S2S IPSec Tunnels between OCI and Azure

July 2022

Contents

Disclaimer

This disclaimer informs readers that the views, thoughts and opinions expressed in the text belong solely to the author, and not necessarily to the author's employer. This document was prepared by *Luis Catalán Hernández* in his personal capacity.

What's IPSEC VPN

Internet Protocol security (IPSec) is a framework of open standards for helping to ensure private, secure communications over Internet Protocol (IP) networks through the use of cryptographic security services. IPSec supports network-level data integrity, data confidentiality, data origin authentication, and replay protection. Because IPSec is integrated at the Internet layer (layer 3), it provides security for almost all protocols in the TCP/IP suite, and because IPSec is applied transparently to applications, there is no need to configure separate security for each application that uses TCP/IP.

IPSec helps provide defense-in-depth against:

- Network-based attacks from untrusted computers, attacks that can result in the denial-of-service of applications, services, or the network
- Data corruption
- Data theft
- User-credential theft
- Administrative control of servers, other computers, and the network.

You can use IPSec to defend against network-based attacks through a combination of host-based IPSec packet filtering and the enforcement of trusted communications.

Goal of this document

This document explains step-by-step the VPN IPSec tunnel configuration between Oracle Cloud Infrastructure and Azure Cloud. It's helpful to know the basics of networking before following the steps outlined in this white paper.

This document helps you complete all the necessary steps in Oracle Cloud Infrastructure and Azure Cloud. You'll be required to have all the necessary Cloud tenancies/subscription and access to the necessary resources from both cloud providers (credits, authorizations and authentications, etc, etc).

Scope of the document

The scope of this document is limited to a quick start guide for deploying VPN IPSec tunnels to connect to/from Oracle Cloud Infrastructure From/to Azure Cloud. This document outlines some best practices, and should not be used as a full reference guide to VPN IPSec tunnels.

Readers of the current document should first:

- Be familiar with the fundamentals of the Oracle Cloud Infrastructure and Azure Cloud
  - https://docs.oracle.com/en/learn/oci-basics-tutorial/index.html
  - https://azure.microsoft.com/en-gb/get-started/

- Have a background in VPN IPSec tunnel functionality:
  - https://en.wikipedia.org/wiki/IPsec

- Get familiar with Azure and Oracle networking concepts
  - https://azure.microsoft.com/en-us/products/category/networking/
  - https://www.oracle.com/cloud/networking/

VPN IPSec Tunnels Concepts

IPSec stands for Internet Protocol Security or IP Security. IPSec 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 Mode: IPSec only encrypts and/or authenticates the actual payload of the packet, and the header information stays intact.
- Tunnel Mode (supported by Oracle): IPSec encrypts and/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:

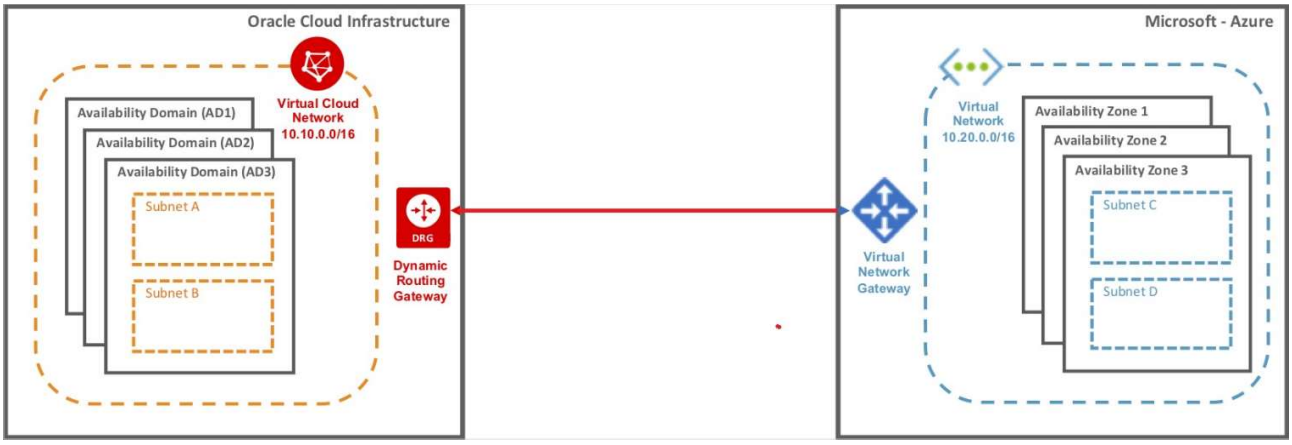
- No need to buy dedicated expensive lease lines from one site to another, as public telecommunication lines are used to transmit data.
- The internal IP addresses of both the participating networks and nodes are hidden from external users.
- The entire communication between the source and destination sites is encrypted, significantly lowering the chances of information theft. Oracle Cloud Infrastructure supports only the tunnel mode of VPN IPSec and is offered as self-service using the web console

VPN IPSec Tunnels on Oracle Cloud Infrastructure

VPN IPSec service provides a connection between a customer's on-premises network and Oracle Cloud Infrastructure Virtual Cloud Network (VCN). It consists of multiple redundant IPSec tunnels that can use static routes or dynamic routing to route traffic (BGP).

IPSec tunnels connect Dynamic Routing Gateway (DRG) and Customer Premises Equipment (CPE) that are created and attached to the VCN. By default, two IPSec tunnels are created on Oracle Cloud Infrastructure. This provides redundancy in case a tunnel fails. Each tunnel has configuration information (that is, Oracle Cloud Infrastructure endpoint IP address and secret key for authentication) that are configured on your on-prem router.

In this document, the on-prem “role” will be replaced by an Azure Cloud subscription using the Virtual Network Gateway as an IPSec tunnel initiator.



Network concepts OCI

Oracle Cloud Identifier (OCID)

Oracle Cloud Identifier (OCID) is a unique name assigned to every resource you provision on Oracle Cloud Infrastructure. The OCID is an auto-generated string and is used by support engineers to identify your cloud resource when working with any support tickets. Customers can’t choose a preferred value for OCID and can’t modify it for the life of cloud resource. You also use OCIDs extensively when working with REST APIs.

Virtual Cloud Network (VCN)

Virtual Cloud Network (VCN), also known as Cloud Network, is a software-defined network that you set up on the Oracle Cloud Infrastructure platform. Think of VCN as an extension of your on-premises to the cloud, with firewall rules and specific types of communication gateways. A VCN

covers a single, contiguous CIDR (range of IP addresses) block of your choice. A VCN is a regional resource, meaning it covers all the availability domains (ADs) within a region.

Oracle Cloud Infrastructure VCN supports VCN size ranges of /16 to /30 and you can't change the CIDR of a VCN after it's created. The VCN's CIDR should not overlap with your on-premises network. So work with your on-premises network administrator to get an available range of IP addresses (CIDR) that can be used with the VCN.

Subnet

A subnet is a subdivision of a cloud network (VCN). It consists of a contiguous range of IP addresses that don't overlap with other subnets within the same VCN. You build a subnet by specifying the CIDR (range of IP addresses), Availability Domain, and a user-friendly name for the subnet. Originally subnets were designed to cover only one Availability Domain (AD). They were AD-specific and you had to have one subnet per AD in a region. Now subnets can either be AD-specific or regional. Both can coexist within the same architecture.

Subnets have virtual network interface cards (VNIC), which attach to instances. You can label a subnet as private when you create it, which means **VNICs in the subnet can't have a public IP address**. https://en.wikipedia.org/wiki/Private_network https://en.wikipedia.org/wiki/IP_address

A subnet is associated with security lists, route tables, and DHCP (Dynamic Host Configuration Protocol) options to control what traffic is allowed to flow in which direction (DRG or IG for public/private traffic). You can't change security lists or route table attachments once a subnet is built, however you can change the rules of security lists and route tables. Note, you can't alter the CIDR after a subnet is built.

Virtual Network Interface Card (VNIC)

A 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**. If needed, you can add secondary VNICs to an existing instance (in the same AD as the primary AD).

Dynamic Routing Gateway (DRG)

Dynamic Routing Gateway (DRG) is a virtual router that provides a path for private traffic between Oracle Cloud Infrastructure cloud network (VCN) and the on-premises (datacenter) network. DRG is a standalone resource on Oracle Cloud Infrastructure and is designed to give you the full flexibility to attach or detach to a different VCN as per business needs. A DRG is required for both VPN IPSec tunnels and FastConnect virtual circuits. A network administrator might think of the DRG as the VPN headend on their Oracle Cloud Infrastructure service.

Internet Gateway (IG)

Internet Gateway (IG) is an optional virtual router that you can add to a VCN for internet connectivity. It provides internet access to your VCN and is controlled by the route tables and security list configuration on the subnet level. In addition to IG, you must have the following to access internet from the compute instance:

- Routing rule in the route table that points to the IG.
- Appropriate port open in the security list, e.g., Port 80/443 must be opened for Web Server Traffic.

Note: Having an Internet Gateway alone DOES NOT expose your subnet to the internet unless you satisfy the above conditions.

Security Lists

Security lists are virtual firewall rules for your VCN 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 gets attached to the subnet when you create a subnet and you can change the traffic type and destination dynamically.

Example:

An ingress security rule in security lists with source CIDR 10.100.200.0/24 with destination port 22 of TCP protocol allows all ingress traffic from on-premises IP addresses (10.100.200.0/24) to Oracle Cloud Infrastructure instances on port 22 for SSH connection.

Route Table

Route tables are virtual route tables where you configure traffic rules using DRG, IG, NAT Gateway (NAT GW) or Local Private Gateways (LPG). The route table rules provide mapping for the traffic from subnets via gateways to a destination outside the VCN, e. g., private traffic flows using DRG and public traffic flows using IG. You can build multiple route tables within a VCN or use the default route table.

Network concepts Azure

Virtual network

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. You can use VNets to:

- **Communicate between Azure resources**: You can deploy VMs, and several other types of Azure resources to a virtual network, such as Azure App Service Environments, the Azure Kubernetes Service (AKS), and Azure Virtual Machine Scale Sets. To view a complete list of Azure resources that you can deploy into a virtual network, see Virtual network service integration.
- **Communicate between each other**: You can connect virtual networks to each other, enabling resources in either virtual network to communicate with each other, using virtual network peering. The virtual networks you connect can be in the same, or different, Azure regions. For more information, see Virtual network peering.
- **Communicate to the internet**: All resources in a VNet can communicate outbound to the internet, by default. You can communicate inbound to a resource by assigning a public IP address or a public Load Balancer. You can also use Public IP addresses or public Load Balancer to manage your outbound connections.
- **Communicate with on-premises networks**: You can connect your on-premises computers and networks to a virtual network using VPN Gateway or ExpressRoute (we are not covering Express Route in this doc).

Subnet & NIC

A subnet is a range of IP addresses in the virtual network. You can divide a virtual network into multiple subnets for organization and security. Each NIC in a VM is connected to one subnet in one virtual network. NICs connected to subnets (same or different) within a virtual network can communicate with each other without any extra configuration.

When you set up a virtual network, you specify the topology, including the available address spaces and subnets. Select address ranges that don't overlap if the virtual network is connected to other virtual networks or on-premises networks. The IP addresses are private and can't be accessed from the Internet. Azure treats any address range as part of the private virtual network IP address space. The address range is only reachable within the virtual network, within interconnected virtual networks, and from your on-premises location.

Virtual Network Gateway

Azure Virtual Network Gateway serves as the cross-premises gateway connecting your workloads in Azure Virtual Network to your on premises sites. It is required to connect to on premises sites through IPsec S2S VPN tunnels, or through ExpressRoute circuits. For IPsec/IKE VPN tunnels, the gateways perform IKE handshakes, and establish the IPsec S2S VPN tunnels between the Virtual Networks and on premises sites. For ExpressRoute, the gateways advertise the prefixes in your virtual networks via the peering circuits, and also forward packets from your ExpressRoute circuits to your VMs inside your virtual networks.

Notice in this example we will treat OCI as an external on-premise site from Azure perspective, and Azure as an external on-premise site from OCI perspective.

Azure Network Security Group

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

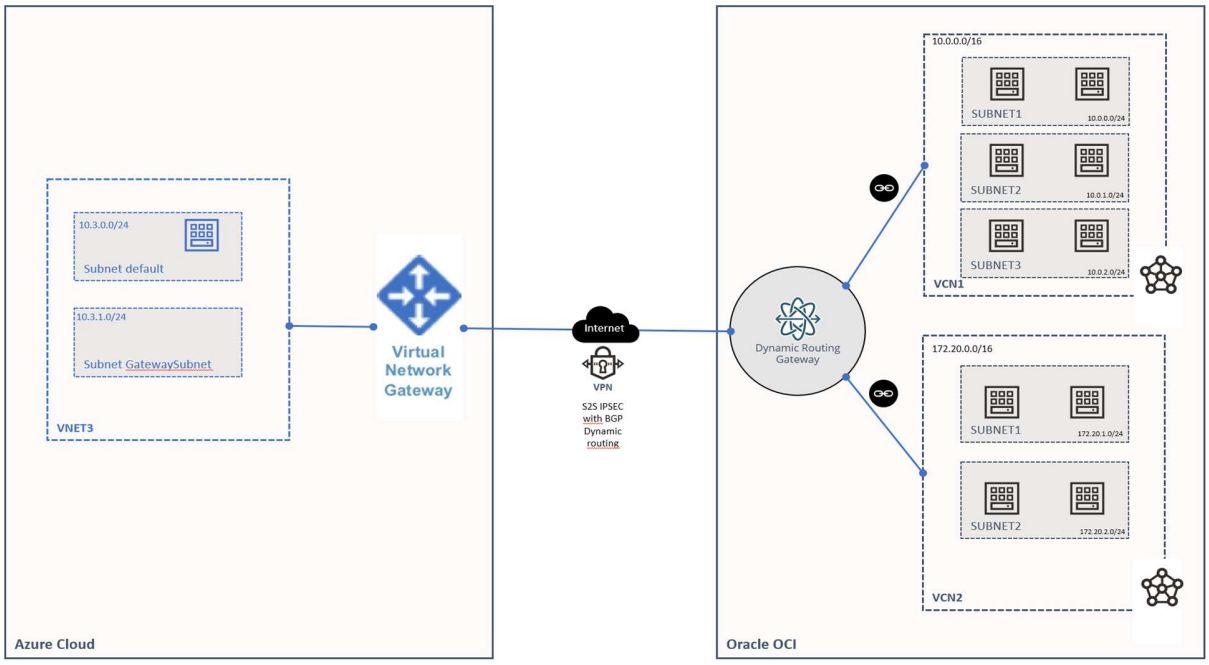
Route Network Traffic

Azure routes traffic between subnets, connected virtual networks, on-premises networks, and the Internet, by default. You can implement either or both of the following options to override the default routes Azure creates:

- Route tables: You can create custom route tables with routes that control where traffic is routed to for each subnet. Learn more about route tables.
- Border gateway protocol (BGP) routes: If you connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute connection, you can propagate your on-premises BGP routes to your virtual networks. Learn more about using BGP with Azure VPN Gateway and ExpressRoute.

S2S VPN IPSec configuration steps

The following picture represents the network diagram of the working sample that will be included in this document as a reference.

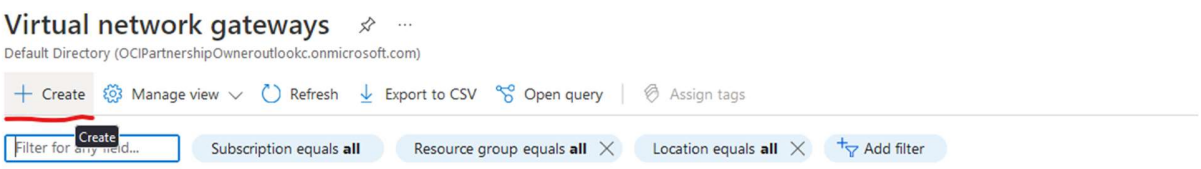


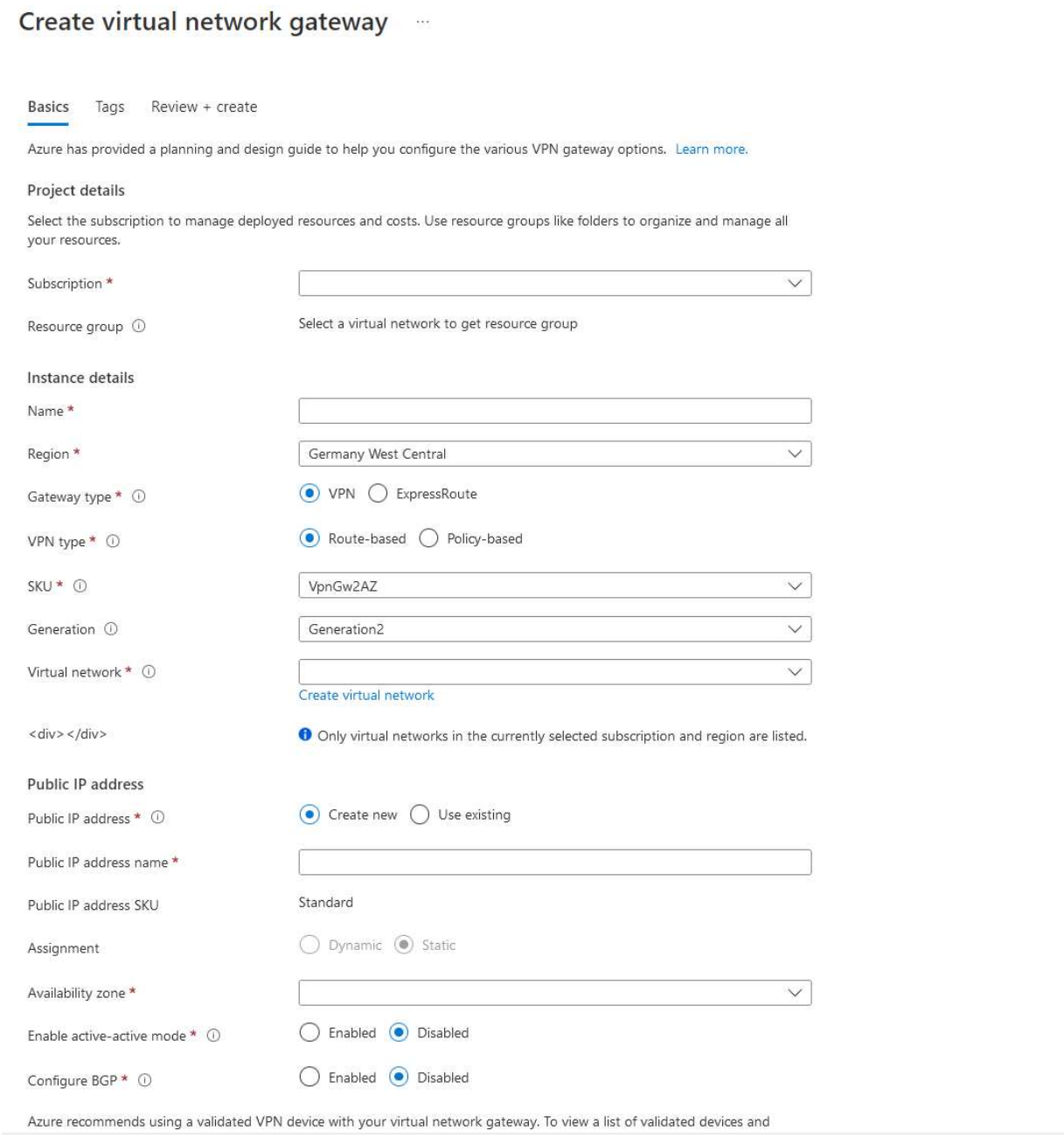
Configuration steps

1. Azure: Create Virtual Network Gateway

   From the main Azure portal, search for **Virtual Network Gateway**. Select it from the search result

   On the next page, click the Create button to create a new Virtual Network Gateway.





You are taken to the Create Virtual Network Gateway page.

- Subscription: Your Azure subscription
- Resource group: The virtual network gateway will be created in the same resource group as the chosen virtual network.
- Name: Give your gateway a name.

- Region: Select your Azure region. The region must be the same as your virtual network.
- Gateway Type: Select VPN.
- VPN type: Select Route-based.
- SKU and Generation: Select a gateway SKU that supports IKEv2 and meets your throughput requirements. For more information on gateway SKUs, see the Azure documentation on VPN Gateway.
- Virtual network: Choose the virtual network for your gateway. This virtual network also needs a gateway subnet.
- Gateway subnet address range: If your virtual network already has a GatewaySubnet, select it. Otherwise, choose an unused address range.
- Public IP address: Your Virtual Network Gateway needs a public IP address. If one has already been created, select it. Otherwise, choose Create new and give your Public IP address a name.
- Enable active-active mode: Leave this option disabled.
- Configure BGP: Select Enabled. Leave this option as disabled if you want to use static routing.
- Autonomous system number (ASN): By default Azure uses BGP ASN 65515. Choose the default.

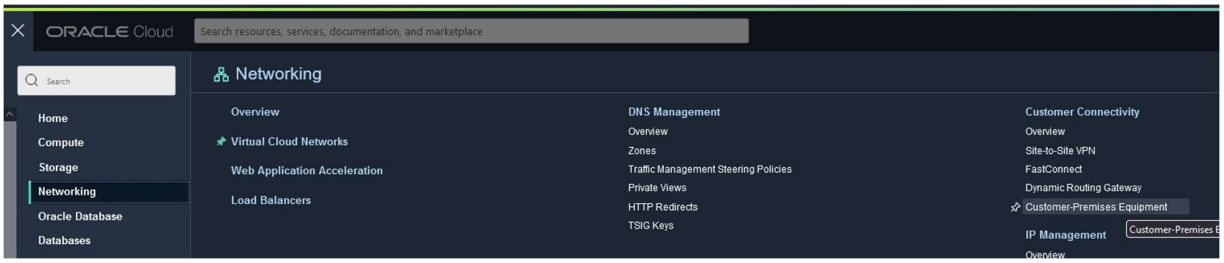
- Custom Azure APIPA BGP IP address: Select a /30 subnet from within 169.254.21.0/24 or 169.254.22.0/24. These addresses are your BGP IP addresses for Azure and OCI. Enter one of the two available IPs from the chosen /30 here. This scenario uses 169.254.21.50 for OCI and 169.254.21.49 for Azure.

When you are finished configuring your Virtual Network Gateway, click the Review + create button, then the Create button on the following page.

After approximately 30-35 mins later, browse to your newly created Virtual Network Gateway and save the public IP address. The IP address is used to create the IPSec connection in OCI.

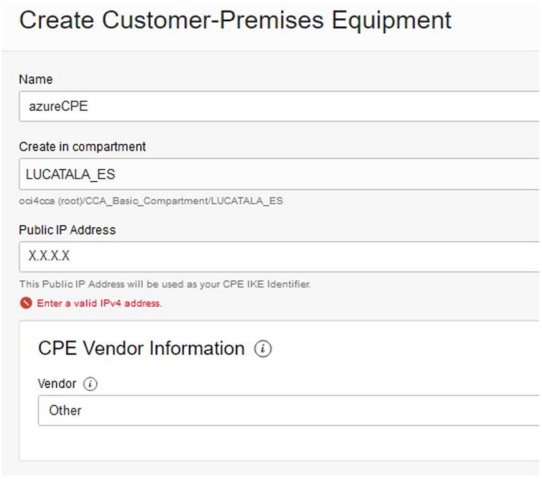
2. OCI: Create CPE object

   Open the navigation menu and click Networking. Under Customer Connectivity, click Customer-Premises Equipment, found in the Customer Connectivity group.



Click Create Customer-Premises Equipment.

- Create in Compartment: select the compartment for the VCN you want.
- Name: A descriptive name for the CPE object. It doesn't have to be unique, and it cannot be changed later in the Console (but you can change it with the API).
- IP Address: Enter the **public IP of your Azure Virtual Network Gateway**. You can find this public IP in the Azure console by browsing to the overview page of the Virtual Network Gateway created in the previous task.
- CPE Vendor: Select Other.



Click **Create CPE**.

3. OCI: Create IPSEC connection

Open the navigation menu and click **Networking**. Under **Customer Connectivity**, click **Site-to-Site VPN**, found in the Customer Connectivity group.

Click **Create IPSec Connection**.

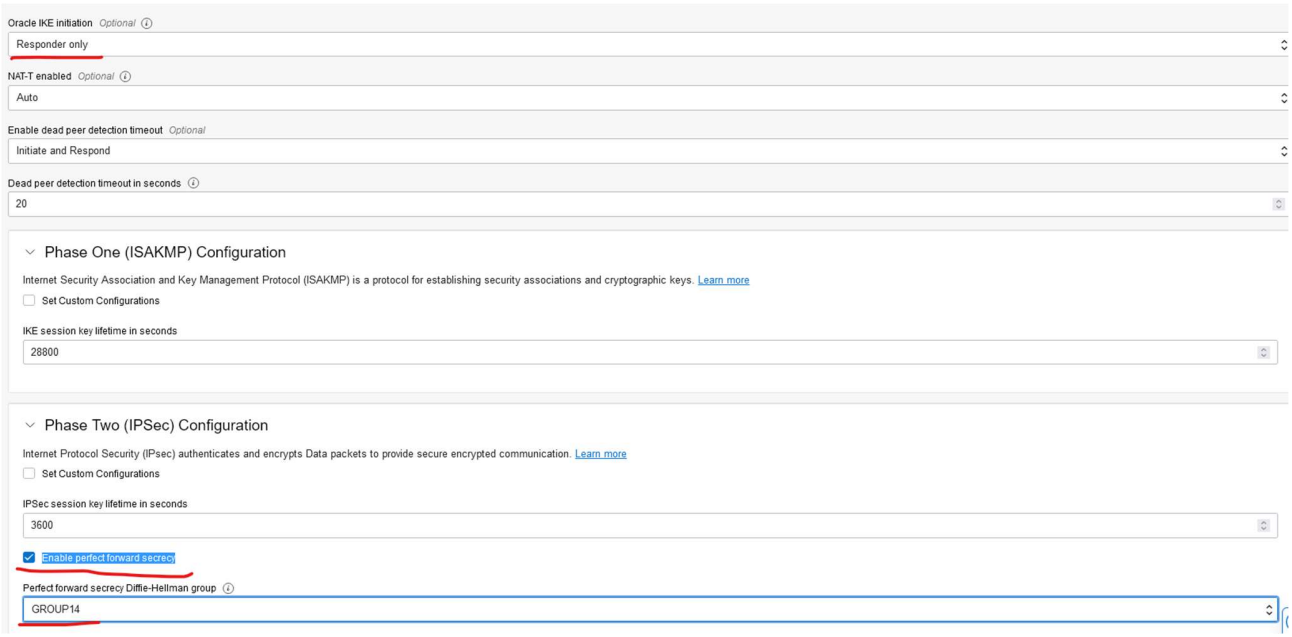
- Create in Compartment: Leave as is (the VCN's compartment).
- Name: Enter a descriptive name for the IPSec connection. It doesn't have to be unique, and you can change it later (in this example ToAzure)
- Customer-Premises Equipment: Select the CPE object that you created earlier, named azureCPE.
- This CPE is behind a NAT device: Leave it **unchecked**
- Dynamic Routing Gateway: Select the DRG that you created earlier.
- Routes to your On-Premises Network: input the default 0.0.0.0/0 (this does NOT mean all the traffic will be routed since BGP is used and OCI will ignore this route).

Now let's setup Tunnel1 (we will use just one tunnel for this example):

- Name: Enter a descriptive **name** for the tunnel 1
- Provide custom shared secret: Leave it blank (we will use the autogenerated share secrets)
- IKE Version: This must be set to **IKEv2**
- Routing type: **BGP**
- BGP ASN: Input the **BGP ASN** used by Azure. The Azure BGP ASN is configured during Step 3 of section Azure - Create VPN Gateway. This scenario uses the default Azure BGP ASN of **65515**.
- IPv4 Inside Tunnel Interface - **CPE**: The **BGP IP** address used by **Azure**. Use full CIDR notation for this IP address. The Azure BGP IP address is configured during Step 3 of section Azure - Create VPN Gateway. In this example **169.254.21.49/30**
- IPv4 Inside Tunnel Interface - **Oracle**: The **BGP IP** address used by **OCI**. Use full CIDR notation for this IP address. This IP address is the other leftover usable IP from the chosen /30. In this example **169.254.21.50/30**

Click into “Show Advanced Options”

- Oracle IKE initiation: **Set it as RESPONDER ONLY.** If you leave it by default (Initiator or Responder), then, if OCI initiates the tunnel first, Azure will reject the Phase 2 proposals from OCI, and Azure will never play the role of initiator.
- Phase Two (IPSec) Configuration: Click there and **CHECK Enable perfect forward secrecy**, choosing the Diffie-Hellman group 14. The default DH group 5 is not available in Azure.



Tunnel2: Set it as Static Routing (we will be ignoring tunnel2)

Click **Create IPSec Connection**.

4. OCI - Save Site-to-Site VPN IP Address and Shared Secret

After your IPSec connection has been provisioned, save the **Site-to-Site VPN IP address** to use as the CPE IP in the Azure portal and the shared secret for the tunnel.

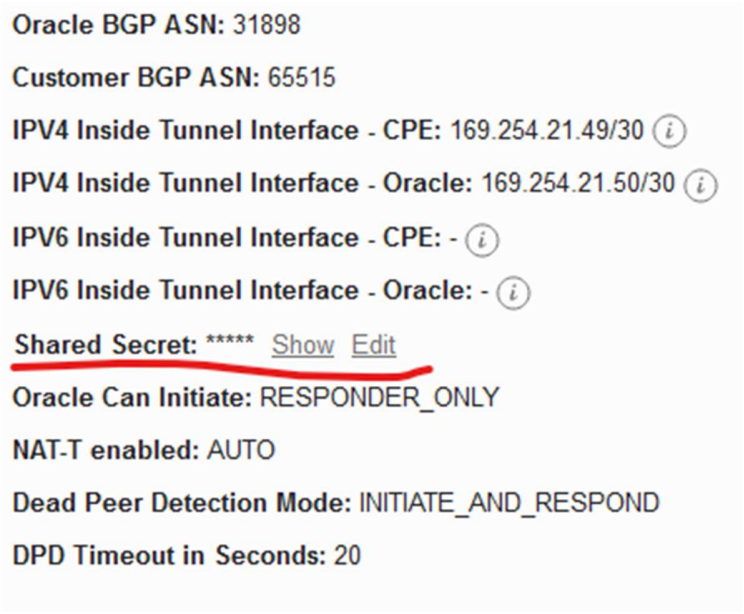
- Browse to your IPSec connection in the OCI Console.
- Choose which tunnel to use as your primary. Save the Site-to-Site VPN IP address of that tunnel. Next, click the tunnel name of that tunnel to be taken to the tunnel view.


Tunnels *in* LUCATALA_ES *Compartment*

Name	Lifecycle State	IPSec Status	IPV4 BGP Status	IPV6 BGP Status	Oracle VPN IP Address	Routing Type
ipsectunnel20220707163847-2	Available	Down	-	-	193.122.49.8	Static Routing
ipsectunnel20220707163847-1	Available	Down	Down	Down	193.122.4.1[illegible]	BGP Dynamic Routing

Click in the **tunnel Name**, and in the next page, **click on Share Secret Show**

Save it. The shared secret is used to complete the IPSec VPN configuration in Azure.


Oracle BGP ASN: 31898

Customer BGP ASN: 65515

IPV4 Inside Tunnel Interface - CPE: 169.254.21.49/30

IPV4 Inside Tunnel Interface - Oracle: 169.254.21.50/30

IPV6 Inside Tunnel Interface - CPE: -

IPV6 Inside Tunnel Interface - Oracle: -

Shared Secret: ***** Show Edit

Oracle Can Initiate: RESPONDER_ONLY

NAT-T enabled: AUTO

Dead Peer Detection Mode: INITIATE_AND_RESPOND

DPD Timeout in Seconds: 20

5. Azure - Create Local Network Gateway

From the main Azure portal, search for **Local Network Gateway**. Select it from the search results.

On the next page, click the **Create** button to create a **Local Network Gateway**.

- Subscription: Your Azure Subscription
- Resource Group: The resource group you are working with.
- Region: Select your Azure region. The region must be the same as your virtual network and Virtual Network Gateway.
- Name: Give your local network gateway a name. In this example LNGOCI33
- IP Address: Input the **saved OCI VPN IP address for Tunnel 1**.
- Address space: Leave blank

Next: Advanced>

- Configure BGP Settings: Select this check box.
- Autonomous system number (**ASN**): Input the **OCI BGP ASN of 31898**.
- BGP peer IP address: The OCI BGP IP address. The same IP address used for IPV4 Inside Tunnel Interface - Oracle in Step 4 of OCI - Create IPSec Connection. In this example 169.254.21.50 (without /30 mask)

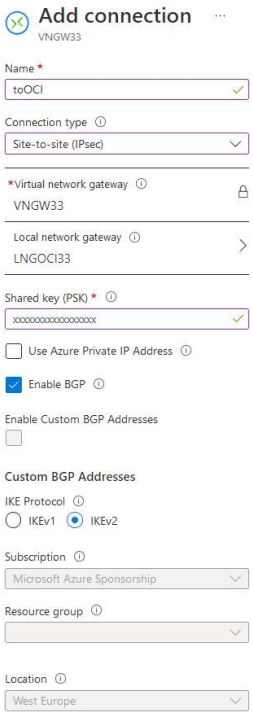
6. Azure – Create VPN Connection

Browse to your previously created **Virtual Network Gateway**. From the left-hand menu, click **Connections**, then the Add button to **add a connection**.

- Name: Give your connection a **name**.
- Connection type: **Select Site-to-site (IPsec)**
- Virtual network gateway: Leave the default (current VNET gateway)
- Local network gateway: Select the **previously created local network gateway**.
- Shared key (PSK) - Input the **shared secret from your OCI tunnel**. Refer to OCI - Save Site-to-Site VPN IP Address and Shared Secret if you need to identify where the shared key is found in the OCI Console.
- Enable BGP: Check this box.
- IKE Protocol: Select IKEv2

Leave all other options as default. When you are finished configuring your VPN connection, click the OK button at the bottom of the page.

After a couple minutes, Azure will complete provisioning the new VPN connection and your IPSec VPN between Azure and OCI will come up.



7. Verification

Browse to your IPSec connection in OCI and the Virtual Network Gateway connection in Azure to verify status of the tunnel.

Your OCI tunnel under **IPSec connection displays** Up for IPSec status to confirm an operational tunnel.

The IPV4 **BGP Status also displays Up** indicating an established BGP session.

The **connection status** under the Virtual Network Gateway for this tunnel displays **Connected** to confirm an operational tunnel.