# Table of Contents

Purpose of this Whitepaper 1

Scope & Assumptions 1

Virtual Cloud Network (VCN) Overview 1

VCN Components 3

- Subnet 3
- Virtual Network Interface Card (VNIC) 3
- Private IP 3
- Internet Gateway (IG) 4
- Dynamic Routing Gateway (DRG) 4
- Local Peering Gateway (LPG) 4
- Route Tables 4
- DNS Choices 5
- DHCP Options 5
- Security Lists 6

VCN Connectivity 6

Connect Your On-Premises Network to Your VCN 6

VCN Peering 6

Internet Access for Your VCN 6

- Scenario A: Public Subnets in a single AD 8
- Scenario B: Public Subnets in two ADs 9
- Scenario C: Private Subnets with an IPSec VPN 10
- Scenario D: Public and Private Subnets 11
- Scenario E: Network Address Translation (NAT) 12
Purpose of this Whitepaper

The purpose of this document is to provide an understanding of the Oracle Cloud Infrastructure Virtual Cloud Network (VCN) and common VCN deployment scenarios. You should have a basic knowledge of networking and internet routing to understand this whitepaper. This document is not intended to be a production deployment reference architecture.

Scope & Assumptions

This document outlines brief descriptions of various VCN components, typical deployment scenarios, and best practices for using a VCN. After reading this document, you will have a good understanding of what a VCN is, how to use a VCN in different scenarios, and the security best practices associated with it.

There are a number of products and topics that are beyond the scope of this document. While not all topics are listed, Identity Access Management (IAM) and FastConnect are examples of additional components used during typical VCN deployments.

Readers of this document 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/infrastructure/compute

» Have a basic understanding of Oracle Cloud Infrastructure Networking
  » https://cloud.oracle.com/networking

» Have a basic understanding of Oracle Cloud Infrastructure Identity Access Management (IAM)
  » https://docs.us-phoenix-1.oraclecloud.com/Content/Identity/Concepts/overview.htm?Highlight=Identity

» Have a basic understanding of VPN IPSec tunnel functionality

» Have a basic understanding of Oracle Cloud Infrastructure FastConnect
  » https://docs.us-phoenix-1.oraclecloud.com/Content/Network/Concepts/fastconnect.htm

Virtual Cloud Network (VCN) Overview

A virtual cloud network (VCN) is a virtual network that closely resembles a traditional network that you'd set up with firewall rules and specific types of communication gateways. A VCN covers a single, contiguous IPv4 CIDR block of your choice, where the IP ranges are private as per RFC 1918 and not publicly routable. VCNs also support a publicly routable range and customers can bring their public IP addresses. The allowable VCN size range is /16 to /30. VCNs reserve the first two IP addresses and the last one in each subnet's CIDR. After creating a VCN, you can't change its size, so it's important to think about the size of VCN and subnets you need before creating them.

A VCN can be configured with the following components automatically populated or manually:

» Default route table

» Default security list
» Default set of DHCP options

You can't delete these default components. However, you can change their contents, e.g. individual route rules, and you can create more of each kind of component, e.g. additional route tables. When you create a new subnet, you can associate a route table with it. If you don't, the default route table is automatically associated with the subnet. The same is true for security lists and sets of DHCP options. After you associate a particular route table, security lists, or sets of DHCP options with a subnet, you can't change that association, but you can change the contents of the components.

Figure 1. Default VCN Components
VCN Components

Subnet
A VCN resides within a single region but can cross multiple availability domains (AD). Each VCN network is subdivided into subnets (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 exists in a single AD and consists of a contiguous range of IP addresses that do not overlap with other subnets in the VCN. 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. You can designate a subnet as either public or private when you create it.

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 of 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 AD as the primary VNIC), or remove them as you like. Each secondary VNIC can be in the same subnet as other VNICs on the instance, or in a different subnet (in either the same or a different VCN). However, all the VNICs must be in subnets in the same AD as the instance. Here are a few reasons why you might use secondary VNICs:

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

Here are more secondary VNICs details and parameters:

- They are supported only for Linux instances (both VM and bare metal)
- There is 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 address and related information are 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. You can add a secondary private IP address 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. Here are a few reasons why you might use secondary private IPs:
» Run multiple services or endpoints on a single instance
» Instance failover

Here are more secondary private IP addresses details and parameters:

» They are 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)
» Removing a secondary IP from a VNIC returns the address to the pool of available addresses in the subnet
» They are automatically unassigned 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

Internet Gateway (IG)

Internet Gateway (IG) is an optional virtual router that you can add to a VCN for Internet connectivity. It provides Internet access to your VCN and is controlled by the Route Tables and Security List configuration at the subnet level. In addition to IG, you must have the following to access the Internet from the compute instance:

» Routing rule in Route Table that points to the IG
» Appropriate port open in the security list, e.g. Port 80/443 must be opened for web server traffic

Note: Having an Internet Gateway alone DOES NOT expose your subnet to the Internet unless you satisfy both conditions above.

Dynamic Routing Gateway (DRG)

A DRG is another optional virtual router that you can add to the VCN. The DRG provides a path for private network traffic between the VCN and on-premises network. You can use it with other networking service components and a router in your on-premises network to establish a connection via IPSec VPN or Oracle Bare Metal Cloud Services FastConnect.

Local Peering Gateway (LPG)

A LPG is a component on a VCN that lets that VCN peer with another VCN in the same region. Peering means that the two VCNs can communicate using private IP addresses, but without the traffic traversing the internet or routing through your on-premises network. A given VCN must have a separate LPG for each local peering it establishes (maximum 10 LPGs per VCN).

Route Tables

Virtual route tables for the VCN. The route table is a set of route rules that provides mapping for the traffic from subnets via gateways to destinations outside of the VCN. The VCN comes with a default route table and you can add more.
DNS Choices

The Domain Name System (DNS) enables lookup of other computers using hostnames. The following are the choices for DNS name resolution for the instances in your cloud network. You make this choice for each subnet using 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 use hostnames that are publicly published on the internet. The instances do not need to have access by way of either an Internet Gateway or an IPSec VPN connection.
    » VCN Resolver: Lets instances use host names (which you can assign) to communicate with other instances in the VCN.

» Custom Resolver
  » Use your own DNS servers (maximum three). These could be internet IP addresses for DNS (e.g. 216.146.35.35 for Don's Internet Guide), DNS servers in your VCN, or DNS servers in your on-premises network, which is connected to your VCN by way of an IPSec VPN connection.

When you launch an instance, you may assign a hostname. It's assigned to the VNIC that's automatically created during instance launch. 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

Your VCN uses DHCP options to automatically provide configuration information to the instances when they boot up. Each VCN comes with a default set of DHCP options with an initial value that you can change. If you don't specify otherwise, every subnet will use the VCN's default set of DHCP options. The following table lists the available DHCP options and the initial value for each in the default set of DHCP options.

<table>
<thead>
<tr>
<th>DHCP Option</th>
<th>Initial Value in the Default DHCP Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name Server</td>
<td>DNS Type: Internet and VCN Resolver</td>
</tr>
<tr>
<td>Search Domain</td>
<td>This option is present in the default set of DHCP options only if you specify a DNS label for the VCN during creation. In that case, the option's default value is the VCN domain name (&lt;VCN DNS label&gt;.oraclevcn.com)</td>
</tr>
</tbody>
</table>
Each subset 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. When you create the subnet, you specify which set to associate with the subnet. If you don't, the default set of DHCP options for the VCN is used.

Security Lists

Security Lists are a virtual firewall for your VCN on OCI. Each security list consists of ingress and egress rules that specify the destination (CIDR) and type of traffic (Protocol and Port) allowed in and out of instances within a subnet. A security list is attached to a subnet and you can change the traffic type/destination dynamically. For example, a rule in security lists with source CIDR 0.0.0.0/0 with destination port 22 of TCP protocol will allow all ingress traffic from any IP address on to OCI instances on port 22 for ssh connection.

VCN Connectivity

Connect Your On-Premises Network to Your VCN

There are two ways to connect your on-premises network to your VCN:

» IPSec VPN: Offers multiple IPSec tunnels between your existing network’s edge router and the Dynamic Routing Gateway (DRG) that you create and attach to your VCN.

» Oracle Cloud Infrastructure FastConnect: Offers a private connection between your existing network’s edge router and your DRG. Traffic does not traverse the internet.

You can use one or both types of connections. If using both, you can use them simultaneously, or in a redundant configuration. All connections come to your VCN via a single DRG that you create and attach to your VCN, using either the Console or API. Without that DRG attachment and a route rule for the DRG, traffic will not flow between your VCN and on-premise 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 VPN and FastConnect, see Section References.

VCN Peering

VCN peering is the process of connecting multiple VCNs. As of today, peering among the VCNs residing in the same region is possible. This is called Local Peering. This enables the resources of each VCN present in the same region and tenancy to communicate using private IP addresses without routing the traffic over the internet or through your on-premises network. Without peering, a given VCN would need an Internet Gateway and public IP addresses for the instances that need to communicate with another VCN. Two VCNs in a peering relationships cannot have overlapping CIDRs. For more information on VCN Peering, refer to ‘Typical Scenarios for using a VCN’ section.

Internet Access for Your VCN

For instances in a given subnet to have direct access to the internet:

» The VCN must have an Internet Gateway that is enabled

» The subnet must have a route rule that directs traffic to the gateway
» The subnet must have security list rules that allow the traffic (and each instance's firewall must allow the traffic)

» Each instance must have a public IP address

Instances without public IP addresses or access to an Internet Gateway cannot access the internet directly. However, you can configure a subnet to access the internet indirectly by setting up an internet proxy in your on-premises network and then connecting that network to your VCN via a DRG. With the recent enhancements to networking service, you can now enable outbound Internet access from your private instances using NAT instances.
Typical Scenarios for Using a VCN

Scenario A: Public Subnets in a single AD

Example Use Cases: VCN for running a single-tier, public-facing web application such as a blog or simple website in a single AD.

This is the fastest way to try out the Networking Service. The following figure illustrates the scenario. You set up a VCN with:

» One public subnet in a single AD
» An Internet Gateway
» A corresponding route rule in the default route table
» The default security list
» The default set of DHCP options
» A DNS hostname

If you want the instances in the VCN to have DNS hostnames (which can be used with the Internet and VCN resolvers, a built-in DNS capability in the VCN), you can specify a DNS label for the VCN, or let the console auto-generate one for you. The DNS name for the VCN will be in the format <VCN DNS label>.oraclevcn.com. The instance FQDN will be in the format <hostname>.<subnet DNS label>.VCN DNS label>.oraclevcn.com

You then launch one or more compute instances in one of the subnets. Each instance automatically gets both a public and private IP address. You can then communicate with the instances via the public IP address over the internet from your on-premises network.

Figure 2. Public Subnets in a single AD.
Scenario B: Public Subnets in two ADs

Example Use Cases: VCN for running a single-tier, high availability (HA), public-facing web application.

This scenario adds redundancy in a second AD for high availability. A public load balancer pair can be used in this scenario which can be used to distribute the traffic across the backend instances. A public load balancer can distribute traffic to the instances across multiple ADs. The following figure illustrates the scenario. For more information on OCI's Load Balancing, see section References.

You set up a VCN with:

- One public subnet per AD
- An Internet Gateway
- A corresponding route rule in the default route table
- The default security list
- The default set of DHCP options
- A public load balancer pair (Active/Standby) in separate subnets and ADs, not overlapping with the instance subnets
- Appropriate security lists and route rules to direct the traffic from the load balancer to the backend subnets in separate ADs.

![Diagram of Public Subnets]

Figure 3. Public Subnets.

You then launch one or more compute instances in one of the subnets. Each instance automatically gets both a public and private IP address. You can then communicate with the instances via the public IP address over the internet from your on-premises network or you can include the instances as part of a backend pool of servers and can be accessed seamlessly using the public IP of the load balancer.
Scenario C: Private Subnets with an IPSec VPN

Example Use Cases: VCN for extending your data center into OCI and leverage OCI’s infrastructure without exposing your network to the Internet.

In this scenario, you set up a VCN with:

- Two private subnets in separate ADs (to illustrate redundancy)
- A VPN connection to provide private communication with your on-premises network
- A corresponding route rule in the default route table
- A modified default security list with additional rules to allow these additional types of traffic:
  - Stateful ingress rule for traffic from anywhere on TCP port 80 (HTTP)
  - Stateful ingress rule for traffic from anywhere on TCP port 443 (HTTPS)
  - Stateful ingress rule for traffic from anywhere on TCP port 1521 (for Oracle Databases)
- The default set of DHCP options

![Diagram of Private Subnets with an IPSec VPN](image)

Figure 4. Private Subnets with an IPSec VPN.

Figure 4 illustrates the general layout. To use this scenario, you must have a network administrator configure the router at your end of the IPSec VPN. You can then launch an instance in your VCN and communicate with it using its private IP address from your on-premises network. You might use this scenario, if you want to extend your private database servers in your on-premises network into the cloud.
Scenario D: Public and Private Subnets

Example Use Cases: VCN for running a multi-tier, HA, public-facing web application while still maintaining non-publicly accessible back-end servers in a second subnet.

The instances in the public subnet can send outbound traffic directly to the Internet, whereas the instances in the private subnet can’t. The instances in the private subnet can only connect with their on-premises network via an IPSec tunnel. This way the private subnets just act as an extension of their on-premises environment typically hosting Databases which need connectivity only with the web servers within the VCN and also with the on-premises environment.

In this scenario, you set up a VCN with:

» Both a public subnet and a private subnet in a single AD
» Similar subnets in a second AD for redundancy
» An Internet Gateway so that instances in the public subnets can communicate with the internet using their public IP addresses
» An IPSec VPN so that instances in the private subnets can communicate securely with your on-premises network using their private IP addresses
» Two route tables to direct traffic out of the VCN; one for traffic to the internet and one for traffic to your on-premises network
» A modified default security list where you change all the existing stateful ingress rules to allow traffic only from your on-premises network’s CIDR block
» A separate security list just for the public subnets with these rules:
  » Stateful ingress rule for traffic from anywhere on TCP port 80 (HTTP) and port 443 (HTTPS)
  » Stateful egress rule for any traffic to the private subnets on TCP port 1521 (for Oracle DB)
» A separate security list just for the private subnets with these rules:
  » Stateful ingress rule for any traffic to the public subnets on TCP port 1521 (for Oracle DB)
  » Stateful ingress rule for any traffic to the private subnets on TCP port 1521 (for Oracle DB)
  » Stateful egress rule for any traffic to the private subnets on TCP port 1521 (for Oracle DB)
» The default set of DHCP options

Notice that the public subnet would use both the default security list and the public subnet security list. Likewise, the private subnet would use both the default security list and the private subnet security list. Default security list contains a core set of stateful rules that all subnets in the scenario need to use.

To use this scenario, you must have a network administrator configure the router at your end of the IPSec VPN. You might use this scenario to host a cloud-based website that’s connected to a DB. The web servers reside in the public subnet and are thus reachable from the internet. The DB servers reside in the private subnet.
Scenario E: Network Address Translation (NAT)

Example Use Cases: VCN for running a multi-tier, HA, public-facing web application while still maintaining non-publicly accessible back-end servers in a second subnet, while implementing a Network Address translation (NAT) or a virtual network function (such as firewall or intrusion detection) that filters outgoing traffic from instances. This can also be used to provide outbound Internet access to instances that don’t have direct Internet connectivity. Additionally, this feature can also be used to manage an overlay network on the VCN, which lets you run container orchestration workloads.

In this scenario, you can setup a VCN with:

- Both a public subnet and a private subnet in a single AD.
- Two instances, NAT 1 and NAT 2 in the public subnet.
- One or more instances in the backend or private subnet, with the private IPs in the same VCN as the route table.
- Private IPs VNIC configured to skip the source/destination check so that the VNIC can forward the traffic.
- A route rule for the private subnet with destination CIDR as 0.0.0.0/0 and route target as the private IP of the NAT instances.
Scenario F: VCN Peering

Example Use Cases: Business Groups or Lines of Businesses may wish to divide their network into multiple VCNs (for example, based on departments or lines of business), with each VCN having direct, private access to the others. There is no need for traffic to flow through on-premises network via an IPSec or FastConnect. Without peering, a given VCN would need an Internet Gateway and public IP addresses for the instances that need to communicate with another VCN.

There are a few IAM policies which need to be taken into consideration while setting up VCN Peering. To implement the IAM policies required for peering, the two VCN administrators must designate one administrator as the requestor and the other as the acceptor. The requestor must be the one to initiate the request to connect the two LPGs. In turn, the acceptor must create a particular IAM policy that gives the requestor permission to connect to LPGs in the acceptor’s compartment. Without that policy, the requestor’s request to connect fails.

In this scenario, you set up two VCNs with:

» Non-overlapping CIDR ranges in the same region, but same or different ADs.

» Private or public subnets in each VCN.

» A Local Peering Gateway (LPG) per VCN so that instances in each VCN’s subnets can communicate with one another by peering.
An information sharing between the administrators. An Acceptor of the information shares the following information with the requestor.

- VCNs’ name and compartment
- LPG’s name, OCID and compartment.

Requestor shares the following information with the acceptor

- Name of the IAM group that should be granted permission to create a connection in the acceptor’s compartment

IAM policies to ensure that both the requestor and acceptor have the right IAM polices in place which govern which groups within each VCN can initiate/accept connections with one another.

A task to establish the connection to the acceptor’s LPG by the requestor, based on the information shared by the acceptor. At this point, the details of each LPG update to show the Peer VCN CIDR Block for the other VCN. This is the CIDR of the other VCN across the peering from the LPG. Each administrator can use this information to update the route tables and security lists for their own VCN.

Route rules in the Route tables of both the VCNs, by determining which subnets in each VCN need to communicate with the other VCN and accordingly adding the rules that direct traffic destined for the other VCN’s CIDR to the local LPG.

Without the required routing, traffic doesn’t flow between the peered LPGs. If a situation occurs where you need to temporarily stop the peering, you can simply remove the route rules that enable traffic. You don’t need to delete the LPGs.

Ingress security rules to control which types of traffic you want to allow from the other VCN, specially from the VCN’s CIDR or specific subnets.

Egress security rule to allow outgoing traffic from your VCN to the other VCN. If the subnet already has a broad egress rule for all types of protocols to all destinations (0.0.0.0/0), then you don’t need to add a special one for the other VCN.
A VCN can be secured with the help of 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 may configure the 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 taking with another instance in the VCN or a host outside of the VCN. You can choose whether a given rule is stateful or stateless. The VCN comes with a default security list and you can add more.

**Stateful Security Lists:** Stateful rules indicate connection tracking for any traffic that matches the rules. 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 Security Lists:** Stateless rules indicate no connection tracking for any traffic that matches the rules. This means that response traffic is not automatically allowed. To allow response traffic for a stateless ingress rule, you must create a corresponding stateless egress rule.
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. After you create a subnet, you can’t change which security lists are associated with it. However, you can change the rules in the lists.

» 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 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.

» Stateful ingress: Allow ICMP traffic type 3 code 4 from source 0.0.0.0/0 and any source port. This rule makes it easy to receive Path MTU Discovery fragmentation messages if you’re using jumbo frames.

» Stateful ingress: Allow ICMP traffic type 3 (all codes) from your VCN’s CIDR and any source port. This rule makes it easy for your instances to receive connectivity error messages from other instances within the VCN.

» Stateful egress: Allow all outgoing traffic. This allows instances to initiate traffic of any kind to any destination.

The default security list comes with no stateless rules. However, you can add or remove rules from the default security list as you like. Stateless rules are recommended if you have a high-volume internet-facing website.

Conclusion

This white paper captures the key Oracle Cloud Infrastructure Virtual Cloud Network components and their descriptions. It also outlines a few typical scenarios for using a VCN – public subnets, private subnets with an IPSec VPN, public & private subnets and VCN peering.

References

» Overview of Networking Service
» VCN FAQ
» VCN Video
» IPSec VPN Deployment Guide
» OCI FastConnect overview
» VCN Peering
» OCI Network Address Translation (NAT)
» Load Balancing as a Service