



ORACLE

Connectivity Redundancy Guide

Oracle Cloud Infrastructure

March 2021, Version 2.0
Copyright © 2021, Oracle and/or its affiliates
Public

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. 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 in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

Revision History

Date	Revision
April 5, 2021	<ul style="list-style-type: none">Revised outdated information and diagramsUpdated template
January 24, 2020	Corrected statement about FastConnect
September 5, 2019	Updated Figure 11
May 30, 2019	Initial publication

Table of Contents

Overview	4
Design Considerations	4
Routing Between Oracle Cloud and Your On-Premises Network	4
Routing from Oracle Cloud to Your On-Premises Network	5
Routing from Your On-Premises Network to Oracle Cloud	6
Verify Redundancy Status	6
Oracle Cloud Redundancy Overview	6
IPSec VPN Redundancy Overview	7
IPSec VPN with a Single Customer-Premises Device	8
IPSec VPN with a Single Customer-Premises Device (Static Routing)	9
IPSec VPN with Redundant Customer-Premises Devices	10
FastConnect Overview	12
FastConnect (Partner Model)	13
FastConnect (Direct Model)	15
FastConnect with IPSec VPN Backup	17
References	18

Overview

Enterprise customers experience growth in their cloud deployments, and more critical applications are increasingly deployed to the cloud. With this growth, you need to ensure that your cloud infrastructure is available and connected to your on-premises network in a redundant way so that it can support planned maintenance outages and unplanned downtime.

The purpose of this document is to help you verify the redundancy of your current deployment and to describe options for upgrading a single, nonredundant connection to Oracle Cloud Infrastructure to a redundant connection. This document reviews use cases and options for connectivity through FastConnect and IPSec VPN over the internet. It assumes that you're familiar with routing protocols and concepts, IPSec VPN technology and configuration, and Oracle Cloud Infrastructure concepts and components.

Design Considerations

When you deploy resources to Oracle Cloud Infrastructure, you might start small, with a single connection to your on-premises network. This single connection could be through FastConnect or through IPSec VPN.

To plan for redundancy, consider all the components (hardware devices, facilities, circuits, and power) between your on-premises network and Oracle Cloud Infrastructure. Also consider diversity, to ensure that facilities are not shared between the paths.

The following table shows the components that you need to consider for a redundant solution.

Components	Comments
Internet service provider (ISP)	Not all ISPs are the same. Peering relationships from your ISP might impact how your traffic is routed over the internet.
Hardware devices	Enable services with redundant hardware devices and ensure that no single point of failure exists anywhere in the network path. How will you handle infrastructure maintenance (by Oracle or your own IT department)? Can you tolerate downtime? If so, how much?
Facilities diversity	Do you have redundant power feeds? Do you have diverse telecommunication entry points into your building? Is your equipment in different racks or data centers?
Oracle FastConnect point of presence (POP) diversity	Do you want to terminate both FastConnect circuits into the same POP or into different locations? POP diversity is available only in the Frankfurt, London, Ashburn, and Phoenix regions.
Circuit provider diversity	Are you planning to use diverse carriers? Are your WAN or internet circuits fully diverse, or do they share a POP? Having different carriers doesn't mean that the circuits are fully diverse.

Routing Between Oracle Cloud and Your On-Premises Network

FastConnect private peering and IPSec VPN provide the resources in your on-premises network with private access to an Oracle Cloud Infrastructure virtual cloud network (VCN). FastConnect and IPSec VPN connections can terminate on the same dynamic routing gateway (DRG) that is attached to your VCN, and they both support Border Gateway Protocol (BGP) for route exchange. IPSec VPNs also support static routing, but we recommend using BGP whenever possible.

When you use BGP, the DRG attached to your VCN advertises routes for each individual subnet in the VCN across each connection to your on-premises network with the same metrics. If your DRG has been enabled for transit routing, then routes for the peered VCNs are also advertised over each connection. Transit routing is an advanced routing scenario and outside of the scope for this document. For more information about transit routing, see the “References” section.

Routing from Oracle Cloud to Your On-Premises Network

When making a forwarding decision, routers prefer the more-specific route over the less-specific route. The DRG uses similar routing logic when deciding which connection to use for traffic destined for your on-premises network.

If the same on-premises route is advertised across multiple diverse connections to Oracle Cloud, then the shortest AS path is used as a tiebreaker when sending traffic back to the on-premises network. This routing decision is made regardless of the path used for the initiating traffic arriving in Oracle Cloud. For example, if traffic arrives to Oracle Cloud from an on-premises resource through your IPSec VPN tunnel, the return traffic might take an alternate path back through FastConnect. This behavior is called *asymmetric routing*, and Oracle doesn’t restrict asymmetric traffic.

It’s important to consider this behavior when designing for redundancy and specific failover scenarios. We recommend being deterministic with your routing and forcing sent and received traffic along a consistent symmetric path. You can achieve this behavior by modifying the BGP AS Path attribute with AS path prepending when advertising routes to Oracle Cloud. Oracle honors the AS path metric that is configured and uses the shortest AS path as a tiebreaker when deciding how to send traffic back to the on-premises network.

By default, Oracle implements AS path prepending to determine which connection to take if your on-premises device advertises the same route over multiple diverse connections (FastConnect and IPSec VPN).

Oracle Preference	Path	Details of How Oracle Prefers the Path	Resulting AS Path for the Route
1	FastConnect	Oracle prepends no ASNs to the routes that your on-premises device advertises, for a total AS path length of 1.	Your ASN
2	IPSec VPN with BGP routing	Oracle prepends a single private ASN on all the routes that your on-premises device advertises over VPN Connect with BGP, for a total AS path length of 2.	Private ASN, Your ASN
3	IPSec VPN with static routing	Oracle prepends three private ASNs on the static routes that you provide (Oracle advertises those routes to the DRG at the Oracle end of the IPSec VPN). This results in a total AS path length of 3.	Private ASN, Private ASN, Private ASN

If you have two connections of the same type (for example, two IPSec VPN tunnels with BGP or two FastConnect connections) and the same routes are advertised across both connections, then Oracle prefers the oldest established route as the tiebreaker for determining which path to use to send return traffic.

To simplify failover scenarios, we recommend using BGP when possible across all connections to Oracle Cloud and relying on BGP to make forwarding decisions. Avoid mixing connections that use both BGP and static routing.

Routing from Your On-Premises Network to Oracle Cloud

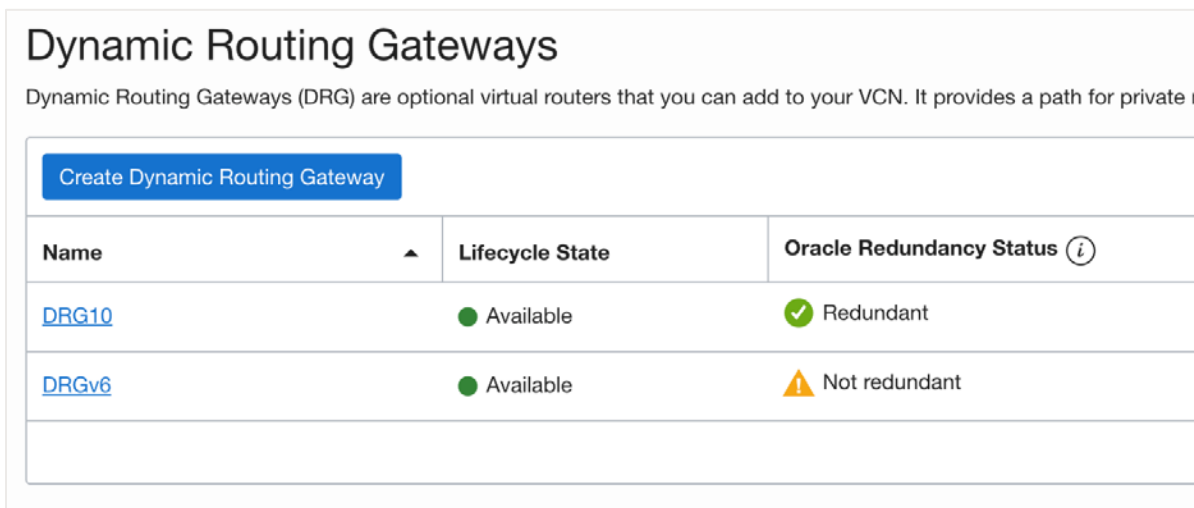
After you build redundancy, it's essential to configure your on-premises device to prefer a specific path when sending traffic destined for Oracle Cloud. You should do this regardless of whether your connections rely on private connectivity (FastConnect private peering and IPsec VPN) or public connectivity (FastConnect public peering and the internet).

Similar to the DRG routing logic, an on-premises router can make a forwarding decision based on longest prefix match, or more-specific routes preferred over less-specific, summarized routes. Alternatively, you can modify BGP metrics to prefer sending outbound traffic destined to OCI on a specific connection. You do this by modifying the local preference BGP attribute for specific routes. A higher local preference value on a route is preferred over a lower value for outbound traffic.

To simplify failover scenarios, we recommend using BGP when possible across all connections to Oracle Cloud and relying on BGP to make forwarding decisions. Avoid mixing connections that use both BGP and static routing.

Verify Redundancy Status

Through the Oracle Cloud Console, you can verify the redundancy status of your connections to a dynamic routing gateway (DRG). In the main menu, navigate to your DRG by selecting **Networking** and then **Dynamic Routing Gateway**. A status indicator for each DRG notifies you whether the attached connections are redundant or not.



The screenshot shows the 'Dynamic Routing Gateways' page in the Oracle Cloud Console. It includes a 'Create Dynamic Routing Gateway' button and a table with the following data:

Name	Lifecycle State	Oracle Redundancy Status ⓘ
DRG10	● Available	✓ Redundant
DRGv6	● Available	⚠ Not redundant

Figure 1: Verify Redundant Connections in the Console

Oracle Cloud Redundancy Overview

To help you build end-to-end redundancy, Oracle provides the following connectivity features:

- Multiple FastConnect providers per Oracle Cloud region
- At least one FastConnect point of presence (POP) location per region
- Two FastConnect POP locations in the following regions: Frankfurt, London, Ashburn, and Phoenix
- Two FastConnect routers in each FastConnect POP location
- Multiple physical connections between Oracle and each FastConnect provider for a given region
- Two diverse IPsec VPN tunnel endpoints per IPsec connection for a given region

Regardless of which connectivity option you choose, Oracle provides the necessary resources to build redundant and diverse connections between your on-premises network and Oracle Cloud. Likewise, it's essential that you also build redundancy on your side of the connection to avoid any single points of failure.

The rest of this document describes how to create a redundant connection to Oracle Cloud, starting from a single FastConnect or IPsec VPN connection. The following use cases are described:

- IPsec VPN with a single customer-premises device
- IPsec VPN with a single customer-premises device (static routing)
- IPsec VPN with redundant customer-premises devices
- FastConnect (partner model)
- FastConnect (direct model)
- FastConnect with IPsec VPN backup

The use cases provide best practice recommendations on how to set up primary and backup connections within the same region only.

IPsec VPN Redundancy Overview

Oracle Cloud Infrastructure IPsec VPN is the quickest way to privately connect your on-premises network to Oracle Cloud by using the internet as the transport and encryption to secure your traffic from the internet. When you create an IPsec VPN connection, Oracle provides the public IP addresses for two tunnel endpoints in the same region for redundancy. In this document, the Oracle VPN public IP addresses are represented as independent components to make it easier to understand the concepts and the endpoints for the tunnels. However, logically the connection is to the dynamic routing gateway (DRG) that was used when the IPsec connection was created.

A single IPsec VPN connection solution consists of a single edge device (customer-premises equipment, or CPE) in your on-premises network and two VPN endpoints in a single Oracle Cloud region. Your CPE can be located in your company's headquarters, a data center, a colocation facility, or even another cloud.

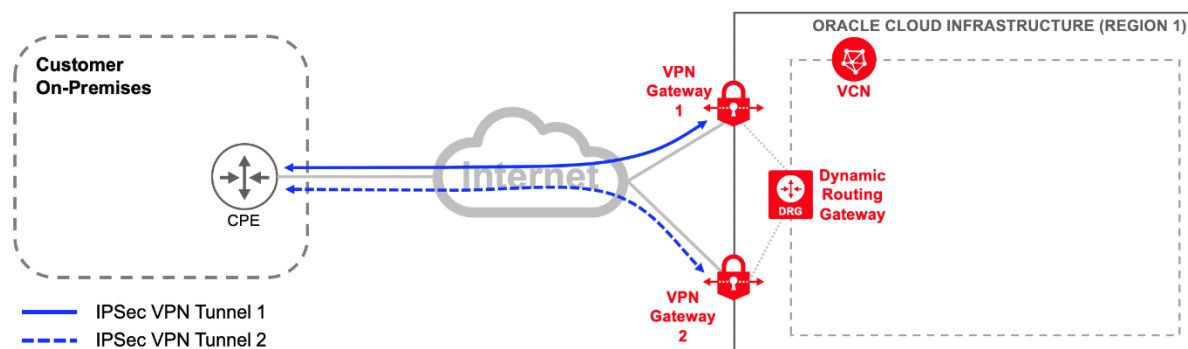


Figure 2: Single IPsec Connection Solution

IPSec VPN with a Single Customer-Premises Device

Figure 3 shows a high-level overview of the routing required to enable a consistent primary and backup path across both tunnels when using BGP and a single IPSec VPN connection with both tunnels.

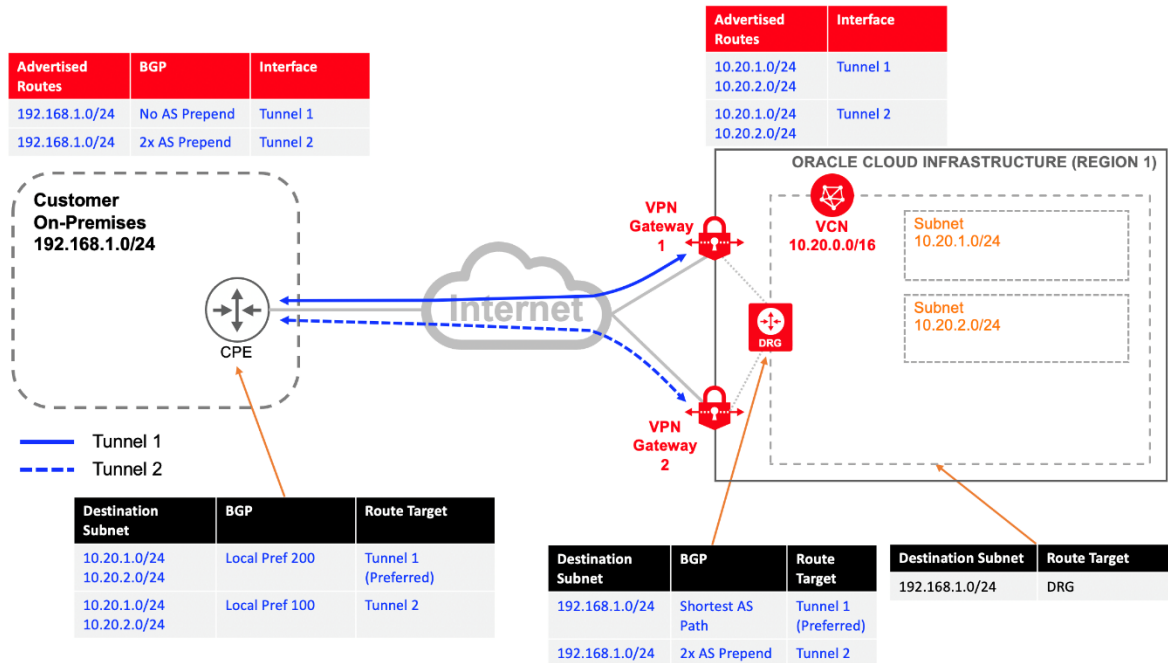


Figure 3: BGP Routing with a Single IPSec Connection and Single Customer-Premises Device

In the figure, BGP metrics are modified at the customer-premises device (CPE) to influence outgoing and incoming traffic to create symmetric routing by preferring Tunnel 1 as the primary and Tunnel 2 as the backup in both directions.

BGP local preference is used to influence outgoing traffic from on premises to Oracle Cloud. When BGP is used, Oracle advertises each subnet as a separate route. A higher local preference on the routes learned over the Tunnel 1 BGP session influences on-premises traffic destined for Oracle Cloud to be forwarded over Tunnel 1. Routes learned over Tunnel 2 use the default local preference value of 100 and are used to send traffic to Oracle Cloud only if Tunnel 1 is not available.

Oracle Cloud prefers to use the oldest continuously advertised route if the same route is advertised across multiple like connections. In this use case, because both connections are IPSec VPN, this is the tiebreaker used to decide how Oracle sends traffic back to on premises. This tiebreaker can potentially lead to asymmetric routing if your CPE sends traffic to Oracle Cloud on Tunnel 1 but Tunnel 2 is preferred on the return path because of an older established route. In this use case, AS path prepending is used to extend the AS path length on routes advertised to Oracle Cloud across the BGP session for Tunnel 2. In the BGP best-path selection algorithm, AS path length is used to prefer a certain route before the oldest-established-route tiebreaker. As a result, you can modify your AS path length with AS path prepending to influence how Oracle sends traffic back to on premises.

In this use case, the routes advertised over Tunnel 2 have had their AS path increased by prepending the on-premises ASN twice. The longer AS path length makes these routes less attractive. When Oracle sends traffic to the on-premises network, it compares the AS path on each tunnel's routes and prefers to send traffic using the route with the shorter AS path, thus disregarding the oldest-established-route tiebreaker. Tunnel 2 is used to send traffic on premises only if Tunnel 1 is not available.

In this use case, redundancy has been configured only on the Oracle side of the connection. The CPE located on premises is a single point of failure. For recommendations on how to overcome this single point of failure, see “IPSec VPN with Redundant Customer-Premises Devices.”

IPSec VPN with a Single Customer-Premises Device (Static Routing)

Oracle Cloud IPSec VPN supports BGP or static routing. We recommend using BGP routing when possible. If using BGP is not an option, you can use static routing to achieve redundancy.

Note: To create redundancy with IPSec VPN and static routing, you need to create two separate IPSec VPN connections between the same DRG and CPE object. Use at least one tunnel in each IPSec VPN connection to ensure redundancy and symmetric routing.

To influence routing, we recommend using more-specific routes over the primary path and less-specific routes over the backup path. With this approach, traffic is symmetric in both directions. If the primary path fails, a less-specific route is available through the backup path. When the primary path is restored, traffic falls back to the primary path because it uses a more specific route.

Static routes for IPSec VPN are configured at the IPSec connection level. All tunnels within an IPSec connection use the same static routes when forwarding traffic to on premises. If both tunnels are used within a single IPSec connection, Oracle might choose to send traffic back on a different tunnel within the same IPSec connection (asymmetric routing).

To force traffic to a symmetric path, create a second IPSec connection between the same CPE and DRG using a less-specific static route, and bring up at least one tunnel in each IPSec connection. OCI prefers to send traffic back on the tunnel for the first IPSec connection with the more-specific static route, using the tunnel on the second IPSec connection only if the first is not available.

Figure 4 details the routing for this use case. The CPE has two specific static routes configured, one for each subnet, and a less-specific route on the second tunnel that represents the whole VCN CIDR.

On the return path, Oracle Cloud sends traffic on the tunnel with the more-specific on-premises route and uses the second tunnel with the default route only if the tunnel with the more-specific route is not available.

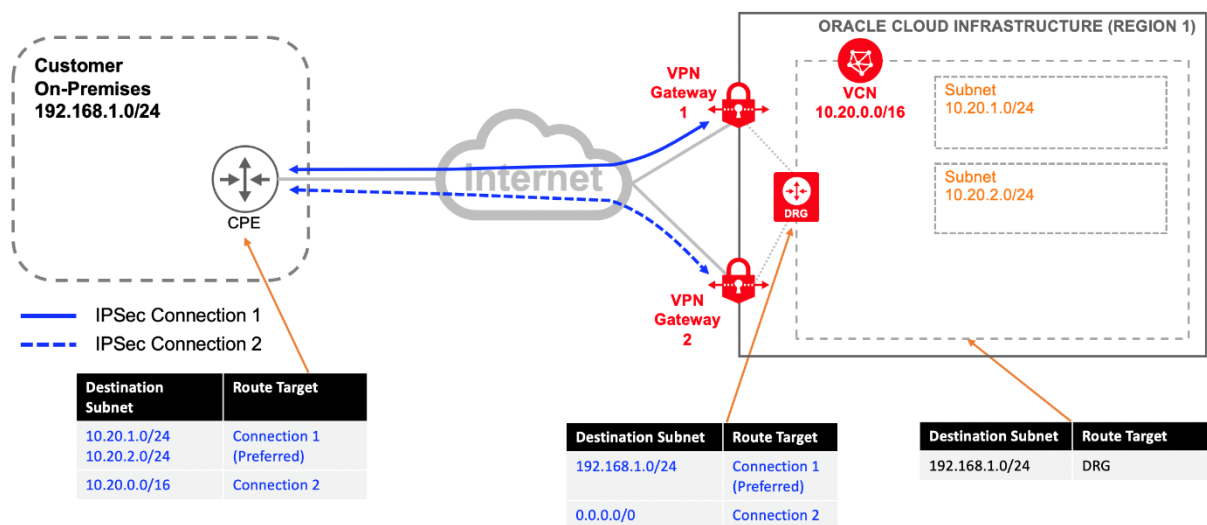


Figure 4: Static Routing with a Single Customer-Premises Device

IPSec VPN with Redundant Customer-Premises Devices

The IPSec VPN solution depicted in the previous sections has a single point of failure: the customer-premises device, or CPE. To overcome this single point of failure, deploy a second CPE in the same location as the primary one or in a different data center. If the second CPE is in the same location as the primary one, verify that they connect to different internet providers, LAN switches, and power units. Ensure that your CPEs don't share a common point of failure.

For simplicity, Figure 5 shows two CPEs deployed at the same location. As stated earlier, when you create an IPSec VPN connection in Oracle Cloud, two IPSec VPN termination points are provided per connection on the Oracle side for redundancy. Each Oracle IPSec tunnel endpoint within an IPSec VPN connection is terminated on a separate logical device and has diverse connections to the internet.

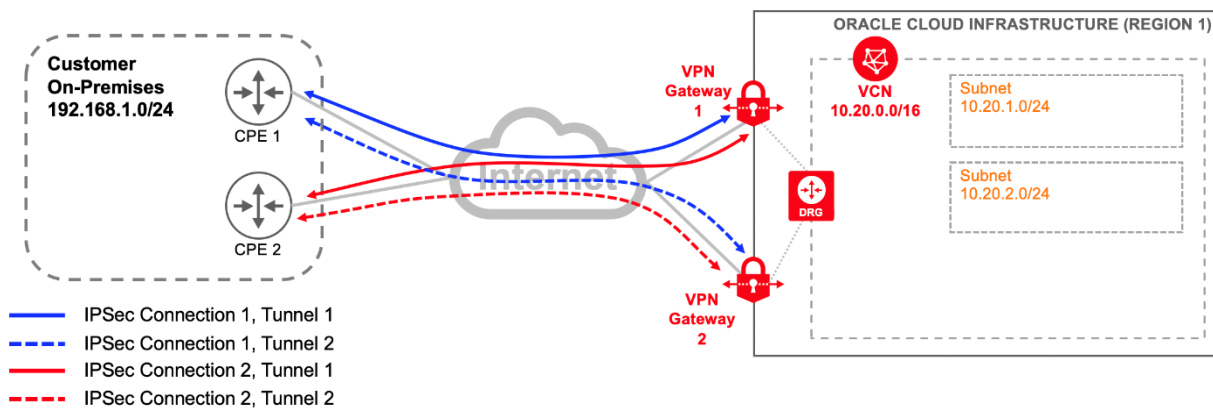


Figure 5: IPSec VPN with Two Customer-Premises Devices and Four Tunnels

As shown in the figure, each CPE has two tunnels. Four tunnels provide redundancy, but they can complicate your routing deployment. Now you must configure your routing over four tunnels and prioritize routes for each tunnel. In the diagram, traffic fails back from the CPE 1 to the CPE 2 only if CPE 1 fails or its internet circuit fails.

Note: Oracle has several diverse, redundant tunnel endpoints per region. Every endpoint for Oracle automatically uses multiple carriers. For simplicity, the diagrams in this section show only two of them.

As long as redundancy is maintained, you can choose not to establish the second tunnel per IPSec connection. You can simplify the solution by reducing the number of tunnels from four to two. Oracle still provides connectivity information and a usable tunnel endpoint for a second tunnel per IPSec connection if you want to configure one in the future. This design still provides redundancy and diversity because each CPE builds a tunnel to a different Oracle VPN endpoint, as shown in the Figure 6. This simplified solution provides an active/passive architecture that you can control more effectively through routing.

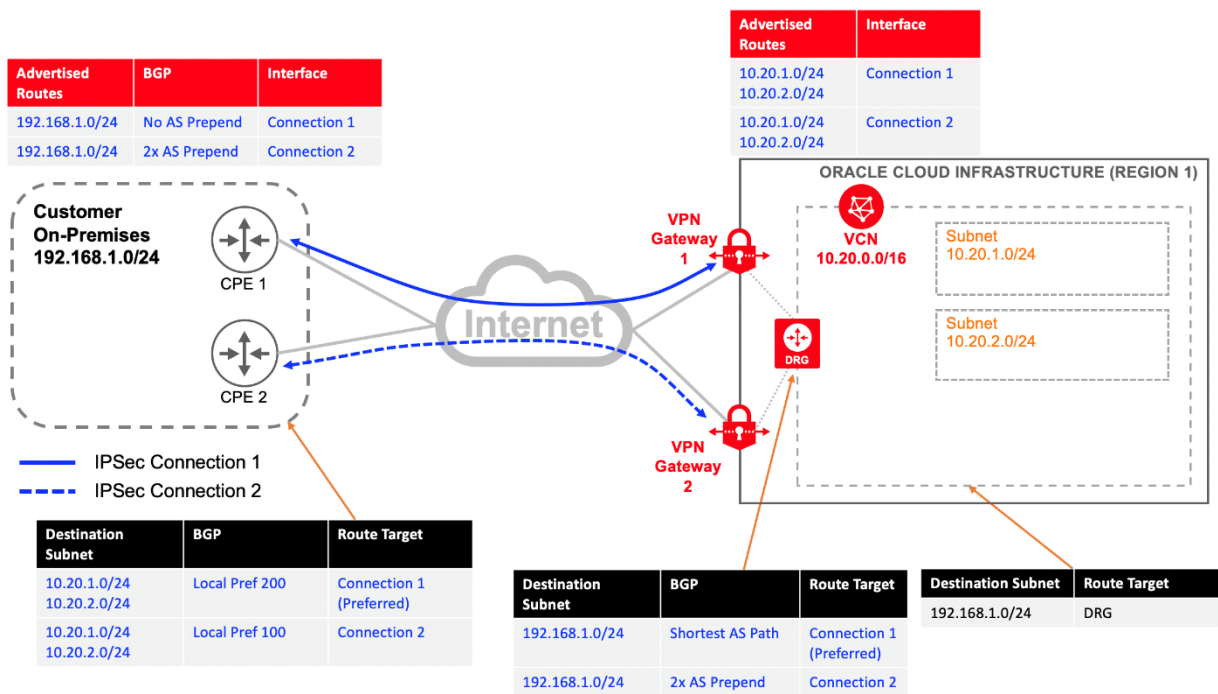


Figure 6: IPsec VPN with BGP Routing, Two Customer-Premises Devices, and Two Tunnels

With fully diverse paths, the next step is to ensure that routing is configured correctly to define the primary and backup paths. In the figure, each line between a CPE and a VPN Gateway represents a different IPsec connection with a single configured tunnel. BGP metrics are modified at the CPE to influence outgoing and incoming traffic to create symmetric routing by preferring the relevant tunnel as primary. In this example, the solid line connection is configured as the primary path, and the dashed line connection is the backup.

BGP local preference is used to influence outgoing traffic from on-premises to Oracle Cloud. When BGP is used, Oracle advertises each subnet as a separate route. A higher local preference on the routes learned over IPsec Connection 1 tunnel's BGP session influences on-premises traffic destined for Oracle Cloud to be forwarded over that path. Routes learned over IPsec Connection 2 use the default local preference value of 100 and are used for sending traffic to Oracle Cloud only if IPsec Connection 1 is not available.

Oracle Cloud prefers to use the oldest continuously advertised route if the same route is advertised across multiple like connections. In this use case, because both connections are IPsec VPN, this is the tiebreaker used to decide how Oracle sends traffic back to on premises. This tiebreaker can potentially lead to asymmetric routing if your CPE sends traffic to Oracle Cloud on IPsec Connection 1's tunnel, but the IPsec Connection 2's tunnel is preferred on the return path because of an older established route. In this use case, AS path prepending is used to extend the AS path length on routes advertised to Oracle Cloud across the BGP session for IPsec Connection 2. In the BGP best-path selection algorithm, AS path length is used to prefer a certain route before the oldest-established-route tiebreaker. As a result, you can modify your AS path length with AS path prepending to influence how Oracle sends traffic back to on premises.

In this use case, the routes advertised over IPsec Connection 2 to Oracle Cloud have had their AS path increased by prepending the on-premises ASN twice. The longer AS path length makes these routes less attractive. When Oracle sends traffic to the on-premises network, it compares the AS path on each connection's routes and prefers to send traffic using the route with the shorter AS path, thus disregarding the oldest-established-route tiebreaker. IPsec Connection 2's tunnel is used to send traffic on premises only if the tunnel for IPsec Connection 1 is not available.

In this use case, redundancy has now been established on both sides of the connection. In addition to the end-to-end redundancy that was built, you can optionally use a different ISP for one of the CPEs and tunnels for provider diversity. In a multiple-provider scenario, you can use the same routing design between on premises and Oracle Cloud as long as the encrypted traffic for each tunnel is routed over a different provider.

FastConnect Overview

Oracle Cloud Infrastructure FastConnect is a dedicated, private, and secure network connectivity option for connecting your on-premises locations to Oracle Cloud. FastConnect is an alternative to internet-based connectivity and allows for more predictable performance and faster bandwidth options for critical enterprise workloads.

Oracle offers the following types of connections through FastConnect.

FastConnect Connectivity Model	Description
Oracle Partner	This option is suitable if you plan to use or are already using network connectivity services from any FastConnect partner. Depending on your partner, you might have to order redundant cloud connectivity services from them. For a full list of partners, see FastConnect Provider by Region .
Direct (colocation)	This option is suitable if you already have presence at a FastConnect POP location or want to establish a colocation presence at one. You can order multiple such connections into a data center for redundancy.
Direct (third-party provider)	This option is suitable if you have existing relationships with certain network carriers, or if your on-premises or remote data center location is not serviced by any of Oracle's FastConnect partners.

FastConnect redundancy best practices vary depending on the connectivity model used. Regardless of the FastConnect connectivity model, however, Oracle provides the following tools to ensure end-to-end redundancy:

- Multiple Oracle partners in each region
- At least one FastConnect POP location per region (certain regions contain two)
- Two routers in each POP location
- Multiple, redundant physical connections between each Oracle partner and Oracle in a given region

When provisioning a FastConnect connection, it's critical to ensure that each connection terminates on a different FastConnect router in Oracle Cloud to avoid any single points of failure. If you're using FastConnect in a region that has two FastConnect POP locations, the redundant FastConnect can optionally be terminated at a router in the second FastConnect location. Pay special attention to the physical connectivity to ensure that it's redundant and diverse. As you work with partners and carriers, ensure that they understand the physical connectivity of your existing connection so they can provide the diversity that you require.

For the FastConnect direct model, a router proximity option is available when you configure the cross-connect to direct Oracle to terminate the connection on a different hardware device.

In the following figure, FastConnect Cross-connect 1 (solid blue line) was provisioned first and terminates at Edge Device 1 for FastConnect Location 1. When you deploy your second FastConnect connection, we recommend terminating it at an edge device in FastConnect Location 2, as depicted by the red dotted line. If an Oracle partner, third-party provider, or you are colocated only at Location 1, you don't have location diversity. However, you can ensure that you have hardware diversity by provisioning the second FastConnect connection to terminate at Edge Device 2 in Location 1, as shown by the green dotted line.

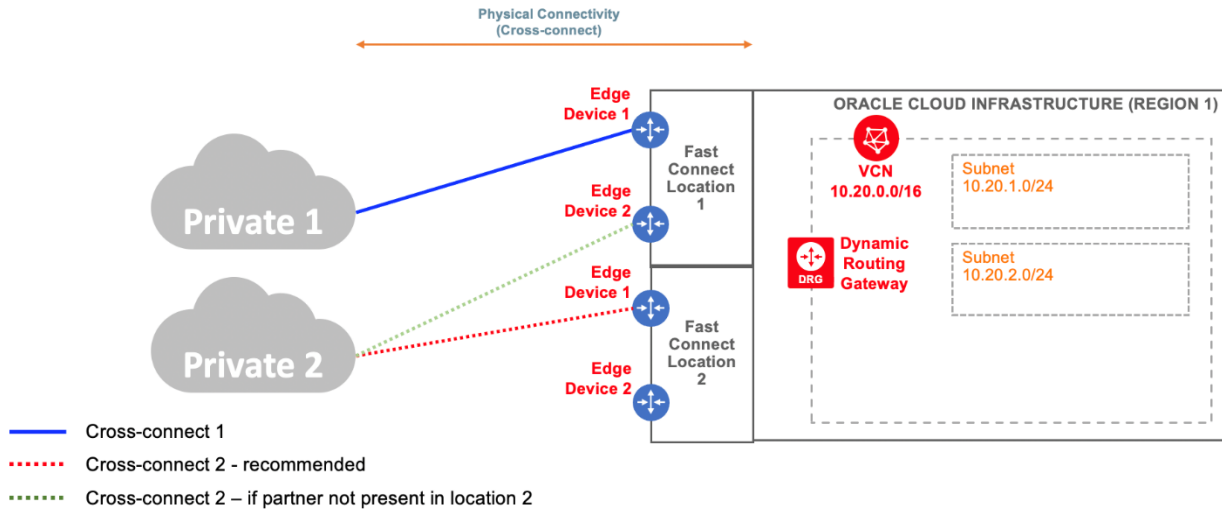


Figure 7: FastConnect Physical Connectivity

FastConnect (Partner Model)

With the FastConnect partner model, Oracle is responsible for building redundant physical connections between Oracle and the partner, and for the redundancy of FastConnect routers in each FastConnect POP location. Conversely, you should build physical redundancy between your on-premises network and the Oracle partner.

Redundancy best practices for the FastConnect partner model vary slightly based on the partner. This primarily depends on whether your FastConnect BGP sessions are between your on-premises device and Oracle (Layer 2 connection) or are between your on-premises device and the Oracle partner (Layer 3 connection). Depending on the required level of redundancy, consider using multiple Oracle partners but consider the differences between each partner.

The next two sections provide redundancy recommendations depending on the type of FastConnect partner connection used.

BGP Session Is to Oracle

Each Oracle partner has, at a minimum, two separate physical connections to Oracle Cloud. When provisioning your FastConnect virtual circuits, ensure that there is a virtual circuit per physical connection and redundant physical connections between the on-premises network and the Oracle partner.

If you're in an Oracle Cloud region with multiple FastConnect POP locations, your redundant virtual circuit may optionally terminate at a different POP for location diversity.

With fully diverse paths, the next step is to ensure that routing is configured correctly to define the primary and backup virtual circuit. In the following figure, each line between the on-premises device (CPE) and each Oracle Cloud edge device represents a FastConnect virtual circuit. BGP metrics are modified at the CPE to influence outgoing and incoming traffic to create symmetric routing by preferring the relevant virtual circuit as primary. In this use case, Virtual Circuit 1 is the primary path and Virtual Circuit 2 is the backup for both incoming and outgoing traffic.

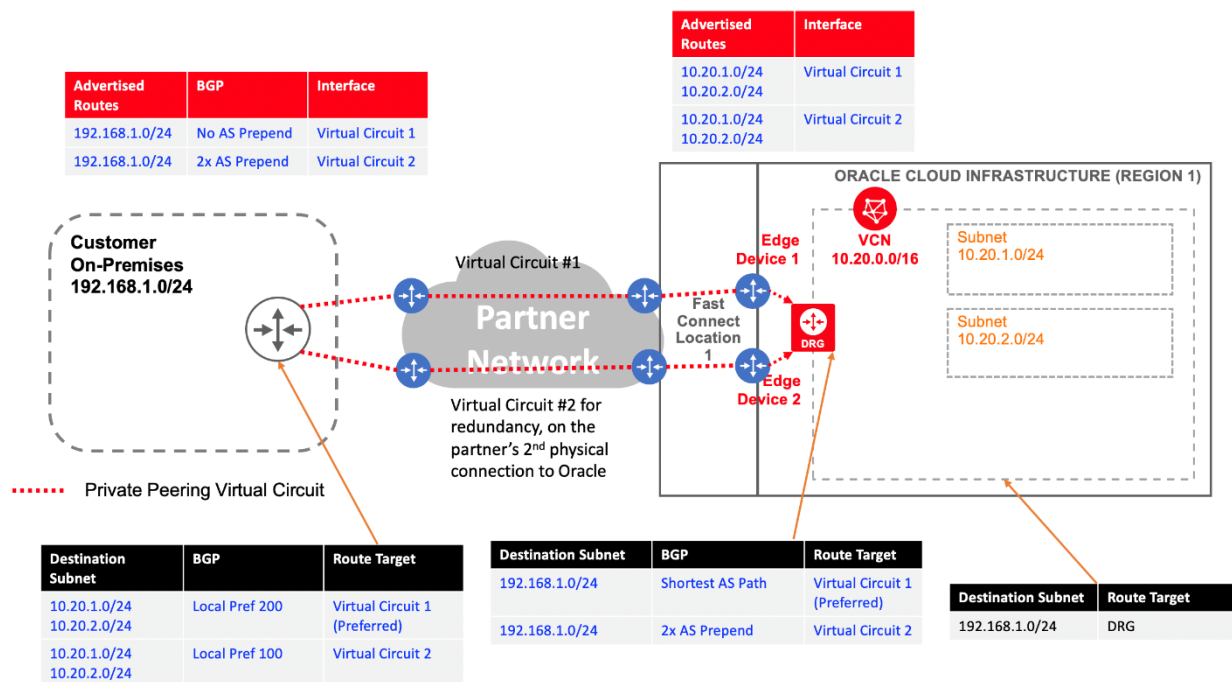


Figure 8: FastConnect Partner Model—BGP Session Is to Oracle

BGP local preference is used to influence outgoing traffic from on premises to Oracle Cloud. When BGP is used, Oracle advertises each subnet as a separate route. A higher local preference on the routes learned over the BGP session for Virtual Circuit 1 influences on-premises traffic destined for Oracle Cloud to be forwarded over that path. Routes learned over Virtual Circuit 2 use the default local preference value of 100 and are used for sending traffic to Oracle Cloud only if Virtual Circuit 1 is not available.

Oracle Cloud prefers to use the oldest continuously advertised route if the same route is advertised across multiple like connections. In this use case, because both connections are FastConnect, this is the tiebreaker used to decide how Oracle sends traffic back to on premises. This tiebreaker can potentially lead to asymmetric routing if your CPE sends traffic to Oracle Cloud on Virtual Circuit 1 but Virtual Circuit 2 is preferred on the return path because of an older established route. In this use case, AS path prepending is used to extend the AS path length on routes advertised to Oracle Cloud across the BGP session for Virtual Circuit 2. In the BGP best-path selection algorithm, AS path length is used to prefer a certain route before the oldest-established-route tiebreaker, with a shorter AS path being preferred. As a result, you can modify your AS path length with AS path prepending to influence how Oracle sends traffic back to on premises.

In this use case, the routes advertised over Virtual Circuit 2 to Oracle Cloud have had their AS path length increased by prepending the on-premises BGP ASN twice. The longer AS path length makes these routes less attractive when BGP decides the best path to use. When Oracle Cloud sends traffic to the on-premises network, the DRG prefers to use the route learned with the shorter AS path, thus disregarding the oldest-established-route tiebreaker. Virtual Circuit 2 is used only to send traffic on premises if Virtual Circuit 1 is not available.

You can achieve a similar routing architecture by advertising more-specific and less-specific routes over BGP representing your on-premises network. Advertise the more-specific on-premises routes to Oracle over the preferred primary virtual circuit, and a less-specific, summary route for the backup virtual circuit. Oracle prefers to use the virtual circuit with the more-specific routes to send traffic destined for on premises. The backup virtual circuit with the less-specific route is used only if the primary is not available. For an example of a routing architecture that uses similar routing logic, see “IPSec VPN with a Single Customer-Premises Device (Static Routing).”

Note: We recommend modifying BGP metrics when possible to influence incoming and outgoing routing across redundant connections, instead of relying on a longest-prefix match.

BGP Session Is to an Oracle Partner

When the FastConnect BGP session is between the on-premises device (CPE) and an Oracle partner, redundant physical connections exist between the partner and Oracle, and redundant BGP sessions exist between the partner edge and the Oracle edge.

In this use case, only a single virtual circuit is required. Each virtual circuit uses two separate BGP sessions between the partner edge and the Oracle edge, each on a separate physical connection. As a result, each virtual circuit is redundant and diverse.

To maintain end-to-end redundancy, it's essential to also separately build physical redundancy between the Oracle partner and the on-premises network.

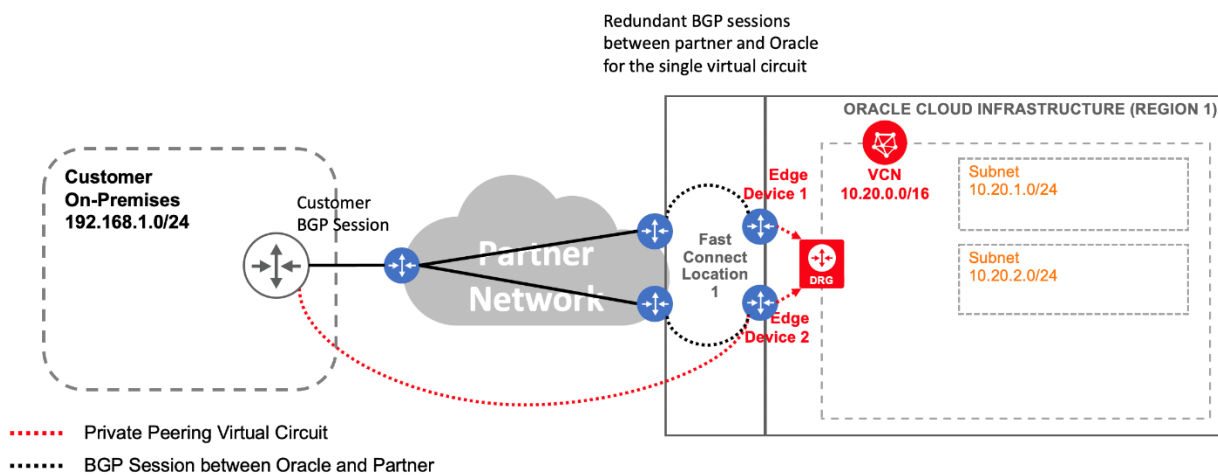


Figure 9: FastConnect Partner Model—BGP Session Is to an Oracle Partner

When your BGP session is between the Oracle partner and your CPE, a single virtual circuit is automatically designed to be redundant and diverse. As a result, you don't need to provision more virtual circuits for active/backup redundancy. In this use case, Oracle advertises each subnet as a separate route through BGP. Ensure that you're advertising your relevant on-premises network to Oracle through the FastConnect BGP session.

FastConnect (Direct Model)

The FastConnect direct model includes colocation and third-party provider connections. Both of these connection types have the same strategy for building redundancy.

In the FastConnect direct model, Oracle is responsible for redundancy on the Oracle Cloud side by providing redundant physical FastConnect routers at each FastConnect POP location. Separately, you need to ensure redundancy between your on-premises network and Oracle by building redundant physical connections. When creating these redundant physical connections, ensure that each one terminates at a different FastConnect router or, optionally, separate FastConnect POP locations if you're in a region with multiple locations.

After you establish the redundant physical connections, configure two separate virtual circuits, one for each physical connection. Each virtual circuit will have its own BGP session between your CPE and the Oracle edge devices.

With fully diverse paths, the next step is to ensure that routing is configured correctly to define the primary and backup virtual circuit. In the following figure, each line between the CPE and each Oracle edge device represents a physical cross-connect with a single virtual circuit. BGP metrics are modified at the CPE to influence outgoing and incoming traffic to create symmetric routing by preferring the relevant virtual circuit as primary. In this example, Virtual Circuit 1 is the primary path and Virtual Circuit 2 is the backup for both incoming and outgoing traffic.

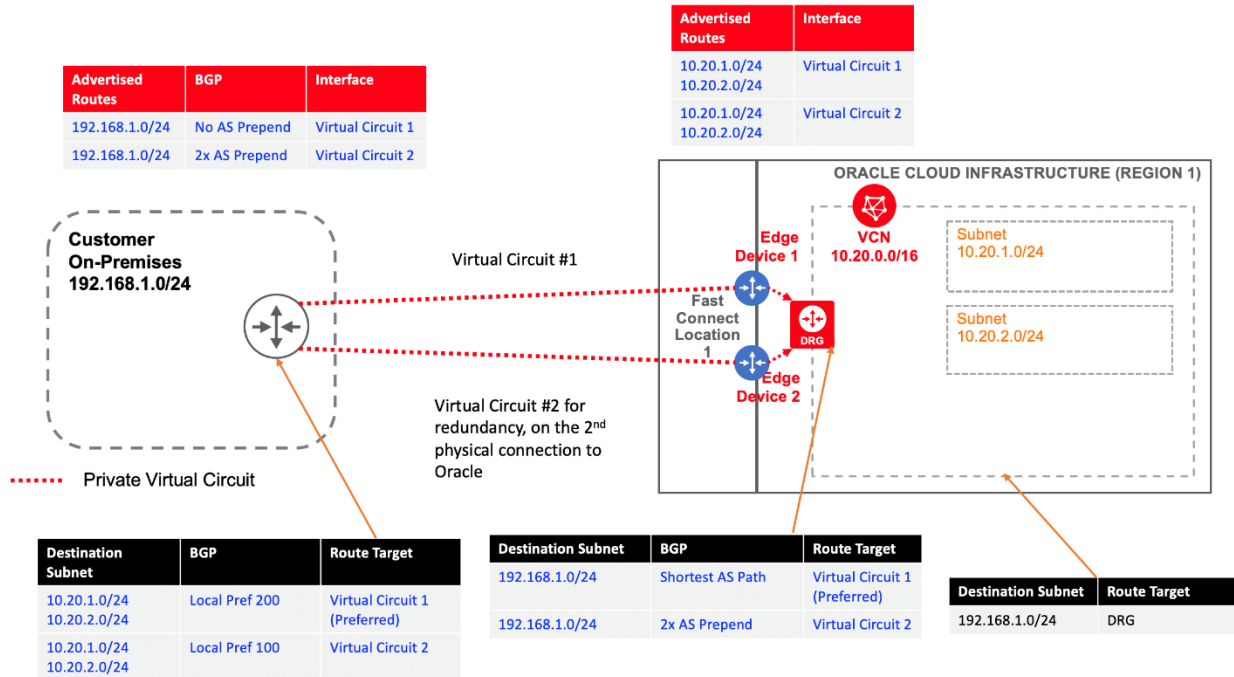


Figure 10: BGP Routing with FastConnect Direct Model

BGP local preference is used to influence outgoing traffic from on-premises to Oracle Cloud. When BGP is used, Oracle advertises each subnet as a separate route. A higher local preference on the routes learned over the BGP session for Virtual Circuit 1 influences on-premises traffic destined for Oracle Cloud to be forwarded over that path. Routes learned over Virtual Circuit 2 use the default local preference value of 100 and are used for sending traffic to Oracle Cloud only if Virtual Circuit 1 is not available.

Oracle Cloud prefers to use the oldest continuously advertised route if the same route is advertised across multiple like connections. In this use case, because both connections are FastConnect, this is the tiebreaker used to decide how Oracle sends traffic back to on premises. This tiebreaker can potentially lead to asymmetric routing if your CPE sends traffic to Oracle Cloud on Virtual Circuit 1 but Virtual Circuit 2 is preferred on the return path because of an older established route. In this use case, AS path prepending is used to extend the AS path length on routes advertised to Oracle Cloud across the BGP session for Virtual Circuit 2. In the BGP best-path selection algorithm, AS path length is used to prefer a certain route before the oldest-established-route tiebreaker, with a shorter AS path being preferred. As a result, you can modify your AS path length with AS path prepending to influence how Oracle sends traffic back to on premises.

In this use case, the routes advertised over Virtual Circuit 2 to Oracle Cloud have had their AS path length increased by prepending the on-premises BGP ASN twice. The longer AS path length makes these routes less attractive when BGP decides the best path to use. When traffic is sent from Oracle Cloud to the on-premises network, the DRG prefers to use the route learned with the shorter AS path, thus disregarding the oldest-established-route tiebreaker. Virtual Circuit 2 is used to send traffic on premises only if Virtual Circuit 1 is not available.

FastConnect with IPsec VPN Backup

You can use IPsec VPN as a backup connection for FastConnect. If you do, ensure that the VPN tunnels are configured to use BGP routing and a route-based VPN configuration. Use at least one tunnel in the IPsec connection, but you can use two for extra redundancy.

Don't terminate both FastConnect and IPsec VPN connections on the same on-premises device (CPE). Doing so would create a single point of failure. Instead, deploy each connection on a separate CPE.

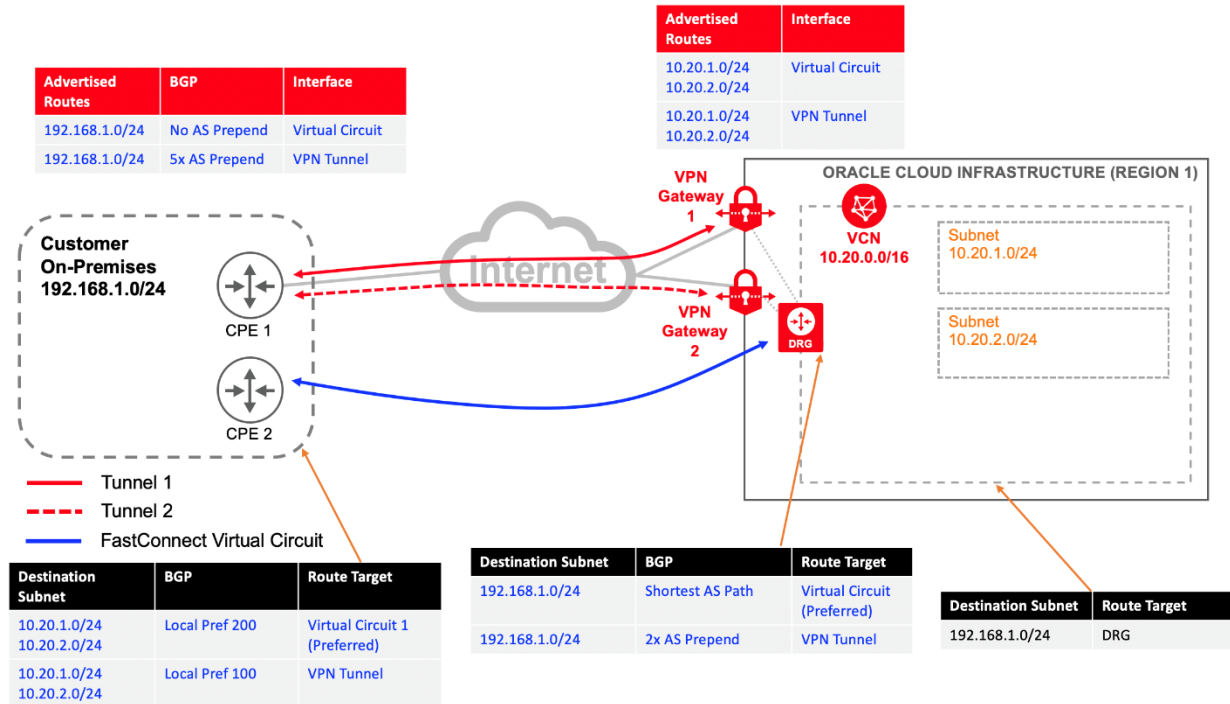


Figure 11: BGP Routing with FastConnect and IPsec VPN Backup

For routing, follow the same approach as the previous solutions, in which you use BGP local preference to prefer FastConnect for traffic destined to Oracle Cloud, with the IPsec VPN tunnel being the backup connection.

If the same route is advertised across multiple different connection types, for example FastConnect and IPsec VPN, Oracle Cloud uses the shortest AS path as a tiebreaker. In this use case, for routes learned over FastConnect, Oracle doesn't prepend more ASNs, so these routes have a default AS path length of 1. For the routes learned over the BGP session for IPsec VPN, Oracle by default prepends a single ASN to each route learned, for an AS path of length of 2. For details about which routes Oracle prefers, see "Routing from Oracle Cloud to Your On-Premises Network."

Note: It's important to not rely on this default behavior and expect traffic to always use FastConnect as primary and the IPsec VPN as backup when advertising routes with the same AS path length across both connection types. Treat this default behavior as a fallback policy to ensure that FastConnect is always used as the primary. Use AS path prepending on the routes advertised to Oracle Cloud over IPsec VPN to make them less attractive. In the preceding figure, VPN routes are prepended 5 times, but this can be any value as long as the AS path length is longer for IPsec VPN.

References

- [IPSec VPN Overview](#)
- [FastConnect Overview](#)
- [Networking Overview](#)
- [Transit Routing](#)

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

Copyright © 2021, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0120
