Deploying VPN IPSec Tunnels with Cisco ASA/ASAv VTI on Oracle Cloud Infrastructure

Table of Contents

Overview

This guide provides step-by-step instructions for configuring VPN IPSec tunnels on Oracle Cloud Infrastructure. It is helpful to know the basics of networking before following the steps outlined in this solution guide. Working with the on-premises network or security engineers is often required when setting up VPN, IPSec, and FastConnect services.

This guide helps operators to complete all the necessary steps on Oracle Cloud Infrastructure and to configure the Cisco Adaptive Security Appliance/ Adaptive Security Virtual Appliance (ASA/ASAv) device to create an IPSec connection to an Oracle Cloud Infrastructure virtual cloud network (VCN).

Scope and Assumptions

This guide is a quickstart guide for deploying VPN IPSec tunnels to connect from an on-premises network to Oracle Cloud Infrastructure. It outlines some best practices and should not be used as a full reference guide to IPSec tunnels. Identity Access Management (IAM) on Oracle Cloud Infrastructure is beyond the scope of this document. Cloud, Network, Virtualization, Server, and On-Premises IT administrators and operators should all be able to use this guide to assist in creating IPSec connections to Oracle Cloud Infrastructure.

This guide covers the configuration of the Cisco ASA device with an IPSec connection via the Virtual Tunnel Interface (VTI). It works for both the hardware-based ASA firewall devices and the virtual ASA (ASAv) that can run on KVM, Hyper-V, or ESXi hypervisors. The steps in this guide require ASA/ASAv software release 9.7.1 or later.

An important prerequisite for setting up IPSec tunnels with Oracle Cloud Infrastructure is that the on-premises devices (called *customer-premises equipment* or *CPE*) must not be behind a NAT. Neither 1:1 NAT nor port-forwarding works in the current implementation of Oracle Cloud Infrastructure IPSec on the dynamic routing gateway (DRG).

The guide assumes that the required privileges are properly assigned to manage network components (such as the virtual cloud network, subnet, dynamic routing gateway, and internet gateway) in the compartment that you want to work in.

Readers of this guide should first be familiar with the fundamentals of the Oracle Cloud Infrastructure. See the following resources for information:

- Oracle Cloud Infrastructure product web page
- Oracle Cloud Infrastructure Getting Started guide

Readers should also be familiar with the basics of Cisco ASA/ASAv. See the following resources for information:

- [Quick Start](#)

- [Command References](#)

- [General Operations Configuration Guide](#)

- [Firewall Configuration Guide](#)

- [VPN Configuration Guide](#)

VPN IPSec Tunnel Concepts

IPSec (short for *Internet Protocol Security*, or *IP Security*) is a protocol suite that encrypts the entire IP traffic before the packets are transferred from the source node to the destination. IPSec can be configured in two modes, transport and tunnel. Tunnel mode is used for both VTI and classic IPSec (crypto maps). In tunnel mode, IPSec encrypts or authenticates the entire packet. After encryption, the packet is then encapsulated to form a new IP packet that has different header information.

IPSec VPN site-to-site tunnels offer the following advantages:

- Public telecommunication lines are used to transmit data, so dedicated, expensive lease lines from one site to another aren't necessary.

- The internal IP addresses of the participating networks and nodes are hidden from external users.

- The entire communication between the source and destination sites is encrypted, significantly lowering the chances of information theft.

Oracle Cloud Infrastructure supports only the tunnel mode of VPN IPSec. It is offered as self-service by using either the Console or the REST APIs.

CPE Configuration

The four main steps for configuring the customer-premises equipment (CPE) are as follows:

- IKE security association, which is required to exchange keys used to establish the IPSec association

- IPSec security association, which handles the tunnel encryption, authentication, and so on

- Tunnel interface, which receives traffic going to and from the tunnel

- Routing, which deals with setting up routes between on-premises networks and networks in the cloud

General Requirements for Connecting to the Oracle Cloud Infrastructure DRG via IPSec

The following requirements must be met in order to connect the on-premises network to Oracle Cloud Infrastructure.

Establish the IKE Security Association Using Pre-Shared Keys

The IKE security association (SA) is established first between the virtual private gateway and the CPE by using the pre-shared key as the authenticator. Upon establishment, IKE negotiates an ephemeral key to secure future IKE messages. Proper establishment of an IKE SA requires complete agreement among the parameters, including encryption and authentication parameters. When an IPSec connection is created, a pre-shared key is generated.

To show IKE associations on the ASA/ASAv device, run `show crypto ikev1 sa`.

Establish the IPSec Security Association

Using the IKE ephemeral key, keys are established between the DRG and the CPE to form an IPSec security association (SA). Traffic between gateways is encrypted and decrypted using this SA. The ephemeral keys used to encrypt traffic within the IPSec SA are automatically rotated by IKE on a regular basis to ensure confidentiality of communications.

To show the IPSec state and tunnel on the ASA/ASAv device, run `show crypto ipsec sa`.

Use AES 256-Bit Encryption

The encryption function is used to ensure privacy among the IKE and IPSec SAs.

To verify AES-256, run `show crypto ipsec sa | include peer|transform` (no space on either side of the second pipe | symbol).

Use the SHA-1 or SHA-256 Hashing Function

The SHA-1 or SHA-256 hashing function is used to authenticate both the IKE and IPSec SAs.

Run `show crypto ipsec sa | include peer|transform` (no space on either side of the second pipe | symbol).

Use Diffie-Hellman with Perfect Forward Secrecy

IKE uses Diffie-Hellman to establish ephemeral keys to secure all communication between CPEs and virtual private gateways (Phase 1 group: 5, Phase 2 group: 5).

To see what ASA/ASAv has configured for the peers, run `show crypto ipsec sa | include peer|settings` (no space on either side of the second pipe | symbol).

IPSec Dead Peer Detection

The use of Dead Peer Detection (DPD) enables the VPN devices to rapidly identify when a network condition prevents delivery of packets across the internet. When this occurs, the gateways delete the security associations and attempt to create new associations. During this process, the alternate IPSec tunnel is used, if possible. The default DPD threshold for L2L IPSec tunnels is 10 seconds with a retry count of 2.

```
config t
tunnel group 129.213.6.54 ipsec-attributes
(config-tunnel-ipsec) # isakmp keepalive threshold 10 retry 2
```

Do not disable DPD on the L2L tunnel. The Oracle Cloud Infrastructure headend will respond to these keepalive checks. If the peer does not respond with the R-U-THERE-ACK message, the ASA device starts retransmitting R-U-THERE messages, every `<retry-interval>` seconds with a maximum of three retransmissions until the peer is declared dead.

Bind Tunnel to Logical Interface (Route-Based VPN)

The gateway must support the ability to bind the IPSec tunnel to a logical interface. This is the whole premise of Virtual Tunnel Interface (VTI). The logical interface contains an IP address used to establish peering to the DRG. This logical interface should perform no additional encapsulation (for example, GRE, IP in IP). Your interface should be set to a 1300 byte Maximum Transmission Unit (MTU).

A 1300-byte packet creates a 1368-byte packet after IPSec is added with AES-256 and SHA-1:

- 20 bytes IPSec header (tunnel mode)

- 4 bytes SPI (ESP header)

- 4 bytes Sequence (ESP Header)

- 16 byte IV (IOS ESP-AES)

- --- 1300 payload size

- 10-byte pad (ESP-AES 128 bit)

- 1-byte Pad length (ESP Trailer)

- 1-byte Next Header (ESP Trailer)

- 12 bytes ESP SHA 96 digest

1300 should leave 10-11 bytes free.

The ASA/ASAv device doesn't behave like a router. It automatically sets the VTI/Tunnel Interface MTU based on the underlying physical interface and IPSec overhead. This can be seen and validated with by running `show crypto ipsec sa | include peer|mtu`.

If there are MTU-related issues, the tunnel MTU can be changed by modifying the interface MTU (outside): `(config) # mtu outside 1300`. Don't do this unless there are MTU-related issues.

Fragment IP Packets Before Encryption

When packets are too large to be transmitted, they must be fragmented. Fragmented encrypted packets aren't reassembled. The VPN device must fragment packets before encapsulating with the VPN headers. The fragments are individually transmitted to the remote host, which reassembles them. This is default behavior on ASA/ASAv.

To do this, run `show crypto ipsec fragmentation outside`.

Recommendations for TCP Maximum Segment Size and DF Flags

Use the following recommendations for the TCP Maximum Segment Size parameter and Don't Fragment (DF) flags.

Adjust the Maximum Segment Size of TCP Packets in the Tunnel

TCP packets are often the most prevalent type of packet across IPSec tunnels. Some gateways have the ability to change the TCP Maximum Segment Size parameter, which causes the TCP endpoints (clients, servers) to reduce the amount of data sent with each packet. This is an ideal approach because the packets arriving at the VPN devices are small enough to be encapsulated and transmitted.

The default of the ASA/ASAv device is set to 1380. Run `show running-config all sysopt` and look for `sysopt connection tcpmss 1380`. You should not need to change this global parameter unless there are fragmentation issues.

Copy (Respect) the "Don't Fragment" Flag on Packets

Some packets carry a flag known as Don't Fragment (DF) that indicates that the packet should not be fragmented. If a packet carries that flag, the gateways generate an ICMP Path MTU Exceeded message. In some cases, applications don't contain adequate mechanisms for processing these ICMP messages and reducing the amount of data transmitted in each packet. Some VPN devices have the ability to override the DF flag and fragment packets unconditionally as required.

The "DF bit with IPSec tunnels" feature lets you specify whether the security appliance can clear, set, or copy the DF bit from the encapsulated header. The DF bit within the IP header determines whether a device is allowed to fragment a packet.

Use the `crypto ipsec df-bit` command in global configuration mode to configure the security appliance to specify the DF bit in an encapsulated header.

When you encapsulate tunnel mode IPSec traffic, use the `copy-df` setting for the DF bit. This setting lets the device send packets larger than the available MTU size. In addition, this setting is appropriate if you don't know the available MTU size.

Cisco recommends copy (respect) the DF bit by default. If there are issues related to MTU and DF, change the MTU of the outside interface (interface carrying the VTI tunnels) before adjusting this setting.

To see the current `df-bit` setting, run `show crypto ipsec df-bit outside`.

Data Lifetime Rekey Interval

Data lifetime rekeys are generally considered vestigial and are generally exceeded long before time-based rekeys occur. The best practice is to disable tracking of data lifetime rekeys on IPSec tunnels. This setting is only visible in `show crypto ipsec sa | include peer|lifetime` when a data lifetime counter exists. This can be set with:

```
(config) # crypto ipsec security-association lifetime kilobytes unlimited
```

VPN IPSec Tunnels on Oracle Cloud Infrastructure

An IPSec VPN provides a connection between a customer's on-premises network and an Oracle Cloud Infrastructure virtual cloud network (VCN). It consists of multiple redundant IPSec tunnels that use static routes to route traffic.

IPSec tunnels connect a dynamic routing gateway (DRG) and customer-premises equipment (CPE) that are created and attached to the VCN. By default, three IPSec tunnels, one per

availability domain, are created on Oracle Cloud Infrastructure. This provides redundancy in case of tunnel failures. Oracle recommends configuring the on-premises router to support all of the IPSec tunnels in case one of the tunnels fails. Each tunnel has configuration information (that is, an Oracle Cloud Infrastructure DRG-external IP address and pre-shared key for authentication) that are configured on the on-premises router.

It is possible to scale to a large number of tunnels against a single DRG. Configurations have been done with over 40 tunnels against a single DRG.

The limit of the number of tunnels from a single CPE device is eight. If more than eight IPSec tunnels per CPE are required, an additional public IP address can be used. For a given VCN, there is a possibility of having one DRG instance.

When scaling with IPSec, the use of Oracle Cloud Infrastructure FastConnect should always be considered after a certain point, which varies on a case-by-case basis.

This guide explains how to configure VPN IPSec tunnels from on-premises to Oracle Cloud Infrastructure data centers using the web console. You can also use the REST APIs to perform the same steps. For more information about the API, see https://docs.us-phoenix-1.oraclecloud.com/api/.

Key Components of VPN IPSec Tunnels on OCI

When you set up an IPSec VPN for your VCN, you must create several Networking components. You can create the components by using either the Console or the API. See the following descriptions of the components.

Oracle Cloud Identifier (OCID)

A unique name assigned to every resource provisioned on Oracle Cloud Infrastructure. The OCID is an autogenerated long string and it is used by Support Engineers to identify cloud resources when you are working with Support. OCIDs are also used extensively when working with REST APIs, Orchestration services (Terraform), and SDKs.

Cloud Resource

Anything provisioned on a cloud platform. In Oracle Cloud Infrastructure, it can be a VCN, a Compute instance, a user, a compartment, a database, a load balancer, or any other service component on the platform.

On-Premises

A widely used term in cloud technologies that refers to traditional data center environments. It includes any colocation, dedicated floor space, dedicated data center buildings, and servers located locally at a customer data center.

Customer-Premises Equipment (CPE)

A virtual representation of an on-premises VPN router (hardware or software). The CPE object contains basic information (for example, IP address) about the on-premises VPN router that is used by the VCN for routing private traffic. In this example, the CPE is the virtual IP or IP address of the outside interface for the Cisco ASA or ASAv device.

Virtual Cloud Network (VCN)

Also called a *cloud network*. A software-defined network that is set up on the Oracle Cloud Infrastructure platform. Think of a VCN as an extension of local or on-premises networks to the cloud, with firewall rules and specific types of communication gateways. A VCN covers a single contiguous CIDR (range of IP addresses) block, which is configurable. VCNs are regional resources; they cover all of the availability domains within a region.

Oracle Cloud Infrastructure VCN supports VCN size ranges of /16 to /30, and this can't be changed after a VCN is created. The VCN's CIDR must not overlap with the on-premises network. It is important to lay out the appropriate VCN networks with the on-premises network team to get an available range of IP addresses (CIDR) that can be used with the VCN when moving past the proof-of-concept phase.

Subnet

A subdivision of a virtual cloud network (VCN). A subnet is specific to an availability domain. In order to start a database system, a VM, a bare-metal instance, or a load balancer in Oracle Cloud Infrastructure, the VCN must have at least one subnet. A subnet consists of a contiguous range of IP addresses that don't overlap with other subnets within the same VCN.

Subnets have virtual network interface cards (VNIC) that attach to instances. Subnets can be labeled as private when they are created, which means resources in the subnet can't have a public IP address; some other method of accessing external networks must be used for private subnets such as bastion hosts, load balancers, NAT hosts, or DRG connections that use IPSec tunnels or FastConnect.

A subnet is associated with security lists, route tables, and DHCP options to control what traffic is allowed to flow in which direction (DRG or IG for public/private traffic). Security lists and route table

attachments can't be changed after a subnet is built. The security list rules and route table entries can be changed after subnet creation.

Virtual Network Interface Card (VNIC)

Resides in a subnet and gets attached to an instance to enable connections to the subnet's VCN. Each instance has a default primary VNIC that is created during instance launch and can't be removed. Secondary VNICs can be added to an existing instance if required.

Dynamic Routing Gateway (DRG)

A virtual router that provides a path for private traffic between the Oracle Cloud Infrastructure VCN and the on-premises (data center) network. A DRG is a standalone resource on Oracle Cloud Infrastructure and is designed to give full flexibility to attach to and detach from different VCNs. A DRG is required for both VPN IPSec tunnels and FastConnect circuits. A network administrator might think of the DRG as the VPN headend on their Oracle Cloud Infrastructure services.

Internet Gateway (IG)

An optional virtual router that adds internet connectivity to a VCN. It provides internet access to the VCN and is controlled by the route tables and security list configuration on the subnet level. In addition to an internet gateway, the following items must be configuring before resources can access the internet via the subnet:

- Route rule in the route table that points to the internet gateway.

- Appropriate port open in a security list. For example, egress allowed, port 80/443 must be open for web server traffic.

- A subnet that permits public IP address assignments to hosts. In addition to being a public subnet, the instance must be configured for public IP on creation.

Note: Having an internet gateway alone does not expose the subnet to the internet unless the preceding conditions are satisfied. Access to the internet can also be obtained via IPSec VPNs on an Oracle Cloud Infrastructure DRG rather than through the internet gateway. In this example, the Oracle Cloud Infrastructure resources use the internet gateway for all networks other than the VCN network and the on-premises networks connected via the VPN.

Security Lists

Virtual firewall rules for the VCN and subnets on Oracle Cloud Infrastructure. These security lists consist of ingress and egress rules that specify the destination (CIDR) and type of traffic (protocol

and port) allowed in and out of instances within a subnet. A security list is attached to the subnet when it is created. Security lists can be modified dynamically.

Example: An ingress security rule in security lists with source CIDR 10.100.0.0/16 with destination port 22 of TCP protocol allows all ingress traffic from on-premises IP addresses (10.100.0.0/16) to Oracle Cloud Infrastructure instances on port 22 for SSH connection.

Route Tables

Virtual route tables where NAT instances, DRGs, or IGs are the targets. The route table rules provide mapping for the traffic from subnets via gateways to a destination outside the VCN (for example, private traffic flows using a DRG and public traffic flows using an IG). The default route table can be used within the VCN or multiple route tables can be created and associated with one or more subnets.

A route table must be assigned to a subnet within a VCN. The default route table is used when a subnet is created and no route table is specified. Route tables associated with a subnet can't be changed after creation but the route rules can change at any time.

Access Requirements for VPN IPSec Tunnels Configuration

To manage VPN IPSec tunnels on Oracle Cloud Infrastructure, operators must have been granted full access to Network components within a given compartment. As an example, the following policy statement must be attached to the target compartment. In this example, a user that belongs to GroupNetworkAdmin can manage all networking components within CompatmentA:

```
allow group GroupNetworkAdmin to manage virtual-network-family in compartment
CompartmentA
```

The user must be member of the `GroupNetworkAdmin` user group, and `CompartmentA` is the compartment where the VPN IPSec tunnels and related network components (VCN, subnet, and so on) will be created. `in compartment CompartmentA` could also be `in TENANCY`.

Network administrators should have at least read-only access to the tenancy so they can assist in configuring the IPSec tunnel. For example:

```
allow group GroupNetworkAdmin to read virtual-network-family in TENANCY
```

More information about how policies work and how to construct policies is provided at
https://docs.us-phoenix-1.oraclecloud.com/Content/Identity/Concepts/overview.htm.

Configure the VPN IPSec

The following diagram shows the components required to build VPN IPSec connectivity from on-premises to Oracle Cloud Infrastructure. The rest of the guide provides the steps required to build each component in this diagram. The CPE IP address is the IP address or virtual IP address on the outside interface on the ASA/ASAv device. This cannot be 1:1 NAT or port-forwarded to the IPSec peer; it must be untranslated.

For the on-premises side, the subnet or subnets that will be connecting to the Oracle Cloud Infrastructure VCN must be provided. In this case, the on-premises networks are a larger 10.100.0.0/16 network and specific 10.100.6.0 subnet, which will be configured on the inside interface of the ASA/ASAv device.

The ASA/ASAv outside interface, seen in the diagram as 147.75.91.84, must also be provided. This interface will be the one used to build the tunnels to Oracle Cloud Infrastructure.
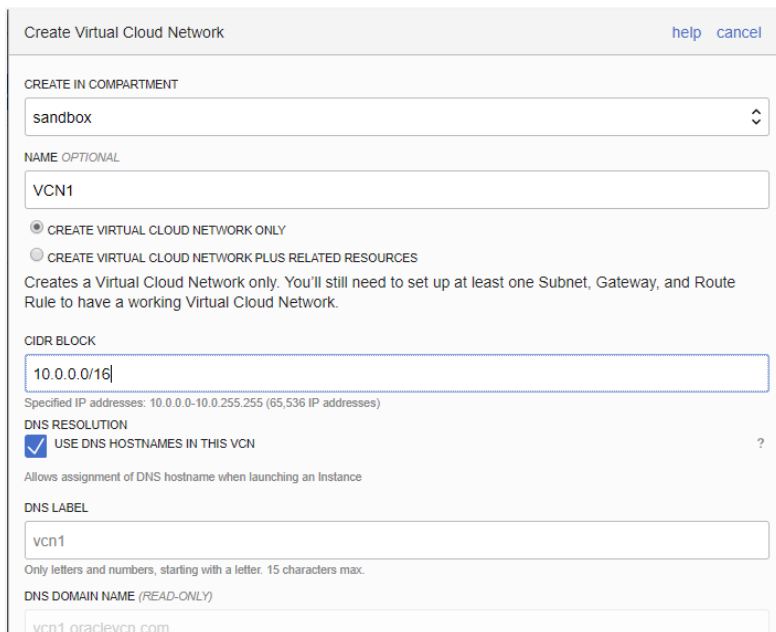
IPSec VTI is limited to sVTI IPv4 over IPv4 using IKEv1 in single-context, routed mode with ASA/ASAv version 9.7.1 or later.
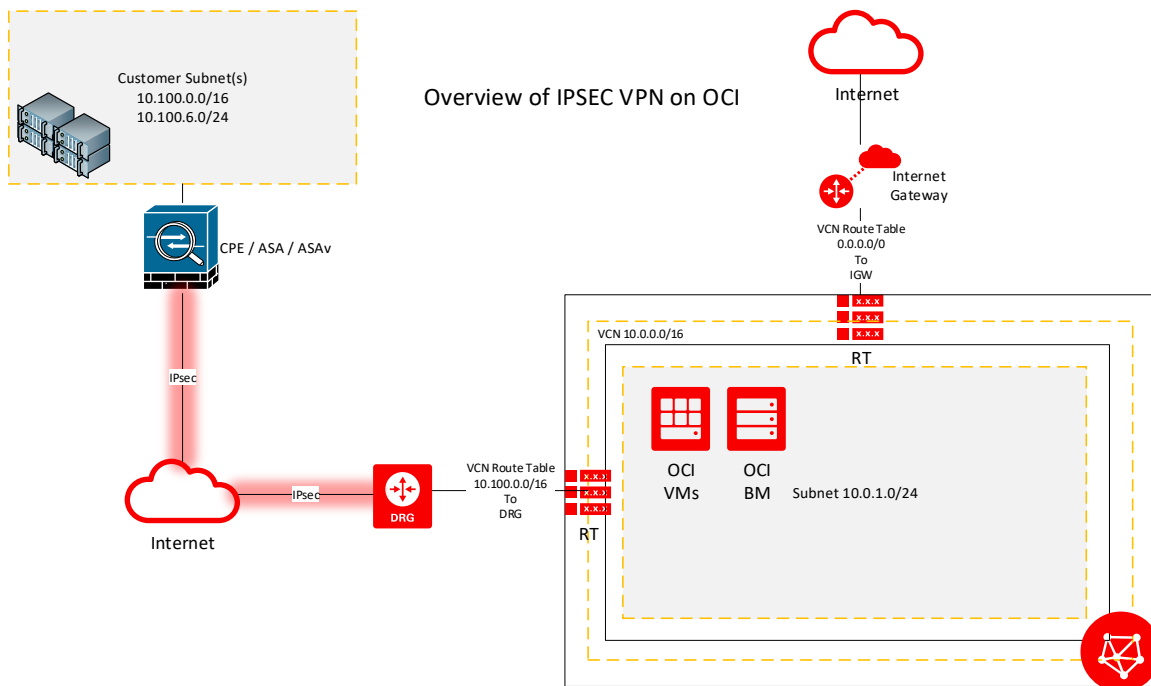
Step 1: Create a VCN

To facilitate IPSec connections, you must create various networking resources on Oracle Cloud Infrastructure. The first resource is a VCN.

1. In the Oracle Cloud Infrastructure Console, click **Networking**.

2. On the left side of the page, choose a compartment you have permission to work in. The page updates to display only the resources in that compartment.

3. Click Create **Virtual Cloud Network**.

4. Enter the following values:

    *   **Create in Compartment:** Leave as is.

    *   **Name:** A descriptive name for the cloud network. It doesn't have to be unique, and it can't be changed later in the Console (but you can change it with the API). Avoid entering confidential information.

    *   **Create Virtual Cloud Network Only:** Select this option.

    *   **CIDR Block:** A single, contiguous CIDR block for the cloud network. For example, 10.0.0.0/16. You can't change this value later.

5. You can provide values for the rest of the options, or you can ignore them:

- **Use DNS Hostnames in this VCN:** If you want the instances in the VCN to have DNS hostnames (which can be used with the **Internet and VCN Resolver**, a built-in DNS capability in the VCN), select this check box. Then you can specify a DNS label for the VCN, or the Console will generate one for you. The dialog box automatically displays the corresponding **DNS Domain Name** for the VCN (`<VCN DNS label>.oraclevcn.com`).

- **Tags:** Optionally, you can apply tags. If you have permissions to create a resource, you also have permissions to apply free-form tags to that resource. To apply a defined tag, you must have permissions to use the tag namespace.

6. Click **Create Virtual Cloud Network**.

The VCN is created and displayed on the page. Ensure that it's done being provisioned before continuing.

Step 2: Create the DRG

1. Click **Networking**, and then click **Dynamic Routing Gateways**.

2. Click **Create Dynamic Routing Gateway**.

3. Enter the following values:

- **Create in Compartment:** Leave as is (the VCN's compartment).

- **Name:** A descriptive name for the DRG. It doesn't have to be unique, and it can't be changed later in the Console (but you can change it with the API). Avoid entering confidential information.

4. Click **Create Dynamic Routing Gateway**.

The DRG is created and displayed on the page. Ensure that it's done being provisioned before continuing.

Step 3: Attach the DRG to the VCN

1. Click the name of the DRG that you just created (DRG1).

2. On the left side of the page, click **Virtual Cloud Networks**.

3. Click **Attach to Virtual Cloud Network**.

4. Select the VCN that you created earlier (VCN1), and then click **Attach to Virtual Cloud Network**.

The attachment will be in the Attaching state for a short period before it's ready.

Step 4: Modify the Default Route Table for the VCN

Edit the default route table that will be used by the subnet.

1. Click **Networking**, click **Virtual Cloud Networks**, and then click the name of your VCN.

2. Click **Route Tables** to see your VCN's route tables.

3. Click the name of the default route table (Default Route Table for VCN1).

4. Click **Create Route Rule**.

5. Enter the following values:

    - **Destination CIDR Block:** 10.100.0.0/16 (on-premises CIDR)

    - **Target Type:** Dynamic Routing Gateway (DRG1)

    - **Target Compartment:** Leave as is.

Note: For this example, the internet gateway is being used for traffic not destined to the on-premises networks. This internet gateway is seen as 0.0.0.0/0 target "IGW."

6. Click **Create**.

Step 6: Edit the Default Security List for the Subnet

By default, incoming traffic to the instances in your VCN is set to DENY on all ports and all protocols. In this task, you set up four ingress rules and one egress rule to allow on-premises networks to reach the VCN.

Important: In the following procedure, ensure that the on-premises CIDR that you specify in the security list rules is the same (or smaller) than the CIDR that you specified in the route rule in the preceding task. Otherwise, traffic will be blocked by the security lists.

1. While still viewing your VCN, click **Security Lists** on the left side of the page.

2. Click the name of the default security list (Default Security List for VCN1).

3. Click **Edit All Rules**.

4. Add ingress rules with the following values:

   - Stateful: SSH Allow from 0/0

     o **Source CIDR:** 0.0.0.0/0

     o **IP Protocol:** TCP

     o **Source Port Range:** Empty (Default All)

     o **Destination Port Range:** 22 (for SSH traffic)

   - Stateful: ICMP 3,4 from 0/0

     o **Source CIDR:** 0.0.0.0/0

     o **IP Protocol:** ICMP

     o **Type and Code:** 3,4

     Note: A rule for ICMP type 3, code 4 is required for path MTU discovery. Without this rule, connectivity problems are harder to troubleshoot.

   - Stateful: ICMP 3 from VCN1/self (10.0.0.0/16)

     o **Source CIDR:** 10.0.0.0/0 (VCN1/self)

     o **IP Protocol:** ICMP

     o **Type:** 3

- Stateful: All IP from on-premises network (10.100.0.0/16)

    - **Source CIDR:** 10.100.0.0/0

    - **IP Protocol:** All Protocols

5. Add an egress rule that allows outgoing traffic on all ports to any network:

- **Destination CIDR:** 0.0.0.0/0

- **IP Protocol:** All Protocols

6. Click **Save Security List Rules**.

Step 7: Create a Subnet

In this task you create a subnet in the VCN with a CIDR smaller than the VCN CIDR, using the default route table and security lists that you modified in the preceding steps. Any instances that you launch into this subnet have access to your on-premises network. A subnet is specific to a particular availability domain, which means that all the private IP addresses within a subnet belong to a single availability domain.

1. While still viewing your VCN, click **Subnets** on the left side of the page.

2. Click **Create Subnet**.

3. Enter the following values:

   - **Create in Compartment:** Leave as is.

   - **Name:** A descriptive name for the subnet (for example, SUB1AD1). It doesn't have to be unique, and it can't be changed later in the Console (but you can change it with the API). Avoid entering confidential information.

   - **Availability Domain:** The availability domain that you want to use for the subnet (for example, AD-1).

   - **CIDR Block:** A single, contiguous CIDR block for the subnet (for example, 10.0.1.0/24). It must be smaller than the VCN CIDR block and can't overlap with any other subnets. You can't change this value later.

   - **Route Table:** The default route table that you modified earlier.

   - **Public Subnet:** Select this option to have public IP address available for Compute instances.

   - **Use DNS Hostnames in this Subnet:** Leave as is (selected).

   - **DHCP Options:** The default set of DHCP options for the VCN.

   - **Security Lists:** The default security list that you modified earlier.

4. Click **Create**.

A subnet with a range of IP address CIDR 10.0.1.0/24 that is a subset of VCN IP address CIDR 10.0.0.0/16 is created. This subnet is attached to availability domain AD1 with the route table and security lists that were modified earlier. The basic VCN in this example is now set up, and you're ready to create the remaining components for the IPSec VPN.
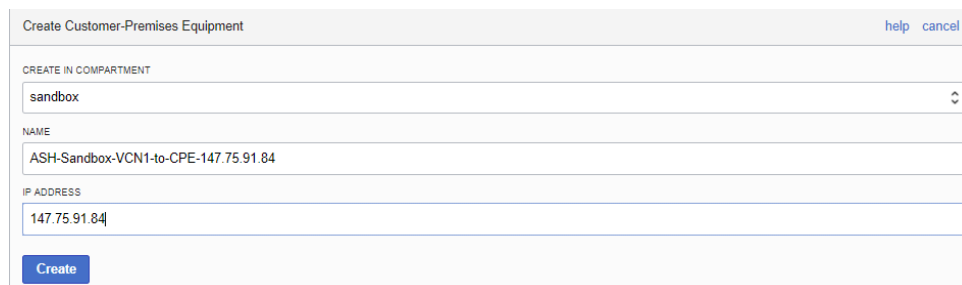
Step 8: Create a CPE Object

The outside IP address of the on-premises VPN is used to create a CPE object on Oracle Cloud Infrastructure. This object is a logical representation of the on-premises VPN device.

1. Click **Networking**, and then click **Customer-Premises Equipment**.

2. Click **Create Customer-Premises Equipment**.

3. Enter the following values:

- **Create in Compartment:** Leave as is (the VCN's compartment).

- **Name:** A descriptive name for the CPE object (for this example, ASH-Sandbox-VCN1-to-CPE-147.75.91.84). It doesn't have to be unique, and it can't be changed later in the Console (but you can change it with the API). Avoid entering confidential information.

- **IP Address:** The IP address of the on-premises VPN router for this CPE.

4. Click **Create**.

The CPE object is created and displayed on the page.

Step 9: Create an IPSec Tunnel Between the DRG and CPE

1. Click **Networking**, and then click **Dynamic Routing Gateways**.

2. Click the DRG that you created earlier (DRG1).

3. Click **Create IPSec Connection**.

4. Enter the following values:

- **Create in Compartment:** Leave as is (the VCN's compartment).

- **Name:** Enter a descriptive name for the IPSec connection. It doesn't have to be unique, and it can't be changed later in the Console (but you can change it with the API). Avoid entering confidential information.

- **Customer-Premises Equipment Compartment:** Leave as is (the VCN's compartment).

- **Customer-Premises Equipment:** Select the CPE object that you created earlier (ASH-Sandbox-VCN1-to-CPE-147.75.91.84).

- **Static Route CIDR:** The CIDR for the on-premises network. For this example, enter 0.0.0.0/0. You can't change this value later. If you want to change the static routes later, you must delete these tunnels and then create and configure new ones.

5. Click **Create IPsec Connection**.

The IPSec connection is created and displayed on the page. It will be in the Provisioning state for a short period.

Step 10: Verify the IPSec Tunnels

After the IPSec connection is provisioned, it is displayed on the console.

To view the tunnel configuration, click the actions icon (● ● ●), and then click **Tunnel Information**.

In the IPsec Connection Status page, the tunnels that are built by default are listed. All tunnels should show a status of Down because they are not configured with the on-premises VPN device yet. Copy the tunnel configuration information (IP address and shared secret), which you will need when configuring the on-premises VPN device.

Summary

In the preceding steps, you set up Oracle Cloud Infrastructure for IPSec VPN with multiple tunnels. Several IP addresses and pre-shared keys must now be configured on the on-premises/CPE VPN peer device. Configuring the Cisco ASA/ASAv with VTI/Virtual Tunnel Interface is covered in the next section.

Configure the ASA/ASAv On-Premises Device

Now that the Oracle Cloud Infrastructure VPN has been configured, you need to configure the Cisco ASA/ASAv device to connect to each of the tunnel endpoint IP addresses and pre-shared key. The following diagram shows what needs to be configured:

On Prem Network:
10.100.0.0 /16

Local Servers
10.100.6.3

10.100.6.2

ASA/ASAv

147.75.91.84   Internet

129.213.6.52
129.213.7.50
129.213.6.63
129.213.7.61

OCI DRG
IPSec

OCI VCN:
10.0.0.0 / 16
SUB1AD1
10.0.1.0 / 24

OCI VMs   OCI BM

OCI VM on SUB1AD1
10.0.1.16

OCI SUB1AD1 Router
10.0.1.1

Tunnel Information:
IKE Proposal
Encryption: AES-256
Hash: sha
D-H Group: 5
Authentication: pre-share
Lifetime: 28800
Perfect Forward Secrecy: group 5
Pre-shared key: Stored

IPSec Proposal-
Mode: ESP, Tunnel
ESP Encryption: AES-256
ESP Authentication: SHA
PFS: Enabled
D-H Group: 5
Ipsec key lifetime: 3600

Step 1: Note All the Values Used in the ASA/ASAv Configuration

Record all the networks and values to be used in the configuration:

Parameter	Source	Example Value
ipAddress1	Console/API	129.213.6.52
sharedSecret1	Console/API	(long string)

Parameter	Source	Example Value
ipAddress2	Console/API	129.213.7.50
sharedSecret2	Console/API	(long string)
ipAddress3	Console/API	129.213.6.63
sharedSecret3	Console/API	(long string)
ipAddress4	Console/API	129.213.7.61
sharedSecret4	Console/API	(long string)
cpePublicIpAddress	User	147.75.91.84
vcnID	Console/API/User	1
VcnCidrBlock	User	10.0.0.0/16
VcnCidrNetwork	User	10.0.0.0
VcnCidrNetmask	User	255.255.0.0
outsideInterface	User CPE	Gigabit 0/0
outsideInterfaceName	User CPE	Outside
looopbackIpAddress1	User CPE	169.254.101.1
looopbackIpAddress2	User CPE	169.254.102.1
looopbackIpAddress3	Not applicable	Not applicable
looopbackIpAddress4	Not applicable	Not applicable
tunnelInterfaceName1	User CPE	Tunnel1 / ORACLE-VPN1
tunnelInterfaceName2	User CPE	Tunnel2 / ORACLE-VPN2
tunnelInterfaceName3	Not applicable	Not applicable
tunnelInterfaceName4	Not applicable	Not applicable

Note: If there are more the two tunnels in the Oracle Cloud Infrastructure Console, you don't need to configure more than two at a time.

Step 2: Configure the IKE and IPSec Policy and IPSec Profile

In this step, you enable IKEv1 on the outside interface. This interface was used as the CPE IP address. You also create a policy with a value of 1 for the Oracle Cloud Infrastructure VPN configuration. The 1 puts this policy as a higher priority than built-in policies that start at 10.

Enter the Console or via SSH, get to privileged enable mode, and enter the configuration. It is helpful to save the running configuration to an alternative file name before configuration so that you can start from the beginning if there are issues (it's easier to start from scratch than to try to undo all the configuration at the command line).

```
crypto ikev1 enable outside
crypto ikev1 policy 1
 authentication pre-share
 encryption aes-256
 hash sha
 group 5
 lifetime 28800

crypto ipsec ikev1 transform-set oracle-vcn-transform esp-aes-256 esp-sha-hmac
crypto ipsec security-association lifetime kilobytes unlimited
crypto ipsec profile oracle-vcn-vpn-policy
   set ikev1 transform-set oracle-vcn-transform
   set pfs group5
   set security-association lifetime seconds 3600
```

The command to verify the preceding setting is `show crypto ikev1 sa detail`. The output for `ikev1 sa detail` will cycle until the tunnel is formed.

Note: A value of 28800 for `lifetime` is important. It *must match* in multivendor and cloud-based VPN headend scenarios.

Step 3: Set Up Some IPSec and Tunnel Friendly Parameters

```
crypto ipsec security-association replay window-size 128
```

The default settings for `crypto ipsec df-bit copy outside`, `sysopt connection tcpmss 1380`, and `crypto ipsec fragmentation before-encryption outside` are proper for this use case. To verify the settings at runtime, run:

```
show running-config all sysopt | include mss

sysopt connection tcpmss 1380

show crypto ipsec df-bit outside

df-bit outside copy

show crypto ipsec fragmentation outside

fragmentation outside before-encryption

show running-config | include replay

crypto ipsec security-association replay window-size 128
```

Step 4: Configure the Tunnel Group

For each of the tunnel IP addresses and key pairs, create a tunnel group entry as follows. Note that `*****` signifies the pre-shared key, a 64-character string that looks like the following example: bB8u6Tj60uJL2RKYR0OCyiGMdds9gaEUs9Q2d3bRTTVRKJ516CCc1LeSMChAI0rc.

If the pre-shared keys need to be revealed in the configuration on an ASA/ASAv device, use the more `system:running-config` command rather than the usual `show run` command.

Note that the tunnel group is named after the IP address provided by Oracle Cloud Infrastructure along with the pre-shared key.

```
tunnel-group 129.213.6.52 type ipsec-l2l
tunnel-group 129.213.6.52 ipsec-attributes
 ikev1 pre-shared-key *****

tunnel-group 129.213.7.50 type ipsec-l2l
tunnel-group 129.213.7.50 ipsec-attributes
 ikev1 pre-shared-key *****
```

Note: The default of Dead Peer Detection timers can be modified under the tunnel `ipsec-attributes`. The default of 10 threshold 2 second retry is good.

Step 5: Configure the VTI

Next you create the tunnels along with their `nameif` and "no shut" them. Note the tunnel destinations the IP address provided by Oracle Cloud Infrastructure.

```
interface Tunnel1
 nameif ORACLE-VPN1
 ip address 169.254.101.1 255.255.255.0
 tunnel source interface outside
 tunnel destination 129.213.6.52
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile oracle-vcn-vpn-policy

interface Tunnel2
 nameif ORACLE-VPN2
 ip address 169.254.102.1 255.255.255.0
 tunnel source interface outside
 tunnel destination 129.213.7.50
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile oracle-vcn-vpn-policy
```

Note: The IP address here is a loopback IP address. This is not related to on-premises IP addressing or to VPN addressing. This IP address in the future will be used in BGP configuration.

To see the tunnel configuration and statistics, run `show crypto ipsec sa`. The interfaces are shown as follows with all of the parameters given in the tunnel interface configuration:

```
show crypto ipsec sa
interface: oraclevpn1
    Crypto map tag: __vti-crypto-map-5-0-1, seq num: 65280, local addr: OUTSIDE
IP ADDRESS for ASA / CPE IP
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer: CLOUD IP ADDRESS / VPN HEAD END
      #pkts encaps: 3939963, #pkts encrypt: 3939963, #pkts digest: 3939963
      #pkts decaps: 7180123, #pkts decrypt: 7180123, #pkts verify: 7180123
      local crypto endpt.: OUTSIDE IP ADDRESS for ASA / CPE IP , remote crypto
endpt.: CLOUD IP ADDRESS / VPN HEAD END
      path mtu 1500, ipsec overhead 74(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
    inbound esp sas:
        SA State: active
        transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, VTI, }
        sa timing: remaining key lifetime (sec): 1942
        replay detection support: Y
    outbound esp sas:
        SA State: active
        transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, VTI, }
        sa timing: remaining key lifetime (sec): 1942
        replay detection support: Y
```

To see the interface, use `show interface Tunnel 1`.

```
Interface Tunnel1 "oraclevpn1", is up, line protocol is up
  Hardware is Virtual Tunnel    MAC address N/A, MTU 1500
        IP address 192.168.101.1, subnet mask 255.255.255.252
  Tunnel Interface Information:
        Source interface: outside      IP address: 147.75.203.51
        Destination IP address: 129.213.6.54
        Mode: ipsec ipv4       IPsec profile: oracle-vcn-vpn-policy
```

Step 6: Configure the Static Routes

Set up the routes for the tunnels. Note the route destination is the IP address of the first IP in the destination subnet on the Oracle Cloud Infrastructure side.

```
route ORACLE-VPN1 10.0.0.0 255.255.0.0 10.0.1.1 1 track 1
route ORACLE-VPN2 10.0.0.0 255.255.0.0 10.0.1.1 100
```

With this configuration, the route's lowest metric and tracking will be used unless it goes down. The `track` command is used to validate connectivity of your primary tunnel interface. The tracking will validate that the Cloud IP for the VPN connection is available via ICMP and the route will be to the subnet in the VCN that is to receive the tunneled traffic.

Also, set up the tracking and monitoring for the primary and backup links. For this ICMP echo test, ping the external VPN peer IP (DRG external public IP). Without a routing protocol, the route with the lowest metric and tracking will be the primary link. Traffic only flows across the second tunnel if there is a failure in the first.

Note: VTI tunnels should come up without traffic traversing the tunnel. The SLA monitor configuration is not a mechanism to keep the tunnel but to detect if the primary route target is valid.

```
      track 1 rtr 10 reachability
      sla monitor 10
        type echo protocol ipIcmpEcho 129.213.6.52 interface outside
        frequency 5
      sla monitor  schedule 10 start-time now life forever
```

To verify the `sla monitor`, use `show sla monitor configuration`, `show sla monitor operational-state`, and `show route`.

The active route in `show route` will be shown for the VNC IP.

```
asavnine# show route

S*      0.0.0.0 0.0.0.0 [1/0] via 147.75.203.49, outside
S       10.0.0.0 255.255.0.0 [1/0] via 10.0.1.1, oraclevpn1
```

Note: oraclevpn1 is the current route target for 10.0.0.0/16.

At this point, it is useful to have a VM or host on the Oracle Cloud Infrastructure side brought up in the subnet for ping tests. Ping tests are often difficult to do from the ASA/ASAv device, so it is best to test reachability with these tests hosts. In this test setup, there is a host behind the ASA/ASAv, 10.100.6.3, and on the Oracle Cloud Infrastructure side, 10.0.1.16. A useful test is to test that each host on both sides can ping each other. In order to have ping work though the ASA/ASAv, the ICMP/ICMP error inspection should be enabled.

Important Note on This Configuration: If this is enabled, ping through the firewall will work. For some security scenarios, this is considered undesirable.

```
asavnine(config)# policy-map global_policy
asavnine(config-pmap)# class inspection_default
asavnine(config-pmap-c)# inspect icmp
asavnine(config-pmap-c)# inspect icmp error
asavnine(config-pmap-c)# exit
asavnine(config-pmap)# exit
```

Note that with ICMP inspection enabled, when link failover occurs, ICMP flows will be interrupted. You can't rely on ping testing to detect tunnel failures.

Step 7: Verify That the Tunnels Are Up on Oracle Cloud Infrastructure

1. In the Console, click **Networking**.

2. On the left side of the page, click **Dynamic Routing Gateways**.

3. Click the DRG that you created (DRG1).

4. On the IPsec Connections page, click the actions icon (● ● ●) for ASH-Sandbox-IPSEC-to-147.75.91.84, and then click **Tunnel Information**.

   Each of tunnels should be shown as UP, as in the following screenshot:
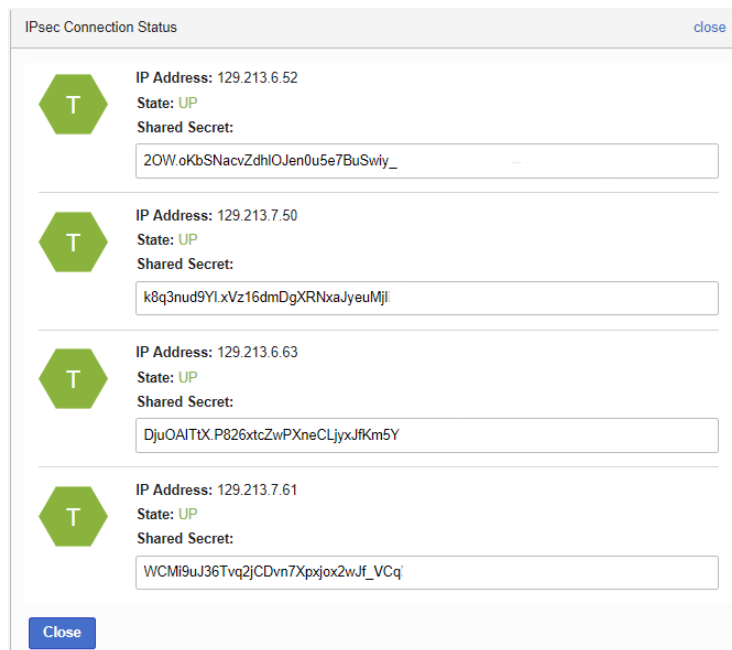
Sample ASA/ASAv Configuration File from this Document

These sections of the ASA/ASAv configuration have been changed throughout the document.

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 147.75.91.84 255.255.255.240
!
interface GigabitEthernet0/1
 nameif inside
```

```
 security-level 100
 ip address 10.100.6.2 255.255.255.0
!
interface Management0/0
 management-only
 nameif management
 security-level 0
 ip address 172.31.254.254 255.255.255.0
!
interface Tunnel1
 nameif ORACLE-VPN1
 ip address 169.254.101.1 255.255.255.0
 tunnel source interface outside
 tunnel destination 129.213.6.52
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile oracle-vcn-vpn-policy
!
interface Tunnel2
 nameif ORACLE-VPN2
 ip address 169.254.102.1 255.255.255.0
 tunnel source interface outside
 tunnel destination 129.213.7.50
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile oracle-vcn-vpn-policy
!!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object network remote_10_16
 subnet 10.0.0.0 255.255.0.0
object-group network inside-networks-object
 network-object 10.100.6.0 255.255.255.0
route ORACLE-VPN1 10.0.0.0 255.255.0.0 10.0.1.1 1 track 1
route ORACLE-VPN2 10.0.0.0 255.255.0.0 10.0.1.1 100
route outside 0.0.0.0 0.0.0.0 147.75.91.81 1
sla monitor 10
 type echo protocol ipIcmpEcho 129.213.6.52 interface outside
 frequency 5
sla monitor schedule 10 life forever start-time now
crypto ipsec ikev1 transform-set oracle-vcn-transform esp-aes-256 esp-sha-hmac
crypto ipsec profile oracle-vcn-vpn-policy
 set ikev1 transform-set oracle-vcn-transform
 set pfs group5
 set security-association lifetime seconds 3600
crypto ipsec security-association replay window-size 128
crypto ikev1 enable outside
crypto ikev1 policy 1
 authentication pre-share
 encryption aes-256
 hash sha
 group 5
 lifetime 28800
tunnel-group 129.213.6.52 type ipsec-l2l
tunnel-group 129.213.6.52 ipsec-attributes
 ikev1 pre-shared-key
 ************************************************************
tunnel-group 129.213.7.50 type ipsec-l2l
tunnel-group 129.213.7.50 ipsec-attributes
```

```
 ikev1 pre-shared-key
*************************************************************
policy-map global_policy
 class inspection_default
  inspect icmp
  inspect icmp error
```

Conclusion

Oracle Cloud Infrastructure VPN IPSec tunnels establish private network connectivity from an on-premises location to a virtual cloud network (VCN) on Oracle Cloud Infrastructure. Because multiple redundant tunnels are created, connectivity is highly available.

Future revisions of this guide will examine the specifics of the SLA feature and route tracking, along with HA configuration on the ASA/ASAv side.

Another version of this guide will go over a policy-based (crypto maps-based) ASA/ASAv IPSec configuration.

Oracle recommends that this service be configured by network engineers following the best practices for the VPN IPSec device and that security lists and security rules are created with care.

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

Deploying VPN IPSec Tunnels with Cisco ASA/ASAv VTI on Oracle Cloud Infrastructure
March 2018
Author: Brendan Howes

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