ORACLE

Site-to-Site VPN (IPSec) Best Practices

August 2021, version 2.0

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

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

DATE	REVISION
August 2021	• Updated with new dynamic routing gateway (DRG) and Site-to-Site VPN enhancements • Updated the document title to reflect the updated content
February 2020	Removed statement that NAT-T is not supported
May 2019	Initial publication

Table of Contents

Overview

Many vendors provide physical and virtual appliances that can build IP Security (IPSec) tunnels. Although these products support standard IPSec tunnels, some incompatibility exists among the different vendors. This document provides best practices for how to connect your on-premises network to Oracle Cloud Infrastructure (OCI) with the most success by using a virtual private network (VPN) over the internet. It assumes that you're familiar with routing protocols and concepts, VPN (IPSec) technology and configuration, and OCI concepts and components. This document also includes simple, redundant, and complex use cases to help you deploy various VPN solutions. It doesn't provide step-by-step instructions, but it does provide references to OCI documentation. This document is vendor independent.

Design Principles

When designing a VPN solution, consider the following principles:

- **Hardware capabilities:** Depending on the required workload, your infrastructure needs enough capacity to support the required bandwidth from your on-premises network to OCI. All the devices (VPN gateways, routers, firewalls, and switches) and internet circuits in the infrastructure must be able to support the required capacity. If one of the components in the path doesn't have the capacity, the whole connection is affected. The VPN gateway needs enough resources to encrypt the traffic at the required capacity level.
- **Availability:** Because the workloads that you deploy in the cloud are mission critical, you need to build redundancy into the solution to avoid downtime. You need hardware diversity and site diversity, if possible. When you build a VPN solution with OCI, Oracle by default provides two gateways to terminate the tunnels. The two tunnels are always active, so allow traffic from both tunnels into your network.
- **Performance:** A VPN solution uses the public internet to connect your on-premises network to OCI. The throughput of the connection depends on many things, such as the quality of the internet, latency between your VPN gateway (edge device) and the Oracle VPN gateways, the bandwidth of the internet circuit, and the capacity of the VPN devices. If you need a more reliable connection, Oracle offers FastConnect, which provides a robust and reliable connection over a private network.
- **Routing:** Routing dictates how traffic is directed to the tunnels that you build. The tunnels could be in an UP state on both sides, but if routing isn't set properly, traffic doesn't flow through the tunnel. Oracle's Site-to-Site VPN supports static routing and dynamic routing with border gateway protocol (BGP). Ensure that routes are configured to withdraw from the route table when a tunnel is down for proper failover and that they have the correct priority for failback.
- **VPN configuration:** For two endpoints to establish an IPSec tunnel and for traffic to flow through the tunnel successfully, the settings on both ends must match completely. Otherwise, the performance of the connection is affected. The next section provides recommended settings.
- **Security:** Security also plays an important role in the overall strategy. Access lists enable you to allow specific traffic to use the connection. Although routing and the encryption domain allow traffic in a more general way, access lists let you filter traffic more granularly at the port level. This document provides little guidance about access lists because their use depends on the type of traffic that you want to allow over the connection.
- **Cost:** The infrastructure that you need to support your workloads has a cost associated with it. A VPN solution might satisfy your requirements during your initial cloud deployment. As you grow, however, you might need to upgrade your environment. If you continue to use a VPN, you might need to upgrade your VPN gateway, or you might decide to move to a private connection using FastConnect. Both options require an investment.

OCI Site-to-Site VPN (IPSec)

OCI Site-to-Site VPN (IPSec) enables you to connect your on-premises network to a virtual cloud network (VCN), which is deployed in one or more OCI regions. From the Oracle Cloud Console, configure the Oracle end of the VPN connection. We recommend that you engage your networking team to configure the Site-to-Site VPN in the Oracle Cloud Console and on your edge device. For instructions in the Oracle Cloud Console, see Setting Up Site-to-Site VPN. For information about how to configure your edge device, see CPE Configuration.

Figure 1 provides a high-level overview of the connection and the different components involved in OCI and your on-premises network. The VPN configuration is done at your edge device and in the Oracle Cloud Console.

Note: When you configure Site-to-Site VPN in the Oracle Cloud Console, Oracle provides you with two VPN gateways in the region to terminate the tunnels. However, the VPN gateways aren't objects that you can configure in the Console. In the diagrams shown in this document, the VPN gateways are represented as independent components to illustrate the concepts and the termination points for the tunnels, but mainly the connection terminates in the dynamic routing gateway (DRG).

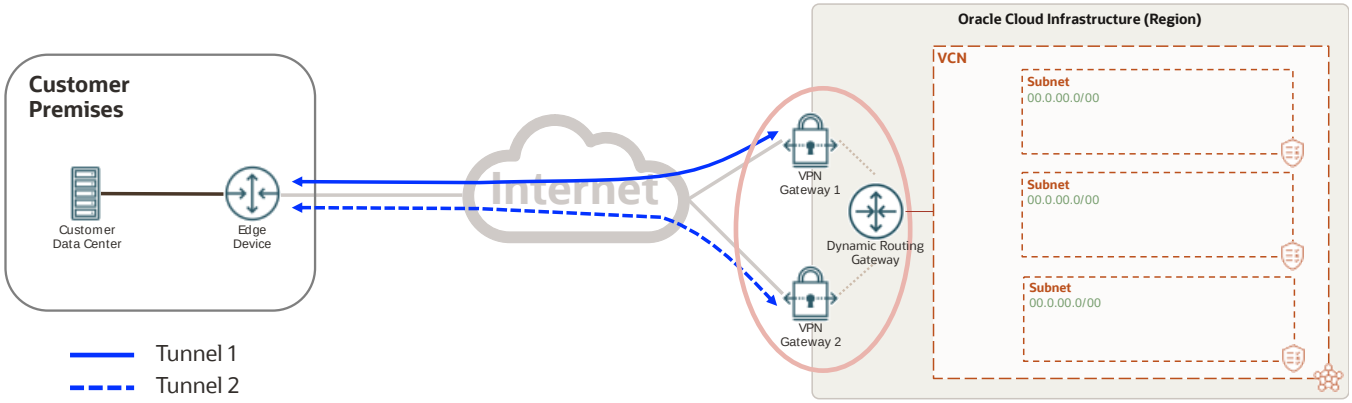

Figure 1: OCI Site-to-Site VPN (IPSec) Overview

Recommendations for Your Edge Device

Your edge device can be a router, a firewall, an SD-WAN device, or a virtual machine (VM), if it supports standard IPSec tunnels. The edge device is managed and supported by your network engineering team or by a managed service provider. We recommend that you configure your VPN-capable edge device in your on-premises network with the following guidelines:

- Support tunnel mode encryption. Transport mode is not supported.
- In your on-premises network, use the IKE identifier as your edge device's public IP address. The remote IKE identifier is the IP address of Oracle's VPN gateways.
- If your edge device is behind a NAT device and you can't set your edge device's IKE identifier to match your public IP address, you can modify the Site-to-Site VPN configuration in the Oracle Cloud Console and enter the correct private IP address of your edge device.
- By default, Oracle supports a single encryption domain. The encryption domain defines the "interesting traffic" that's encrypted in the tunnel. Don't create multiple encryption domains to accommodate the various subnets in the Oracle VCN of your on-premises network. Instead, summarize the subnets into a single supernet—several subnets combined or summarized into one network with a single CIDR prefix.

For example, if your VCN network is 10.40.0.0/17 and 10.40.128.0/17, and your on-premises network is 10.0.0.0/18, 10.0.64.0/18, 10.0.128.0/18, and 10.0.192.0/18, you can use either of the following options to create a single encryption domain:

Table 1: Encryption Domain Examples

ALLOW EVERYTHING	SUMMARIZE SUBNETS
Source IP address: Any (0.0.0.0/0) Destination IP address: Any (0.0.0.0/0) Protocol: IPv4	Source IP address: Customer Subnet (10.0.0.0/16) Destination IP address: VCN Subnet (10.40.0.0/16) Protocol: IPv4

- If you require multiple encryption domains for policy-based tunnels, Oracle supports them on our new VPN service, and it needs to be enabled for each tunnel. In the Console, if the Site-to-Site VPN is version 2, it supports policy-based tunnels. Here, you can specify the CIDRs for on-premises and OCI.
- Use the parameters in Table 2 for the most compatibility and success when connecting to OCI. When more than one value is shown, the bolded item represents the recommended parameter to use when configuring your edge device. You can't configure these parameters in the Console, but the policies are already preconfigured to support all the options. If a parameter isn't listed in the table, it's not supported. Oracle supports the following parameters for IKEv1 or IKEv2. For the latest supported parameters check Supported IPSec Parameters.

Table 2: Phase 1 and Phase 2 Supported Parameters

ISAKMP POLICY OPTIONS (PHASE 1)	IPSEC POLICY OPTIONS (PHASE 2)
ISAKMP version 1 Exchange type: Main mode Authentication method: Preshared-keys Encryption: **AES-256-cbc**, AES-192-cbc, AES-128-cbc Authentication algorithm: **SHA-2 384**, SHA-2 256, SHA1 (also called SHA or SHA1-96) Diffie-Hellman group: Group 2, group 5, group 14, group 19, **group 20** IKE session key lifetime: 28,800 seconds (8 hours)	IPSec protocol: ESP, tunnel-mode Encryption: **HMAC-SHA-256-128**, AES-192-gcm, AES-128-gcm, AES-256-cbc, AES-192-cbc, AES-128-cbc Authentication algorithm: **HMAC-SHA-256-128**, HMAC-SHA1-96 IPSec session key lifetime: 3,600 seconds (1 hour) Perfect Forward Secrecy (PFS): Enabled, group 5

Table 3 shows an example of your edge device's configuration and how the Oracle end is already configured by using the recommended parameters from Table 2. The edge device and Oracle configurations are the same.

Table 3: VPN Configuration Example for Both Phases on Both Ends of the VPN

CUSTOMER EDGE DEVICE	ORACLE
ISAKMP Policy Options (Phase 1) • ISAKMP version 1 • Exchange type: Main mode • Authentication method: Preshared-keys • Encryption: AES-256-cbc • Authentication algorithm: SHA-2 384 • Diffie-Hellman group: Group 20 • IKE session key lifetime: 28,800 seconds	**ISAKMP Policy Options (Phase 1)** • ISAKMP version 1 • Exchange type: Main mode • Authentication method: Preshared-keys • Encryption: AES-256-cbc • Authentication algorithm: SHA-2 384 • Diffie-Hellman group: Group 20 • IKE session key lifetime: 28,800 seconds
IPSec Policy Options (Phase 2) • IPSec protocol: ESP, tunnel-mode • Encryption: AES-256-gcm • Authentication algorithm: HMAC-SHA-256-128 • IPSec session key lifetime: 3,600 seconds • Perfect Forward Secrecy (PFS): Enabled, group 5	**IPSec Policy Options (Phase 2)** • IPSec protocol: ESP, tunnel-mode • Encryption: AES-256-gcm • Authentication algorithm: HMAC-SHA-256-128 • IPSec session key lifetime: 3,600 seconds • Perfect Forward Secrecy (PFS): Enabled, group 5

- With most VPN-capable edge devices, the IPSec tunnel comes up only after "interesting traffic" is sent through the tunnel. Interesting traffic is the traffic that is allowed in the encryption domain. By default, interesting traffic is initiated from the on-premises network. You can initiate the connection from an instance on the Oracle end only if you have configured the tunnel by using any-to-any for the encryption domain.
- SLA monitoring ensures that interesting traffic is sent and that the IPSec tunnel remains active. This monitoring can be accomplished with a ping or probe. For Cisco devices, it's mandatory to configure an SLA monitor for policy-based tunnels if the IP address of the edge device is part of the encryption domain.
- By default, Oracle generates a key per tunnel that's available to you in the Oracle Cloud Console. You can use it or provide your own.
- OCI supports IPSec NAT Traversal (RFC 3947).

After the VPN is configured based on our recommendations, you can direct traffic to the IPSec tunnels. Routing and security play an important role in this step. Even if the VPN is configured correctly and the IPSec tunnels are in an UP state on both ends, traffic doesn't flow through the IPSec tunnels if the routing or security lists are set incorrectly. To ensure that routing and security lists are configured correctly on both OCI and on-premises, consider the following recommendations:

- Routing
  - Configure the on-premises edge device to ensure traffic destined for the VCN is pointing to the VPN edge device and the correct VPN or tunnel interface.
  - When using static routing, ensure that the on-premises edge device withdraws the route from the route table when the tunnel is down. Otherwise, it doesn't fail over properly.
  - Because each Site-to-Site VPN connection has two tunnels, ensure that traffic can route through both tunnels, and give the routes the correct priority.

- Security
    - For on-premises networks, ensure that any firewall in the path to Oracle isn't blocking any communication with the VCN. This configuration is key for the success of the connection because the firewall can block traffic for tunnel enablement and interesting traffic.
    - Each Site-to-Site VPN connection has two tunnels, and you need to allow traffic through both tunnels in your firewalls. Don't treat the tunnels as active and standby because Oracle can use either tunnel to send traffic.
    - Ensure that the firewalls or any other security list in your on-premises network allow ICMP type 3 code 4 messages, which enable path maximum transmission unit discovery (PMTUD) to determine the maximum protocol data units (PDU) used during data transmission.

Following the design principles, we also recommend building redundant solutions and avoiding single points of failure. Redundancy allows the connection to persist even when Oracle, the vendor or carrier, or your organization performs any maintenance in the network.

- Identify any single points of failure in the network and eliminate them by deploying redundant or diverse hardware and paths.
- After Site-to-Site VPN is configured in the Console, Oracle automatically provides the public IP addresses of two diverse VPN gateways within the same region for redundancy.
- Advertise more-specific routes through the primary tunnel and less-specific routes through the backup tunnel for predictable failover and failback.

Recommendations for Oracle Cloud Infrastructure

In the Oracle Cloud Console, you need to create and enable some components to correctly configure the Site-to-Site VPN. You cloud administrator or network team can do this configuration. For instructions, see Overview of Networking.

Consider the following steps for a successful deployment:

1. Create a dynamic routing gateway (DRG).
2. Attach the DRG to your VCN.
3. Create a customer-premises equipment (CPE) object.
4. Create a Site-to-Site VPN connection.
5. Configure routing:
    - During the Site-to-Site VPN configuration, specify your on-premises network prefixes. This configuration tells the DRG how to reach your on-premises network.
    - The VCN in OCI must have a route rule that points to the DRG attached to the VCN for any routes destined to the on-premises network. The route rule can be in the default route table or in a subnet-specific route table.
    - You can control which subnets in the VCN can communicate with your on-premises network. In the route tables for each of your VCN's subnets, specify some subnets instead of advertising your whole on-premises network.
    - Each Site-to-Site VPN connection has two tunnels, and Oracle uses any of them based on availability. The traffic might be asymmetric between OCI and the on-premises network. Ensure that traffic is allowed on the on-premises network for both tunnels.

- Oracle provides two VPN gateways for each Site-to-Site VPN connection. Oracle places the first tunnel in the route table. If Oracle has a route to the same destination, it always uses the oldest one. If the current tunnel goes down, traffic fails over to the other tunnel. When the first tunnel is restored, traffic doesn't fail back to it because the route from the restored tunnel is newer than the current route.
- The DRG supports equal cost multi-path (ECMP), so for Site-to-Site VPN, the DRG places the routes for each tunnel in the routing table if ECMP is enabled.

6. Configure security:
   - Update the ingress and egress rules in the subnet's security list or network security groups to allow or deny traffic back to the on-premises network.
   - Use security lists or network security groups to control what traffic is allowed between the on-premises network and the VCN at a more granular level.
   - Ensure that both the VCN security lists and the instance firewalls allow ICMP type 3 code 4 messages, which enable PMTUD to determine the maximum PDU used during data transmission.

Redundancy Testing

Redundancy is an important design principle for an effective VPN solution. We recommend testing your design during deployment to ensure that the routing is set correctly and that failover and failback work as expected. Use the following steps for testing. These steps apply to all the use cases described in the next section.

1. Ensure all paths (tunnels and FastConnect) are up.
2. Initiate a continuous ping from the on-premises network to the VCN. Keep this ping running during the test.
3. Verify that the traffic is taking the primary path by doing a trace route and comparing the results to the design. Trace route works only if the devices in the path are allowed to respond to it and no firewalls or security lists are blocking it.
4. Disable the primary path by shutting down the tunnel interface or the FastConnect interface. The ping fails until the traffic failover to the backup path. For future reference, record how long the failover takes.
5. Perform another trace route and compare the results to the results from step 3. The results are now different and now match your design.
6. Enable the primary path by bringing up the tunnel interface or the FastConnect interface. You might see a few packets drop as the traffic fails back to the primary path. With Site-to-Site VPN, traffic fails back to the primary path if a more-specific subnet is advertised over the primary path and a less-specific route is advertised over the secondary path. If the same route is advertised over both paths, traffic doesn't fail back.
7. Perform another trace route to verify that the traffic is taking the primary path. The result is the same as the result from step 3.
8. The preceding steps verify failover and failback. As an extra step, disable the backup path to verify that it doesn't affect the solution. No packets should drop on your continuous ping. If you advertised the same subnets over both paths, this step forces the traffic to fail back to the primary path.
9. During this test, check the route table to ensure that a route is removed from it when the path isn't available.

Use Cases

This section describes typical use cases for connecting on-premises network to OCI by using Site-to-Site VPN over the internet. Routing requirements are provided for each use case.

Note: When you configure Oracle Site-to-Site VPN, Oracle provides you with two VPN gateways in the region to terminate the tunnels. However, the VPN gateways aren't objects that you can configure in the Console. In this section, the diagrams show the VPN gateways represented as independent components to illustrate the concepts and to show the termination points for the tunnels, but mainly the connection is to the DRG.

- Single region, single customer edge device (standard availability, low cost)
- Single region, redundant customer edge devices (high availability, medium cost)
- FastConnect plus single region, single customer edge device VPN (high availability, high cost)
- Single region, multiple VCNs, single or dual customer edge device (high availability, medium cost)
- Dual region, single or dual customer edge device (high availability, medium cost)

Single Region, Single Customer Edge Device

This use case is the simplest design for connecting to OCI using a Site-to-Site VPN over the internet. It consists of one edge device in the on-premises network and two VPN gateways (default) in a single OCI region. The edge device can be in your headquarters, a data center, a colocation facility, or in another cloud. The position of the edge device depends on who and what needs to communicate with OCI from your on-premises network. Figure 2 shows the general design of this use case.

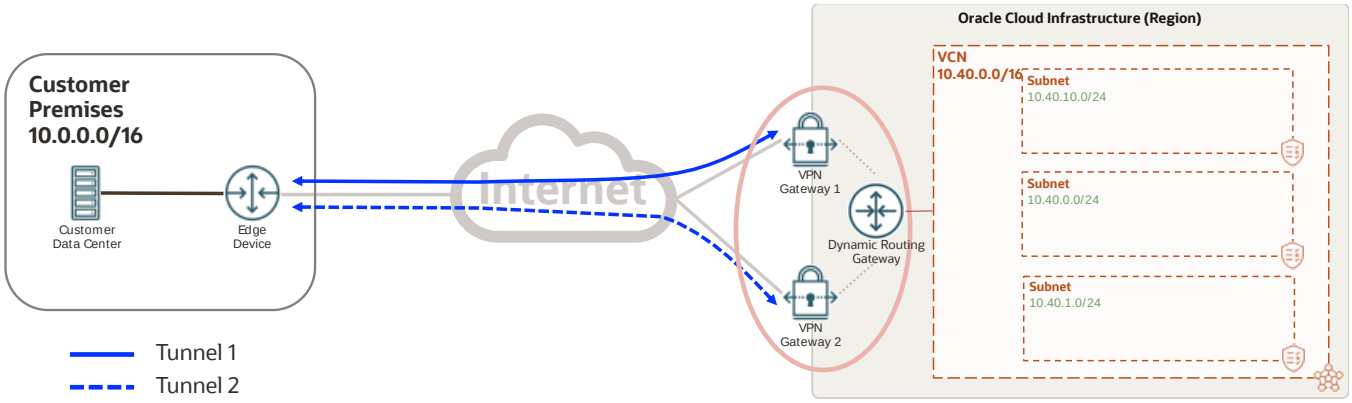

Figure 2: Site-to-Site VPN for a Single Region with a Single Customer Edge Device

Routing is necessary for the solution to work correctly. Figure 3 shows the routing details for the different components. On your edge device, the VCN subnet is advertised through the two tunnels. We recommend that you give priority to one of the tunnels. Oracle uses asymmetric routing across the two tunnels that make up the Site-to-Site VPN connection. Even if you configure one tunnel as primary and the other as backup, traffic from the VCN to your on-premises network can use any tunnel that is up. As a result, you can send traffic from on-premises network to OCI through one tunnel while Oracle sends traffic to on-premises network through a different tunnel. To avoid symmetry, advertise more specific prefixes through one tunnel and less specific prefixes through the other tunnel, or if using BGP, prepend one path.

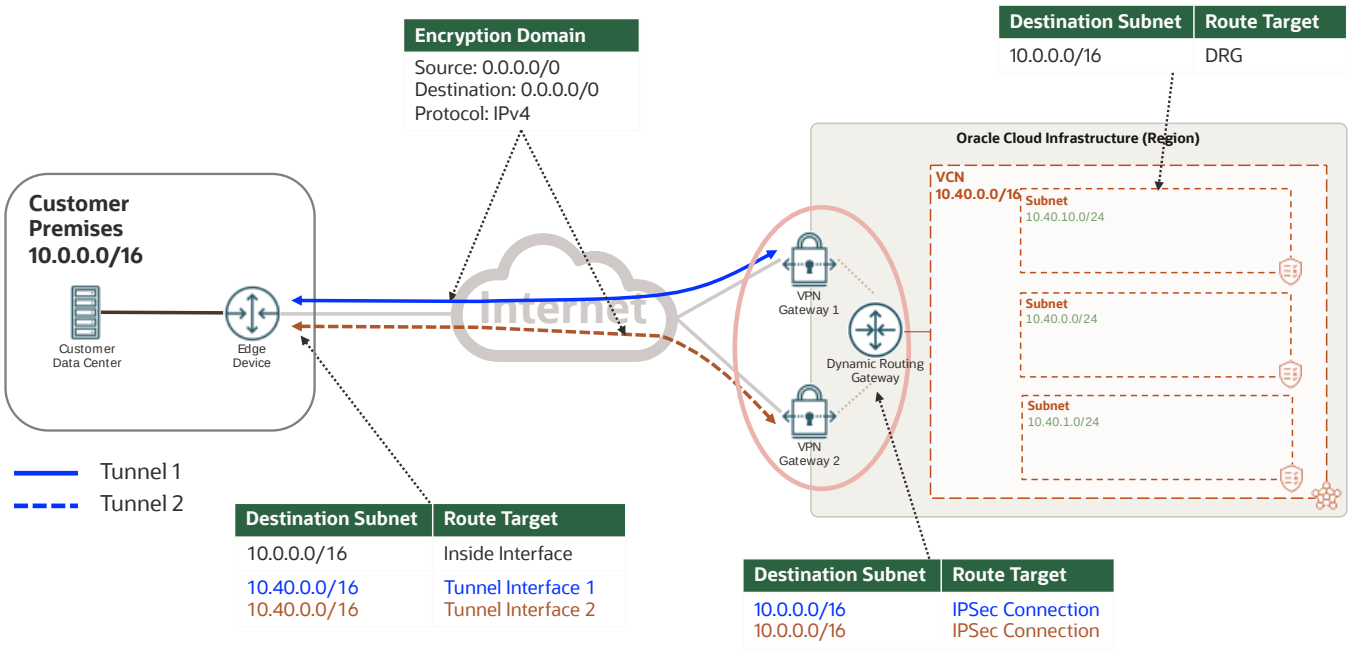

Figure 3: Routing for Site-to-Site VPN for a Single Region and a Single Customer Edge Device

When you create the Site-to-Site VPN connection, include all on-premises network prefixes if using static routing. To avoid changing them in the future, include a supernet that covers all on-premises networks. Use BGP to advertise them dynamically and control prefix advertisement. On-premises network prefixes are entered on the Site-To-Site VPN configuration not on the DRG. Figure 3 also shows that both tunnels use the same encryption domain.

If the edge device supports ECMP, you can enable it on both sides of the VPN, so traffic uses the two tunnels to distribute itself. This configuration also eliminates any routing asymmetry.

Security lists must be updated accordingly to allow the traffic. However, this document focuses more on the network because security depends on the different types of applications and traffic allowed through this connection.

Single Region, Redundant Customer Edge Devices

One of the key design points highlighted in this document is redundancy. The previous solution has a single point of failure in the design: the edge device. To correct this issue, deploy a redundant edge device in the on-premises network. This device can exist in the same location as the primary device, in a different data center, or even in another cloud.

If the second edge device is in the same facility as the primary device, validate that both devices do *not* connect to the same internet provider, the same LAN switch, or the same power unit. That is, ensure that your edge devices don't share a common point of failure. If the second device is deployed at a different site, ensure that the two sites are connected by your backbone and traffic can flow between them. For simplicity, Figure 4 shows the two edge devices at the same location with two carriers connecting to the internet.

By default, Oracle provides two VPN gateways for you to create two tunnels from each edge device. As a result, you have four tunnels, two tunnels per edge device, as represented by the brown and blue lines in Figure 4. Also shown in Figure 4, Oracle provides diverse VPN gateways per Site-to-Site VPN connection to both edge devices.

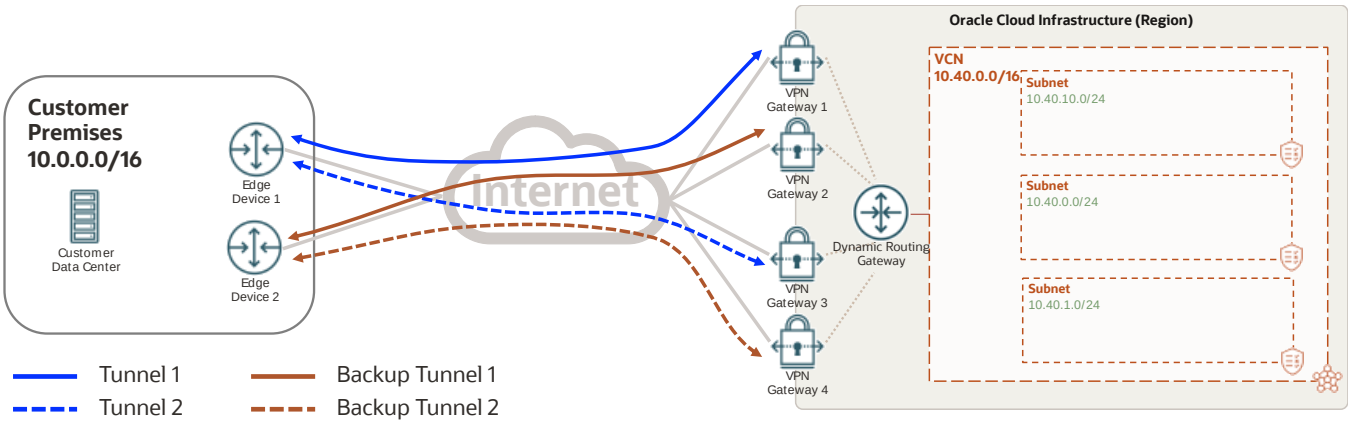

Figure 4: Site-to-Site VPN for a Single Region with Redundant Customer Edge Devices

If redundancy is maintained, you can choose *not* to create the second tunnel from each edge device. This configuration is represented in Figure 5, in which Tunnel 2 (the dotted blue line) is removed from edge device 1 and backup tunnel 1 (the solid brown line) is removed from edge device 2. Oracle still provides the VPN gateways and accepts the connection if you configure them. This design provides redundancy because each edge device builds a tunnel to diverse Oracle VPN gateways. You can verify that the gateways are diverse by checking the third octet in the IP address of the Oracle VPN gateway.

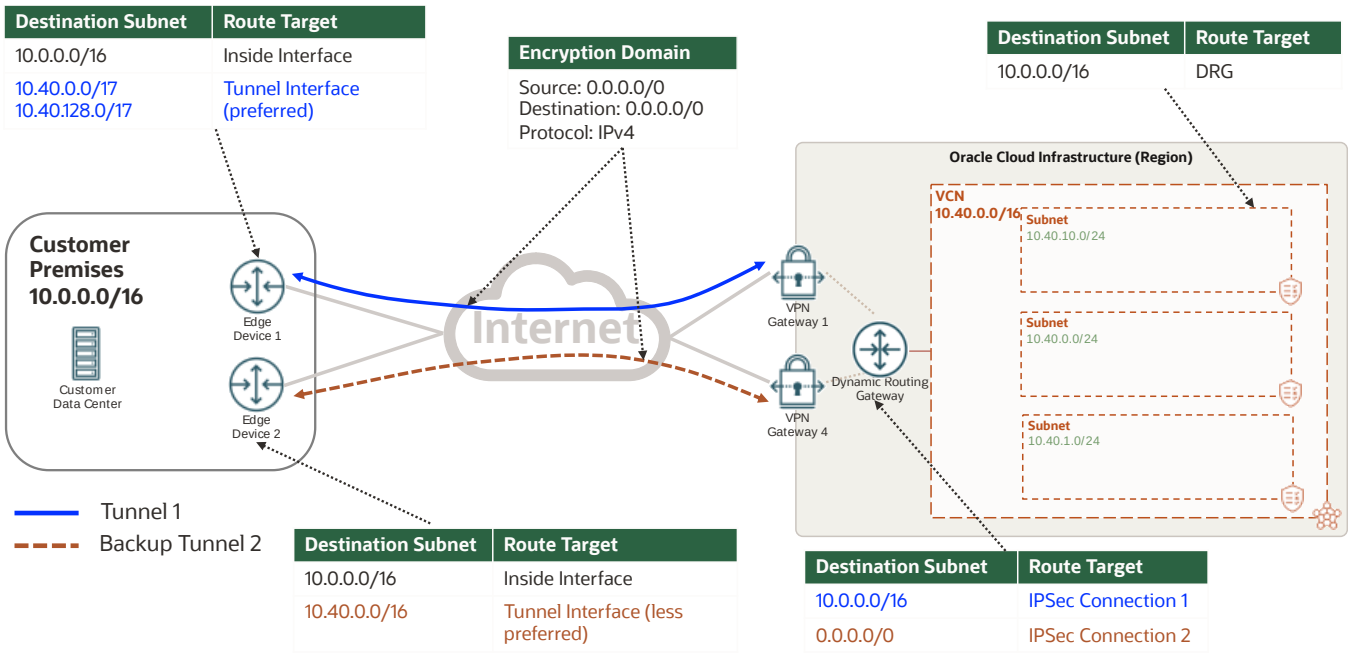

Figure 5: Routing and Encryption Domain for Site-to-Site VPN for a Single Region with Redundant Customer Edge Devices

Now that the solution has at least two fully diverse tunnels, ensure that routing is correctly set on both ends of the connection. First, define the primary and backup tunnels. As depicted in Figure 5, Tunnel 1 is the primary path and backup tunnel 2 is the backup. To influence the routing, we recommend advertising specific subnets over the primary tunnel and advertising less specific or summarized routes over the backup tunnel. With this approach, traffic is symmetrical. If the primary path fails, a less specific route is still available through the backup path. After the primary path is restored, traffic routes using the more specific route advertised for the primary path. Remember to set your routing to withdraw the route from the route table when the tunnel is not available; otherwise traffic doesn't fail over to the backup tunnel.

Figure 5 shows the routing for each of the components (the color assigned to the route highlights which path it belongs to). In your on-premises network, influence traffic to take the primary path (blue) based on your internal routing protocol because both edge devices advertise the same VCN prefix. From the Oracle end, you advertise your on-premises network for the primary (blue) path and advertise the default route through the backup (brown) path as represented in Figure 5. You can achieve the same scenario by manipulating the metrics on BGP to prefer the primary path.

Routing is independent of the encryption domain configuration in the tunnels. With routing, you can decide what traffic is sent to the tunnel interface, while the encryption domain defines what traffic is encrypted and placed into the tunnel. In Figure 5, the encryption domain (middle of the diagram) is the same for both tunnels on both sides, allowing any traffic, while routing is handled at each end of the connection to make a primary and backup tunnel to maintain redundancy. This solution maintains a single encryption domain per our recommendation even though the routing uses multiple and more specific prefixes.

FastConnect Plus Single Region, Single Customer Edge Device VPN

If your current edge device doesn't support the required new bandwidth, or you need a more reliable connection, you might need to upgrade your connection by deploying a FastConnect solution to OCI. You can continue to use the Site-to-Site VPN, but instead of using it as your primary connection, use it as a backup if it meets your backup needs.

FastConnect doesn't use the internet. Instead, it uses private circuits through Oracle partners, third-party providers, or cross-connects. To avoid a single point of failure, deploy FastConnect and Site-to-Site VPN from different edge devices in your network. When you use FastConnect, you need to create a private virtual circuit (VC) between the on-premises network and OCI, as represented by the top (solid green) line in Figure 6.

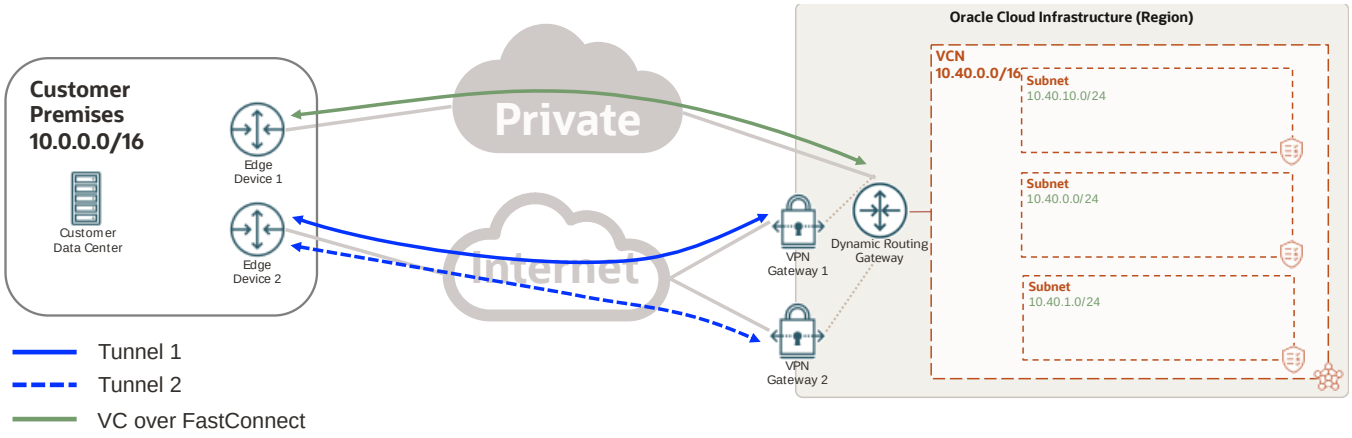

Figure 6: FastConnect Plus a Single Region and a Single Customer Edge Device VPN

For routing, follow the same approach as the previous solution, in which you advertise more specific routes through the primary path (now the VC) and less specific routes through the backup tunnels (Site-to-Site VPN). The DRG learns on-premises prefixes on FastConnect through BGP and advertises the VCN subnets back to your edge device. The DRG also has a static route for a default route that points to the Site-to-Site VPN or could use BGP to learn your on-premises routes dynamically through the Site-to-Site VPN.

On your end of the connection, you advertise to your network the VCN's subnets learned by BGP over FastConnect while advertising a less specific route through the Site-to-Site VPN. If you can't advertise the default route through the Site-to-Site VPN, you can manipulate the route accordingly based on the routing protocol that you use in your network. For example, use AS prepend, or local preference. Figure 7 shows the routing for this use case.

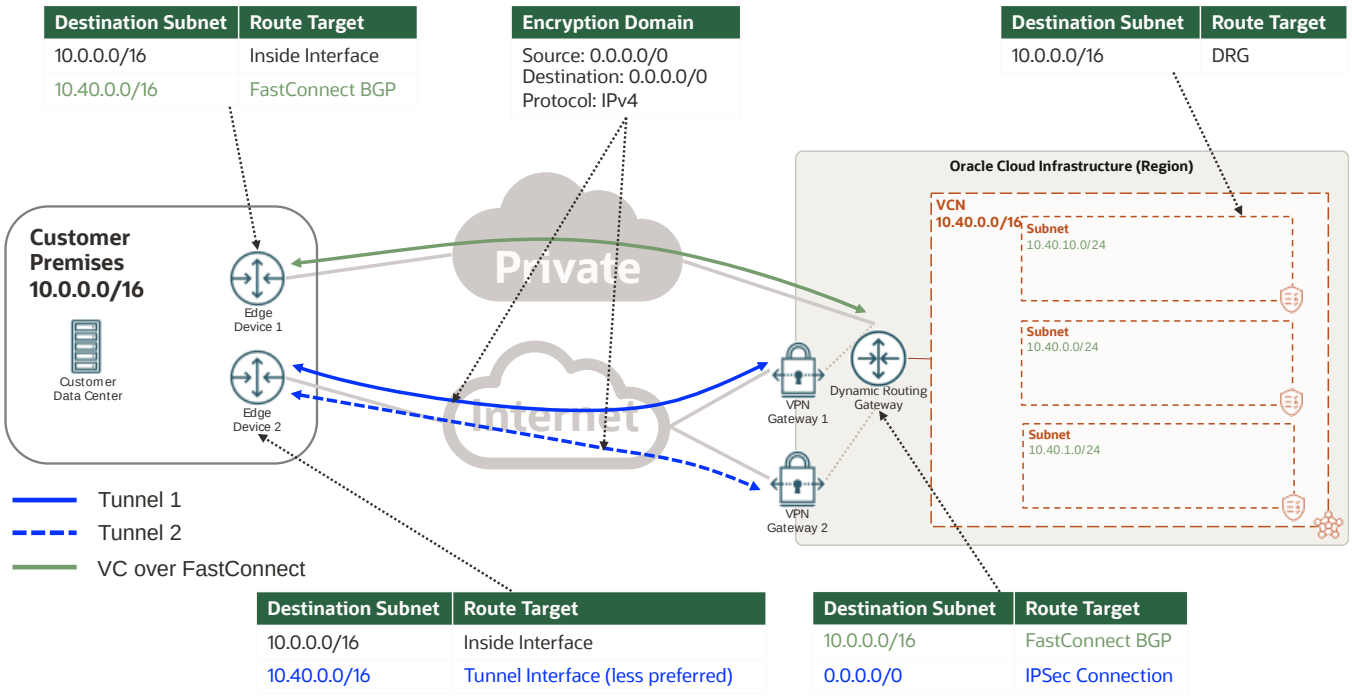

Figure 7: Routing for FastConnect Plus a Single Region and a Single Customer Edge Device VPN

Single Region, Multiple VCNs, Single or Dual Customer Edge Device

Cloud deployments might be initiated by different groups or business units within your organization. You might have resources in multiple VCNs in the same region. This use case lets you use a Site-to-Site VPN to connect to a single OCI region that hosts multiple VCNs. The enhancements deployed for the DRG allow you to connect to multiple VCNs with a single DRG. Figure 8 shows the general design of this use case.

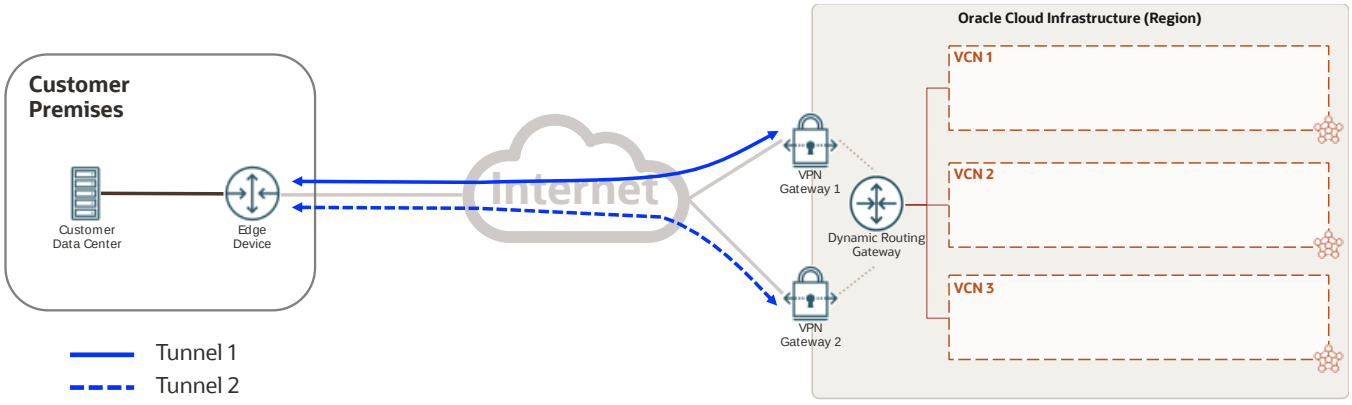

Figure 8: Site-to-Site VPN for the Same Region with Multiple VCNs—High-Level Design

The example in Figure 9 uses only two VCNs connecting to your on-premises network through single edge device. You can use any of the previous use cases to build redundancy for this solution. To connect multiple VCNs to a single DRG, ensure that no IP addresses overlap between the VCNs and on-premises.

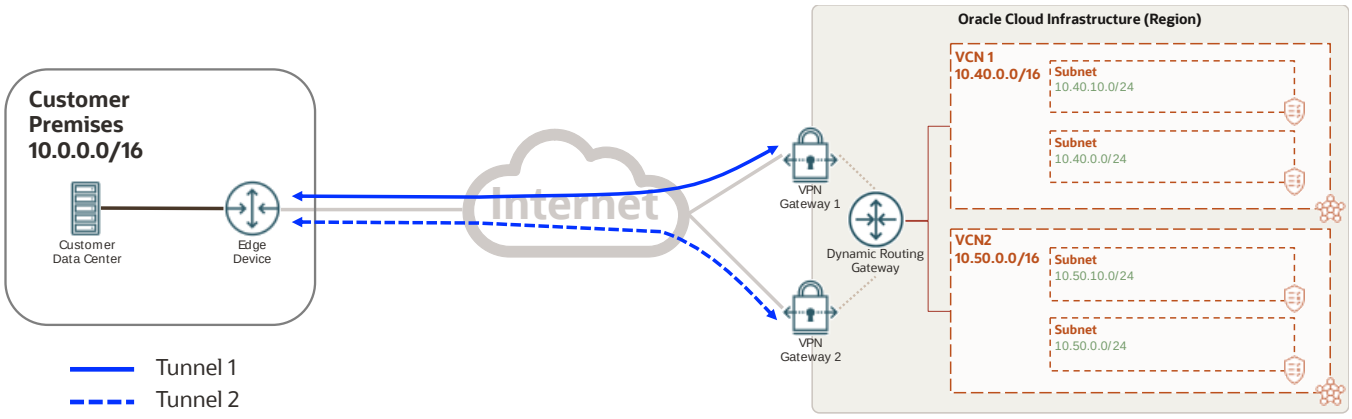

Figure 9: Site-to-Site VPN for the Same Region with Multiple VCNs with a Single Customer Edge Device

From on-premises, advertise the subnets for both VCNs pointing to the tunnel interface. You still maintain a single encryption domain that allows all the traffic (0.0.0.0/0). Each VCN's subnet needs a route to reach the on-premises network and the other VCN, as represented in Figure 10:

- VCN 1 subnets need a route for on-premises network and for VCN 2 that points to the DRG.
- VCN 2 subnets need a route for on-premises network and for VCN 1 that points to the DRG. You can add a specific route to it or use a default route as shown in Figure 10.

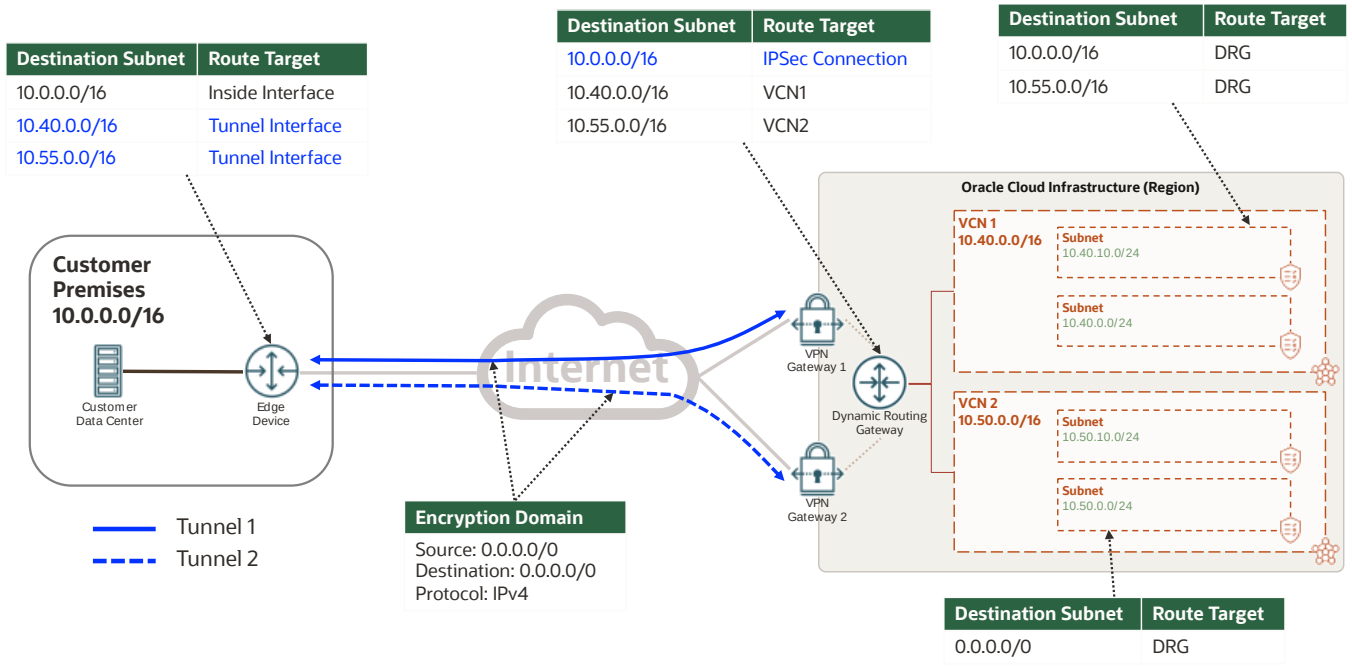

Figure 10: Routing for Site-to-Site VPN for the Same Region with Multiple VCNs with a Single Customer Edge Device

Dual Region, Single or Dual Customer Edge Device

Based on your geographic locations, you might use VCNs in multiple Oracle Cloud Infrastructure regions. To enable the resources in your on-premises network to communicate with resources in these regions, you need to create independent connections to each region. For redundancy, you can use the second use case with dual Site-to-Site VPN connections, or use the third use case to deploy FastConnect in each region.

From the on-premises network, you can connect to one region and then jump to another region by using a region as a transit network. However, we recommend deploying FastConnect or Site-to-Site VPN to both regions for redundancy. Oracle allows resources in the VCNs in various regions to communicate with each other only by using a regional peering connection (RPC). From the Oracle Cloud Console, you can set up an RPC in your DRG, as shown in Figure 11. For more information about RPC, see Remote VCN Peering (Across Regions). These concepts apply for both single and dual customer edge devices in your network. For simplicity, Figure 11 shows a single customer edge device.

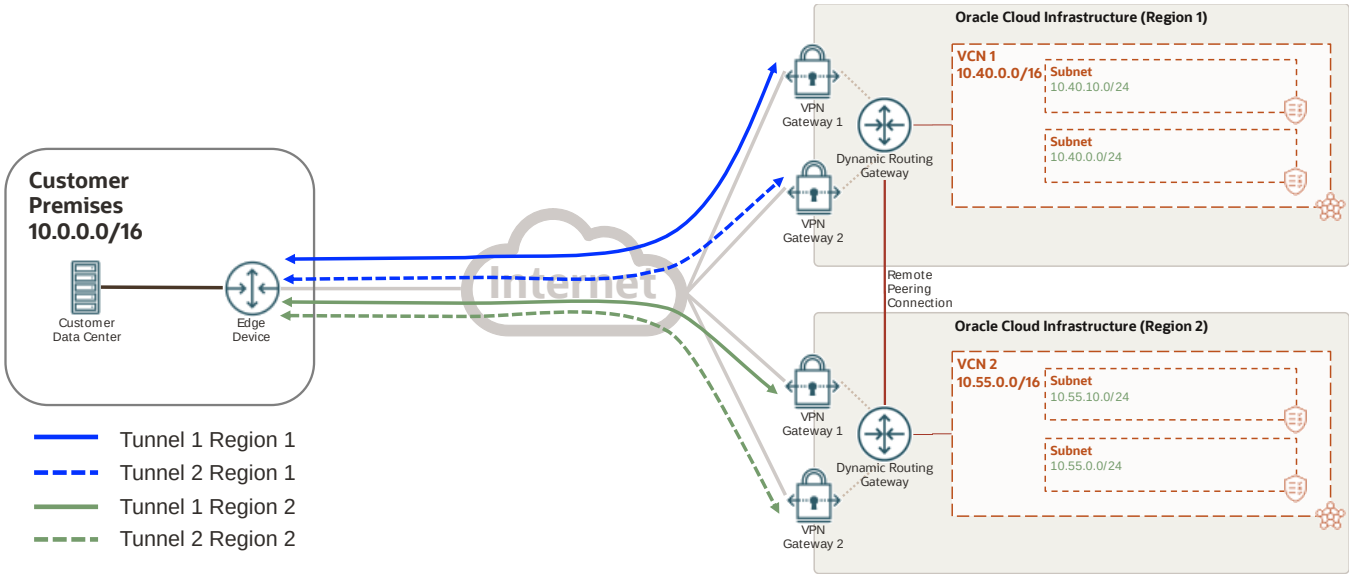

Figure 11: Site-to-Site VPN for Dual Regions with a Single Customer Edge Device

The routing for this use case is the same as for the first use case, the two sets of tunnels (blue and green tunnels in Figure 12) are independent from each other. The VCN and the subnets in the VCN need a route that points to their respective DRG for traffic going to the remote VCN and to on-premises. Traffic between the VCNs uses the remote peering connection, as indicated in Figure 12.

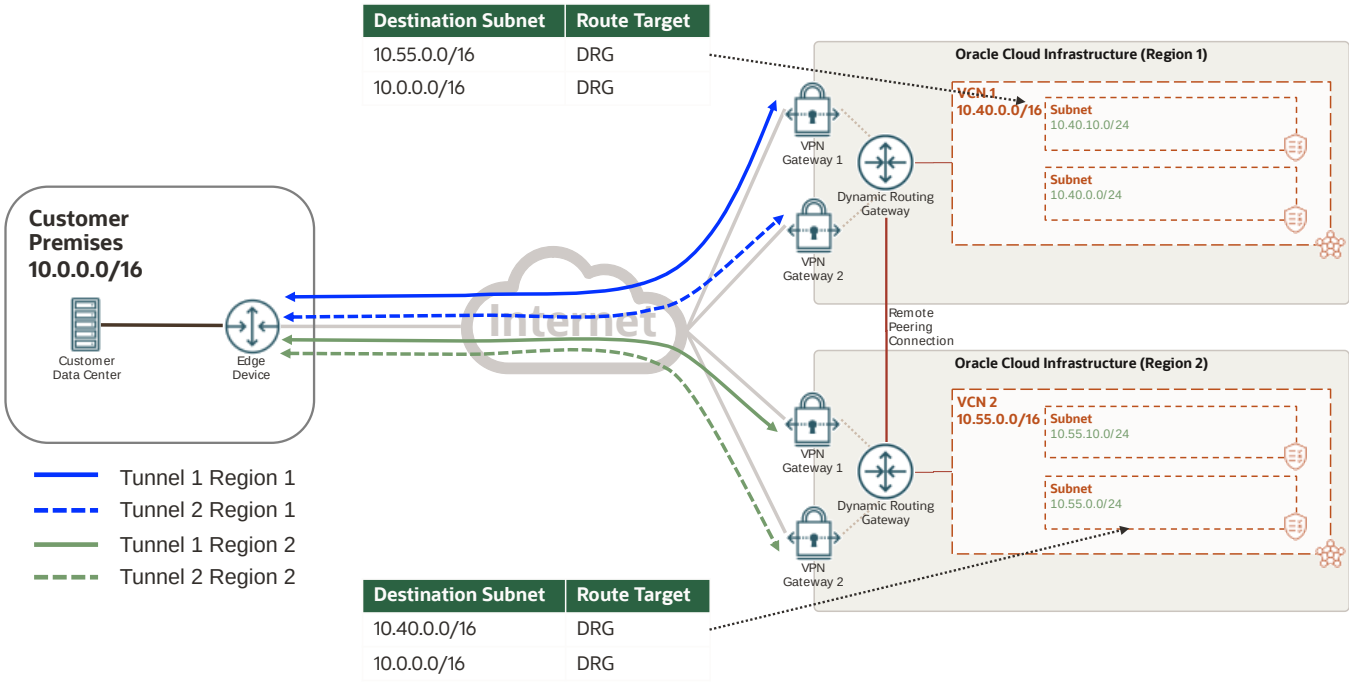

Figure 12: Site-to-Site VPN for Dual Regions with a Single Customer Edge Device Routing

References

- For more information about the Site-to-Site VPN in Oracle Cloud Infrastructure, see Site-to-Site VPN.
- For more information about the Oracle Cloud Infrastructure Networking service, see Overview of Networking.
- For help with subnets and mask check, see the Visual Subnet Calculator.

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