Connectivity - VPN Connect (IPSec)

Level 200

Jamal Arif
Oracle Cloud Infrastructure
October, 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

After completing this lesson, you should be able to:

- VPN Connect Design details
- VPN Connect Demo

Connectivity options

Public Internet

- Reserved IPs
- Ephemeral IPs
- Internet Data out Pricing (first 10TB free)

VPN Connect (IPSec)

- IPSec authentication and encryption
- Two main options
  - OCI managed VPN Service (free)
  - Software VPN (running on OCI Compute)

FastConnect

- Private dedicated Connection
- Consistent network experience
- Port speeds of 1 Gbps, 10 Gbps
- SLA

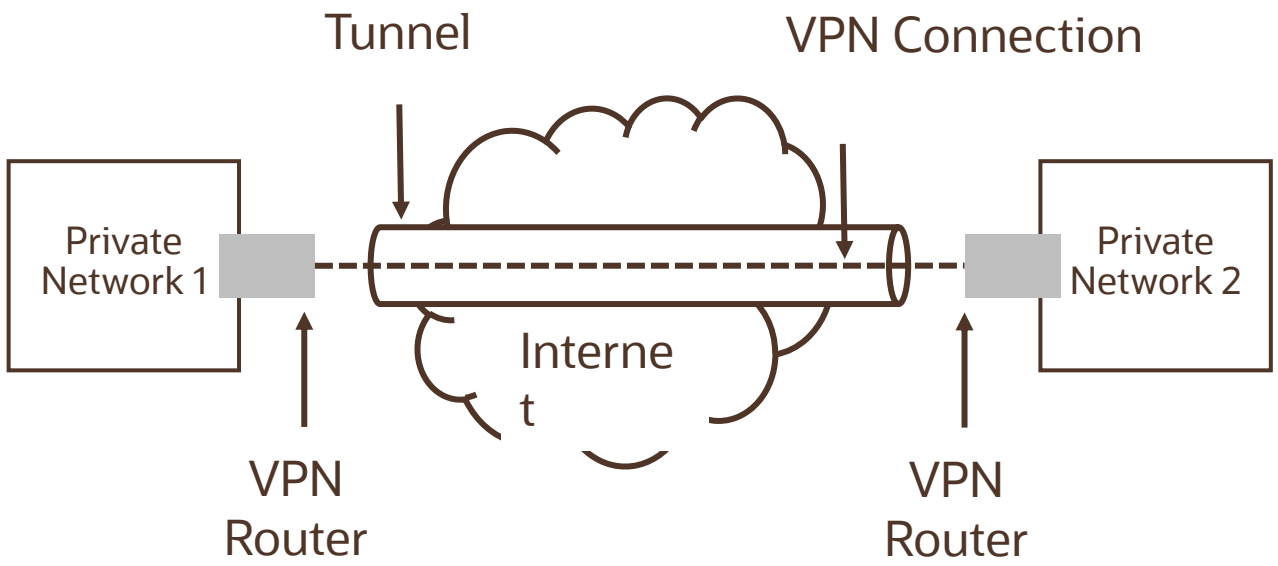
Connectivity to on-premises network planning

Connecting your virtual cloud network (VCN) to your on-premises network requires certain design considerations

- What kind of **Bandwidth/throughput** your application requires?
- Is your application **Latency sensitive**?
- Are you planning to provide **Redundancy** to your on-premises connectivity and avoid single point of failure?
- Do you require a **secure** and **private dedicated** connection or a public connection over the internet ?
- Do you see your services growing, and plan to dynamically **scale up** your application bandwidth needs?

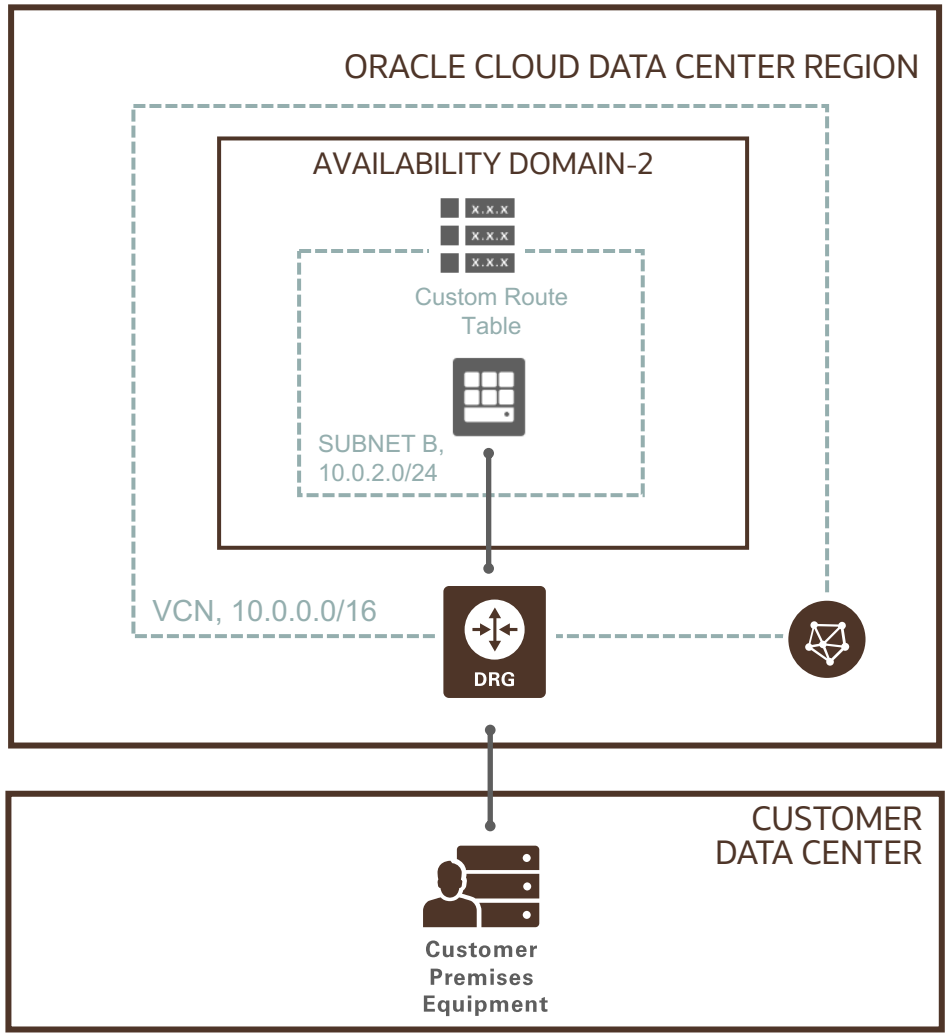
VPN Basics

VPN – using a public network to make end to end connection between two private networks in a secure fashion



- **Tunnel** – a way to deliver packets through the internet to private RFC 1918 addresses
- **Authentication** – provides a mechanism to authenticate who you are
- **Encryption** – packets need to be encrypted, so they cannot be sniffed over the public internet
- **Static routing**: configure a router to send traffic for particular destinations in preconfigured directions
- **Dynamic routing**: use a routing protocol such as BGP to figure out what paths traffic should take

VPN Connect (IPSec)



- VPN Connect is a managed VPN service which securely connects on-premises network to OCI VCN through an **IPSec VPN connection**
- VPN Connect ensures secure remote connectivity via industry standard IPSec encryption
- Bandwidth is dependent on the customer's access to the Internet and general Internet congestion (Typically less than 250 Mbps – but your mileage may vary)
- VPN Connect is offered for free
- Customer Proof of Concepts usually start as a VPN and then morph into FastConnect designs
- OCI provisions redundant VPN tunnels located on physically and logically isolate tunnel endpoints

OCI VPN Concepts

- Dynamic Routing Gateway - VPN headend at OCI end of the VPN connection.
- Customer Premise Equipment (CPE)
  - Actual VPN router/Edge device in your on-premises network (hardware or software)
  - When setting up the VPN, you create a virtual representation of your on-premises router, which is known as CPE object
  - To Create a CPE Object – Name, Outside Public IP address
- IPSec Connection
  - After creating the CPE object and DRG, you connect them by creating an IPSec connection, which results in multiple redundant IPSec tunnels
- While creating an IPSec connection, configure the type of routing
  - BGP dynamic routing
  - static routing
- When you set up an IPSec VPN, by default Oracle provides each tunnel's shared secret/pre-shared key. You can also specify your own shared secret key instead.

OCI IPSec VPN Routing Choices

- When you create an IPSec VPN, it has two redundant IPSec tunnels. We encourage you to configure your CPE device to use both tunnels
- Two routing types are available :
  - Static routing
  - Dynamic Routing based on Border Gateway Protocol (BGP)
- You configure the routing type per tunnel. Only one type of routing at a time is supported for a given tunnel.
- Static routing is the default type of routing for all tunnels unless you explicitly configure each tunnel to use BGP.
- If you choose BGP, for each tunnel you must provide two IP addresses along with ASN. Incase you opt static, you must provide at least one static route with maximum of 10.

Changing Routing Type of IPSec tunnel

- You can change an existing tunnel's routing type at any time
- While you change the routing, the tunnel remains up - its IPSec status does not change.
- However, traffic flowing through the tunnel is disrupted temporarily during re-provisioning and while you reconfigure your CPE device
- Since you configure the routing type separately for each tunnel, if you want to switch your IPSec VPN from static routing to BGP, you can do it one tunnel at a time. This avoids the entire IPSec VPN being down
- If you want to change a tunnel from BGP to static routing, you must first ensure that the IPSec connection itself has at least one static route associated with it.

VPN Quickstart WorkFlow

- The Oracle Console includes a VPN Connect workflow to help you quickly set up an IPSec connection between your on-premises network and virtual cloud network (VCN)
- You can now provide all the information to configure an IPSec VPN connection, CPE and DRG in one single, guided workflow page.
- This workflow provides an alternate to manually setting up these components on the individual object pages in the Console, reducing the number of separate configuration windows
- It includes automatic VCN creation and setup, along with routes and security lists to connect the VCN successfully to the on-premises network.
- Workflow Assumptions:
  - Only set up static routing for your IPSec tunnels.
  - You do not already have a VCN.
  - You want an internet gateway for easy initial access to the VCN.

Demo

Summary

You should be able to learn ..

- How to create a IPSec VPN connection.
- Design principles for VPN Connectivity.

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