CIDR: Example

192.168.1.0/27 would equate to IP range 192.168.1.0 – 192.168.1.31

- Same network is divided into 8 subnets, with 32 hosts each due to the /27 mask (255.255.255.224)

192.168.1.44	1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 0 1	0 0 1 0 1 1 0 0
/27 subnet mask	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 0 0 0 0 0
Logical AND	1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 0 1	0 0 1 0 0 0 0 0

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

Private IPv4 Addresses

The Internet Engineering Task Force (IETF) has directed the Internet Assigned Numbers Authority (IANA) to reserve the following IPv4 address ranges for private networks:

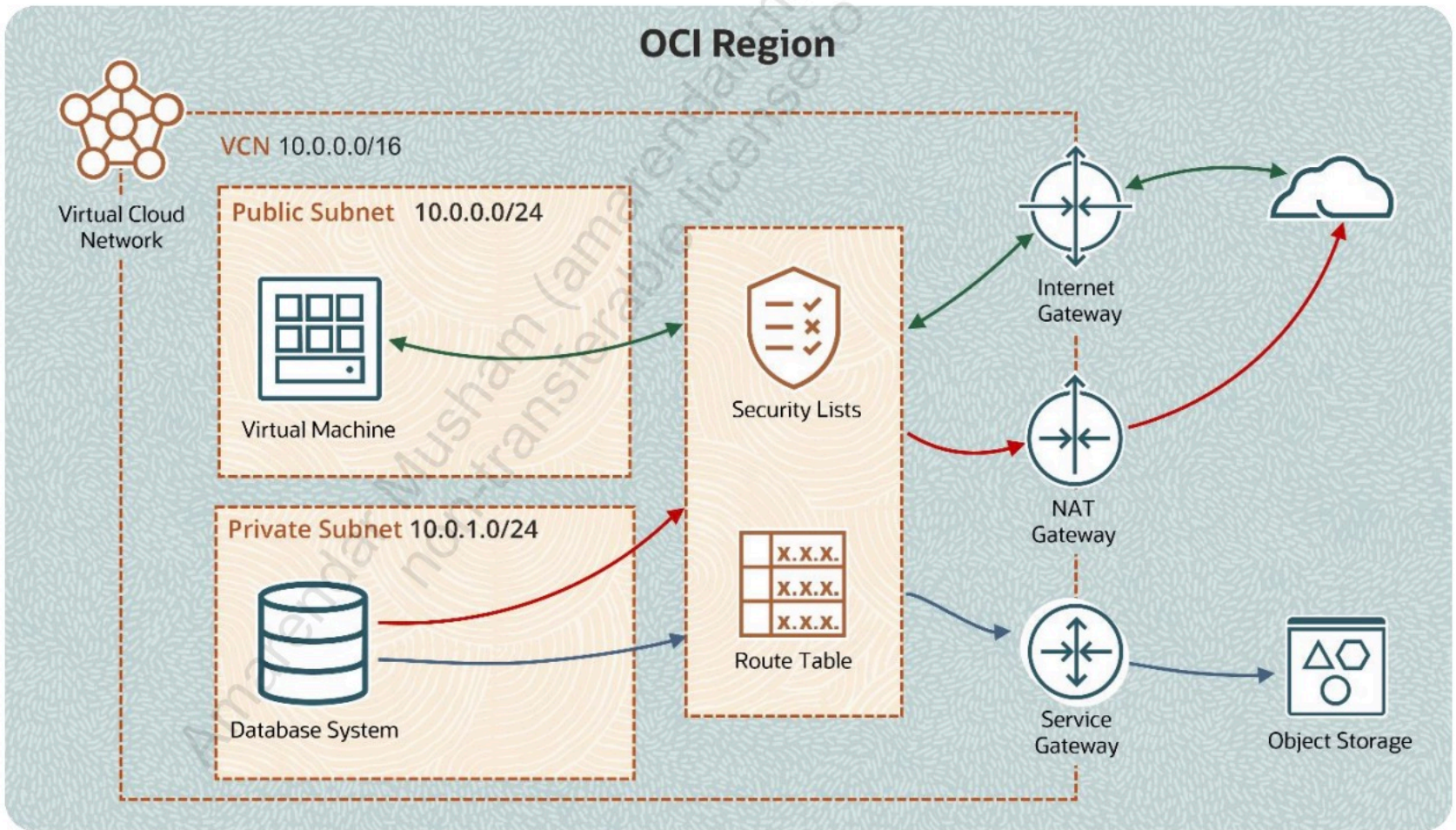
RFC 1918 prefix	Mask	IP address range	Number of addresses	Host ID size	Mask bits	Description
10.0.0.0/8	255.0.0.0	10.0.0.0 – 10.255.255.255	16777216	24 bits	8 bits	Single class A network
172.16.0.0/12	255.240.0.0	172.16.0.0 – 172.31.255.255	1048576	20 bits	12 bits	16 contiguous class B networks
192.168.0.0/16	255.255.0.0	192.168.0.0 – 192.168.255.255	65536	16 bits	16 bits	256 contiguous class C networks

A VCN that is launched with the OCI VCN Wizard tool automatically creates the following:

- Public and Private subnets
- Internet Gateway (IG)
- NAT Gateway (NAT)
- Service Gateway (SG)
- Two Route Tables (RT)
- Two Security Lists (SL)

For more information about Virtual Cloud Networks, see the [OCI Networking Documentation]:

https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/landing.htm



VCN Gateways

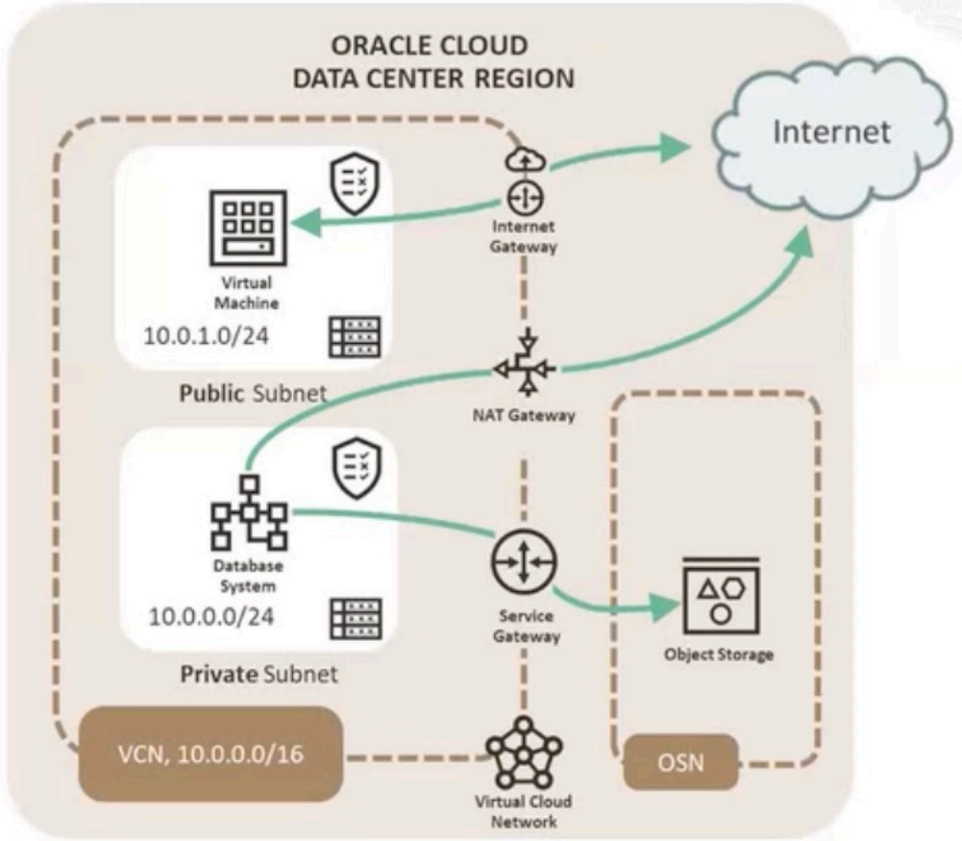
Hosts in your on-premises network:

- Private access through a VCN with FastConnect private peering or Site-to-Site VPN: Use private IP addresses and reach the Oracle Services Network by way of the VCN and the VCN's service gateway.
- Public access with FastConnect public peering: Use public IP addresses.

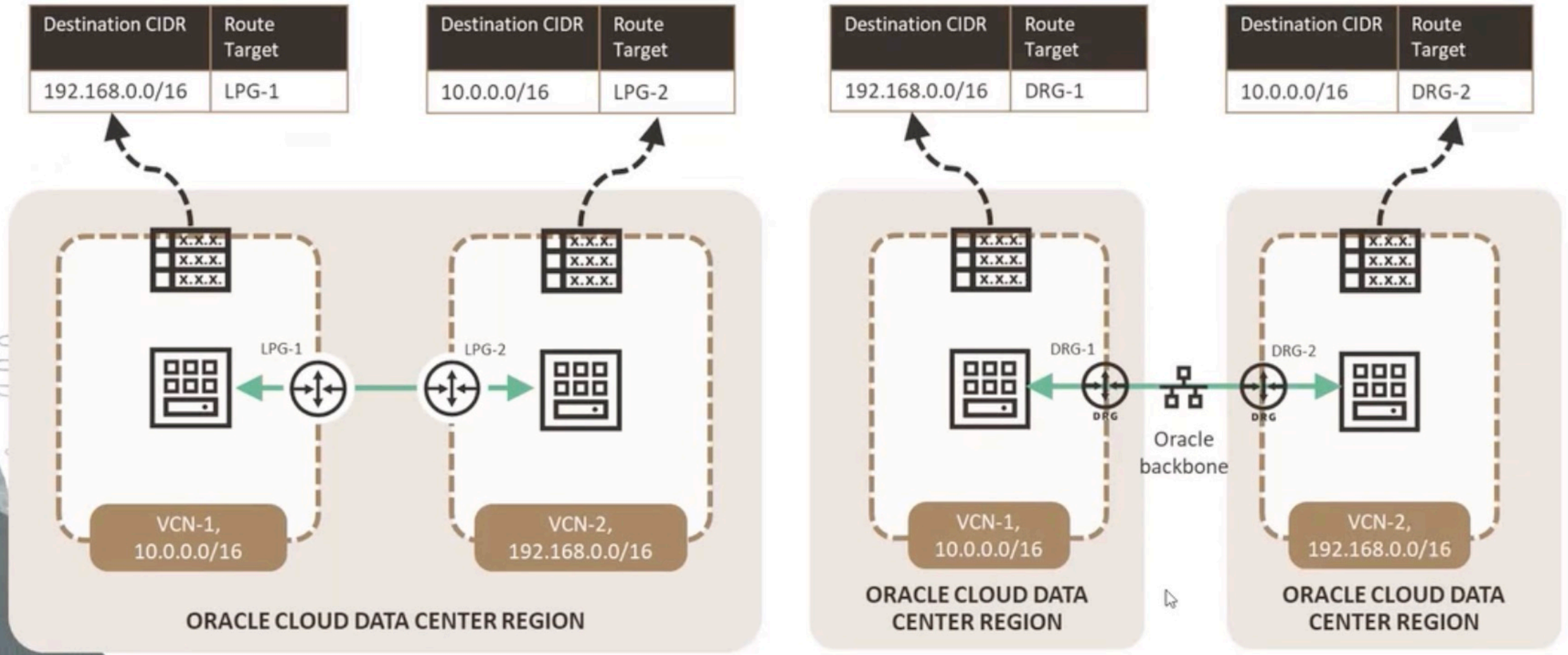
Hosts in your VCN:

- Private access through a service gateway: The VCN's hosts use private IP addresses.

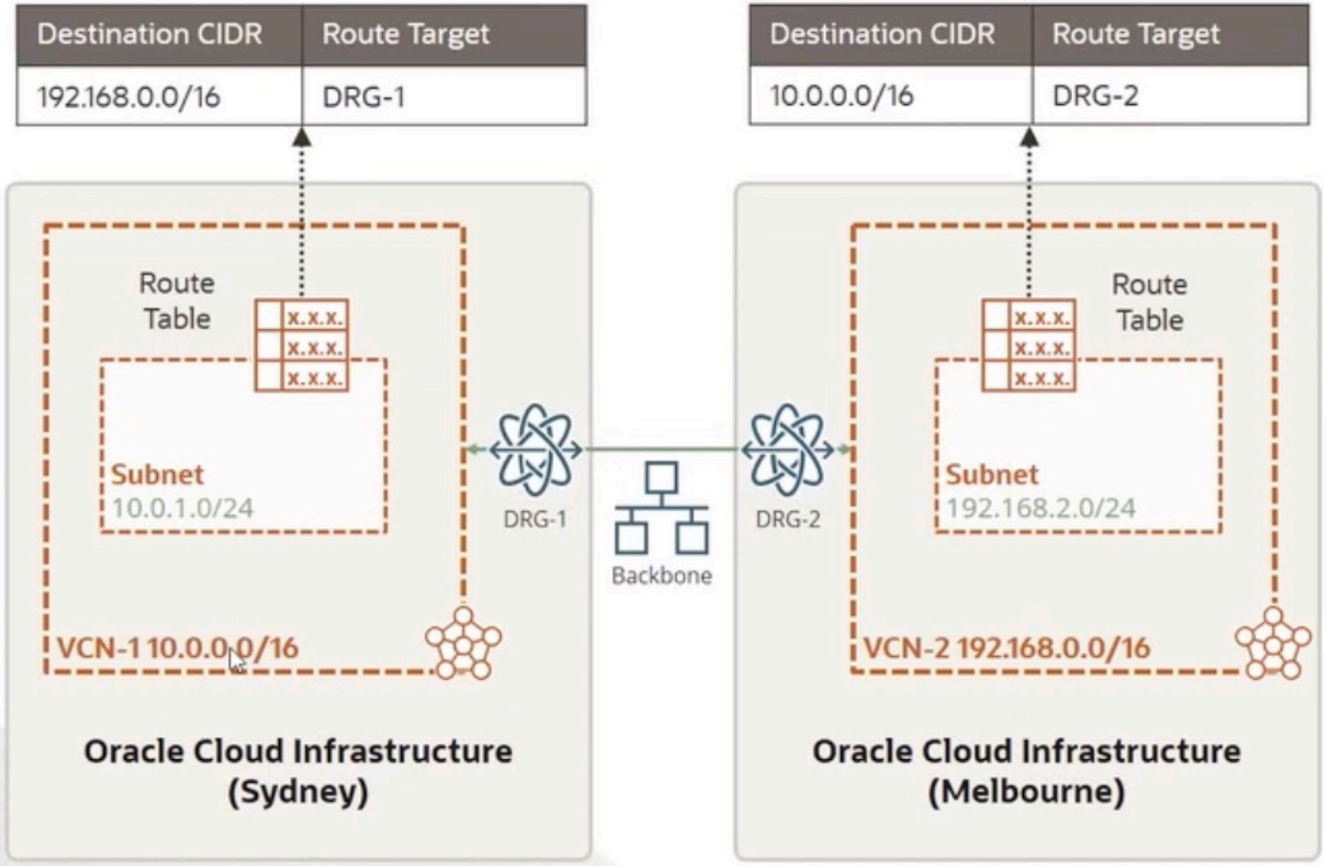
NAT Gateway



Local Peering vs. Remote Peering

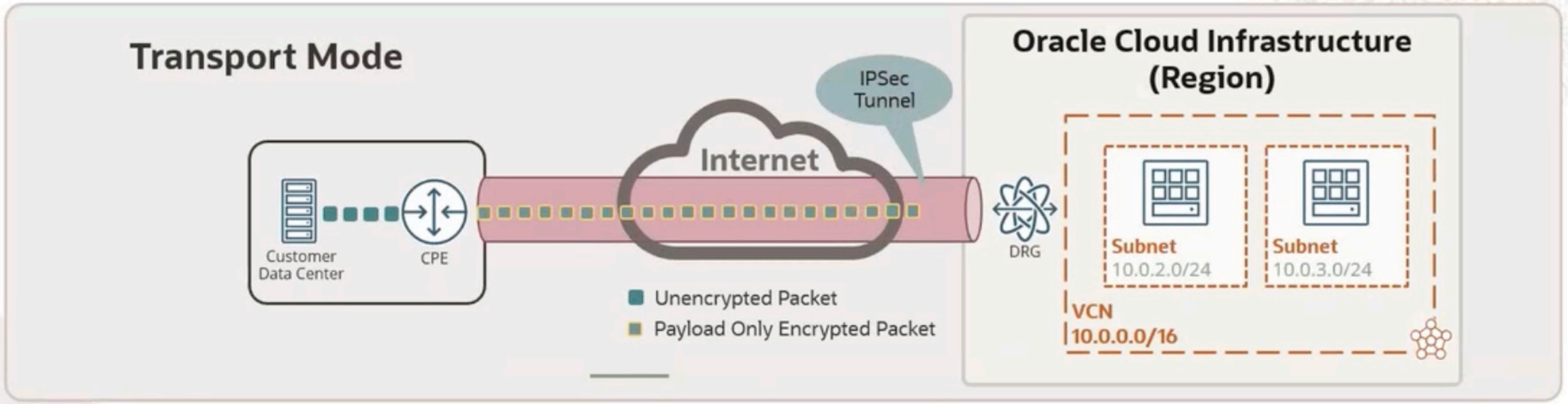


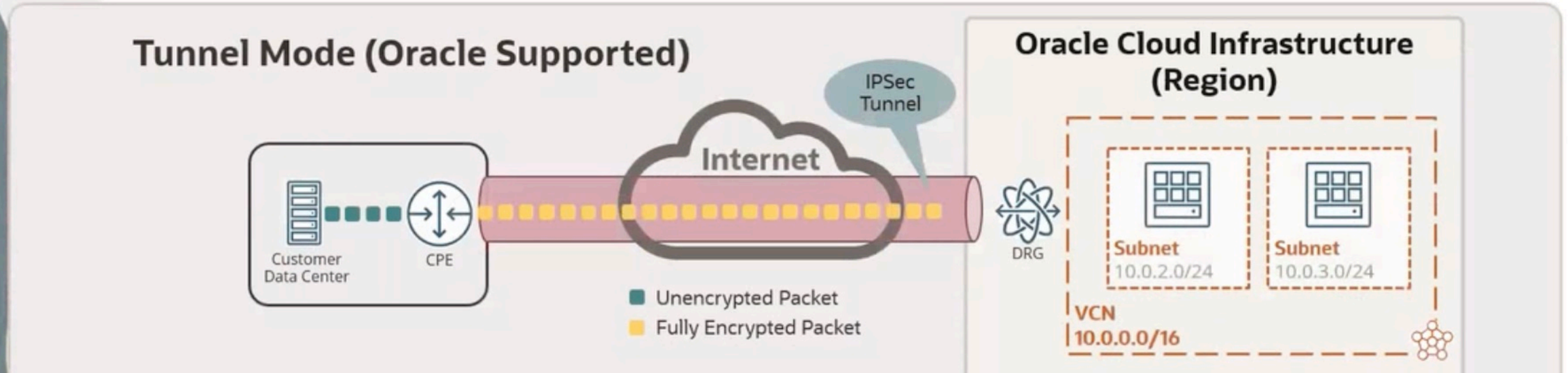
Remote Peering Connection



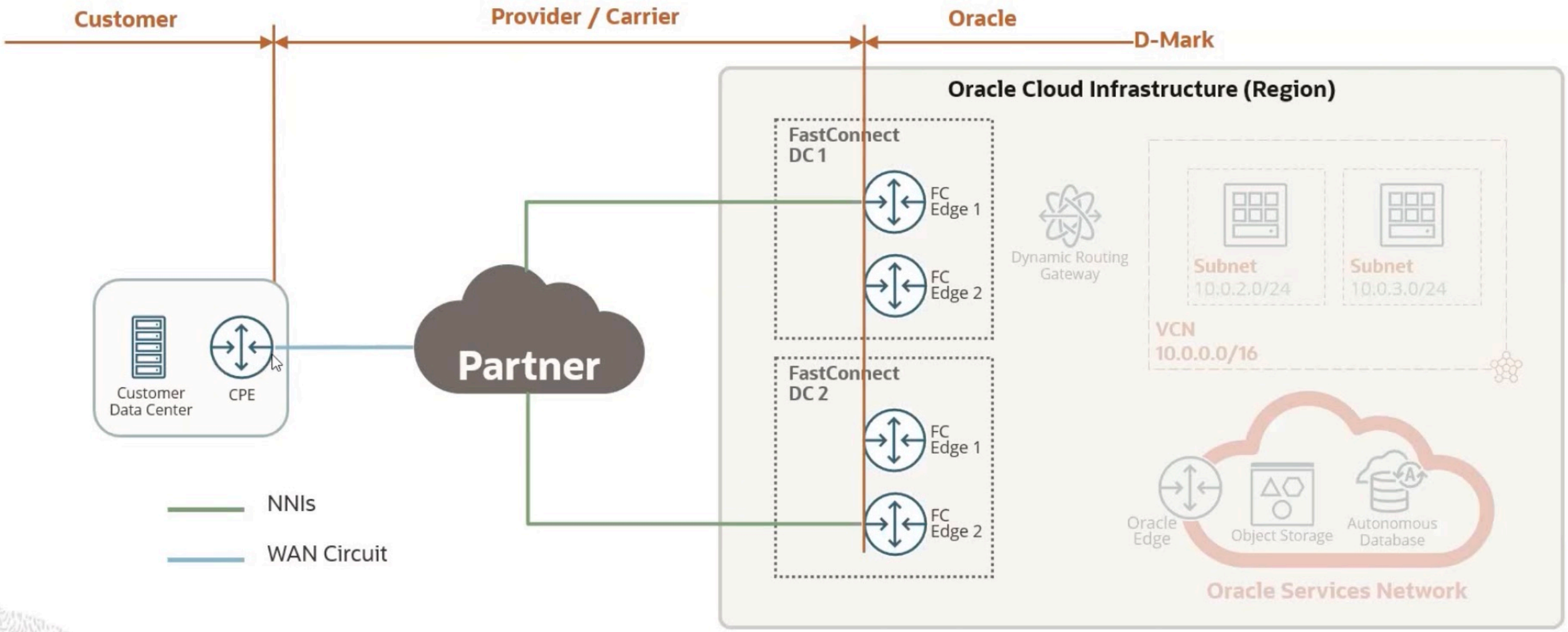
- Remote VCN peering is the process of connecting two VCNs so that their resources can communicate using private IP addresses
- Requires a remote peering connection (RPC) to be created on the DRGs. RPC's job is to act as a connection point for a remotely peered VCN
- The two VCNs in the peering relationship must not have overlapping CIDRs.
- Typically RPC is for VCNs located in different Regions. But it can be used for VCNs in the same region too.
- The VCNs can be located in different tenancies.

Site-to-Site VPN: Tunnel Mode



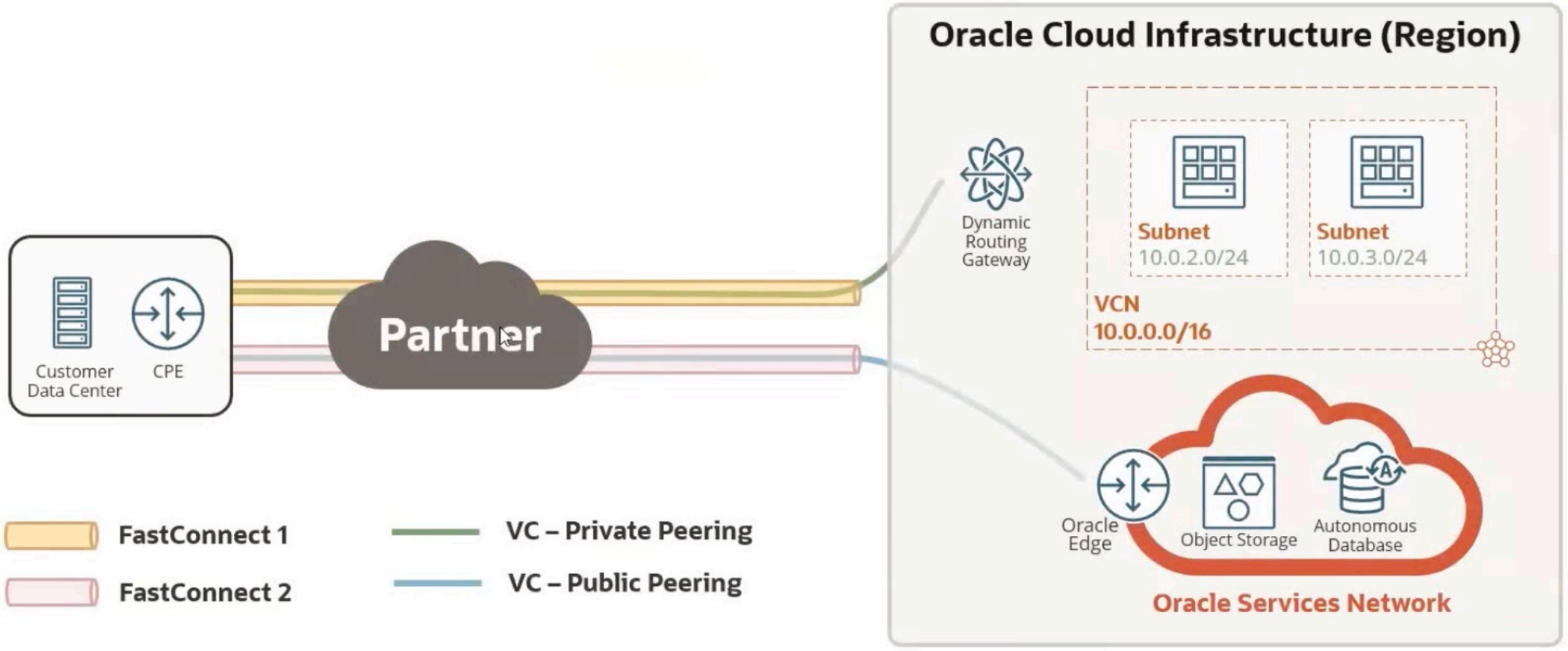


Option 1 - FastConnect with an Oracle Partner

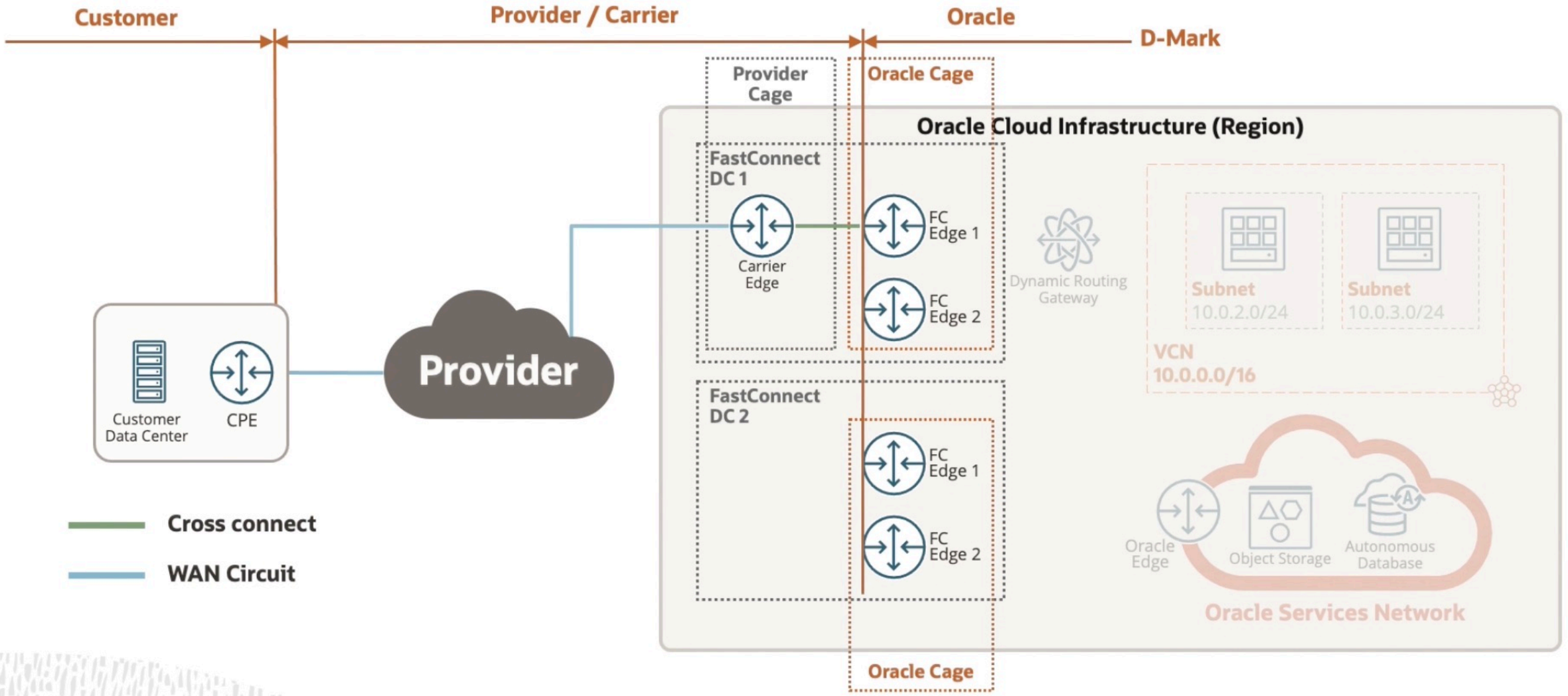


Supported Partners

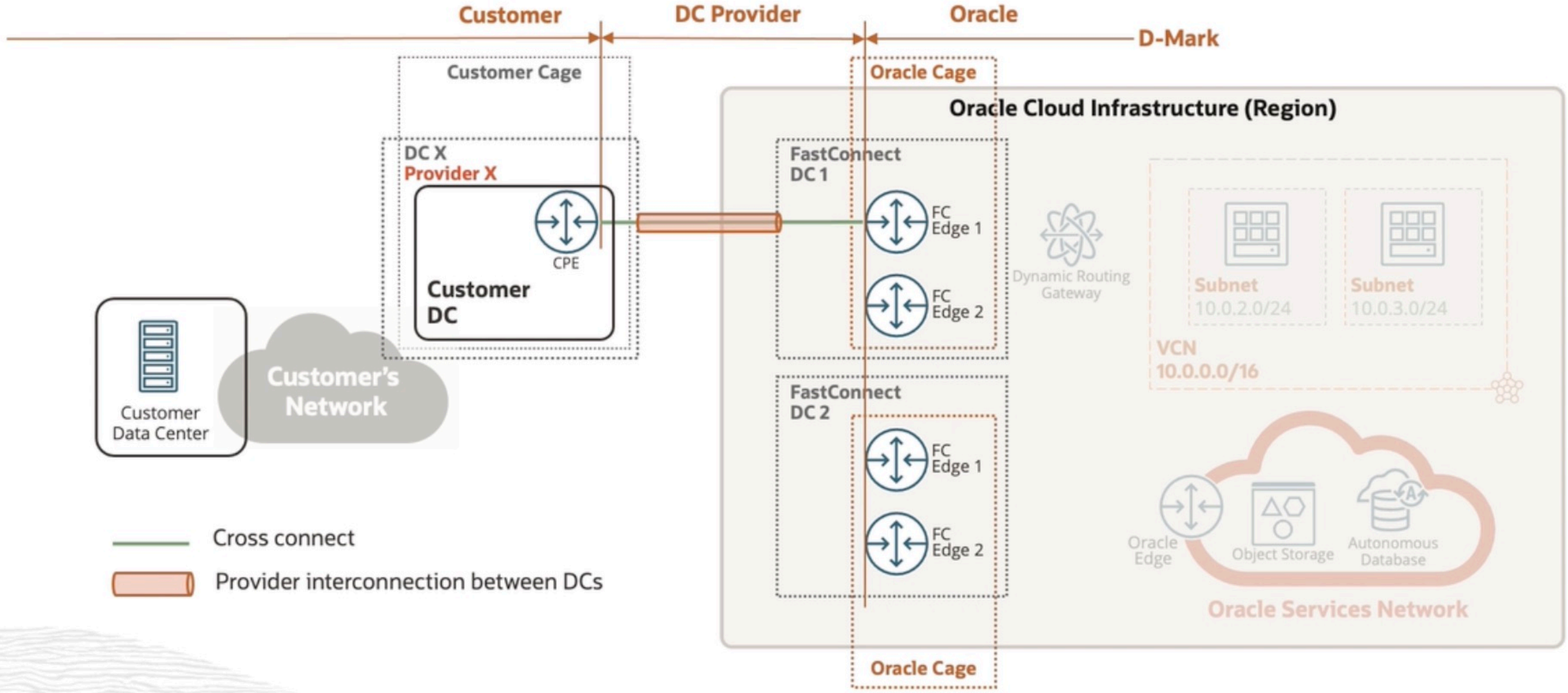
Option 2 - FastConnect with a Third-Party Provider



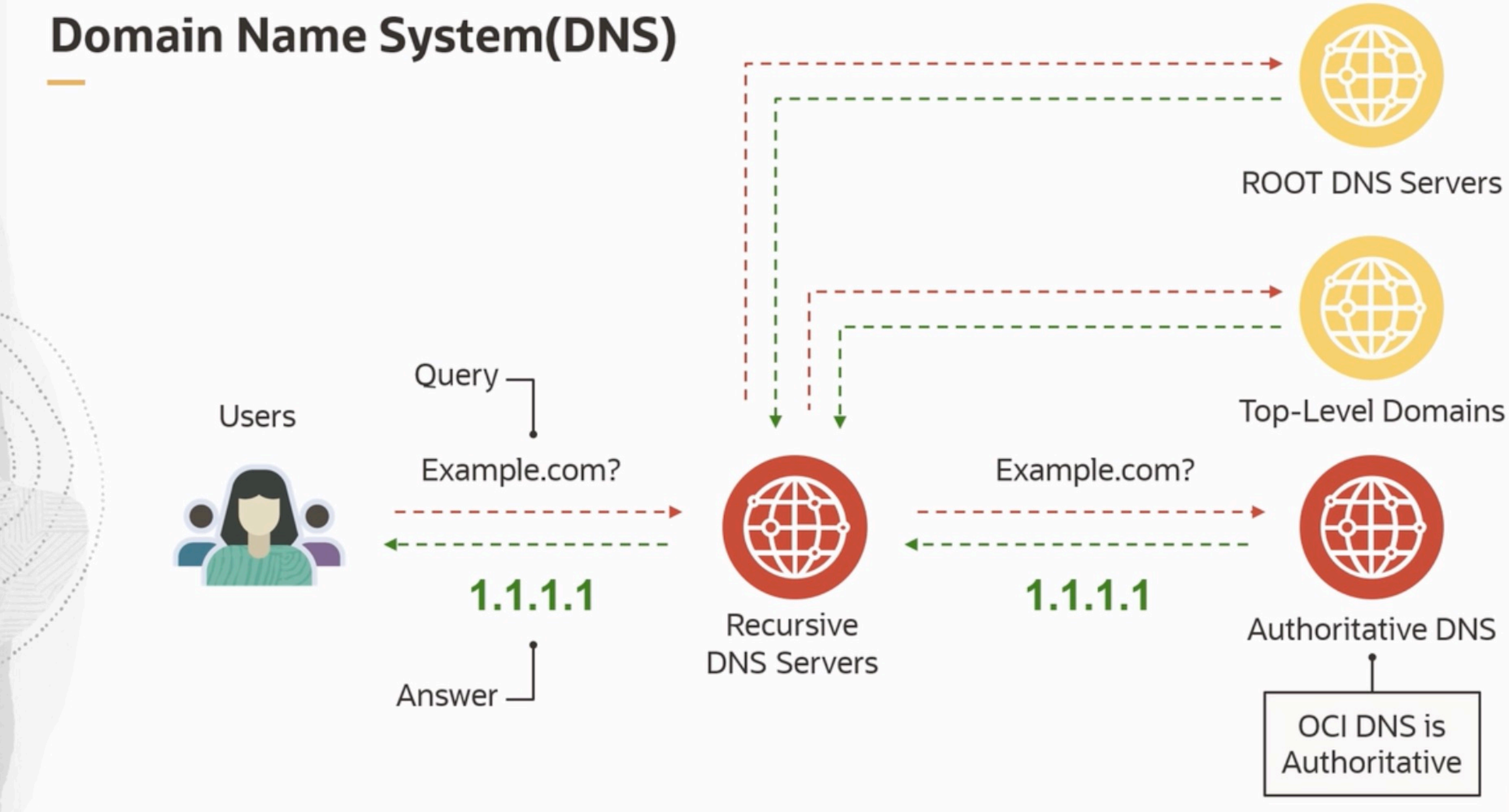
Option 2 - FastConnect with a Third-Party Provider



Option 3 - FastConnect Colocation with Oracle - Multiple DCs same Provider



Domain Name System(DNS)



Set the following permissions policies to use Network Path Analyzer:

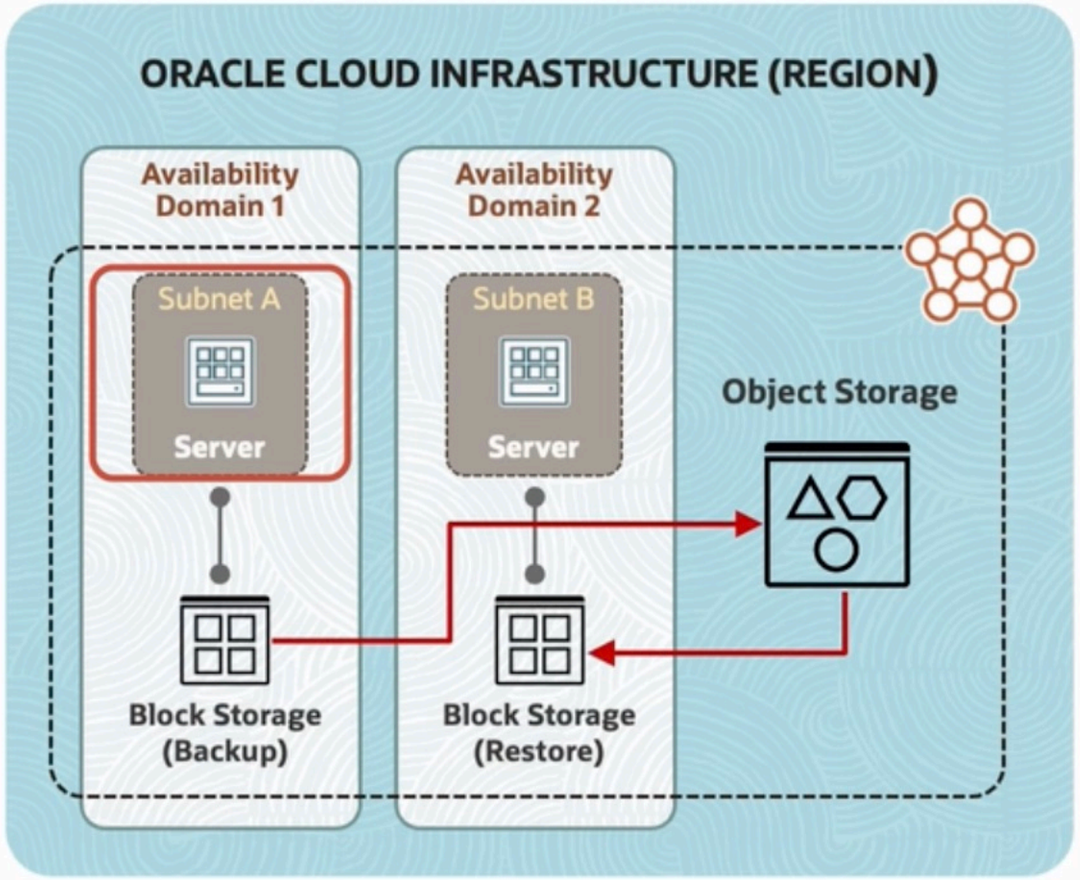
```
allow group <your-group-name> to manage vn-path-analyzer-test in TENANCY or <compartment>
allow any-user to inspect compartments in TENANCY where ALL {request.principal.type = 'vnpa-service' }
allow any-user to read instances in TENANCY where ALL { request.principal.type = 'vnpa-service' }
allow any-user to read virtual-network-family in TENANCY where ALL {request.principal.type = 'vnpa-service' }
allow any-user to read load-balancers in TENANCY where ALL {request.principal.type = 'vnpa-service' }
allow any-user to read network-security-group in TENANCY where ALL {request.principal.type = 'vnpa-service' }
```

Oracle Cloud Infrastructure Storage Services

	Local NVMe	Block Volume	File Storage	Object Storage	Archive Storage
Type	NVMe SSD-based temporary storage	NVMe SSD-based block storage	NFSv3 compatible file system	Highly durable Object storage	Long-term archival and backup
Durability	IP addresses, Non-persistent; survives reboots	Durable (multiple copies in an AD)	Durable (multiple copies in an AD)	Highly durable (multiple copies in a region)	Highly durable (multiple copies in a region)
Capacity	Terabytes+	Petabytes+	Fully Elastic	Unlimited	Unlimited
Unit Size	51.2 TB for BM, 6.4-25.6 TB for VM	50 GB - 32 TB/vol. 32 vols/instance	Up to 8 Exabyte	10 TiB/object	10 TiB/object
Use cases	Big Data, OLTP, high performance workloads	Apps that require SAN like features (Oracle DB, Exchange)	Apps that require shared file system (E-Business Suite, HPC)	Unstructured data incl. logs, images, videos	Long-term archival and backups (Oracle DB backups)

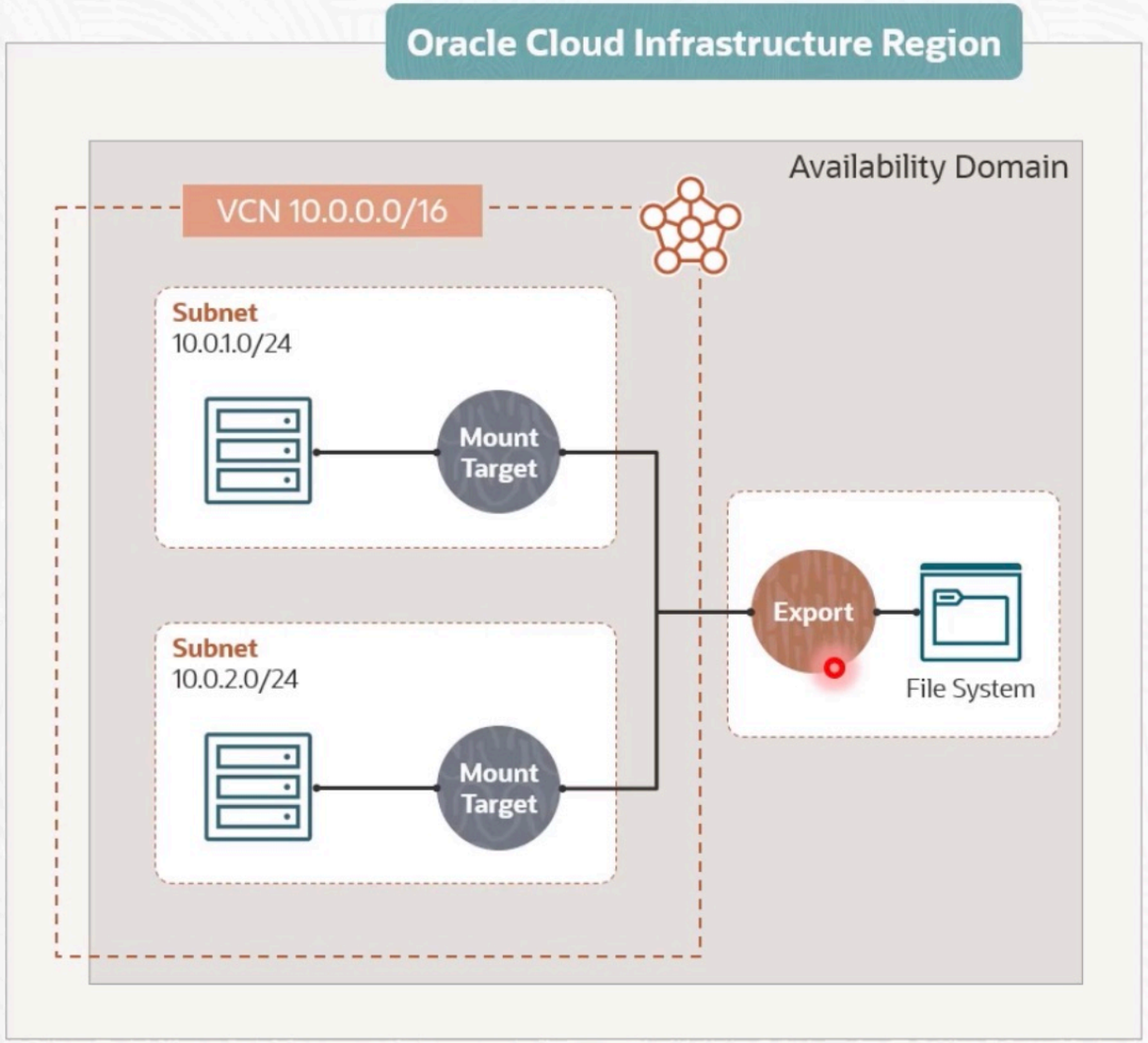
Backup and Restoration

- Point-in-time snapshot
- Encrypted and stored
- Restored as new volumes
- Tags are automatically included



Backup Versus Clone

	Volume Backup	Volume Clone
Description	Point-in-time backup of data	Single point-in-time copy of a volume
Speed	Slower (minutes or hours)	Faster (seconds)
Cost	Lower cost	Higher cost
Storage Location	Object Storage	Block volume
Retention Policy	Manual backups don't expire. Policy-based backups do expire.	No expiration
Volume Groups	Supported	Supported
Use Case	Supports business continuity requirements; meets compliance regulatory requirements	Rapidly duplicates an existing environment Example: To test configuration changes without impacting production environment



File System: Storage where files exist

Export: NFS Control Layer

Mount Target: Endpoint used by clients to connect to the file system

NFS Export Options

Edit NFS Export Options

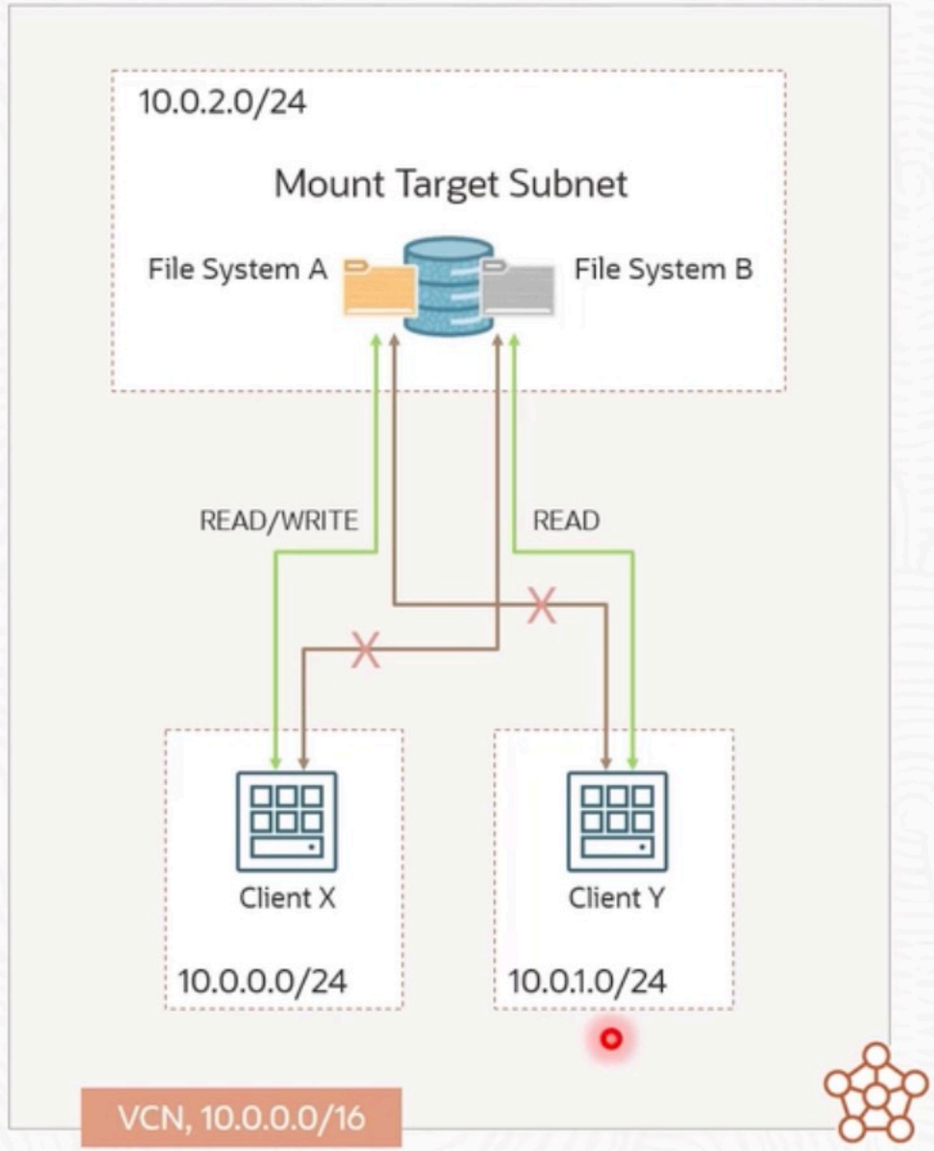
NFS export options control how clients can access your file system. Learn more.

Source	Ports	Access
10.0.0.0/24	Any	Read/Write

Edit NFS Export Options

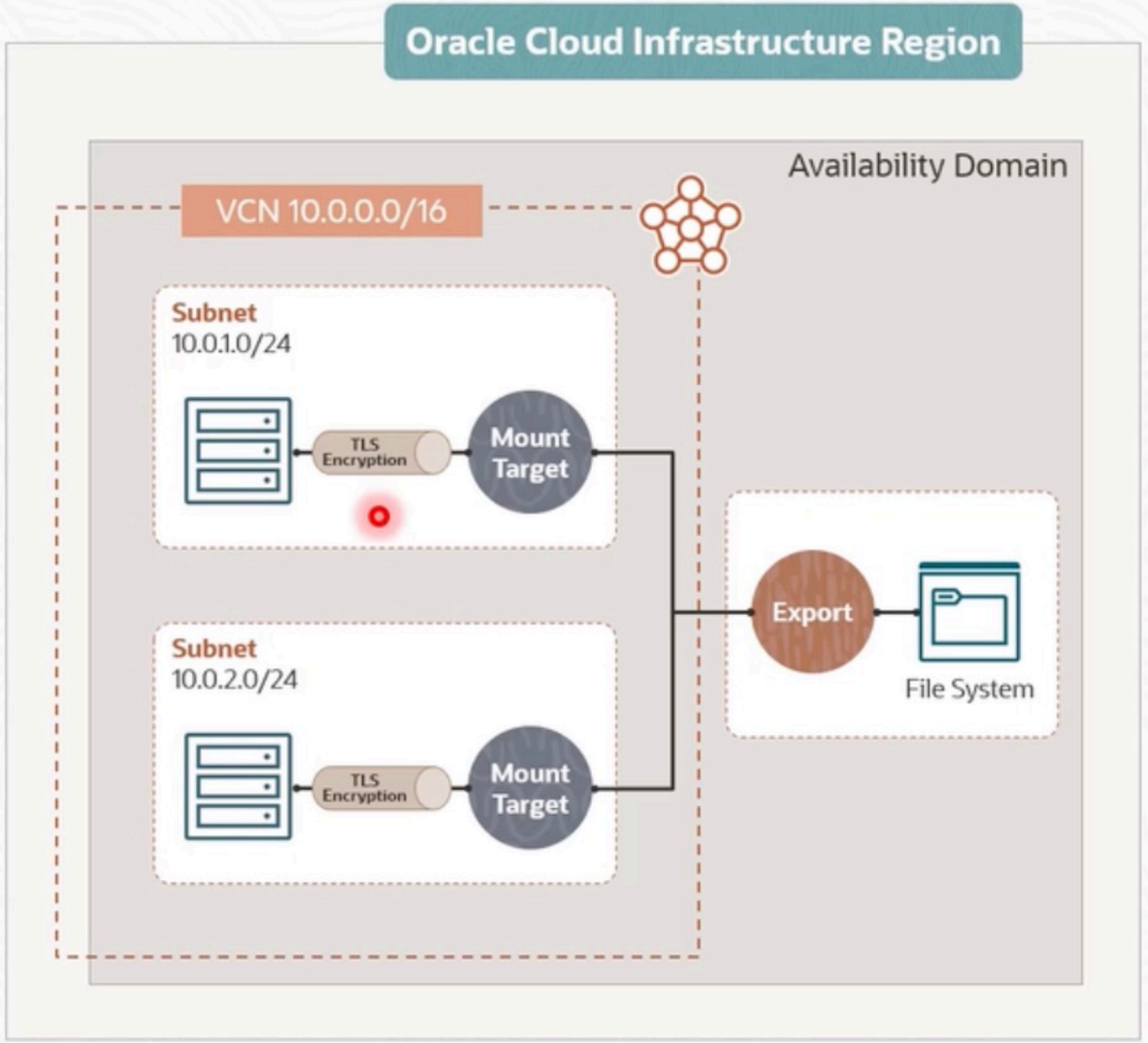
NFS export options control how clients can access your file system. Learn more.

Source	Ports	Access
10.0.1.0/24	Any	Read Only



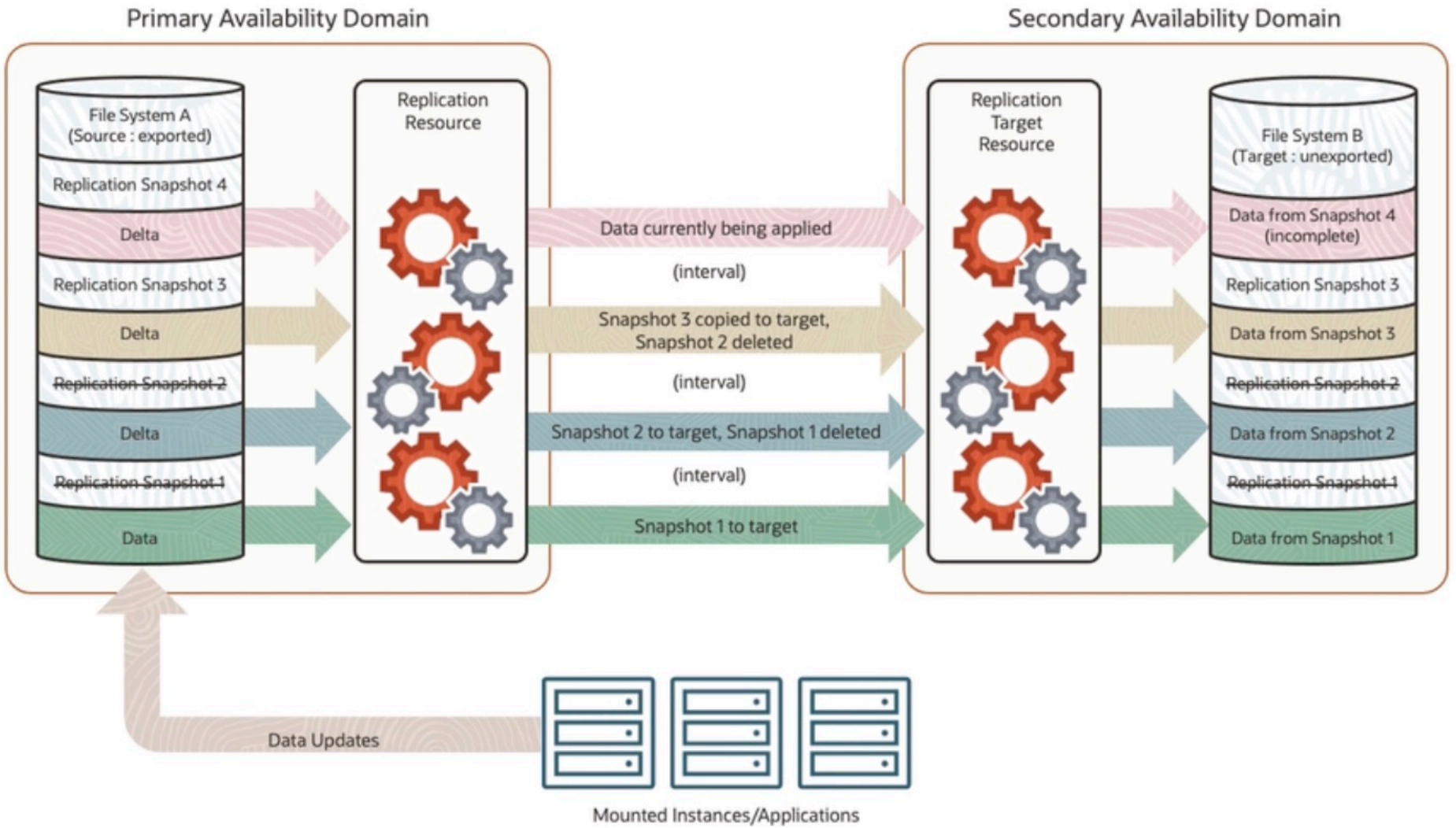
In-Transit Encryption

- Secure data between instances and mounted file systems using TLS v.1.2
- Download and install a package `oci-fss-utils` on the instance.
- Use the in-transit encryption command to mount the file system.




```
$ sudo mount -t oci-fss 10.x.x.x:/fs-export-path /mnt/yourmountpoint
```

Replication Process



Use Cases

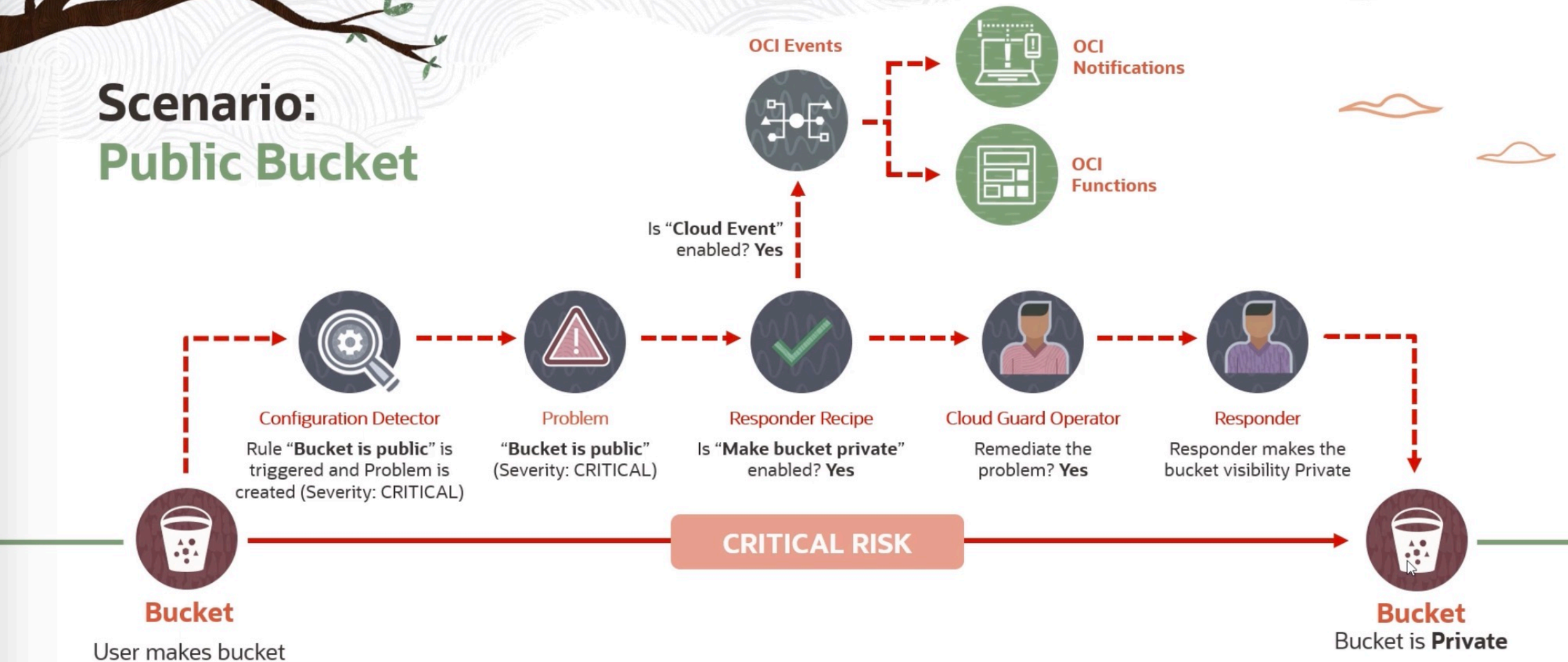
Detection and Remediation	○ Security posture management ○ Secure Enclave ○ Security Advisor ○ Vulnerability & exposure scanning
Data Protection	○ Encryption for data at rest and in transit ○ Centralized key storage & management ○ Rotate, manage, and retrieve secrets ○ Discover, classify, and protect data
OS and Workload Protection	○ Secure Boot, Measured Boot, TPM ○ Workload isolation ○ Managed Bastion ○ OS patch and package management
Identity and Access Management	○ Manage user access and policies ○ Manage multi-factor authentication ○ Single sign-on to identity providers ○ Record API calls automatically
Infrastructure Protection	○ DDoS protection ○ Network security controls ○ Virtual firewalls ○ Filter malicious web traffic.

Security Services

Typical Security Roles with Cloud Guard

Role	Cloud Guard Functions	IAM Permissions and Resources	Accessible Functions
Service Owner (Root)	• Enable Cloud Guard • Create IAM groups and policies	• cloud-guard-family	Manage cloud-guard-family in tenancy
Security Architect (Security Analyst)	• Clone detector recipes • Manage detectors • Assign detector recipes to targets • Read/manage problems and problem scores and other metrics	• cloud-guard-detectors • cloud-guard-targets • cloud-guard-detector-recipes • cloud-guard-responder-recipes • cloud-guard-managed-lists • cloud-guard-problems • cloud-guard-risk-scores • cloud-guard-security-scores	Manage, inspect, read these resources in tenancy or compartments
Security Operations Administrator	• Manage, inspect, or read Cloud Guard problems	• cloud-guard-problems	Manage, inspect, read Cloud Guard problems

Scenario:
Public Bucket



Configuration Detector Rules (Oracle-Managed)

Compute Resources

+ Instance has a public IP address
+ Instance is publicly accessible
+ Instance is running on Oracle public image
+ Instance is running without required Tags

Database Resources

+ Database is not backed up automatically
+ Database patch is not applied
+ Database System has public IP address
+ Database System is publicly accessible
+ Database System patch is not applied
+ Database System version is not sanctioned
+ Database version is not sanctioned

Networking Resources

+ Load balancer allows weak cipher suites
+ Load balancer allows weak SSL communication
+ Load balancer has no backend set
+ Load balancer has no inbound rules or listeners
+ Load balancer SSL certificate expiring soon
+ NSG egress rule contains disallowed IP/port
+ NSG ingress rule contains disallowed IP/port
+ VCN has Internet Gateway attached
+ VCN has Local Peering Gateway attached
+ VCN has no inbound Security List
+ VCN Security list allows traffic to non-public port from all sources (0.0.0.0/0)
+ VCN Security list allows traffic to restricted port
+ VNIC without associated network security group

Activity Detector Rules (Oracle-managed)

IAM Resources

+ IAM API keys created
+ IAM API keys deleted
+ IAM Auth Token created
+ IAM Auth Token deleted
+ IAM Customer Keys created
+ IAM Customer Keys deleted
+ IAM Group created
+ IAM Group deleted
+ IAM OAuth 2.0 credentials created
+ IAM OAuth 2.0 credentials deleted
+ IAM User capabilities modified
+ IAM User created
+ IAM User UI password created or reset
+ Security policy modified

Networking Resources

+ DRG attached to a VCN
+ DRG created
+ DRG deleted
+ DRG detached from a VCN
+ Subnet changed
+ Subnet deleted
+ VCN created
+ VCN deleted
+ VCN DHCP Option changed
+ VCN Internet Gateway created
+ VCN Internet Gateway terminated
+ VCN Local Peering Gateway changed
+ VCN Network Security Group deleted

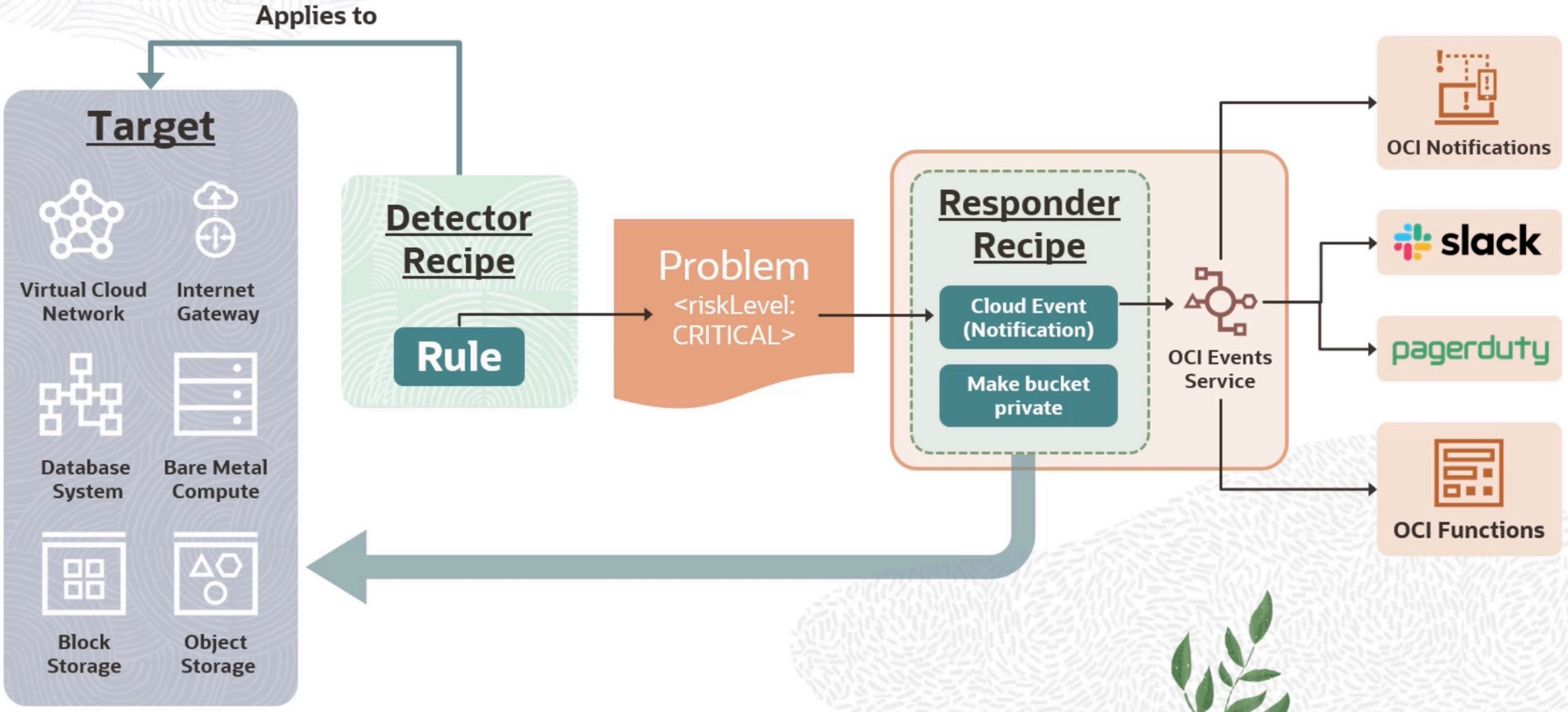
Compute Resources

+ Export Image
+ Import Image
+ Instance terminated
+ Update Image

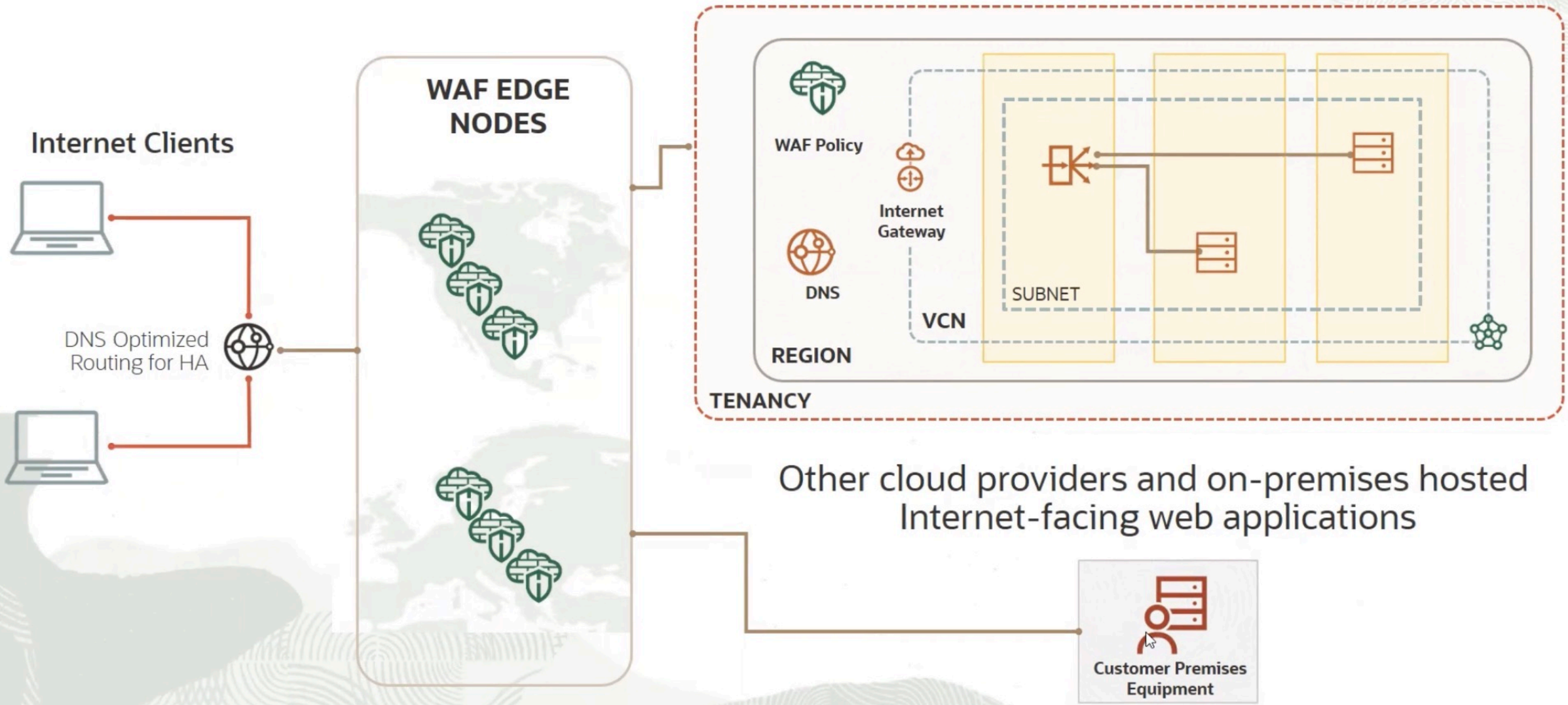
Database Resources

+ Database System terminated

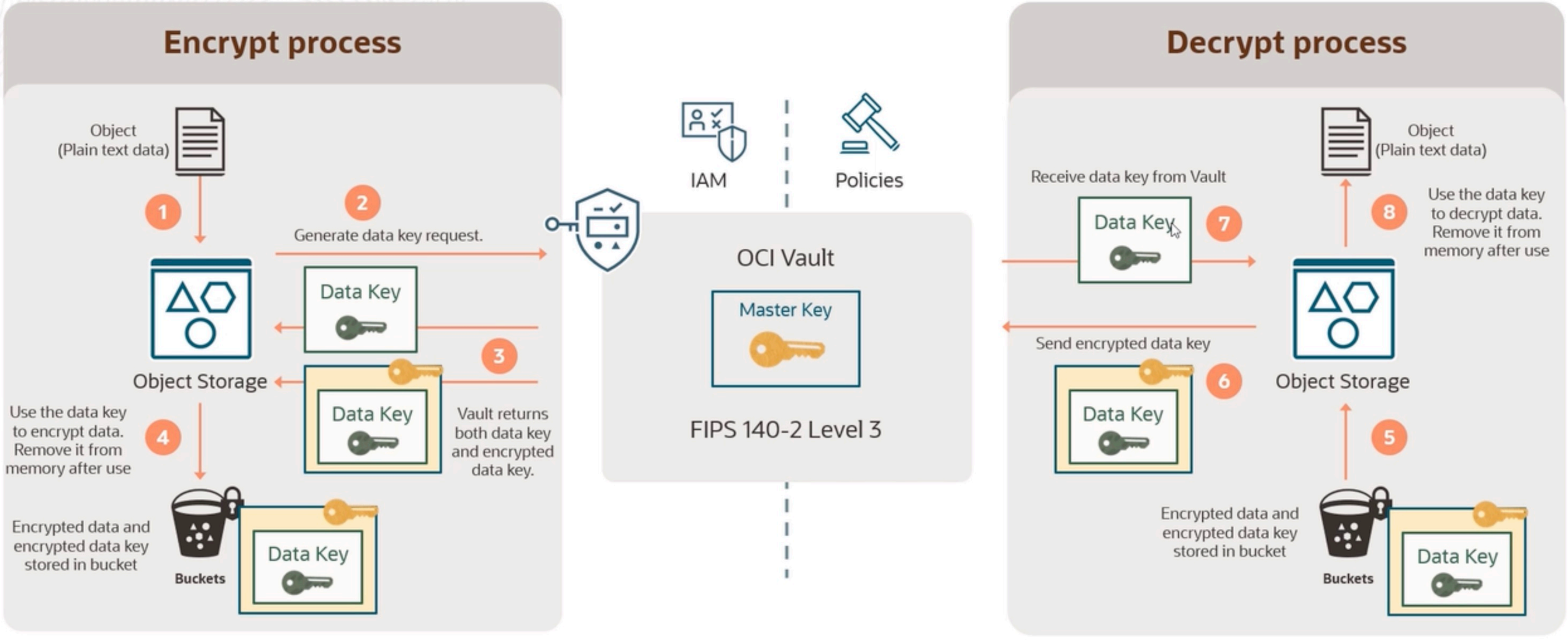
Integration with Events and Notification Services



OCI WAF Architecture



OCI Object Storage Integration with Vault



Service Connector Workflow