Oracle® Cloud

Setting Up VPN from a Third-Party Gateway to an IP Network in Oracle Cloud

E65839-11
May 2020

Oracle Cloud Setting Up VPN from a Third-Party Gateway to an IP Network in Oracle Cloud,

E65839-11

Primary Author: Sylaja Kannan

Contributing Authors: Kunal Rupani, Anamika Mukherjee, Babu Suryanarayanan, Henry Shen, Neeraj Sharma

Contents

Preface

This document describes how to set up VPN access from a third-party gateway to an IP network in Oracle Cloud Infrastructure Compute Classic.

Topics

- Audience
- Conventions

Audience

This document is intended for administrators who want to set up VPN access through an third-party VPN gateway in their data center to an IP network in a multitenant Compute Classic site.

Conventions

This table describes the text conventions used in this document.

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Accessible Access to Oracle Support

Oracle customers who have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Related Resources

For more information, see these Oracle resources:

- Database Backup on the Oracle Cloud website

  `https://cloud.oracle.com/database_backup`

- Oracle Database Backup Service FAQ (My Oracle Support Doc ID 1640149.1)

  `http://support.oracle.com`

- *Getting Started with Oracle Cloud*
- *Using Oracle Storage Cloud Service*
- *Using Oracle Database Cloud Service (Database as a Service)*

1 Solution Overview

This document describes how to set up VPN access from an Oracle-certified third-party VPN device in your data center to Compute Classic instances that are attached to an IP network defined by you in a multitenant Compute Classic site.

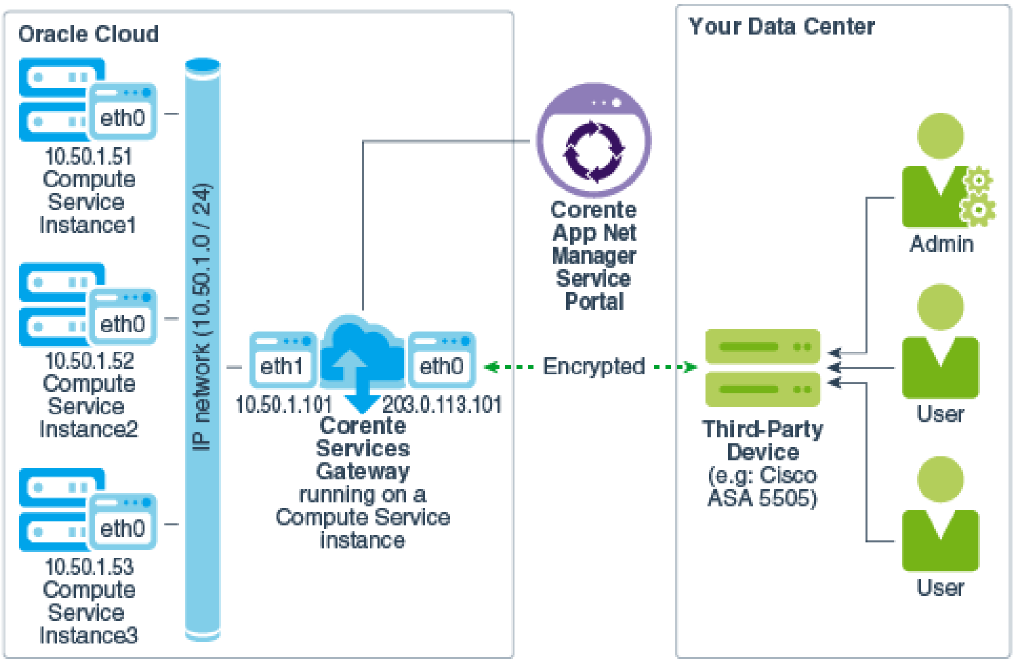
Topics

- Solution Architecture and Key Components
- Certified Third-Party VPN Devices and Configurations
- Workflow for Setting Up VPN
- Solution Architecture for Setting Up VPN Gateways in Active-Active HA Mode
- Workflow for Setting Up VPN Gateways in Active-Active HA Mode

> **Note:**
>
> The following other VPN solutions are available for instances in multitenant sites:
>
> - VPN access through a Corente Services Gateway in your data center to instances attached to an IP network defined by you in the cloud. See *Setting Up VPN From a Corente Services Gateway to an IP Network in Oracle Cloud*.
> - VPN access through a third-party gateway or Corente Services Gateway in your data center to instances attached to the Oracle-provided shared network. See the following documentation:
>   - *Setting Up VPN from a Third-Party Gateway On-Premises to the Shared Network*
>   - *Setting Up VPN from Corente Services Gateway On-Premises to the Shared Network*

Solution Architecture and Key Components

The following figure provides an overview of the solution:


Oracle Cloud
eth0
10.50.1.51
Compute Service Instance1
eth0
10.50.1.52
Compute Service Instance2
eth0
10.50.1.53
Compute Service Instance3
IP network (10.50.1.0 / 24)
eth1
eth0
10.50.1.101
203.0.113.101
Corente Services Gateway running on a Compute Service instance
Corente App Net Manager Service Portal
Encrypted
Your Data Center
Third-Party Device (e.g: Cisco ASA 5505)
Admin
User
User

The following are the key components of this solution:

- **Corente Services Gateway**: Corente Services Gateway is installed on an Compute Classic instance running in Oracle Cloud. It serves as a proxy that facilitates secure access and data transfer in the VPN solution.
- **Corente App Net Manager Service Portal**: You use App Net Manager to create, configure, modify, delete, and monitor the components of your Corente-powered network. You can create, configure, modify, delete, and monitor the components of your Corente-powered network using the Compute Classic web console as well. For advanced configurations in your Corente-powered network, use the App Net Manger.
- **Third-Party Device**: Any certified third-party VPN solution that allows interoperability with Corente Services Gateway.

Certified Third-Party VPN Devices and Configurations

The following table lists the third-party VPN device configurations that are certified for the Corente 9.4 release.

Certified Configurations	Devices
• Encryption AES256; Hash SHA-256 • DH phase 1 group 14 • No Perfect Forward Secrecy (PFS); so no Diffie-Hellman (DH) phase 2 group	Cisco 2921 Cisco ISR 4331 Checkpoint 3200 Palo Alto 3020 FortiGate-200D

Certified Configurations	Devices
• Encryption AES256; Hash SHA-256 • DH phase 1 group 14; DH phase 2 group 14	Cisco 2921 Cisco ISR 4331 Checkpoint 3200 Palo Alto 3020 FortiGate-200D
• Encryption AES128; Hash SHA-256 • DH phase 1 group 14; no PFS	Cisco 2921 Cisco ISR 4331 Checkpoint 3200 Palo Alto 3020 FortiGate-200D
• Encryption AES192; Hash SHA-1 • DH phase 1 group 2, DH phase 2 group 2	Cisco ASA5505
• Encryption AES256; Hash SHA-1 • DH phase 1 group 5; no PFS	Cisco ISR 4331 Checkpoint 3200 Palo Alto 3020 FortiGate-200D

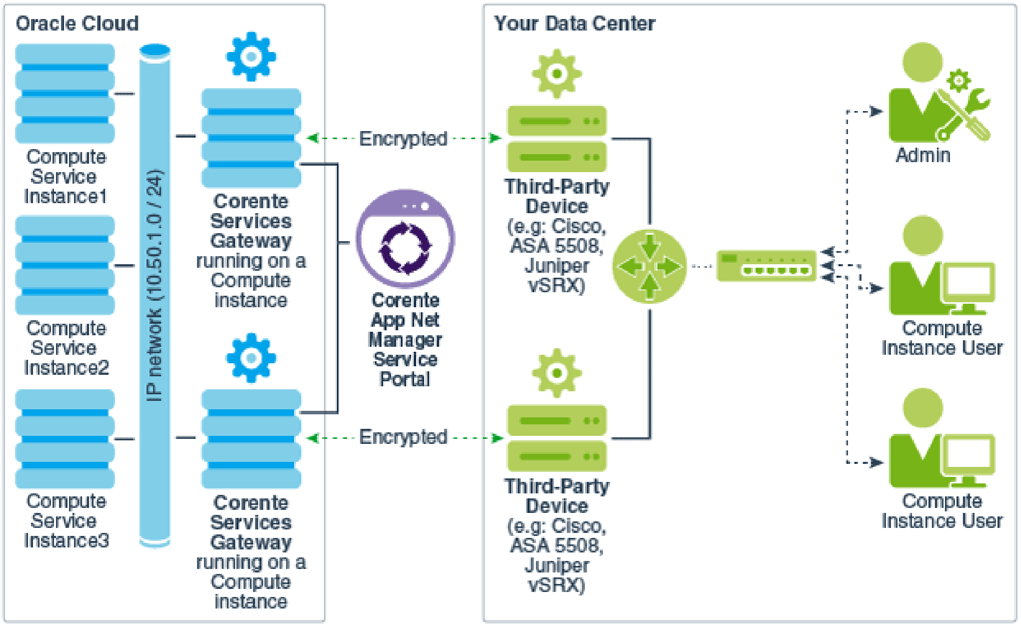
> **Note:**
>
> Other devices may work if they are configured with the certified configurations.
>
> The Corente Services Gateway uses IPSec and is behind a NAT, so network address translator traversal (NAT-T) is required. Ensure that the third-party device in your data center supports NAT-T.

Workflow for Setting Up VPN

Task	More Information
Create and configure your account on Oracle Cloud	Getting an Oracle.com Account in *Getting Started with Oracle Cloud*
Obtain a trial or paid subscription to Compute Classic. After you subscribe to Compute Classic, you will get your Corente credentials through email. Make a note of these credentials.	How to Begin with Compute Classic Subscriptions in *Using Oracle Cloud Infrastructure Compute Classic*
Create an IP network.	Creating an IP Network
Set up Corente Services Gateway (cloud gateway) on a Compute Classic instance.	Creating a Cloud Gateway
Establish partnership between the third-party VPN device and the cloud gateway.	Registering a Third-Party VPN Device Connecting the Cloud Gateway with the Third-Party Device
Configure your guest instances for VPN access.	Configuring Your Guest Instances for VPN Access

Solution Architecture for Setting Up VPN Gateways in Active-Active HA Mode

You can deploy two Corente Services Gateway as failover partners to ensure high availability. The following figure provides an overview of the solution.


Oracle Cloud
Compute Service Instance1
Compute Service Instance2
Compute Service Instance3
IP network (10.50.1.0 / 24)
Corente Services Gateway running on a Compute instance
Corente Services Gateway running on a Compute instance
Encrypted
Encrypted
Corente App Net Manager Service Portal
Your Data Center
Third-Party Device (e.g: Cisco, ASA 5508, Juniper vSRX)
Third-Party Device (e.g: Cisco, ASA 5508, Juniper vSRX)
Admin
Compute Instance User
Compute Instance User

In this solution, two Corente Services Gateways, configured identically, are deployed as failover partners. Each Corente Service Gateway is connected to a separate third-party VPN device, setting up two VPN tunnels between Oracle Cloud network and your data center. When both VPN tunnels are available, load is balanced between the two Corente Services Gateways. If one of the VPN tunnel fails, Corente Services Gateway detects the failure and forwards the incoming traffic to its failover partner. This offers redundancy against VPN tunnel failures.

Workflow for Setting Up VPN Gateways in Active-Active HA Mode

Task	More Information
Create and configure your account on Oracle Cloud	Getting an Oracle.com Account in *Getting Started with Oracle Cloud*
Obtain a trial or paid subscription to Compute Classic. After subscribing to Compute Classic, you will get your Corente credentials through email. Make a note of these credentials.	How to Begin with Compute Classic Subscriptions in *Using Oracle Cloud Infrastructure Compute Classic*
Create an IP network.	Creating an IP Network
Set up two Corente Services Gateways (cloud gateways) in Oracle Cloud.	Creating a Cloud Gateway
Add the first third-party VPN device.	Registering a Third-Party VPN Device
Add the second third-party VPN device.	Registering a Third-Party VPN Device

Task	More Information
Establish partnership between the first pair of cloud gateway and third-party VPN device in your data center.	Connecting the Cloud Gateway with the Third-Party Device
Establish partnership between the second pair of cloud gateway and third-party VPN device in your data center.	Connecting the Cloud Gateway with the Third-Party Device
Configure the two Corente Services Gateways (cloud gateways) in Oracle Cloud as failover partners.	Configuring Active-Active HA
Configure your guest instances for VPN access.	Configuring Your Guest Instances for VPN Access

2 Creating an IP Network

To make your guest Compute Classic instances accessible over VPN, you should attach them *and* the Corente Services Gateway instance in the cloud to an IP network that you define in Compute Classic.

You can use an existing IP network or create a new one. For information about creating an IP network, see Creating an IP Network in *Using Oracle Cloud Infrastructure Compute Classic*. Note down the name of the IP network as you'll need to provide this name later while creating the Corente Services Gateway on the Cloud.

3

Creating a Cloud Gateway

If you want to establish a VPN connection to your Compute Classic instances, start by creating a Corente Services Gateway instance.

Prerequisites

- You must have already reserved the public IP address that you want to use with your gateway instance. See Reserving a Public IP Address in *Using Oracle Cloud Infrastructure Compute Classic*.
- You must have already created the IP network that you want to add your gateway instance to. See Creating an IP Network in *Using Oracle Cloud Infrastructure Compute Classic*.
- To complete this task, you must have the `Compute_Operations` role. If this role isn't assigned to you or you're not sure, then ask your system administrator to ensure that the role is assigned to you in Oracle Cloud Infrastructure Classic Console. See Modifying User Roles in *Managing and Monitoring Oracle Cloud*.

Procedure

1. Sign in to the Compute Classic console. If your domain spans multiple sites, select the appropriate site. To change the site, click the **Site** menu near the top of the page.
2. Click the **Network** tab.
3. In the **Network** drop-down list, expand **VPN**, expand **Corente**, and then click **VPN Gateways**.
4. Click **Create VPN Gateway**.
5. Select or enter the required information:
   - **Name:** Enter a name for the Corente Services Gateway instance.
   - **IP Reservation:** Select the IP reservation that you want to use with this instance. This is the public IP address of your VPN gateway.
   - **Image:** Select the machine image that you want to use to create the instance. You must select the most recent Corente Gateway image.
   - **Interface Type:** Select **Dual-homed**. Your gateway instance is added to an IP network as well as to the shared network. All instances that are on the same IP network as the Corente Services Gateway instance, as well as instances on IP networks that are connected to that IP network through an IP network exchange, can be accessed using VPN.
   - **IP Network:** Select the IP network that you want to add the Corente Services Gateway instance to.
   - **IP Network Address:** Select the IP address for your gateway instance. The IP address that you specify must belong to the subnet of the specified IP network. An available IP address is allocated by default. You can specify a different LAN IP address, if required.

  - **Subnets:** Enter a comma-separated list of subnets (in CIDR format) that should be reachable using this gateway. The subnet of the IP network specified in the **IP Network** field is added by default. Don't modify or delete this subnet in this field.
  - **Add reachable IP networks:** (Optional) You can select additional IP networks that should be reachable using this gateway. Ensure that the IP networks that you specify here, and the IP network that the Corente Services Gateway is added to, all belong to the same IP network exchange. See Adding an IP Network to an IP Network Exchange in *Using Oracle Cloud Infrastructure Compute Classic*.
    You must also add a route on the gateway to the subnet of each additional IP network. You can't do this using the web console. Use App Net Manager to add this route.

    > **Note:**
    >
    > You must also add the subnets that you specify here to the list of destination IP addresses that you specify in your third-party device.

6. Click **Create**.

A Corente Services Gateway instance is created. The required orchestrations are created and started automatically. For example, if you specified the name of the Corente Gateway instance as **CSG1**, then the following orchestrations are created:

- **vpn–CSG1–launchplan:** This orchestration creates the instance using the specified image, and associates the instance interfaces with the shared network and the specified IP network.
- **vpn–CSG1–bootvol:** This orchestration creates the persistent bootable storage volume.
- **vpn–CSG1–secrules:** This orchestration creates the required security list, security applications, and security rules.
- **vpn–CSG1–master:** This orchestration specifies relationships between each of the nested orchestrations and starts each orchestration in the appropriate sequence.

While the Corente Services Gateway instance is being created, the instance status displayed in the **Instance** column on the VPN Gateways page is **Starting**. When the instance is created, its status changes to **Ready**.

To use this gateway in a VPN connection, add a third-party device and then create a connection. See Registering a Third-Party VPN Device and Connecting the Cloud Gateway with the Third-Party Device.

You can also update the gateway instance to modify the reachable routes, or delete the gateway instance if you no longer require this gateway. See Modifying the Reachable Subnets for a VPN Gateway or Deleting a VPN Gateway.

Note:

You can list the gateway instance and view details on the Instances page, or view the corresponding orchestrations on the Orchestrations page. However, it is recommended that you always use the VPN Gateways page to manage your gateway instances.

4

Registering a Third-Party VPN Device

To establish a VPN connection to your Compute Classic instances, after creating a Corente Services Gateway instance, register a VPN device to provide information about the third-party VPN gateway used in your data center.

To complete this task, you must have the `Compute_Operations` role. If this role isn't assigned to you or you're not sure, then ask your system administrator to ensure that the role is assigned to you in Oracle Cloud Infrastructure Classic Console. See Modifying User Roles in *Managing and Monitoring Oracle Cloud*.

1. Sign in to the Compute Classic console. If your domain spans multiple sites, select the appropriate site. To change the site, click the **Site** menu near the top of the page.
2. Click the **Network** tab.
3. In the **Network** drop-down list, expand **VPN**, expand **Corente**, and then click **Customer Devices**.
4. Click **Create VPN Device**.
5. Select or enter the required information:
   - **Name:** Enter a name for the third-party VPN device.
   - **Type:** Select a supported third-party VPN device from the list.
   - **Model:** Enter the model of your third-party VPN device.
   - **WAN IP Address:** Enter the IP address of the WAN interface of your third-party VPN device.
   - **Visible IP Address:** Enter the public IP address of your third-party VPN device that the Corente Services Gateway should connect to. If you use network address translation (NAT), then this IP address would be different from the WAN IP address. Otherwise, the visible IP address would be the same as the WAN IP Address.
   - **Subnets:** Enter (in CIDR format) a comma-separated list of subnets in your data center that should be reachable using this third-party device.
   - **PFS:** This option is selected by default. If your third-party device supports Perfect Forward Secrecy (PFS), retain this setting to require PFS.
   - **DPD:** This option is selected by default. If your third-party device supports Dead Peer Detection (DPD), retain this setting to require DPD.
6. Click **Create**.

   A record of your third-party VPN device is created. Next, to use this VPN device to establish a VPN connection between your data center and your Compute Classic instances, create a VPN connection. See Connecting the Cloud Gateway with the Third-Party Device.

5

Connecting the Cloud Gateway with the Third-Party Device

After you've created a Corente Services Gateway instance and added a third-party device, to establish a VPN connection between your data center and your Compute Classic instances you must connect the cloud gateway with the third-party VPN device.

Prerequisites

- You must have already created the cloud gateway that you want to use. See Creating a Cloud Gateway.
- You must have already configured your third-party VPN device in your data center. See Certified Third-Party VPN Devices and Configurations.
- You must have already added the third-party VPN device that you want to connect to in your data center. See Registering a Third-Party VPN Device.
- To complete this task, you must have the `Compute_Operations` role. If this role isn't assigned to you or you're not sure, then ask your system administrator to ensure that the role is assigned to you in Oracle Cloud Infrastructure Classic Console. See Modifying User Roles in *Managing and Monitoring Oracle Cloud*.

Procedure

1. Sign in to the Compute Classic console. If your domain spans multiple sites, select the appropriate site. To change the site, click the **Site** menu near the top of the page.
2. Click the **Network** tab.
3. In the **Network** drop-down list, expand **VPN**, expand **Corente**, and then click **Connections**.
4. Click **Create VPN Connection**.
5. Select or enter the required information:
   - **Gateway:** Select the Corente Services Gateway that you want to use. Each Corente Services Gateway can be used in multiple connections. However, each connection must reach distinct destination subnets.
   - **Device:** Select the third-party device that you want to use. Each device can be used in multiple connections. However, each connection must reach distinct destination subnets.
   - **IKE ID:** The Internet Key Exchange (IKE) ID. Only IKE v1 in Main Mode is supported. The IKE ID can be the name or IP address used to identify the Corente Services Gateway on the third-party device. Alternatively, you can specify a string that you want to use as the IKE ID.

     Select one of the following:

> **Note:**
>
> The third-party device that you use might not support all of the following options for IKE ID. Select the appropriate option for your device.

- **Gateway Name:** The name of the Corente Services Gateway instance in the format `Corente_Domain_name.Corente_Services_Gateway_instance_name`. The name is auto-populated when you select this option.
- **Gateway IP Address:** The private IP address (on the shared network) of the instance hosting the Corente Services Gateway. The IP address is auto-populated when you select this option. Note, however, that this address will change each time the instance is re-created.
- **User-Defined IKE ID:** Enter text that you want to use as the IKE ID. You can specify either an alternative IP address, or any text string. If you specify a text string, you must prefix the string with `@`. For example, if you want to specify the text `IKEID-for-VPN1`, enter `@IKEID-for-VPN1`. If you specify an IP address, don't prefix it with `@`. The IKE ID is case sensitive and can contain a maximum of 255 ASCII alphanumeric characters including special characters, period (.), hyphen (-), and underscore (_). The IKE ID can't contain embedded space characters.

  > **Note:**
  >
  > If you specify the IKE ID, ensure that you specify the Peer ID type as **Domain Name** on the third-party device in your data center. Other Peer ID types, such as email address, firewall identifier or key identifier, aren't supported.

- **Shared Secret:** The shared secret, also called the pre-shared key (PSK) on some devices, is used while setting up the VPN connection to establish the authenticity of the Corente Services Gateway that is requesting the VPN connection. You must enter the same shared secret here and on your third-party device. The shared secret must contain only alphanumeric characters.

The VPN connection is created.

An IP route is created automatically. The destination address of this route is the subnet address of the local side of the third-party device that will participate in the VPN connection. This route uses the vNIC of the Corente Services Gateway instance as the next hop vNICset, to route traffic from the IP network to the third-party VPN device. This allows devices in your data center's subnet to communicate with devices in the IP network over VPN.

An orchestration is created automatically to manage this vNICset and IP route and you can view this orchestration on the Orchestrations page of the web console. The name of the orchestration indicates the name of the Corente Services Gateway instance as well as the name of the third-party device used in the connection. For example, if you create a VPN connection between a Corente

Services Gateway **CSG1** and a third-party device **TPD1**, the name of the route and the corresponding orchestration would be: **vpn-CSG1–to–TPD1**.

6 Advanced Configuration

Topics

Adding IP Networks to an Existing VPN Connection

When you set up a VPN connection using a dual-homed Corente Services Gateway, all instances that have an interface on the same IP network as the gateway instance are reachable over the VPN connection. You can expand the network of reachable instances by creating other IP networks and adding all the IP networks to an IP network exchange.

Prerequisites

- You've already created a VPN connection from a third-party gateway to an IP Network in Oracle Cloud.
- To complete this task, you must have the `Compute_Operations` role. If this role isn't assigned to you or you're not sure, then ask your system administrator to ensure that the role is assigned to you in Oracle Cloud Infrastructure Classic Console. See Modifying User Roles in *Managing and Monitoring Oracle Cloud*.

Procedure

To add an IP network to an existing VPN connection, complete the following steps:

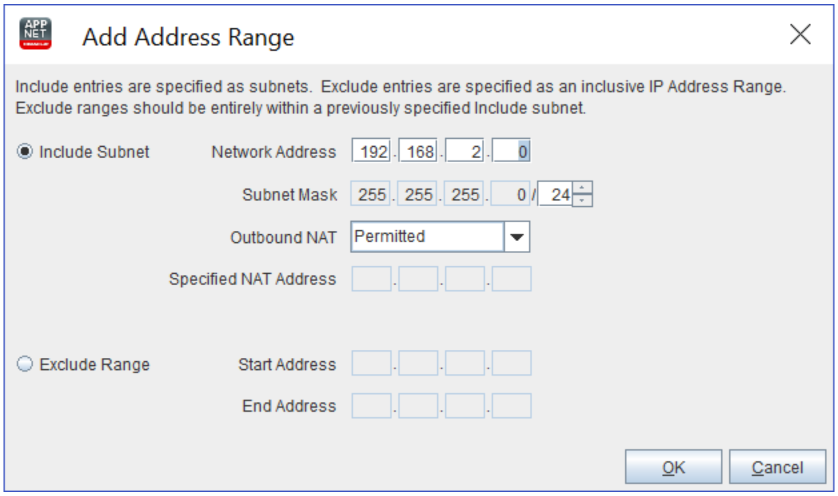
1. Let's consider that you want to add IP network 2 to an existing VPN connection, which has the Corente Services Gateway on IP network 1. Create IP network 2. See Creating an IP Network in *Using Oracle Cloud Infrastructure Compute Classic*.
2. Create an IP network exchange. See Creating an IP Network Exchange in *Using Oracle Cloud Infrastructure Compute Classic*.
3. Update both IP networks (IP network 1 and IP network 2) to add them to the IP network exchange. See Updating an IP Network in *Using Oracle Cloud Infrastructure Compute Classic*.
4. Download App Net Manager from https://www.corente.com/appnet, if you haven't downloaded it already. A JNLP file is downloaded.
5. Start App Net Manager by launching the downloaded JNLP file.
6. Log in to App Net Manager using the Corente credentials that you received in an email when you subscribed to Compute Classic.
7. In App Net Manager, update user groups for your Corente Services Gateway to add the new IP network.

a. From the **Domains** panel on the left, under **Locations**, right-click the location file of the Corente Services Gateway on Oracle Cloud, and then click **Edit**. The Edit Location dialog box appears.

b. In the **User Groups** tab, double-click **Default User Group**. The Edit User Group dialog box appears.

c. Click **Add**. The Add Address Range dialog box appears.

d. Select **Include Subnet**, and then provide details of the IP network that you want to add. Let's consider that IP network 2, which you want to add, has the IP address prefix `192.168.2.0/24`. The following image shows the details provided for IP network 2.



Add Address Range

Include entries are specified as subnets. Exclude entries are specified as an inclusive IP Address Range.
Exclude ranges should be entirely within a previously specified Include subnet.

● Include Subnet

Network Address: 192 . 168 . 2 . 0

Subnet Mask: 255 . 255 . 255 . 0 / 24

Outbound NAT: Permitted

Specified NAT Address: . . .

○ Exclude Range

Start Address: . . .

End Address: . . .

e. Select **Permitted** in the **Outbound NAT** drop-down list, and then click **OK**. A new row is added to the **User Group Subnets/ Address Ranges** pane. Click **OK** to close the Edit User Group dialog box.

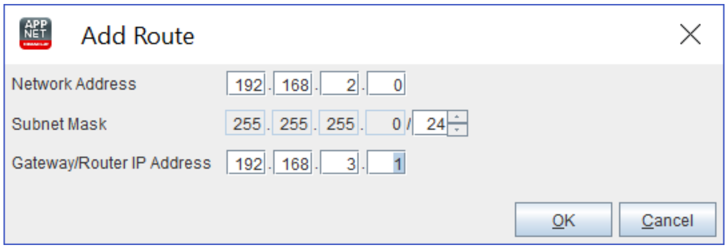
8. In App Net Manager, add a route to the subnet of the new IP network.

a. From the **Domains** panel on the left, under **Locations**, right-click the location file of the Corente Services Gateway on Oracle Cloud, and then click **Edit**. The Edit Location dialog box appears.

b. In the **Routes** tab, click **Add**. The Add Route dialog box appears.

c. Enter details about the IP network that you want to add to the existing VPN connection in the **Network Address** and **Subnet Mask**. Let's consider that IP network 2, which you want to add, has the IP address prefix `192.168.2.0/24`. Then, you'll enter `192.168.2.0` as the **Network Address** and `255.255.255.0/24` as the **Subnet Mask**.

d. In the **Gateway/Router IP Address** box, specify the first IP address of the IP subnet defined for IP network 1. The first IP address of the IP network subnet is reserved as the default gateway address for that IP network. For example, if the IP subnet defined for IP network 1 is `192.168.3.0/24`, then you'll provide `192.168.3.1` as the Router IP Address.



Network Address 192 . 168 . 2 . 0

Subnet Mask 255 . 255 . 255 . 0 / 24

Gateway/Router IP Address 192 . 168 . 3 . 1

e. Click **OK** to add the route.

9. Add the subnets that you specify here to the list of destination IP addresses that you specify in your third-party device.

Configuring Active-Active HA

To set up active-active HA, two Corente Services Gateways, configured identically, are deployed as failover partners. Each Corente Service Gateway is connected to a separate third-party VPN device, setting up two VPN tunnels between Oracle Cloud network and your data center. When both VPN tunnels are available, load is balanced between the two Corente Services Gateways. If one of the VPN tunnel fails, Corente Services Gateway detects the failure and forwards the outgoing traffic to its failover partner. This offers redundancy against VPN tunnel failures.

> **Note:**
>
> Skip this section if you don’t want to set up active-active HA.

Prerequisites

Before you begin configuring active-active HA, ensure that you have completed the following tasks:

1. Set up two Corente Services Gateways (cloud gateway), configured identically. See Creating a Cloud Gateway.
2. Registered two third-party VPN devices. See Registering a Third-Party VPN Device.
3. Connected the cloud gateways with the third-party VPN devices. See Connecting the Cloud Gateway with the Third-Party Device.

Complete the following steps to configure active-active HA:

1. Download App Net Manager from http://www.oracle.com/technetwork/server-storage/corente/downloads/index.html, if you haven’t downloaded it already.
2. Log in to App Net Manager using the Corente credentials that you received in an email when you subscribed to Compute Classic.
3. From the **Domains** panel on the left, under **Locations**, right-click a location file, and then click **Edit**. The Edit Location dialog box appears.
4. In the **Cloud Failover** pane, enter the LAN IP address of the partner Corente Services Gateway in the **Failover Location Address**, and then click **OK**.
5. Repeat steps 3 and 4 for the other Corente Services Gateway in the cloud.

6. From the **Domains** panel on the left, under **3rd-Party Devices**, right-click one of the third-party devices that you have added, and then click **Edit**. The Edit 3rd-Party Device dialog box appears.
7. In the **Settings** pane, select the **DPD** checkbox, and then click **OK**.

   Dead Peer Detection (DPD) is used to detect VPN failure to a remote VPN device.
8. Repeat steps 6 and 7 for the other third-party device.

7 Configuring Your Guest Instances for VPN Access

To make your guest Compute Classic instances accessible over VPN, you should attach them to the same IP network that the Corente Services Gateway instance is attached to.

1. Download the sample orchestration, `csg-sdn-guestinstance.json`, which is included in the `greconf_orchsamples.zip` file at the following location: http://www.oracle.com/technetwork/topics/cloud/downloads/network-cloud-service-2952583.html.
2. Open `csg-sdn-guestinstance.json` in a plain-text editor, and make the following changes:
   - Replace all occurrences of `myidentitydomain` with the ID of your identity domain.
   - Change all occurrences of `john.doe@example.com` to your user name.
3. Under the `launchplan` object type, update the following attributes:
   - Change the `name`, `ha_policy`, `label`, `imagelist`, and `shape` attributes to values of your choice. See Instance Attributes in *Using Oracle Cloud Infrastructure Compute Classic*.
   - Change `ipnetwork` to the name of the IP network that you created earlier and attached the Corente Services Gateway instance to. See Creating an IP Network.
     Here's a *partial* example of an instance orchestration showing the `networking` attribute.

     ```
     {
     "networking": {
       ...
       "eth1": {
         ipnetwork": "/Compute-acme/john@example.com/ipnet1",
         ...
        }
      }
     }
     ```
4. Save and close the orchestration JSON file.
5. Upload the orchestration to Compute Classic.

   See Uploading an Orchestration in *Using Oracle Cloud Infrastructure Compute Classic*.
6. Start the orchestration.

   See Starting an Orchestration in *Using Oracle Cloud Infrastructure Compute Classic*.
7. (Optional) If you specified multiple interfaces for the guest instance, and if one of those interfaces is attached to the Oracle-provided shared network, then you must

explicitly configure the Corente Services Gateway as the gateway to the on-premises subnet. You don't have to perform this additional step for instances that are only connected to the IP network and are not connected to the Oracle-provided shared network.

Here's a *partial* example of an instance orchestration showing the `networking` attribute with two interfaces: `eth1` attached to the IP network that the cloud gateway is attached to, and `eth0` attached to the Oracle-provided shared network with the IP address you had reserved earlier.

```
...
"networking": {
   "eth0": {
    "seclists": [
      "/Compute-acme/john@example.com/mySecList"
    ],
    "nat": "ipreservation:/Compute-acme/john@example.com/ipres1"
   },
   "eth1": {
     "ipnetwork": "/Compute-acme/john@example.com/ipnet1",
     ...
   }
}
```

On your guest instance, to configure the Corente Services Gateway as the gateway to the on-premises subnet, complete the following steps:

a. Log in to the instance.

b. Add a route:

> **Note:**
>
> You may need root or administrator privileges for this step.

- **Linux**:

  Command syntax: `ip route add` *`onprem_subnet`* `via` *`cloud_gateway_ip`*

  Example: `ip route add 10.248.64.176/28 via 172.31.200.1`

- **Windows**:

  Command syntax: `route add` *`onprem_subnet`* `mask` *`subnet_mask`* *`cloud_gateway_ip`*

  Example: `route add 192.168.49.0 mask 255.255.255.0 172.31.200.1`

When you run this command, set `cloud_gateway_ip` to the first address in the IP network that the cloud gateway instance is attached to, and set `onprem_subnet` to the subnet address of the on-premises network. For example, if `172.31.200.0/24` is the IP address prefix of the IP network that is attached to the cloud gateway instance, then the `cloud_gateway_ip` is `172.31.200.1`. If `192.168.0.128/25` is the IP address prefix of the IP network that is attached to the cloud gateway instance, then the `cloud_gateway_ip` is `192.168.0.129`.

Note:

You must add this route every time the instance is rebooted or re-created. You can also configure the route to persist across reboots. For detailed instructions to configure the route to persist across reboots, refer to documentation for your operating system.

8 Managing VPN

Topics

> **Note:**
>
> You must have the `Compute_Operations` role to access the pages under the **VPN** tab. If you don’t have this role, you won’t be able to view these pages.

Listing VPN Gateways

After you’ve created one or more VPN gateways, you can see information about all your VPN gateways by using the web console.

To complete this task, you must have the `Compute_Operations` role. If this role isn’t assigned to you or you’re not sure, then ask your system administrator to ensure that the role is assigned to you in Oracle Cloud Infrastructure Classic Console. See Modifying User Roles in *Managing and Monitoring Oracle Cloud*.

1. Sign in to the Compute Classic console. If your domain spans multiple sites, select the appropriate site. To change the site, click the **Site** menu near the top of the page.
2. Click the **Network** tab.
3. In the **Network** drop-down list, expand **VPN**, expand **Corente**, and then click **VPN Gateways**.

The VPN Gateways page displays a list of all your Corente Services Gateways, along with information about each gateway such as the interface type and status of the gateway.

> **Note:**
>
> This page also displays Corente Services Gateways deployed on hosts outside of Compute Classic.

Each gateway can have any of the following statuses:

Status	Description
Active	The Corente Services Gateway instance is running.
Inactive	The Corente Services Gateway instance has been shut down or is being restarted. **Action:** If the instance is restarting, wait for it to return to the running state. If the instance has been shut down, start it to return to the Active state.
Download	The configuration file for the Corente Services Gateway is available to download, but hasn't been downloaded to the gateway instance. **Action:** Check that the required security rules or ACLs are in place and enabled, to allow the gateway instance to download the configuration file.
Downloaded	The configuration file for the Corente Services Gateway has been downloaded but not activated. This status usually indicates that the Corente Services Gateway is not yet installed or started. **Action:** Check that the gateway instance is running or restart the instance if required. Check that the required security rules or ACLs are in place and enabled.
Upgrade	A software upgrade is available for the Corente Services Gateway. **Action:** Schedule a maintenance time for the Corente Services Gateway in App Net Manager. The upgrade will occur automatically during the scheduled maintenance time. See the App Net Manager online help for more information.
Disconnected	The Corente Services Gateway has lost connectivity, without being powered off safely. **Action:** Check your network configuration to see if outbound connectivity has been blocked by firewall rules.
Denied	The Corente Services Gateway connection has been denied. **Action:** Contact Oracle Support.
New	A new Corente Services Gateway instance has been created using App Net Manager, but the configuration of this new gateway instance hasn't been completed. **Action:** Complete and save the configuration of the new gateway using App Net Manager. The new configuration will then be downloaded.
Unknown	The Corente Services Gateway is in an unknown state. **Action:** Check the status again after some time, or contact Oracle Support.

Modifying the Reachable Subnets for a VPN Gateway

You must specify the list of reachable subnets while creating a VPN gateway. If required, you can modify this list of subnets at any time after creating a VPN gateway.

To complete this task, you must have the `Compute_Operations` role. If this role isn't assigned to you or you're not sure, then ask your system administrator to ensure that the role is assigned to you in Oracle Cloud Infrastructure Classic Console. See Modifying User Roles in *Managing and Monitoring Oracle Cloud*.

1. Sign in to the Compute Classic console. If your domain spans multiple sites, select the appropriate site. To change the site, click the **Site** menu near the top of the page.
2. Click the **Network** tab.
3. In the **Network** drop-down list, expand **VPN**, expand **Corente**, and then click **VPN Gateways**.
4. Go to the VPN gateway for which you want to modify the set of subnets. From the ☰ menu, select **Update**.
5. Modify the list of reachable subnets or IP networks as required, and then click **Update**.

   > **Note:**
   >
   > You can't modify or delete the subnet of the IP network to which your gateway belongs.

   The list of subnets or IP networks reachable by the VPN gateway is updated. If you added IP networks, ensure that the IP networks that you specify here, and the IP network that the Corente Services Gateway is added to, all belong to the same IP network exchange. See Adding an IP Network to an IP Network Exchange in *Using Oracle Cloud Infrastructure Compute Classic*.
   You must also add a route on the gateway to the subnet of each additional IP network. You can't do this using the web console. Use App Net Manager to add this route.

Deleting a VPN Gateway

If you no longer require a VPN connection, you can stop the connection and delete the VPN gateway instance. Each VPN gateway instance is managed by a master orchestration that can be used to start or stop several nested orchestrations. To delete a VPN gateway instance, go to the VPN Gateways page in the web console and stop the master orchestration.

Prerequisites

- The VPN gateway that you want to delete must not be connected to any device. If the gateway is used in a VPN connection, stop the connection first. See Stopping, Restarting, and Deleting a VPN Connection.

- To complete this task, you must have the `Compute_Operations` role. If this role isn't assigned to you or you're not sure, then ask your system administrator to ensure that the role is assigned to you in Oracle Cloud Infrastructure Classic Console. See Modifying User Roles in *Managing and Monitoring Oracle Cloud*.

Procedure

1. Sign in to the Compute Classic console. If your domain spans multiple sites, select the appropriate site. To change the site, click the **Site** menu near the top of the page.
2. Click the **Network** tab.
3. In the **Network** drop-down list, expand **VPN**, expand **Corente**, and then click **VPN Gateways**.
4. Go to the Corente Services Gateway instance that you want to delete.
   - If you want to delete only the gateway instance, from the ☰ menu, select **Stop**. The orchestration that controls the gateway instance is stopped. This deletes the Corente Services Gateway instance.
   - If you want to delete the gateway instance as well as other associated resources, from the ☰ menu, select **Stop All**. The master orchestration that controls the gateway instance and its associated resources is stopped. This deletes the gateway instance as well as resources created by the nested orchestrations, such as the bootable storage volume and networking objects.

   > **Note:**
   >
   > Resources created outside the master orchestration, such as the public IP address reservation or IP networks, aren't deleted when you stop the master orchestration for the gateway instance. If you no longer need those resources, remember to delete them after you've stopped the master orchestration.

   After you've deleted a gateway instance, it continues to be listed on the VPN Gateways page, with the status **Stopped**. At any time, you can restart the master orchestration to re-create the cloud gateway instance and its associated resources.
5. If you want to delete the orchestrations associated with your gateway instance, go to the gateway instance and from the ☰ menu, select **Delete**.

   The master orchestration and the associated orchestrations for the instance, storage volumes, and security rules are deleted. The VPN gateway is no longer listed on the VPN Gateways page.

Listing Third-Party VPN Devices

After you've added third-party devices, you can see information about all your third-party devices by using the web console.

To complete this task, you must have the `Compute_Operations` role. If this role isn't assigned to you or you're not sure, then ask your system administrator to ensure that the role is assigned to you in Oracle Cloud Infrastructure Classic Console. See Modifying User Roles in *Managing and Monitoring Oracle Cloud*.

1. Sign in to the Compute Classic console. If your domain spans multiple sites, select the appropriate site. To change the site, click the **Site** menu near the top of the page.
2. Click the **Network** tab.
3. In the **Network** drop-down list, expand **VPN**, expand **Corente**, and then click **Customer Devices**.

The Customer Devices page displays a list of all the third-party devices that you've added, along with information about each device such as its model and type and its IP address.

Updating a Third-Party Device

After you've added a third-party device, if required, you can modify the information associated with a third-party devices by using the web console.

To complete this task, you must have the `Compute_Operations` role. If this role isn't assigned to you or you're not sure, then ask your system administrator to ensure that the role is assigned to you in Oracle Cloud Infrastructure Classic Console. See Modifying User Roles in *Managing and Monitoring Oracle Cloud*.

1. Sign in to the Compute Classic console. If your domain spans multiple sites, select the appropriate site. To change the site, click the **Site** menu near the top of the page.
2. Click the **Network** tab.
3. In the **Network** drop-down list, expand **VPN**, expand **Corente**, and then click **Customer Devices**.
4. Go to the device that you want to update. From the ☰ menu, select **Update**.
5. In the Update VPN Device dialog box, modify the information as required. Note that you can't change the device name or type. If you need to modify that information, add a new device. You can modify the following device information:
   - **Model:** The model of your third-party VPN device.
   - **WAN IP Address:** The IP address of the WAN interface of your third-party VPN device.
   - **Visible IP Address:** The public IP address of your third-party VPN device that the Corente Services Gateway should connect to. If you use network address translation (NAT), then this IP address would be different from the WAN IP address. Otherwise, the visible IP address would be the same as the WAN IP Address.
   - **Subnets:** A list of IP addresses or subnets in your data center that should be reachable by this third-party device.
   - **PFS:** Perfect Forward Secrecy.
   - **DPD:** Dead Peer Detection.
6. Click **Update**. The device information is updated.

Deleting a Third-Party Device

After you've added a third-party device, if you no longer want to use the device in a VPN connection, you can delete the device information by using the web console.

Prerequisites

- The device that you want to delete must not be used in a VPN connection. If the device is used in a VPN connection, stop the connection first. See Stopping, Restarting, and Deleting a VPN Connection.
- To complete this task, you must have the `Compute_Operations` role. If this role isn't assigned to you or you're not sure, then ask your system administrator to ensure that the role is assigned to you in Oracle Cloud Infrastructure Classic Console. See Modifying User Roles in *Managing and Monitoring Oracle Cloud*.

Procedure

1. Sign in to the Compute Classic console. If your domain spans multiple sites, select the appropriate site. To change the site, click the **Site** menu near the top of the page.
2. Click the **Network** tab.
3. In the **Network** drop-down list, expand **VPN**, expand **Corente**, and then click **Customer Devices**.
4. Go to the device that you want to delete. From the ☰ menu, select **Delete**.

   The information about the selected device is deleted and the device is no longer displayed on the Customer Devices page.

Listing VPN Connections

After you've created a connection between your VPN gateway and your third-party device, you can see a list of connections by using the web console.

To complete this task, you must have the `Compute_Operations` role. If this role isn't assigned to you or you're not sure, then ask your system administrator to ensure that the role is assigned to you in Oracle Cloud Infrastructure Classic Console. See Modifying User Roles in *Managing and Monitoring Oracle Cloud*.

1. Sign in to the Compute Classic console. If your domain spans multiple sites, select the appropriate site. To change the site, click the **Site** menu near the top of the page.
2. Click the **Network** tab.
3. In the **Network** drop-down list, expand **VPN**, expand **Corente**, and then click **Connections**.

When a dual-homed gateway is used in a connection, then an IP route is created with the subnet of the third-party device as the destination. This IP route uses the vNIC of the cloud gateway as the next hop vNICset, to route traffic from the IP network to the third-party VPN device. An orchestration is created to manage the required vNICset and IP route and the **IP Route** column displays the status of the route.

The Connections page also shows the status of each of your VPN connections. If a VPN connection has any status other than **Up**, check the status again after some time. If the status doesn't change to **Up**, then contact Oracle Support.

Updating a VPN Connection

After you've created a connection between a VPN gateway and a third-party device, if required, you can modify the IKE ID or the shared secret by updating the VPN connection.

The IKE ID and shared secret that you enter here must match the corresponding entries on the third-party device used in this connection. If you make any changes to these fields, ensure that the corresponding changes are made on the connected third-party device.

To complete this task, you must have the `Compute_Operations` role. If this role isn't assigned to you or you're not sure, then ask your system administrator to ensure that the role is assigned to you in Oracle Cloud Infrastructure Classic Console. See Modifying User Roles in *Managing and Monitoring Oracle Cloud*.

1. Sign in to the Compute Classic console. If your domain spans multiple sites, select the appropriate site. To change the site, click the **Site** menu near the top of the page.
2. Click the **Network** tab.
3. In the **Network** drop-down list, expand **VPN**, expand **Corente**, and then click **Connections**.
4. Go to the connection that you want to modify. From the ☰ menu, select **Update**.
5. Update the IKE ID or modify the shared secret as required, and then click **Update**.

   The IKE ID or shared secret is updated.

   > **Note:**
   >
   > The IKE ID and shared secret are used to identify and authenticate the Corente Services Gateway on the third-party device. If you modify these fields, ensure that the information you enter here matches the corresponding entries on the third-party device used in this connection.

Stopping, Restarting, and Deleting a VPN Connection

After you've created a connection between a VPN gateway and a third-party device, if you no longer want to use this VPN connection, you can stop the connection. You can then restart the VPN connection later, or delete it.

To complete this task, you must have the `Compute_Operations` role. If this role isn't assigned to you or you're not sure, then ask your system administrator to ensure that the role is assigned to you in Oracle Cloud Infrastructure Classic Console. See Modifying User Roles in *Managing and Monitoring Oracle Cloud*.

1. Sign in to the Compute Classic console. If your domain spans multiple sites, select the appropriate site. To change the site, click the **Site** menu near the top of the page.
2. Click the **Network** tab.
3. In the **Network** drop-down list, expand **VPN**, expand **Corente**, and then click **Connections**.
4. You can stop and restart a connection by stopping and starting the orchestration that controls the vNICset and route.
   - To stop a connection, delete the route between the IP network and the destination subnet. This effectively prevents traffic from the IP network from accessing the VPN connection. To stop the route orchestration, go to the connection that you want to stop. From the ☰ menu, select **Stop**. The route orchestration is stopped.
   - To restart a VPN connection, restart the route orchestration. Go to the connection that you want to restart. From the ☰ menu, select **Start**. The route orchestration is started, and traffic from the IP network can once again access the VPN connection.
5. To delete a VPN connection, go to the connection that you want to delete. From the ☰ menu, select **Delete**.

   This ends the partnership between the specified VPN gateway and the third-party device and deletes the route orchestration. The VPN connection is no longer listed on the Connections page.

After stopping or deleting a VPN connection, you can also delete the gateway instance or delete the information about the third-party device used in this connection. See Deleting a VPN Gateway or Deleting a Third-Party Device.

9 Troubleshooting

This section describes common problems that you might encounter when setting up VPN and explains how to solve them. If you cannot find a solution in this section, raise a service request with My Oracle Support.

- If you encounter issues while setting up a cloud gateway by creating a Corente Services Gateway instance, see Orchestration Problems in *Using Oracle Cloud Infrastructure Compute Classic*.
- If you encounter issues while connecting the cloud gateway with the partner device, see Partner VPN Device Problems.

Partner VPN Device Problems

This section describes common problems that you might encounter while connecting the cloud gateway with the partner device.

When there are issues setting up the connection to the partner device, alarms are created in App Net Manager. See Working with Alarms and Events in *Oracle Corente Cloud Services Exchange Administration Guide*.

Could Not Fit Range from Partner

Description

When the tunnel is not set up between the CSG gateway and the partner gateway, the following message is displayed as an active tunnel alarm in App Net Manager.

```
Gateway [identity-domain.name-of-CSG-gateway] could not fit range [remote acl range
10.0.0.0–10/63.255.255] from Partner [name-of-partner-device] because it is nested
within committed range [local LAN range 10.18.7.112–10.18.7.115] from Gateway/
Partner [identity-domain.name-of-CSG-gateway]. Consequently, the secure subnet
tunnel between the two Partners has not been brought up. Please check the partners’
NAT policies and User Groups.
```

Solution

This error indicates that the subnets provided in `10.18.x.x` range are already nested in `10.0.0.x`.

To resolve this issue, remove the `10.0.0.0` subnet.

IPsec Phase1 Failure Brings Down Tunnel

Description

The following error message is displayed under the **Alarms** section in the App Net Manager.

```
The secure tunnel between [identity-domain.name-of-CSG-gateway] and [name-of-partner-
device] is DOWN. (IPsec Phase1 ISAKMP SA Failed).
```

Solution

This error indicates that there is IPsec Phase 1 failure and the connection between the cloud gateway and the partner device could not be set up. Such failures usually occur if you have provided incorrect information, such as incorrect **WAN IP Address** or **Visible IP Address** while registering the third-party VPN device. See Registering a Third-Party VPN Device. Such failures can also occur if you have provided incorrect pre-shared key (PSK) as the **Shared Secret**. See Connecting the Cloud Gateway with the Third-Party Device.

To resolve this error, ensure that the information you have provided is correct. For information about updating a third-party VPN device, see Updating a Third-Party Device. For information about updating the PSK, see Updating a VPN Connection.

IPsec Phase2 Failure Brings Down Tunnel

Description

When you add another subnet, the VPN tunnel (which was established previously) fails and the following error message is displayed under the **Alarms** section in the App Net Manager.

```
The secure tunnel between [identity-domain.name-of-CSG-gateway] and [name-of-partner-
device] is DOWN.
detail
[IPsec Phase2 Failed
192.128.0.0/16-10.50.0.0/16:UP
10.0.0.0/16-10.50.0.0/16:DOWN]
```

Solution

This error indicates that the IP addresses announced by Corente doesn’t match with the IP addresses accepted or published by the partner device. In this example, the partner device is not configured to receive traffic from `10.0.0.0/16` subnet.

Add the new subnet to the firewall of the partner device.