OCI Networking Gateways

Internet Gateway

ORACLE CLOUD DATA CENTER REGION

Availability Domain – AD1

Instance with public IP
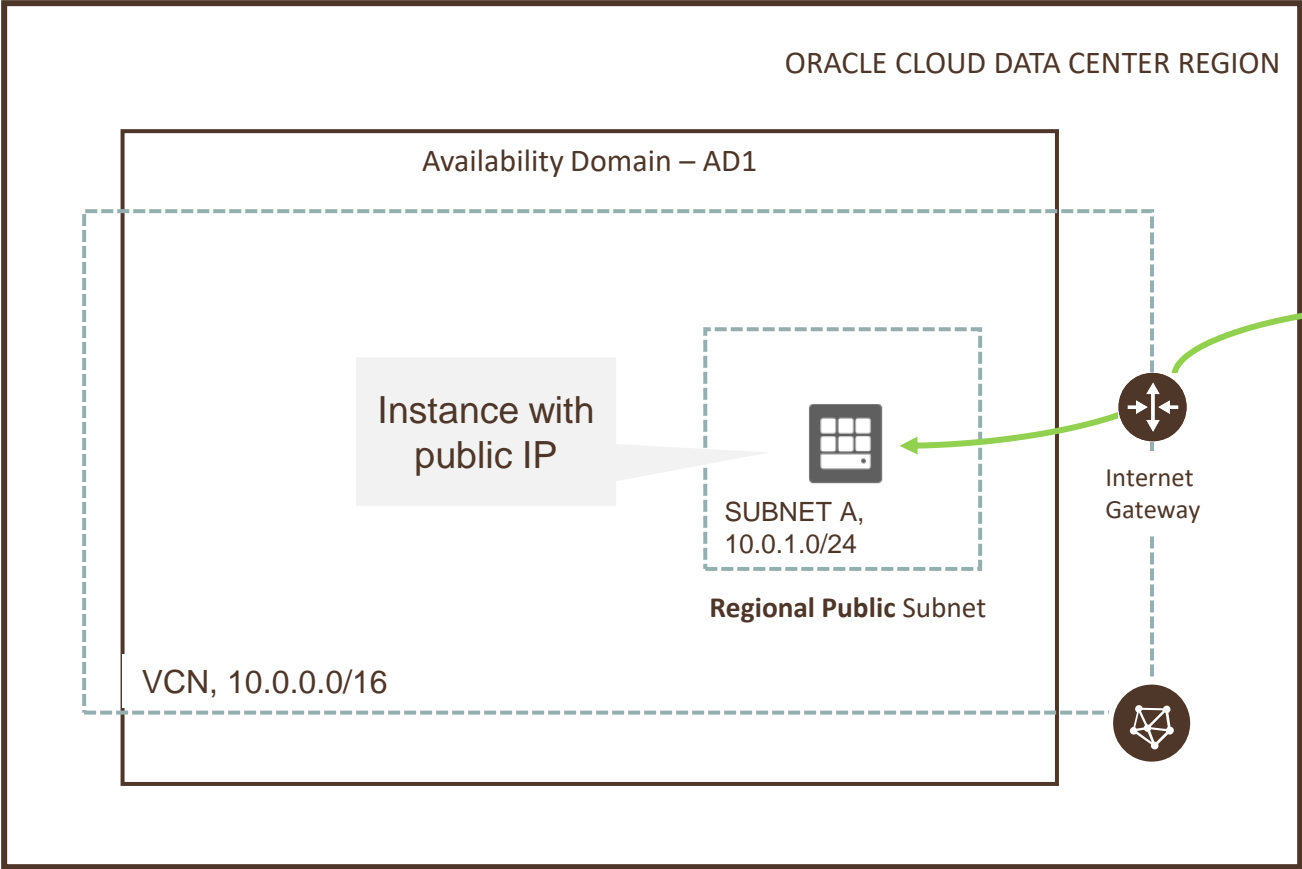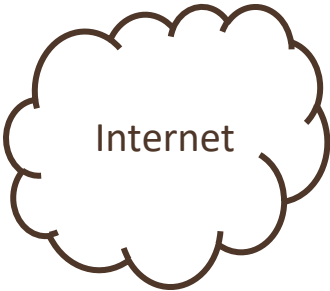
SUBNET A, 10.0.1.0/24

Regional Public Subnet
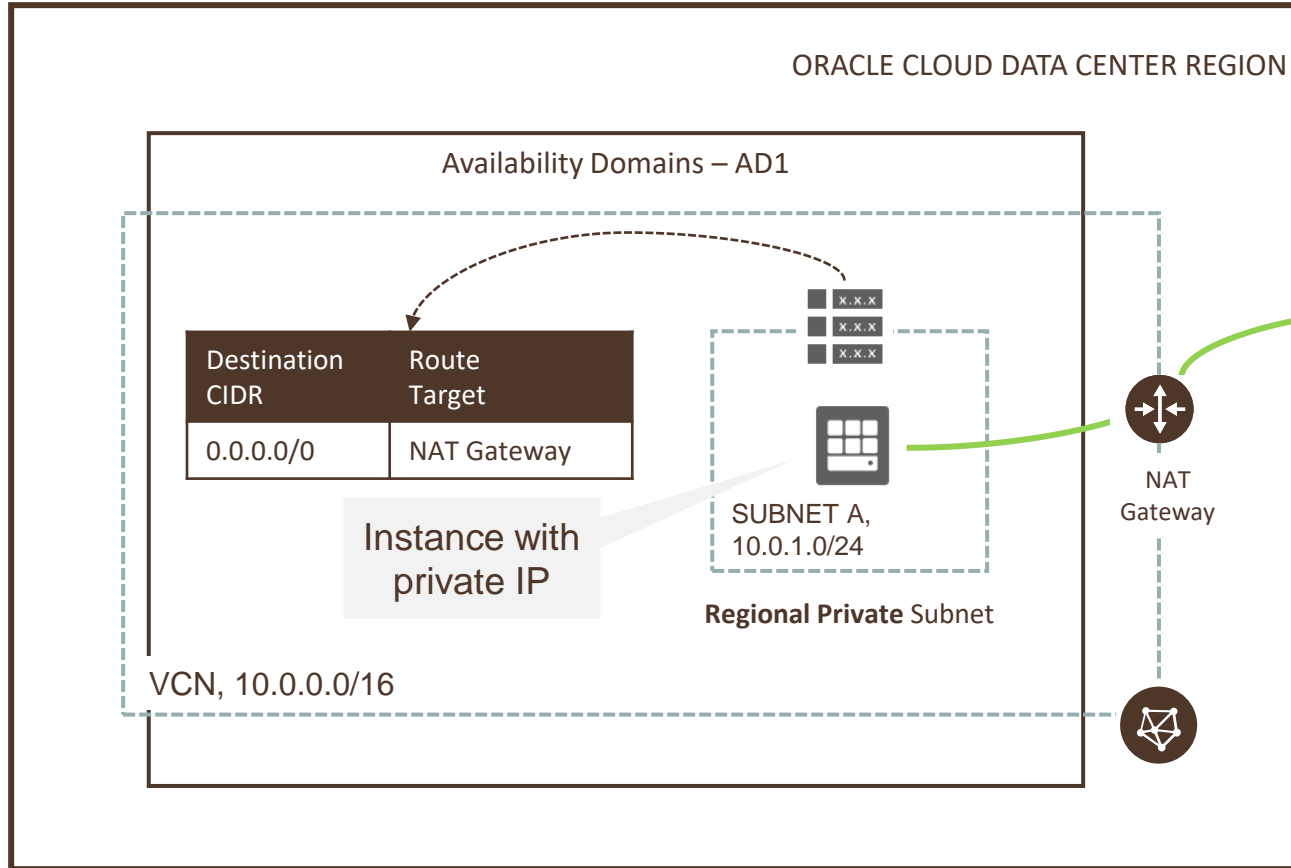
VCN, 10.0.0.0/16

Internet Gateway

Internet

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

NAT Gateway

ORACLE CLOUD DATA CENTER REGION

Availability Domains – AD1

Destination CIDR	Route Target
0.0.0.0/0	NAT Gateway

Instance with private IP

SUBNET A, 10.0.1.0/24

Regional Private Subnet

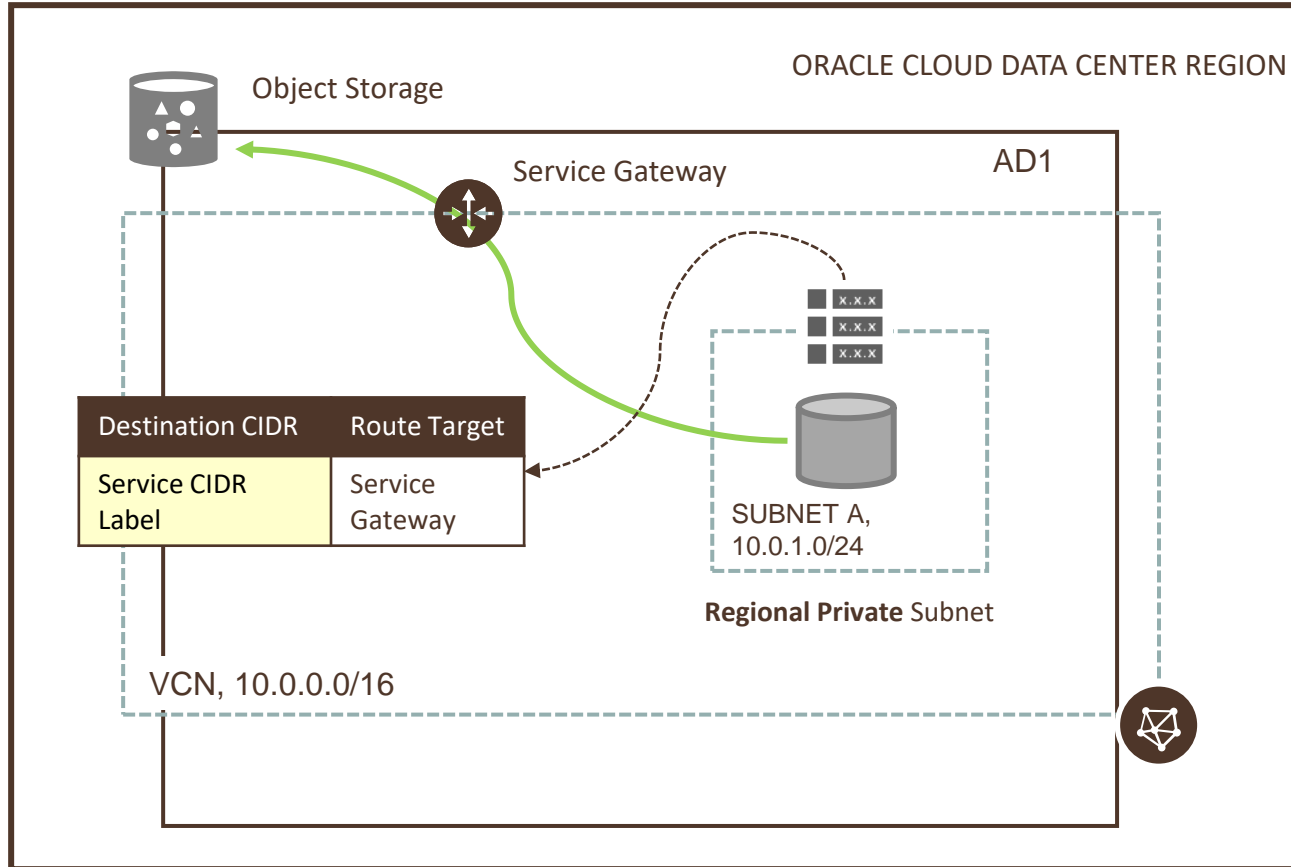VCN, 10.0.0.0/16

NAT Gateway

Internet

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

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

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

Service Gateway

ORACLE CLOUD DATA CENTER REGION

Object Storage

Service Gateway

AD1

Destination CIDR	Route Target
Service CIDR Label	Service Gateway

SUBNET A, 10.0.1.0/24
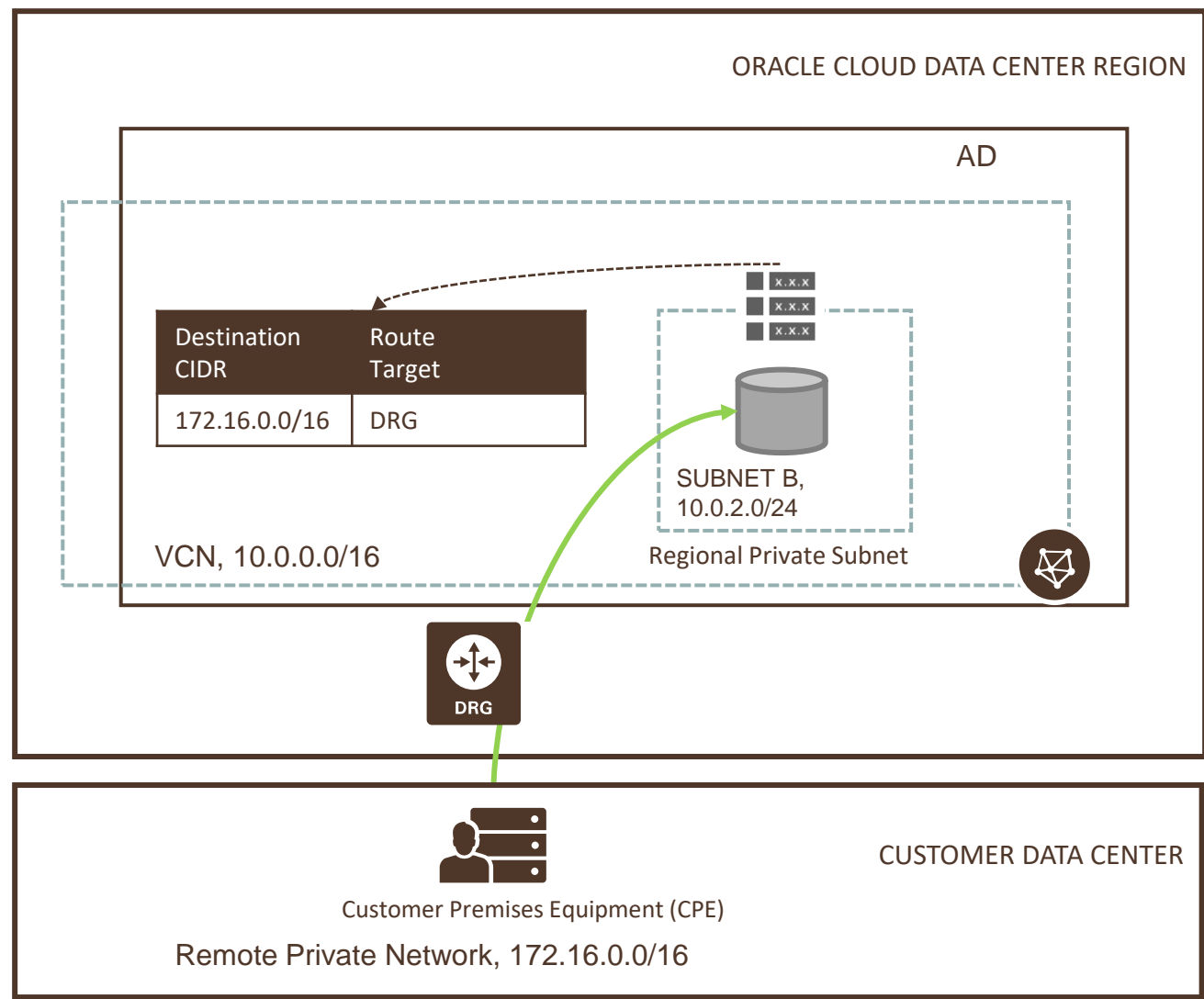
Regional Private Subnet

VCN, 10.0.0.0/16

Service gateway lets resources in VCN access public OCI services, exposed on the Oracle Services Network, 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

Dynamic Routing Gateway

ORACLE CLOUD DATA CENTER REGION

AD

Destination CIDR	Route Target
172.16.0.0/16	DRG

SUBNET B, 10.0.2.0/24

Regional Private Subnet

VCN, 10.0.0.0/16

DRG

CUSTOMER DATA CENTER

Customer Premises Equipment (CPE)

Remote Private Network, 172.16.0.0/16

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

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

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

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

DRG Routing Engine

Design

1. Each VCN, FastConnect, IPSEC, or RPC connection is "connected" to the DRG via an Attachment.

2. Each "Attachment" has a route table assigned, which directs ingress traffic to a specific egress attachment.

Operation

1. A Packet arrives from VCN or on-premise into the DRG

2. The DRG routing engine determines which Attachment to egress the packet out of based on the associated route table.

IP Packet

On-Premise

Route Table #2, #3, etc.
Route Target : Dest Att
Route Target : Dest Att

(3)

IPSEC Attachment
IPSEC Attachment
FC Attachment

DRG 1
DRG Routing Engine
RPC Attachment
RPC Attachment
DRG 2

VCN 1 Attachment
VCN 2 Attachment
VCN 3 Attachment

(1)

VCNs

(2) Route Table #1
Route Target : Dest Att

IP Packet

(1) Packet arrives into DRG from VCN (VCN attachment) or on-premise (FC/IPSEC attachment) or remote region (RPC attachment).
(2) A route lookup is performed on the route table associated with the ingress attachment.
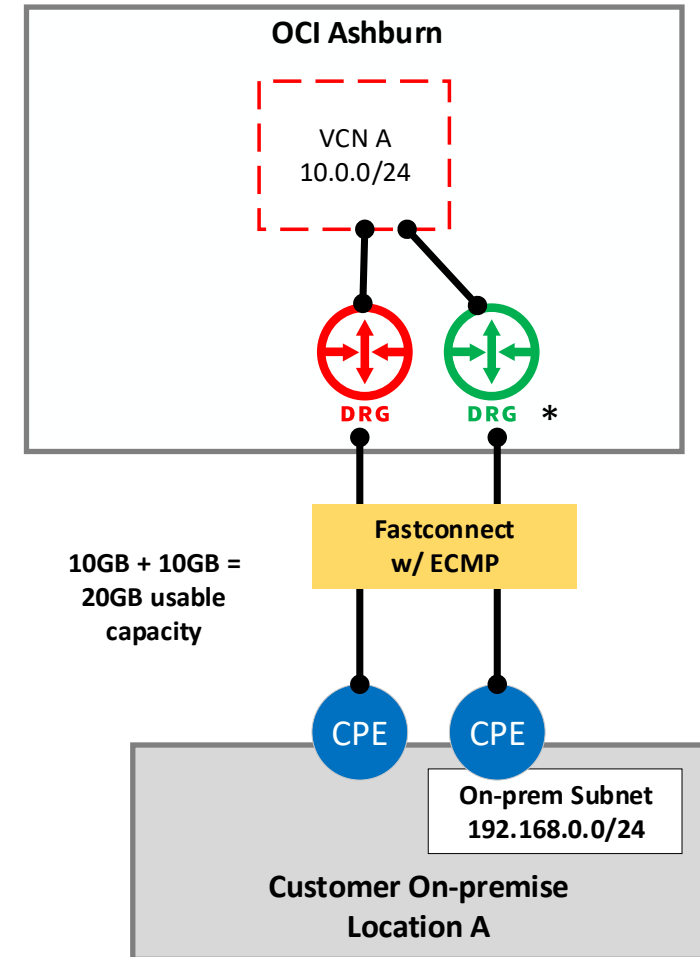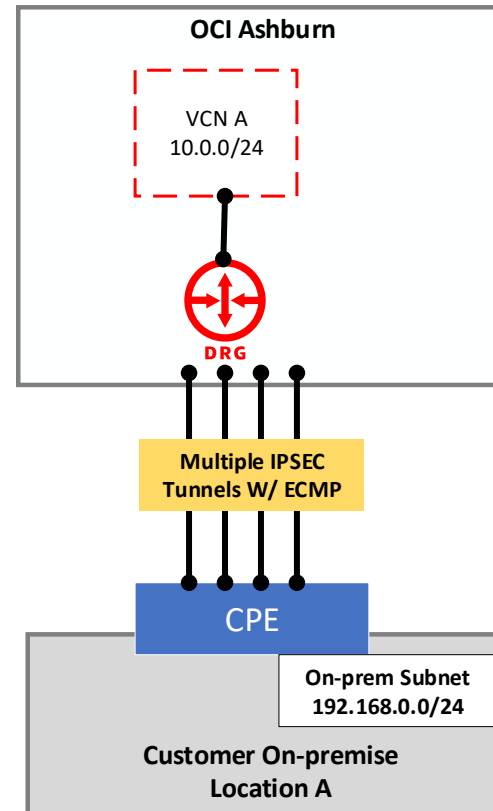**(3)** The packet is forwarded by the DRG routing engine out an Egress attachment.

DRG Enhancements: Remote On Ramp

- FastConnect or IPSEC VPN in Region (A)

- Able to access resources in Region (B)

- Uses the OCI Private backbone.

- Can also provide redundancy.
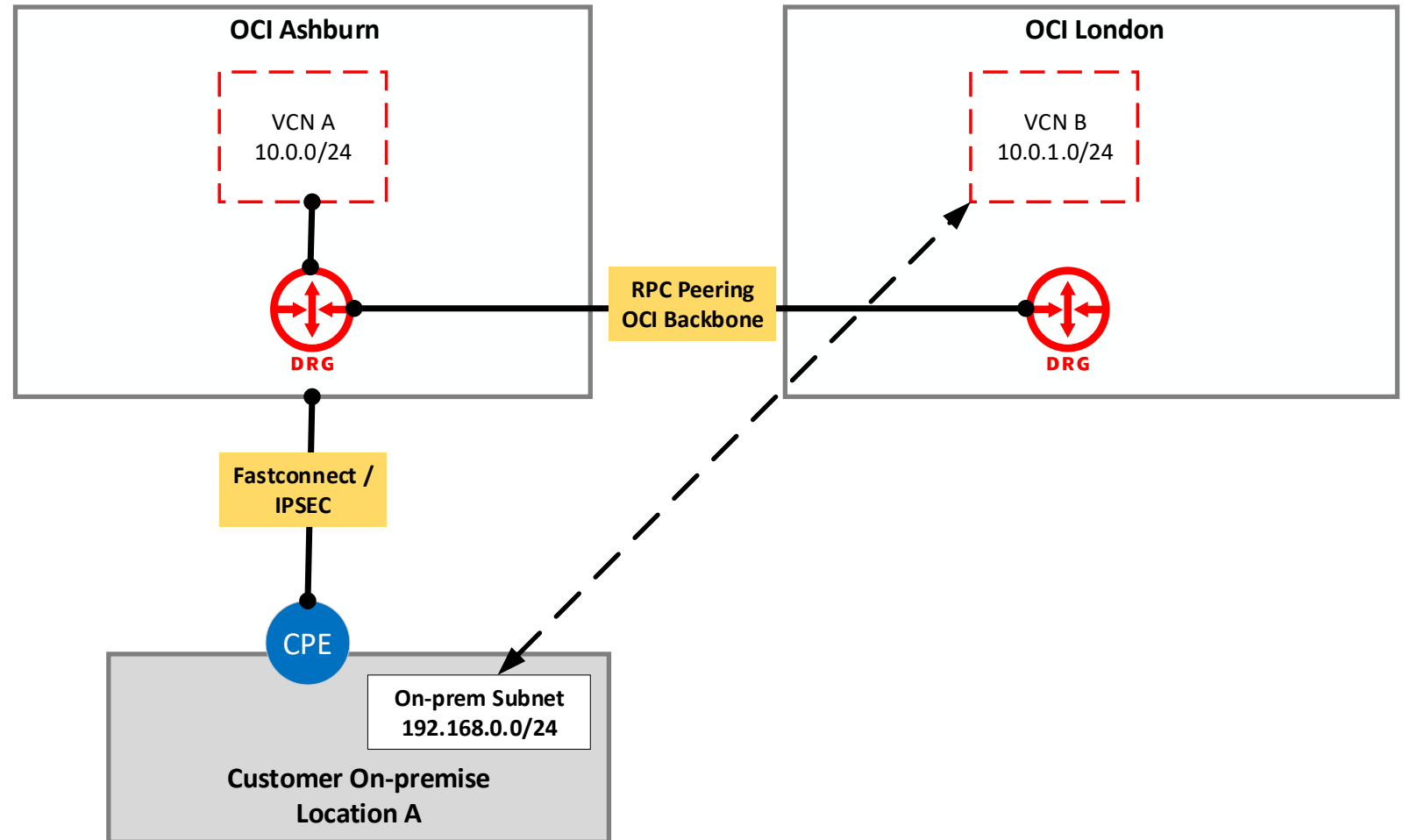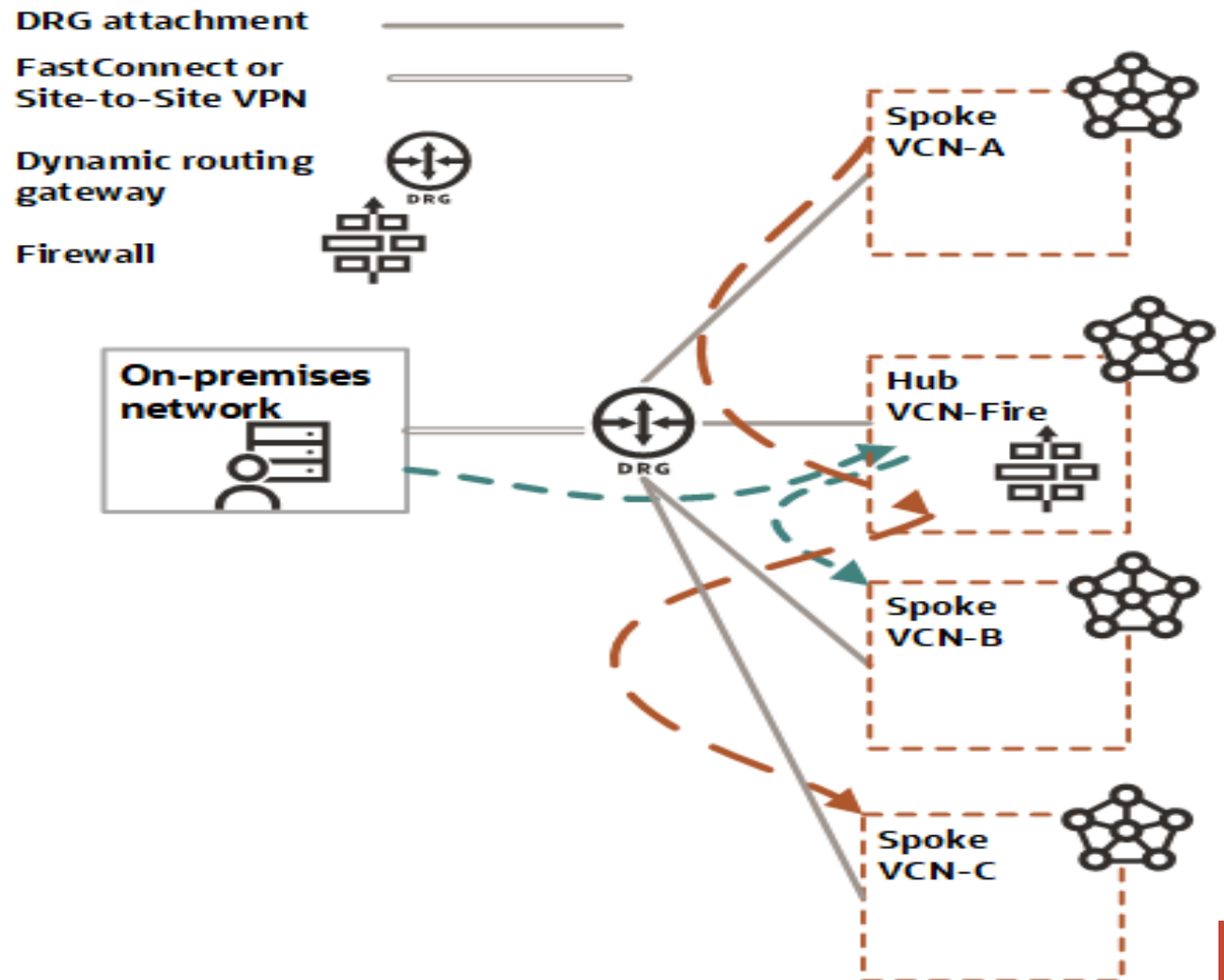
DRG : ECMP (Active/Active) support

- OCI now support "ECMP" for Active/Active load sharing.

- Bundle up to (8) IPSEC or FastConnect connections.

- Enabled on a per-route table basis.

OCI Ashburn

VCN A
10.0.0/24

DRG

Multiple IPSEC Tunnels W/ ECMP

CPE

On-prem Subnet
192.168.0.0/24

Customer On-premise Location A

OCI Ashburn

VCN A
10.0.0/24

DRG   **DRG**   *

10GB + 10GB =
20GB usable
capacity

Fastconnect w/ ECMP

CPE   **CPE**

On-prem Subnet
192.168.0.0/24

Customer On-premise Location A

* OCI only has a single DRG , but it can contain multiple physical routers.
For clarity, the second DRG refers to a different physical Oracle (PE) router.

DRG: L3 Firewall

- All traffic between VCNs is routed via L NVA (Network Virtual Appliance – or Firewall)

- Routing tables are used to direct traffic via a specific VCN, and the DRG-attachment routing table forces all traffic to the NVA.

Thank you