IPSec VPN Best Practices

ORACLE®

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Revision History

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

Date	Revision
May 21, 2019	Initial publication

You can find the most recent versions of the Oracle Cloud Infrastructure white papers at
https://cloud.oracle.com/iaas/technical-resources.

Table of Contents

Overview

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

Design Principles

When designing an IPSec VPN solution, consider the following principles:

- **Hardware capabilities:** Depending on the required workload, your infrastructure must have enough capacity to support the required bandwidth from your on-premises network to Oracle Cloud. 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 must have 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 an IPSec VPN with Oracle Cloud Infrastructure, Oracle by default provides two gateways to terminate the tunnels. The two tunnels are always active, and you should allow traffic from both tunnels into your network. Don't treat them as active and standby.

- **Performance:** An IPSec VPN in Oracle Cloud Infrastructure uses the public internet to connect your on-premises network to the Oracle Cloud. 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 is not set properly, traffic won't flow through the tunnel. IPSec VPN supports static routing and 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.

- **IPSec VPN configuration:** For two endpoints to establish an IPSec connection and for traffic to flow through the tunnel successfully, the settings on both ends must match 100 percent. 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. An IPSec 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 an IPSec 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.

Oracle Cloud Infrastructure VPN Connect

Oracle Cloud Infrastructure VPN Connect enables you to connect your on-premises network to a virtual cloud network (VCN) that is deployed in one or more Oracle Cloud regions. You use the Oracle Cloud Infrastructure Console to configure the Oracle end of the IPSec VPN connection. We recommend that you engage your networking team to configure VPN Connect in the Oracle Console and on your edge device. For step-by-step instructions, see Setting Up VPN Connect.

Figure 1 provides a high-level overview of the connection and the different components involved in the Oracle Cloud and your on-premises network. The IPSec VPN configuration is done at your edge device and at the dynamic routing gateway (DRG) in the Oracle Cloud.

Note: When you configure VPN Connect in the DRG in the 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 is to the DRG.
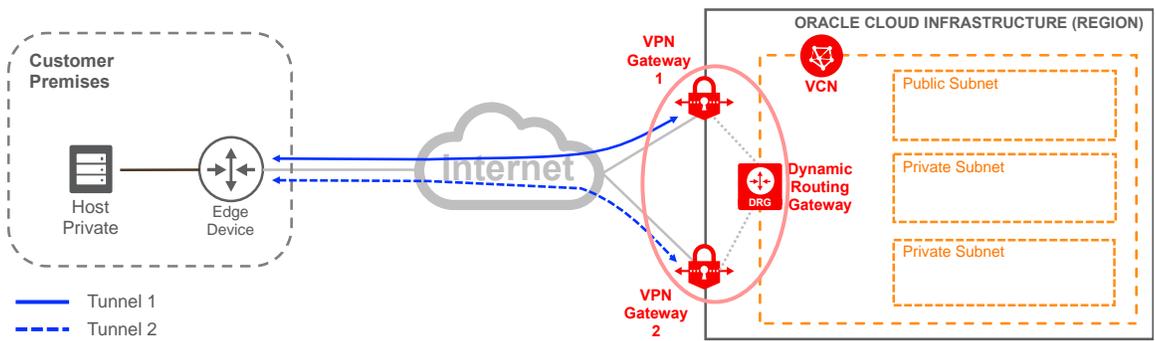
Figure 1. VPN Connect Overview

Recommendations for Your Edge Device

Your edge device could be a router, a firewall, an SD-WAN device, or a VM, as long as it supports standard IPSec VPN tunnels. This 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 for your tunnels:

- Support **tunnel mode** encryption. Transport mode is not supported.

- In your on-premises network, the **IKE identifier** should be 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 IPSec connection in the Oracle Console and enter the correct public IP address or hostname.

- Oracle supports a **single encryption domain**. The encryption domain defines the "interesting traffic" that is encrypted in the tunnel. Don't create multiple encryption domains to accommodate the various subnets in the Oracle VCN or 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 could 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

- Use the **parameters** in Table 2 for the most compatibility and success when connecting to Oracle Cloud. Where more than one value is shown, the bolded items represent the *recommended* parameters to use when configuring your edge device. These parameters can't be configured on the Console, but the policies are already preconfigured to support all the options. If a parameter is not listed in the table, it's not supported.

TABLE 2. PHASE 1 AND PHASE 2 SUPPORTED PARAMETERS

ISAKMP Policy Options (Phase 1)	IPSec Policy Options (Phase 2)
- ISAKMP Protocol version 1 - Exchange type: Main mode - Authentication method: pre-shared-keys - Encryption: **AES-256-cbc**, AES-192-cbc, AES-128-cbc - Authentication algorithm: **SHA-384**, SHA-256, SHA1 (also called SHA or SHA1-96) - Diffie-Hellman group: **group 5**, group 2, group 1 - IKE session key lifetime: **28800 seconds** (8 hours)	- IPSec protocol: ESP, tunnel-mode - Encryption: **AES-256-cbc**, AES-192-cbc, AES-128-cbc - Authentication algorithm: **HMAC-SHA1-96** - IPSec session key lifetime: **3600 seconds** (1 hour) - Perfect Forward Secrecy (PFS): **enabled, group 5**

Table 3 shows an example of how your edge device should be configured and how the Oracle end is already configured by using the recommended parameters from Table 2. Note that the edge device and Oracle configurations are the exactly the same.

TABLE 3. IPSEC VPN CONFIGURATION EXAMPLE FOR BOTH PHASES ON BOTH ENDS OF THE VPN

Customer Edge Device	Oracle
ISAKMP Policy Options (Phase 1)	**ISAKMP Policy Options (Phase 1)**
- ISAKMP Protocol version 1 - Exchange type: Main mode - Authentication method: pre-shared-keys - Encryption: **AES-256-cbc** - Authentication algorithm: **SHA-384** - Diffie-Hellman group: **group 5** - IKE session key lifetime: **28800 seconds**	- ISAKMP Protocol version 1 - Exchange type: Main mode - Authentication method: pre-shared-keys - Encryption: **AES-256-cbc** - Authentication algorithm: **SHA-384** - Diffie-Hellman group: **group 5** - IKE session key lifetime: **28800 seconds**
IPSec Policy Options (Phase 2)	**IPSec Policy Options (Phase 2)**
- IPSec protocol: ESP, tunnel-mode - Encryption: **AES-256-cbc** - Authentication algorithm: **HMAC-SHA1-96** - IPSec session key lifetime: **3600 seconds** - Perfect Forward Secrecy (PFS): **enabled, group 5**	- IPSec protocol: ESP, tunnel-mode - Encryption: **AES-256-cbc** - Authentication algorithm: **HMAC-SHA1-96** - IPSec session key lifetime: **3600 seconds** - Perfect Forward Secrecy (PFS): **enabled, group 5**

- With most VPN 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 your end. 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 some kind of probe. For Cisco devices, it's mandatory to configure an SLA monitor for policy-based tunnels as long as the IP address of the edge device is part of the encryption domain.

- Oracle generates, by default, a **key** per tunnel and provides it to you in the Console. You can use it or provide your own.

- Oracle Cloud Infrastructure doesn't support IPSec NAT Traversal ([RFC 3947](#)). This affects only customers who aren't using 1:1 NAT.

After you configure the IPSec tunnel based on our recommendations, the next step is to direct the traffic to the IPSec VPN. Routing and security play an important role in this step. Even if the IPSec VPN is configured correctly and in an UP state on both ends, traffic won't be directed to the IPSec VPN if the routing or security lists are set incorrectly. To ensure that routing and security lists are configured correctly on both the Oracle Cloud and your on-premises network, consider the following recommendations:

- Routing

  o Configure your edge device to ensure that traffic destined for the VCN is pointing to the VPN edge and the correct VPN interface.

  o When using IPSec VPN with static routing, ensure that the route is withdrawn from the route table when the tunnel is down; otherwise, it will not fail over properly.

  o Because each IPSec VPN connection has two tunnels, ensure that traffic can be routed through both tunnels, and give the routes the correct priority.

- Security

  o For your on-premises network, ensure that any firewall in the path isn't blocking any communication with the VCN. This is key for the success of the connection because the firewall could block traffic for tunnel enablement as well as interesting traffic.

  o Each IPSec 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 could use either tunnel to send traffic.

  o 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 PDU used during data transmission.

Following the design principles, Oracle also recommends 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 VPN Connect 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 the Oracle Cloud

In the Oracle Cloud Infrastructure Console, some components must be created and enabled to correctly configure the VPN Connect. This configuration can be done by your cloud administrator or by your network team. For step-by-step instructions, see Overview of Networking.

Consider the following points for a successful deployment:

- Create a dynamic routing gateway (DRG).

- Attach the DRG to your VCN.

- Create a customer-premises equipment (CPE) object.

- Create an IPSec connection.

- Configure routing:

  o You create a CPE object, which includes the public IP address of your edge device. Then within your DRG, you create an IPSec connection that points to the CPE object and specifies your on-premises network subnets. This configuration tells the DRG what connection to use to reach your on-premises network.

  o The VCN in the Oracle Cloud must have a route rule that points to the DRG that is attached to the VCN for any routes destined to your on-premises network. The route rule could be in the default route table or in a subnet route table.

  o 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.

  o Each IPSec VPN connection has two tunnels, and Oracle uses either of them based on availability. The traffic might be asymmetric between Oracle Cloud and your on-premises network. Ensure that the traffic is allowed on your on-premises network for both tunnels.

- Oracle provides two VPN gateways for each IPSec VPN connection. Oracle places the first tunnel to come up 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.

- Configure security:

  - Update the ingress and egress rules in the default security list or in the lists associated with the subnets in your VCN to allow/deny traffic back to your on-premises network.

  - Use security lists to control, at a more granular level, what traffic is allowed between your on-premises network and your VCN.

  - Ensure that both the VCN security lists and the instance firewalls allow ICMP type 3 code 4 messages, which enable Path Maximum Transmission Unit Discovery (PMTUD) to determine the maximum PDU used during data transmission.

Redundancy Testing

Redundancy is one of the design principles for an effective IPSec 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 that all your paths (tunnels and FastConnect) are up.

2. Initiate a continuous ping from your on-premises network to your VCN. Keep this ping running for the duration of the test.

3. Verify that the traffic is taking the primary path by doing a trace route and comparing the results to the design. Note that 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 should fail until the failover to the backup path is completed. For future reference, record how long the failover took.

5. Perform another trace route and compare the results to the results from step 3. The results should be different and should match your design.

6. Enable the primary path by bringing up the tunnel interface or the FastConnect interface. You might see a small number of packets drop as the traffic fails back to the primary path. With VPN Connect, traffic fails back to the primary path if a more-specific subnet is advertised over the primary path and a less-specific 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 should be the same as the result from step 3.

8. The preceding steps verify failover and failback. As an additional step, disable your backup path to verify that doing so doesn't affect anything in the solution. When you do this, 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 path is removed from it when the path isn't available.

Use Cases

This section describes the following typical use cases for connecting from your on-premises network to Oracle Cloud Infrastructure by using VPN Connect over the internet. Routing requirements are provided for each use case.

Note: When you configure VPN Connect in the DRG in the 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 in this section, the VPN gateways are represented as independent components to illustrate the concepts and 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/Dual Customer Edge Device (high availability, medium cost)

- Dual Region, Single/Dual Customer Edge Device (high availability, medium cost)

Single Region, Single Customer Edge Device

This use case is the simplest design for connecting to Oracle Cloud Infrastructure using an VPN Connect over the internet. It consists of one edge device in your on-premises network and two VPN gateways (default) in a single Oracle Cloud region. The edge device could be located 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 the Oracle Cloud from your on-premises network.
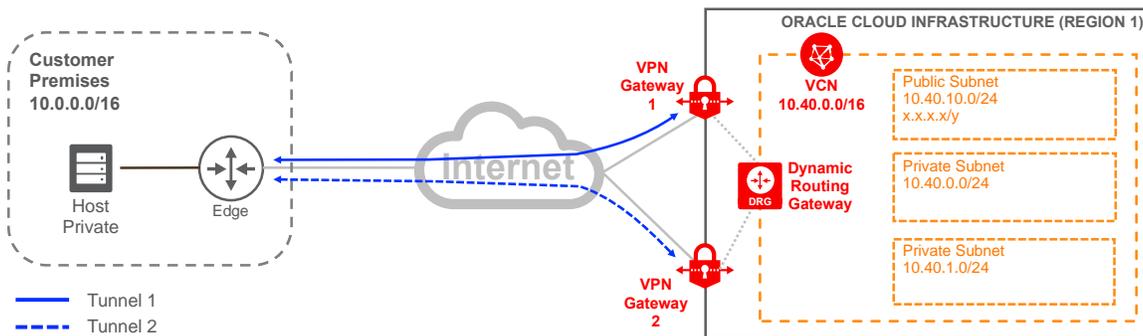
Figure 2. VPN Connect for a Single Region with a Single Customer Edge Device

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 via the two tunnel interfaces. We recommend that you give priority to one of the tunnels. Oracle uses asymmetric routing across the two tunnels that make up the IPSec 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" on your device. As a result, you could send traffic from your on-premises network to Oracle Cloud via one tunnel while Oracle might send traffic to your on-premises network via a different tunnel.
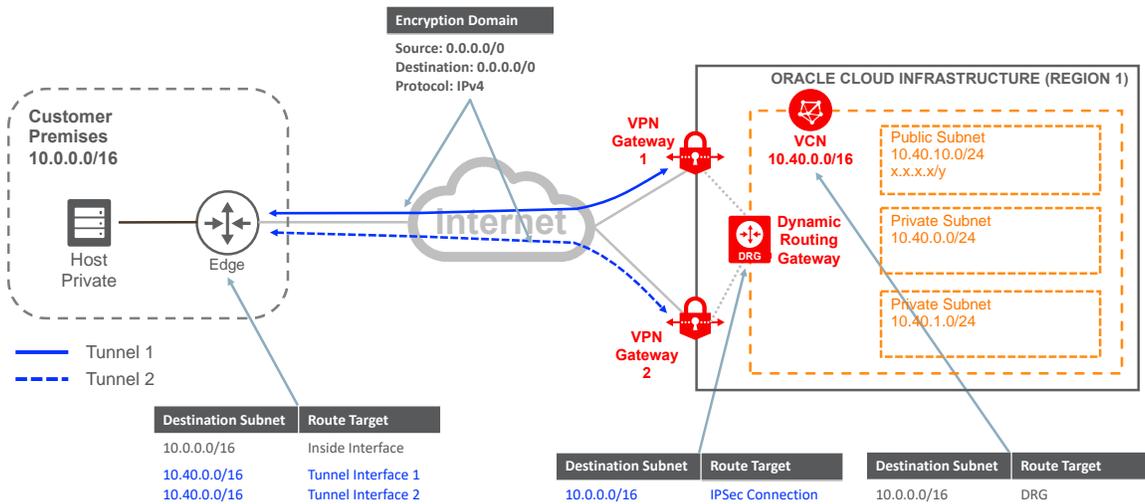
Encryption Domain

Source: 0.0.0.0/0
Destination: 0.0.0.0/0
Protocol: IPv4

Customer Premises
10.0.0.0/16

Host Private

Edge

Tunnel 1
Tunnel 2

ORACLE CLOUD INFRASTRUCTURE (REGION 1)

VCN 10.40.0.0/16

VPN Gateway 1

VPN Gateway 2

Dynamic Routing Gateway

Public Subnet
10.40.10.0/24
x.x.x.x/y

Private Subnet
10.40.0.0/24

Private Subnet
10.40.1.0/24

Destination Subnet	Route Target
10.0.0.0/16	Inside Interface
10.40.0.0/16	Tunnel Interface 1
10.40.0.0/16	Tunnel Interface 2

Destination Subnet	Route Target
10.0.0.0/16	IPSec Connection

Destination Subnet	Route Target
10.0.0.0/16	DRG

Figure 3. Routing for IPSec VPN for a Single Region and a Single Customer Edge Device

When you create the IPSec connection, include all the subnets located on your on-premises network. Or, to avoid changing them, you can include a supernet that covers all your on-premises networks if using static routing, or use BGP to advertise them dynamically. It's important to note that the subnets for your on-premises networks are *not* entered in a route table assigned to the DRG; they are entered when you create the IPSec connection.

Security lists must also be updated accordingly. However, this document focuses more on the network because security depends on the different types of applications and traffic that you want to allow through this connection. You need to modify the security lists at the same points in the network as the routing. As recommended, Figure 3 also shows that both tunnels use the same single encryption domain.

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: your edge device. To correct this issue, deploy a redundant edge device. This device can be 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 via 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 of your edge devices. As a result, you will have four tunnels, two tunnels per edge device, as represented by the red and blue lines in Figure 4. Also shown in Figure 4, Oracle provides diverse VPN gateways per IPSec VPN connection to both edge devices.
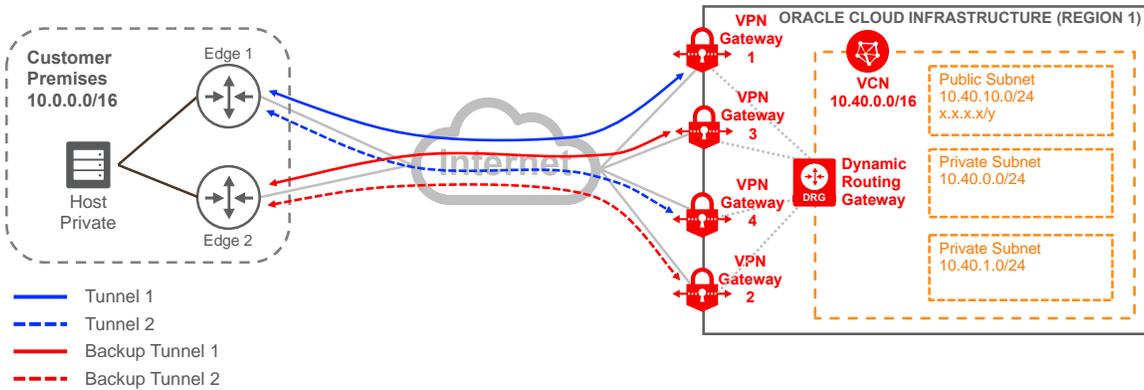

Figure 4. VPN Connect for a Single Region with Redundant Customer Edge Devices

As long as 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 red line) is removed from edge device 2. Oracle still provides the VPN gateways and accepts the connection if you configure it. 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.
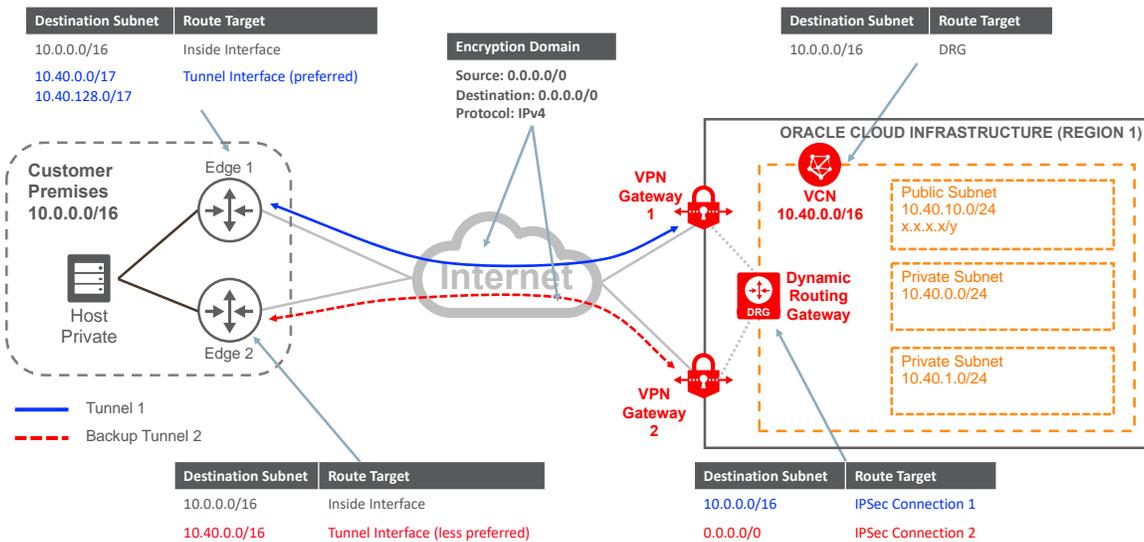
Figure 5. Routing and Encryption Domain for VPN Connect for a Single Region with Redundant Customer Edge Devices

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 symmetric. If the primary path fails, there is still a less specific route 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, you should influence traffic to take the primary path (blue) based on your internal routing protocol because both edge devices will advertise the same VCN subnet. From the Oracle end, you advertise your on-premises network for the primary path and advertise the default route via the backup (red) path. Figure 5 reflects the advertisement of more specific subnets. 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 should be encrypted and placed into the tunnel. In Figure 5, note that 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 subnets.

FastConnect Plus Single Region, Single Customer Edge Device VPN

If you need better performance in your connectivity to the cloud, you might need to upgrade your connection by deploying a FastConnect solution to Oracle Cloud. This could be the case if your current edge device can't support required new bandwidth or you need a more reliable connection. You can continue to use the VPN Connect, but instead of using it as your primary connection, you use it as a backup, as illustrated in Figure 6.

FastConnect doesn't use the internet. Instead, it uses private circuits via Oracle partners, third-party providers, or cross-connects if your data center is collocated at an Oracle FastConnect data center. To avoid a single point of failure, deploy FastConnect and VPN Connect from different edge devices in your network. When you use FastConnect, you need to create a virtual circuit (VC) between your on-premises network and the Oracle Cloud, as represented by the top (green) line in Figure 6.
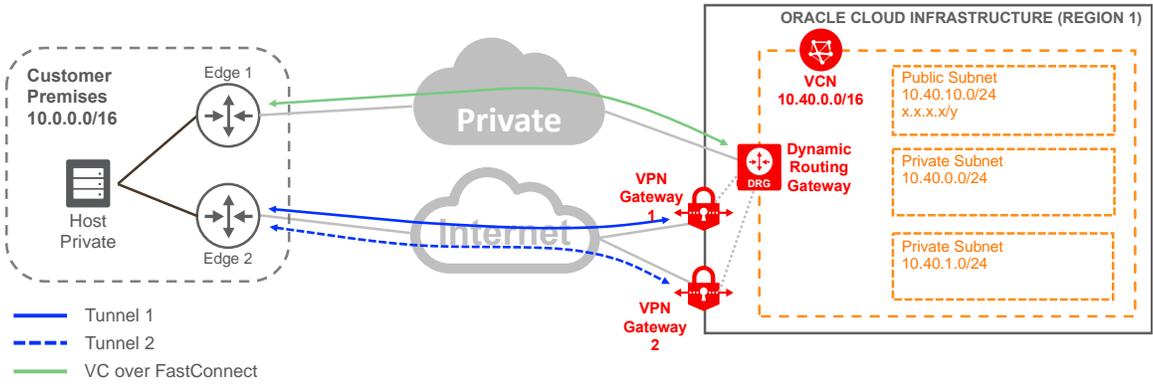
Figure 6. FastConnect Plus a Single Region and a Single Customer Edge Device VPN

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 (VPN Connect). The DRG learns your on-premises subnets via 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 CPE object associated with the IPSec connection, or could use BGP to learn your on-premises routes dynamically via the IPSec connection. On your end of the connection, you advertise to your network the VCN's subnets learned via BGP over FastConnect while advertising a less specific route through the IPSec VPN connection. If it's not possible to advertise the default route via the IPSec 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 show the routing for this use case.
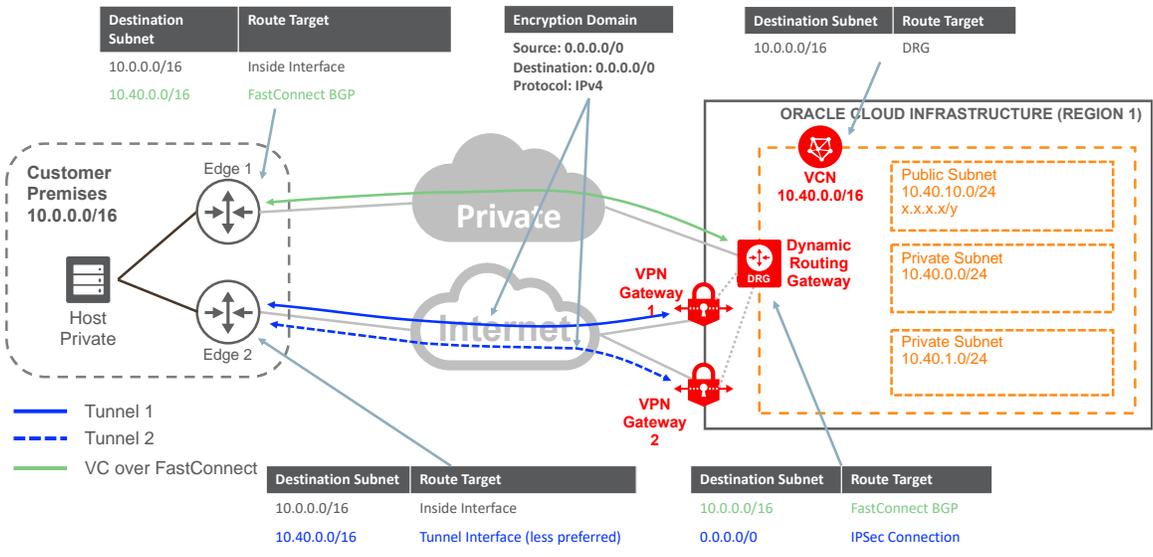
Figure 7. Routing for FastConnect Plus a Single Region and a Single Customer Edge Device VPN

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

Cloud deployment 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 an IPSec VPN to connect to a single Oracle Cloud region that hosts multiple VCNs. After you are connected, you configure a local peering gateway (LPG) to interconnect your VCNs.

This solution uses a hub-and-spoke approach in which the hub is the VCN that has a DRG attached with the IPSec connection, and the spokes connect to the hub via the LPG. For more information, see Local VCN Peering (Within Region). If traffic doesn't need to flow between the VCNs, you can create a separate IPSec VPN connection to each VCN if the Oracle VPN gateways are different for each VCN. Figure 8 shows the high-level design of connecting multiple VCNs via VPN Connect.
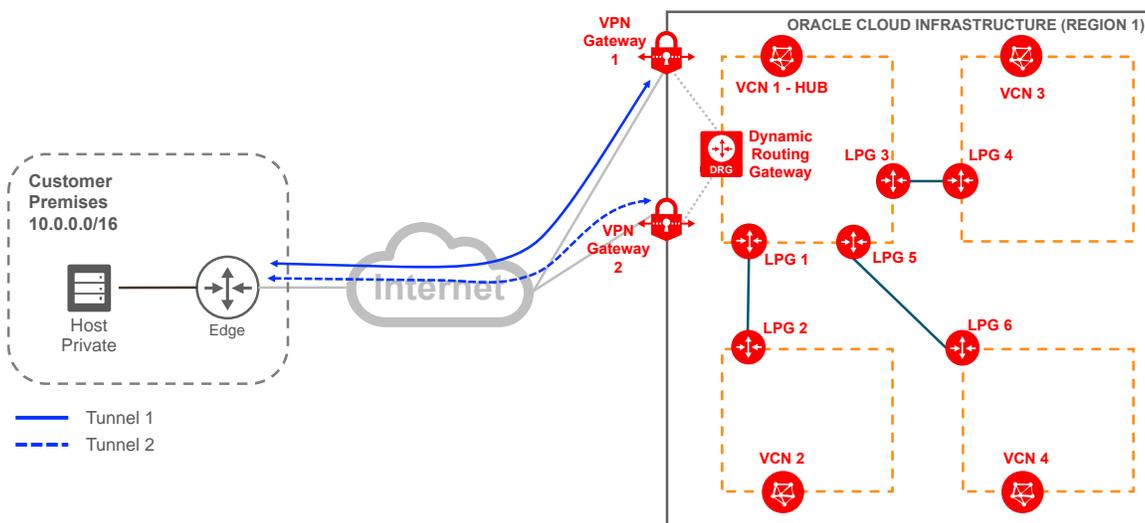
Figure 8. VPN Connect for the Same Region with Multiple VCNs—High-Level Design

This example uses only two VCNs (see Figure 9), 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.
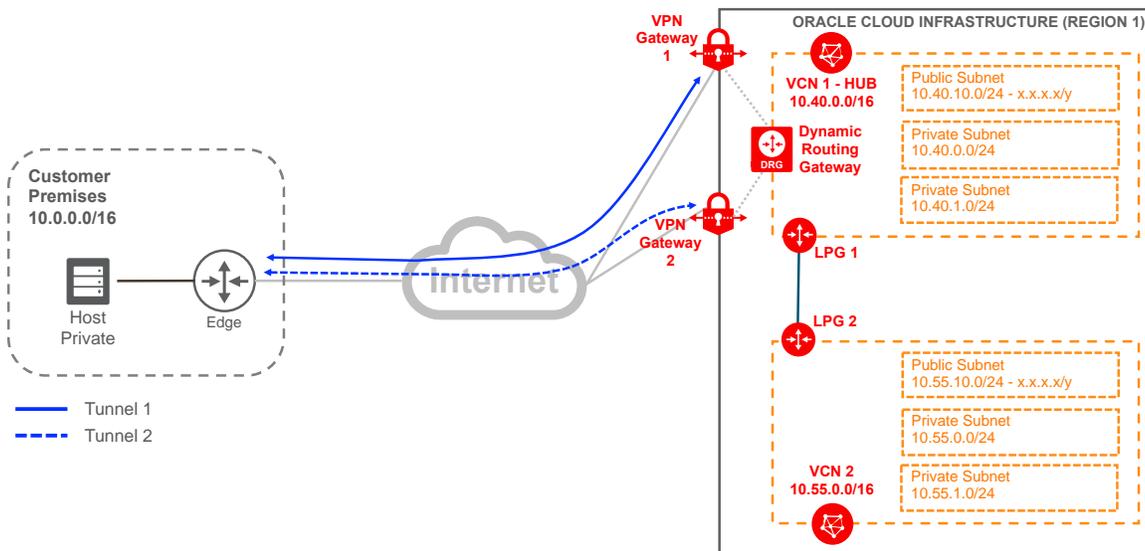
Figure 9. VPN Connect for the Same Region with Multiple VCNs with a Single Customer Edge Device

This use case has more routing changes than the previous use cases. On your end of the connection, you 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). When an LPG is created, by default it has a route to the peered VCN. In the Oracle Console, after you create the LPGs in each VCN and establish the relationship, you need to add more routes to various components. These routes allow traffic to flow end-to-end in both directions. The following list shows what you need to add, and it's represented in Figure 10:

- After the DRG is attached to a VCN, you can associate a route table with the DRG. You need a route for your second VCN that points to LPG 1.

- VCN 1 subnets need a route for your on-premises network that points to the DRG and a route to VCN 2 that points to LPG 1.

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

- LPG 1 needs a route to reach your on-premises network for traffic coming from VCN 2 that points to the DRG.
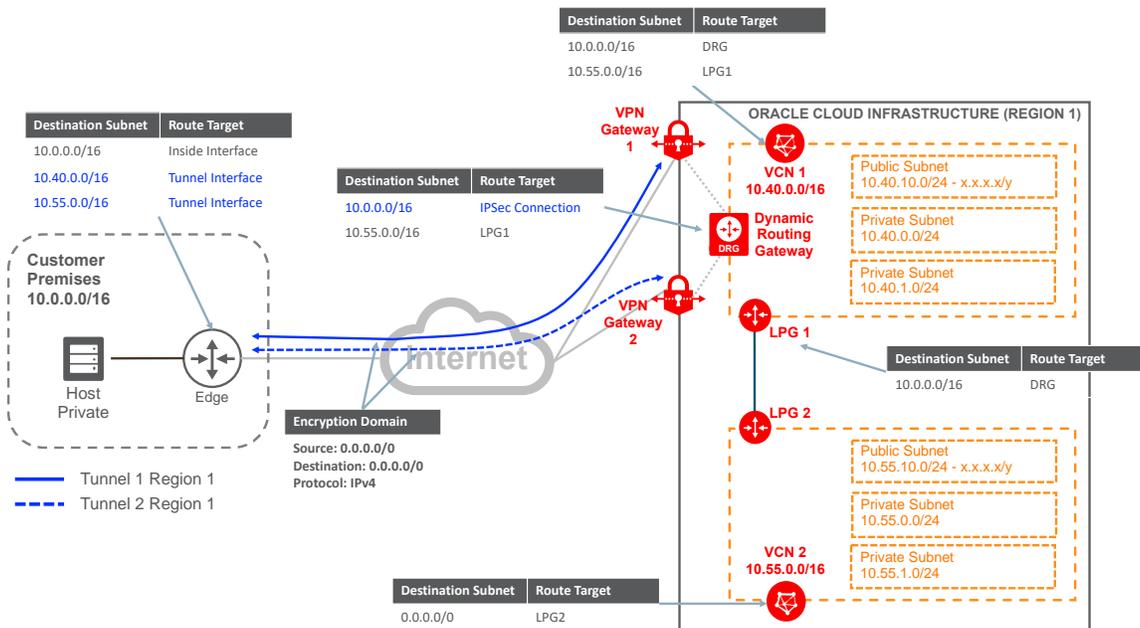
Figure 10. Routing for VPN Connect for the Same Region with Multiple VCNs with a Single Customer Edge Device

Dual Region, Single/Dual Customer Edge Device

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

From your on-premises network, you are *not* allowed to connect to one region and then jump to other regions using a region as a transit network. You can't have one tunnel terminating in one region backed up by another tunnel or FastConnect terminating in a different region. 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 Console, you can set up an RPC in your DRG as shown in Figure 11. Only resources in the VCNs can use the RPC. 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.
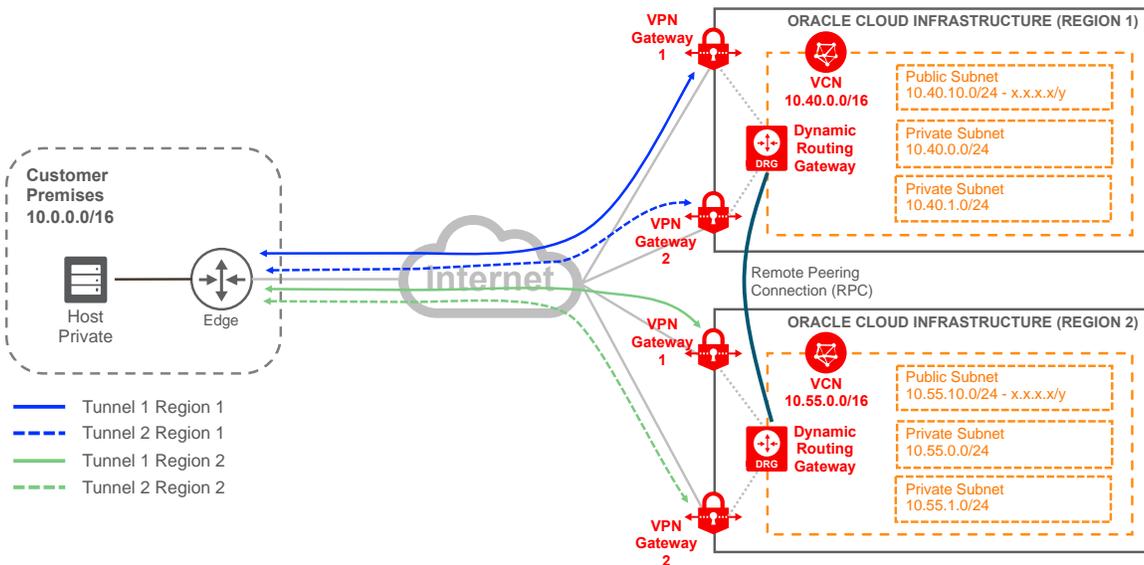
Figure 11. VPN Connect for Dual Regions with a Single Customer Edge Device

The routing for this use case is the same as for the first use case for VPN Connect; 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, as indicated in Figure 12.
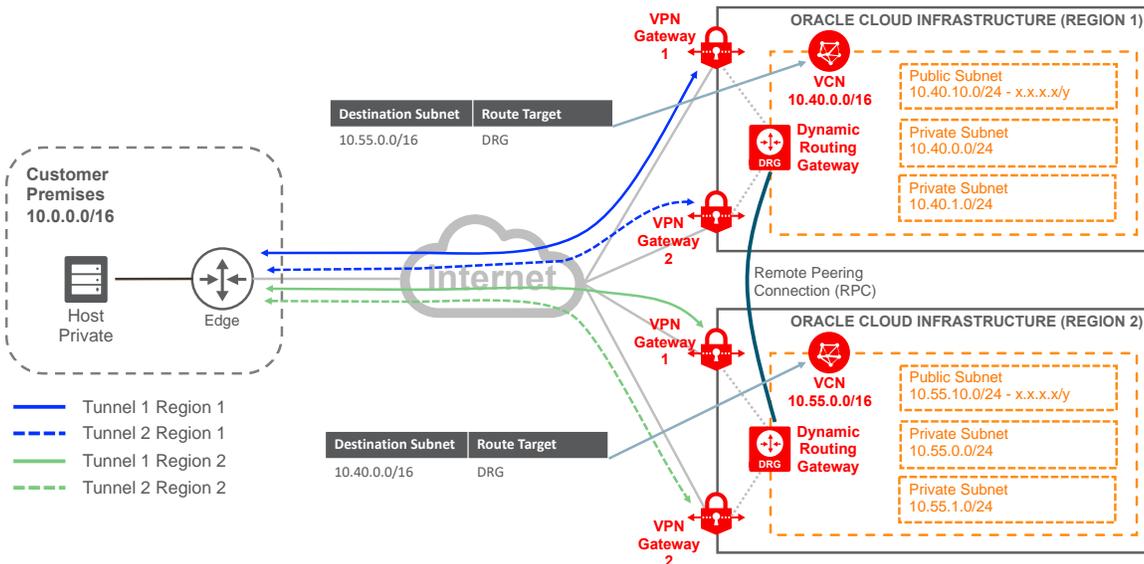

Figure 12. VPN Connect for Dual Regions with a Single Customer Edge Device Routing

References

- For more information about the VPN Connect in Oracle Cloud Infrastructure, see VPN Connect.

- 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.

ORACLE®

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services

IPSec VPN Best Practices
May 2019
Author: Oracle Corporation

Oracle is committed to developing practices and products that help protect the environment