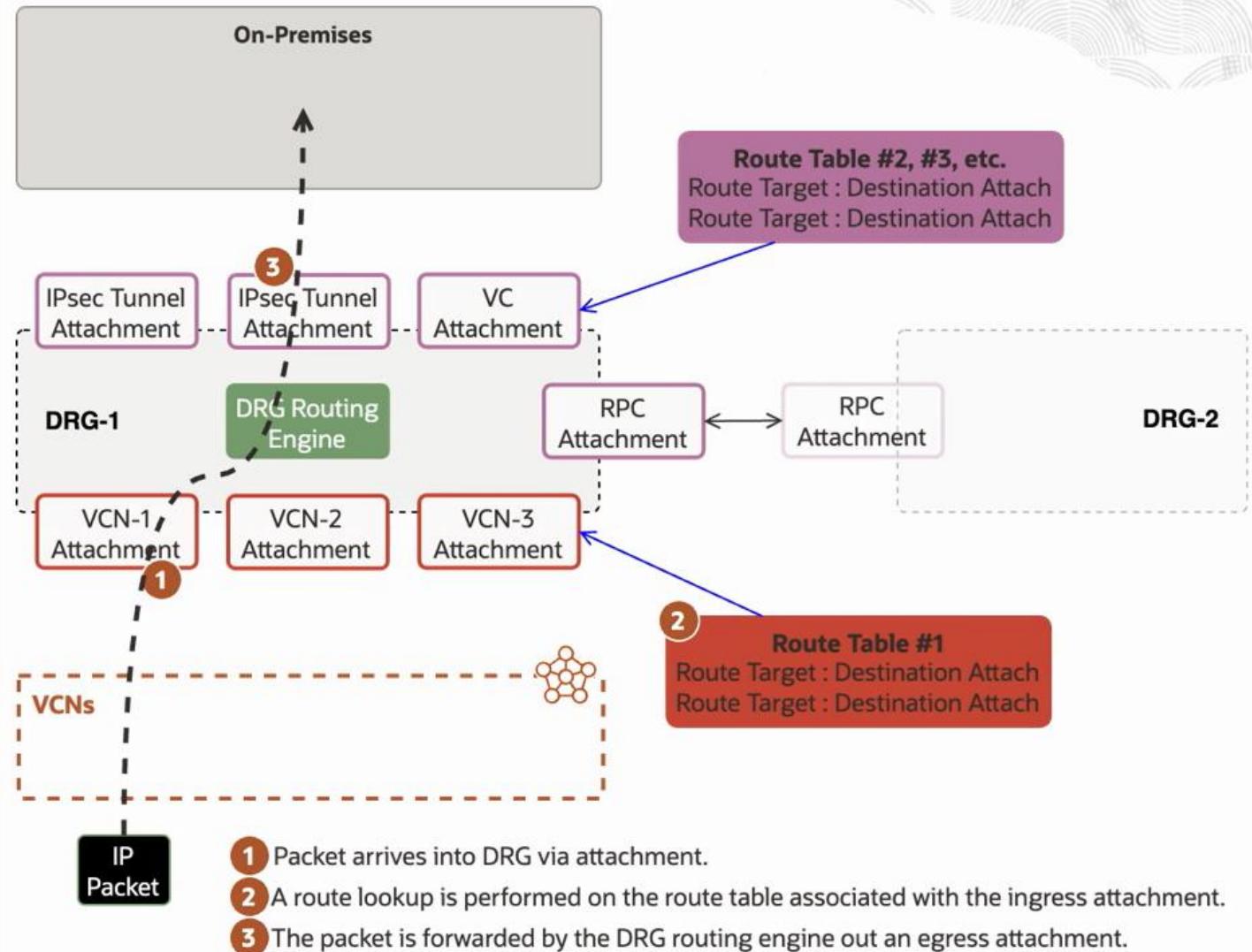


DRG Routing Engine

- 1) An attachment connects a DRG to another network resource:
 - *Virtual Cloud Network (VCN)*.
 - *Remote Peering Connection (RPC)*.
 - *FastConnect (Virtual Circuit)*.
 - *IPSec VPN*.

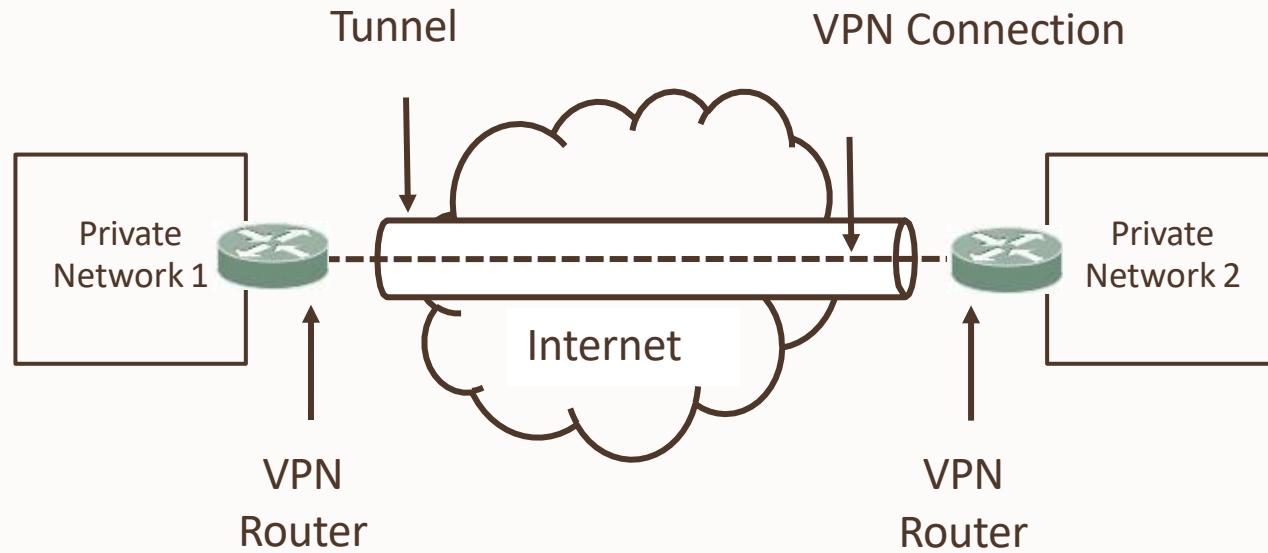
It enables traffic routing between OCI networks and external networks through the DRG.

- 2) Each “Attachment” has a route table assigned, which directs ingress traffic to a specific egress attachment.



VPN Basics

VPN (Virtual Private Network): using a public network to make end to end connection between two private networks in a secure fashion.



- **Tunnel:** A way to deliver packets securely through the internet to private RFC 1918 addresses.
- **Authentication:** Provides a mechanism to authenticate who you are.
- **Encryption:** Packets need to be encrypted, so they cannot be sniffed over the public internet.
- **Static routing:** Configure a router manually to send traffic to a particular destination in preconfigured directions.
- **Dynamic routing:** Use a routing protocol such as BGP to figure out what paths traffic should take.

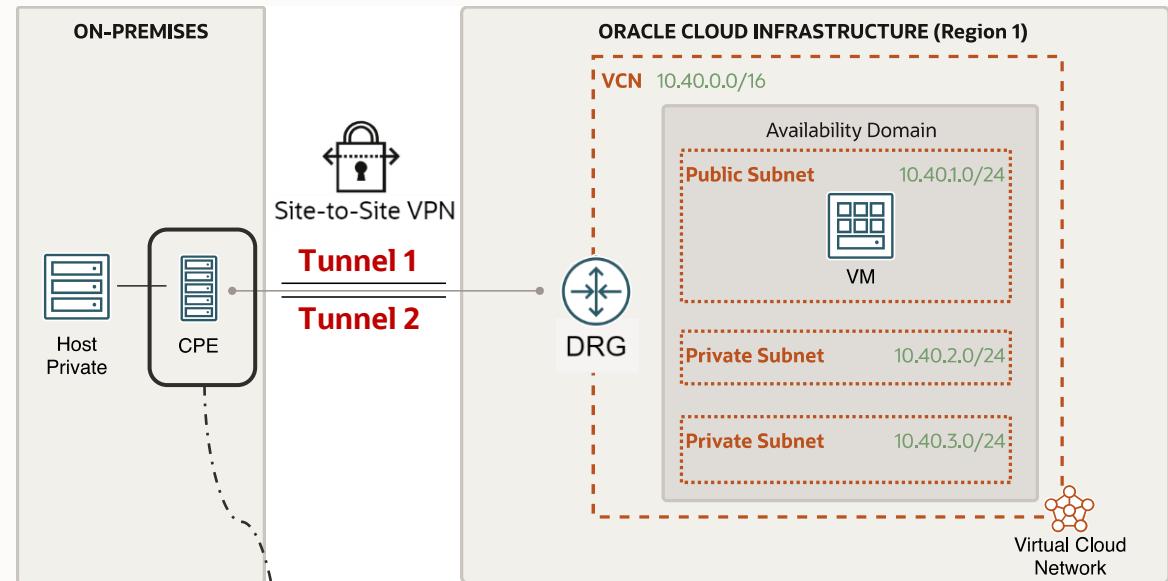
Site-to-Site VPN

- A managed OCI service that encrypts your data and tunnels it through the public internet for enhanced security and privacy with an IPSec VPN connection.
- Bandwidth depends on the customer's access to the Internet and general Internet congestion (Typically less than 250 Mbps – but your mileage may vary).
- OCI provisions redundant VPN tunnels located on physically and logically isolate tunnel endpoints.
- Free service.

Site-to-Site VPN

Use Cases

- Customer Proof of Concepts usually start as a VPN and then morph into FastConnect designs.
- Connect your headquarters branch locations, and private datacenters to the Oracle Cloud so all of your offices can access applications.
- Securely connect your existing infrastructure to the cloud or connect multiple clouds.
- Use VPN as a backup connection for FastConnect.



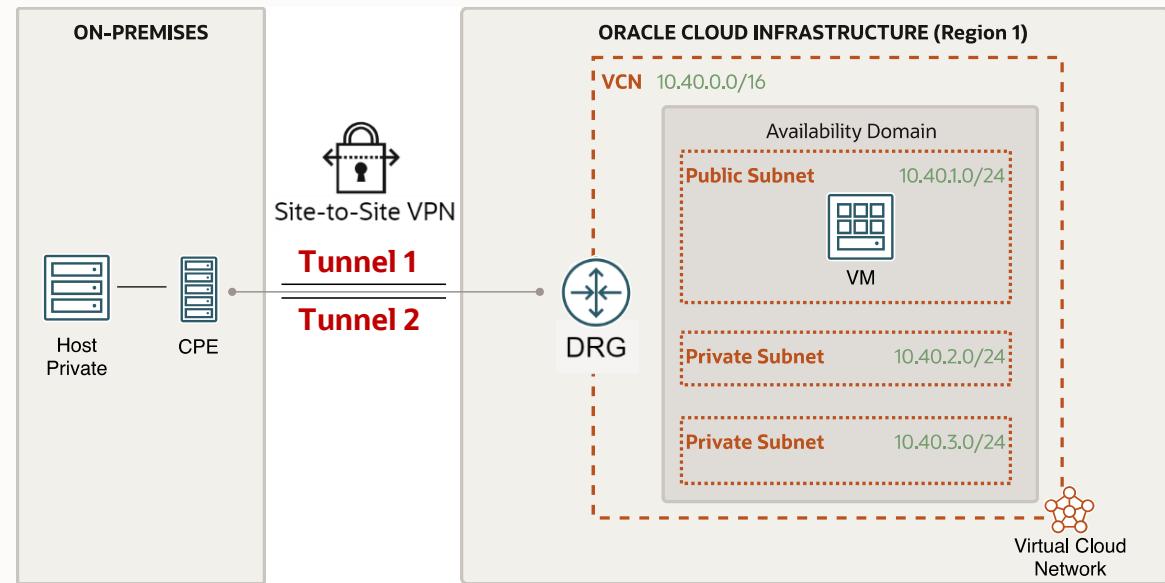
Verified CPE Devices

- Check Point
- Cisco
- FortiGate
- Palo Alto
- Libreswan
- Openswan
- Strongswan
- Juniper
- WatchGuard
- Yamaha
- Furukawa Electric
- NEC

Site-to-Site VPN

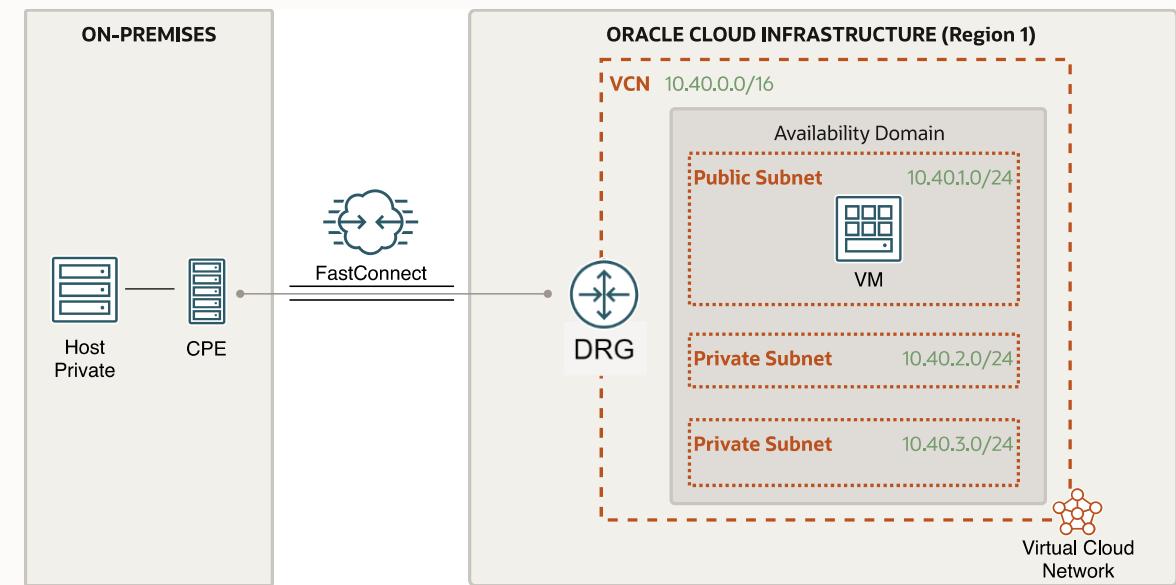
Workflow

1. Create a Virtual Cloud Network (VCN).
2. Create a Dynamic Routing Gateway (DRG).
3. Attach DRG to your VCN.
4. Update VCN routing to send traffic to DRG.
5. Create a CPE Object and add on-premises router (firewall) Public IP address.
6. Create an IPsec Connection between CPE and DRG and provide a Static Route or use BGP routing.
7. Configure on-premises CPE Router. Make sure to configure the appropriate IPSec parameters on both ends.



FastConnect

- Dedicated, private, secure network connectivity from customer locations to OCI via integrated Network Partners.
- Port speeds of 1Gbps, 10Gbps, 100Gbps, or 400Gbps are available.
- Recommended to use 2x for redundancy.
- Use BGP protocol.
- No charges for inbound/outbound data transfer. FastConnect only charges a per-hour port fee based on the port speed.



FastConnect

Use Cases

- Latency-sensitive enterprise applications.
 - Ensures consistent network performance and low latency.
- Big data and high-performance computing.
 - When transferring large amounts of data, FastConnect provides the throughput and consistency required for data-intensive jobs.
- Sensitive data that cannot traverse the internet.
 - FastConnect isolates sensitive data traffic and improves security and privacy because data traffic flows strictly over trusted endpoints.
- Lift and shift to the cloud.
 - Migration involves large data transfers and short-time windows. FastConnect provides high performance and dedicated network connectivity.

FastConnect Models

1) Oracle FastConnect Partner Network

- Direct connection between the customer and Oracle through a pre-established FastConnect partner.
- The most flexible and typically least expensive to set up.

Partners like:

- AT&T Business
- BT
- Digital Realty
- EdgeConnex
- Equinix
- InterCloud
- Interxion
- Megaport
- NextDC
- NTT Communications
- Orange Business Services
- TATA Communications
- Verizon

2) Direct Cross-Connect (Colocation)

- Direct connection between the customer and Oracle when both are in the same FastConnect facility.
- Good model if the customer and Oracle are already collocated.

3) Direct Cross-Connect (Third-Party Provider)

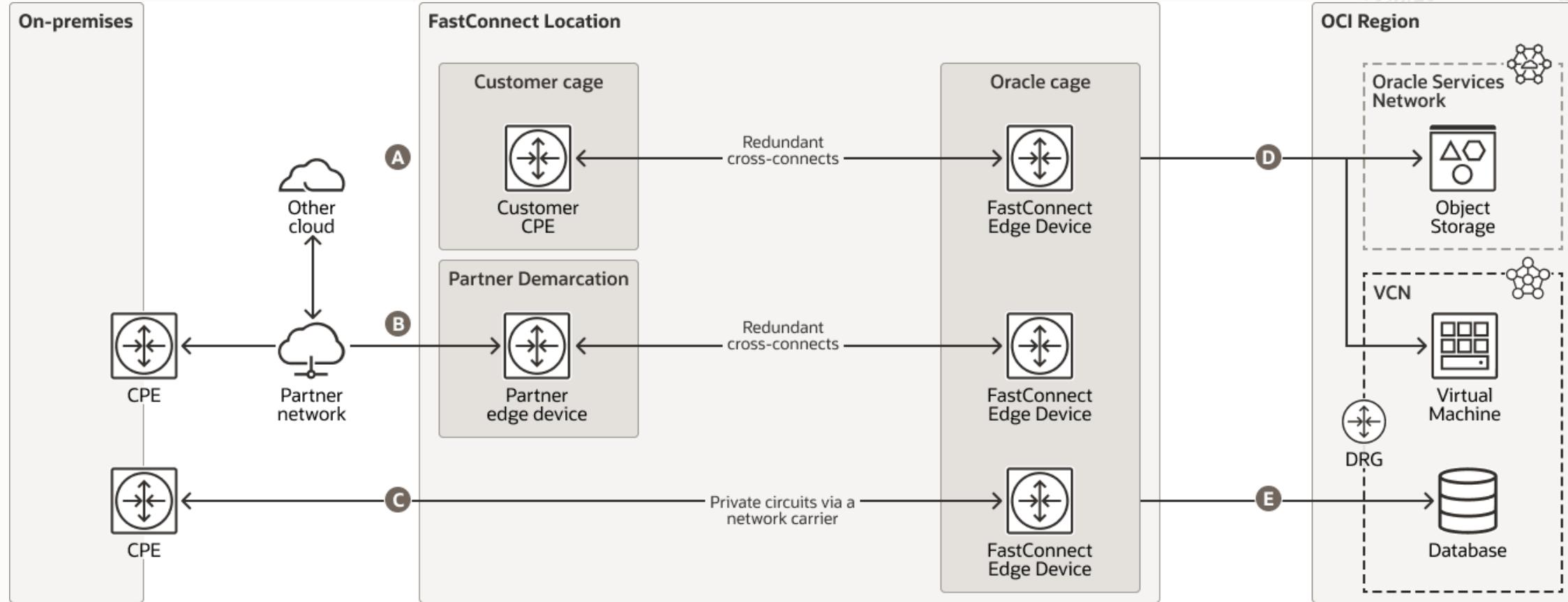
- Connection between the customer's network provider and Oracle using a dedicated circuit.
- Least flexible and typically most expensive to set up.

FastConnect Models

Colocation

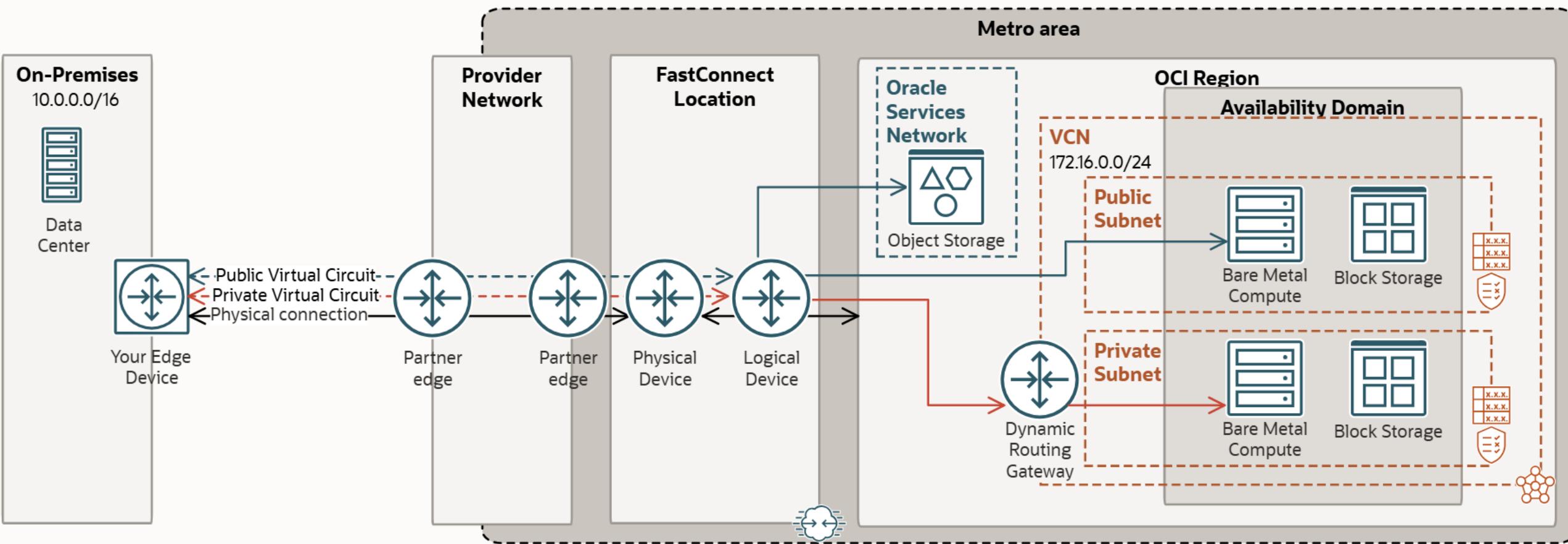
Partner

3rd Party Provider



FastConnect Peering Types

- **Private Peering (Infrastructure Extension):** When a dedicated connection between on-premise and OCI VCN is needed. Traffic does not go over public internet.
- **Public Peering (Internet Alternative):** If customer requires only direct access to Oracle Service Network from on-premise.



Private Peering Network Design

- **Routing Protocol**

- OCI currently supporting BGP (Border Gateway protocol) as a routing protocol for FastConnect connectivity to connect to partners as well as customers.
- BGP is standardized exterior gateway protocols designed to exchange routing and reachability information between ASNs.
- BGP is open standard protocol supported by all hardware vendor.

- **BGP IP address assignment**

- Customer/L3 Provider can use any /30 or /31 IP address that they want to use.
- This IP address is used for point-to-point addressing as well as BGP peer addresses.

Private Peering Network Design

- **BGP ASN**
 - Similar to public and private addresses there are private (64512- 65535) & public ASN allocation.
 - 2-byte or 4-byte ASNs are supported.
 - Oracle's BGP ASN for the commercial cloud is 31898.
 - Customer can use any ASN that they comfortable using.
- **LAG Support (Cross-Connect Groups)**
 - You can aggregate multiple physical links into a single logical channel based on IEEE 802.3ad also known as LACP (Link Aggregation Control Protocol).
 - LAG provides link level redundancy and OCI always recommend partners and customer to build LAG even with a single physical member so when we have to scale up there is no downtime.

Private Peering Network Design

- **BGP Authentication**

- OCI supports BGP authentication mechanisms like Message Digest5 (MD5) algorithms. When authentication is enabled any TCP segment belonging to BGP exchanged between peers is verified and accepted only if authentication is successful.
- Most types of authentication require administration and can disproportionately consume router resources as a result. OCI doesn't recommend using it unless customer have hardcore requirement.

- **BGP Prefix-Acceptance**

- OCI will accept any-prefix advertised by customer over the FastConnect BGP session.
- No restriction on prefix-length.
- The only limit is the number of prefixes that customer can advertise over the VC/BGP session:
 - For private virtual circuits: 2000 IPv4, and 500 IPv6 prefixes.

Public Peering Network Design

- **BGP IP address assignment**
 - In contrast to FastConnect-private, Customer's Layer 3 point-to-point interface will be part of shared Internet routing-instance instead of unique DRG routing-instance.
 - Because of customers are going to share same routing-instance we need to make sure that the IP addresses are unique.
 - OCI will assign the point-to-point IPs from range (169.254.0.0/16).
- **BGP Prefix-advertisement**
 - You can use route filtering to choose to advertise public routes used by ephemeral IP address ranges, reserved IP address ranges, and Oracle Services Network (OSN) to your on-premises network at the region, market, or global (all regions in all markets) scope.
 - Public prefixes will include IP ranges that covers all public services offering by OCI.
 - Public prefixes will also covers all the customer's public VCN host prefixes.

Public Peering Network Design

- **BGP Prefix-acceptance**

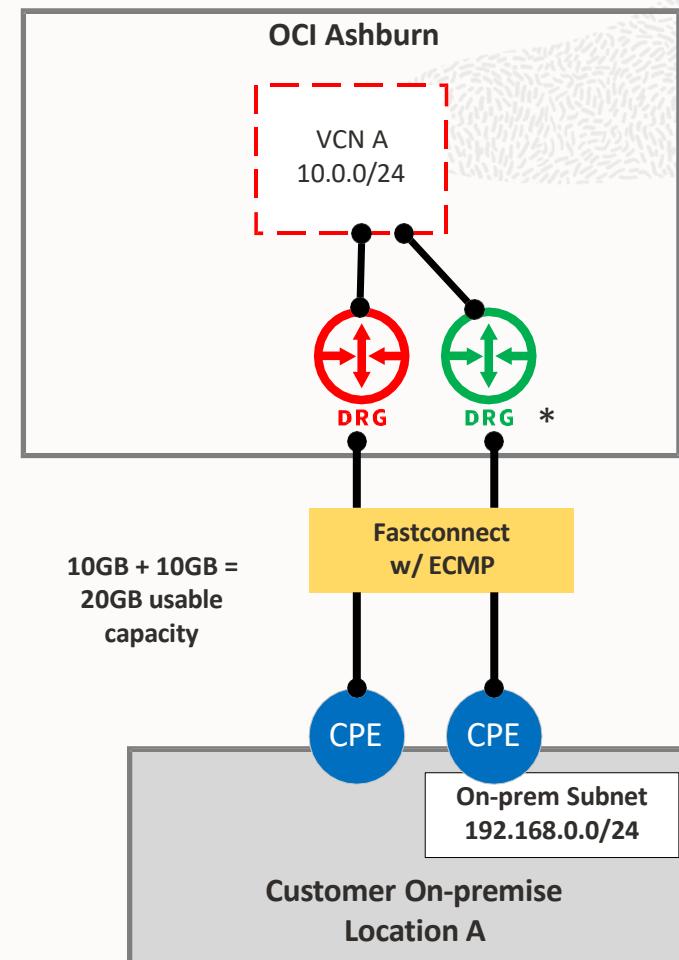
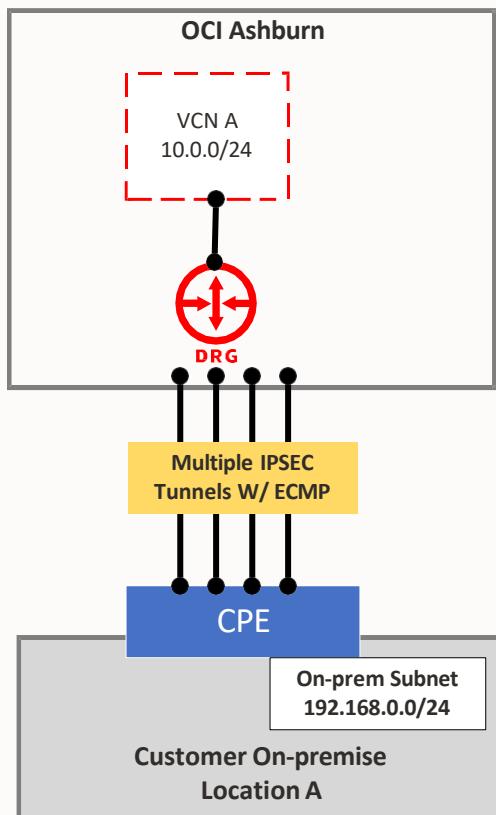
- Customer provides list of prefixes that they want to advertise via console.
- OCI accepts the public-prefixes only if prefixes are owned by customer.
- OCI Check multiple Internet Route Registry database (Using Dyn tool) to verify who owns the prefixes before accepting the prefix from the customer.
- There is a limit on the number of prefixes that customer can advertise over the VC/BGP session:
 - For public virtual circuits: 200 prefixes.

- **BGP ASN**

- OCI will use 31898 ASN.
- Customer needs public ASN to peer with OCI.

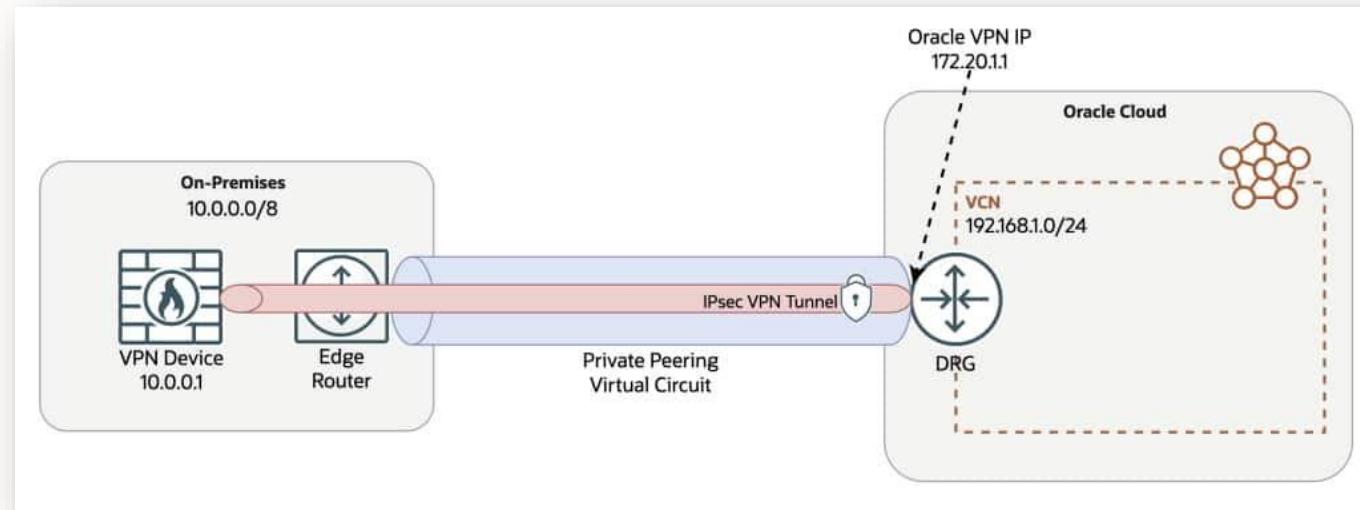
DRG: ECMP (Active/Active)

- OCI Supports **Equal-Cost Multi-Path** for Active/Active load sharing and failover of network traffic between on-premise and OCI.
- You can bundle up to **8** IPsec or FastConnect connections (but not mix of them).
- Enabled on a per-route table basis.



IPSec Over FastConnect

- Standard IPSec VPNs to encrypt FastConnect private peering traffic.
- Combine Site-to-Site VPN and FastConnect services.
- No need for public peering/customer-managed network virtual appliance.
- Multiple tunnels per virtual circuit.
- Route encrypted and unencrypted traffic on the same virtual circuit.



Multicloud Architecture

Offers private, low-latency connectivity between selected OCI Regions, with Azure and GCP Networks.

Oracle Interconnect for Azure

- Use a direct interconnection between OCI and Microsoft Azure that provides less than two milliseconds of latency for superior multicloud network performance.
- Run applications, including Oracle E-Business Suite, on OCI with distributed data stores on OCI and Microsoft Azure.
- Maximize application performance by connecting directly to Oracle Autonomous Database, Exadata Database Service, and MySQL HeatWave environments in OCI.



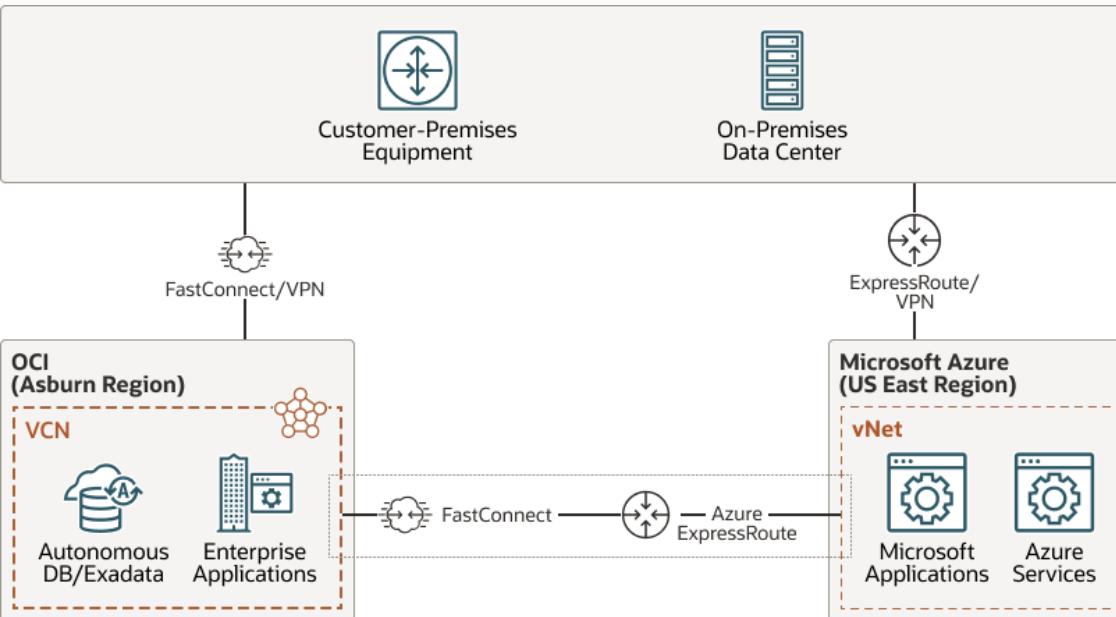
Oracle Interconnect for Google Cloud

- Create a low-latency, high-throughput, private connection with seamless interoperability for first-class multicloud network performance.
- Deploy workloads across both OCI and Google Cloud regions with no cross-cloud data transfer charges.
- Raise support issues through Oracle or Google. Oracle and Google will collaborate to resolve them.

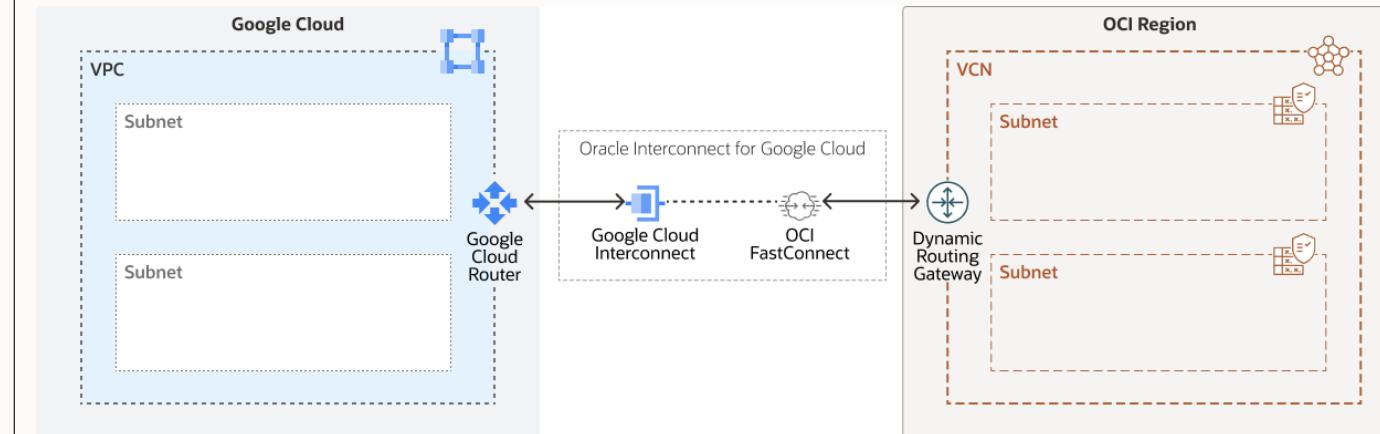


Multicloud Architecture

Oracle Interconnect for Azure



Oracle Interconnect for Google Cloud



Customer Onboarding

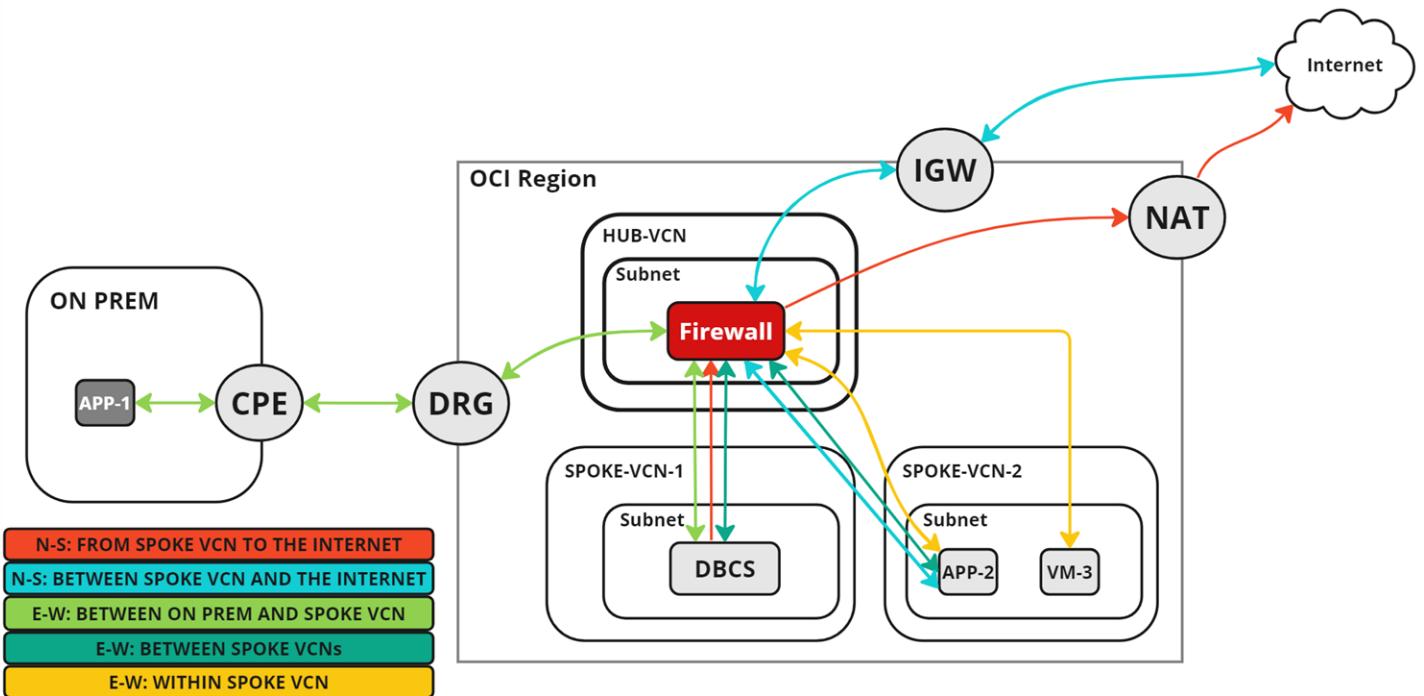
Chapter Agenda

- 1 Hub & Spoke Architecture
- 2 Redundant Connectivity
- 3 Multi-Region Communication
- 4 DRCC

Case Study 1: Hub & Spoke Architecture

It is the most common due to the security and ease of management advantages it gives to organizations. In this scenario, all the communication traverse through a Central “Hub” network, where a Firewall inspect traffic before it reaches the Destination “Spoke” network where the actual workload resides. This provides enhanced security, improved management to your network environment as routing can be controlled between other networks using the hub, and higher scalability as customer can add new networks at any point of time to their existing hub.

- **North-South Traffic:**
 - Between Internet and OCI networks.
- **East-West Traffic:**
 - Between OCI Spoke networks.
 - Between OCI and on-premise networks.
 - Within the Spoke VCN.



Monitoring traffic using OCI Network firewall

Scenario: Monitoring E-W and N-S traffic using different Network firewalls.

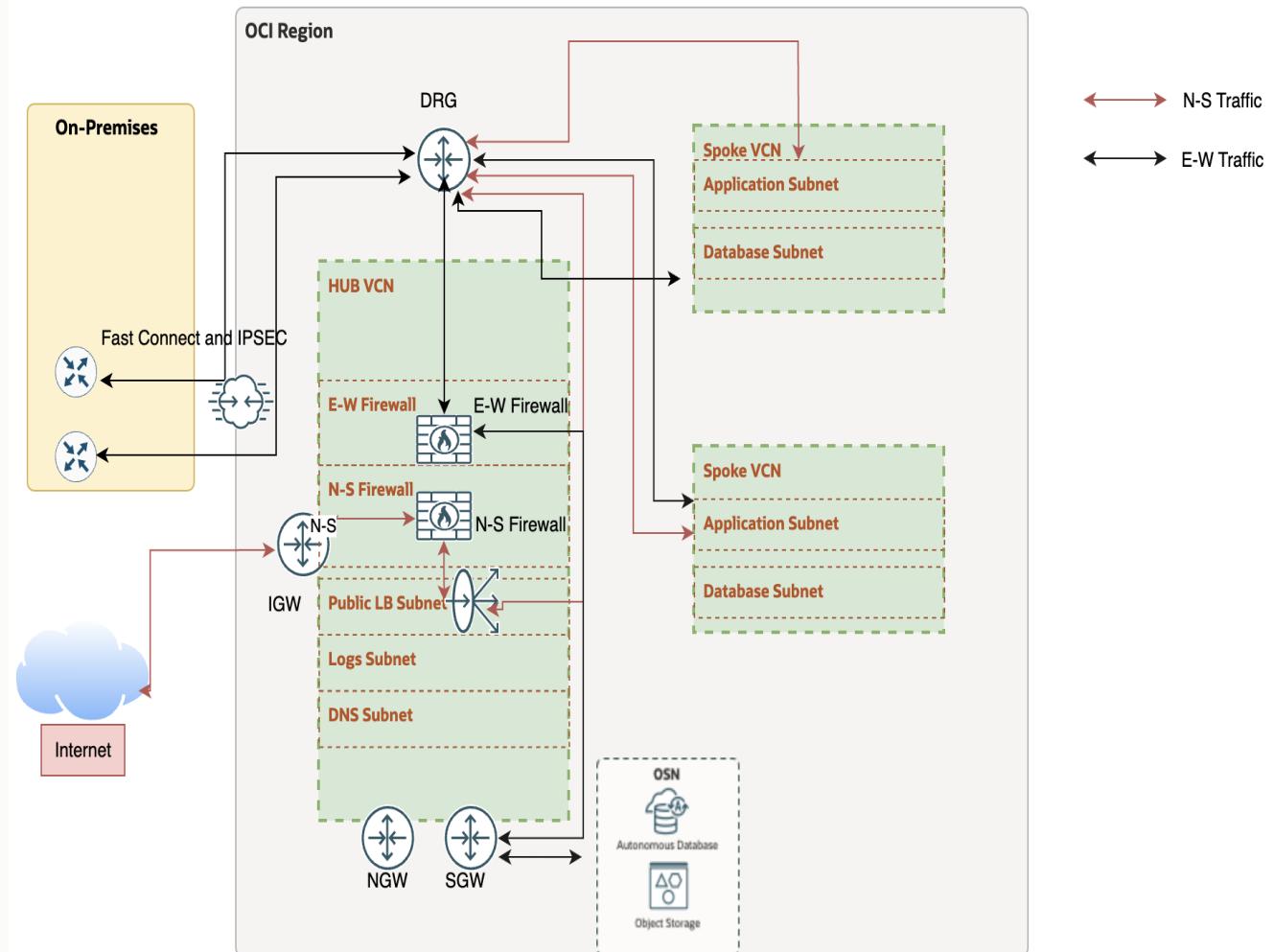
Enhance Security by segregating and monitoring different types of network traffic.

- **E-W firewall Monitoring:**

- Focuses on traffic exchanged between private IP addresses over DRG and subnet to subnet communication for inter VCN and intra VCN both.
- Monitors the traffic initiated for OSN over SGW on OCI Backbone and initiated traffic for internet over NAT GW.

- **N-S Firewall Monitoring:**

- Concentrates on supervising traffic utilizing the IGW (Internet Gateway).
- It provides granular visibility and enables better detection of internal and external attacks.

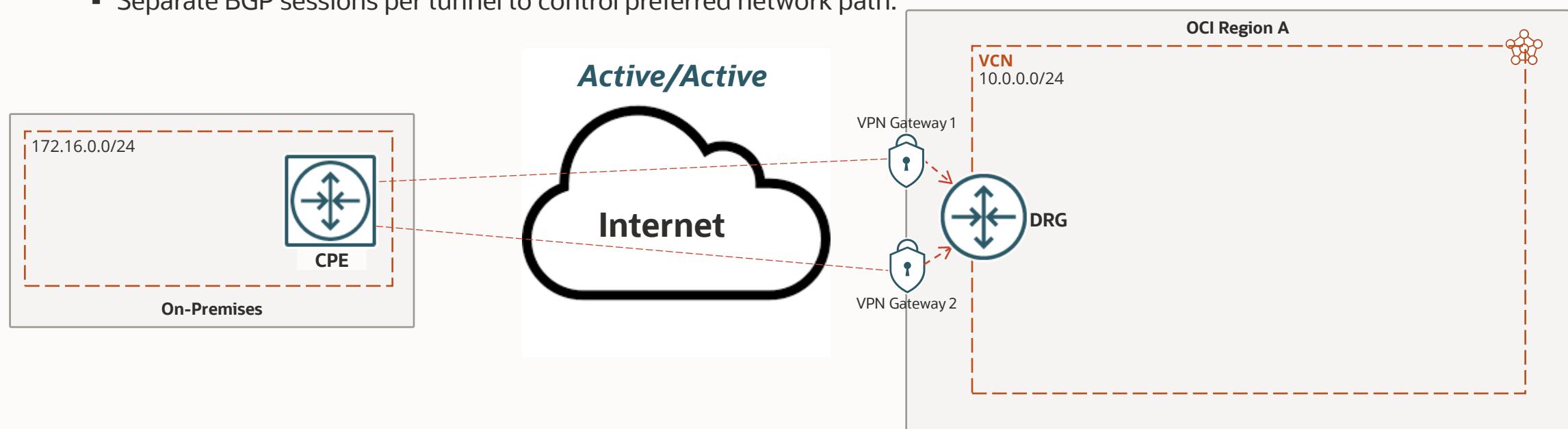


Case Study 2: Redundant Connectivity

To avoid single point of failure, there are many options to design a highly available network, depending on the cost, and how critical your workload is:

Scenario A: Site-to-Site IPSec VPN Redundancy (Single CPE)

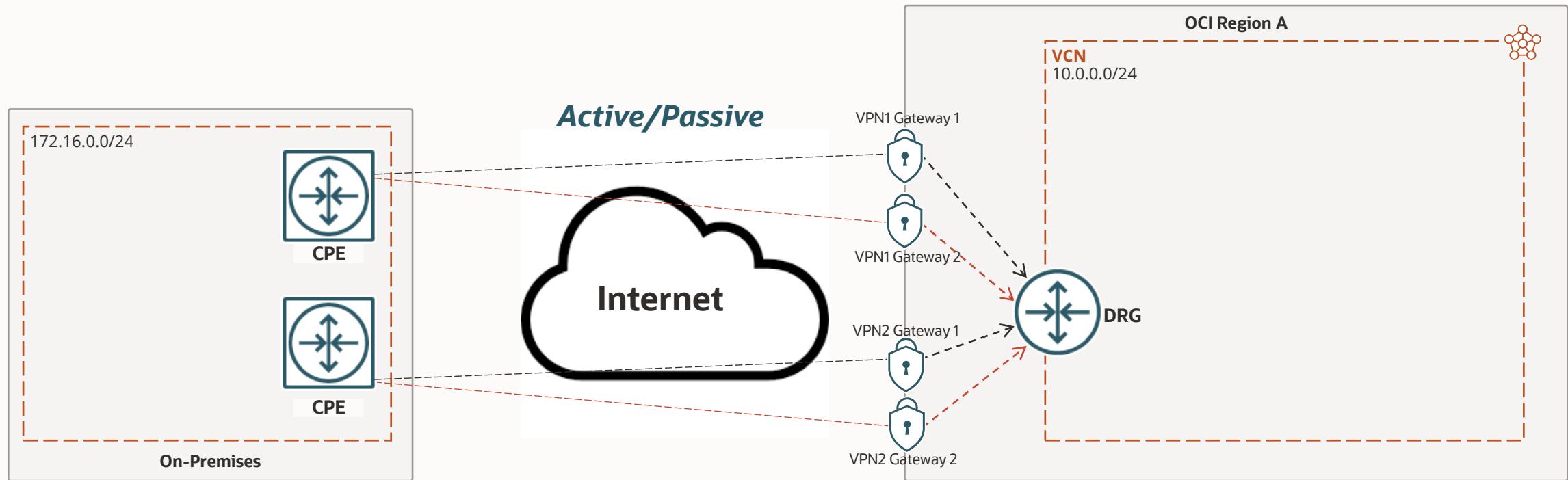
- Two redundant tunnels per IPsec connection.
- Each tunnel in an IPsec Connection terminates on a different VPN Gateway.
- Multiple IPsec Connections is more than two tunnels are required.
- Separate BGP sessions per tunnel to control preferred network path.



Case Study 2: Redundant Connectivity

Scenario B: Site-to-Site IPSec VPN Redundancy (Multiple CPEs)

- One active tunnel per IPSec connection.
- Each tunnel in one IPSec connection.
- Two different CPEs On-premises.

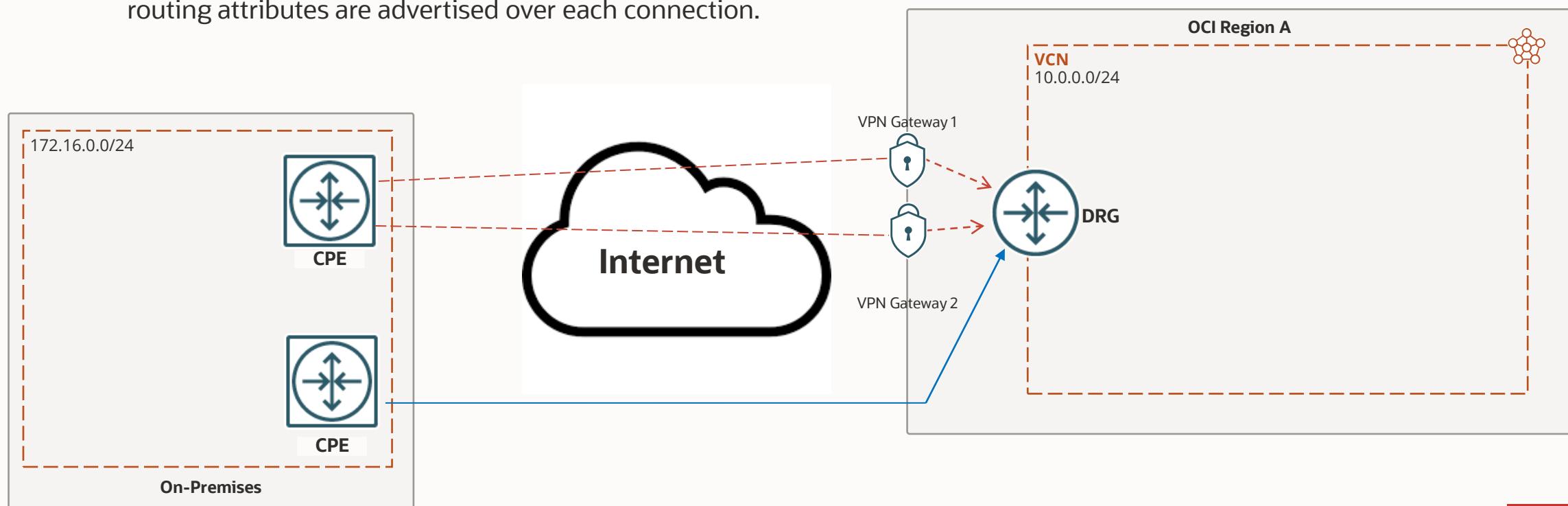


Case Study 2: Redundant Connectivity

Scenario C: FastConnect with Site-to-Site IPSec VPN Backup

- Configure at least one available tunnel.
- Use ECMP across multiple tunnels for additional VPN bandwidth.
- Prefer FastConnect as primary.
- Use BGP for route exchange.
- FastConnect is preferred over VPN when the same route and routing attributes are advertised over each connection.

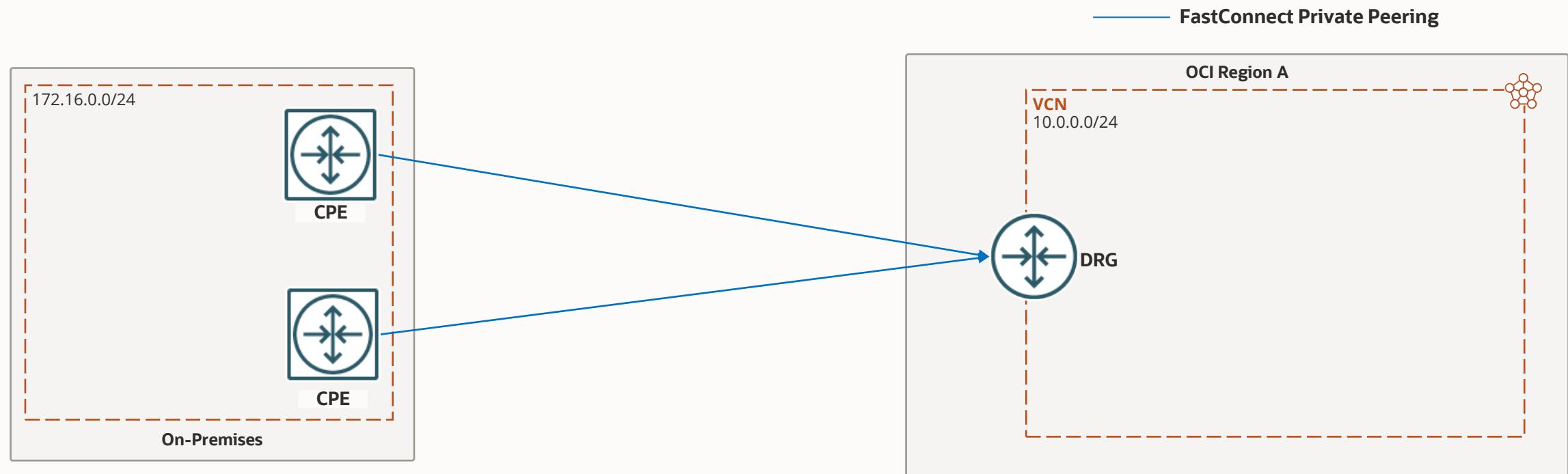
- Site-to-Site IPSec VPN Tunnel
— FastConnect Private Peering



Case Study 2: Redundant Connectivity

Scenario D: Redundant FastConnects

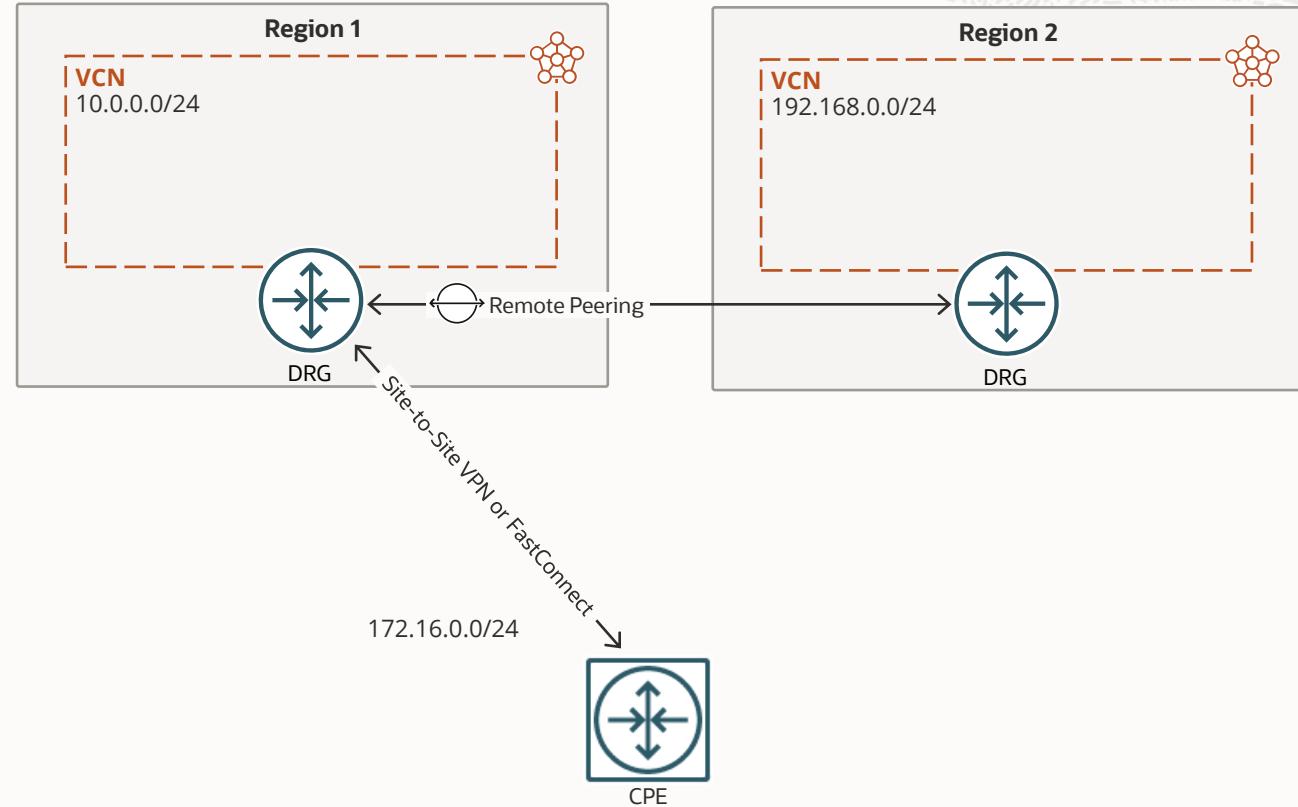
- Primary and Secondary Cross-Connect



Case Study 3: Multi-Region Communication

Scenario A: Remote On-ramp/Transit Routing

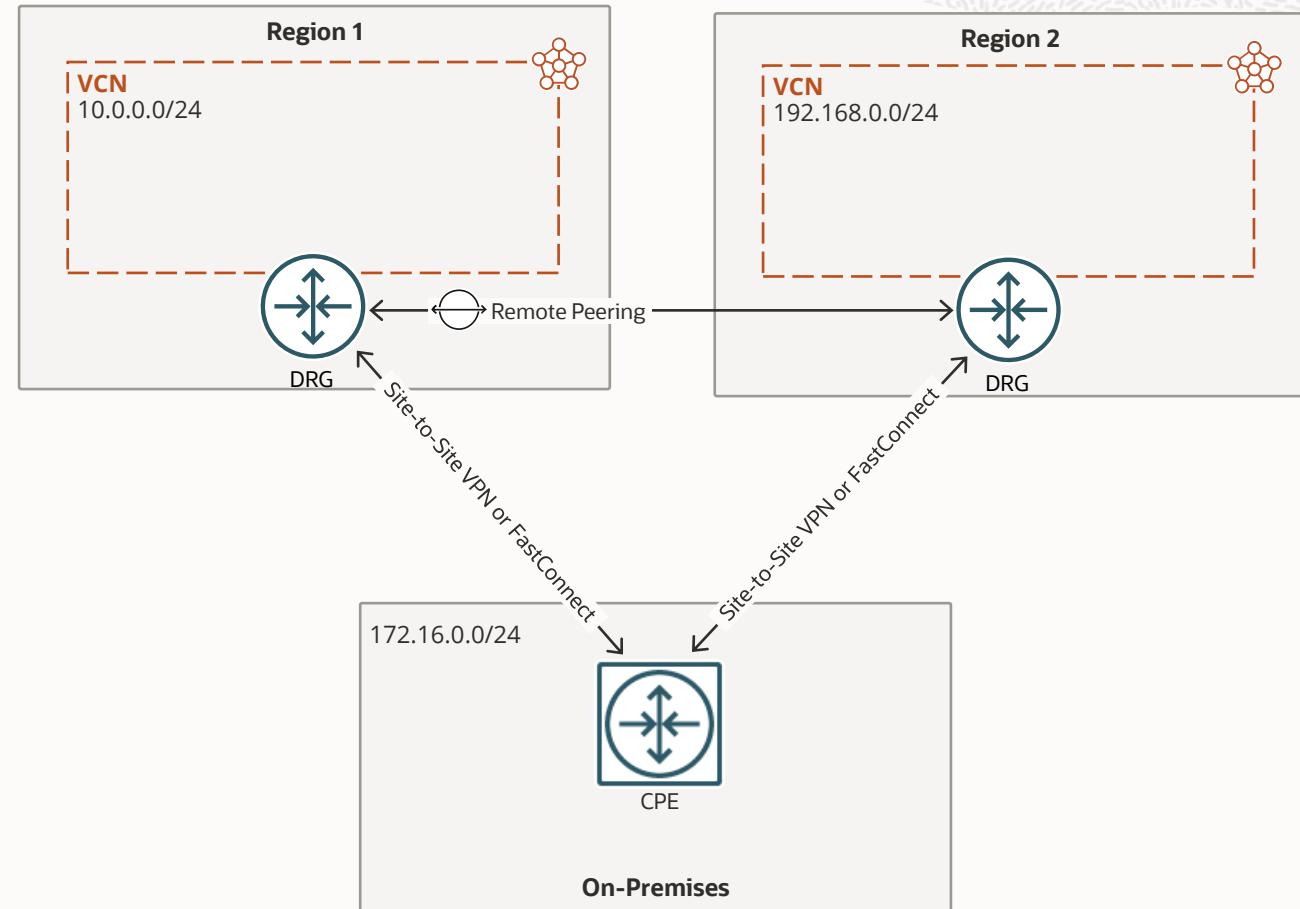
- FastConnect or Site-to-Site IPsec VPN to Region A.
- Access resources in Region A and Region B.
- Uses the OCI private Backbone.
- Transit Routing can use similar configuration.
- Can also provide redundancy.



Case Study 3: Multi-Region Communication

Scenario B: Multiple Region Redundancy

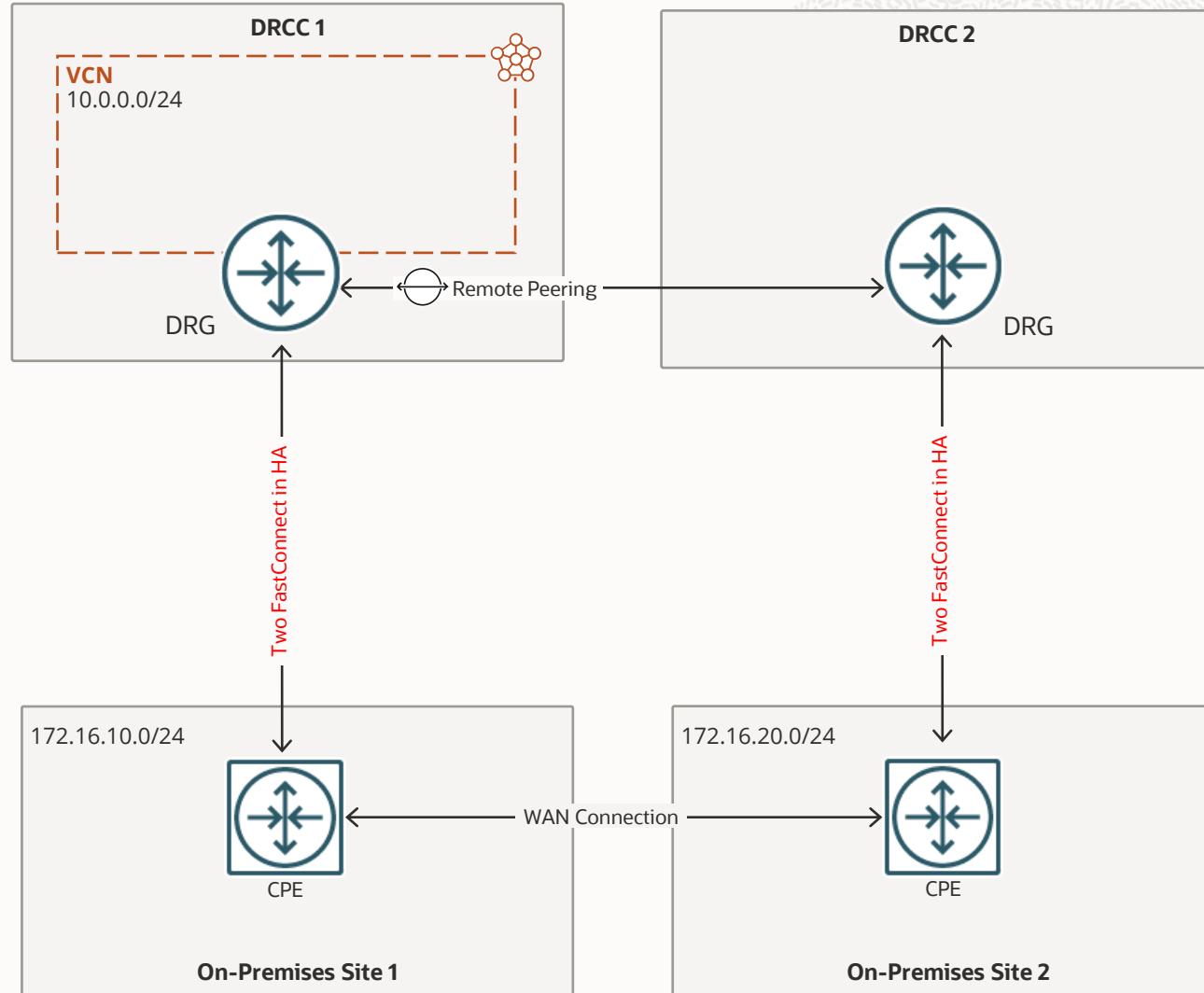
- FastConnect or Site-to-Site IPsec VPN to both regions.
- Uses the OCI private backbone.
- Use BGP attributes like local preference and AS PATH prepending to influence egress/ingress routing.
- Oracle will prefer local region egress in case of routing tiebreaks.



Case Study 3: Multi-Region Communication

Scenario C: Multiple Region with Multiple CPEs Redundancy

- Two FastConnect in HA to both regions.
- Uses the OCI private backbone in HA.
- Use BGP attributes like local preference and AS PATH prepending to influence egress/ingress routing.
- Configure DRG routing to advertised routes for RPC to On-premises Sites.



Case Study 4: DRCC

We assist customers in adopting DRCC for running their applications, which involves designing network architecture and collaborating with the DC team to establish various connections such as Fast Connect, inter-region connectivity, and internet connectivity.

DRCC Physical Network components

Inter-Region Routers.

- Private and public peering between OCI regions over Oracle backbone.
- Oracle managed Layer-2 connections with MACsec.

Fast Connect Routers.

- Private and public peering between customer premises and OCI region.
- MACsec option for customer managed Layer-2 connections.
- IPsec VPN option inside partner managed Layer-3 connections.

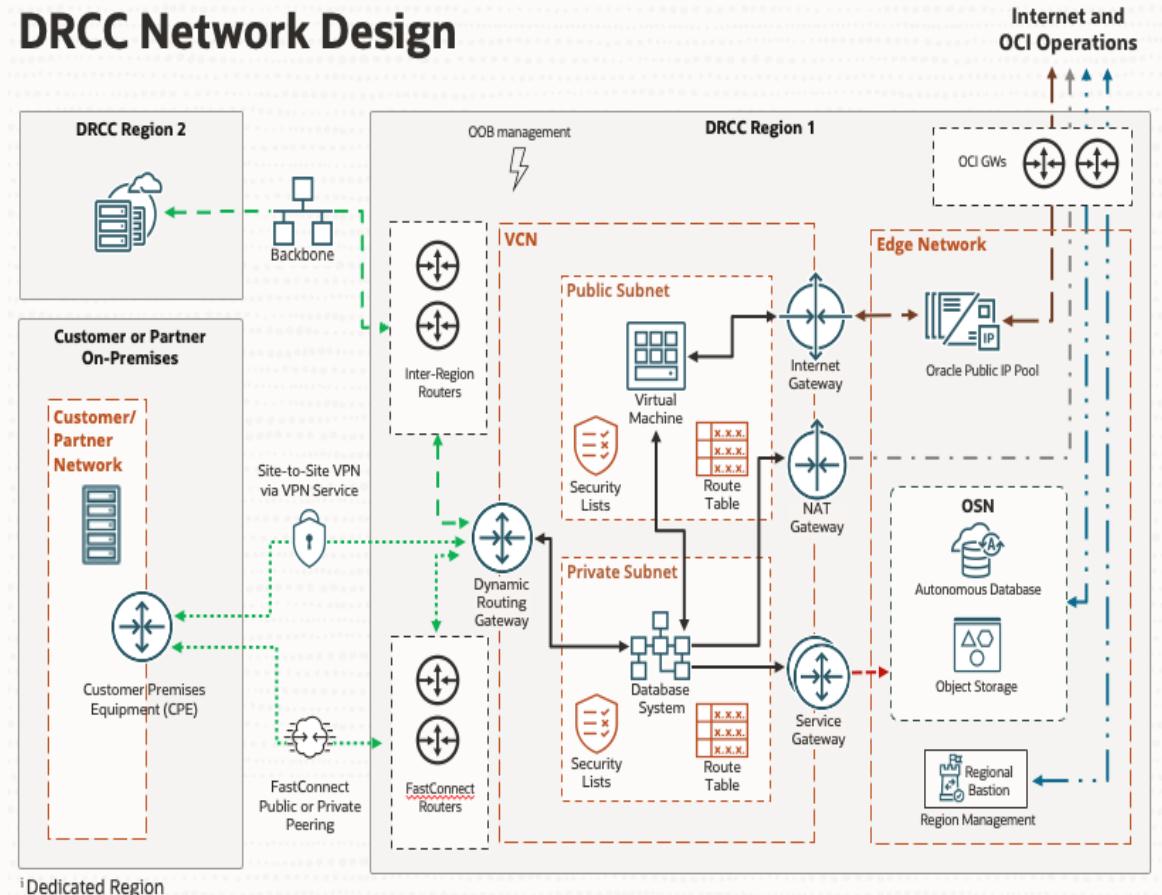
OCI Gateways (OCI GW).

- Direct peering between region ASN and diverse Internet providers.
- Always on DDoS.

Edge Network.

- Internet access to customer workloads via region public IPs mapped to tenant public subnets.
- Access to Oracle Service Network (OSN) endpoints.
- OCI operator access to regional bastions.

DRCC Network Design



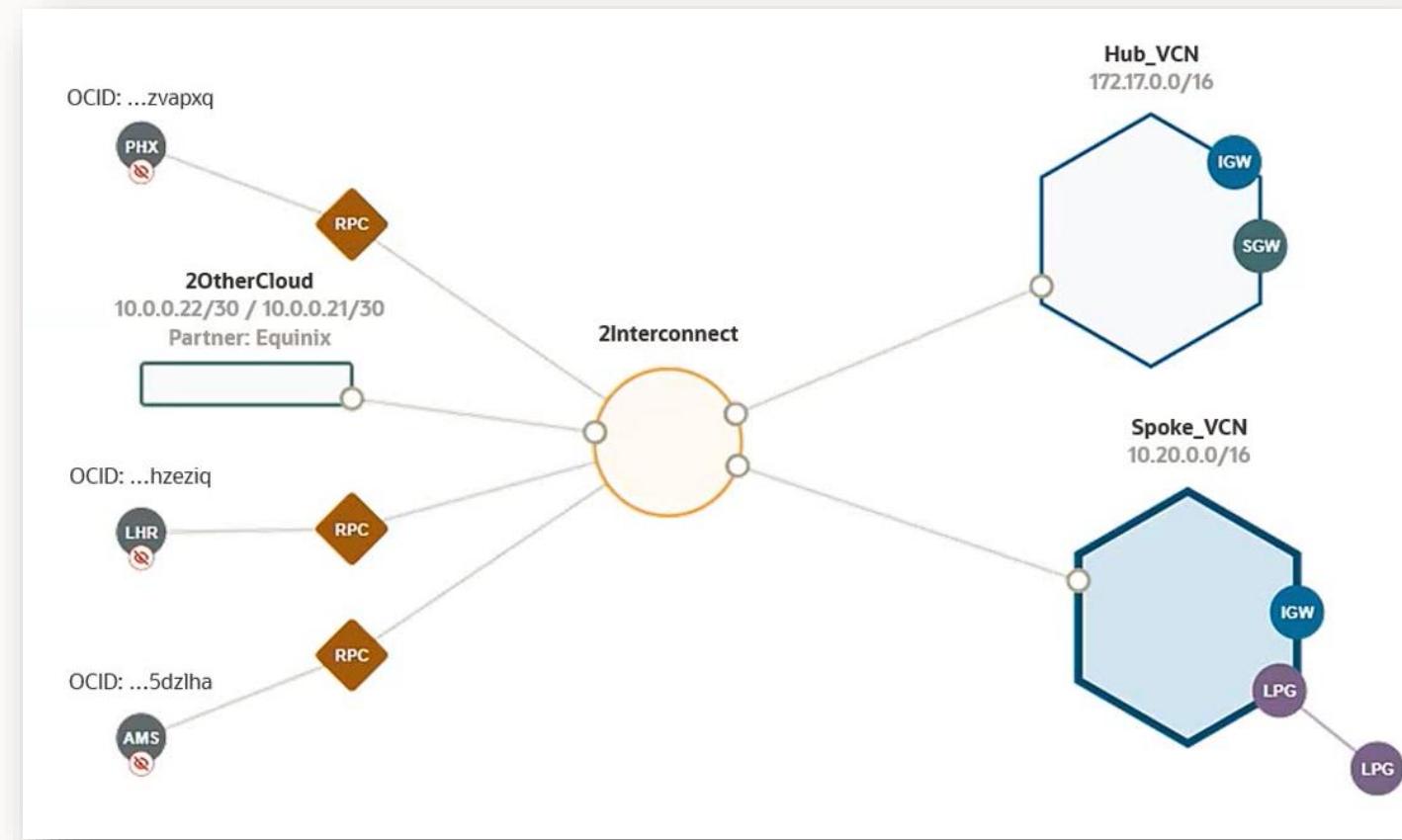
Tools to Troubleshoot Network Issues

Chapter Agenda

- 1 Network Visualizer
- 2 Network Path Analyzer (NPA)
- 3 Inter-Region Latency Dashboard
- 4 VCN Flow Logs

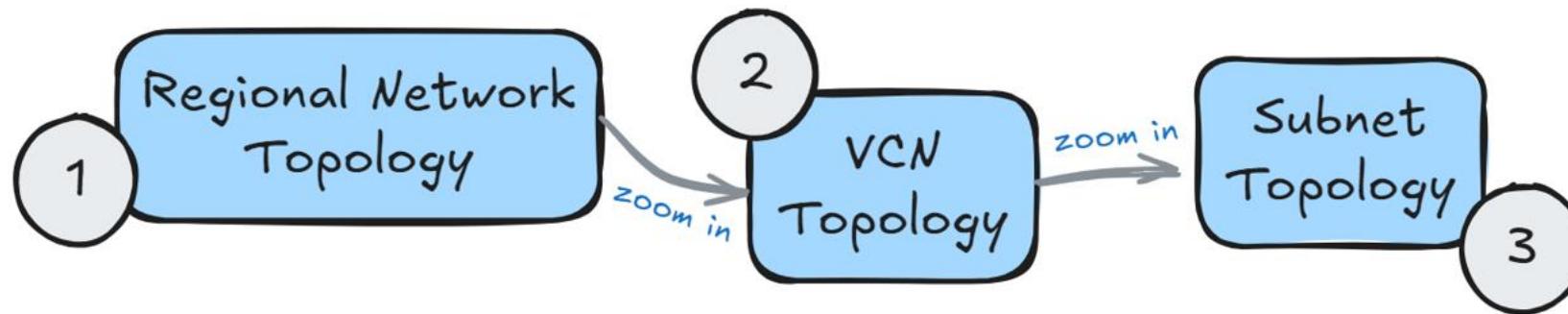
Network Visualizer

- A service that provides a diagram of the implemented topology of all VCNs in a selected region and tenancy.
- Each resource is represented with a notation.



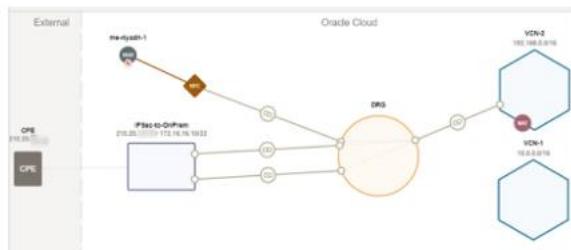
OCI Network Visualizer

Provides the following levels of granularity



A high-level layout and routing topology of the entire virtual network configuration within a region.

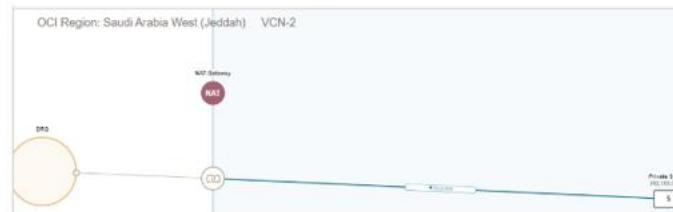
This topology includes DRGs, VCNs, CPEs, and various types of gateway.



Shows the organization of a single VCN including its subnets and routing configuration.

This topology includes subnets, VLANs, and gateways to other resources.

> VCN Routing Map



> VCN Security Map



Shows the resource information about instances, load balancers, FSS, and OKE clusters in the subnet.

> Subnet Inventory Map

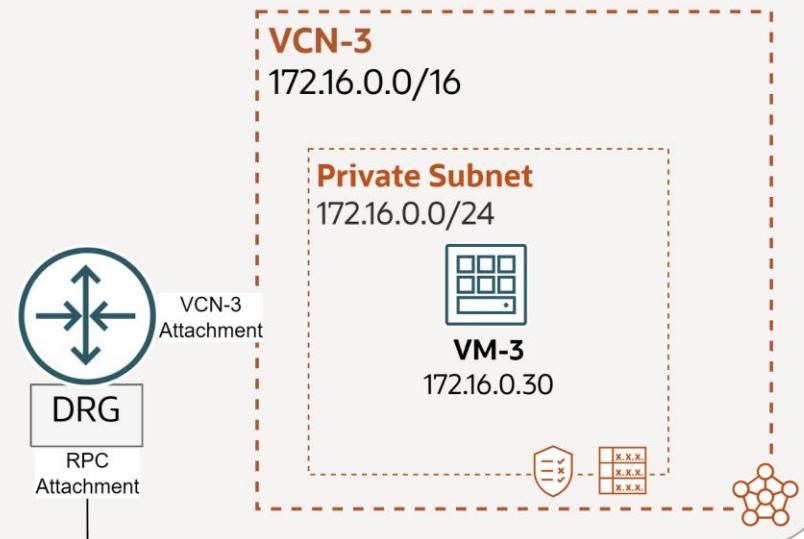


> Subnet Security Map

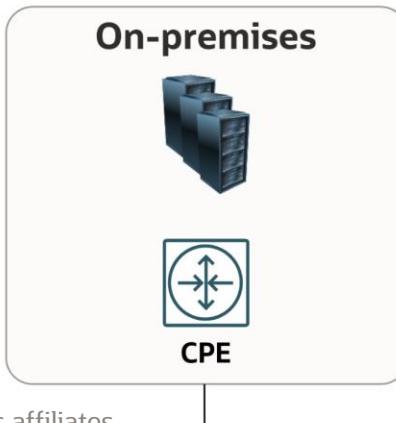
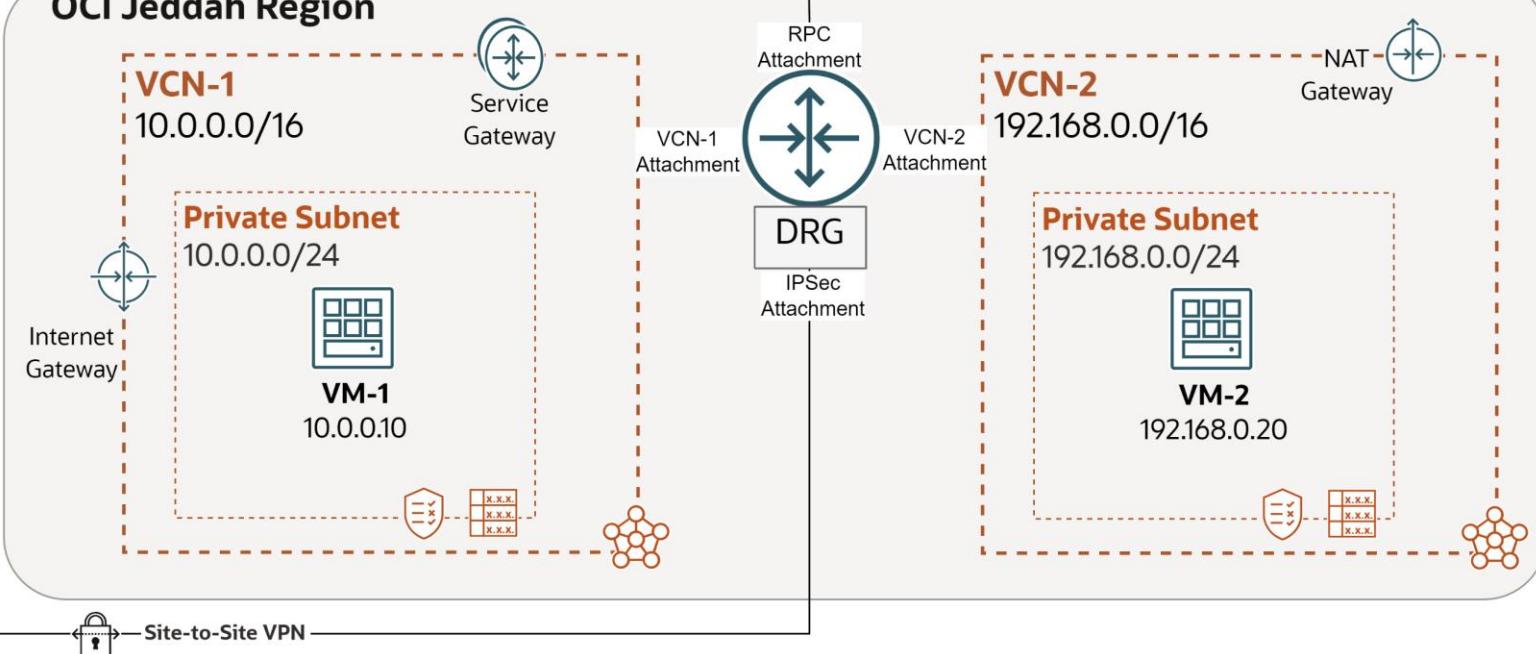


Network Visualizer Example

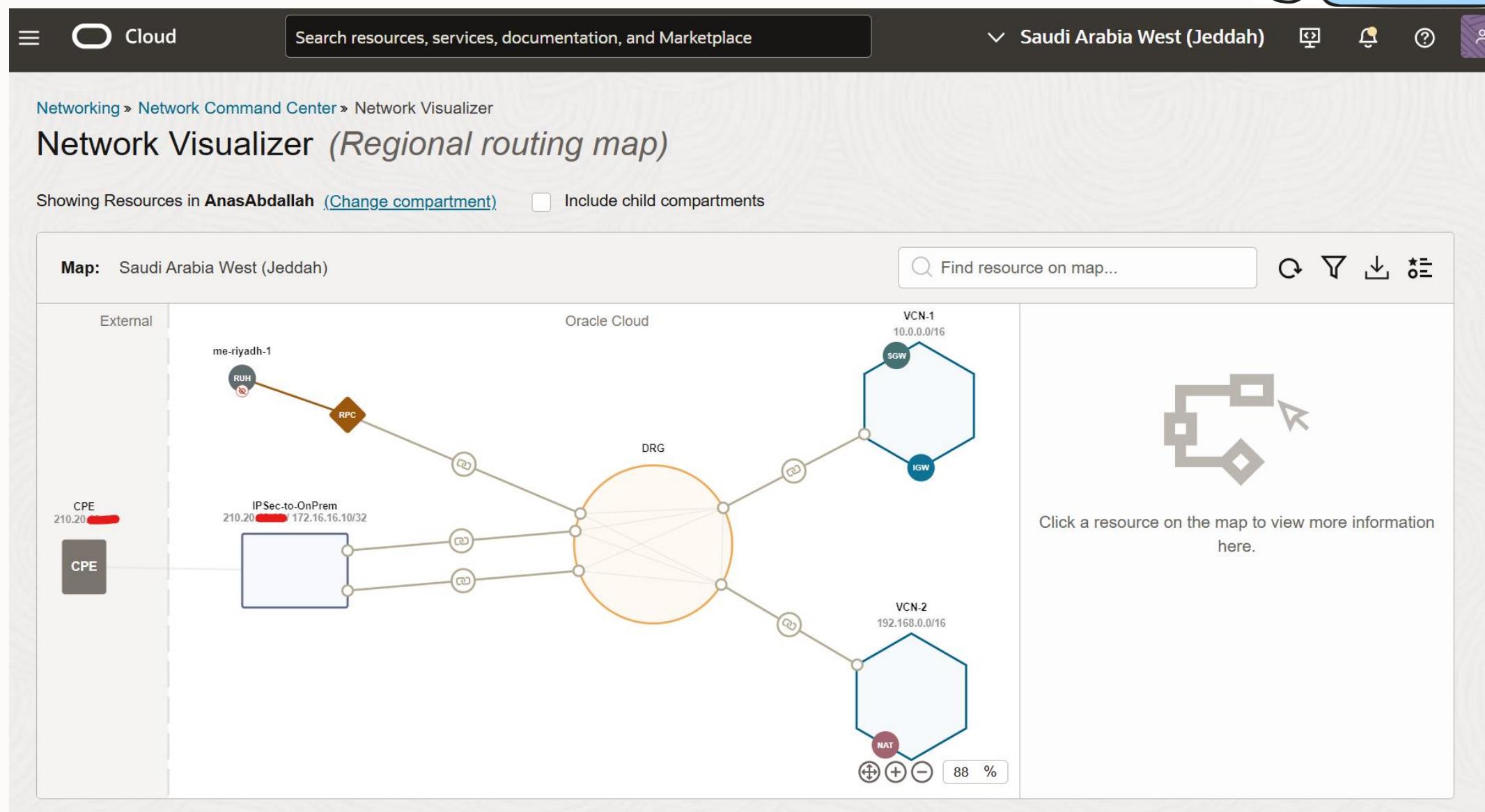
OCI Riyadh Region



OCI Jeddah Region



Network Visualizer Example



Network Visualizer Example

Cloud Saudi Arabia West (Jeddah)

Networking » Network Command Center » Network Visualizer

Network Visualizer (Regional routing map)

Showing Resources in AnasAbdallah ([Change compartment](#)) Include child compartments

Map: Saudi Arabia West (Jeddah)

The diagram illustrates a network topology across three main regions: External, Oracle Cloud, and Virtual Cloud Networks (VCNs). In the External region, there is a CPE (210.20.0.0/16) connected to a RUH device (me-riyadh-1) via an RPC connection. This connection is labeled 'IPSec-to-OnPrem' with the IP range 210.20.0.0/16 to 172.16.16.10/32. In the Oracle Cloud region, there is a DRG (Autogenerated Drg Route Table for Table: VCN attachments) represented by a central orange circle. It connects to a VCN-1 attachment (SGW, 10.0.0.0/16) and a VCN-2 attachment (NAT, 192.168.0.0/16). A red arrow labeled '1' points from the DRG to the VCN-1 attachment. Another red arrow labeled '2' points from the DRG to the VCN-2 attachment. The VCN-1 attachment is connected to an IGW (10.0.0.0/16). The VCN-2 attachment is connected to a NAT device.

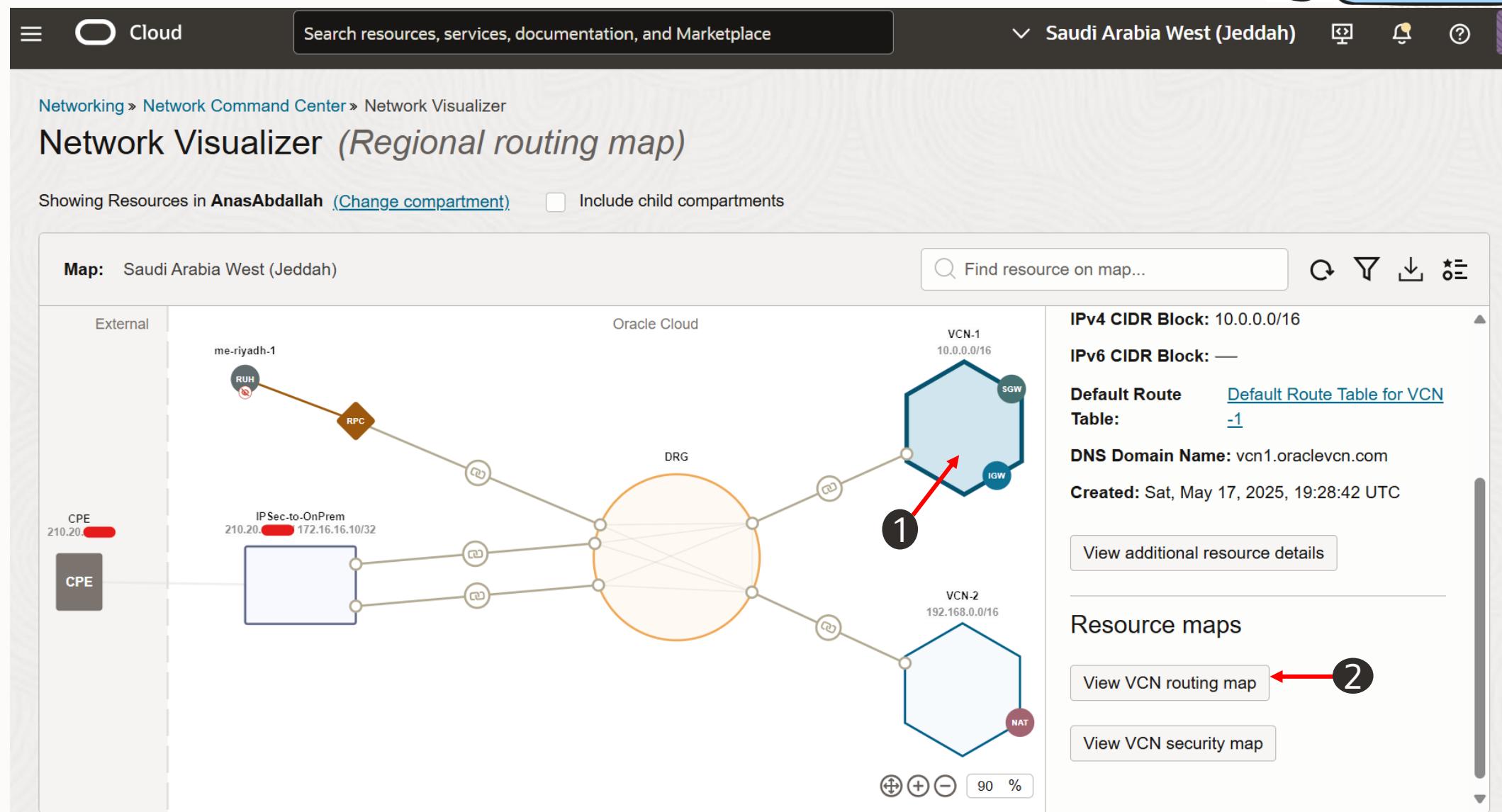
Resource summary

- OCID: ...qy27ia [Show](#) [Copy](#)
- Name: [VCN-1 Attachment](#)
- Compartment: [AnasAbdallah](#)
- DRG: [DRG](#)
- DRG Route Table: [Autogenerated Drg Route Table for Table: VCN attachments](#)
- ECMP: Disabled
- Virtual Cloud Network: [VCN-1](#)
- Created: Fri, May 23, 2025, 15:07:28 UTC

Connection Information

Persist routing information

Network Visualizer Example



Network Visualizer Example

Cloud Search resources, services, documentation, and Marketplace

Saudi Arabia West (Jeddah) 2 VCN Topology

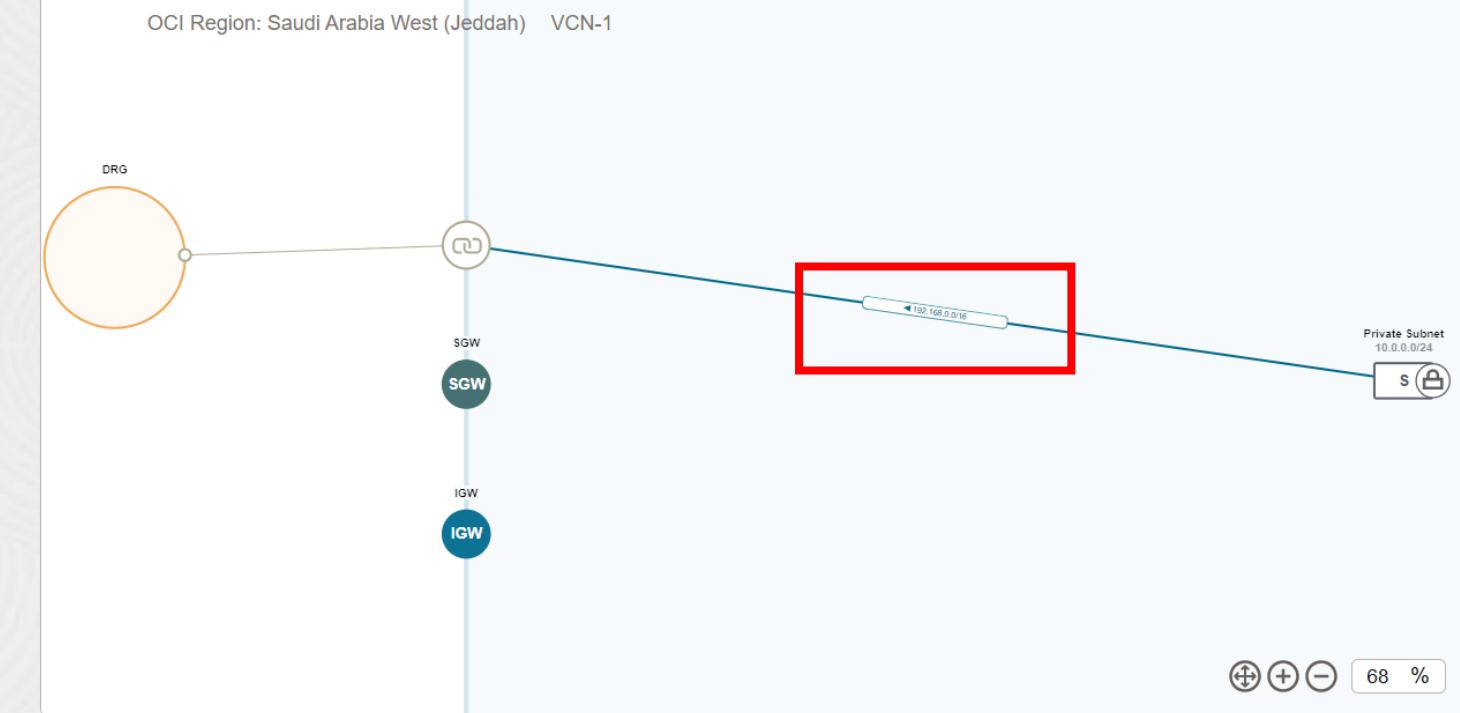
Networking » Network Command Center » Network Visualizer

Network Visualizer (Virtual cloud network routing map)

Showing Resources in AnasAbdallah ([Change compartment](#)) Include child compartments Map Mode: Routing Security

Map: Saudi Arabia West (Jeddah) » VCN-1 Find resource on map...    

OCI Region: Saudi Arabia West (Jeddah) VCN-1



The diagram illustrates the network topology within VCN-1. A DRG (represented by an orange circle) is connected to an SGW (green circle) and an IGW (blue circle). The SGW and IGW are connected to a Private Subnet (represented by a red-bordered rectangle). The subnet has an IP range of 192.168.0.0/16 and a CIDR block of 10.0.0.0/24. A small icon indicates it is a Private Subnet.

Resource summary

OCID: ...m3q7ir6pjq [Show](#) [Copy](#)
Name: [Private Subnet](#)
Compartment: [AnasAbdallah](#)
State: Available
Subnet Type: Regional
Subnet Access: Private Subnet
IPv4 CIDR Block: 10.0.0.0/24
Default Route Table: [Default Route Table for VCN](#)
Table: -1
Created: Sat, May 17, 2025, 19:30:38 UTC

Resource maps

Network Visualizer Example

Cloud

Saudi Arabia West (Jeddah)

Networking » Network Command Center » Network Visualizer

Network Visualizer (*Virtual cloud network security map*)

Showing Resources in AnasAbdallah ([Change compartment](#)) Include child compartments Map Mode: Routing Security

Map: Saudi Arabia West (Jeddah) » VCN-1 Find resource on map...

Region: Saudi Arabia West (Jeddah) VCN-1

Subnet Access: Private Subnet
IPv4 CIDR Block: 10.0.0.0/24
Default Route Table: [Default Route Table for VCN-1](#)
Created: Sat, May 17, 2025, 19:30:38 UTC

[View resource security details](#)

Resource maps

[View subnet inventory map](#)

[View subnet security map](#)

[Create Path Analysis](#)

Network Visualizer Example

Cloud Search resources, services, documentation, and Marketplace

Saudi Arabia West (Jeddah) 3 Subnet Topology

Networking » Network Command Center » Network Visualizer

Network Visualizer (Subnet inventory map)

Showing Resources in AnasAbdallah ([Change compartment](#)) Include child compartments Map Mode: Inventory Security

Map: Saudi Arabia West (Jeddah) » VCN-1 » Private Subnet Find resource on map...    

Private Subnet

VM-1

Resource summary

OCID: ...ntnc6q [Show](#) [Copy](#)

Name: [VM-1](#)

Compartment: [AnasAbdallah](#)

State: Unknown

Public IP: —

Private IP: 10.0.0.10

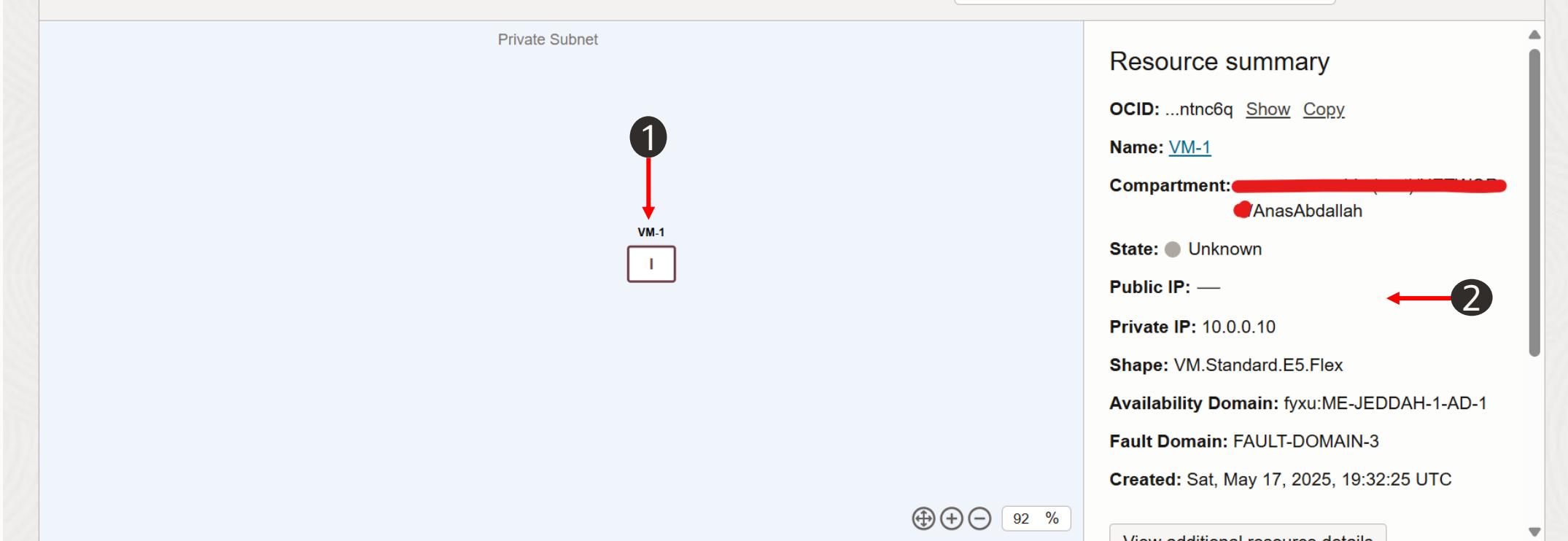
Shape: VM.Standard.E5.Flex

Availability Domain: fyxu:ME-JEDDAH-1-AD-1

Fault Domain: FAULT-DOMAIN-3

Created: Sat, May 17, 2025, 19:32:25 UTC

View additional resource details



Network Visualizer Example

Cloud Saudi Arabia West (Jeddah)

3 Subnet Topology

Networking > Network Command Center > Network Visualizer

Network Visualizer (Subnet security map)

Showing Resources in AnasAbdallah ([Change compartment](#)) Include child compartments Map Mode: Inventory Security

Map: Saudi Arabia West (Jeddah) » VCN-1 » Private Subnet

Private Subnet

Security Lists
Default Security List for VCN-1
SL

VM-1

Network Security Groups

Public IP: —
Private IP: 10.0.0.10
Shape: VM.Standard.E5.Flex
Availability Domain: fyxu:ME-JEDDAH-1-AD-1
Fault Domain: FAULT-DOMAIN-3
Created: Sat, May 17, 2025, 19:32:25 UTC

[View additional resource details](#)

Network Path Analyzer Overview

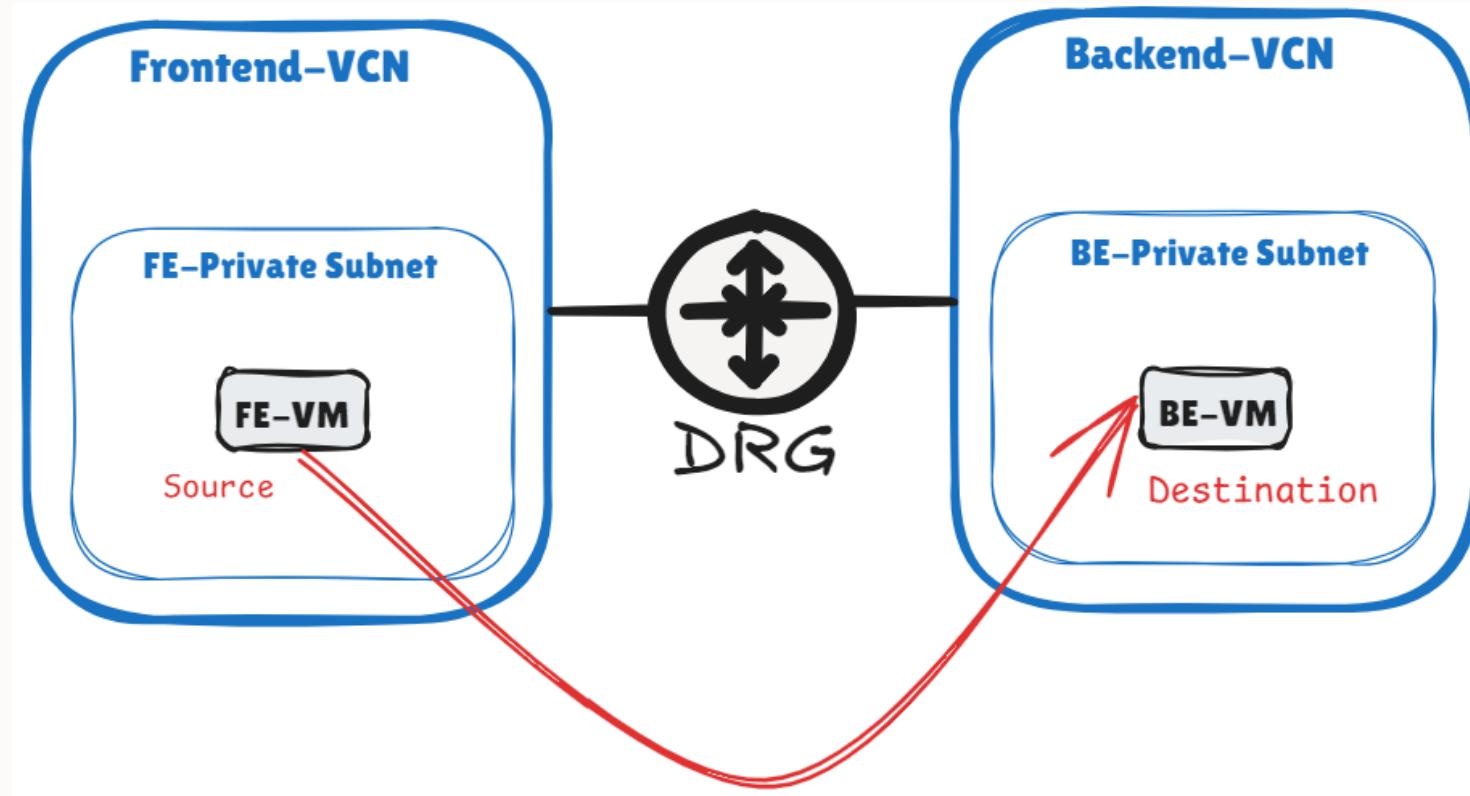
- **Network Path Analyzer (NPA)** is your virtual network detective, designed to inspect your network routing and security configuration in real-time. It collects and analyzes them to determine how the paths between the source and the destination will **function** or **fail**.
- No actual traffic is sent, instead, the configuration is examined and used to confirm reachability.
- **Supported scenarios:** OCI  OCI OCI  On-premises OCI  Internet
- **Customer Benefits:**
 1. Assist in troubleshooting of routing and security misconfigurations.
 2. On-demand validation of the logical network paths.
 3. Verify virtual network connectivity setup before starting to send traffic.

Network Path Analyzer Overview

- Using NPA, you can:
 - Troubleshoot *routing and security misconfiguration* that are causing connectivity issues.
 - Validate that the logical network paths match your intent.
 - Verify that the virtual network connectivity setup works as expected before starting to send traffic.
- To achieve any of these objectives, create a test that you think should work and then run the test. You can also save this test definition to run it again later. Saved tests are displayed in the Network Path Analyzer page for you to select.

EXAMPLES

Example Architecture



Create path analysis

1 Configure analysis 2 Run analysis

Protocol *i*

1 ICMP

Source 2

Enter IP address
Enter an IP address for a resource when known

Find OCI resource
Select a load balancer, network load balancer, or other resource

Source type

Select a source type

Subnet IP address

VLAN IP address

Compute instance (VNIC)

VNIC OCID

Load balancer

Network load balancer

Destination 3

Enter IP address
Enter an IP address for a resource when known

Find OCI resource
Select a resource

Destination IPv4 address

This IP address is an on-premises endpoint
Select if the IP address you entered is for an on-premises endpoint.

Destination port *i*

4 Direction

Bi-directional
Analyze both the forward and reverse paths

Uni-directional
Analyze only the forward path

Show tagging options

Run analysis Save as stack Cancel

Network Path Analyzer – Example 1

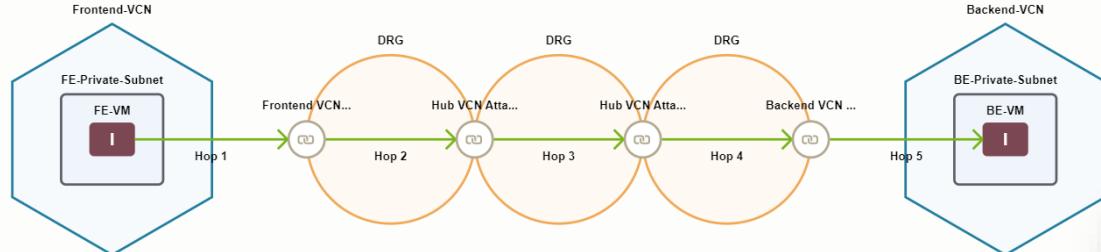


FE-VM can ping BE-VM successfully

Forward path

Status: ● Reachable Successful hops: 5

Analysis performed: Sun, Nov 17, 2024, 18:42:14 UTC



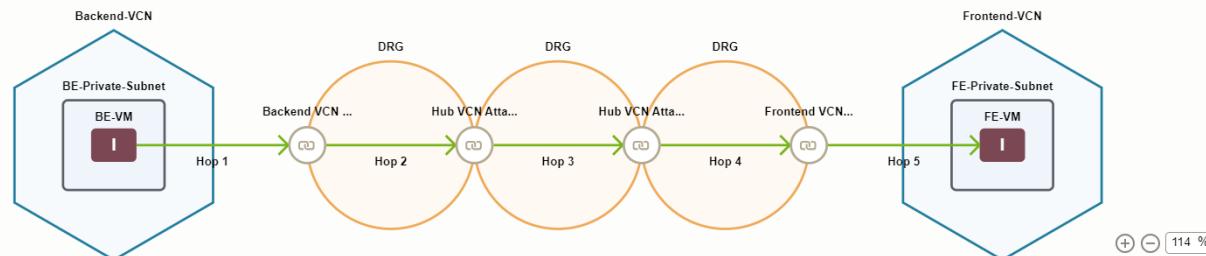
View diagram information

Path hop	From	To	Routing status	Security status	Traffic
Hop 1	FE-VM	Frontend VCN Attachment	● Forwarded	● Allowed	ICMP: code:0 type: 8
Hop 2	Frontend VCN Attachment	Hub VCN Attachment	● Forwarded	● Allowed	ICMP: code:0 type: 8
Hop 3	Hub VCN Attachment	Hub VCN Attachment	● Forwarded	● Allowed	ICMP: code:0 type: 8
Hop 4	Hub VCN Attachment	Backend VCN Attachment	● Forwarded	● Allowed	ICMP: code:0 type: 8
Hop 5	Backend VCN Attachment	BE-VM	● Forwarded	● Allowed	ICMP: code:0 type: 8

Return path

Status: ● Reachable Successful hops: 5

Analysis performed: Sun, Nov 17, 2024, 18:42:14 UTC



View diagram information

Path hop	From	To	Routing status	Security status	Traffic
Hop 1	BE-VM	Backend VCN Attachment	● Forwarded	● Allowed	ICMP: code:0 type: 8
Hop 2	Backend VCN Attachment	Hub VCN Attachment	● Forwarded	● Allowed	ICMP: code:0 type: 8
Hop 3	Hub VCN Attachment	Hub VCN Attachment	● Forwarded	● Allowed	ICMP: code:0 type: 8
Hop 4	Hub VCN Attachment	Frontend VCN Attachment	● Forwarded	● Allowed	ICMP: code:0 type: 8
Hop 5	Frontend VCN Attachment	FE-VM	● Forwarded	● Allowed	ICMP: code:0 type: 8

Showing 5 items

Network Path Analyzer – Example 2

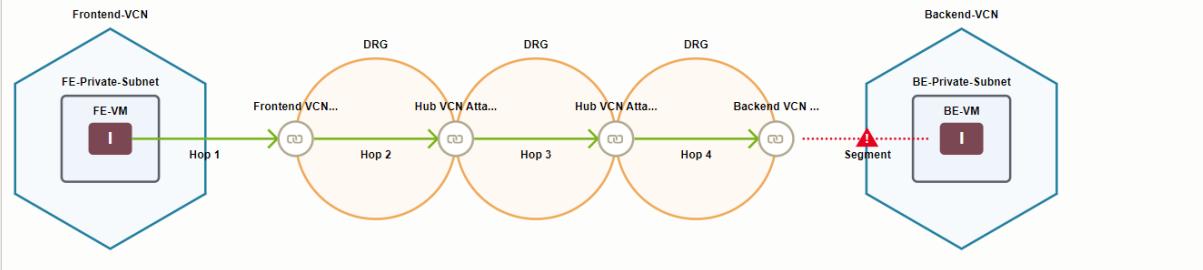


FE-VM cannot ping BE-VM due to a **missing security rule** at the destination.

Forward path

Status: ● Unreachable Successful hops: 4

Analysis performed: Sun, Nov 17, 2024, 19:04:10 UTC



[View diagram information](#)

Path hop	From	To	Routing status	Security status	Traffic
Hop 1	FE-VM	Frontend VCN Attachment	● Forwarded	● Allowed	ICMP: code:0 type: 8
Hop 2	Frontend VCN Attachment	Hub VCN Attachment	● Forwarded	● Allowed	ICMP: code:0 type: 8
Hop 3	Hub VCN Attachment	Hub VCN Attachment	● Forwarded	● Allowed	ICMP: code:0 type: 8
Hop 4	Hub VCN Attachment	Backend VCN Attachment	● Forwarded	● Allowed	ICMP: code:0 type: 8
Segment	Backend VCN Attachment	BE-VM	● Forwarded	● Denied	ICMP: code:0 type: 8

Showing 5 items

Return path

! We didn't analyze a return path.

Path hop	From	To	Routing status	Security status	Traffic
Segment	Backend VCN Attachment	BE-VM	● Forwarded	● Denied	ICMP: code:0 type: 8

Path hop details:

- Segment:** Backend VCN Attachment → BE-VM
- Routing status:** ● Forwarded
- Security status:** ● Denied
- Traffic:** ICMP: code:0 type: 8

Routing forwarded: Routing status: ● Forwarded. Routing action: Forwarded based on implicit routing.

Security denied: Egress access control status: ● Allowed. Egress access control action: Allowed based on implicit rules. Ingress access control status: ● Denied. Ingress access control action: We couldn't find a matching security rule for the traffic in the following security resources:

- [Default Security List for Backend-VCN](#)

Segment from: DRG attachment: [Backend VCN Attachment](#)
Segment to: VNIC: ...j3wcumgviq [Show](#) [Copy](#)
DRG: [DRG](#)
Instance: [BE-VM](#)
VCN: [Backend-VCN](#)
Subnet: [BE-Private-Subnet](#)

Network Path Analyzer – Example 3

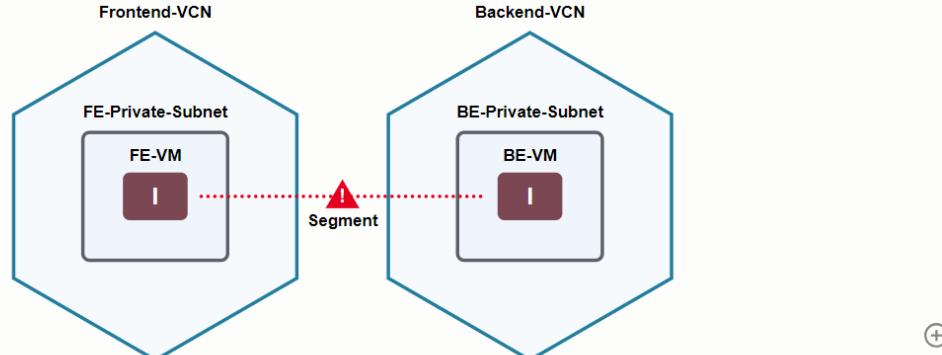


FE-VM cannot ping BE-VM due to a **missing route rule** at the source.

Forward path

Status: ● Unreachable Successful hops: 0

Analysis performed: Sun, Nov 17, 2024, 19:19:47 UTC



^ View diagram information

Path hop	From	To	Routing status	Security status	Traffic
Segment	FE-VM	BE-VM	● No route	● Allowed	ICMP: code:0 type: 8

Showing 1 item

Return path

! We didn't analyze a return path.

Path hop	From	To	Routing status	Security status	Traffic
Segment	FE-VM	BE-VM	● No route	● Allowed	ICMP: code:0 type: 8

!	No route Routing status: ● No route Routing action: We couldn't find a matching routing rule for this destination in the following route table: Default Route Table for Frontend-VCN
✓	Security allowed Egress access control status: ● Allowed Egress access control action: Allowed based on rule: [all protocols to 0.0.0.0 : any port] found in the following security list: Default Security List for Frontend-VCN Ingress access control status: ● Not applicable Ingress access control action: Security information is not applicable

Segment from	Segment to
VNIC: ...rp5unb32jq	VNIC: ...j3wcumgviq
Show	Show
Copy	Copy
Instance: FE-VM	Instance: BE-VM
VCN: Frontend-VCN	VCN: Backend-VCN
Subnet: FE-Private-Subnet	Subnet: BE-Private-Subnet

Inter-Region Latency Dashboard

- A tool that provides insights into the average network round-trip latency (RTT) between all OCI regions in a given realm. This dashboard is designed to help users plan scenarios such as data replication, backup, or disaster recovery by offering visibility into latency metrics between regional pairs.
- OCI users can verify latency value between two any OCI public regions from one single dashboard”.
- Mostly used for troubleshooting and testing purposes.

Inter-Region Latency Dashboard – Use Cases

Network Planning

Regional selection requires the balance of requirements in DR, compliance, data residency, and performance. Performance can be relative; lower latency is always better, or it can be driven by an absolute application requirement for latency below a certain value.

Troubleshooting

You can now validate network performance, both actively and historically, utilizing the inter-region latency dashboard. When a problem is not currently occurring, you can use historical data to validate network performance.

Monitoring & Alarming

With latency information available through the monitoring API, you can also integrate latency metrics into your on-premises monitoring platform. You can also utilize the OCI Metrics alarming service to actively notify you by e-mail or SMS when defined latency thresholds are exceeded.

Inter-Region Latency Dashboard

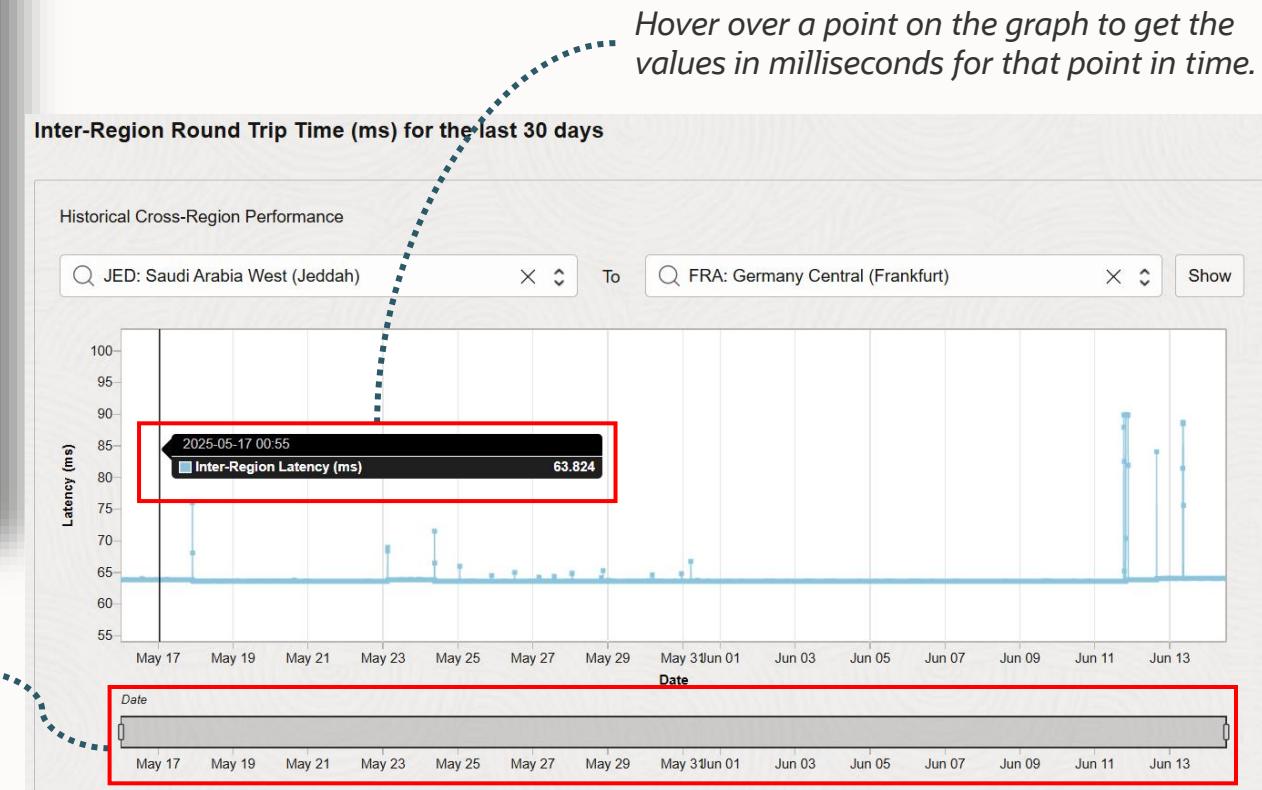
Current Inter-Region Round Trip Time (ms) ⓘ

JED: Saudi Arabia West (Jeddah) X To FRA: Germany Central (Frankfurt) X Show

Last Updated: Sun, Nov 17, 2024, 21:00:00 UTC

Region	AUH	BMC	BOG	BOM	CDG	CWL	DFW	DXB	FRA	GRU	HYD	IAD	ICN	JED	JNB
AGA	204.60	⚠️	139.47	235.22	128.89	122.72	⚠️	207.12	130.91	158.46	218.89	53.62	139.64	182.76	281.54
AMS	92.77	⚠️	168.42	120.26	7.85	8.72	⚠️	95.29	7.87	183.77	134.00	83.81	265.31	70.56	166.28
ARN	108.74	⚠️	193.68	144.06	31.53	32.57	⚠️	116.30	37.11	207.76	157.82	105.97	288.28	91.27	190.29
AUH		⚠️	240.07	31.25	78.89	93.74	⚠️	2.88	85.82	263.10	43.77	154.03	171.59	22.61	251.27
BMC		⚠️	⚠️	⚠️	⚠️	⚠️	⚠️	⚠️	⚠️	⚠️	⚠️	⚠️	⚠️	⚠️	⚠️
BOG				274.64	162.01	165.48	⚠️	242.61	174.52	113.37	287.85	87.10	254.64	217.88	324.91
BOM					113.42	122.83	⚠️	33.92	110.20	297.90	14.39	188.62	151.74	55.05	278.25
CDG						10.40	⚠️	81.42	8.31	185.19	127.12	76.02	263.99	56.68	168.06
CWL							⚠️	96.27	14.22	184.08	136.72	79.38	261.85	71.80	163.04
DFW								⚠️	⚠️	⚠️	⚠️	⚠️	⚠️	⚠️	⚠️
DXB									88.38	266.73	48.62	156.56	170.26	25.13	253.88
FRA										190.71	122.88	87.36	269.99	63.62	173.17
GRU											312.89	115.63	298.10	240.86	340.19

Select two regions (one is the "from" region and one is the "to" region) and then select **Show**.



Using the date bar under the chart, slide the beginning and end of the bar to change the time period covered by the chart.

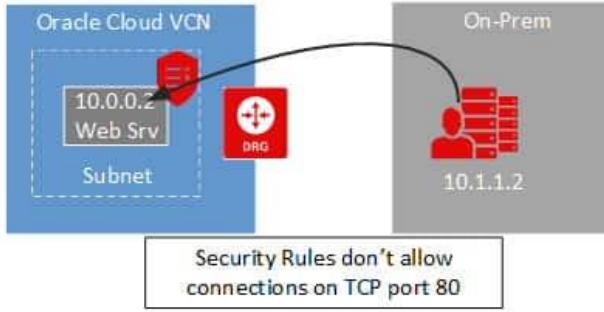
VCN Flow Logs

With **VCN flow logs**, you can record detailed information about network traffic flowing in and out of your VCNs. These logs provide visibility into traffic patterns, helping you monitor network activity, troubleshoot connectivity, and audit network traffic for compliance.

Flow logs capture metadata such as source and destination IPs, ports, and protocols, making it an essential tool for network analysis and security management.

VCN Flow Logs – Use Cases

Troubleshooting & Monitoring



Tue, Sep 1, 2020, 05:03:49 UTC vcn.flowlogs.DataEvent REJECT TCP 10.1.1.2 Port 32040 --> 10.0.0.2 Port 80 Bytes 40 Packets 1

Flow logs show attempts to connect to your resources (Compute Instance or a Database) from other networks (OCI, On-premises, or a Multicloud environment). Logs also show whether security rules allow or deny the traffic. You can use this information to make quick, informed decisions about managing your network resources, such as capacity-planning and network security response.

Regulatory & Compliance

Through the visibility afforded by VCN flow logs and flexible data-retention options provided by the Logging export, you can meet requirements in financial, healthcare, and other regulated industries.

VCN Flow Logs – Example

Accessing a web application through an OCI Load Balancer over HTTPS (port 443) from the internet.

Showing 4 log event(s) for the **past 5 minutes** starting at Mon, Feb 10, 2025, 16:49:11 UTC

Actions ▾

datetime	type	X	data.message	X	
Feb 10, 2025, 16:53:09 UTC	vcn.flowlogs.DataEvent		ACCEPT TCP 192.168.0.19 Port 40412 → 84.8.88.160 Port 443 B...	▼	
Feb 10, 2025, 16:53:09 UTC	vcn.flowlogs.DataEvent		ACCEPT TCP 84.8.88.160 Port 443 → 192.168.0.19 Port 40412 B...	▼	...

"datetime": 1739206389000
⊖ "logContent": {
 "id": "1e36f2e6"
 "time": "2025-02-10T16:53:09Z"
⊖ "oracle": {
 "compartmentid": "ocid1.compartment.oc1..aaaaaaaaacmshv5fz52nhmn4p3juzja3waom4lehfeyeeykxgy3qvetychowq"
 "filterOcid": "DEFAULT_CAPTURE_FILTER"
 "format": "IngestorFormat"
 "ingestedtime": "2025-02-10T16:53:29.417Z"
 "instanceOcid": "ocid1.instance.oc1.me-riyadh-1.anqwuljrldij5aicuzwiaqb5w6gepnv5vh5flzxpp2gabvrkevvhlryp6mq"
 "loggroupid": "ocid1.loggroup.oc1.me-riyadh-1.amaaaaaaldij5aiaw4i5grjbxalmyl672t5oif5oxs2ierua3mwwz7zzjybq"
 "logid": "ocid1.log.oc1.me-riyadh-1.amaaaaaaldij5aianee7sviwouth6diopuzmv2c2tlf4mpc7hhcxcof3l5qq"
 "tenantid": "ocid1.tenancy.oc1..aaaaaaaaab2affulc4dt4tqs7lbojyhqi6hzn5mjllxlnuqnletufsofoyvq"
 "vcnOcid": "ocid1.vcn.oc1.me-riyadh-1.amaaaaaaldij5aiabjk2w7uvsbvelthm2l2r2hcyzvewdydhyd547ufm3q"
 "vniccompartmentocid": "ocid1.compartment.oc1..aaaaaaaaacmshv5fz52nhmn4p3juzja3waom4lehfeyeeykxgy3qvetychowq"
 "vnicocid": "ocid1.vnic.oc1.me-riyadh-1.abqwuljrccrx3hu7o2jaoksam3hp6urb7lq3hhurxdonfk4kjfjelmahv3wq"
 "vnicsubnetocid": "ocid1.subnet.oc1.me-riyadh-1.aaaaaaaaaldov4e5sef2grcmdzvxv4j4mc7fnz6en5c7wdjpckmfjnjuvakxpva"
}

}

 "source": "-"
 "specversion": "1.0"
 "subject": "-"
 "type": "com.oraclecloud.vcn.flowlogs.DataEvent"
⊖ "data": {
 "flowid": "1e36f2e6"
 "version": "2"
 "sourceAddress": "84.8.88.160"
 "destinationAddress": "192.168.0.19"
 "sourcePort": 443
 "destinationPort": 40412
 "bytesOut": 215
 "protocol": 6
 "protocolName": "TCP"
 "packets": 4
 "status": "OK"
 "startTime": 1739206389
 "endTime": 1739206389
 "action": "ACCEPT"
}
}
"regionId": "me-riyadh-1"
}

VCN Flow Logs – Example

Custom filters

Enter search filters

Filters

`data.destinationAddress='192.168.0.5' ×` `data.action='REJECT' ×`

Filter by time

Past 5 minutes ▾

- Past 5 minutes
- Past 15 minutes
- Past hour
- Past 3 hours
- Today
- Custom



Thank you

ORACLE