

[Subject]

[Title]

**v0.1**

**Document Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| ***Version No*** | ***Date*** | ***Author*** | ***Comments*** |
| v0.1 | 26 Apr 2020 |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Sign-Off Details**

|  |  |  |
| --- | --- | --- |
| ***Name*** | ***Position*** | ***Comments*** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Distribution List**

|  |  |  |
| --- | --- | --- |
| ***No*** | ***Name*** | ***Note*** |
| 1 |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Confidentiality**

This document is confidential and contains proprietary information and intellectual property of eAppSys Info Solutions Private Limited.

eAppSys Info Solutions Private Limited is providing this information under the agreement that the recipient of this document or any other additional information / files will not use it or disclose it for any purposes other than the intended purpose mentioned in this document.

Neither this document nor any of the information contained herein may be reproduced or disclosed under any circumstances without the express written permission of eAppSys Info Solutions Private Limited.

Please be aware that disclosure, copying, distribution or use of this document and the information contained therein is strictly prohibited

**Table of Contents**

[1 Introduction 1](#_Toc39068872)

[1.1 eAppSys Limited 1](#_Toc39068873)

[1.2 Project Background 1](#_Toc39068874)

[1.3 Purpose of the document 1](#_Toc39068875)

[1.4 Intended Audience 1](#_Toc39068876)

# Introduction

## eAppSys Limited

eAppSys Limited was founded in 2010 in the United Kingdom as an Oracle Solution Provider by a team of Oracle experts.

Today we are a leading Systems Integrator focused exclusively on supporting the core enterprise application systems within Oracle, such as Oracle e-Business Suite and HCM. As an Oracle Platinum Partner, we are able to provide Oracle’s business solutions, consulting and services from strategic locations in the UK and India.

We specialise in working closely with strategic enterprises that are re-engineering their processes and are adapting to today’s dynamic business environment. eAppSys Limited provides a complete range of services by leveraging our domain business expertise and our strategic alliances with leading technology and solution providers. We work globally with partners and new technologies in providing solutions, products and services.

Our approach is a unique quality-based methodology tailored to meet customer requirements. Our Global Delivery Model (GDM) is based on the principle of providing solutions and services using resources at the location where the best talent is available, where it makes the best economic sense and with the least amount of acceptable risk. Using small integrated teams to deliver projects from EBS process implementation to reporting with high quality people, products, processes and services we consistently exceed customer expectation and achieve excellent customer satisfaction ratings, which has resulted in strategic long-term relationships with many of our current Customers.

## Project Background

## Purpose of the document

## Intended Audience

# Site-to-Site VPN Overview

## Definition

Site-to-Site VPN provides a site-to-site IPSec connection between your on-premises network and your Virtual Cloud Network (VCN). The IPSec protocol suite encrypts IP traffic before the packets are transferred from the source to the destination and decrypts the traffic when it arrives. Site-to-Site VPN was previously referred to as VPN Connect and IPSec VPN.

## Required Knowledge

Typically the following types of personnel are involved in setting up Site-to-Site VPN with Oracle Cloud Infrastructure:

* **Dev Ops team member** (or similar function) who uses the Oracle Cloud InfrastructureConsole to set up the cloud components required for the virtual network and Site-to-Site VPN.
* **Network engineer** (or similar function) who configures the customer-premises equipment (CPE) device with information provided by the Dev Ops team member.

## About Oracle IPSec Connection

In general, an IPSec connection can be configured in the following modes:

* **Transport mode:** IPSec encrypts and authenticates only the actual payload of the packet, and the header information stays intact.
* **Tunnel mode (supported by Oracle):** IPSec encrypts and authenticates the entire packet. After encryption, the packet is then encapsulated to form a new IP packet that has different header information.

Oracle Cloud Infrastructure supports only the tunnel mode for IPSec VPNs.

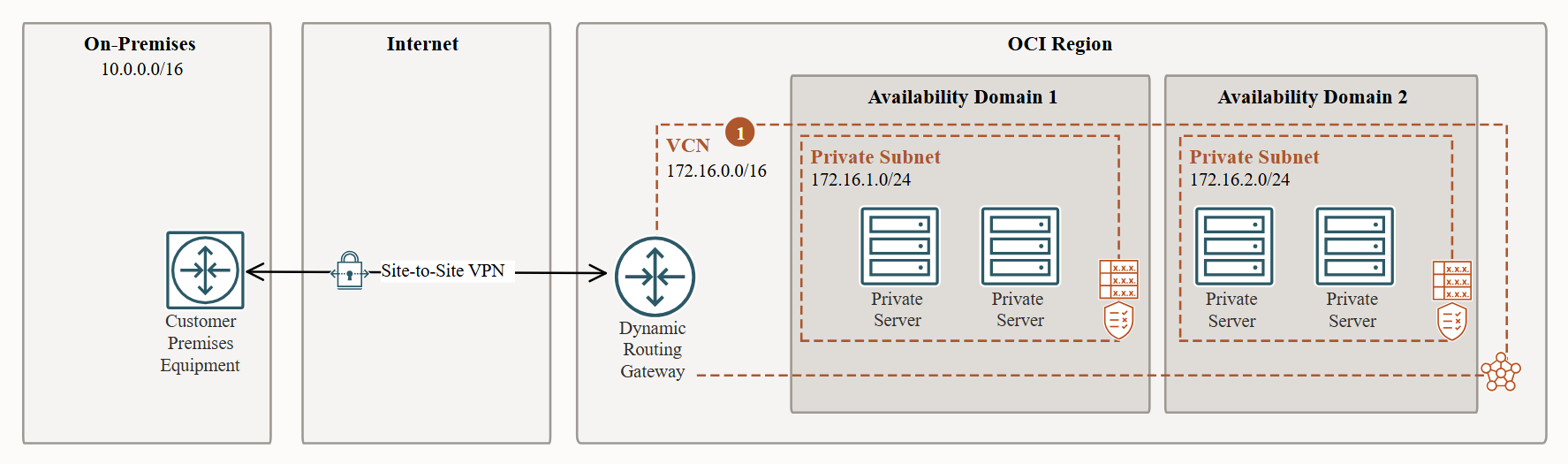
## Routing for Site-to-Site VPN

The following three routing types are available, and you choose the routing type separately *for each IPSec tunnel* in Site-to-Site VPN:

* **BGP dynamic routing:** The available routes are learned dynamically through BGP. The DRG dynamically learns the routes from the on-premises network. On the Oracle side, the DRG advertises the VCN's subnets.
* **Static routing:** When you set up the IPSec connection to the DRG, you specify the particular routes to the on-premises network that you want the VCN to know about. You also must configure the CPE device with static routes to the VCN's subnets. These routes aren't learned dynamically.
* **Policy-based routing:** When you set up the IPSec connection to the DRG, you specify the particular routes to the on-premises network that you want the VCN to know about. You also must configure the CPE device with static routes to the VCN's subnets. These routes aren't learned dynamically.

## Site-to-Site VPN Components

When you set up Site-to-Site VPN for your VCN, you must create several Networking components. You can create the components with either the Console or the API. See the following diagram and description of the components.



**CPE Object**

At your end of Site-to-Site VPN is the actual device in your on-premises network (whether hardware or software). The term *customer-premises equipment (CPE)* is commonly used in some industries to refer to this type of on-premises equipment. When setting up the VPN, you must create a *virtual representation* of the device. Oracle calls the virtual representation a CPE, but this documentation typically uses the term *CPE object* to help distinguish the virtual representation from the actual CPE device. The CPE object contains basic information about your device that Oracle needs. A single CPE object public IP can have up to 8 IPSec connections.

**Dynamic Routing Gateway (DRG)**

At Oracle's end of Site-to-Site VPN is a virtual router called a dynamic routing gateway, which is the gateway into your VCN from your on-premises network. Whether you're using Site-to-Site VPN or Oracle Cloud Infrastructure FastConnect private virtual circuits to connect your on-premises network and VCN, the traffic goes through the DRG. For more information, see Dynamic Routing Gateways.

A network engineer might think of the DRG as the VPN headend. After creating a DRG, you must attach it to your VCN, using either the Console or API. You must also add one or more route rules that route traffic from the VCN to the DRG. Without that DRG attachment and the route rules, traffic does not flow between your VCN and on-premises network. At any time, you can detach the DRG from your VCN but maintain all the remaining VPN components. You can then reattach the DRG, or attach it to another VCN.

**IPSec Connection**

After creating the CPE object and DRG, you connect them by creating an IPSec connection, which you can think of as a parent object that represents the Site-to-Site VPN. The IPSec connection has its own **OCID**. When you create this component, you configure the type of routing to use for each IPSec tunnel, and you provide any related routing information. A single CPE object public IP can have up to 8 IPSec connections.

**TUNNEL**

An IPSec tunnel is used to encrypt traffic between secure IPSec endpoints. Oracle creates two tunnels in each IPSec connection for redundancy. Each tunnel has its own **OCID**. Oracle recommends that you configure your CPE device to support both tunnels in case one fails or Oracle takes one offline for maintenance. Each tunnel has configuration information that your network engineer needs when configuring your CPE device. This information includes an IP address and shared secret, as well as ISAKMP and IPSec parameters. You can use the CPE Configuration Helper to gather the information that the network engineer needs

## Process

Here's the overall process for setting up Site-to-Site VPN:

1. **Complete the tasks listed in**[**Before You Get Started**](https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/settingupIPsec.htm#Before)**.**
2. **Set up Site-to-Site VPN components**(instructions in [Example: Setting Up a Proof of Concept Site-to-Site VPN](https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/settingupIPsec.htm#example_poc)):
   1. Create your VCN.
   2. Create a DRG.
   3. Attach the DRG to your VCN.
   4. Create a route table and route rule for the DRG.
   5. Create a security list and required rules.
   6. Create a subnet in the VCN.
   7. Create a CPE object and provide your CPE device's public IP address.
   8. Create an IPSec connection to the CPE object and provide required routing information.
3. **Use the CPE Configuration Helper:** Your network engineer must configure your CPE device with information that Oracle provides during the previous steps. The CPE Configuration Helper generates the information for your network engineer. For more information, see [Using the CPE Configuration Helper](https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/CPEconfigurationhelper.htm#Using_the_CPE_Configuration_Helper) and also [CPE Configuration](https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/configuringCPE.htm#CPE_Configuration).
4. **Have your network engineer configure your CPE device.**
5. **Validate connectivity.**

## Advantages and Disadvantages

ADVANTAGES

* **1. Secure Communication**

Uses IPsec protocols to encrypt data, ensuring secure communication between on-premises networks and OCI.

* **2. Cost-Effective**

No need for additional hardware as it can be set up with existing on-premises VPN-capable devices and OCI's built-in VPN service.

* **3. High Availability**

OCI VPN Connect supports redundant connections using multiple tunnels, ensuring high availability and reliability.

* **4. Flexibility**

Supports a wide range of on-premises VPN devices from major vendors like Cisco, Palo Alto Networks, and Juniper.

* **5. Quick Setup**

Relatively fast to configure compared to other network solutions like a private physical connection.

* **6. Scalability**

Allows you to connect multiple on-premises networks to OCI regions and virtual cloud networks (VCNs).

* **7. Compliance**

Helps meet compliance requirements by securely extending on-premises infrastructure into the cloud.

* **8. Integration with OCI Services**

Easily integrates with other OCI networking services like FastConnect, NAT Gateway, and Load Balancer for hybrid architecture.

DISADVANTAGES

* **1. Performance Limitations**

Bandwidth is dependent on your internet connection and can be lower compared to FastConnect, which offers dedicated, higher-bandwidth links.

* **2. Latency**

Internet-based communication can introduce latency, which may impact performance for latency-sensitive applications.

* **3. Complex Troubleshooting**

Identifying and resolving connectivity issues may require in-depth knowledge of both OCI and the on-premises VPN device.

* **4. Single Point of Failure (if not redundant)**

If redundancy is not implemented, a failure in the VPN tunnel or internet connection can disrupt connectivity.

* **5. Operational Overhead**

Requires monitoring and maintaining the VPN tunnels, including dealing with rekeying, configuration updates, and certificate management.

* **6. Limited by Public Internet**

Since it relies on the public internet, the connection is subject to disruptions caused by ISP issues or DDoS attacks.

* **7. Security Risks**

While encrypted, using the public internet still poses some inherent security risks compared to private links like FastConnect.

* **8. Dependency on Vendor Support**

Compatibility issues with older or less common VPN devices might require vendor support or additional configurations.

## Information to be communicated with Clients

* **1. Tunnel Endpoint Information**

**OCI VPN IP Addresses:**  
Provide the **public IP addresses** of the OCI VPN endpoints. Typically, OCI provides two IP addresses (one for each tunnel) for high availability.

* **2. Tunnel Configuration Details**

**Pre-Shared Key (PSK):**  
The shared secret key used for IPsec authentication between your VPN and the client's device. This key is auto-generated by OCI or specified by you during configuration.

**Tunnels' Status:**  
Indicate which tunnel(s) are active, if applicable, or suggest using both for redundancy.

* **3. IPsec Configuration Parameters**

Provide details about the IPsec configuration for the tunnels, including:

* + **Encryption Algorithms:** e.g., AES-256
  + **Hashing Algorithms:** e.g., SHA-256
  + **Diffie-Hellman Group:** e.g., Group 14
  + **IKE Version:** IKEv1 or IKEv2 (as per your setup)
  + **Lifetime:** Lifetime of the security association (e.g., 3600 seconds for IKE SA and IPsec SA)
* **4. OCI Virtual Cloud Network (VCN) and Subnet Information**

**VCN CIDR Block:**  
Share the CIDR block of your VCN (e.g., 10.0.0.0/16) that the client will access.

**Subnets to Route:**  
Specify which subnets within the VCN are accessible via the VPN.

* **5. Routing Information**

**On-Premises Subnet(s):**  
Share the client's subnet(s) that are allowed to access OCI resources.

**Static Routes (if applicable):**  
Provide the static routes configured on OCI for your tunnels.

**Dynamic Routing (if applicable):**  
If using BGP for dynamic routing, provide:

* + **BGP IP Addresses:** The BGP peer IP addresses for each tunnel.
  + **Autonomous System Number (ASN):** OCI's ASN and any client-specified ASN.
* **6. Connectivity Validation Information**

**OCI IPs for Testing:**  
Share an OCI-hosted IP address or resource (e.g., pingable instance) for connectivity testing.

**Allowed Ports/Protocols:**  
Mention any specific ports or protocols allowed through the tunnel (e.g., port 22 for SSH).

## Information Clients need to communicate with us

* **1. On-Premises VPN Gateway Information**

**Public IP Address:**  
The public-facing IP address of their on-premises VPN gateway (e.g., a firewall or router) that will connect to OCI's VPN tunnel.

**Device Type and Model:**  
The make and model of their VPN-capable device (e.g., Cisco ASA, Fortinet, Palo Alto Networks) to ensure compatibility.

* **2. On-Premises Subnet Information**

**Subnets or CIDR Blocks:**  
The range(s) of IP addresses in their network that should communicate with OCI. Example: 192.168.1.0/24.

**Static Routes (if applicable):**  
Any specific routes they want to advertise to OCI.

* **3. Security Protocols and Configuration**

**IPsec/IKE Configuration Preferences:**  
Confirm their supported encryption and hashing algorithms, such as:

* + **Encryption Algorithm:** AES-128 or AES-256
  + **Hash Algorithm:** SHA-1 or SHA-256
  + **Diffie-Hellman Group:** (e.g., Group 5, 14, or 19)
  + **IKE Version:** Specify whether they support IKEv1 or IKEv2.

**Pre-Shared Key (PSK):**  
If they prefer a specific PSK, they should provide it, or confirm they’ll use the auto-generated one.

* **4. Routing and Connectivity**

**Routing Preference:**  
Whether they will use static routing or dynamic routing via BGP. If using BGP:

* + Provide their **ASN (Autonomous System Number)**.
  + Share their **BGP Peer IP Address** to establish dynamic routing.
* **5. Firewall and NAT Information**

**Firewall Rules:**  
Confirm that their firewall allows the required ports and protocols for IPsec:

* + UDP 500 (IKE)
  + UDP 4500 (NAT Traversal)
  + ESP (IPsec Protocol 50)
  + ICMP (for testing connectivity)

**NAT Information:**  
If their VPN device is behind NAT, they must confirm NAT-T (NAT Traversal) is enabled and provide any additional NAT details.