ORACLE
Cloud Infrastructure

Virtual Cloud Network Overview and Deployment Guide

ORACLE WHITE PAPER | JUNE 10, 2019

ORACLE

CONTENTS

Virtual Cloud Network Overview and Deployment Guide

Purpose of this White Paper

The purpose of this document is to provide a basic understanding of the Oracle Cloud Infrastructure Networking service and common deployment scenarios for a virtual cloud network (VCN). You should have basic knowledge of networking and internet routing to understand this document. It is not intended to be a production deployment reference architecture.

Scope and Assumptions

This document gives brief descriptions of various Networking service components and typical deployment scenarios. After reading this document, you should have a good understanding of what a VCN is and several scenarios that illustrate VCN usage.

You should first:

- Be familiar with the fundamentals of Oracle Cloud Infrastructure
  - https://cloud.oracle.com/iaas
- Have a basic understanding of Oracle Cloud Infrastructure Compute
  - https://cloud.oracle.com/compute
- Have a basic understanding of Oracle Cloud Infrastructure Networking
  - https://cloud.oracle.com/networking
- Have a basic understanding of IPSec VPN tunnel functionality
  - https://docs.cloud.oracle.com/iaas/Content/Network/Tasks/managingIPsec.htm
- Have a basic understanding of Oracle Cloud Infrastructure FastConnect
  - https://cloud.oracle.com/fastconnect

There are a number of other related products and components that are used during typical VCN deployments, such as Identity and Access Management (IAM). Their details are beyond the scope of this document.

Virtual Cloud Network (VCN) Overview

A VCN is a virtual, private network that you set up in Oracle data centers. It closely resembles a traditional network, with firewall rules and specific types of communication gateways that you can choose to use. A VCN resides in a single Oracle Cloud Infrastructure region and covers a single, contiguous IPv4 CIDR block of your choice. The allowable VCN size range is /16 to /30. Example: 10.0.0.0/16. The Networking service reserves the first two IP addresses and the last one in each subnet's CIDR. After you've created a VCN or subnet, you can't change its size, so it's important to think about the size of VCN and subnets you need before creating them.

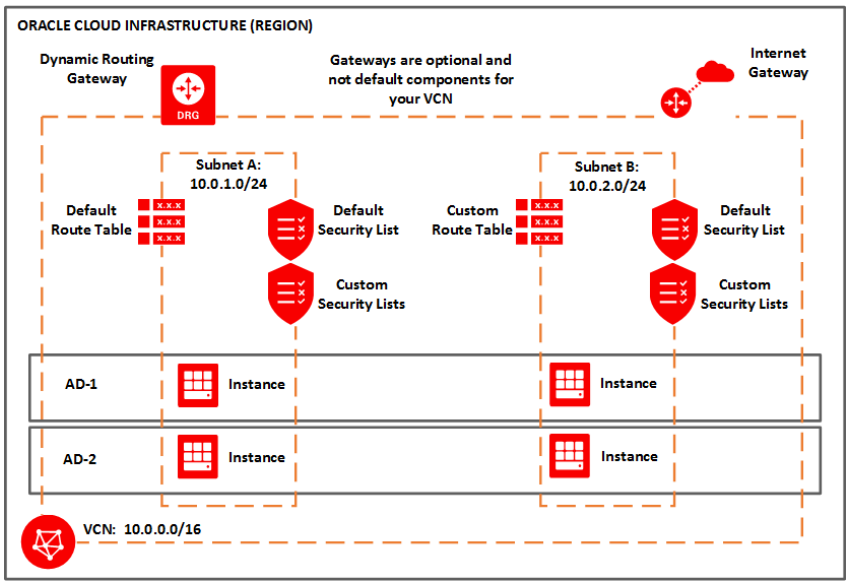
For your VCN, Oracle recommends using one of the private IP address ranges specified in RFC 1918 (10.0.0.0/8, 172.16/12, and 192.168/16). However, you can use a publicly routable range.

Your VCN automatically comes with these *default* components:

- Default route table, with no rules
- Default security list, with default rules
- Default set of DHCP options, with default values

You can't delete these default components. However, you can change their contents (for example, the rules in the default security list). And you can create your own custom versions of each kind of component in your VCN. There are limits to how many you can create and the maximum number of rules.

The following diagram is a simple illustration of a VCN with two regional subnets (which means the subnet spans all availability domains in the region). Each subnet contains instances in both availability domains. Subnet A uses the default route table, and Subnet B uses a custom route table (which you can create). Both subnets use the default security list as well as their own custom security lists. The default set of DHCP options is not explicitly shown in the diagram. The diagram also shows a couple of components that are not default components: a dynamic routing gateway (DRG) and an internet gateway. Keep reading for further discussion of these components.



Other Components

This section covers other Networking service components.

Subnet

Subnets are subdivsions you define in a VCN (for example, 10.0.0.0/24 and 10.0.1.0/24). Subnets contain virtual network interface cards (VNICs), which attach to instances. Each subnet consists of a contiguous range of IP addresses that do not overlap with other subnets in the VCN. You can designate a subnet to exist either in a single availability domain or across an entire region (regional subnets are recommended). Subnets act as a unit of configuration within the VCN: All VNICs in a given subnet use the same route table, security lists, and DHCP options (see the definitions that follow). You can designate a subnet as either public or private when you create it. Private means VNICs in the subnet can't have public IP addresses. Public means VNICs in the subnet can have public IP addresses at your discretion.

Virtual Network Interface Card (VNIC)

A VNIC attaches to an instance and resides in a subnet to enable a connection to the subnet's VCN. The VNIC determines how the instance connects with endpoints inside and outside the VCN. Each instance has a primary VNIC that's created during instance launch and cannot be removed. You can

add secondary VNICs to an existing instance (in the same availability domain as the primary VNIC), and remove them as you like. Each secondary VNIC can be in a subnet in the same VCN as the primary VNIC, or in a different subnet that is either in the same VCN or a different one. However, all the VNICs must be in the same availability domain as the instance.

Here are some reasons why you might use secondary VNICs:

- Use your own hypervisor on a bare metal instance
- Connect an instance to subnets in multiple VCNs

Here are more details about secondary VNICs:

- They're supported for these types of instances:
  - **Linux:** Both VM and bare metal instances.
  - **Windows:** Both VM and bare metal instances, but only on X7/second-generation shapes (shapes with "2" in the name, such as VM.Standard 2.16 and BM.Standard2.52). For bare metal, secondary VNICs are supported only on the second physical NIC.
- There's a limit to how many VNICs can be attached to an instance, and it varies by shape.
- They can be added only after the instance is launched.
- They must always be attached to an instance and cannot be moved. The process of creating a secondary VNIC automatically attaches it to the instance. The process of detaching a secondary VNIC automatically deletes it.
- They are automatically detached and deleted when you terminate the instance.
- The instance's bandwidth is fixed regardless of the number of VNICs attached. You can't specify a bandwidth limit for a particular VNIC on an instance.
- Attaching multiple VNICs from the same subnet CIDR block to an instance can introduce asymmetric routing, especially on instances using a variant of Linux. If you need this type of configuration, Oracle recommends assigning multiple private IP addresses to one VNIC, or using policy-based routing.

Private IP

A private IP consists of a private IP address and related information for addressing an instance (for example, a hostname for DNS). Each VNIC has a primary private IP, and you can add and remove secondary private IPs. The primary private IP address on an instance doesn't change during the instance's lifetime and cannot be removed from the instance. You can add a *secondary private IP* to an instance after it's launched. You can add it to either the primary VNIC or a secondary VNIC on the

instance. The secondary private IP address must come from the CIDR of the VNIC's subnet. You can move a secondary private IP from a VNIC on one instance to a VNIC on another instance if both VNICs belong to the same subnet.

Here are a few reasons why you might use secondary private IPs:

- Instance failover
- Running multiple services or endpoints on a single instance

Here are more details about secondary private IP addresses:

- They're supported for all shapes and OS types, for both bare metal and VM instances.
- A VNIC can have a maximum of 31 secondary private IPs.
- They can be assigned only after the instance is launched (or the secondary VNIC is created/attached).
- A secondary private IP that is assigned to a VNIC in a regional subnet has a null availability domain attribute. Compare this with the VNIC's *primary* private IP, which always has its availability domain attribute set to the instance's availability domain, regardless of whether the instance's subnet is regional or AD-specific.
- Deleting a secondary private IP from a VNIC returns the address to the pool of available addresses in the subnet.
- They are automatically deleted when you terminate the instance (or detach/delete the secondary VNIC).
- The instance's bandwidth is fixed regardless of the number of private IP addresses attached. You can't specify a bandwidth limit for a particular IP address on an instance.
- A secondary private IP can have a reserved public IP assigned to it at your discretion.

Internet Access: Internet Gateway and NAT Gateway

There are two optional gateways (virtual routers) that you can add to your VCN depending on the type of internet access you need:

- **Internet gateway:** For resources with public IP addresses that need to be reached from the internet (example: a web server) or need to initiate connections to the internet.
- **NAT gateway:** For resources without public IP addresses that need to initiate connections to the internet (example: for software updates) but need to be protected from inbound connections from the internet.

Traffic between a given subnet and gateway is controlled by the subnet's route table and security lists.

You can see both gateways used in this scenario later in this document: Multi-Tier Application Running on Oracle Cloud Infrastructure.

Just having an internet gateway alone does not expose the instances in the VCN's subnets directly to the internet. The following requirements must also be met:

- The internet gateway must be enabled (by default, the internet gateway is enabled upon creation).
- The subnet must be public.
- The subnet must have a route rule that directs traffic to the internet gateway.
- The subnet must have security list rules that allow the traffic (and each instance's firewall must allow the traffic).
- The instance must have a public IP address.

Dynamic Routing Gateway (DRG)

A DRG is an optional virtual router that you can add to your VCN. It provides a path for *private* network traffic between your VCN and on-premises network. You can use it with other Networking components and a router in your on-premises network to establish a connection by way of IPSec VPN or Oracle Cloud Infrastructure FastConnect. It can also provide a path for private network traffic between your VCN and another VCN in a different region.

Service Gateway

A service gateway is another optional virtual router that you can add to your VCN. It provides a path for *private* network traffic between your VCN and supported services in the Oracle Services Network (examples: Oracle Cloud Infrastructure Object Storage and Autonomous Database). For example, DB Systems in a private subnet in your VCN can back up data to Object Storage without needing public IP addresses or access to the internet.

Local Peering Gateway (LPG)

A local peering gateway is another optional virtual router that you can add to your VCN. It lets you peer one VCN with another VCN in the same region. *Peering* means the VCNs communicate using

private IP addresses, without the traffic traversing the internet or routing through your on-premises network. A given VCN must have a separate LPG for each peering it establishes.

Route Table

These are virtual route tables for your VCN. They have rules to route traffic from subnets to destinations outside the VCN by way of gateways or specially configured instances. Your VCN comes with an empty default route table, and you can add custom route tables of your own.

DNS Choices

The Domain Name System (DNS) lets computers use hostnames instead of IP addresses to communicate with each other. Following are the choices for DNS name resolution for the instances in your VCN. You make this choice for *each subnet* in the VCN, using the subnet's set of DHCP options. This is similar to how you configure which route table and security lists are associated with each subnet.

DEFAULT CHOICE: INTERNET AND VCN RESOLVER

This is an Oracle-provided option that includes two parts:

- **Internet Resolver:** Lets instances resolve hostnames that are publicly published on the internet. The instances do not need to have internet access by way of either an internet gateway or a connection to your on-premises network (such as an IPSec VPN connection through a DRG).
- **VCN Resolver:** Lets instances resolve hostnames (which you can assign) of other instances in the same VCN.

CUSTOM RESOLVER

Use DNS servers of your choice for resolution (maximum three). They could be DNS servers that are:

- Available through the internet. For example, 216.146.35.35 for Dyn's Internet Guide.
- In your VCN.
- In your on-premises network, which is connected to your VCN by way of an IPSec VPN connection or FastConnect (through a DRG).

When you then launch an instance, you may assign a hostname. It's assigned to the VNIC that's automatically created during instance launch (that is, the *primary VNIC*). Along with the subnet domain name, the hostname forms the instance's fully qualified domain name (FQDN):

- **Instance FQDN:** `<hostname>.<subnet DNS label>.<VCN DNS label>.oraclevcn.com`

For example: `database1.privatesubnet1.abccorpvcn1.oraclevcn.com`.

The FQDN resolves to the instance's private IP address. The Internet and VCN Resolver also enables reverse DNS lookup, which lets you determine the hostname corresponding to the private IP address.

DHCP Options

The Networking service uses DHCP to automatically provide configuration information to instances when they boot up. Although DHCP lets you change some settings dynamically, others are static and never change. For example, when you launch an instance, either you or Oracle specifies the instance's private IP address. Each time the instance boots up or you restart the instance's DHCP client, DHCP passes that same private IP address to the instance. The address never changes during the instance's lifetime.

The Networking service provides *DHCP options* to let you control certain types of configuration on the instances in your VCN. You can change the values of these options at your discretion, unlike the static information that DHCP provides to the instance. The changes take effect the next time you restart a given instance's DHCP client or reboot the instance.

Each subnet in a VCN can have a single set of DHCP options associated with it. That set of options applies to all instances in the subnet. Each VCN comes with a *default set of DHCP options* with initial values that you can change. If you don't specify otherwise, every subnet uses the VCN's default set of DHCP options.

Here are the DHCP options you can set for your VCN:

- **Domain Name Server:** To specify your choice for DNS type (either Internet and VCN Resolver, or Custom Resolver).
- **Search Domain:** A single search domain of your choice. When resolving a DNS query, the OS appends this search domain to the value being queried.

Security Lists

Security lists are virtual firewall rules for your VCN. Security lists have ingress and egress rules that specify the types of traffic (protocol and port) allowed in and out of the instances. You can choose

whether a given rule is stateful or stateless. For example, you can allow incoming SSH traffic from anywhere to a subnet's instances by setting up a stateful ingress rule with source CIDR 0.0.0.0/0, and destination TCP port 22. Your VCN comes with a default security list with default rules, and you can add custom security lists of your own.

For a more detailed discussion of security lists and the types of rules, see VCN Security Lists at the end of this white paper.

VCN Connectivity

This section covers connectivity options for your VCN.

Access to Your On-Premises Network

There are two ways to connect your on-premises network to Oracle Cloud Infrastructure:

- VPN Connect: Offers multiple IPSec tunnels between your existing network's edge and your VCN, by way of a DRG that you create and attach to your VCN.
- Oracle Cloud Infrastructure FastConnect: Offers a private connection between your existing network's edge and Oracle Cloud Infrastructure. Traffic does not traverse the internet. Both private peering and public peering are supported. That means your on-premises hosts can access private IPv4 addresses in your VCN as well as regional public IPv4 addresses in Oracle Cloud Infrastructure (for example, Object Storage or public load balancers in your VCN).

You can use one or both types of the preceding connections. If you use both, you can use them simultaneously, or in a redundant configuration. These connections come to your VCN by way of a single DRG that you create and attach to your VCN. Without that DRG attachment and a route rule for the DRG, traffic does not flow between your VCN and on-premises network. At any time, you can detach the DRG from your VCN but maintain all the remaining components that form the rest of the connection. You could then reattach the DRG again, or attach it to another VCN.

For more information about IPSec VPNs and FastConnect, see the links in Scope and Assumptions.

Access to the Internet

See the previous discussion about internet gateways and NAT gateways.

Private Access to Oracle Services Such as Object Storage

You can have private access to Oracle services such as Oracle Cloud Infrastructure Object Storage by using one or both of the these solutions:

- **FastConnect public peering:** Gives your on-premises network private access to Oracle services. For the list of services, see https://cloud.oracle.com/en_US/fastconnect/services.
- **Service gateway:** Gives your VCN private access to specific supported Oracle services. For this list of services, see https://cloud.oracle.com/networking/service-gateway/supported-services.

For more information, see the scenario in Private Access to Oracle Services.

Access to Other VCNs: VCN Peering

VCN peering is the process of connecting multiple VCNs. There are two types of VCN peering:

- Local VCN peering (within region)
- Remote VCN peering (across regions)

You can use VCN peering to divide your network into multiple VCNs (for example, based on departments or lines of business), with each VCN having direct, private access to the others. There's no need for traffic to flow over the internet or through your on-premises network by way of an IPSec VPN or FastConnect. You can also place shared resources into a single VCN that all the other VCNs can access privately.

Because remote VCN peering crosses regions, you can use it (for example) to mirror or back up your databases in one region to another. For an example, see the scenario in Disaster Recovery Across Regions.

Note that two VCNs in a peering relationship cannot have overlapping CIDRs.

Access to Microsoft Azure

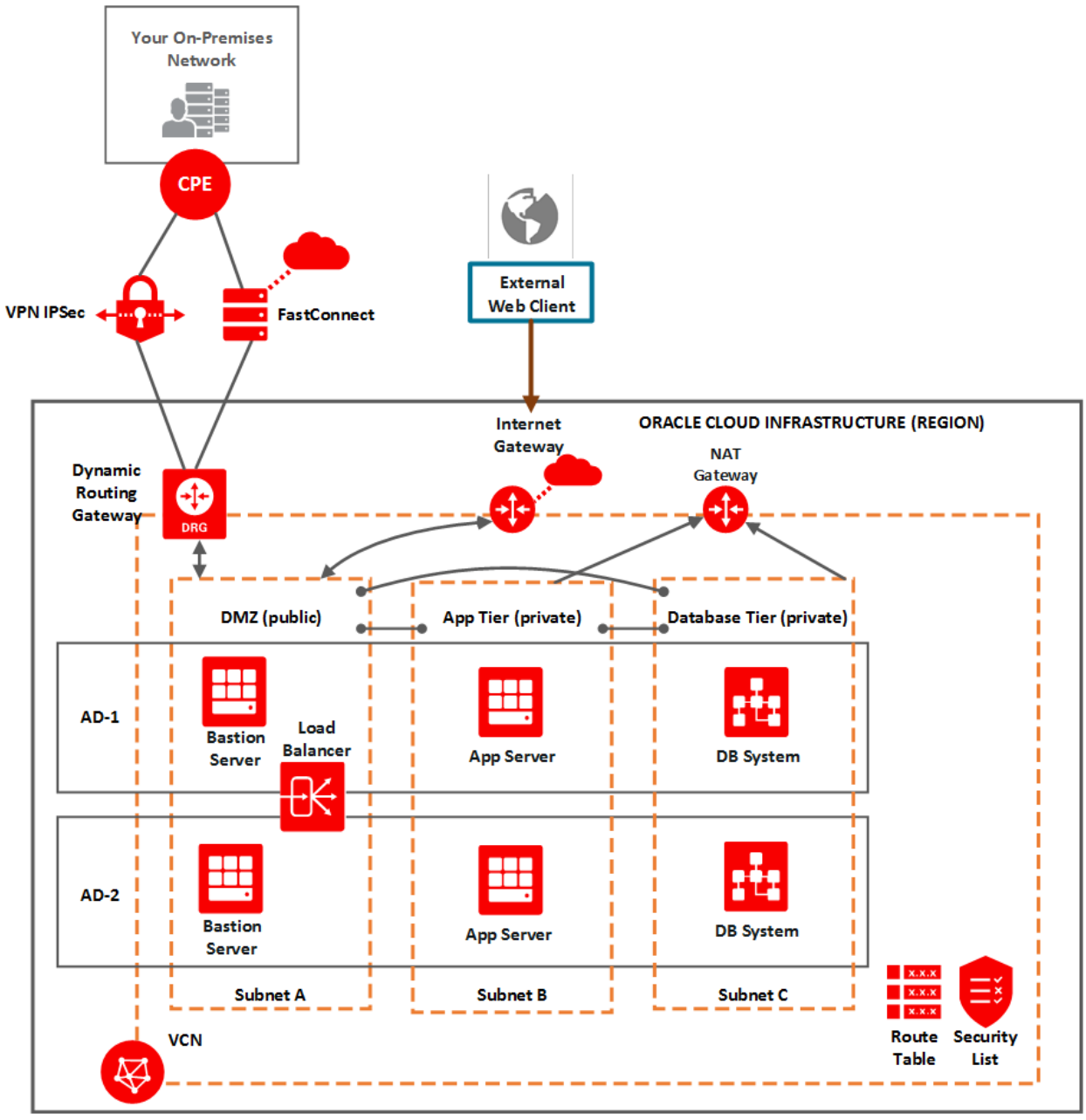
Oracle and Microsoft have created a cross-cloud connection between Oracle Cloud Infrastructure and Microsoft Azure in certain regions. This connection lets you set up cross-cloud workloads without the traffic between the clouds going over the internet. For more information, see https://www.oracle.com/cloud/oci-azure.html.

Scenarios for Using a VCN

This section has some scenarios that illustrate common patterns for using a VCN.

Multi-Tier Application Running on Oracle Cloud Infrastructure

This scenario shows a multi-tier, highly available application such as Oracle E-Business Suite running in multiple availability domains in a single Oracle Cloud Infrastructure region. You set up a single VCN with a set of regional subnets (one per tier) and resources replicated in two availability domains for high availability. The following diagram illustrates the general architecture.



Here's the general list of components:

- A regional public subnet for the DMZ tier, with instances that act as bastion hosts.
- A regional private subnet for the application tier, with instances that run the application logic.

- A regional private subnet for the database tier, with the application's DB systems.
- A connection from the VCN to your on-premises network. This is typically an IPSec VPN during a proof of concept (POC) and FastConnect in production.
- Gateways for the VCN:
    - DRG: For connectivity to the on-premises network, which includes administrative access and inbound application connections from internal clients.
    - Internet gateway: For direct connectivity to the internet, which includes inbound application connections from external clients on the internet.
    - NAT gateway: For indirect connectivity to the internet, so that resources in the private subnets can initiate outbound connections to the internet for software updates. Only the two private subnets have access to the NAT gateway.
- Custom route tables to control traffic from the subnets to the gateways.
- Custom security lists to control the types of traffic to and from resources in each subnet. For example: traffic with the DB systems is limited to incoming SSH traffic from the bastion instances and the required ingress and egress traffic with the application tier instances.
- Load balancers to balance the incoming application traffic.

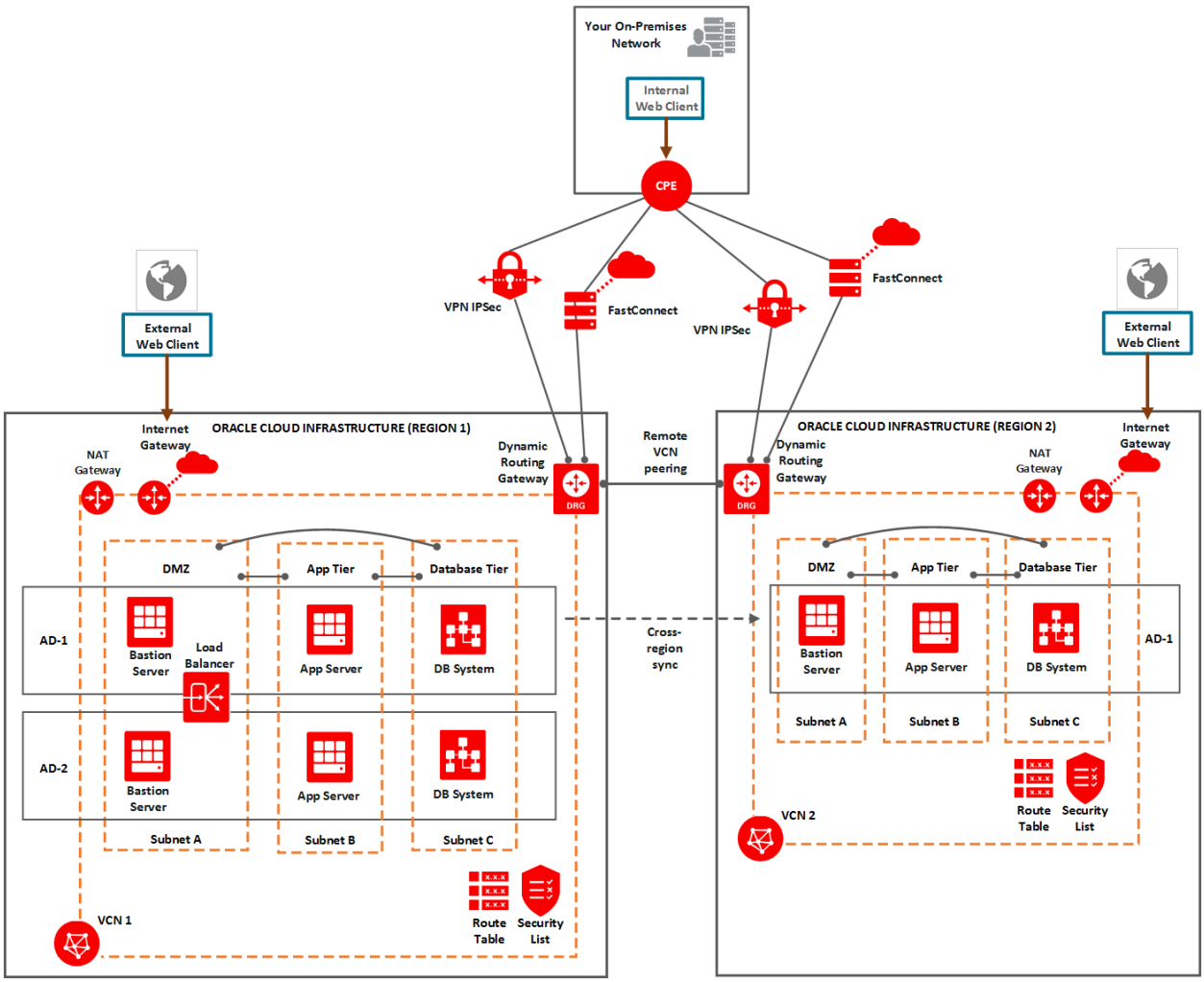
Disaster Recovery Across Regions

This scenario is a variation of scenario 1, but with a second region for disaster recovery (DR). Here you set up two VCNs, one in each region. The VCNs are peered, which means they have a private connection with traffic flowing over the Oracle network fabric and not the internet. The peering is *remote*, which means the two peered VCNs are in different Oracle Cloud Infrastructure regions.

Each VCN has a DRG. The DRG enables the VCN's private connectivity to the on-premises network over IPSec VPN or FastConnect. The DRG also enables the remote peering connection to the other VCN. The peering enables only the resources in the two VCNs to communicate with each other. Hosts in the on-premises network cannot use the peering connection to send traffic through one VCN to the other VCN.

As part of setting up the peering connection, the VCN administrator sets up particular IAM policies, route rules, and security lists for each VCN. Without them, traffic doesn't flow between the two VCNs.

The following diagram illustrates the general architecture.



Private Access to Oracle Services

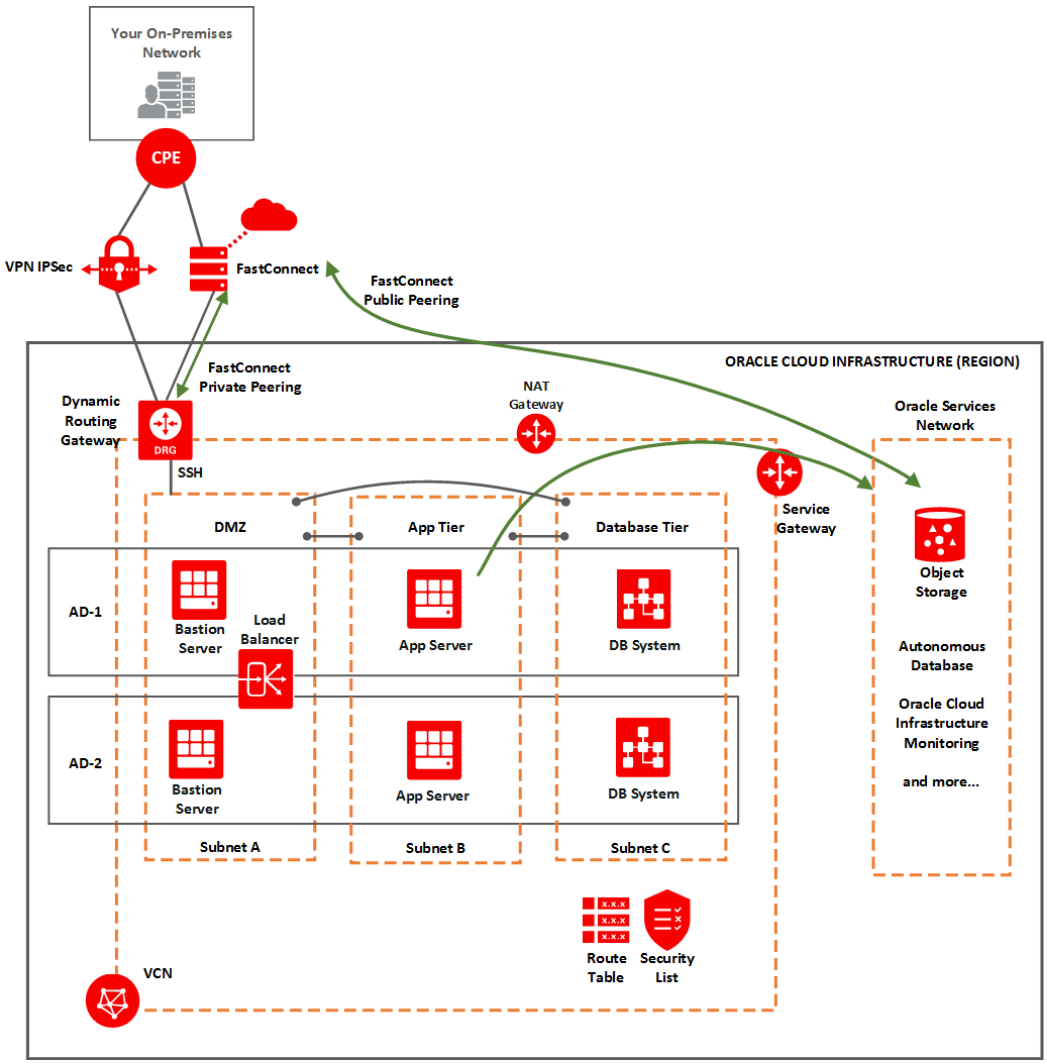
This scenario illustrates private access to Oracle services such as Oracle Cloud Infrastructure Object Storage and Autonomous Database from your on-premises network and your VCN. You can ensure that the traffic flows over the private Oracle network fabric and not the internet by using these components:

- **FastConnect public peering:** Gives your on-premises network private access to Oracle services. For the list of services, see https://cloud.oracle.com/en_US/fastconnect/services.

- **Service gateway:** Gives your VCN private access to specific supported Oracle services. For this list of services, see https://cloud.oracle.com/networking/service-gateway/supported-services.

The following diagram illustrates the general architecture. The FastConnect between the on-premises network and Oracle Cloud Infrastructure enables both the private peering connection through the VCN's DRG and the public peering connection to the Oracle Services Network.

The VCN's service gateway enables resources in the VCN to initiate outbound connections to supported services in the Oracle Services Network without the traffic flowing over the internet. The instances in the VCN can be in private subnets (and therefore have no public IP addresses) but reach the public endpoints of the supported Oracle services.



VCN Security Lists

You can help secure your VCN by using Networking service security lists. A security list provides a virtual firewall for an instance, with ingress and egress rules that specify the types of traffic allowed in and out. Each security list is enforced at the instance level. However, you configure your security lists *at the subnet level*, which means that all instances in a given subnet are subject to the same set of rules. The security lists apply to a given instance whether it's talking with another instance in the VCN or a host outside the VCN.

You can chose whether a given rule is stateful or stateless:

- **Stateful rules:** Marking a security list rule as stateful indicates that you want to use connection tracking for any traffic that matches that rule (for instances in the subnet the security list is associated with). This means that when an instance receives traffic matching the stateful ingress rule, the response is tracked and automatically allowed back to the originating host, regardless of any egress rules applicable to the instance. And when an instance sends traffic that matches a stateful egress rule, the incoming response is automatically allowed, regardless of any ingress rules.
- **Stateless rules:** Marking a security list rule as stateless indicates that you do NOT want to use connection tracking for any traffic that matches that rule (for instances in the subnet the security list is associated with). This means that response traffic is not automatically allowed. To allow the response traffic for a stateless ingress rule, you must create a corresponding stateless egress rule.

Default Security List

Each cloud network has a *default security list*. A given subnet automatically has the default security list associated with it if you don't specify one or more other security lists during subnet creation. At any time after you create a subnet, you can change which security lists are associated with it. And you can change the rules in the lists.

Unlike other security lists, the default security list comes with an initial set of stateful rules, which you can change:

- **Stateful ingress:** Allow TCP traffic on destination port 22 (SSH) from source 0.0.0.0/0 and any source port. This rule makes it easy for you to create a new cloud network and public subnet, launch a Linux instance, and then immediately connect via SSH to that instance without needing to write any security list rules yourself.
- **Stateful ingress:** Allow ICMP traffic type 3 code 4 from source 0.0.0.0/0. This rule enables your instances to receive Path MTU Discovery fragmentation messages.
- **Stateful ingress:** Allow ICMP traffic type 3 (all codes) from source = your VCN's CIDR. This rule makes it easy for your instances to receive connectivity error messages from other instances within the VCN.
- **Stateful egress:** Allow all traffic. This allows instances to initiate traffic of any kind to any destination. Notice that this means the instances with public IP addresses can talk to any internet IP address if the VCN has a configured internet gateway. And because stateful security

rules use connection tracking, the response traffic is automatically allowed regardless of any ingress rules.

The default security list comes with no stateless rules. However, you can add or remove rules from the default security list as you like.

References

- Networking service documentation
  - https://docs.cloud.oracle.com/iaas/Content/Network/Concepts/overview.htm
- Networking service FAQ
  - https://cloud.oracle.com/networking/vcn/faq
- Networking service video
  - https://www.youtube.com/embed/319ltOVoFHQ
- Oracle Cloud Infrastructure IPSec VPN deployment guide
  - https://docs.cloud.oracle.com/iaas/Content/Network/Tasks/managingIPsec.htm
- FastConnect documentation
  - https://docs.cloud.oracle.com/iaas/Content/Network/Concepts/fastconnect.htm
- VCN peering documentation
  - https://docs.cloud.oracle.com/iaas/Content/Network/Tasks/VCNpeering.htm
- Load Balancing service documentation
  - https://docs.cloud.oracle.com/iaas/Content/Balance/Concepts/balanceoverview.htm

Revision History

The following revisions have been made to this white paper since its initial publication:

Date	Revision
June 10, 2019	Add information about connection to Microsoft Azure
March 11, 2019	Update to service gateway information
February 19, 2019	Update for release of regional subnets

Date	Revision
November 2, 2018	New deployment scenarios
October 14, 2018	Editorial changes and small updates
January 2018	Initial publication

ORACLE CORPORATION, WORLD HEADQUARTERS
500 ORACLE PARKWAY
REDWOOD SHORES, CA 94065, USA

WORLDWIDE INQUIRIES
PHONE: +1.650.506.7000
FAX: + 1.650.506.7200

CONNECT WITH US

BLOGS.ORACLE.COM/ORACLE

FACEBOOK.COM/ORACLE

TWITTER.COM/ORACLE

ORACLE.COM

ORACLE
Cloud Infrastructure