ORACLE

OIC and OCI API Gateway

Oracle Cloud Emerging Tech

Pattern Definition Document

November, 2021 | Version 0.1

TABLE OF CONTENTS

1 DOCUMENT CONTROL

1.1 Version Control

Version	Author	Date	Comment
0.1	Harris Qureshi	November, 2021	Initial version

1.2 Abbreviation List

Abbreviation	Meaning
OCI	Oracle Cloud Infrastructure
OIC	Oracle Integration Cloud
API	Application Programming Interface
APIGW	OCI API Gateway
PaaS	Platform as a service
IaaS	Infrastructure as a service

2 NAME

Oracle Integration Cloud and OCI API Gateway

3 PROBLEM

Oracle Integration Cloud (OIC) is an Oracle managed iPaaS platform that is used by many customers to meet their application integration requirements. Customers build Rest Integrations and APIs that are called by various consumers from internal applications to external business partners. Customers have requirements to provide more control on these Rest APIs.

4 SOLUTION

It is recommended to use OCI API Gateway in front of Oracle Integration Cloud to meet various requirements from restricting access to rate limiting and applying various policies.

OCI API Gateway service enables to publish APIs with private endpoints that are accessible from within your network, and which you can expose with public IP addresses if you want them to accept internet traffic. The endpoints support API validation, request and response transformation, CORS, authentication and authorization, and request limiting.

5 ARCHITECTURE

5.1 Scenario 1

Customer wants to apply policies like rate limiting, CORS, Header validation on the backend rest APIs exposed by Oracle Integration Cloud. Customer is okay to traverse the traffic via public internet.

In this scenario, you can setup OCI API Gateway in a public subnet and apply these polices on the back end rest APIs exposed by Oracle Integration Cloud.

[Figure 1] OCI API Gateway and Oracle Integration Cloud over Public Subnet.

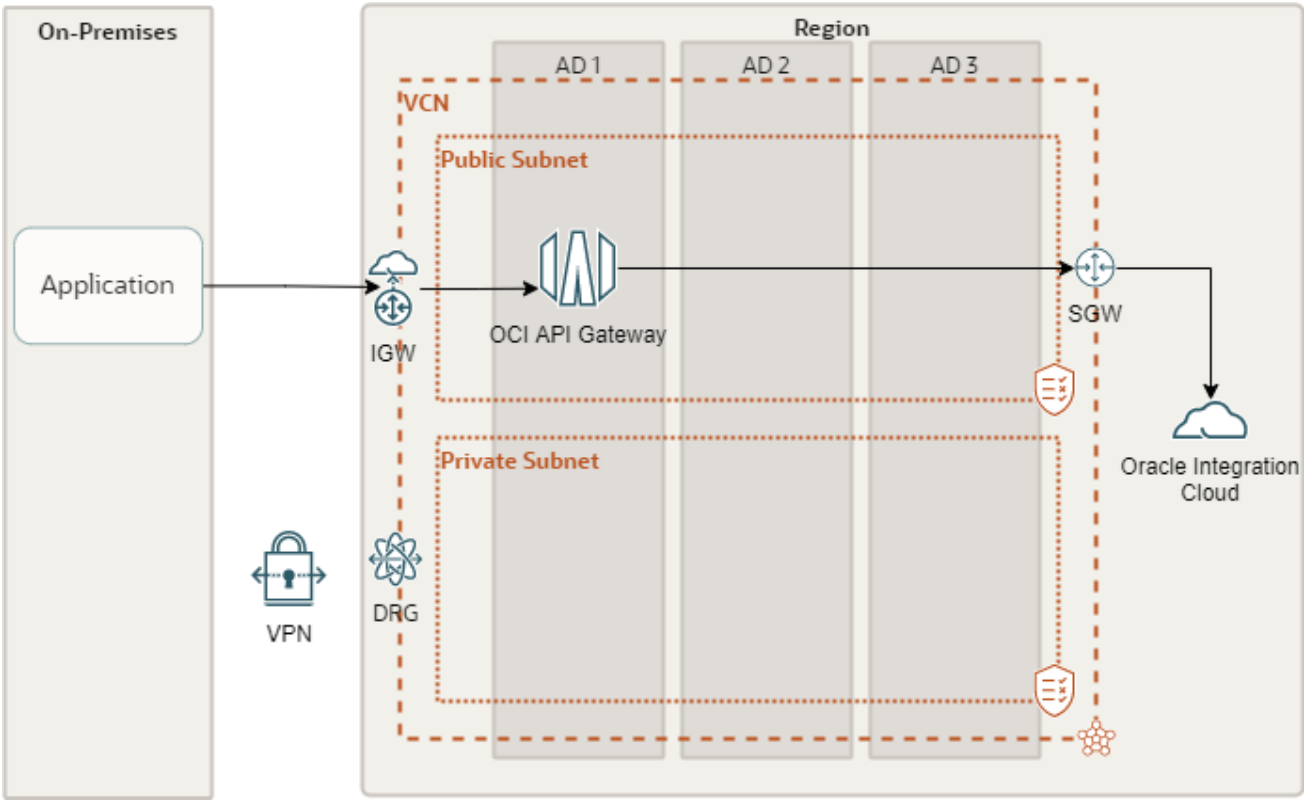

Figure 1: OCI API Gateway and Oracle Integration Cloud over Public Subnet

5.2 Scenario 2

Customer does not want traffic to flow through public internet. Oracle Integration Cloud a public service, if you connect directly all traffic flows through public internet. If customer wishes to invoke a Rest API on OIC from its network via VPN/Fast Connect and ensure private connectivity.

In this scenario, you can setup OCI API Gateway in a private subnet, connect OCI VCN with customer network (on-prem/third party cloud) via IPsec VPN or Fast Connect. OCI API Gateway hosted in a private subnet connects to Oracle Integration Cloud via Service Gateway. In this manner all traffic from Customer Application to OIC traverses through private network.

[Figure 2] OCI API Gateway and Oracle Integration Cloud over Private Subnet.

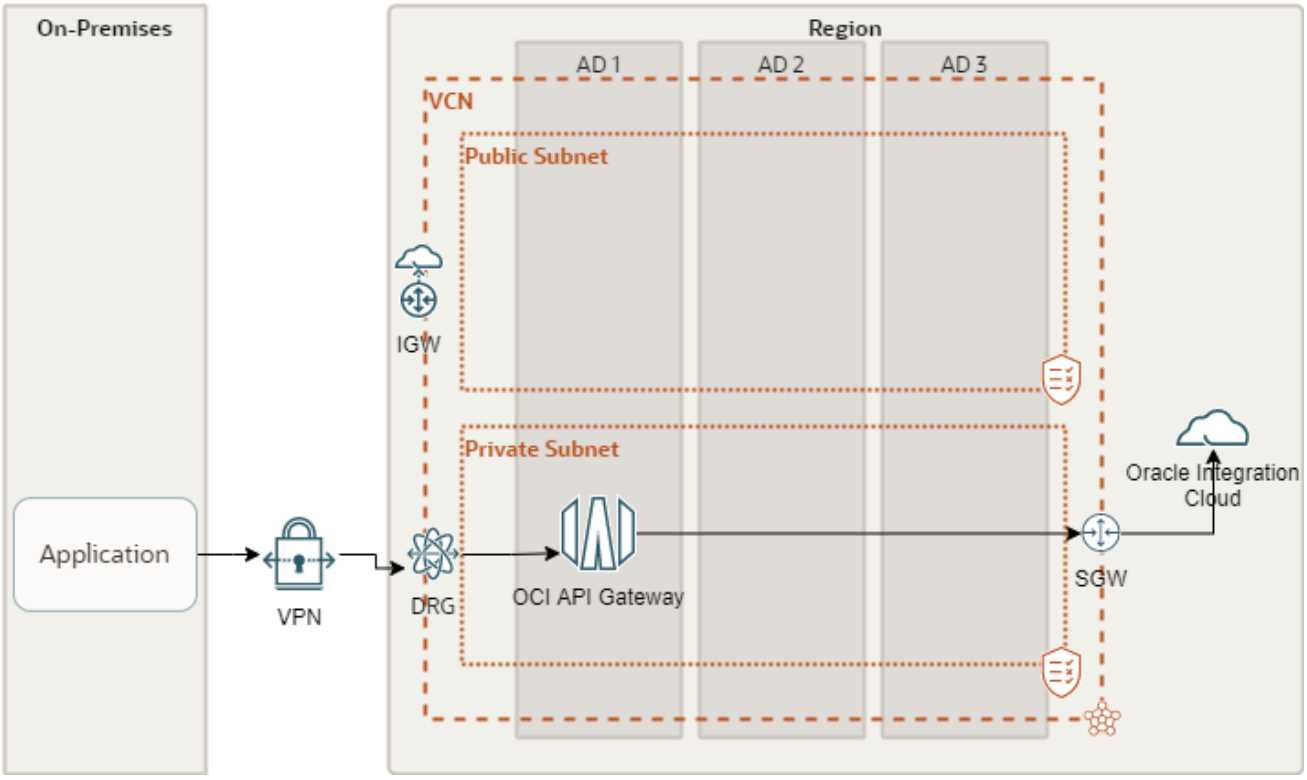

Figure 2: OCI API Gateway and Oracle Integration Cloud over Private Subnet

5.3 Architecture Components

The architecture has the following components

Region :

An Oracle Cloud Infrastructure region is a localized geographic area that contains one or more data centres, called availability domains. Regions are independent of other regions, and vast distances can separate them (across countries or even continents).

Availability domains

Availability domains are standalone, independent data centers within a region. The physical resources in each availability domain are isolated from the resources in the other availability domains, which provides fault tolerance. Availability domains don't share infrastructure such as power or cooling, or the internal availability domain network. So, a failure at one availability domain is unlikely to affect the other availability domains in the region.

Virtual cloud network (VCN) and subnets A VCN is a customizable, software-defined network that you set up in an Oracle Cloud Infrastructure region. Like traditional data center networks, VCNs give you complete control over your network

environment. A VCN can have multiple non-overlapping CIDR blocks that you can change after you create the VCN. You can segment a VCN into subnets, which can be scoped to a region or to an availability domain. Each subnet consists of a contiguous range of addresses that don't overlap with the other subnets in the VCN. You can change the size of a subnet after creation. A subnet can be public or private.

Compartment

Compartments are cross-region logical partitions within an Oracle Cloud Infrastructure tenancy. Use compartments to organize your resources in Oracle Cloud, control access to the resources, and set usage quotas. To control access to the resources in a given compartment, you define policies that specify who can access the resources and what actions they can perform.

Dynamic routing gateway (DRG)

The DRG is a virtual router that provides a path for private network traffic between a VCN and a network outside the region, such as a VCN in another Oracle Cloud Infrastructure region, an on-premises network, or a network in another cloud provider.

Service gateway

The service gateway provides access from a VCN to other services, such as Oracle Cloud Infrastructure Object Storage. The traffic from the VCN to the Oracle service travels over the Oracle network fabric and never traverses the internet.

Internet gateway

The internet gateway allows traffic between the public subnets in a VCN and the public internet.

Integration

Oracle Integration is a fully managed service that allows you to integrate your applications, automate processes, gain insight into your business processes, and create visual applications.

OCI API Gateway

The API Gateway service enables you to publish APIs with private endpoints that are accessible from within your network, and which you can expose to the public internet if required. The endpoints support API validation, request and response transformation, CORS, authentication and authorization, and request limiting.

5.4 Recommendations

Use the following recommendations as a starting point. Your requirements might differ.

VCN

When you create a VCN, determine the number of CIDR blocks required and the size of each block based on the number of resources that you plan to attach to subnets in the VCN. Use CIDR blocks that are within the standard private IP address space. Select CIDR blocks that don't overlap with any other network (in Oracle Cloud Infrastructure, your on-premises data center, or another cloud provider) to which you intend to set up private connections.

Subnets When you design the subnets, consider your traffic flow and security requirements. Attach all the resources within a specific tier or role to the same subnet, which can serve as a security boundary.

Security List

A security list acts as a virtual firewall for your OCI API Gateway, with ingress and egress rules that specify the types of traffic allowed in and out. You configure your security lists at the subnet level, which means that all resources in a given subnet are subject to the same set of security list rules. By setting up the ingress and egress rules you can control granular level of access e.g. what CIDR and IP Addresses can have access to your APIs deployed on the OCI API Gateway.

High Availability

To ensure high availability, you can only create API gateways in regional subnets (not AD-specific subnets). The API Gateway service is regional in scope and fault-tolerant across availability domains (in multiple-AD regions), and fault domains (in single AD regions). In multiple-AD regions, the API Gateway service automatically selects an active availability domain to terminate the API gateway endpoint. Note that depending on the source and destination of the traffic, traffic might be routed across availability domains. If an availability domain or fault domain fails, the API Gateway service automatically

handles failover and routes traffic to a functioning availability domain or fault domain.

Restrict Oracle Integration Network Access

Restrict the networks that have access to your Oracle Integration instance by configuring an allowlist (formerly a whitelist). Only users from the specific IP addresses, Classless Inter-Domain Routing (CIDR) blocks, and virtual cloud networks that you specify can access the Oracle Integration instance. If all traffic to Oracle Integration is in the form of REST API calls, you can setup OCI API Gateway in front and include OCI APIGW address in the allowlist. This will restrict direct access to Oracle Integration Cloud instance and all access will be via OCI API Gateway.

6 REFERENCE ARTICLES & DOCUMENTATIONS

- *A Simple Guide to Setup API Gateway with Oracle Integration Cloud*
- *Restrict Access to an OIC Instance*
- *Private connectivity to Oracle Integration Cloud next generation*
- *OIC & OCI API Gateway Integration: Quick and Easy*