TechKnowledge
Enablement
& DEVs

OCI Networking Professional 2024

1Z0-1124-24 Certification Exam

$ who -u

Alexandre Fagundes
alexandre.af.fagundes@oracle.com
LAD Technical Partner Advisor

20+ years in IT Industry
14+ years of Oracle (3 seasons)

- Cloud Architect
- Database Administrator
- EBS Applications DBA
- Support Engineer
- Partner Enablement

/alexandre-b-fagundes

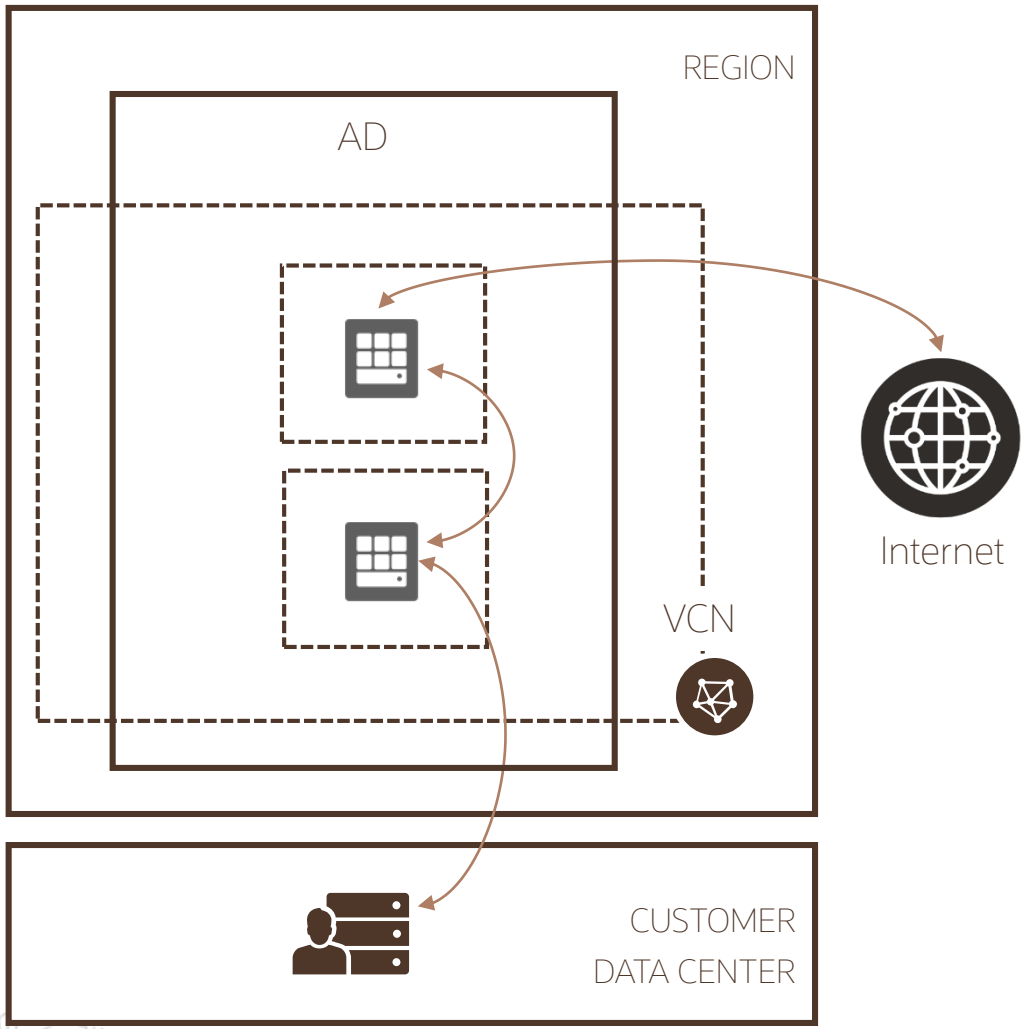
Agenda

- Design & Deploy OCI VCNs
- VCN Gateways
- Networking Solutions
- Hybrid Networking Architectures
- Transitive Routing
- Implement and Operate
- Migrate Workloads
- Troubleshooting Tools

ORACLE
Cloud Infrastructure

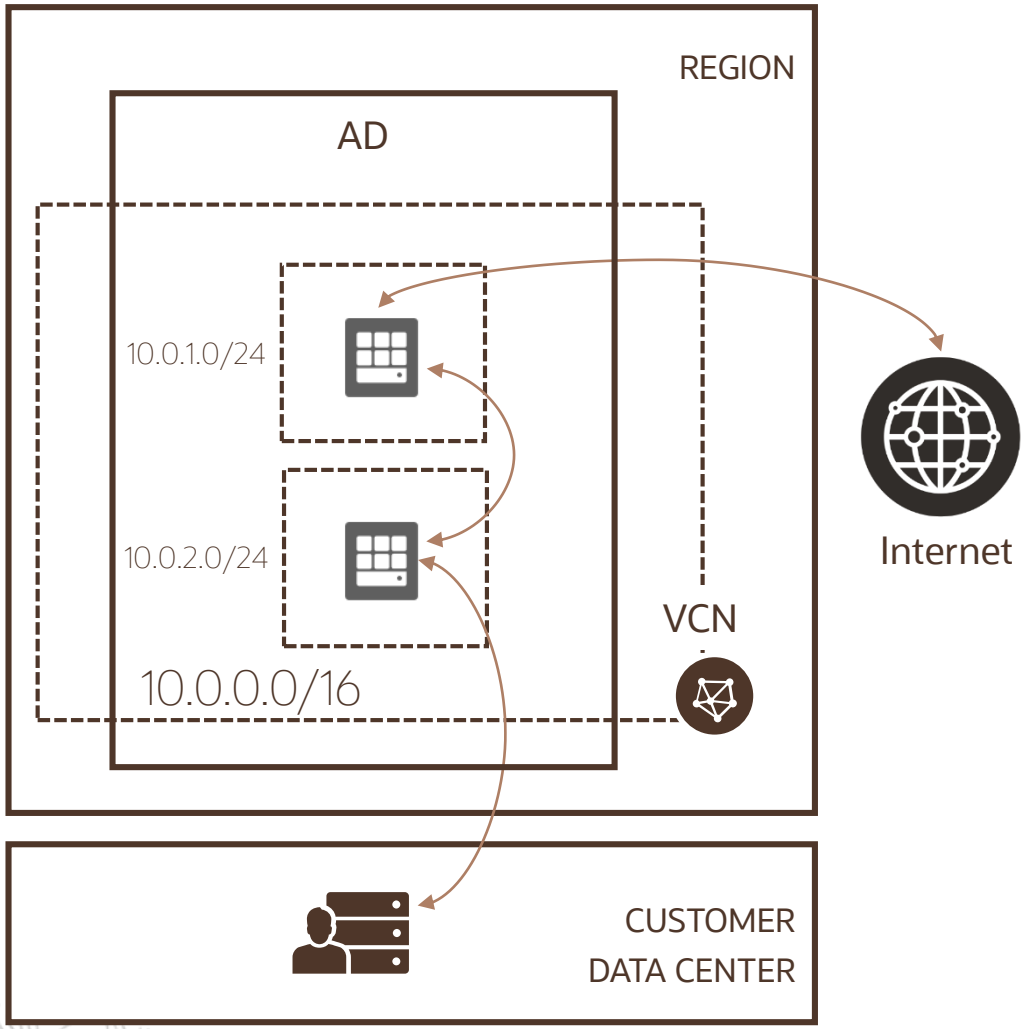
Design & Deploy

VCN Overview



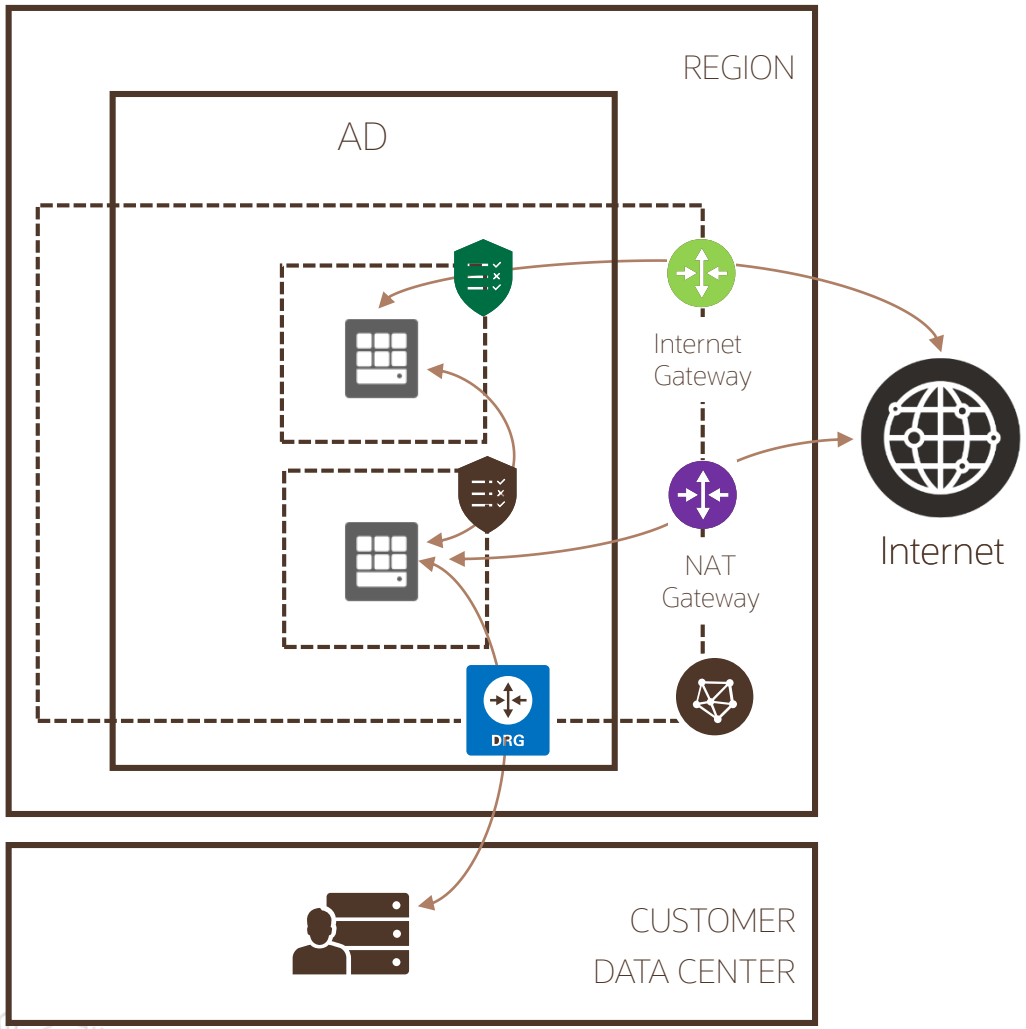
- Software defined private network that you set up in OCI
- Enables OCI resources such as compute instances to securely communicate with Internet, other instances or on-premises data centers
- Lives in an OCI region
- Highly Available, Scalable and Secure

VCN Address Space



- Address space is a range of IP address that you assign to a VCN E.g., 10.0.0.0/16
  - Range: 10.0.0.0 – 10.0.255.255
- Every resource that is connected to this VCN will get its own unique private IP address
  - Server 1 : 10.0.1.2
  - Server 2: 10.0.2.2
- Subnets let you divide the VCN into one or more sub networks
  - E.g., 10.0.0.0/16 – 10.0.1.0/24, 10.0.2.0/24..
  - Compute instances are placed in subnets
  - Subnets can be isolated and secured

VCN Security



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
- Security list apply to a given instance whether it's talking with another instance in the VCN or a host outside the VCN
- Stateful or stateless

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

- Network Security Group consists of set of rules that apply only to a set of VNICs of your choice

Skill check

1. Which RFC 1918 CIDR prefix can be used to create a Virtual Cloud Network (VCN)?

- 8.8.8.8/8
- 172.16. 0.0/12
- 0.0.0.0/0
- 189.215.154.89/32
- 192.168. 0.0/16
- 10.0. 0.0/8

- (•) 192.168. 0.0/16 (*)
- 10.0. 0.0/8

✔Your answer is **Correct**.

Explanation: For a VCN, Oracle recommends using the private IP address ranges specified in RFC 1918. The RFC recommends 10.0/8 or 172.16/12 but Oracle doesn't support those sizes so use 10.0/16, 172.16/16, and 192.168/16.

Skill check

2. Where in Oracle Cloud Infrastructure would you find a key difference between a Network Security Group (NSG) and a Security List (SL)?

- ○ In the configuration of load balancers
- ○ Within the Identity and Access Management (IAM) console
- ○ At the instance level within a subnet
- ○ At the VCN level controlling traffic between subnets

- ● At the VCN level controlling traffic between subnets (*)

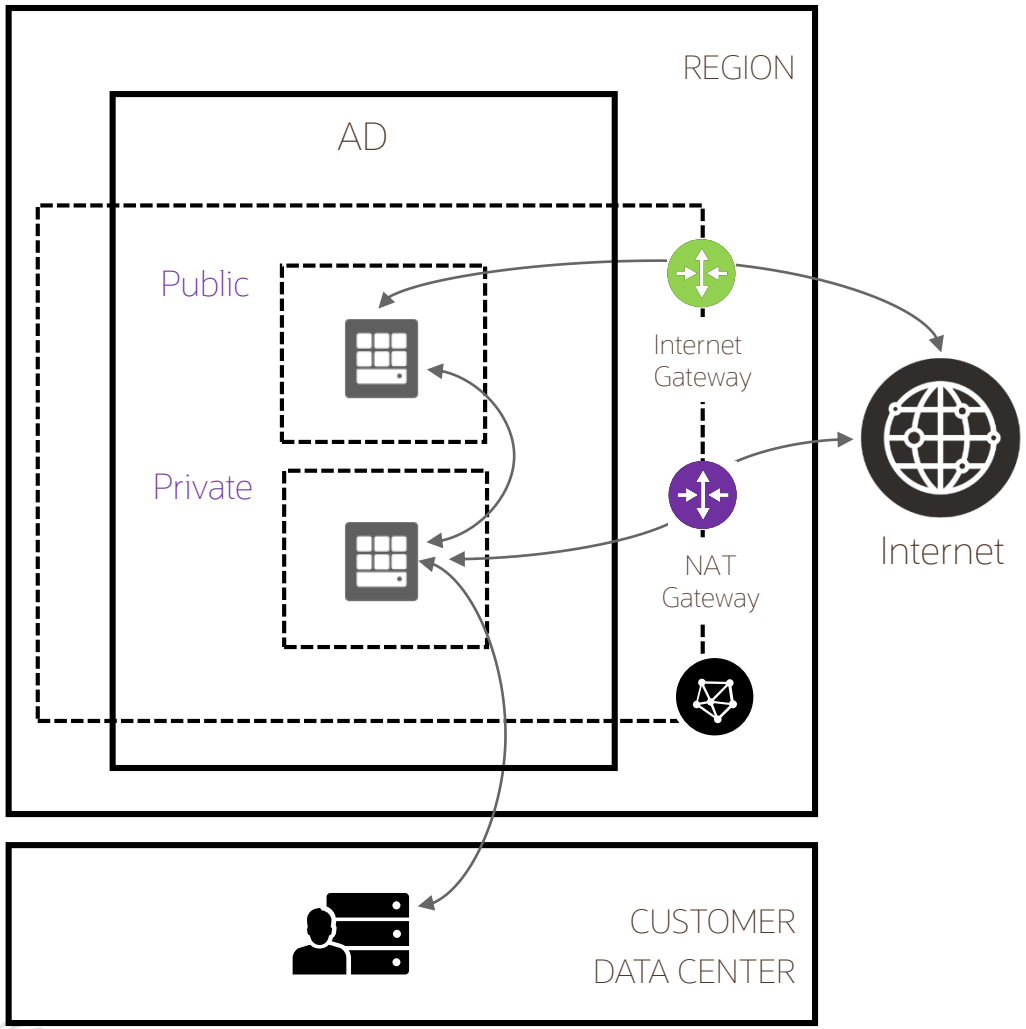
✔Your answer is **Correct**.

Explanation: These two features offer different ways to apply security rules to a set of virtual network interface cards (VNICs) in the Virtual Cloud Network (VCN).

ORACLE
Cloud Infrastructure

VCN Gateways

Communication with the Internet

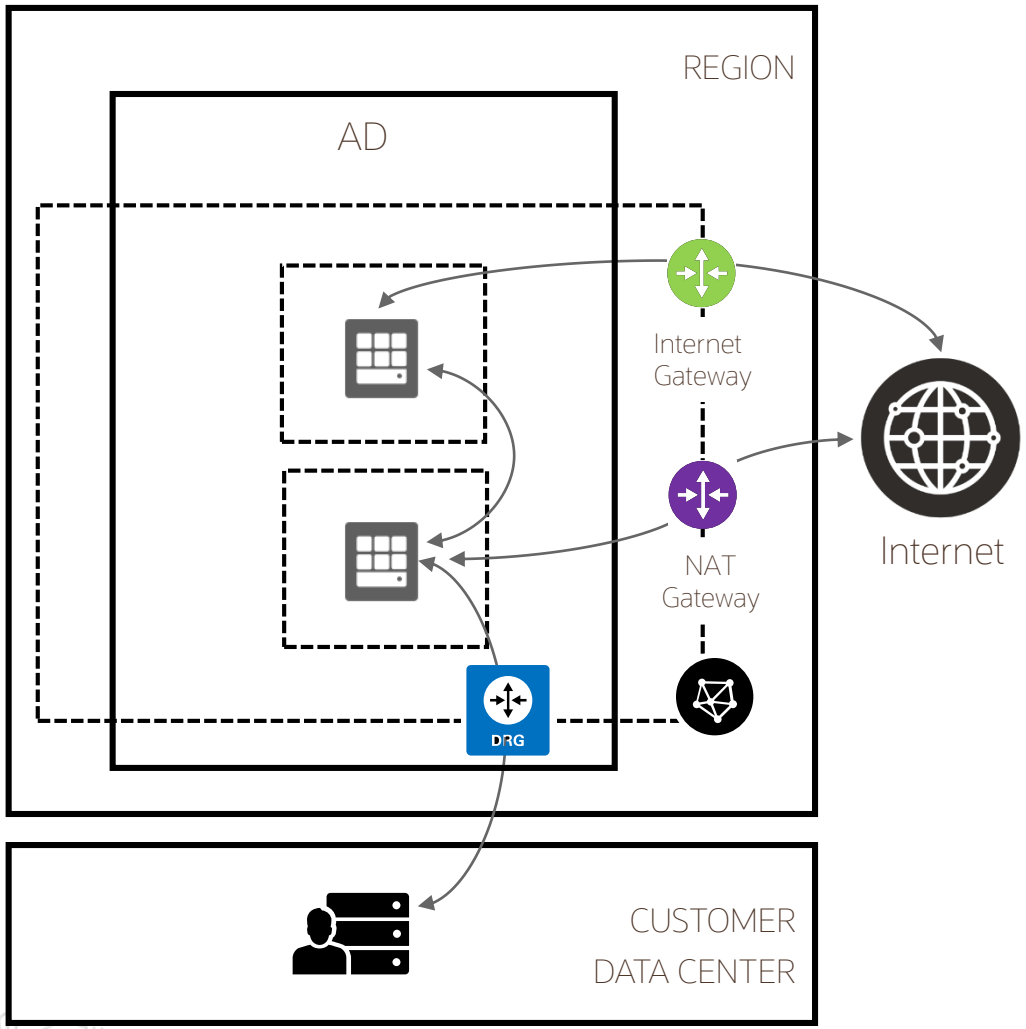


Internet gateway provides a path for network traffic between your VCN and the internet

NAT Gateway enables outbound connections to the internet, but blocks inbound connections initiated from the internet

Use case: updates, patches

Communication to On-Premises

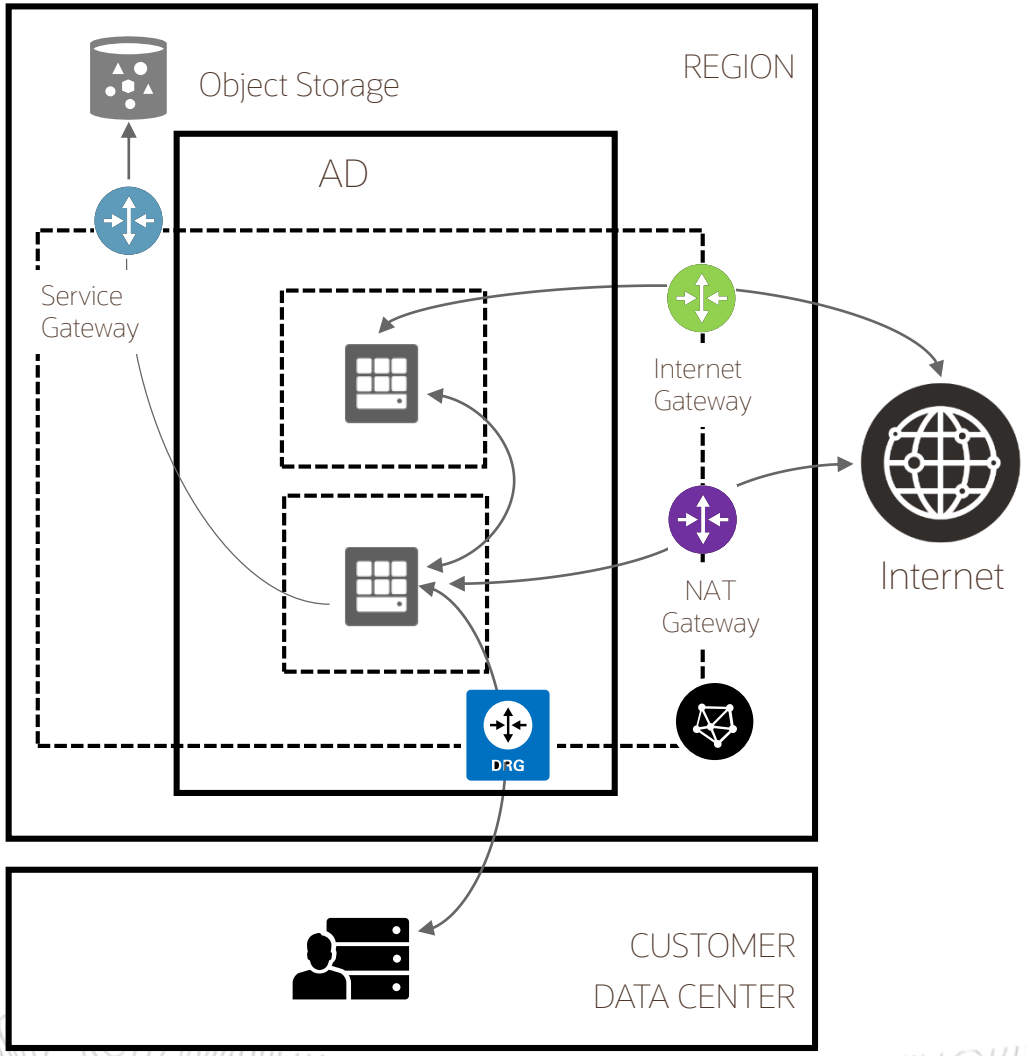


DRG is a virtual router that provides a path for private traffic between your VCN and destinations other than the internet

You can use it to establish a connection with your on-premises network via

- IPsec VPN
- FastConnect (Dedicated connectivity)

Communication to Public OCI Services

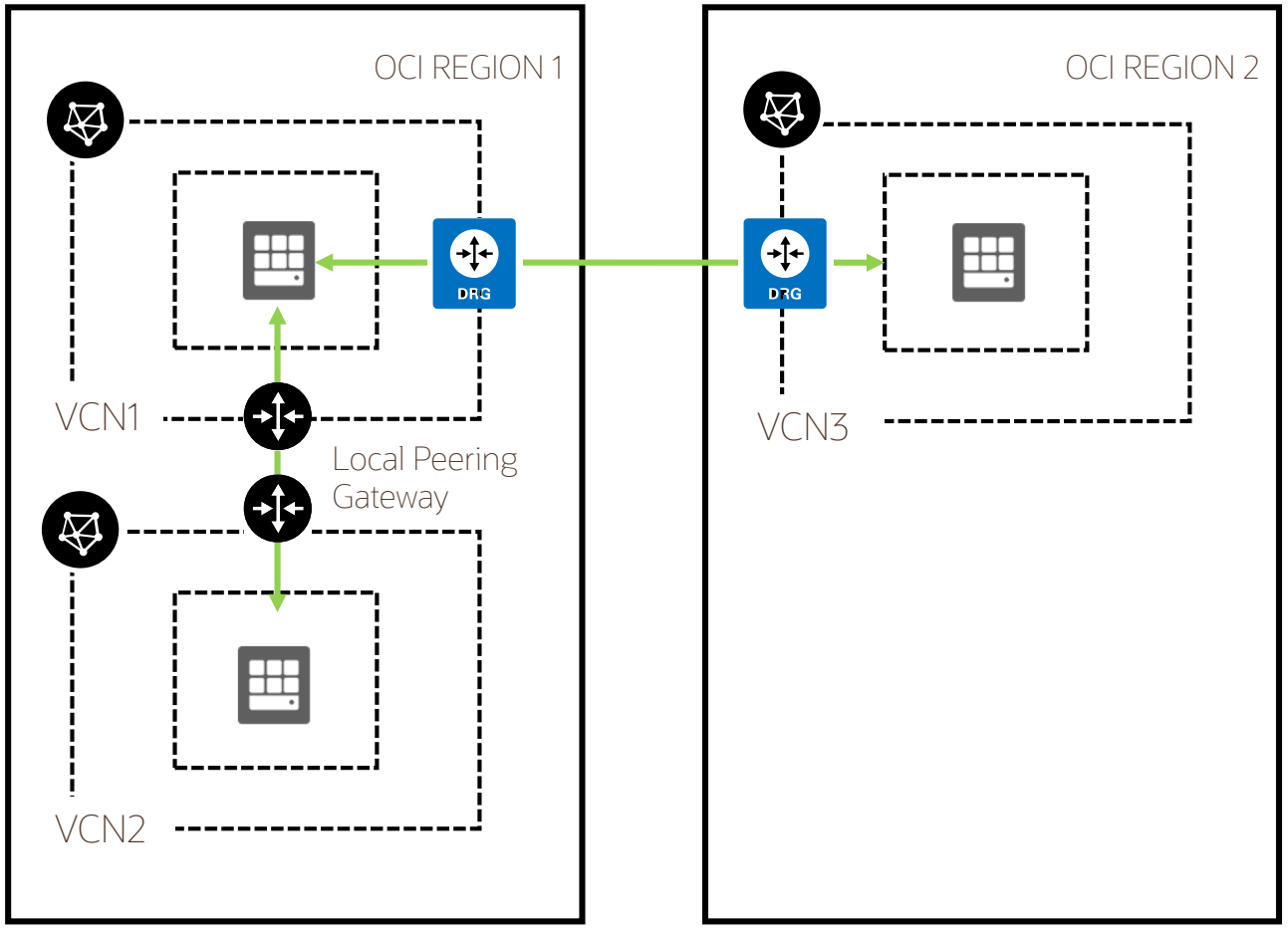


Service gateway lets resources in VCN access public OCI services such as Object Storage, but without using an internet or NAT gateway

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

Use case:
Back up DB Systems in VCN to Object Storage

Communications to Others VCN: Peering



VCN peering is the process of connecting multiple VCNs

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

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

Skill check

1. Which Oracle Cloud Infrastructure gateway is specifically designed to connect different Virtual Cloud Networks (VCNs) within the same region?

- Dynamic Routing Gateway (DRG)
- Network Address Translation (NAT) Gateway
- Internet Gateway (IGW)
- Local Peering Gateway (LPG)

- Local Peering Gateway (LPG) (*)

✔Your answer is **Correct**.

Explanation: A Local Peering Gateway (LPG) is a component on a VCN for routing traffic to a locally peered VCN.

Skill check

2. Which Oracle Cloud Infrastructure gateway is a stand-alone object that can attach a Virtual Cloud Network (VCN)?

- ○ Network Address Translation (NAT) Gateway
- ○ Internet Gateway (IGW)
- ○ Dynamic Routing Gateway (DRG)
- ○ Local Peering Gateway (LPG)

- ● Dynamic Routing Gateway (DRG) (*)
- ○ Network Address Translation (NAT) Gateway
- ○ Internet Gateway (IGW)

✔Your answer is **Correct**.

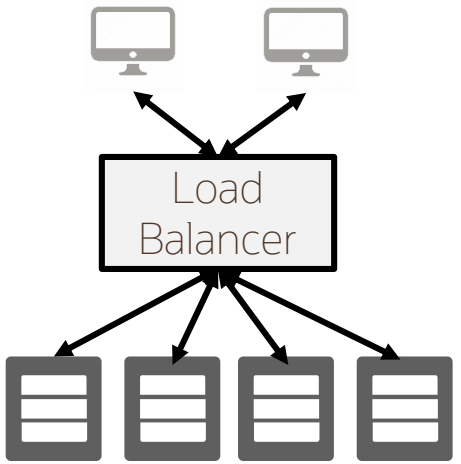
Explanation: A DRG is a virtual router to which you can attach resources, including VCNs.

ORACLE
Cloud Infrastructure

Networking Solutions

Load Balancer

- A load balancer sits between the clients and the backends performs tasks such as:
  - **Service Discovery**: What backends are available? How should LB talk to them?
  - **Health Check**: What backends are currently healthy to accept requests?
  - **Algorithm**: What algorithm should be used to balance individual requests across the healthy backends?

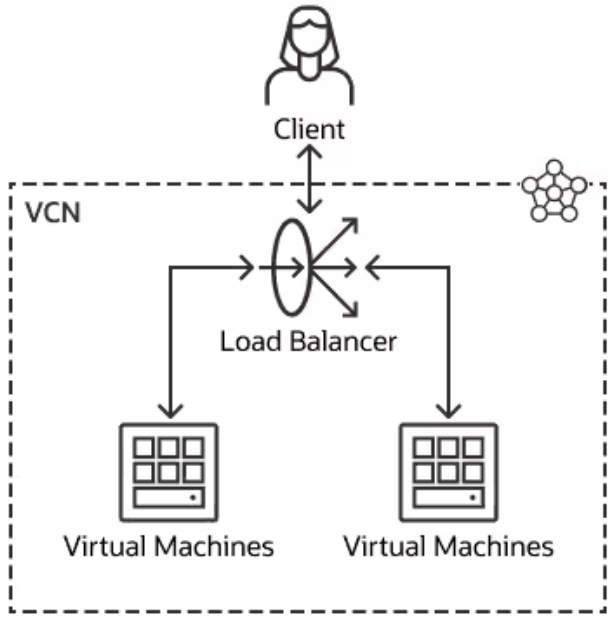


Load Balancer benefits

- **Fault tolerance and HA**: using health check + LB algorithms, a LB can effectively route around a bad or overloaded backend
- **Scale**: LB maximizes throughput, minimizes response time, and avoids overload of any single resource
- **Naming abstraction**: name resolution can be delegated to the LB; backends don't need public IP addresses

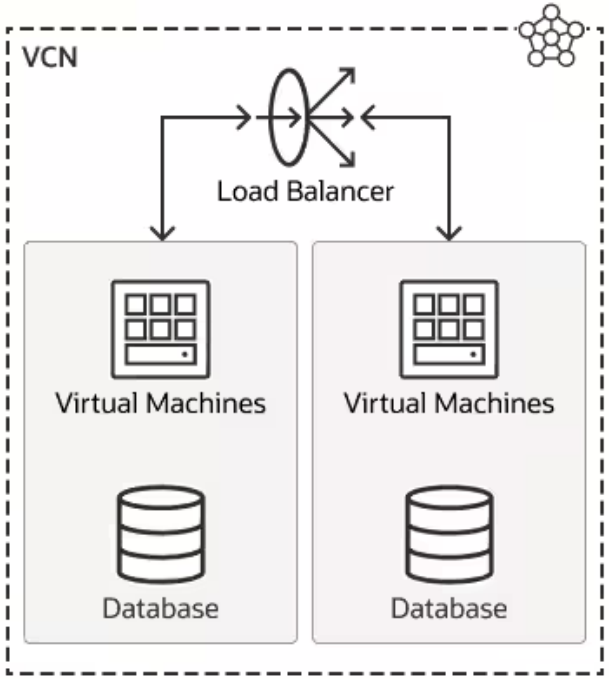
Load Balancer Use Cases

Automatically distribute application load across resources



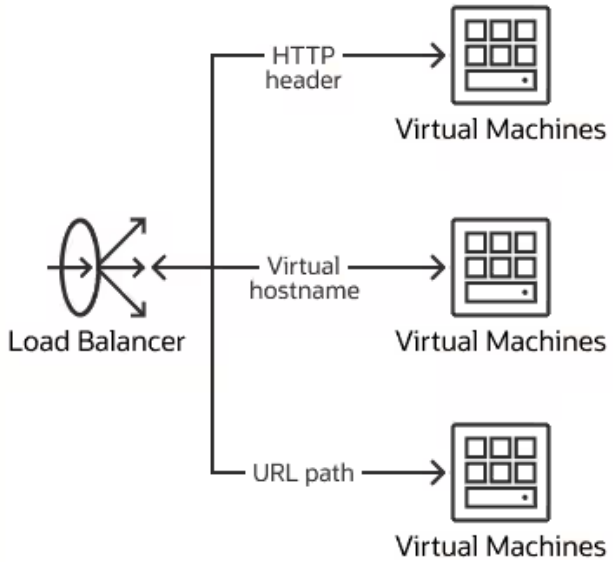
Direct incoming requests to multiple, backend application services through a single IP address in a way that ensures efficient usage of resources. Deliver requests based on different strategies that balance the load across backend resources.

Modernize and create resilient applications



Scale multiple instances of cloud native and legacy applications behind a single load balancer. Actively test the health of backend application services and re-direct traffic automatically when any particular resource fails to respond.

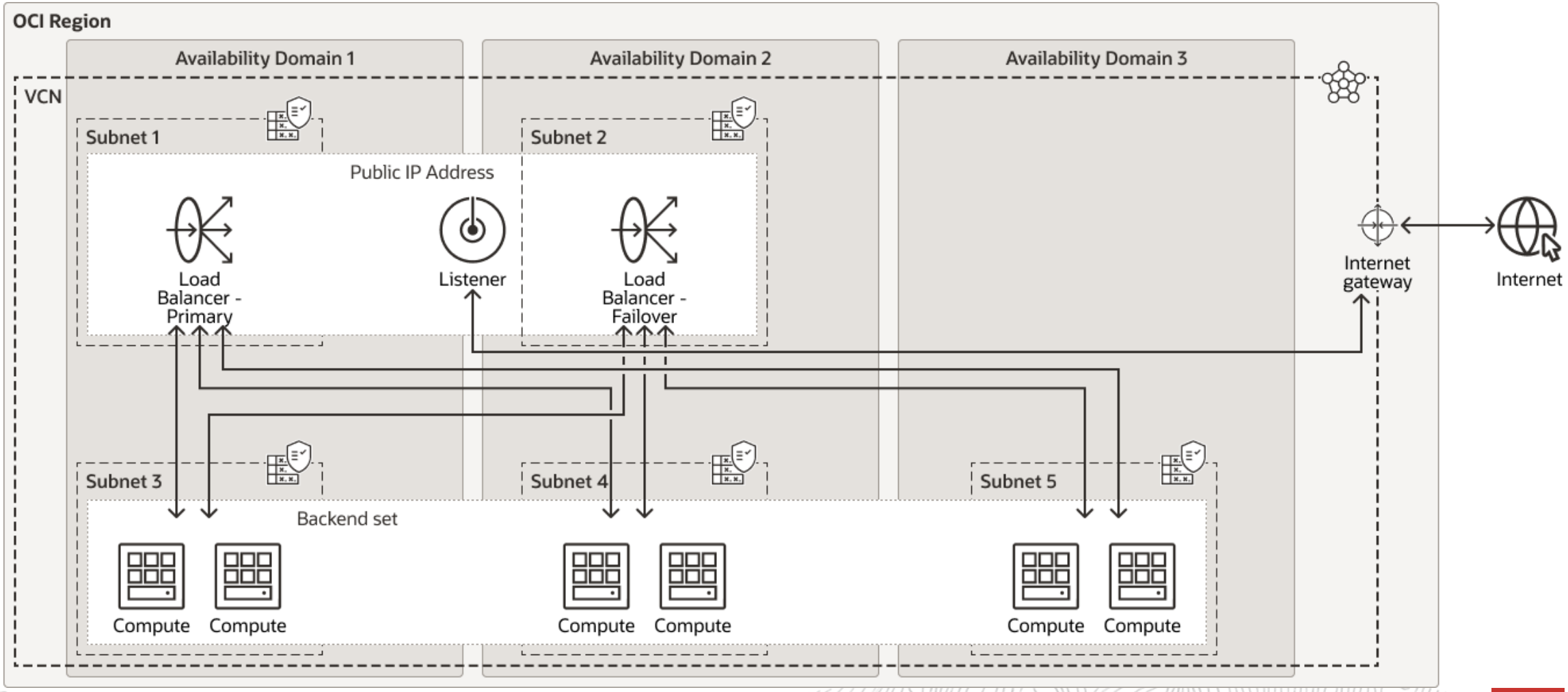
Distribute requests based on traffic characteristics



Direct incoming web requests to specific backend services based on user-defined rules applied to the HTTP headers or URLs.

Public Load Balancer

Simple Load Balancer Diagram



DNS Reference Links

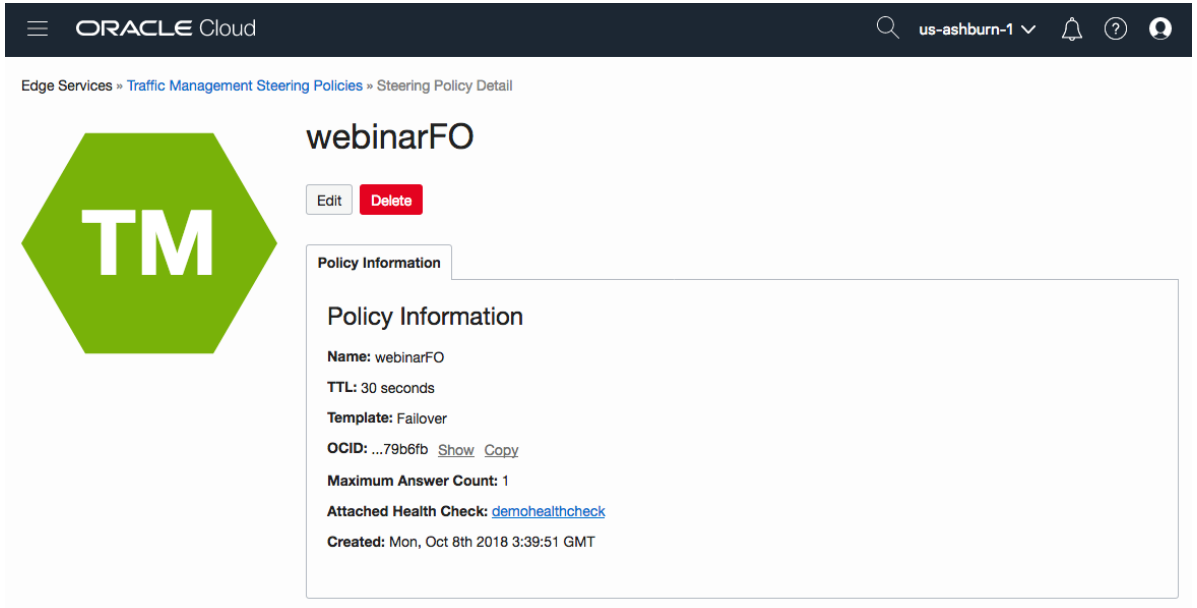
- Documentation Link
- DNS Zone Management
- Traffic Management
- Blog: Manual fail-over is the past (Traffic Management Steering Policies)

DNS Zone Management

- Highly scalable, global anycast Domain Name System (DNS) network that assures high site availability and low latency
- Offers a complete set of functions for zone management:
  - Create and manage zones and records
  - Import/upload zone files
  - Filter and sort views of zones and records
  - Secondary DNS support
  - APIs and SDKs

Traffic Management

- Traffic Management allows customers to configure routing policies for serving intelligent responses to DNS queries.
- Different answers may be served for a query according to the logic in the customer-defined Traffic Management Steering Policy, thus sending users to the most optimal location in your infrastructure.

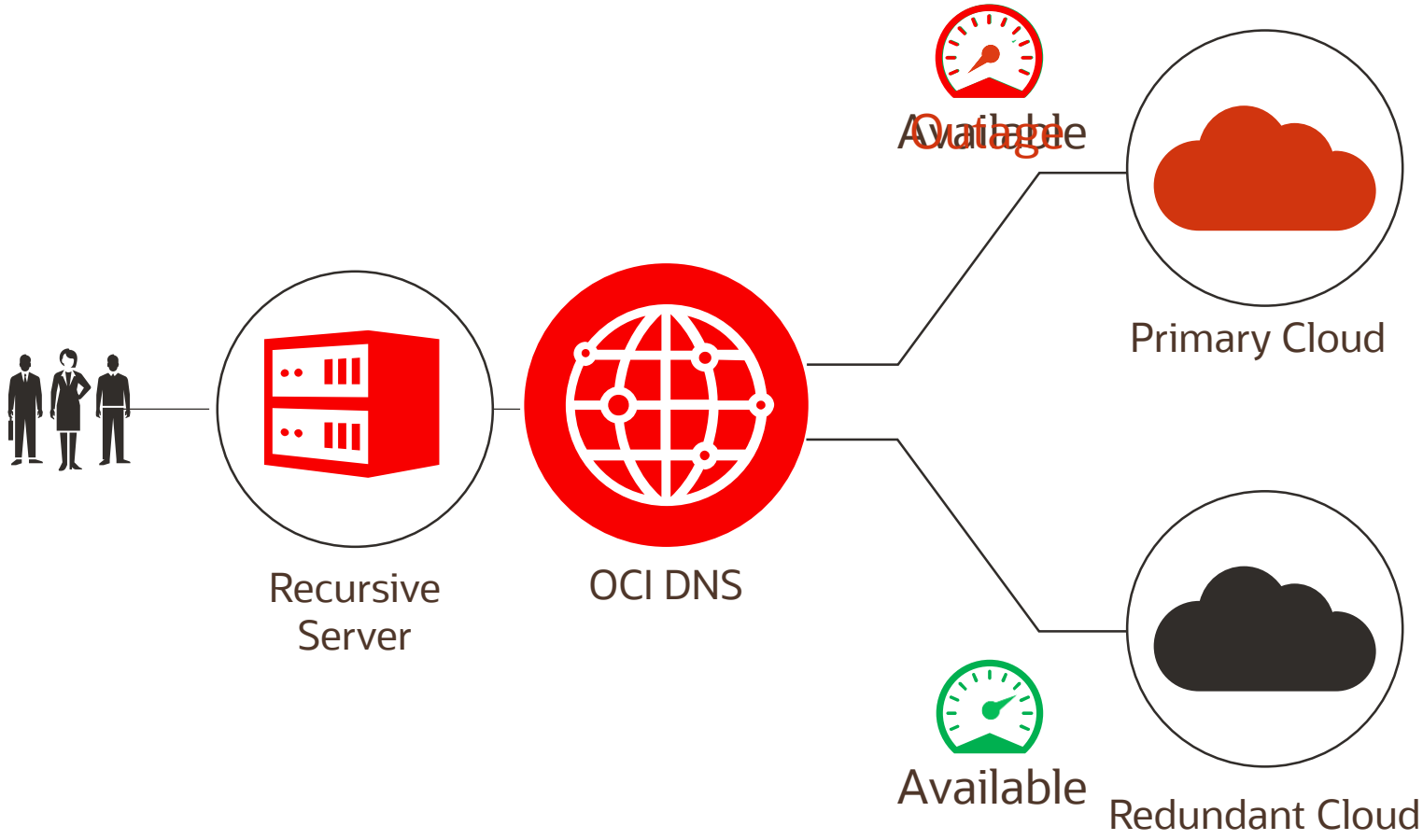


When should I use DNS Traffic Management?

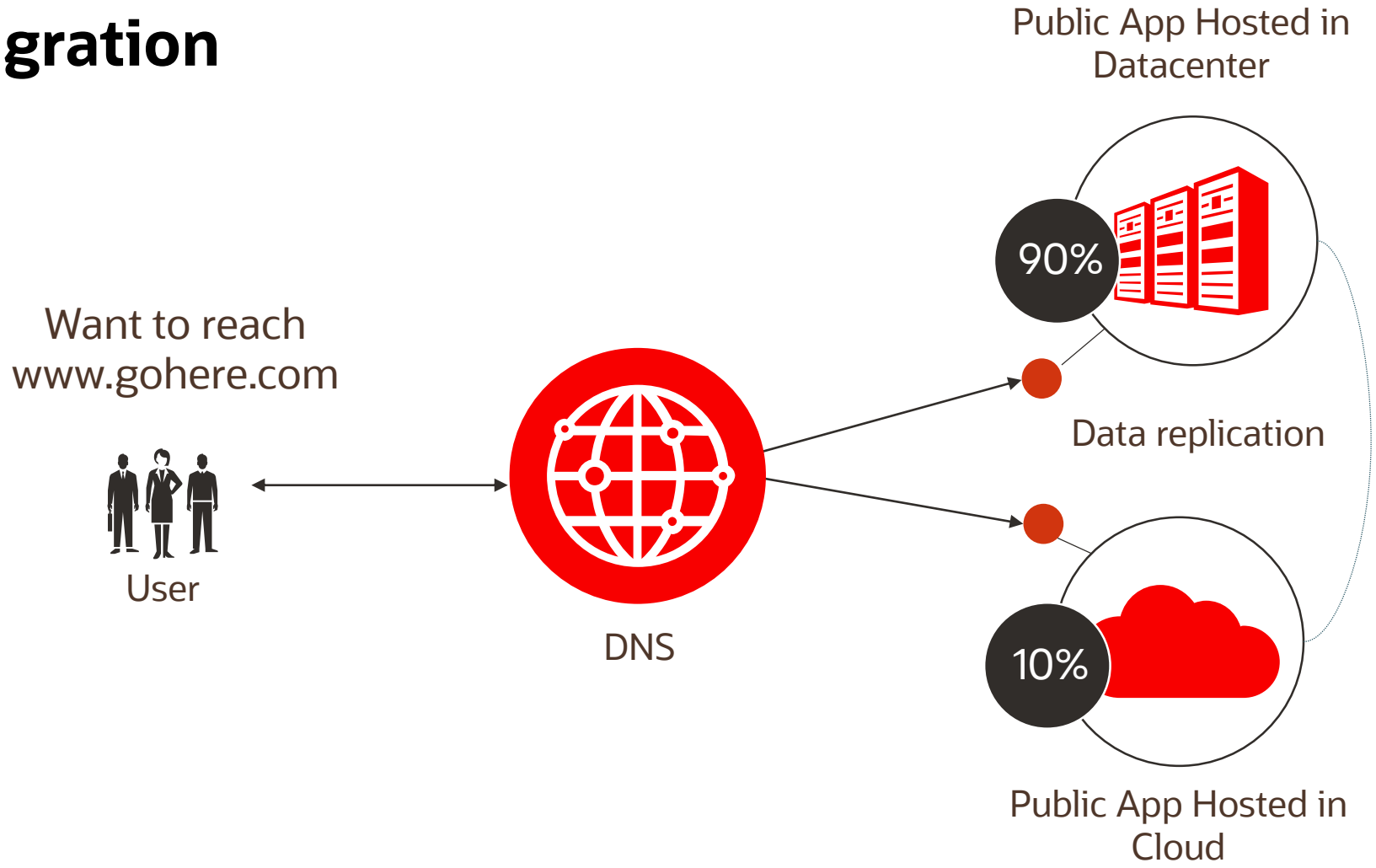
Common Use Cases

- Failover
- Cloud Migration
- Load Balancing For Scale
- Hybrid Environments
- Worldwide Geolocation Steering
- IP-Based Steering
- Zero-Rating Service

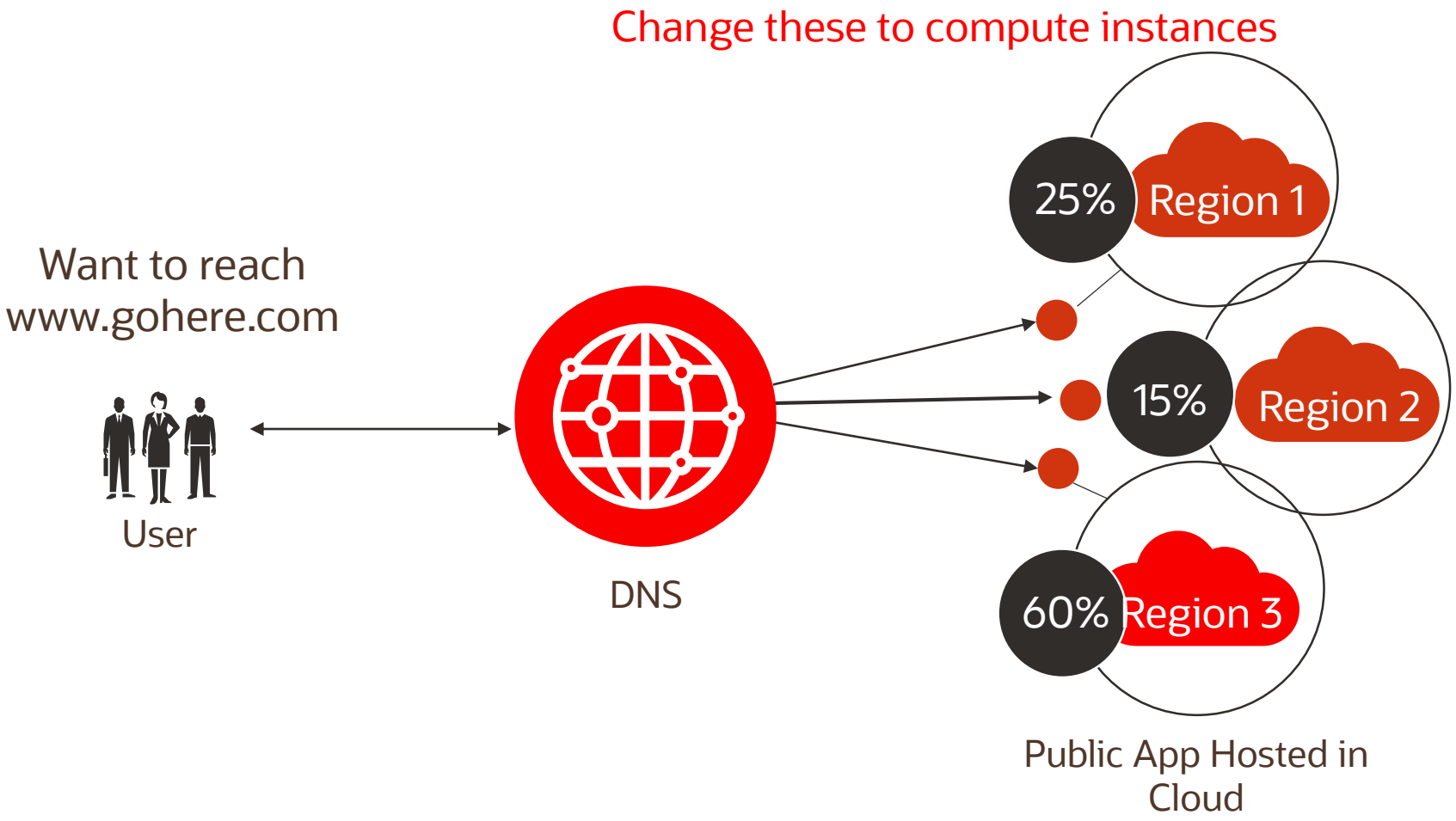
Failover


Outage
Available
Primary Cloud
Recursive Server
OCI DNS
Available
Redundant Cloud

Cloud Migration



Load Balancer for Scale



Health Checks

- **Availability & Performance Monitoring:** Monitor the availability and performance of any public-facing IP address or fully qualified domain name (FQDN).
  - **Simple UI Configuration**: Easy to configure Health Checks for external monitoring from Vantage Points around the globe.
  - **Availability Monitoring**: Monitor for the availability of any publicly visible IP address or FQDN from Vantage Points located around the globe.
  - **Performance Monitoring**: Monitor for latency metrics for any publicly visible IP address or FQDN from Vantage Points located around the globe.
  - **On-Demand Testing**: Perform tests on demand to gauge performance and troubleshoot endpoints.
- **DNS Traffic Management Failover Detection:** Detect failures and use DNS Traffic Management to failover in the event of a problem.
- **Alerting and API:** Fully integrated with Oracle Cloud Infrastructure Monitoring and backed by an extensive REST API.
- **Hybrid Monitoring:** Monitor endpoints within the Oracle cloud and across your hybrid infrastructure.

Health Checks Service Components

- **Monitors:** Monitors allow you to continuously monitor the health of public-facing endpoints. You can configure monitors to use either HTTP and ping protocols.
- **On-demand probes**: On-demand probes allow you to execute a one-time probe to assess the health of a public-facing endpoint. You can configure on-demand probes to use either or both HTTP and ping protocols. This feature is currently only available via the REST API.
- **Vantage points**: Vantage points are geographic locations from which monitors and probes can be executed to your specified target. Oracle Cloud Infrastructure maintains dozens of vantage points around the world.
- **Protocols**: The Health Checks service allows you to configure both HTTP and ping type monitors. Each type has respective protocols.

Demo

- Create VM1
- Create VM2
- Populate index.html
- Create public LB
- HTTP request

ORACLE
Cloud Infrastructure

Hybrid Networking Architectures

Defining multicloud and its advantages

Multicloud *is the coordinated use of cloud computing services from two or more public cloud vendors.*

Companies use multicloud environments to distribute computing resources and minimize the risk of downtime and data loss.

Companies also adopt two or more public cloud providers for their unique capabilities.

Advantages

- Maximize Strengths of Each Provider
- De-Risk Single Provider Outages
- Multicloud Economics
- Reduces Vendor Lock-in
- Reduced Latency
- Regional Availability
- Audit/Compliance Pressure

Explore OCI connectivity solutions for multicloud

OCI and Azure / GCP Interconnect

- Migrate to the cloud or build new applications that leverage OCI and Azure and GCP capabilities
- Use a broader range of tools
- Deploy custom and packaged apps across OCI and Azure / GCP
- Preserve application architectures, optimizations, and interoperability
- A private physical connection
- Lowest latency: < 2ms

Latency-sensitive applications

ORACLE Cloud Infrastructure  Azure Google Cloud

Oracle FastConnect and third-party connection

- Joins virtual cloud networks via high-bandwidth connections
- Fully encrypted traffic through a private physical connection
- Extends on-premises and cloud environment to OCI with third-party providers (Oracle partner, colocation space, etc.)
- Choose from 50+ FastConnect partners globally, including top carriers and network providers

Latency-sensitive applications

ORACLE Cloud Infrastructure  aws etc.

Site-to-Site VPN Connection

- Secure, encrypted IPSec tunnels through the public internet
- Support for Internet Key Exchange (IKE) v1 and v2
- Public internet lines are used to transmit data; could be cheaper than dedicated connections
- The internal IP addresses of the participating networks and nodes are hidden from external users.
- High availability support

More economical for low egress traffic

ORACLE Cloud Infrastructure  aws Google Cloud Azure etc.

Generic Reference Links VPN

VPN Important Reading:

- Sales Page / FAQ
- Blogs:
  - Enhancements to OCI Site-to-Site VPNs
  - Announcing multiple enhancements for Oracle Cloud Infrastructure IPSec VPNs
- Sample Configurations:
  - Launching Your Own Free Private VPN In The Oracle Cloud (Open VPN)
  - Creating an IPSec connection to OCI using Libreswan as a CPE
  - Libreswan Oracle Documentation
- Product Page Documentation / VPN Site-to-Site Best Practices
- Multi Region FastConnect/VPN Redundancy (DR / High Availability)

Connectivity to on-premises network planning

Connecting your virtual cloud network (VCN) to your on-premises network requires certain design considerations

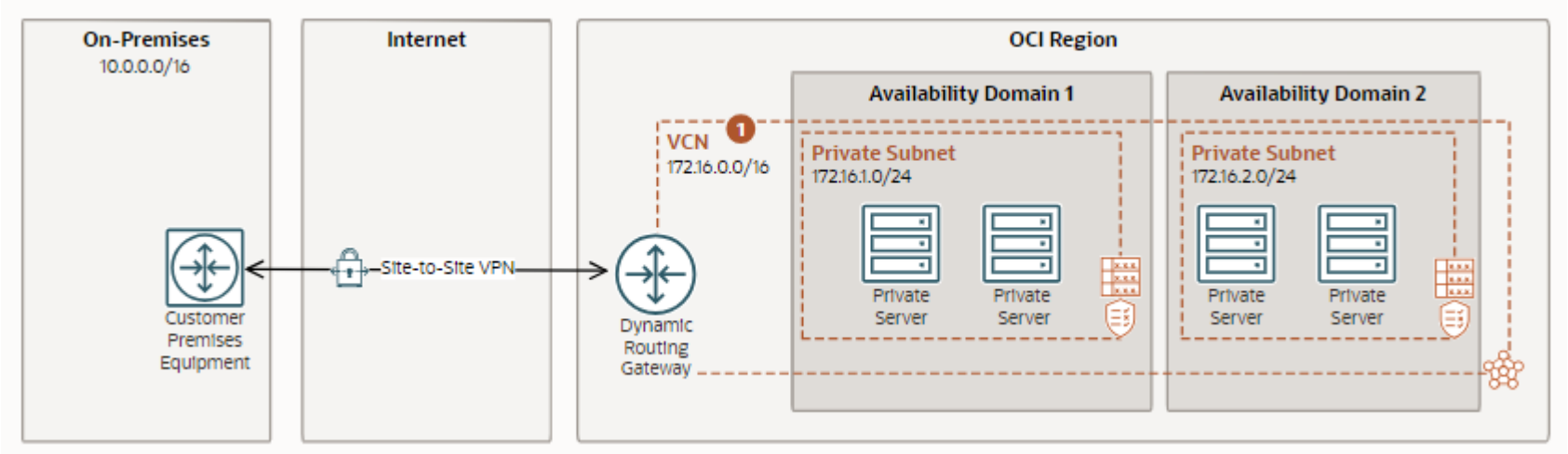
- What kind of **Bandwidth/throughput** your application requires?
- Is your application **Latency sensitive**?
- Are you planning to provide **Redundancy** to your on-premises connectivity and avoid single point of failure?
- Do you require a **secure** and **private dedicated** connection or a public connection over the internet ?
- Do you see your services growing, and plan to dynamically **scale up** your application bandwidth needs?

VPN Concepts

- Dynamic Routing Gateway - VPN headend at OCI end of the VPN connection.
- Customer Premise Equipment (CPE)
    - Actual VPN router/Edge device in your on-premises network (hardware or software)
    - When setting up the VPN, you create a virtual representation of your on-premises router, which is known as CPE object
    - To Create a CPE Object – Name, Outside Public IP address
- IPSec Connection
    - After creating the CPE object and DRG, you connect them by creating an IPSec connection, which results in multiple redundant IPSec tunnels
- While creating an IPSec connection, configure the type of routing
    - BGP dynamic routing
    - static routing
- When you set up an IPSec VPN, by default Oracle provides each tunnel's shared secret/pre-shared key. You can also specify your own shared secret key instead.

VPN Basics Components

VPN – using a public network to make end to end connection between two private networks in a secure fashion



- CPE
- DRG
- IPSec Connection (Connects CPE with DRG)

- **Tunnel** – a way to deliver packets 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

Generic Reference Links FastConnect

FastConnect Important Reading:

- Sales Page / Pricing Model / FAQ
- Blogs:
  - Announcing bidirectional forwarding detection and enhancements for OCI FastConnect
  - FastConnect Design
  - Announcing MACsec encryption for Oracle Cloud Infrastructure FastConnect (Security Feature)
- Sample Configurations:
  - Configure a FastConnect Direct Link with Equinix Cloud Exchange Fabric
  - Oracle Cloud Infrastructure FastConnect Integration with Colt
- Product Page Documentation
- FastConnect Redundancy Best Practices

FastConnect

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

- Connect to OCI directly or via pre-integrated Network Partners
- Port speeds of 1 Gbps,10 Gbps, 100 Gbps and 400 Gbps increments
- Extend remote datacenters into Oracle (“Private peering”) or connect to Public resources (“Public peering”)
- No charges for inbound/outbound data transfer
- Uses BGP protocol

FastConnect Use Cases

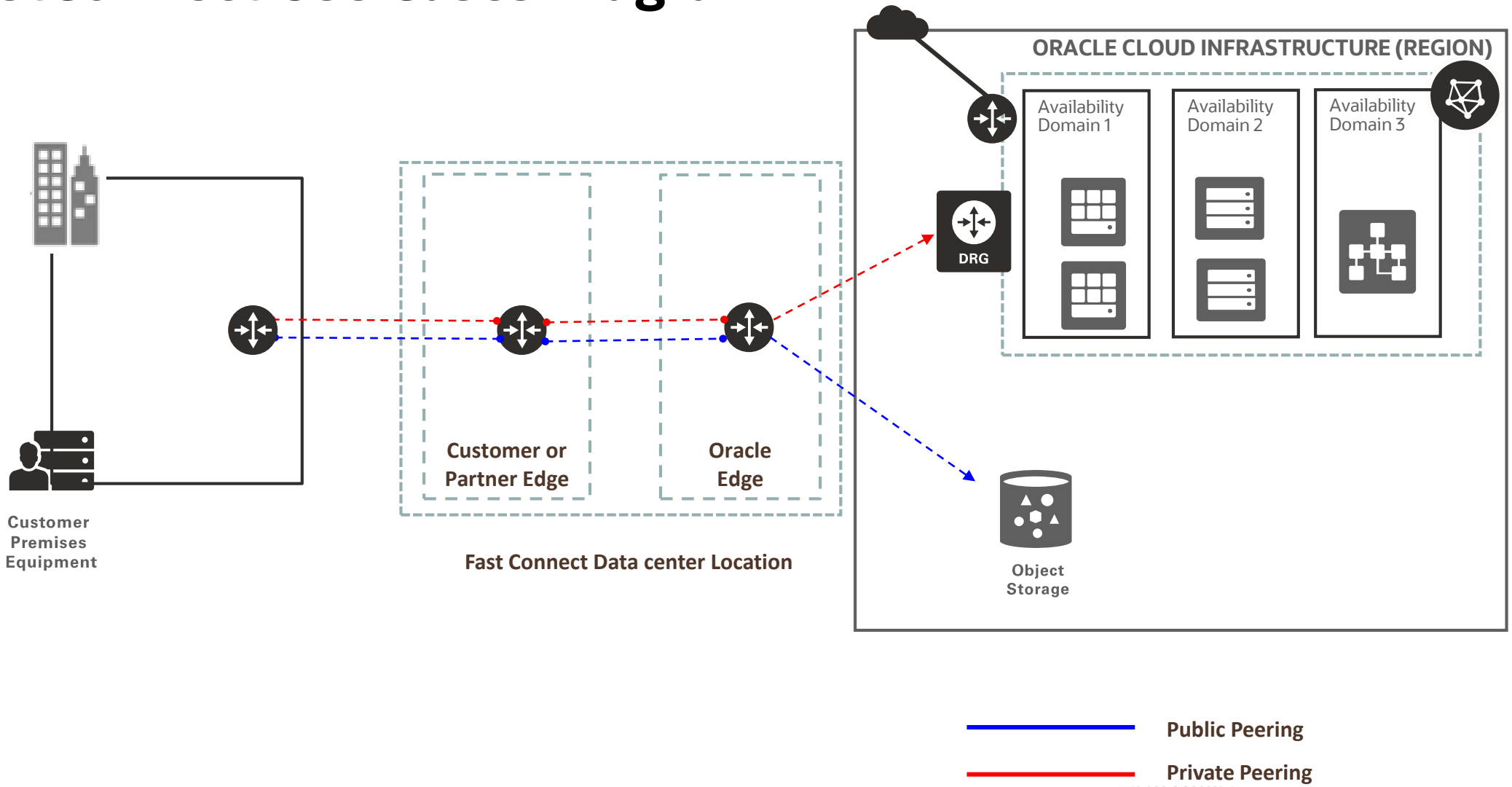
Private Peering

- Extension of the on premise network to the OCI VCN
- Communication across connection with private IP addresses

Public Peering

- To access public OCI services such as Object storage, OCI Console or APIs over dedicated FastConnect connection
- Doesn't use DRG

FastConnect Use Cases Diagram



Skill check

1. You are designing a hybrid cloud solution that involves connecting your on-premises data center to Oracle Cloud Infrastructure (OCI) using a Dynamic Routing Gateway (DRG). For enhanced security, you want to ensure that the traffic passing through the DRG is encrypted. Which OCI service or feature should you leverage to implement encryption for the communication between your on-premises network and OCI via the DRG?

- ○ Oracle Cloud FastConnect
- ○ Oracle Cloud Site-to-Site VPN
- ○ Oracle Cloud Network Firewall
- ○ Oracle Cloud Remote Peering Connection (RPC)

- ● Oracle Cloud Site-to-Site VPN (*)
- ○ Oracle Cloud FastConnect
- ○ Oracle Cloud Remote Peering Connection (RPC)
- ○ Oracle Cloud Network Firewall

✔Your answer is **Correct**.

Explanation: Site-to-Site VPN provides a site-to-site IPSec connection between your on-premises network and Virtual Cloud Network (VCN). The IPSec protocol suite encrypts IP traffic before the packets are transferred from the source to the destination and decrypts traffic when it arrives.

Skill check

2. Which Dynamic Routing Gateway (DRG) feature involves the propagation of routes between different networks connected to the DRG?

- Route Tables
- Route Distributions
- Equal-Cost Multi-Path Routing
- Loopback Attachments

- (●) Route Tables
- Route Distributions (*)
- Equal-Cost Multi-Path Routing
- Loopback Attachments

✖Your answer is **Incorrect**.

Correct Answer: Route Distributions

Explanation: A distribution is a list of declarative statements that contain match criteria (such as an OCID or an attachment type) and an action. Route distributions specify how routes get imported from or exported to a DRG attachment.

ORACLE
Cloud Infrastructure

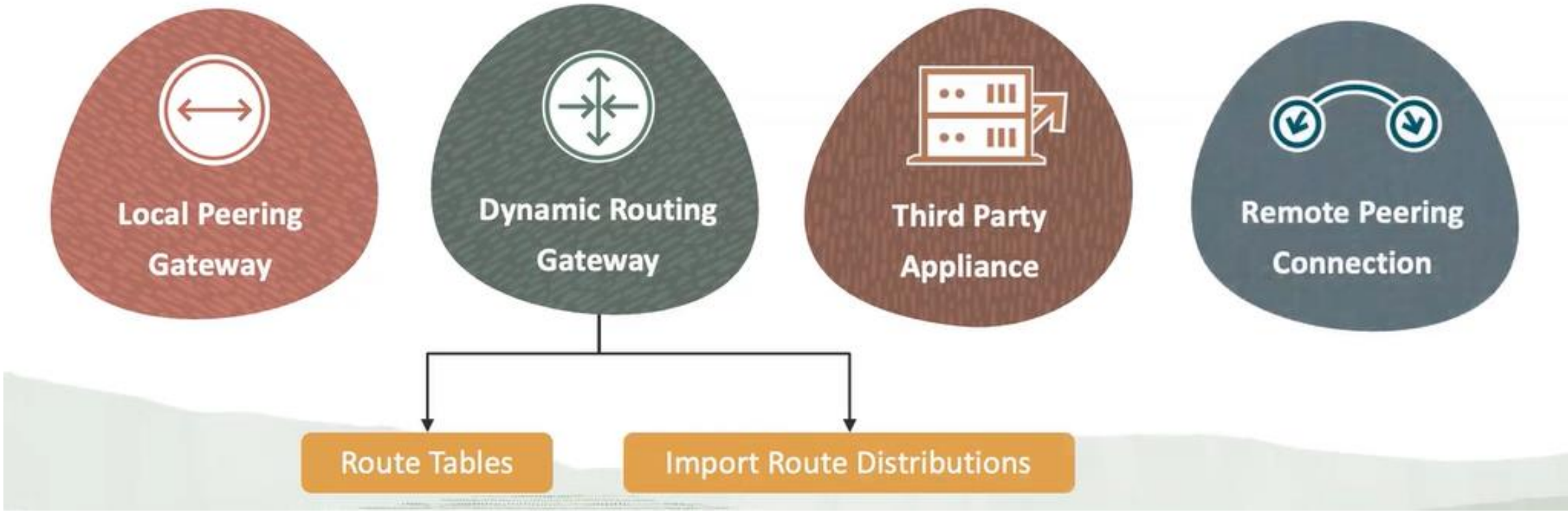
Transitive Routing

What is OCI Transit Routing?

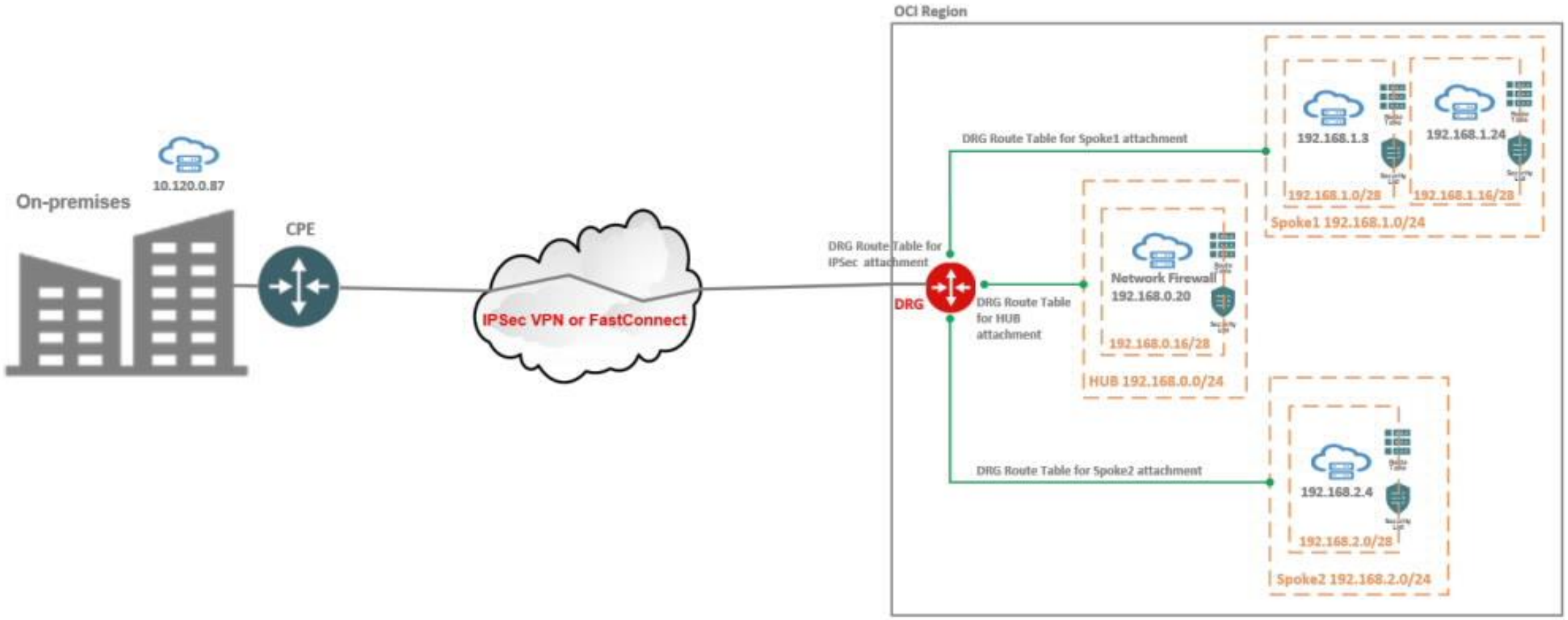
The OCI VCN Transit Routing solution is based on Hub-Spoke Topology and enables the hub VCN to provide transit between multiple spoke VCNs (within the OCI region) and OnPrem networks

VCN transit routing can also be used to transit from one OCI region to another leveraging OCI backbone

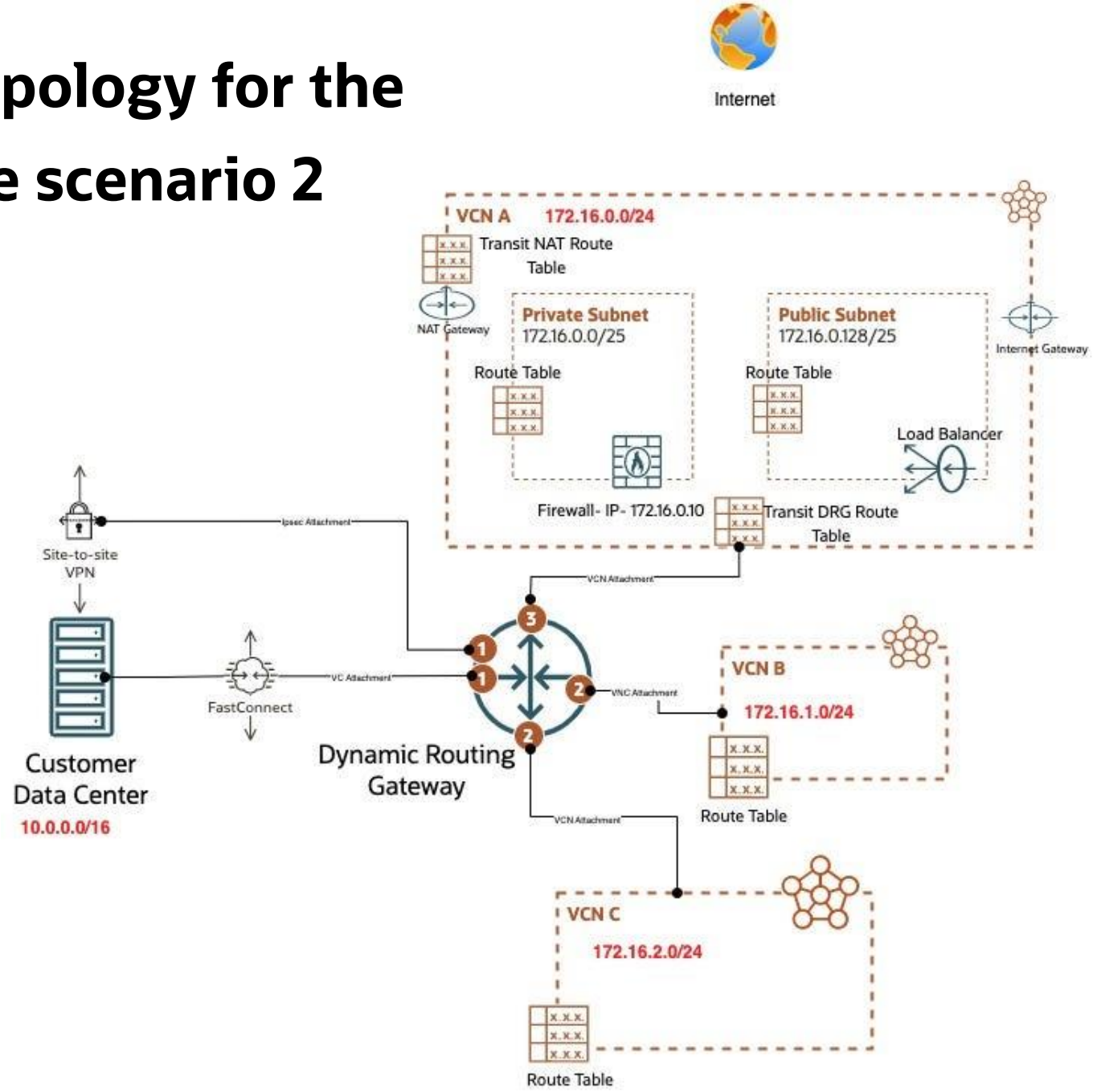
OCI Transit Routing will leverage at least one component



Networking topology for the Hub and Spoke scenario 1



Networking topology for the Hub and Spoke scenario 2



Skill check

1. Which DRG service provides a list of declarative statements that contain match criteria (such as an OCID) and an action for specifying how routes get imported from or exported to a DRG attachment?

- Route Distributions
- Cross-Tenancy Attachments
- Local Peering Attachment
- Route Tables

- (●) Route Distributions (*)
- Cross-Tenancy Attachments
- Local Peering Attachment
- Route Tables

✔Your answer is **Correct**.

Explanation: Route Distributions specify how routes get imported from or exported to a DRG attachment.

Skill check

2. Which three OCI gateways can be leveraged for a Transitive Routing Configuration?

- [ ] Local Peering Gateway
- [ ] NAT Gateway
- [ ] Dynamic Routing Gateway
- [ ] Internet Gateway
- [ ] Services Gateway

2. Which three OCI gateways can be leveraged for a Transitive Routing Configuration?

- [x] Local Peering Gateway (*)
- [ ] NAT Gateway
- [x] Dynamic Routing Gateway (*)
- [ ] Internet Gateway
- [x] Services Gateway (*)

✔Your answer is **Correct**.

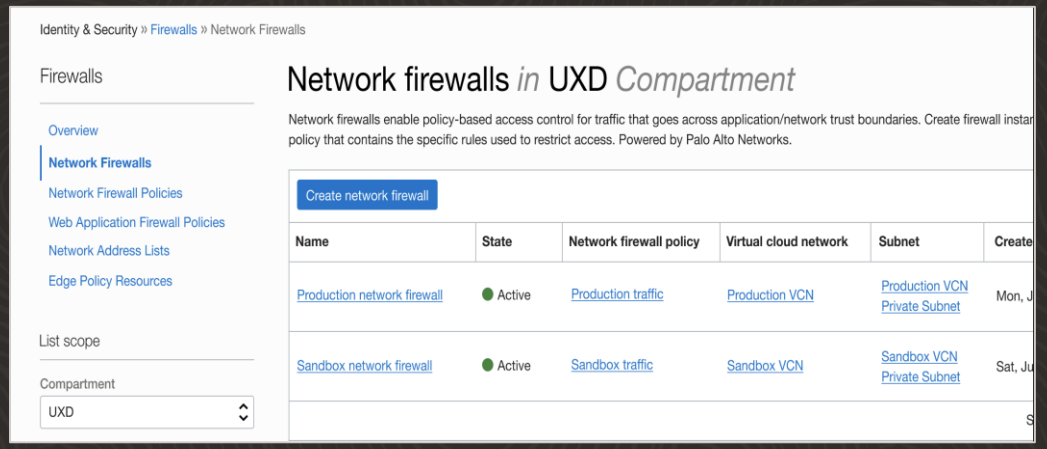
Explanation: Only resources within the VCN can use the Internet and NAT gateways.

ORACLE
Cloud Infrastructure

Implement & Operate Connectivity

OCI Network Firewall

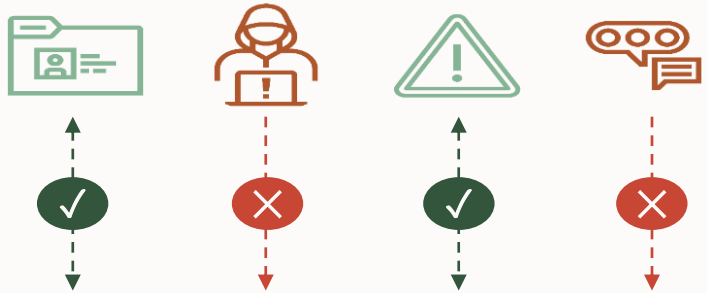
OCI Network Firewall is a cloud-native managed firewall service that is built using industry leading **Palo Alto Networks** next-generation firewall technology. It provides advanced threat protection capabilities including custom URL filtering, intrusion prevention and detection (IDS/IPS), and TLS inspection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



Customer benefits

- **Cloud-Native Firewall** - Scalable native service that eliminates the need to manage additional third-party security infrastructure.
- **Deep Integration with OCI** - Natively integrated with OCI platform including logging and metrics services.
- **Layered Defense** - Easily apply deeper security controls and segmentation for encrypted and non-encrypted traffic to customer workloads on OCI.
- **Advanced Threat Protection** – Industry leading threat protection to help monitor and block malware, spyware and vulnerability exploits.
- **Meet Compliance Goals** – Helps meet compliance requirements and stringent security needs of regulated environments.

OCI Network Firewall features



Stateful Rules

> Stateful filtering Allow or Deny rules based on 5-tuple information for both IPv4 and IPv6 traffic.

IDS and IPS

> Industry-leading signature-based threat detection and prevention (IDS/IPS) engine to automatically stop known malware, spyware, C2 and vulnerability exploits.

URL & FQDN filtering

> Control inbound and outbound HTTP/S traffic to a specified list of FQDN including wild cards and custom URLs.

Flexible Policy Enforcement

> Secure inbound, outboud and lateral network/application traffic.
> Can be enforced on OCI gateways as well as intra-vcn subnet traffic.

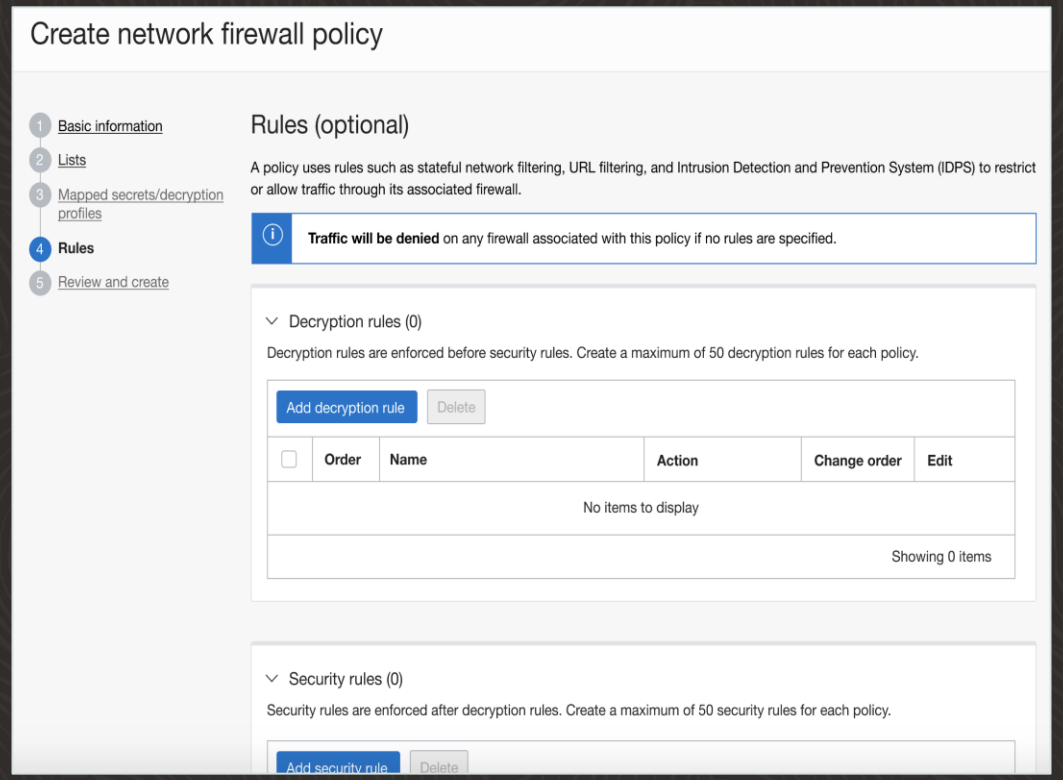
Customer applications

Oracle Cloud Infrastructure

Stateful Firewall Rules

Enforce *allow* or *deny* stateful filtering rules based on 5-tuple information (source and destination IP address (both IPv4 and IPv6), port, and protocol.

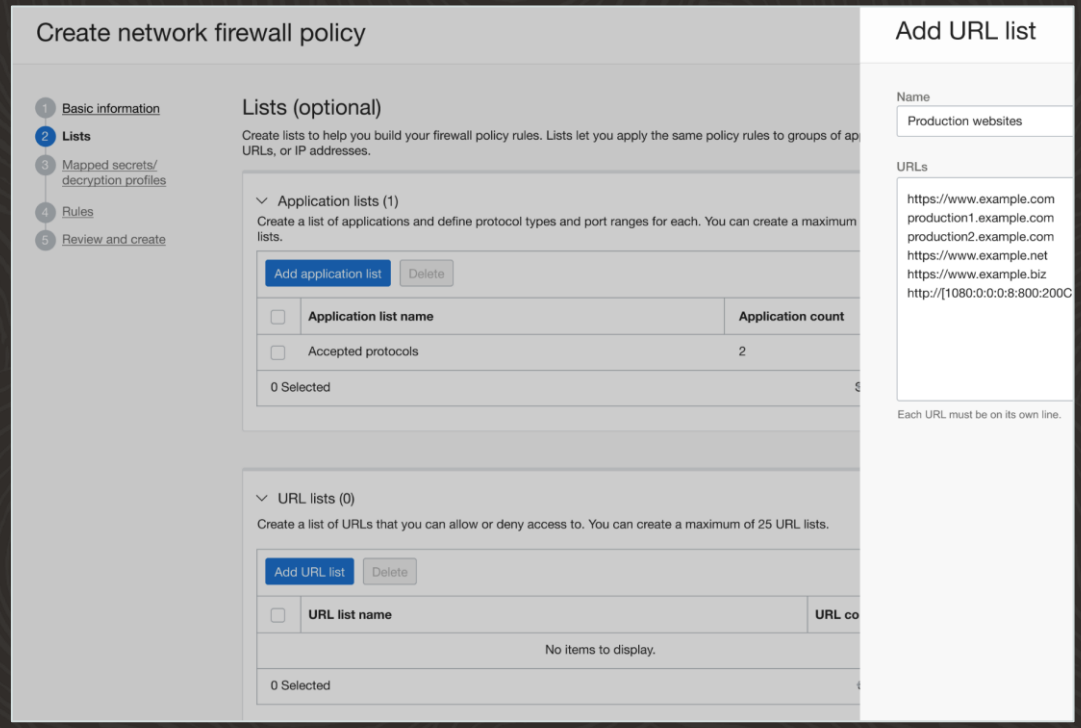
- Rules can be enforced in a customer defined priority order across multiple virtual networks.
- The stateful firewall takes into account the context of traffic flows for more granular policy enforcement.



URL and FQDN Filtering

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.

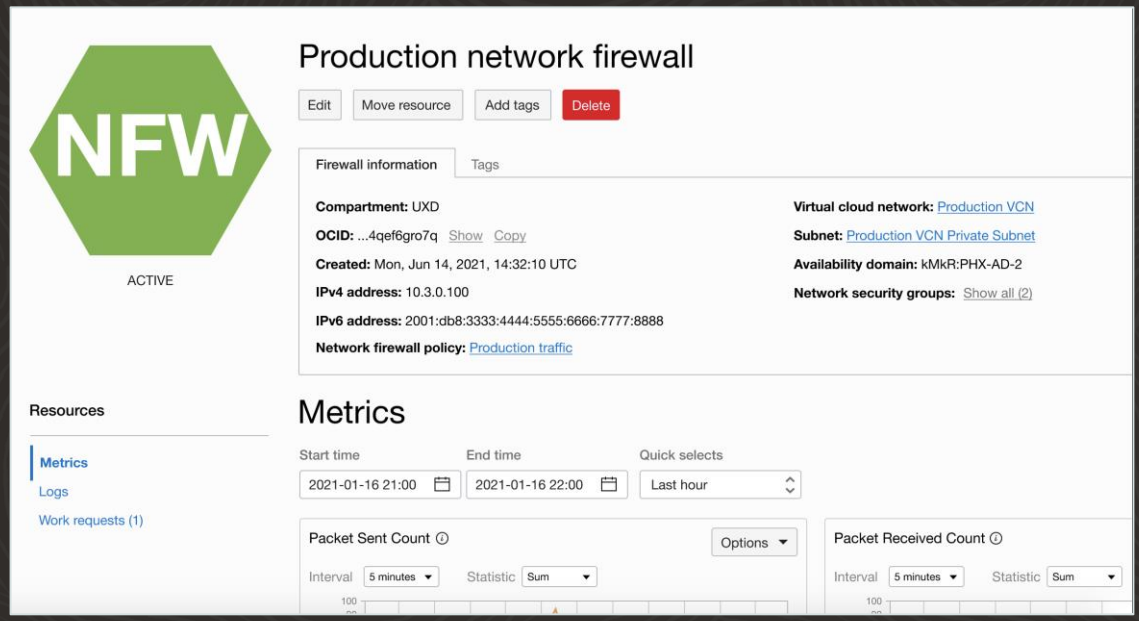


Intrusion Detection and Prevention

- 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.
- Uses App-ID technology to protect against application-layer exploits. App-ID classifies applications and governs per policy regardless of port, protocol, encryption, or evasive techniques.

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 – 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

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.

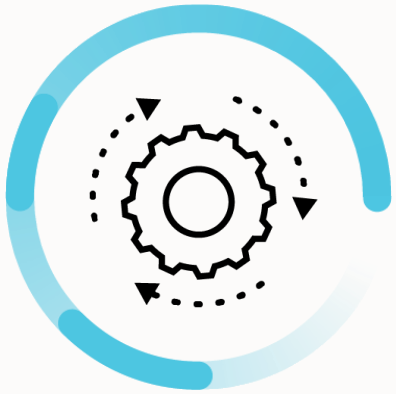
OCI Network Firewall Is...

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

Skill check

1. What is a key difference between the Dynamic Routing Gateway and Local Peering Gateway when implementing Cross-Tenancy Peering?

- The Local Peering Gateway needs the requestor to be in either tenancy.
- The Dynamic Routing Gateway can have a Cross-Tenancy Attachment.
- The Local Peering Gateway can have a Cross-Tenancy Attachment.
- The Dynamic Routing Gateway needs the acceptor to be in either tenancy.

- (•) The Dynamic Routing Gateway can have a Cross-Tenancy Attachment. (*)
- The Local Peering Gateway can have a Cross-Tenancy Attachment.
- The Dynamic Routing Gateway needs the acceptor to be in either tenancy.

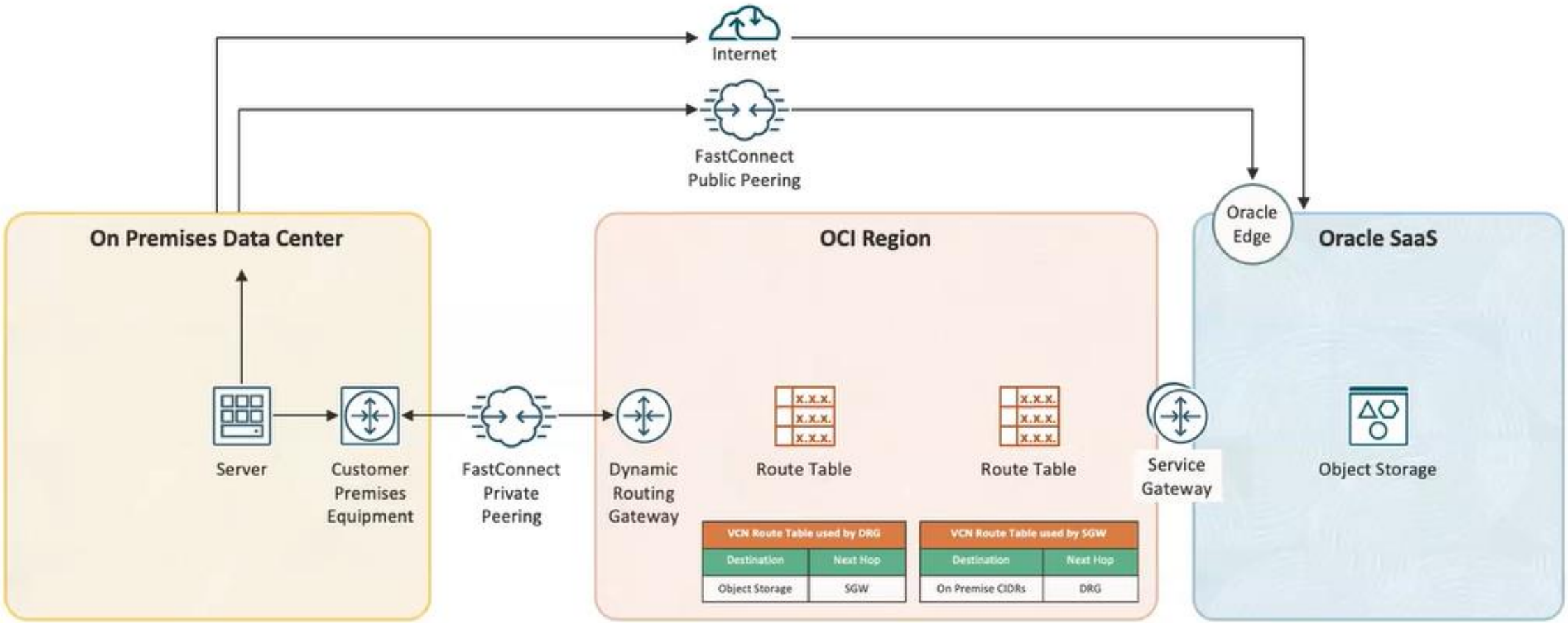
✔Your answer is **Correct**.

Explanation: The DRG can attach VCNs from another tenancy. This attachment type is called Cross-Tenancy Attachment.

ORACLE
Cloud Infrastructure

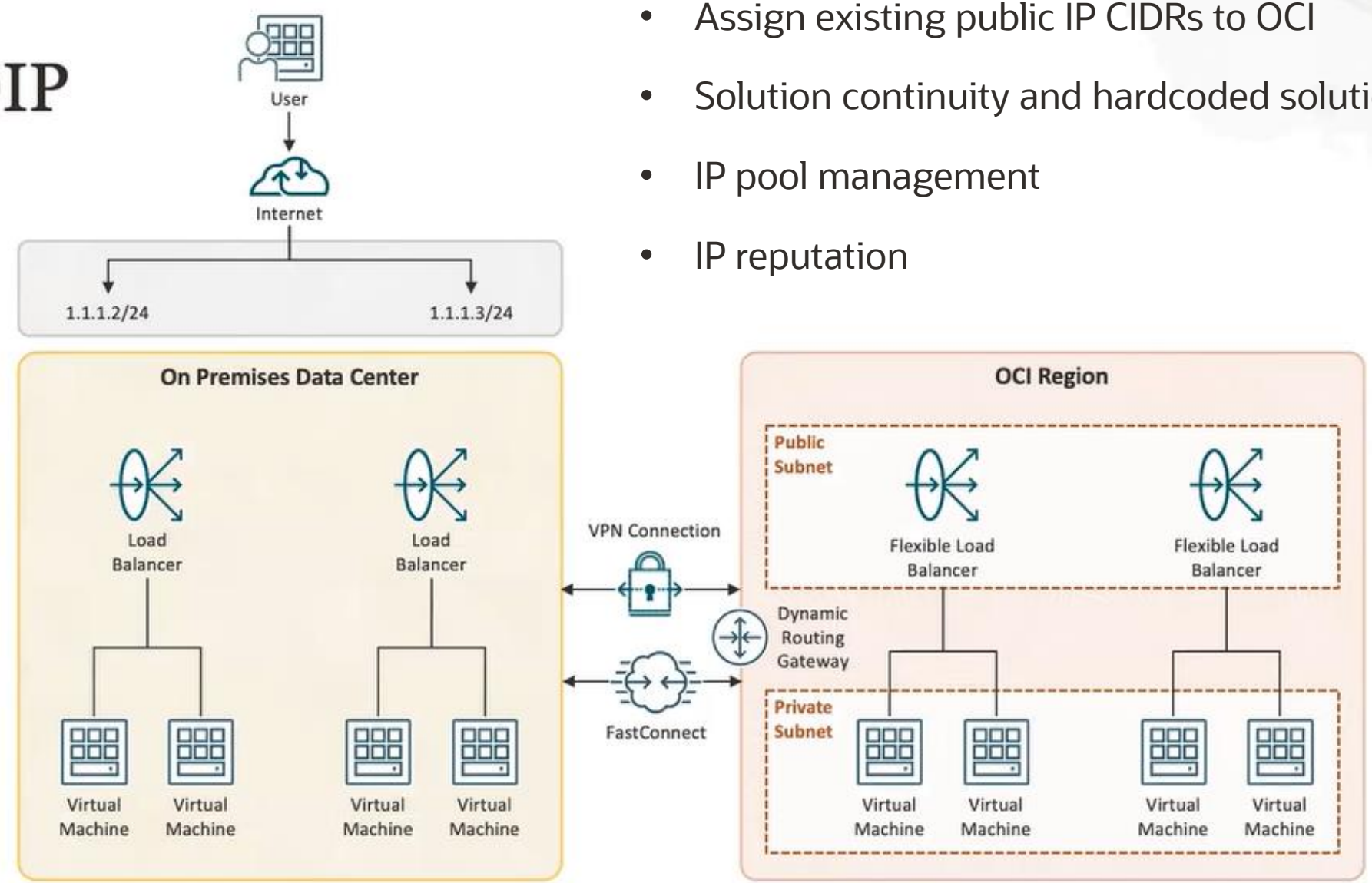
Migrate Workloads

Data Migration



Bring your own IP

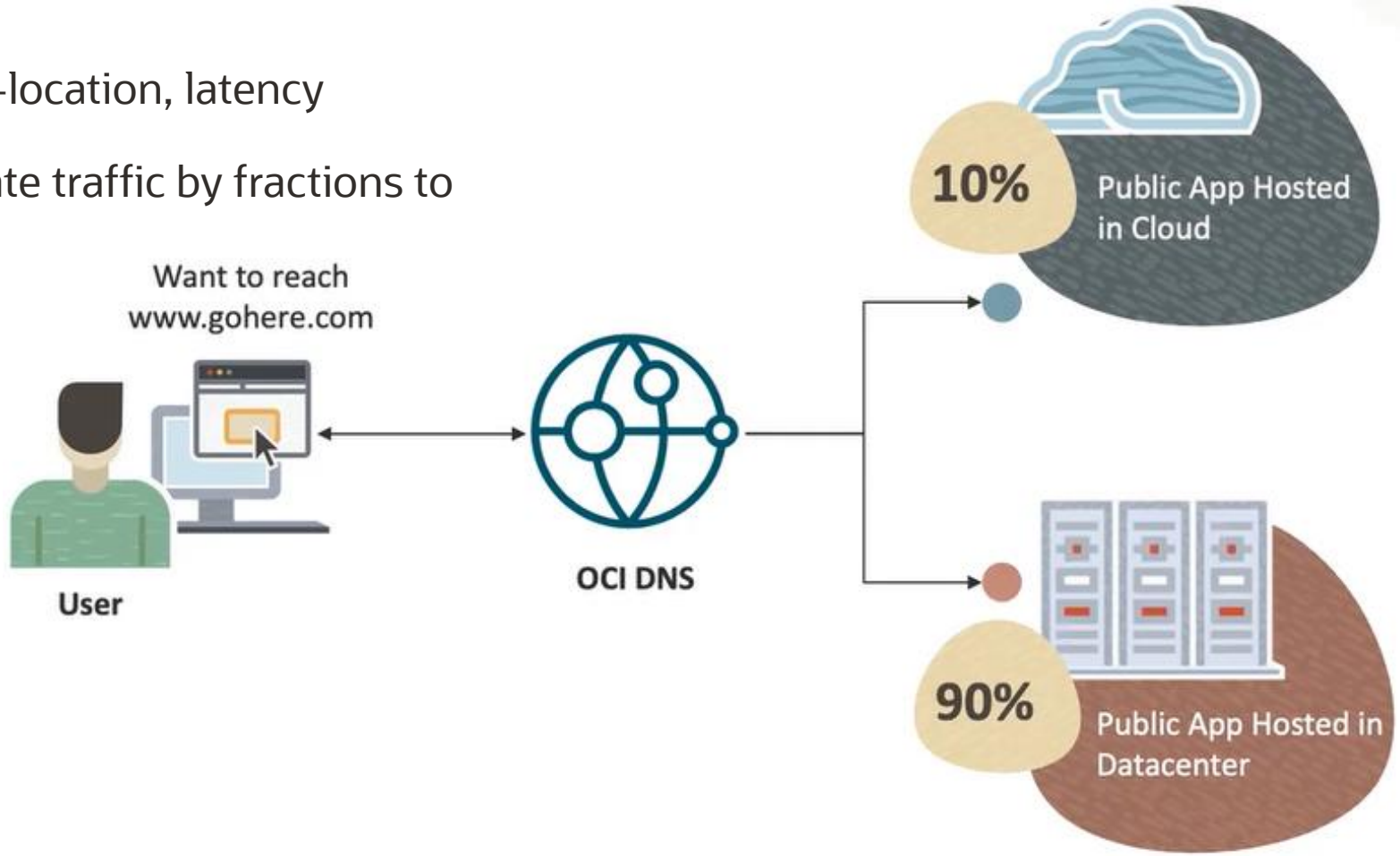
BYOIP



- Assign existing public IP CIDRs to OCI
- Solution continuity and hardcoded solutions
- IP pool management
- IP reputation

DNS

- Create and manage DNS Zones
- OCI DNS can be optimized for GEO-location, latency
- Utilize ratio load balancing to migrate traffic by fractions to new cloud environments
- Gradually migrate

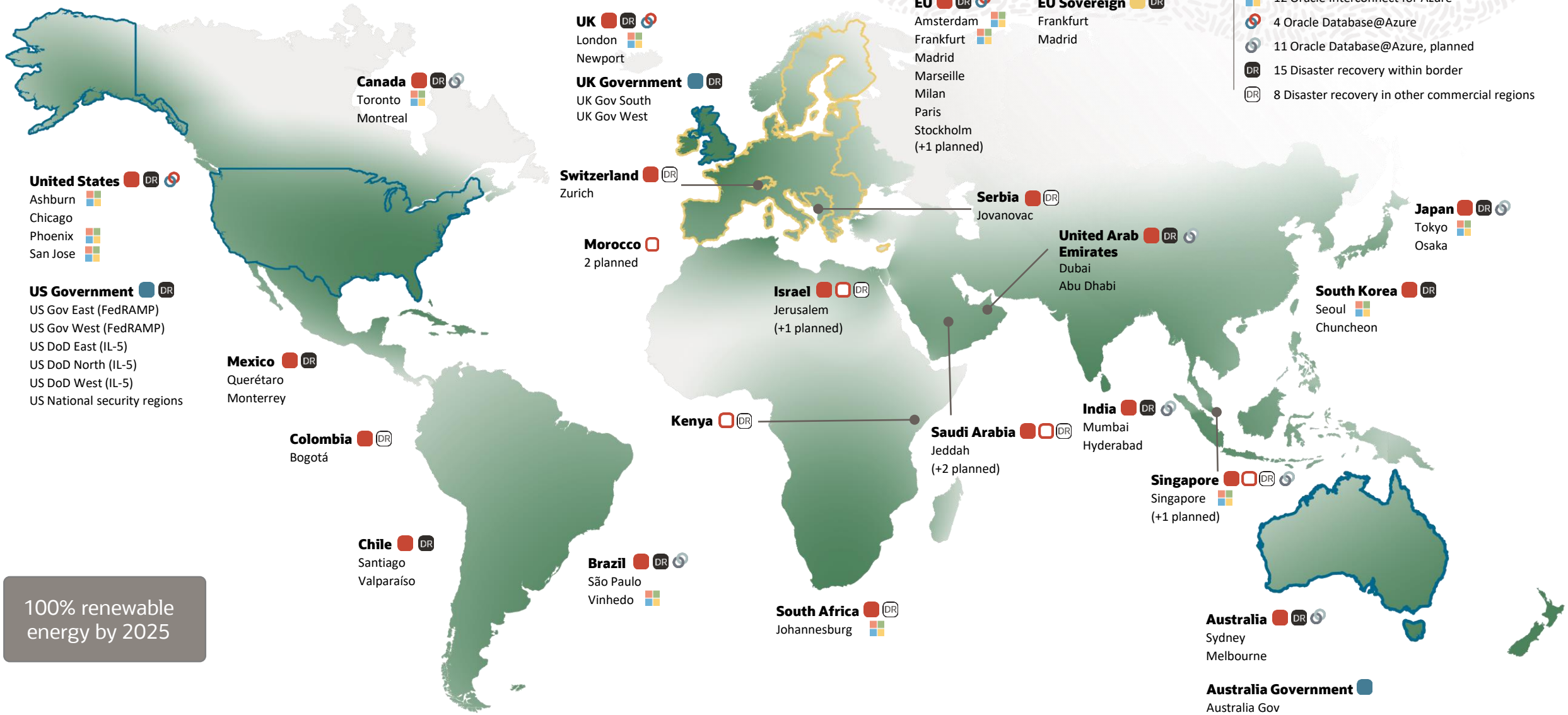


ORACLE
Cloud Infrastructure

Troubleshooting Tools

Oracle Cloud Infrastructure global footprint – 72 regions

June 2024 – 48 public regions, 24 Dedicated, Alloy, Multicloud and secret regions



100% renewable energy by 2025

Tools

- Inter region latency
- Networking visualizer
- VTAP
- Flow logs

Skill check

1. Why is the Oracle Cloud Infrastructure (OCI) Jovanovac Region in Serbia not listed in the Inter-Region Latency dashboard?

- ○ The Oracle Services Network does not reach the OCI Jovanovac region. Therefore, it is not possible to monitor the latency with the rest of the OCI regions.
- ○ There is no such region in Oracle Cloud Infrastructure.
- ○ This region exists within a unique realm and Oracle does not provide the tools to connect regions across a realm boundary via the OCI network backbone.
- ○ There are no FastConnect partners in the OCI Jovanovac region.

- ● This region exists within a unique realm and Oracle does not provide the tools to connect regions across a realm boundary via the OCI network backbone. (*)
- ○ There are no FastConnect partners in the OCI Jovanovac region.

✔Your answer is **Correct**.

Explanation: This region exists within a unique realm and Oracle does not provide the tools to connect regions across a realm boundary via the OCI network backbone. The realm key is OC20.

Skill check

2. As an IT professional managing resources in Oracle Cloud Infrastructure (OCI), you are exploring tools to gain insights into your network architecture and the relationships between different components. Which option accurately describes OCI Network Visualizer?

- ○ OCI Network Visualizer is a performance monitoring tool focused on tracking the CPU and memory usage of individual instances within a Virtual Cloud Network (VCN).
- ○ OCI Network Visualizer is a feature that automatically deploys and configures load balancers for optimal traffic distribution in your VCN.
- ○ OCI Network Visualizer is a tool that provides a visual representation of your VCN, including subnets, instances, and their interconnections, helping you understand and manage your network topology.
- ○ OCI Network Visualizer is a graphical user interface for managing security groups within an OCI tenancy.

- ● OCI Network Visualizer is a tool that provides a visual representation of your VCN, including subnets, instances, and their interconnections, helping you understand and manage your network topology. (*)
- ○ OCI Network Visualizer is a graphical user interface for managing security groups within an OCI tenancy.

✔Your answer is **Correct**.

Explanation: OCI Network Visualizer is a tool that provides a visual representation of your VCN, including subnets, instances, and their interconnections, helping you understand and manage your network topology.

TechKnowledge Enablement & DEVs

Certification: OCI Networking Professional 2024

Oracle University:

→ Become an OCI Networking Professional (2024)

Practice Labs

→ Access LiveLabs

→ Oracle Cloud Infrastructure Networking Professional 2024 Practice Exam


ORACLE