ORACLE

Virtual Cloud Network

Level 200

Harshit Agarwal
Oracle Cloud Infrastructure
September 2019

Safe harbor statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions.

The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Objectives

- Part 0: Virtual Cloud Network (VCN) L100 Recap
- Part I : connect resources in different VCNs – Local Peering & Remote Peering
- Part II: Transit Routing Scenarios
  a) Access to multiple VCNs in the same region
  b) Private access to Oracle services
- Part III: Deploy Virtual Firewall on OCI
    - Juniper vSRX FW
    - Fortinet Fortigate NGFW
    - Palo Alto VM-series FW

ORACLE

Part I: VCN Peering - Local Peering & Remote Peering

VCN Peering

- Enables connectivity between the resources in different VCNs
- Does not require public IPs or NAT to enable connectivity
- Traffic never leaves the Oracle Network
- Over other options such as connecting over the internet, VCN Peering offers
  - Faster connectivity
  - Higher security

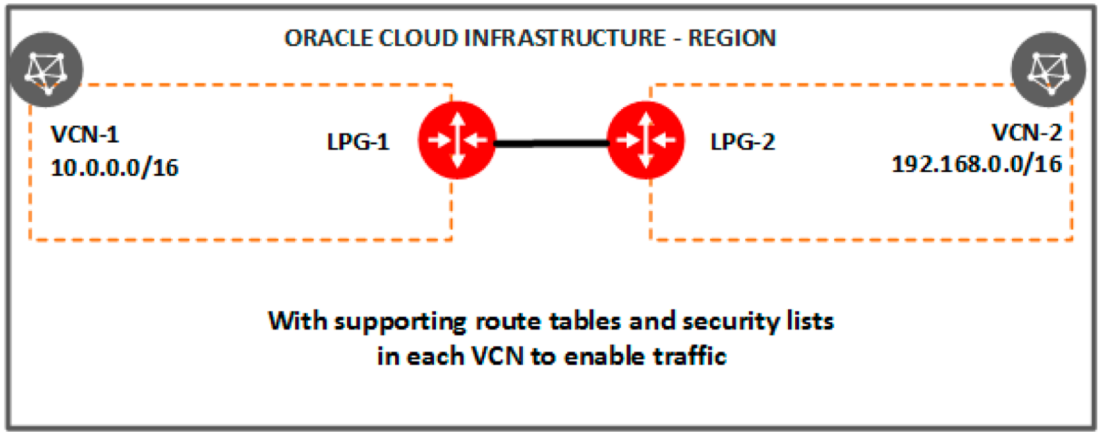
- Types of VCN Peering available
  - Local Peering (In-region)
  - Remote Peering (Cross-region)

Local VCN Peering – connecting VCNs in the same region

- Connecting two VCNs 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)

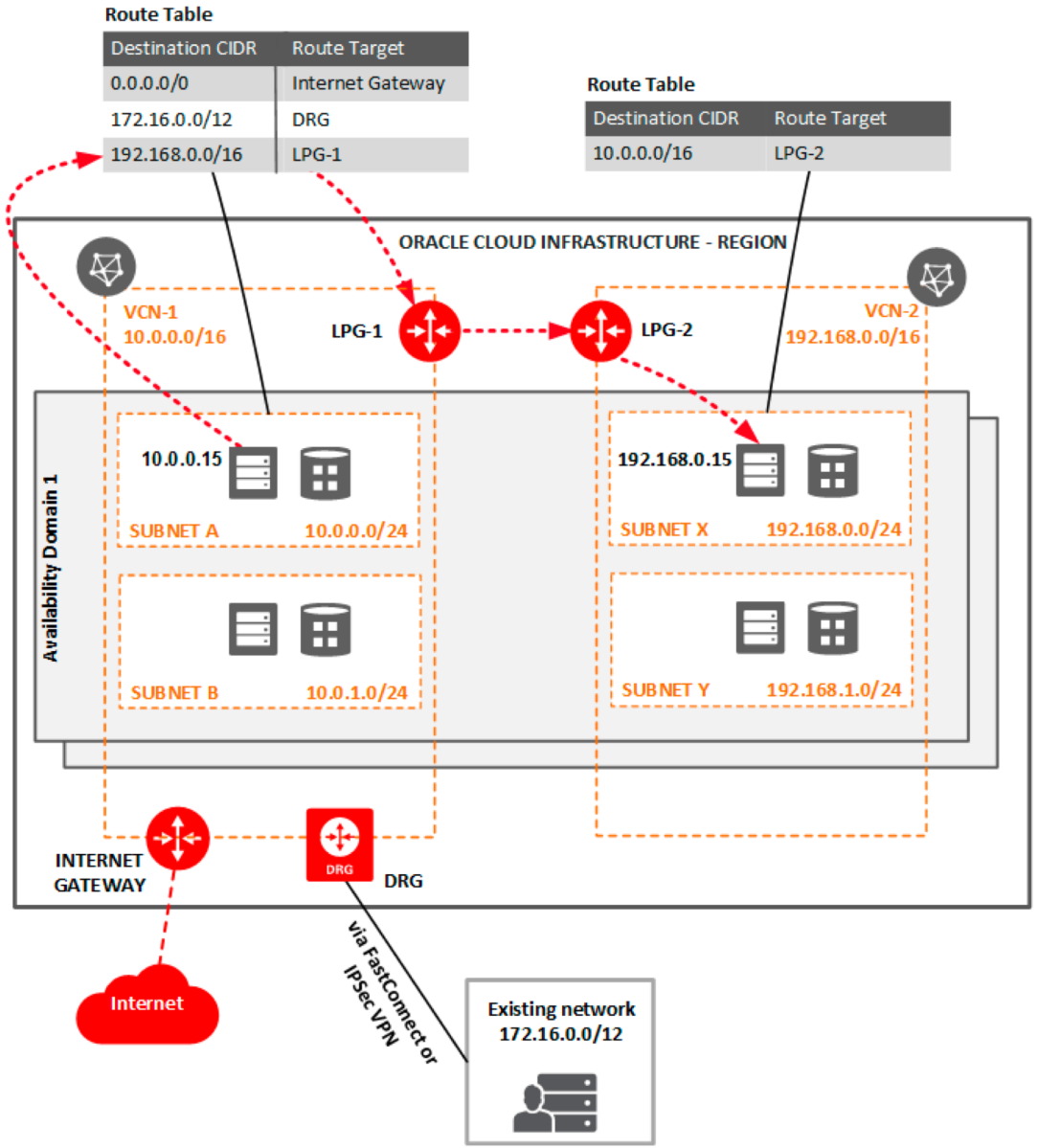
Local Peering Gateway (LPG)

- 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



Local VCN Peering

- Create Local Peering Gateway in each VCN
- Have required IAM policies to establish connection
- Establish connection across LPGs
- Update the Route Table
- Update the Security List
- Test Connectivity

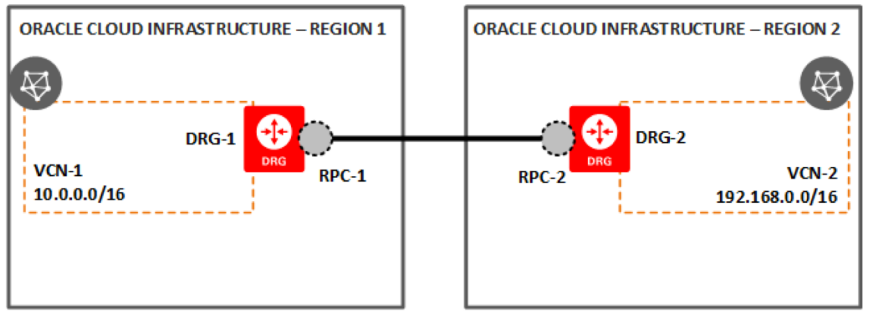


Remote VCN Peering – connecting VCNs in the different region

- Traffic flows between regions through the OCI backbone network
- The two VCNs in the peering relationship must not have overlapping CIDRs
- Requires a DRG to set up the Remote Peering connection; vNIC of one VCN instance forwards traffic to its DRG, which forwards traffic to peer DRG in other region over backbone
- Enables features such as data replication across regions

Remote Peering Connection (RPC)

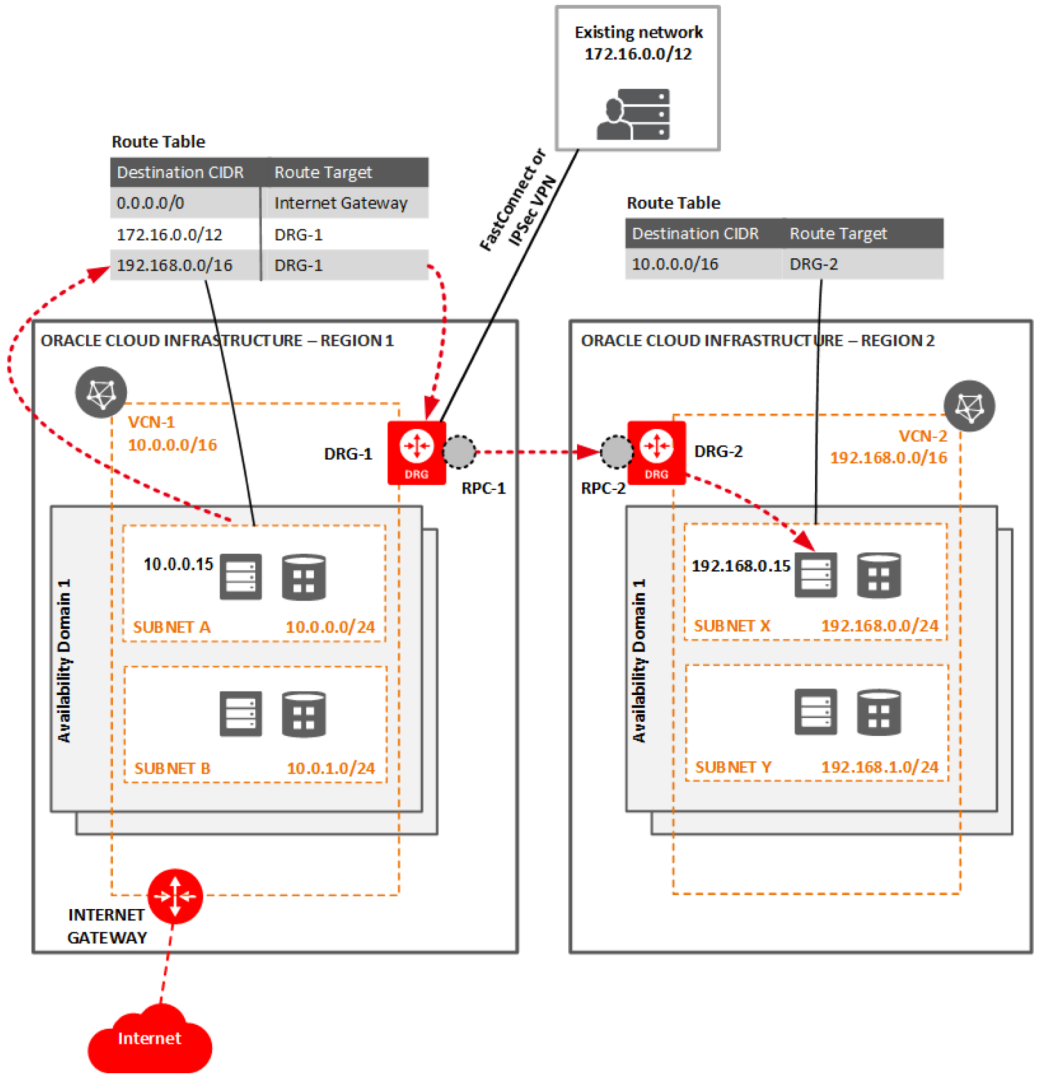
- Like Virtual Circuits, the Remote Peering Connection is a component of DRG
- RPCs of two DRGs from two regions are connected to create a peering relationship



With supporting route tables and security lists in each VCN to enable traffic

Remote VCN Peering

- Existing DRG and attached to a VCN
- Have required IAM policies to establish connection
- Establish connection across DRGs
- Update the Route Table
- Update the Security List
- Test Connectivity



Things to remember for VCN Peering!

- With IAM policies, you can control:
  - Who can subscribe your tenancy to another region (required for remote VCN peering).
  - Who in your organization has the authority to establish VCN peerings.
  - Who can manage route tables and security lists.
- Once the peering connection has been established
  - control the packet flow over the connection with route tables in your VCN
  - control the packet flow over the connection with security lists in your VCN
  - ensure that all outbound and inbound traffic with the other VCN is intended/expected and well defined
  - implement security list rules that explicitly state the types of traffic your VCN can send to the other and accept from the other.
- If you're concerned about high levels of network traffic coming to your VCN, consider using stateless security list rules to limit the level of connection tracking your VCN must perform.

ORACLE

Part II: Transit Routing Scenarios

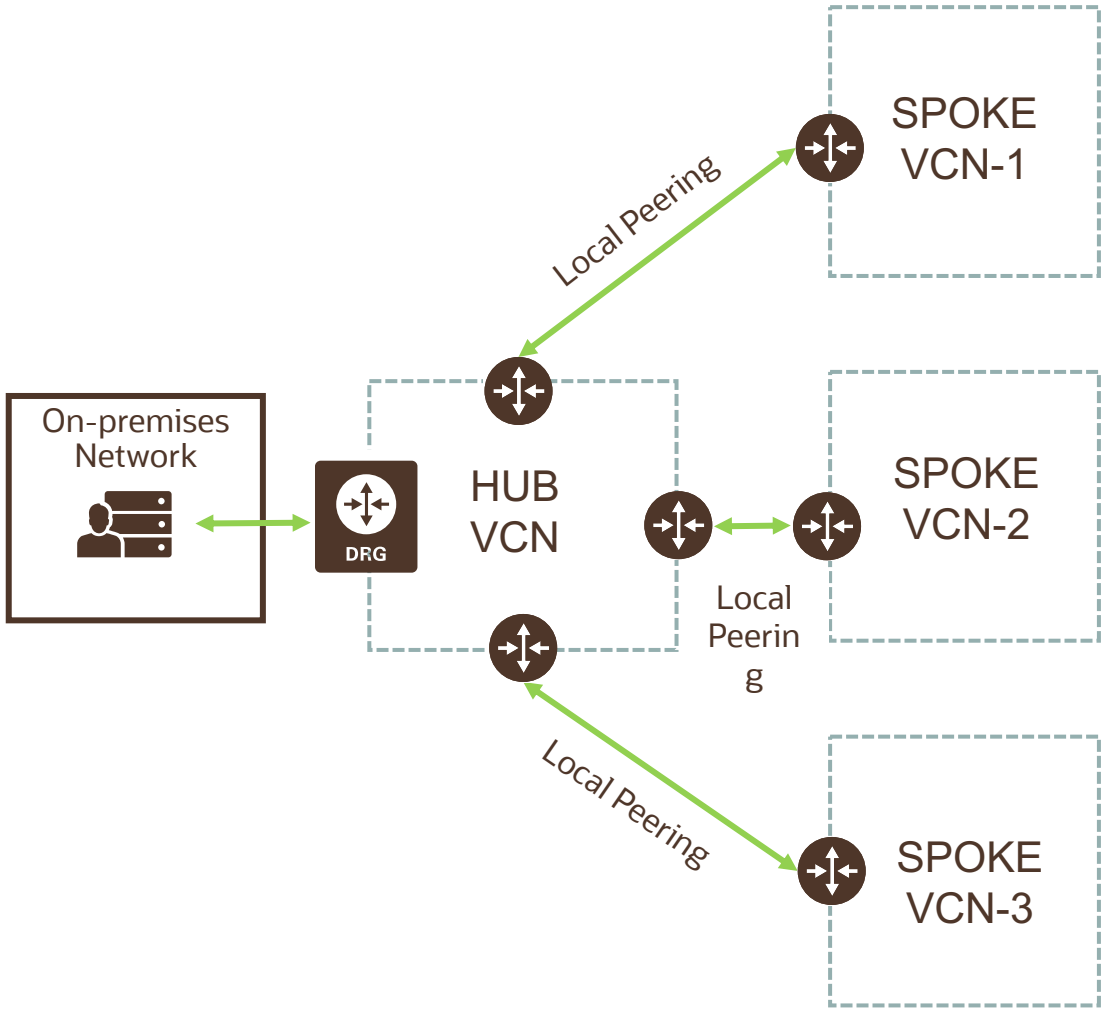
Transit Routing Scenarios

There are two primary transit routing scenarios :

- **Access to multiple VCNs in the same region:** This scenario enables communication between your on-premises network and multiple VCNs in the same region over a single FastConnect private virtual circuit or VPN Connect.

- **Private access to Oracle services:** This scenario gives your on-premises network *private access* to Oracle services, so that your on-premises hosts can use their private IP addresses and the traffic does not go over the internet.

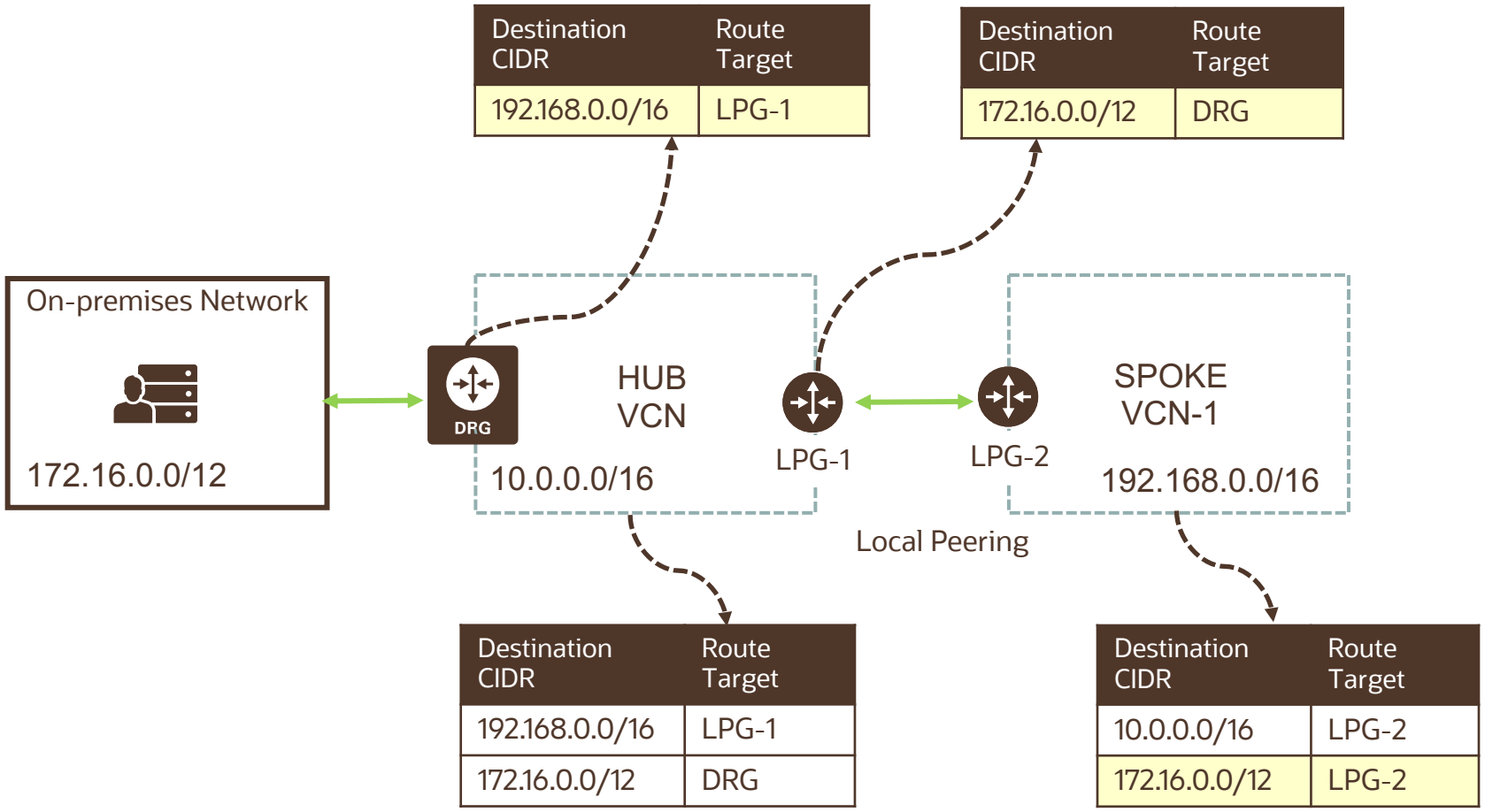
Transit Routing: Access to multiple VCNs



One of the VCNs acts as the hub and connects to on-premises network. The other VCNs are locally peered with the Hub VCN. The traffic between the on-premises network and the peered VCNs transits through the hub VCN.

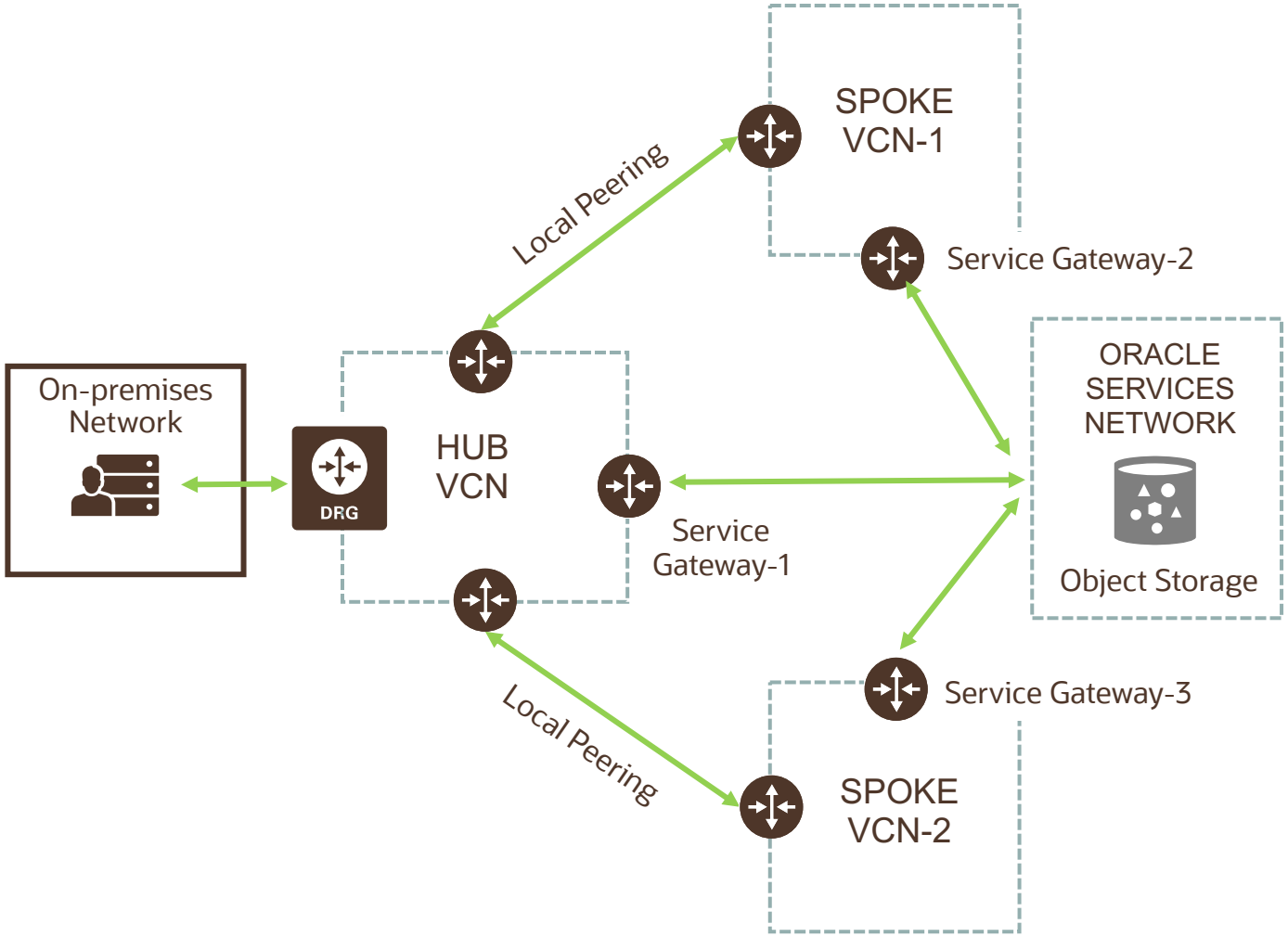
The VCNs must be in the same region but can be in different tenancies.

Transit Routing: Access to multiple VCNs



- A route table that is associated with a DRG can have only rules that target an LPG or a private IP
- A route table that is associated with an LPG can have only rules that target a DRG or a private IP
- DRG or LPG can exist without route table associated with it

Transit Routing: Private Access to Oracle services



On-premises network has private access to Oracle services in the Oracle Services Network. The hosts in the on-premises network communicate with their private IP addresses

The on-premises network can reach the Oracle services only through a single VCN's Service gateway (the one dedicated for this purpose, SG-1) and not through the service gateways of the other VCNs (SG-2,3).

For those other VCNs, only the resources inside those VCNs can reach Oracle services through their VCN's service gateway.

Transit Routing: Private Access to Oracle services

There are two options for routing through the VCN for private access to Oracle services:

- **Transit routing directly through gateways:** You route the traffic directly through the VCN, from one gateway to the other.
- **Transit routing through a private IP:** You set up an instance in the VCN to filter or inspect the traffic between the on-premises network and Oracle Services Network, and route traffic through a private IP on the instance.

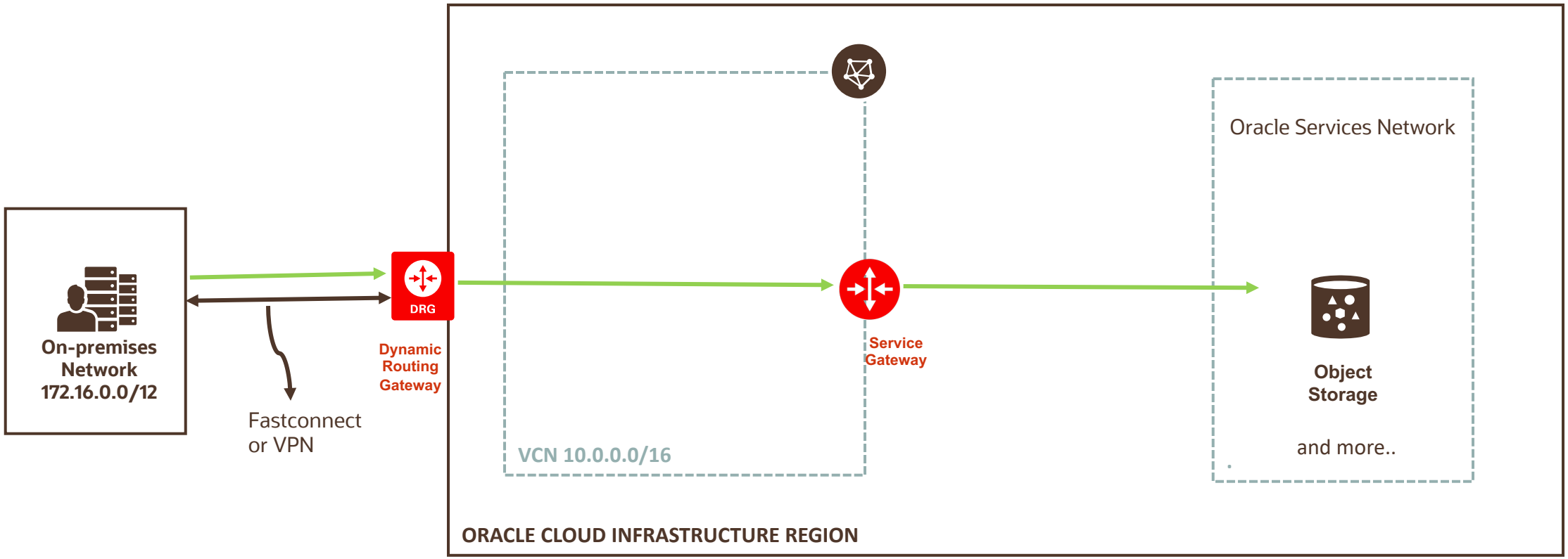
Transit Routing directly through gateways for Private Access to Oracle Services

Route Table associated with DRG

Destination CIDR	Route Target
All Services in Region	Service Gateway

Route Table associated with Service Gateway

Destination CIDR	Route Target
172.16.0.0/12	DRG



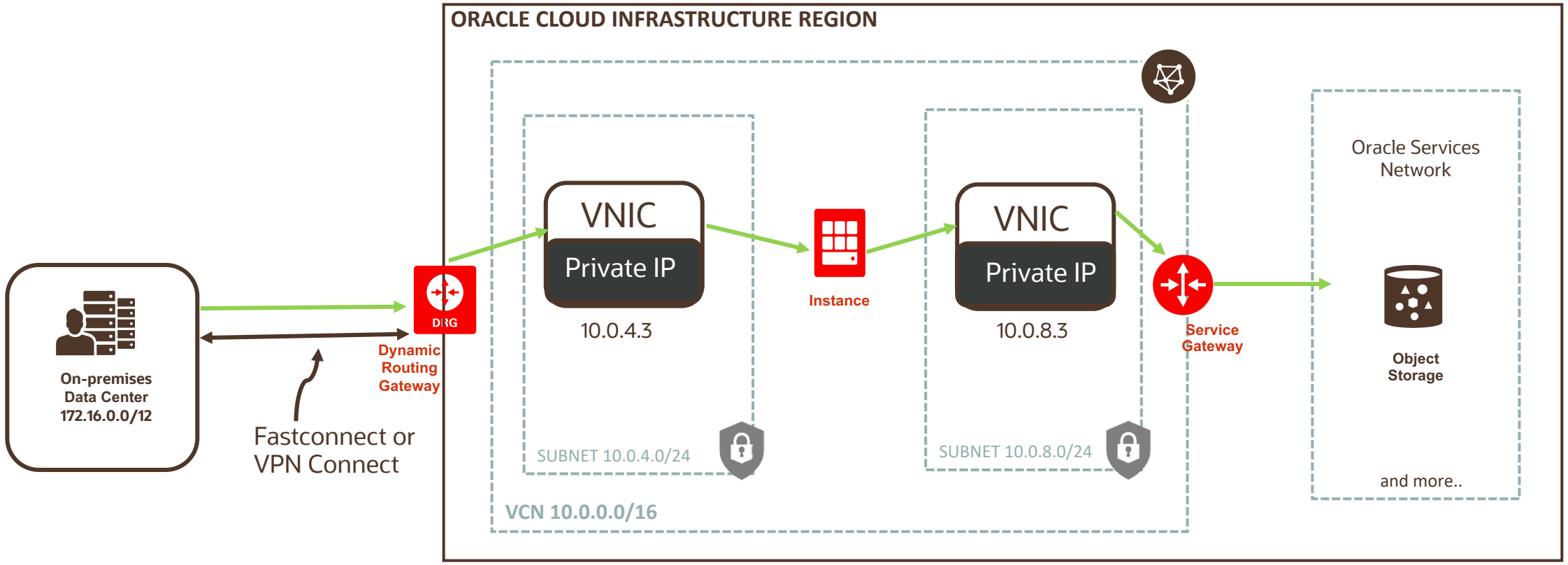
Transit Routing through a Private IP for Private Access to Oracle Services

Route Table associated with DRG

Destination CIDR	Route Target
All Services in Region	10.0.4.3

Route Table associated with Service gateway

Destination CIDR	Route Target
172.16.0.0/12	10.0.8.3



Route Table associated with subnet-frontend

Destination CIDR	Route Target
172.16.0.0/12	DRG

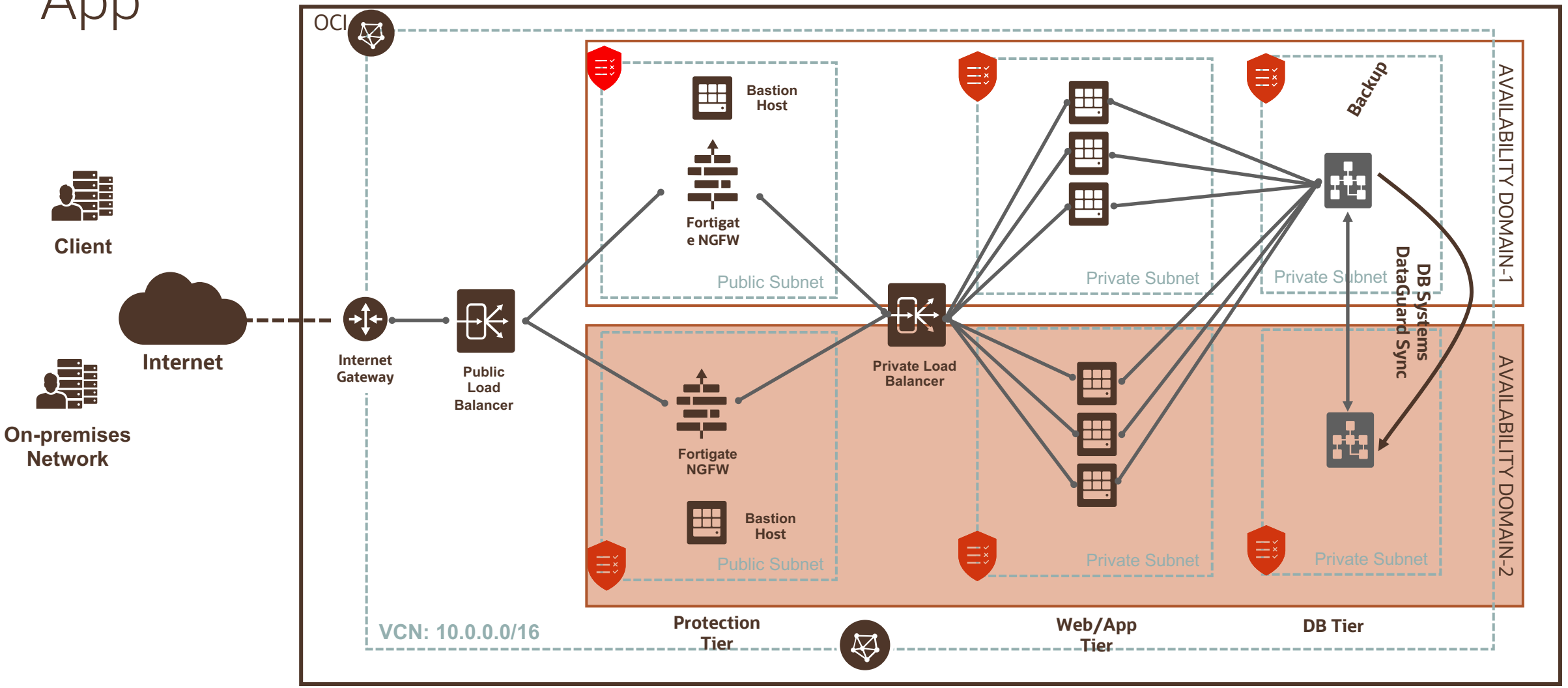
Route Table associated with subnet-Backend

Destination CIDR	Route Target
All Services in Region	Service Gateway

ORACLE

Part III: Deploy Virtual firewall on OCI

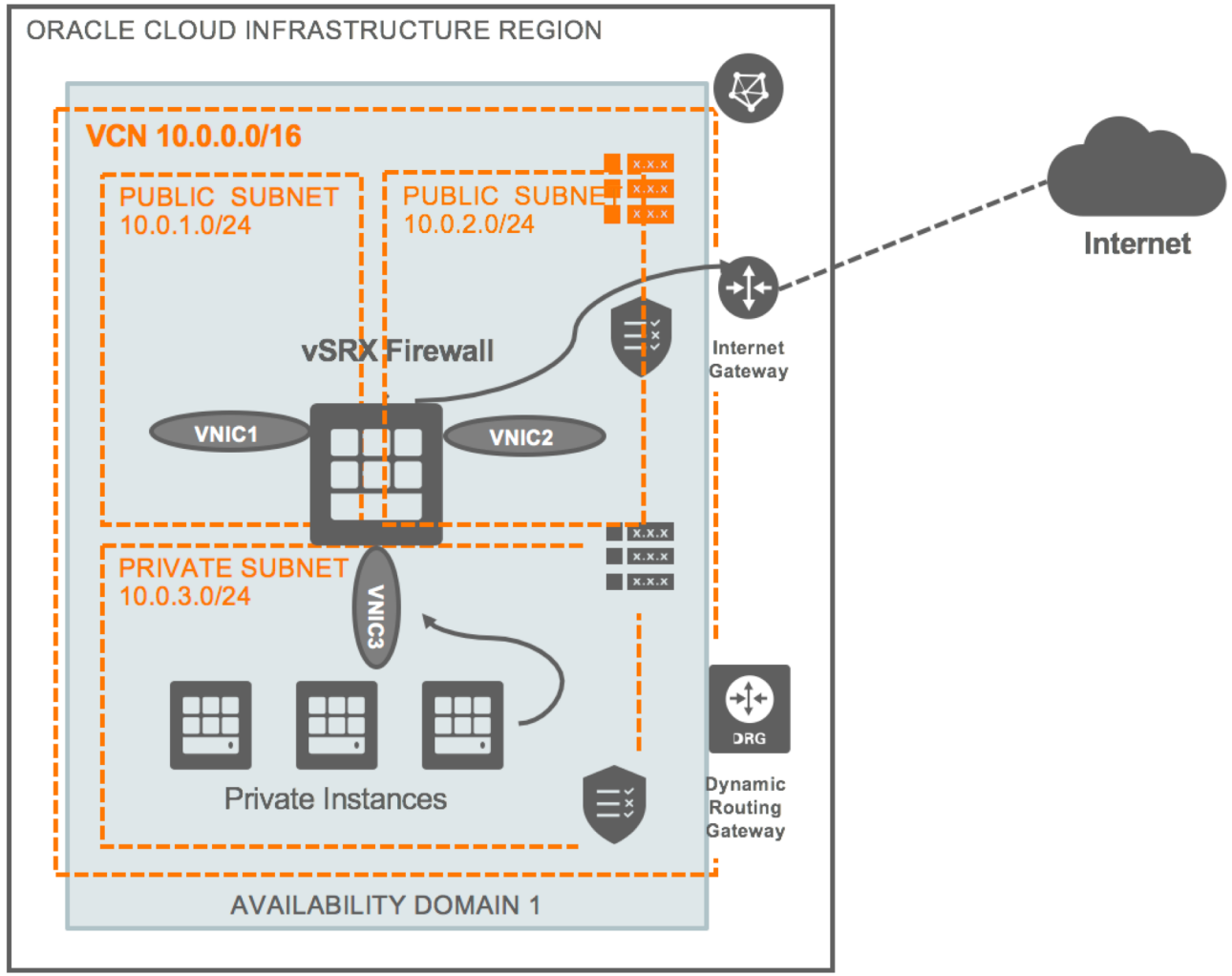
Virtual Firewall Instances – Fortigate NGFW with a Two Tier App



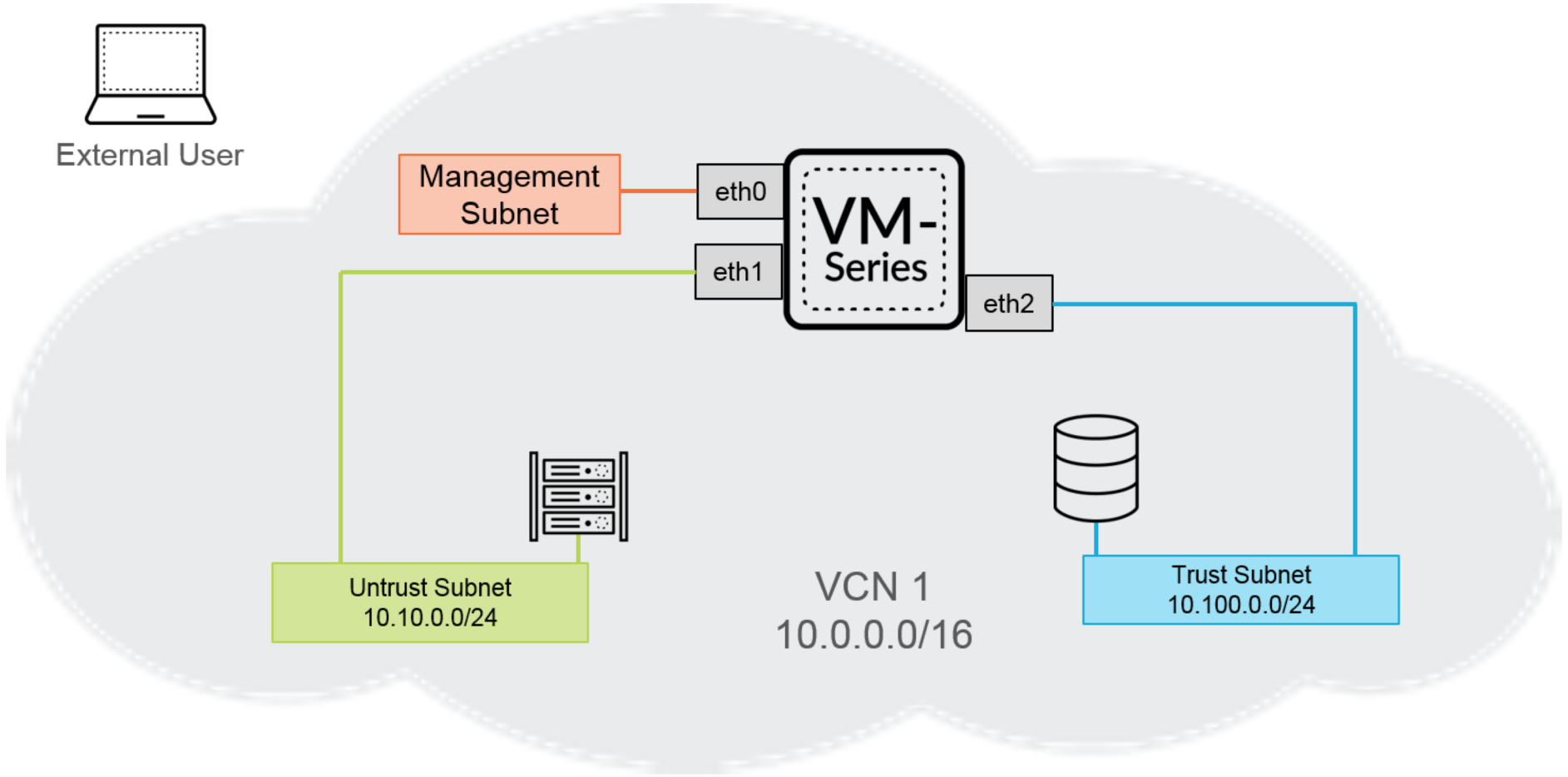
[OCI Blog on Fortigate NGFW]

Using vSRX as a Virtual Firewall/Nat Device

- vSRX provide benefits like stateful firewall protection, and application and content security features like IPS, antivirus, web filtering, and antispam
- High Level workflow
  - Create VCN and three subnets as shown in the figure
  - Import vSRX image and launch a vSRX compute instance in VCN
  - Attach additional vNICs in each subnet
  - Use Instance console connection to setup vSRX
- Following blog post provides details on how to setup a vSRX on OCI - https://blogs.oracle.com/cloud-infrastructure/how-to-deploy-a-virtual-firewall-appliance-on-oracle-cloud-infrastructure

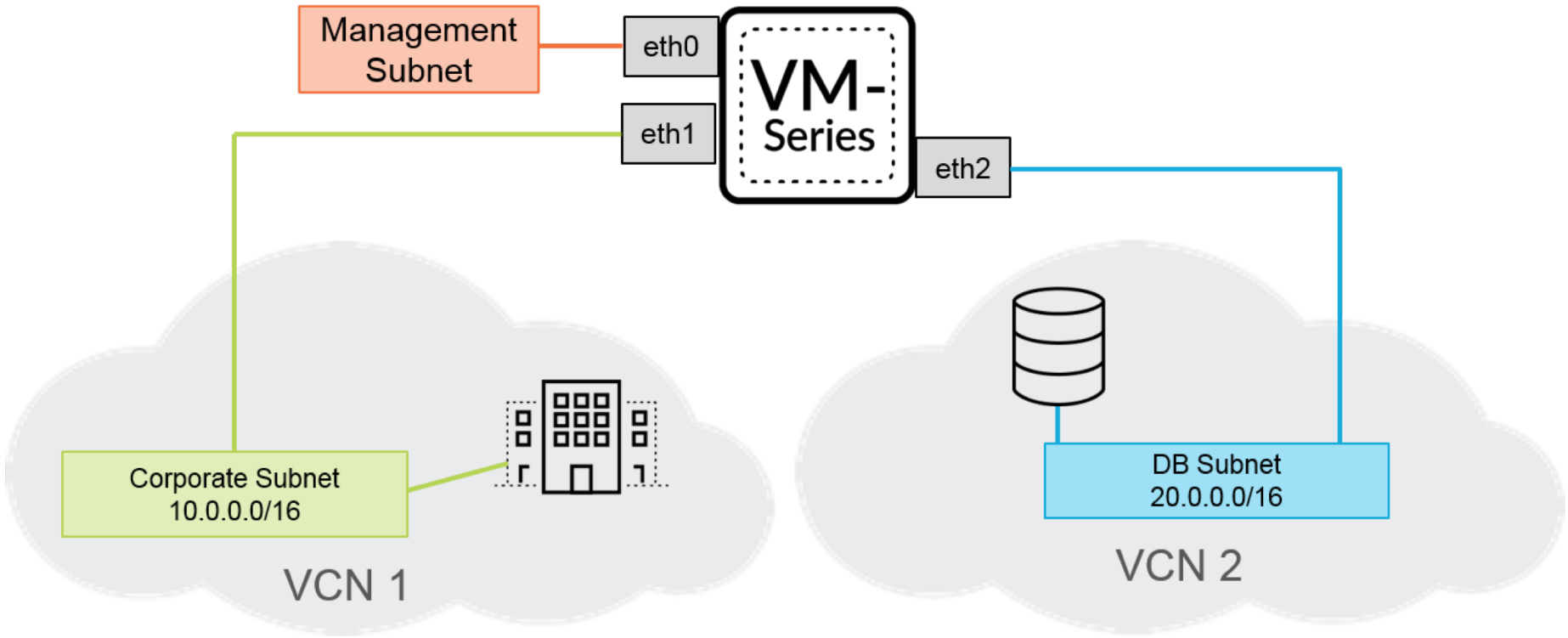


Palo Alto VM-Series Firewall on OCI



North-South Traffic

Palo Alto VM-Series Firewall on OCI (cont..)



Inter-VCN Traffic (East-West)

ORACLE

Oracle Cloud always free tier:
oracle.com/cloud/free/

OCI training and certification:
oracle.com/cloud/iaas/training
oracle.com/cloud/iaas/training/certification
education.oracle.com/oracle-certification-path

OCI hands-on labs:
ocitraining.qloudable.com/provider/oracle

Oracle learning library videos on YouTube:
youtube.com/user/OracleLearning