ORACLE
Cloud Infrastructure

Encrypted FastConnect

Public Peering

ORACLE WHITE PAPER | AUGUST 2019

Disclaimer

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, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Revision History

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

Date	Revision
August 30, 2019	Initial publication

Table of Contents

Overview

FastConnect and VPN Connect are two key ways for Oracle customers to connect to Oracle Cloud Infrastructure. FastConnect provides a private connection between a customer's on-premises network and Oracle Cloud Infrastructure, with predictable performance. VPN Connect provides a secure (encrypted) connection over the internet, which might not provide predictable latency and performance.

Some enterprises need to encrypt the data flowing through FastConnect to meet security and compliance requirements or to protect sensitive and business-critical information as it moves from on-premises to the cloud. You can achieve this by using the FastConnect and VPN Connect services together. VPN Connect leverages IPSec (IP Security) tunneling technology, which uses industry-standard encryption and cryptographic algorithms. When used with a FastConnect virtual circuit, it provides a secure and dedicated connection with predictable performance.

Assumptions and Prerequisites

This document assumes that you're familiar with routing protocols and concepts, IPSec VPN technology (encryption) and configuration, the fundamentals of Oracle Cloud Infrastructure, and the Oracle Cloud Infrastructure Console.

To use the options described in this document, you need to have a virtual cloud network (VCN) in place and use FastConnect to connect to Oracle Cloud Infrastructure from your on-premises network.

Encrypted FastConnect

FastConnect provides two peering options: private and public. This document focuses on encrypting FastConnect with public peering.

You can deploy this solution with any of the FastConnect options currently available: Oracle provider, third-party provider, and colocation with Oracle. FastConnect is represented in the diagrams in this document with a gray cloud.

Note: This document doesn't address FastConnect with private peering. If you're interested in the private peering use case, send a message to oci_c3pm_us_grp@oracle.com.

FastConnect with Public Peering

After you successfully deploy FastConnect from your on-premises network to Oracle Cloud Infrastructure, you configure a public virtual circuit (the blue line in Figure 1) in the Oracle Console. When the connection is established, you create a customer on-premises equipment (CPE) object and an IPSec connection in the Oracle Console. Then, you configure your on-premises VPN CPE and establish an IPSec tunnel to Oracle headends, as depicted in Figure 1 (green line).

Figure 1 assumes that the CPE at the on-premises network where FastConnect terminates can also perform the VPN function. The VPN CPE could also sit behind the CPE as a separate device.

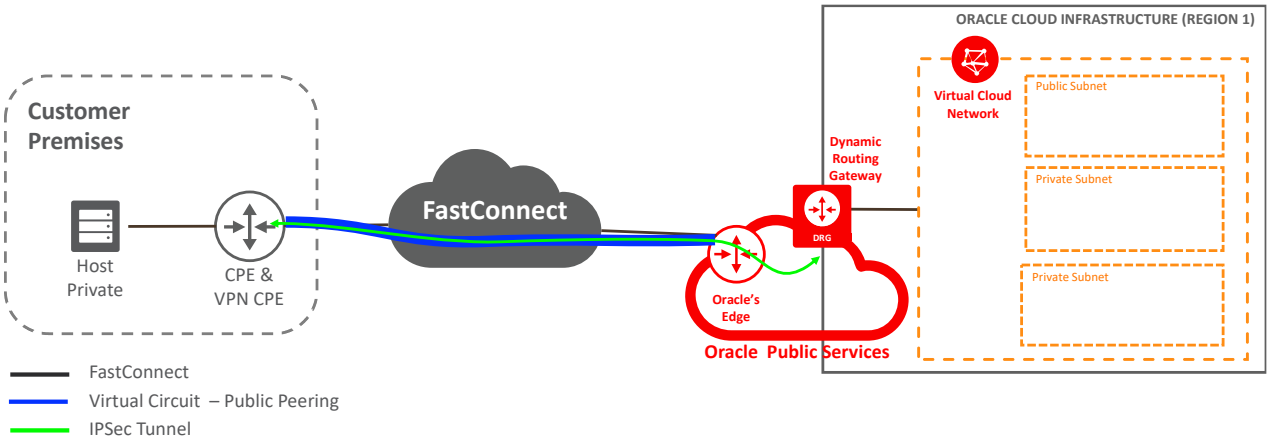

Figure 1. IPSec over FastConnect Public Peering

By default, Oracle provides two VPN headends for redundancy when deploying VPN Connect. For simplicity, the diagrams in this document show only one of the tunnels. The public IP addresses for the Oracle headends are advertised as part of the public subnets of the Oracle Services Network in each region when you create a public virtual circuit. These IP addresses are learned via Border Gateway Protocol (BGP), so they should already be part of your route table when the public virtual circuit was established. Over the BGP connection, advertise the public IP addresses of your VPN CPE to Oracle Cloud. The IPSec tunnel is established over the public virtual circuit, which doesn't go over the internet. Public peering is an alternative to the internet.

When deploying this solution, consider the following points:

- The VPN terminates at the Oracle VPN headends. You configure the VPN tunnel by using the Oracle Console.
- Encryption adds overhead and might not provide the full bandwidth of the subscribed FastConnect.

- By default, Oracle provides two VPN headends, so basically you have two tunnels for each VPN Connect. These tunnels are both active, but Oracle always uses a single tunnel to send traffic to your on-premises network.
- Ensure that you have redundancy deployed for FastConnect.
- Routing has two parts:
    - **FastConnect:** Over the FastConnect public virtual circuit, the public IP addresses of the Oracle headends and your VPN CPE are exchanged via BGP.
    - **VPN Connect:** The standard configuration for VPN Connect using BGP or static routing is followed. If you use static routing, you must point traffic from the on-premises side to the VCN to the VPN interface of your VPN CPE.
- Security lists at the on-premises network and the VCN need to allow traffic based on the applications' requirements.
- FIPS 140-2 validation is available in Government cloud regions only.
- If you need help troubleshooting issues with the VPN Connect connection, contact Oracle Support.

Implementing IPSec over FastConnect Using Public Peering

This section provides the general steps for implementing IPSec over FastConnect by using public peering. For step-by-step instructions on how to deploy FastConnect with public peering and VPN Connect, see the References section at the end of the document or the links provided in the general steps.

These steps assume that you already have Oracle Cloud Infrastructure and a tenancy.

1. In Oracle Cloud Infrastructure, create a VCN.
2. Create subnets within your VCN. These are the subnets that host your compute instances.
3. Create a dynamic route gateway (DRG).
4. Attach the DRG to your VCN.
5. Create FastConnect through a provider (Oracle or third party) or colocated with Oracle. For step-by-step instructions, see the FastConnect documentation.
6. After FastConnect is successfully provisioned, create a public virtual circuit. You establish a BGP peering relationship between your CPE and Oracle's edge. You must provide a public ASN and also registered public IP addresses (the IP addresses for your VPN CPE)

to complete this step. Oracle verifies that the IP addresses belong to you before advertising them. The IP addresses of Oracle's VPN headends are part of the public subnets advertised to you. Oracle provides a /30 subnet to address the BGP peers over the public virtual circuit.

7. Verify that BGP and Layer 3 functionality is established between your CPE and Oracle.

8. Configure VPN Connect by creating a CPE object in the Console. For step-by-step instructions, see Task 2g in Setting Up VPN Connect. This is the logical representation of your VPN CPE, which terminates the IPSec tunnel on your on-premises network.

9. Create an IPSec connection, which is the connection between your VPN CPE and the DRG. In this step, you can select to use static routing or dynamic routing (BGP) between your VPN CPE and the DRG. For step-by-step instructions, see Task 2h in Setting Up VPN Connect.

10. Configure your VPN CPE and set up the IPSec tunnels to the Oracle VPN headends provided in the previous step. For step-by-step instructions, see Task 3 in Setting Up VPN Connect.

11. Update your security lists in the VCN and your on-premises network to allow traffic based on your applications' requirements.

    Figure 2 shows the results of the configuration. Here you can see the various components that make up the solution: FastConnect, VPN Connect, DRG, VCN, customer premises, and routing.

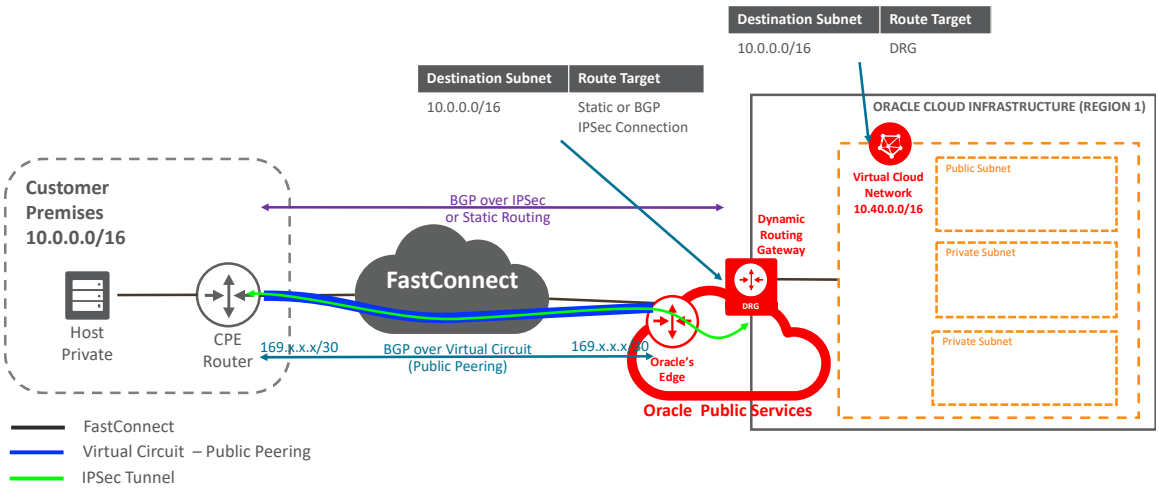

Figure 2. IPSec over FastConnect Public Peering—Routing

12. Initiate interesting traffic from your on-premises network and Oracle Cloud to bring up the tunnel. You can do this by initiating a ping between a device in your on-premises network (10.0.x.x/16) and a VM on any of the subnets in your VCN (10.40.x.x/16).

    As interesting traffic passes through the tunnel, you should see phase 1 and phase 2 up on your VPN CPE and the tunnel should show an Up state. If not, troubleshoot the tunnel configuration parameters and preshared key to ensure that the IPSec parameters match on both sides. Also, check any firewall on your on-premises network that might be blocking VPN traffic.

    If the ping between the two endpoints is successful, you have encrypted the traffic over FastConnect. If not, check routing at the subnet level and at the VPN level to ensure that you receive the correct routes. Also, check security lists to ensure that ping is allowed and application traffic for your requirements is allowed.

Achieving Higher Capacity

Encryption adds overhead to the connection, which directly affects the throughput of the connection. You might have a 10Gbps FastConnect connection, but the devices performing the encryption might not support this speed. To achieve more bandwidth (aggregate) between the on-premises network and Oracle Cloud, you could perform the following tasks:

- Create multiple VPN Connect connections to a single VCN.
- Create multiple VCNs with their respective VPN Connect connections.

This approach requires routing engineering, segregation of traffic on both ends of the connection, no IP address overlapping between tunnels, and individual VPN headends per virtual circuit or VCN. It also adds complexity of the solution and needs detailed documentation for support and troubleshooting.

Create Multiple VPN Connect Connections to a Single VCN

Figure 3 shows a 1Gbps FastConnect connection and a public virtual circuit (blue line). Oracle provides two VPN headends for each VPN Connect connection that you create in the Console. To create multiple VPN Connect connections, you must provide multiple public IP addresses for your VPN CPE. Then, you can create additional CPE objects on the Oracle Console to represent each VPN CPE. Now, there are two VPN headends on your side, and each one creates a tunnel as represented by the green lines.

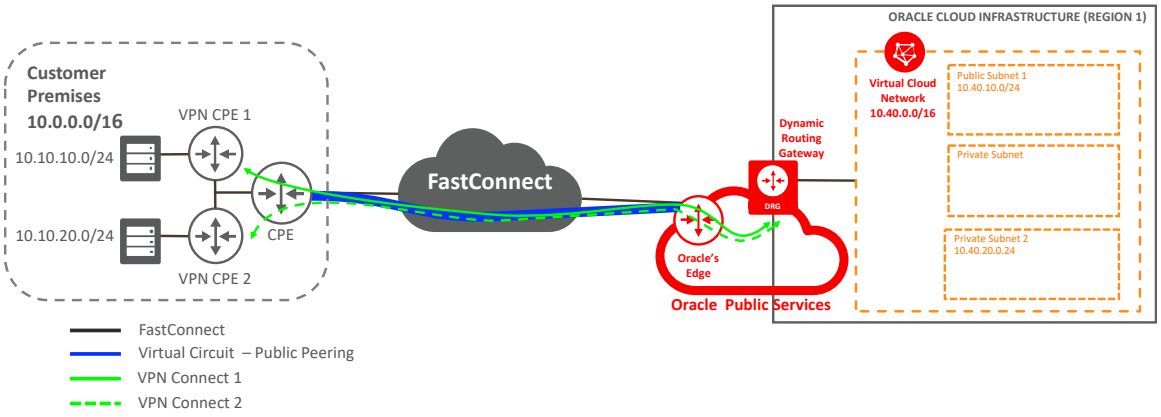

Figure 3. IPSec over FastConnect: Multiple Tunnels

Note: Oracle can provide up to four different headend pairs per region. The limitation to this solution is the number of unique public VPN CPEs that you and Oracle can provide.

VPN Connect 1 (green solid line), built between an Oracle headend and VPN CPE 1, allows traffic between 10.10.10.0/24 and 10.40.10.0/24. VPN Connect 2 (green dotted line), built between an Oracle headend and VPN CPE 2, allows traffic between 10.10.20.0/24 and 10.40.20.0/24. Assuming that each tunnel can support 250Mbps, by creating the two tunnels, you can support 500Mbps in a 1Gbps FastConnect connection.

For routing, there are two parts:

- FastConnect

  Over the public virtual circuit, Oracle advertises all the public subnets for the region. The IP addresses of the headends are part of these subnets. You advertise the public IP addresses of VPN CPE 1 and 2.

- VPN Connect
  - From the Oracle side, Oracle advertises all the VCN subnets over the two tunnels via BGP. You filter the subnets received on VPN CPE 1 and 2 to accept the subnet 1 (10.40.10.0/24) and 2 (10.40.20.0/24) respectively, instead of accepting all the VCN subnets. If you are using static routing, advertise 10.10.10.0/24 via VPN Connect 1 and 10.10.20.0/24 via VPN Connect 2.
  - You advertise 10.10.10.0/24 from VPN CPE 1 and 10.10.20.0/24 from VPN CPE 2 via BGP. If you are using static routing, point 10.40.10.0/24 to VPN CPE 1 and 10.40.20.0/24 to VPN CPE 2.

This solution doesn't allow any-to-any communication. The design is very segmented, which is a limitation of the solution. You can bundle different types of traffic within the same tunnel if you are within the capacity limits of the VPN headend and don't need to talk to other resources that are part of a different VPN Connect connection. This solution doesn't let you multiplex multiple tunnels to achieve higher bandwidths.

Create Multiple VCNs with Respective VPN Connect Connections

Another way to achieve more bandwidth is to create multiple VCNs within Oracle Cloud. The concepts are the same as the previous example. However, in this case, you might have different projects or business units that require separation, so you could create multiple VCNs within the same tenancy in different compartments within the same region. Oracle provides two headends for each VPN Connect connection. Each DRG has its own VPN Connect connection. You could have a single VPN CPE, but the number of VPN Connect connections that you can build is limited to the number of headends that Oracle can provide within the region and the capacity of your VPN CPE.

With this solution, any traffic from the on-premises network can connect to each of the VCNs through the respective VPN Connect connection. It can connect to 10.40.0.0/16 via VPN Connect 1 and to 10.50.0.0/16 via VPN Connect 2. Each DRG has its own route table, so you don't need to adjust any routing. You can use dynamic routing (BGP) or static routing. From the on-premises side, you are connecting to two different VCNs with nonoverlapping IP addresses, so you have two independent VPN Connect connections.

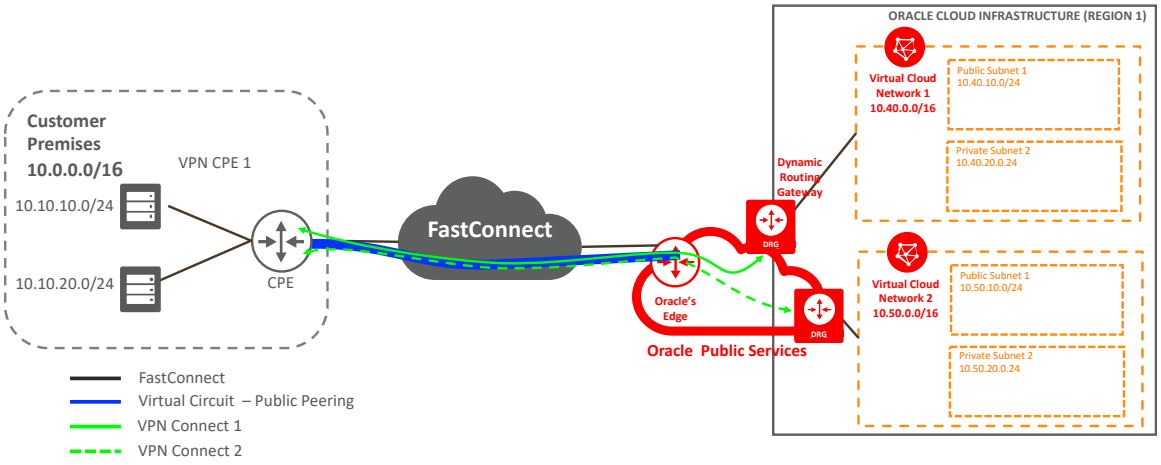

Figure 4. IPSec over FastConnect: Multiple VCNs

References

For more information about the services referenced in this document, see the following pages in the documentation:

- FastConnect
- VPN Connect
- VCN
- DRG

ORACLE

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

Integrated Cloud Applications & Platform Services

Encrypted FastConnect: Public Peering
August 2019
Author: Javier Ramirez