ORACLE

Encrypted FastConnect: Public Peering

Deprecated February 2024

August 2021, version 2.0

Public

Deprecation of This Solution

The solution provided in this paper is a legacy solution. We recommend that customers use OCI Site-to-Site VPN over FastConnect instead, as explained this blog post: Announcing OCI Site-to-Site VPN over FastConnect. We won't be updating or maintaining this paper in the future, and we don't recommend any new deployments using this solution.

Disclaimer

Revision History

The following revisions have been made to this document since its initial publication.

DATE	REVISION
February 2024	Deprecated the paper. The solution provided in this paper is a legacy solution. We recommend that customers use OCI Site-to-Site VPN over FastConnect instead, as explained this blog post: Announcing OCI Site-to-Site VPN over FastConnect. We won't be updating or maintaining this paper in the future, and we don't recommend any new deployments using this solution.
August 2021	Updated with Site-to-Site VPN enhancements
August 2019	Initial publication

Table of Contents

Overview

Note: The solution provided in this paper is a legacy solution. We recommend that customers use OCI Site-to-Site VPN over FastConnect instead, as explained this blog post: Announcing OCI Site-to-Site VPN over FastConnect. We won't be updating or maintaining this paper in the future, and we don't recommend any new deployments using this solution.

FastConnect and Site-to-Site VPN are two key ways for Oracle customers to connect to Oracle Cloud Infrastructure (OCI). FastConnect provides a private connection between the customer's on-premises network and OCI, with predictable performance. Site-to-Site VPN 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 security by using the FastConnect and Site-to-Site VPN services together. Site-to-Site VPN uses IP Security (IPSec) 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 OCI, and the Oracle Cloud 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 OCI 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 as a private gray cloud.

IPSec over FastConnect Public Peering

Following are the general steps to configure this solution:

1. Deploy FastConnect from your on-premises network to OCI and configure a public virtual circuit (the thick blue line in Figure 1) in the Oracle Cloud Console.
2. When the virtual circuit is configured, border gateway protocol (BGP) peering is established, and layer connectivity is in place, create a customer on-premises equipment (CPE) object and a Site-to-Site VPN in the Oracle Cloud Console.
3. Configure your on-premises VPN CPE and establish an IPSec tunnel to Oracle (the thin green line in Figure 1).

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

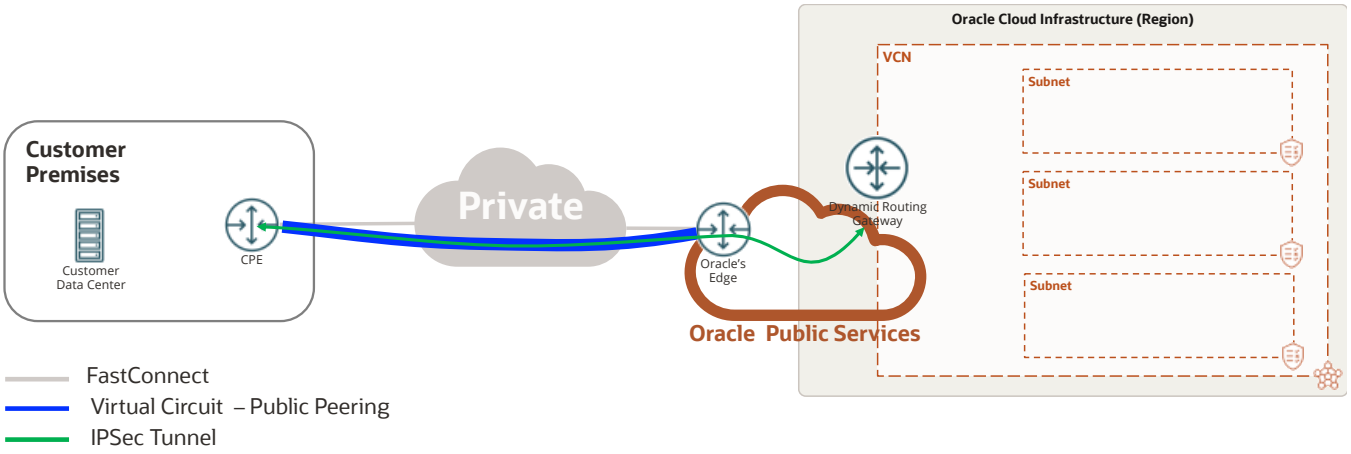

Figure 1: IPSec over FastConnect Public Peering

By default, Oracle provides two VPN gateways for redundancy when deploying Site-to-Site VPN. For simplicity, the diagrams in this document show only one of the tunnels. The public IP addresses for the Oracle gateways are advertised as part of the Oracle Services Network public subnets in each region when you create a public virtual circuit. Oracle advertises these IP addresses through the border gateway protocol (BGP), so they're already part of your route table when the public virtual circuit was established. The public IP address of your VPN CPE should be part of the prefix that you're advertising to Oracle through the BGP. The IPSec tunnel is established over the public virtual circuit, which does *not* go over the internet. Public peering is an alternative to the internet.

When deploying this solution, consider the following points:

- The IPSec tunnels end at the Oracle dynamic routing gateway (DRG).
- FastConnect public peering and the Site-to-Site VPN is configured using the Oracle Cloud Console.
- Encryption adds overhead and might not provide the full bandwidth of the subscribed FastConnect.
- By default, Oracle provides two VPN gateways, so you have two tunnels for each Site-to-Site VPN. These tunnels are both active and can be load balance using ECMP.
- Ensure that redundancy is deployed for FastConnect.
- Routing has two parts:
    - FastConnect: Over the FastConnect public virtual circuit, the public IP addresses of the Oracle gateways and your VPN CPE are exchanged through BGP.
    - Site-to-Site VPN: Configure Site-to-Site VPN using BGP or static routing. If you use static routing, you must point traffic from 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 Site-to-Site VPN connection and FastConnect, contact Oracle Support.

Implementing Site-to-Site VPN over FastConnect Public Peering

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

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

1. In OCI, create a VCN.
2. Create subnets within your VCN. These subnets host your compute instances.
3. Create a DRG.
4. Attach the DRG to your VCN.
5. Create FastConnect with a partner or a third party, or collocated with Oracle. For instructions, see the FastConnect documentation.
6. After FastConnect is successfully provisioned, create a public virtual circuit. Establish BGP peering between your CPE and Oracle’s edge. To complete this step, provide a public ASN and registered public IP addresses (the IP addresses for your VPN CPE). Oracle verifies that the IP addresses belong to you before advertising them. The IP addresses of Oracle’s VPN gateways 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 Site-to-Site VPN by creating a CPE object in the Oracle Cloud Console. For instructions, see Task 2g in Setting Up Site-to-Site VPN. This CPE object is the logical representation of your VPN CPE, which ends the IPSec tunnel on your on-premises network.
9. Create the IPSec connection, which is the connection between your VPN CPE and the DRG. You can select to use static routing or dynamic routing (BGP) between your VPN CPE and the DRG. For instructions, see Task 2h in Setting Up Site-to-Site VPN.
10. Configure your VPN CPE and set up the IPSec connection to the Oracle VPN gateways provided in the previous step. For instructions, see Task 3 and Task 4 in Setting Up Site-to-Site VPN.
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, including the various components that make up the solution: FastConnect, Site-to-Site VPN, DRG, VCN, customer premises, and routing.

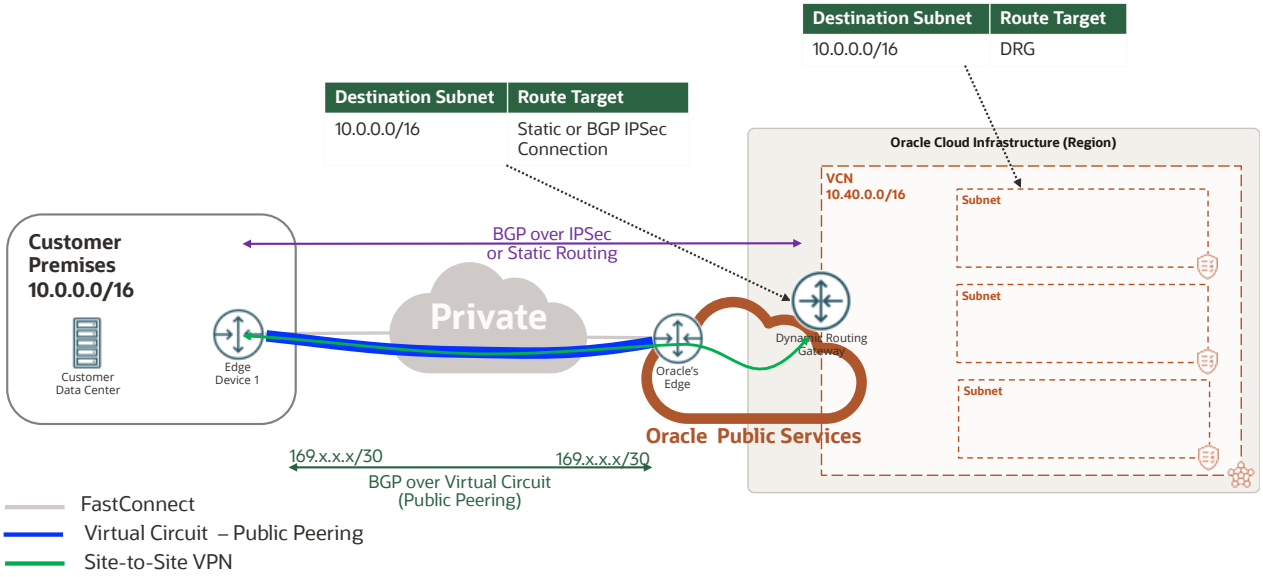

Figure 2: IPSec over FastConnect Public Peering—Routing

12. Initiate interesting traffic from your on-premises network to OCI to bring up the tunnel. Initiate 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 10-Gbps FastConnect connection, but the devices performing the encryption might not support this speed. To achieve more aggregate bandwidth between the on-premises network and OCI, you can perform the following tasks:

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

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

Create Multiple Site-to-Site VPN Connections to a Single VCN

Figure 3 shows a 1-Gbps FastConnect connection and a public virtual circuit, represented by the thick blue line. Oracle provides two VPN gateways for each Site-to-Site VPN connection that you create in the Console. To create multiple Site-to-Site VPN connections, provide multiple public IP addresses for your VPN CPE. Then, you can create more CPE objects on the Console to represent each VPN CPE. With two VPN gateways on-premises, each gateway creates a Site-to-Site VPN to Oracle, represented by the solid thin and dotted green lines.

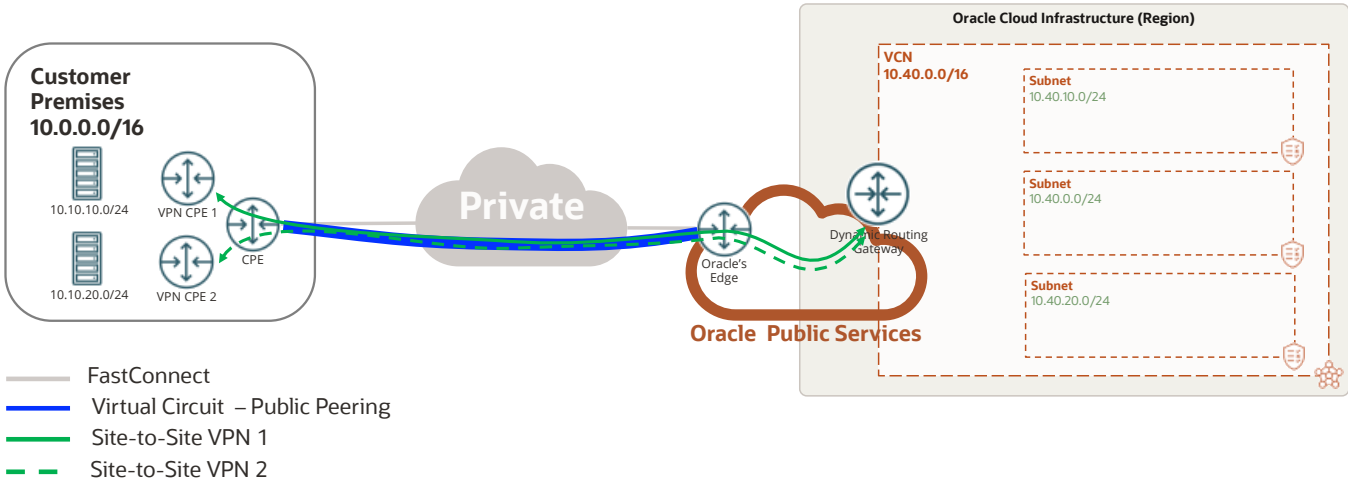

Figure 3: IPSec over FastConnect: Multiple Tunnels

Site-to-Site VPN 1 (the solid thin green line), built between an Oracle headend and VPN CPE 1, is configured to allow traffic between 10.10.10.0/24 and 10.40.10.0/24. Site-to-Site VPN 2 (the dotted green line), built between an Oracle headend and VPN CPE 2, allows traffic between 10.10.20.0/24 and 10.40.20.0/24. If each tunnel can support 250 Mbps, each Site-to-Site VPN has two tunnels and by creating two Site-to-Site VPNs (four tunnels total), you can achieve, in theory, 1 Gbps in a 1-Gbps FastConnect connection.

This routing has the following considerations:

- FastConnect

  Over the public virtual circuit, Oracle advertises all the public prefixes for the region, which belongs to the Oracle Services Network. The IP addresses of the gateways are part of these prefixes. You advertise the public IP addresses of VPN CPE 1 and 2.

- Site-to-Site VPN
  - From the Oracle side, Oracle advertises all the VCN subnets over the two tunnels through BGP. You filter the subnets received on VPN CPE 1 and 2 to accept subnets 1 (10.40.10.0/24) and 2 (10.40.20.0/24), instead of accepting all the VCN subnets. If you're using static routing, configure 10.10.10.0/24 through Site-to-Site VPN 1 and 10.10.20.0/24 through Site-to-Site VPN 2.
  - You advertise 10.10.10.0/24 from VPN CPE 1 and 10.10.20.0/24 from VPN CPE 2 through BGP. If you're using static routing, point 10.40.10.0/24 to VPN CPE 1 and 10.40.20.0/24 to VPN CPE 2.
  - Enable ECMP to use both tunnels per Site-to-Site VPN connection

This solution doesn't allow any-to-any communication. The design is segmented, which is a limitation of the solution. You can bundle different types of traffic within the same tunnel, if you're within the capacity limits of the VPN CPE and don't need to talk to other resources that are part of a different Site-to-Site VPN connection.

Create Multiple VCNs with Respective Site-to-Site VPN Connections

You can also achieve more bandwidth by creating multiple VCNs within OCI. 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 can create multiple VCNs within the same tenancy in different compartments within the same region. By default, Oracle provides two gateways for each Site-to-Site VPN connection. The number of Site-to-Site VPN connections that you can build is limited to the number of gateways 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 Site-to-Site VPN connection. It can connect to 10.40.0.0/16 through Site-to-Site VPN 1 and to 10.50.0.0/16 through Site-to-Site VPN 2. You can use dynamic routing (BGP) or static routing. From the on-premises side, you're connecting to two different VCNs with nonoverlapping IP addresses, so you have two independent Site-to-Site VPN connections. You can control routing from the DRG to advertise and receive routes from each of the Site-to-Site VPN connections.

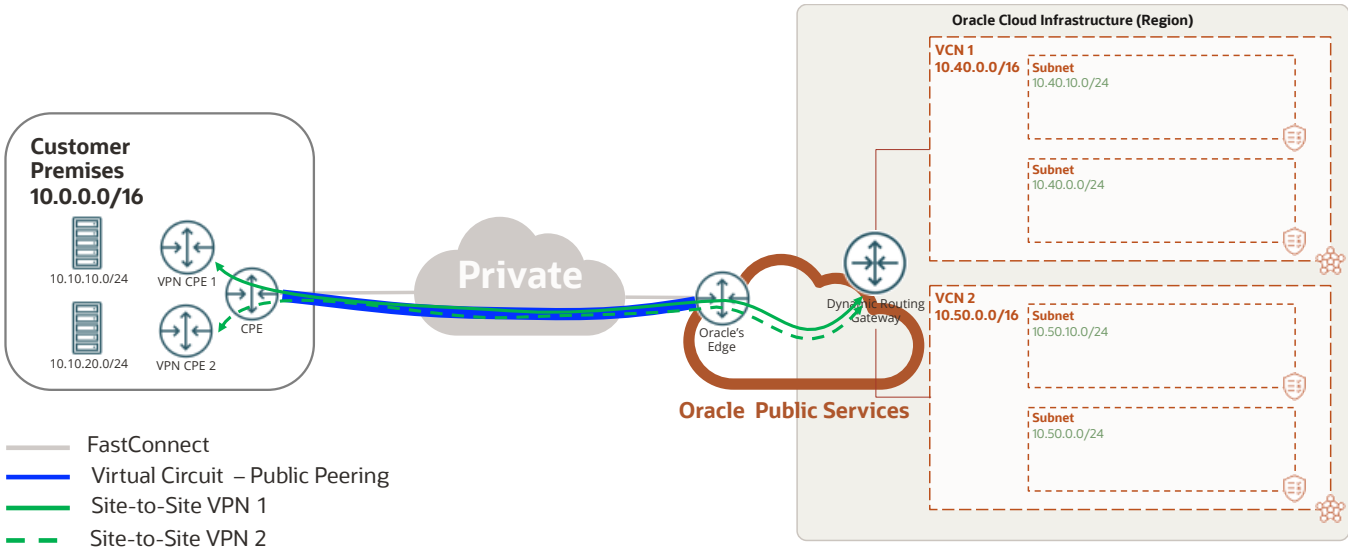

Figure 4: IPSec over FastConnect: Multiple VCNs

References

For more information about the Oracle Cloud Infrastructure services referenced in this document, see the following topics in the documentation:

- FastConnect
- Site-to-Site VPN
- VCNs and subnets
- Dynamic routing gateways (DRGs)

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle