Oracle Field Service

Connectivity Options

Overview and procedures to connect using Oracle Cloud Infrastructure

Version 1.0

Table of Contents

Introduction

The secure and scalable architecture of Oracle Field Service is built on Generation 2 Oracle Cloud Infrastructure (OCI), which lets your business run without interruption. OCI is a set of complementary cloud services that improve performance and security while reducing costs for your enterprise and performance-intensive applications. Oracle Cloud Infrastructure provides a robust, scalable, secure, highly available, and cost-effective cloud platform to meet the needs of your business, combining the utility of the public cloud with the granular control and predictable performance of on-premises enterprise infrastructure.

From a high-level perspective, Oracle Field Service is represented in each geographical region by two active data centers; one of them plays the role of home regional data center and the other one as standby. This approach works well for enterprise customers that require geographically distributed regions for business continuity, disaster protection, and regional compliance requirements.

This *Oracle Field Service Connectivity Options* guide describes typical use cases for connecting your users and systems, including mobile connectivity using the public internet and connectivity from your on-premises networks to Oracle Cloud. This guide also includes simple, redundant, and complex use cases to help you deploy various connectivity solutions. Although it doesn’t provide step-by-step instructions, it does provide references to documentation where those steps are outlined. If you're using this guide, we're assuming that you have cloud security knowledge and an understanding of integration architecture. You can find the high-level Oracle Cloud Infrastructure documentation at https://docs.cloud.oracle.com/en-us/iaas/Content/GSG/Concepts/baremetalintro.htm, and we’ll call out specific sections in the appropriate places within this guide.

Please note that your use of this *Oracle Field Service Connectivity Options* guide is subject to the Terms of Use attached to this document.

Glossary

Before getting started, here are some terms and their definitions used in this *Oracle Field Service Connectivity Options* guide.

Availability domain—A fault-tolerant, completely isolated data center within a region, connected to other availability domains. Because they don't share physical infrastructure or internal networks, they are extremely unlikely to fail simultaneously, helping to deliver OCI's high availability.

DRG (Dynamic Routing Gateway)—An optional virtual router that you can add to your VCN (Virtual Cloud Network) to provide a path for private network traffic between your VCN and on-premises network. You can use it with other networking components and a router in your on-premises network to establish a connection by way of *IPSec VPN* or Oracle Cloud Infrastructure *FastConnect*. It can also provide a path for private network traffic between your VCN and another VCN in a different region.

FastConnect—An Oracle network connectivity alternative to using the public internet to connect your network to Oracle Cloud Infrastructure and other Oracle Cloud services. FastConnect provides private, dedicated connectivity. See also *DRG*.

Instance—A compute host running in the cloud. An OCI compute instance lets you use hosted physical hardware instead of the traditional software-based virtual machines, ensuring a high level of security and performance. For details, refer to https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/Concepts/computeoverview.htm.

Internet gateway—An optional virtual router that you can add to your VCN for bi-directional network traffic between a VCN and the internet.

IPSec (Internet Protocol Security)—A suite of protocols that authenticates and encrypts data packets before they are transferred via VPN from the source to the destination. IPSec provides a path for private traffic between your network and destinations other than the internet. See also *DRG*.

Load balancing—Automated traffic distribution from one entry point to multiple servers reachable from your virtual cloud network. In OCI, you can choose either a public or private IP address and provisioned bandwidth. Load balancers improve resource utilization, facilitate scaling, help ensure high availability, and reduce maintenance windows. For information about load balancing, refer to https://docs.cloud.oracle.com/en-us/iaas/Content/Balance/Concepts/balanceoverview.htm.

NAT gateway (Network Address Translation)—An optional virtual router that you can add to your VCN to give cloud resources without public IP addresses access to the internet without exposing those resources to incoming internet connections.

Network security group—A virtual firewall consisting of a set of security rules that apply only to the individual resources in that group. Oracle recommends using network security groups instead of security lists, where the rules apply to all of the resources in any subnet that uses the list. See also *Security list*.

Region—A localized geographic area, which includes one or more availability domains, or data centers. Most OCI resources are either region-specific, such as a virtual cloud network, or data-center-specific, such as a computer instance. Regions are independent of other regions and can be separated geographically. Generally, you would deploy an application in the region where it is most heavily used, but you might also deploy in different regions to either mitigate the risk of region-wide events like weather systems or to meet a variety of legal or business requirements for data residency. For more information, see https://docs.cloud.oracle.com/en-us/iaas/Content/General/Concepts/regions.htm.

Resources—Network components, storage resources, and compute systems, such as instances, VCNs, load balancers, and block volumes.

Security list—A virtual firewall consisting of a set of security rules to define permissible inbound and outbound traffic for a particular *subnet*. Each cloud network has a default security list, and you can also create other security lists for the VCN. The rules in a subnet's security list apply to every resource in the subnet. See also *Network security group*.

Security rules—A virtual firewall for your VCN that defines ingress and egress rules for specifying the types of traffic, by protocol and port, allowed in and out of the instances. To implement security rules, you can use *network security groups*, which apply to *resources* defined in a group, or *security lists*, which apply to all resources within a *subnet*. Your VCN comes with a default security list with default security rules. For more information, see https://docs.cloud.oracle.com/en-us/iaas/Content/Network/Concepts/securityrules.htm.

Service Gateway—Optional virtual router that you can add to your VCN to provide a path for private network traffic between your VCN and supported services in the Oracle Services Network without using an *internet gateway* or a *NAT gateway*.

Subnet—A subdivision you define in a VCN (for example, 10.0.0.0/24 and 10.0.1.0/24). Subnets contain virtual network interface cards (VNICs), which attach to instances. Each subnet consists of a contiguous range of IP addresses that do not overlap with other subnets in the VCN. Subnets can be isolated and secured.

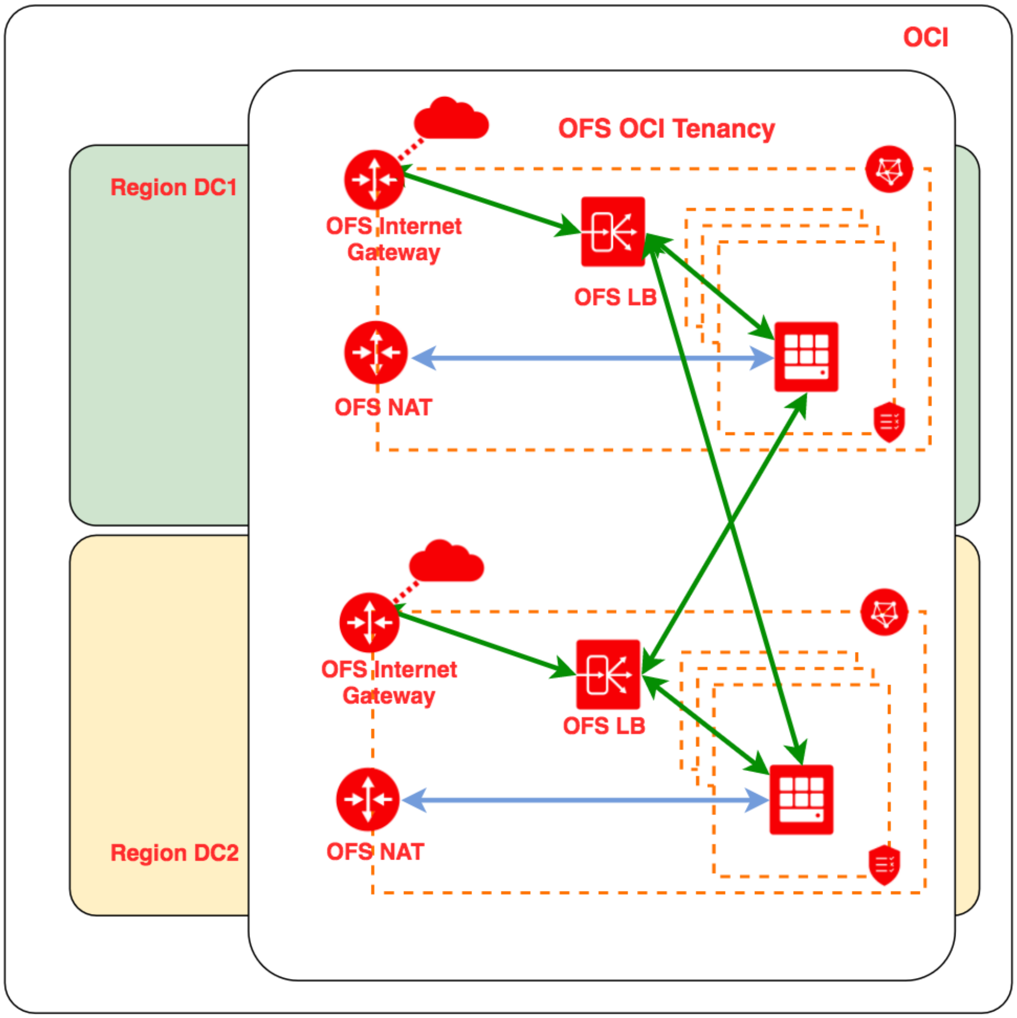
Tenancy—A secure and isolated partition within Oracle Cloud Infrastructure where you can create, organize, and administer your cloud *resources*. Oracle creates a tenancy for your company when you sign up for OCI.

VCN (Virtual Cloud Network)—A virtual, private network that you set up in Oracle data centers on which your instances run. It closely resembles a traditional network, with firewall rules and specific types of communication gateways that you can choose to use, as well as subnets and routing tables. A cloud network resides within a single region but includes all the region's availability domains (data centers). Each subnet you define in the cloud network can either be in a single availability domain or span all the availability domains in the region, which is the recommended approach. You need to set up at least one cloud network before you can launch instances. You can configure the cloud network with an optional *internet gateway* to handle public traffic, and an optional *IPSec VPN* connection or *FastConnect* to securely extend your on-premises network. For an overview of networking concepts, including virtual cloud networks, see https://docs.cloud.oracle.com/en-us/iaas/Content/Network/Concepts/overview.htm.

VPN Connect—An IPSec VPN that can be used to connect your on-premises network and your virtual cloud network.

OCI Tenancy for OFS

This diagram represents the OCI tenancy for Oracle Field Service. Two separate data centers, one home and one standby, ensure connectivity. Because they are geographically separated from each other, any failure at one data center, for example, due to a network disruption or natural disaster, is unlikely to impact the availability of the other. Each data center includes an Internet Gateway, a NAT gateway, and a load balancer. Data enters via the internet gateway, where it is then routed through the load balancer before reaching the OFS application.



Use Case Overview

This section describes the various connectivity use cases for using Oracle Field Service with Oracle Cloud Infrastructure. Basically, they fall into four main categories:

- Standard connectivity (recommended)
- VPN with inbound traffic only
- VPN with inbound and outbound traffic
- FastConnect

It's important to understand that you can use any or all of the various use cases; using one doesn't prevent you from using any of the others. For example, you might have just a limited number of systems – perhaps middleware applications – that require the use of a VPN. In that case, you could configure a VPN for those systems, while using standard connectivity for all the rest of your data traffic.

The great majority of Oracle Field Service customers can use the **standard connectivity option** for connecting over the public internet as their sole means of connectivity. This out-of-the-box option is the recommended method, and even if it turns out not to be your only connectivity option, you'll still want to use it for your mobile connections when technicians connect to OFS using their mobile apps. This method provides high-security management of traffic between data centers when necessary, and it requires no configuration effort on your part.

Even though most customers need only the standard connectivity option, your organization might need one or more additional options. Here are the questions that can help you know if your organization needs to configure another method of connectivity:

- Does your organization have a corporate mandate that requires VPN connectivity for at least some of your systems? If yes, you'll need to configure a VPN option and manage the data traffic within your organization. To understand which VPN option applies, you'll also need to know if you're using the Outbound API for customer notifications.
    - If you need VPN connectivity and you're using the Outbound API, you'll need to select the **VPN with inbound and outbound traffic** option.
    - If you need VPN connectivity and you're not using the Outbound API, you'll select the **VPN with inbound traffic only** option.

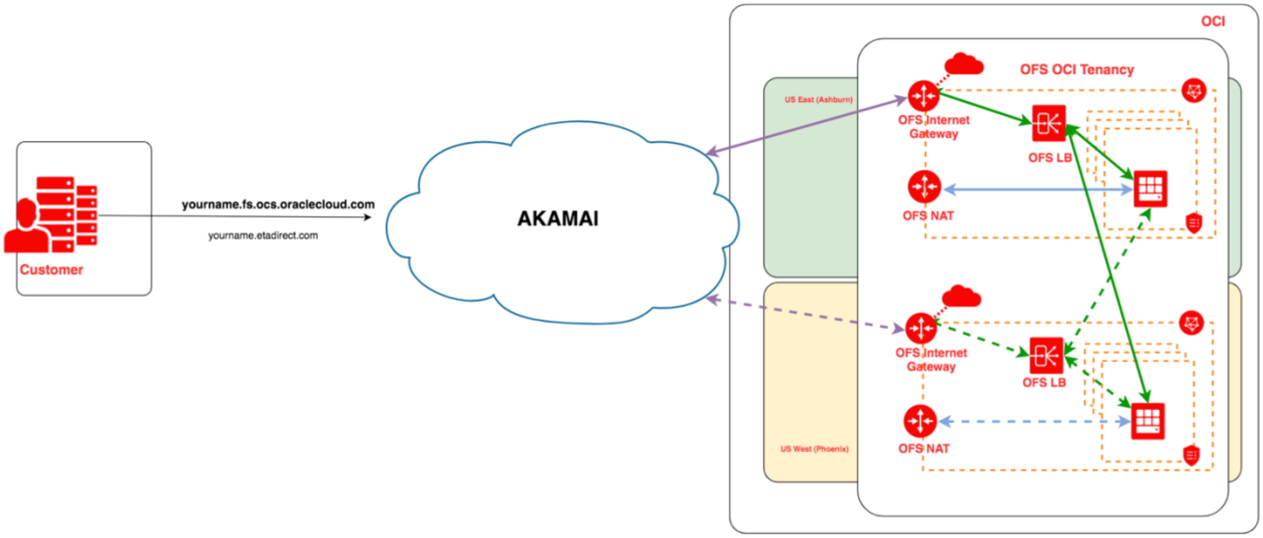
  NOTE: If you're using the Outbound API but do not need VPN connectivity, you can use the standard connectivity option with whitelisting, which is described in the **Standard connectivity** section.

- Does your organization have a high volume of data traffic or does it need a guaranteed bandwidth – or both? If that describes your situation, you may want to consider purchasing Oracle Cloud Infrastructure's **FastConnect service.**

Standard Connectivity (recommended method)

For almost all OFS customers, the standard, out-of-the-box connectivity via the public internet is sufficient for all of their connectivity needs. And even if your organization requires additional connectivity configuration for certain data, you'll still use this connectivity option for mobile connections. With this option, you'll access your OFS subscription via the Akamai content delivery network (CDN) using the URLs and passwords that were provided at OFS service activation. Akamai manages global traffic and routes applications, providing high reliability, short response times, and data encryption.

Standard connectivity works like this, where in this example, the Customer Home Region is US East (Ashburn) and the Customer Standby Region is US West (Phoenix):



The configuration of the standard connectivity option is automatically available to you, and there are no setup steps required on your part. When you use the URL assigned to your instance, your request will be directed to the home region of your service. In the diagram above, your assigned URL is *yourname.fs.ocs.oraclecloud.com.* (If you're a current customer migrating to OCI, the *yourname.etadirect.com* URL is the one that was assigned to your legacy instance.) Static content will be cached closer to your users, which reduces page load time.

If a connection to the home region (here, US East (Ashburn)) cannot be established, for example, due to a failure of a local ISP, the request is automatically redirected to the standby region (US West (Phoenix)), which is geographically separate and where the requests will now be processed. Because there's redundancy at both the datacenter level as well as at the component level within the data centers, Oracle can process requests regardless of the condition of infrastructure networking. This redirection occurs automatically without any oversight on your part.

In addition to the use of secure connections only, you can also limit the IP addresses or networks that can access Oracle Field Service by using the whitelisting functionality, accessed under the Additional Restrictions section of the Applications configuration screen. For information, refer to https://docs.oracle.com/en/cloud/saas/field-service/20b/faadu/configure-oracle-field-service.html#t_createAnApplication.

Using Outbound API with Standard Connectivity

While we recommend using the events subscription methods of the Core REST API for most integrations, you may be using the Outbound API for time-based customer notifications. Because there are no outbound connections originating in the OFS tenancy, the Akamai network is not used. Instead connections are opened from OFS to URLs or IP addresses that were configured in the outbound channels. (Refer to https://docs.oracle.com/en/cloud/saas/field-service/20b/faded/index.html.) To accept that traffic, you may wish to whitelist only Oracle Cloud Infrastructure IP addresses that can be used for that type of communication. To identify IP addresses that can be used to originate traffic via Outbound API from the OFS OCI tenancy, refer to https://docs.cloud.oracle.com/en-us/iaas/Content/General/Concepts/addressranges.htm.

VPN Overview

As previously mentioned, you can use the Outbound API with standard connectivity. If, however, you're using the Outbound API and your corporate IT policy demands the use of a VPN, you'll need to select the connectivity option for both inbound and outbound traffic. If you're not using the Outbound API (that is, you're using the REST API instead) but you need a VPN connection, you'll select the VPN connection for inbound traffic only.

It's important to know that selecting either of the VPN options places the responsibility for configuration, traffic redirection, and any network problems on your organization. Also understand that you can use either of the VPN connectivity options alongside the standard connectivity option.

To create a VPN on Oracle Cloud Infrastructure, you can download *Creating a VPN on OCI.pdf* at https://cx.rightnow.com/app/answers/detail/a_id/11265.

VPN: Inbound Traffic Only

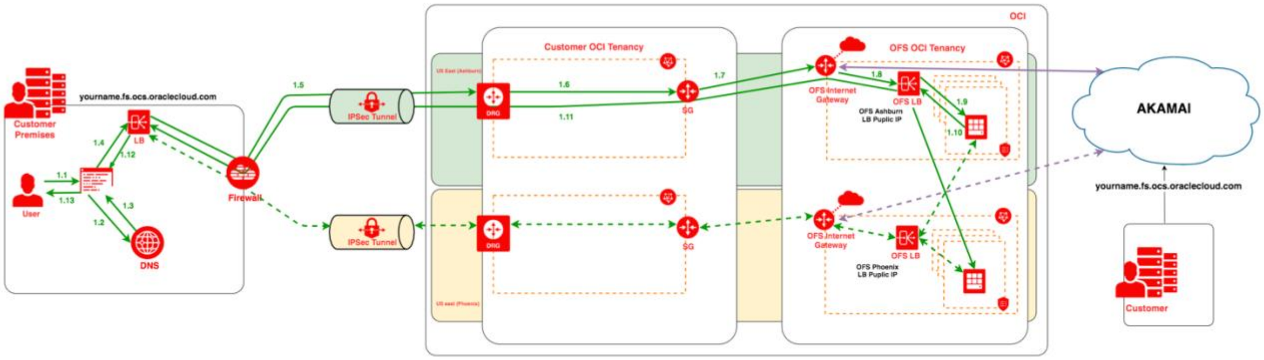
When you're configuring VPN service for inbound traffic only, you can connect your on-premises network and your virtual cloud network (VCN) using VPN Connect, which is an IPSec VPN. The IPSec protocol suite encrypts the entire IP traffic before the packets are transferred from the source to the destination. The IPSec VPN is shown as the IPSec Tunnel in the following diagram.

In general, IPSec can be configured in the transport mode, where only the actual payload of the packet is encrypted and authenticated, while the header information stays intact. **However, Oracle Cloud Infrastructure supports only the tunnel mode,** in which the entire packet is encrypted and authenticated. After encryption, the packet is then encapsulated to form a new IP packet that has different header information.

The following diagram shows one example of a solution consisting of two parts. One part is the VPN itself, and it should be built using OCI resources. The second part can be implemented in your on-premises network to maintain high availability of the service. At a minimum, it can consist of a load balancer and a specially configured DNS subsystem. The load balancer can be software-based, for example HAProxy or NGINX, or hardware-based, such as BigIP or Cisco. It should be able to perform periodic health checks on the status of the home and standby regions and be able to automatically switch traffic between them. The DNS subsystem should be able to do response manipulation so it can substitute public IPs for OFS URLs using the local IPs that you assigned to your load balancer.

One example of this kind of functionality is the Response Policy Zones in BIND name server. An exact list of the domain records that should be modified will be provided via Service Request. We strongly recommend that you do not create an internal local copy of the OFS domain zones because many resources may be necessary for proper OFS functioning, and the RPZ in BIND approach can replace data for only a small subset of OFS resources that should be accessed via VPN. If the number of systems that will use the VPN to communicate with OFS is relatively small, such as three to five systems, you may also use local host files for this.

The following diagram and flow description assume that these two components are built at your premises.



The numbers on the above diagram help describe the inbound flow of traffic, from users to your organization to Oracle Field Service.

1.1 End user enters a URL in a browser address field.

1.2 The browser asks the DNS to resolve the domain name from the URL.

1.3 The DNS responds with a modified IP address.

1.4 The browser connects to your internal load balancer.

1.5 The internal load balancer sends the request to the home or standby region (depending on the status of health checks of each region) via the VPN tunnel to the dynamic routing gateway (DRG).

1.6 From the DRG, traffic containing the request is routed to the service gateway.

1.7 The traffic is then directed from the service gateway to the OFS Internet Gateway in the same region.

1.8 From the OFS Internet Gateway, the traffic reaches the OFS Public Load Balancer.

1.9 The OFS Load Balancer distributes the request to the front end nodes.

1.10 After processing the request, the front end nodes reply back to the OFS Public Load Balancer.

1.11 The response traffic returns from the OFS Load Balancer through the chain of gateways, DRG, IPSec Tunnels back to the internal Load Balancer.

1.12 From the internal load balancer, traffic returns to the end user's browser.

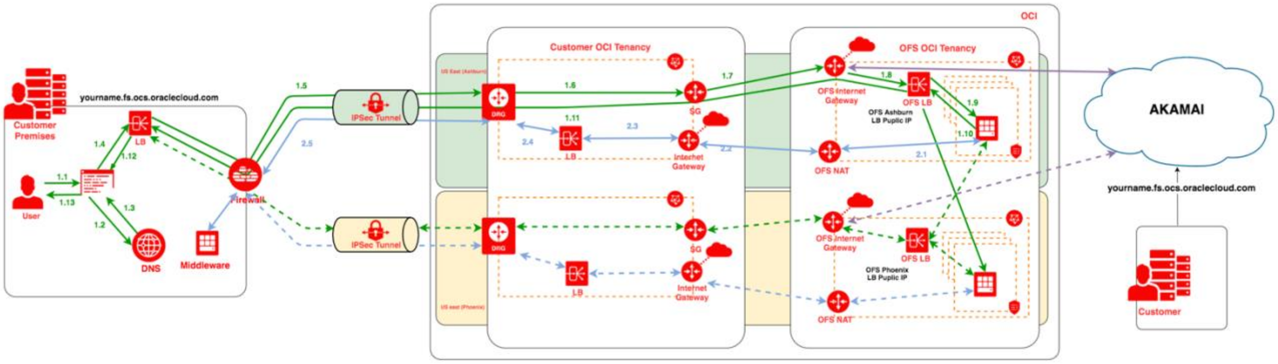
1.13 The end user views the results.

In the event the internal load balancer sends traffic to the standby region due to failure in the home region, steps 1.5 through 1.11 are executed in the standby region, designated by the dashed green lines. Any redirection to the standby region must be configured by your organization.

VPN: Inbound and Outbound Traffic

If you use the Oracle Field Service Outbound API for customer notifications and your corporate policy requires the use of a VPN, you'll want to configure your VPN for both inbound and outbound traffic. This means that the Inbound traffic configuration described above should be supplemented by two new components: an Internet Gateway and Load Balancer in the OCI tenancy. The public IP of this load balancer should be used when configuring external channels in OFS.

If you're using the Events API or Oracle Integration Cloud instead of the Outbound API, configuring for inbound traffic only is sufficient.



The inbound flow of traffic is the same as it is in the VPN for inbound traffic only, and the numbers on the above diagram have been added to define the outbound flow of traffic, from Oracle Field Service to your on-premises network.

2.1 The OFS backend servers send requests for data from your internal systems to the OFS NAT gateway, a virtual router for network address translation.

2.2 From the NAT gateway, traffic is routed to the internet gateway in your OCI tenancy.

2.3 The requests are then sent from your internet gateway to the load balancer in your VCN.

2.4 The load balancer forwards traffic to your DRG.

2.5 And from the DRG, traffic flows to your on-premises network via the VPN tunnel.

Unless otherwise redirected, all traffic moves in your home region data center. Any redirection to the standby data center must be configured by your organization.

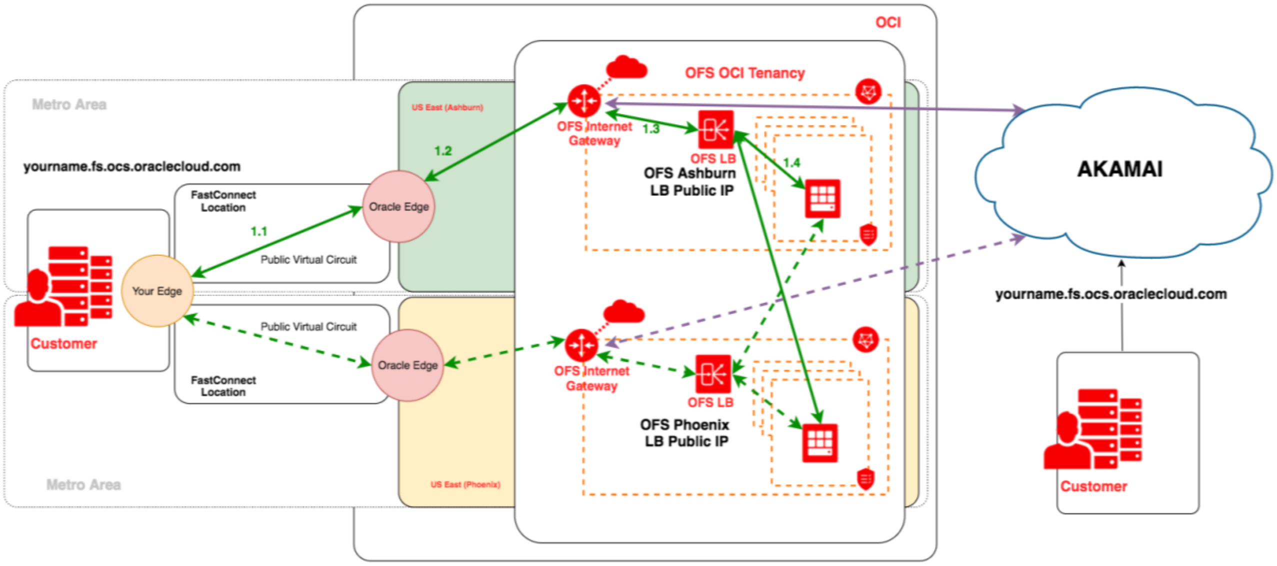
In this configuration, it's a good security practice to configure a subnet for your public load balancer with security rules that accept traffic only from the Oracle network via the OFS NAT gateway. Refer to https://docs.cloud.oracle.com/en-us/iaas/Content/General/Concepts/addressranges.htm for information about IP address ranges for the Oracle network to define the subnet's security list.

FastConnect Public Peering

Oracle Cloud Infrastructure FastConnect is a network connectivity alternative to using the public internet. It connects your network to Oracle Cloud Infrastructure and other Oracle Cloud services. For an additional cost, FastConnect provides a dedicated and private connection with higher bandwidth options and a more reliable and consistent networking experience. Your system is physically connected to the Oracle network for additional security and performance as well as guaranteed bandwidth. You might want to choose this option if you need extremely fast traffic or the ability to download high-volume files, or both.

FastConnect public peering lets you access public services in Oracle Cloud without traffic traversing the internet path. Using FastConnect public peering, you can connect to Oracle Field Service. Oracle will advertise IP prefixes that belong to all public services in the region where you establish FastConnect public peering. Depending on the connectivity model you choose, you will either need to advertise public prefixes that you own, or use network address translations to convert your private network RFC1918 prefixes to public IPs that will be advertised to Oracle.

This diagram represents OFS-FastConnect connectivity.



In the diagram above, your assigned URL is *yourname.fs.ocs.oraclecloud.com.* (If you're a current customer migrating to OCI, the *yourname.etadirect.com* URL was assigned to your legacy instance.)

For information about FastConnect connectivity models, see https://www.oracle.com/cloud/networking/fastconnect-connectivity-models.html.

For information about configuring FastConnect, see https://docs.cloud.oracle.com/en-us/iaas/Content/Network/Concepts/fastconnect.htm.

Revision History

Version	What’s Changed
1.0	Original version

Terms of Use for OFS Connectivity Options

By using the *OFS Connectivity Options* (“Guide”), you agree to the following terms and conditions (“Guide Terms of Use”). The Guide Terms of Use supplement the terms of any agreement that you may have with Oracle or a company acquired by Oracle, but solely with respect to the Guide provided herein. In the event of a direct conflict between the Guide Terms of Use and any other agreement you may have with Oracle or a company acquired by Oracle, the Guide Terms of Use will control your use of the Guide.

You agree that access to the Guide will be granted only to your designated support contacts and that the Guide may be used only in support of your authorized use of the Oracle products and/or cloud services for which you have a current support contract or a current cloud service subscription. You shall be responsible for your designated support contacts’ use of the Guide and for their compliance with these Guide Terms of Use.

THE GUIDE MAY INCLUDE OMISSIONS, INACCURACIES, OR OTHER ERRORS. THE GUIDE IS PROVIDED “AS IS” AND WITHOUT WARRANTY. ORACLE DOES NOT WARRANT THAT THE GUIDE IS COMPATIBLE WITH YOUR ENVIRONMENT OR ERROR-FREE, NOR DOES IT PROVIDE ANY OTHER WARRANTIES, WHETHER EXPRESSED OR IMPLIED IN LAW, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THE GUIDE IS NOT A PROGRAM OR DOCUMENTATION UNDER THE TERMS OF YOUR AGREEMENT(S) WITH ORACLE.

IN NO EVENT SHALL ORACLE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE GUIDE.

The information contained in the Guide is the confidential proprietary information of Oracle. You may not use, disclose, reproduce, transmit, or otherwise copy in any form or by any means the Guide for any purpose, other than to support your authorized use of the Oracle product and/or cloud services without the prior written permission of Oracle.