ORACLE
Cloud Infrastructure

Connecting to a Private IP Serial Console Through a Service Gateway

ORACLE WHITE PAPER | MARCH 2019

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Revision History

The following revisions have been made to this white paper since its initial publication:

Date	Revision
March 26, 2019	Initial publication

You can find the most recent versions of the Oracle Cloud Infrastructure white papers at https://cloud.oracle.com/iaas/technical-resources.

Table of Contents

Introduction

Secure access to the serial console has long been a requested service from our customers. With the release of the new service gateway feature in Oracle Cloud Infrastructure, this compatibility is now available. A service gateway lets resources in your virtual cloud network (VCN) privately access Oracle Cloud services without the use of an internet gateway or Network Address Translation (NAT) device. Using a service gateway lets VCN resources that are on a private subnet with a private IP address be accessible from a public IP source without traversing the internet. All communications to these services traverse solely over the Oracle Services Network, providing a secure communications path.

This paper describes how to configure and access the serial console in a secured manner from a remote connection.

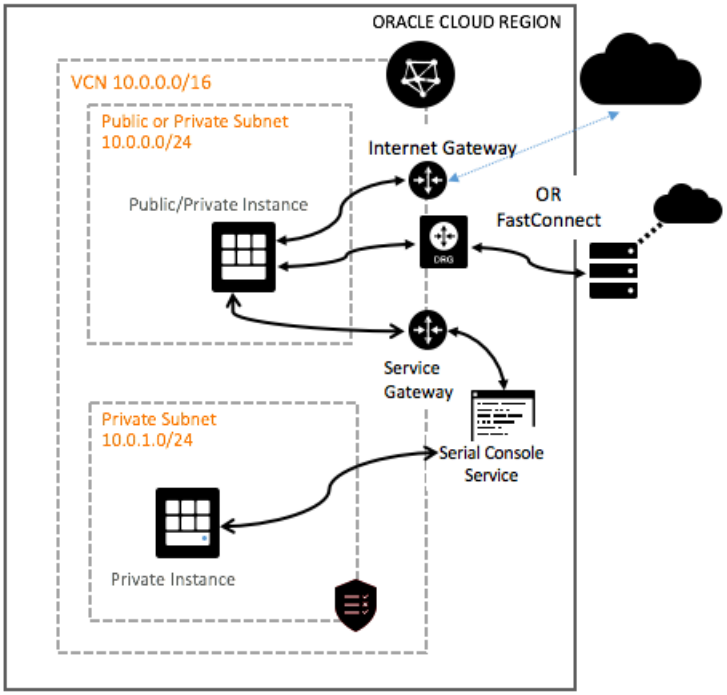
Service Gateway Overview

Each VCN has several gateways associated with it: internet gateways, dynamic routing gateways, NAT gateways, and service gateways. These gateways are divided into two types: data plane or control plane. The internet gateway, dynamic routing gateway, and NAT gateway are the access points for the data plane traffic in and out of the Oracle Cloud Infrastructure tenancy. The service gateway connects to the control plane, allowing access to Oracle's internal cloud services network.

A service gateway can be associated with only a single VCN. If the VCN is peered with another VCN, resources in the other VCN can't access the service gateway. You can't route to a service gateway from another VCN. Resources in an on-premises network connected to the service gateway's VCN with FastConnect or an IPSec VPN can't use the service gateway.

You can connect to a service gateway through an internet gateway or FastConnect to an internal instance that can be on either a public subnet or a private subnet. Then you can use that instance to access the service gateway associated with the VCN.

The following diagram illustrates a VCN that has both a public subnet and a private subnet. Resources in the private subnet have only private IP addresses and can't communicate directly with the internet.



Configuring the Service Gateway

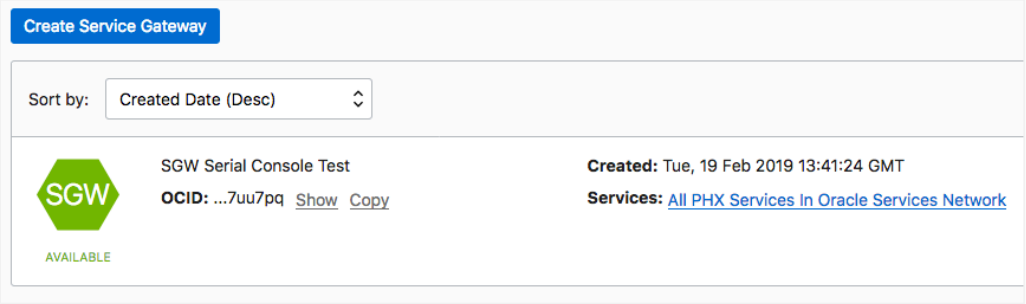
An example use case for configuring a service gateway might be to connect from a bastion or jump-box server in the DMZ to another instance on a private subnet to perform a reboot.

The example in this paper uses a VCN that has one public subnet and one private subnet, each with a single VM instance.

Note: This paper was written using the prereleased service gateway feature and is provided as an example only. Any references to the Phoenix (PHX) region, example services labels, and available services can change from the final GA release.

1. In the Oracle Cloud Infrastructure Console, navigate to the VCN and click **Service Gateways** under **Resources**.
2. Click **Create Service Gateway** and enter the name and services to which you want to provide connectivity. In this case, select **All PHX Services in Oracle Services Network**.
3. Click **Create**.

After the service gateway is created, its details on the Console look like the following example:



Configuring the Route Tables and Security Lists

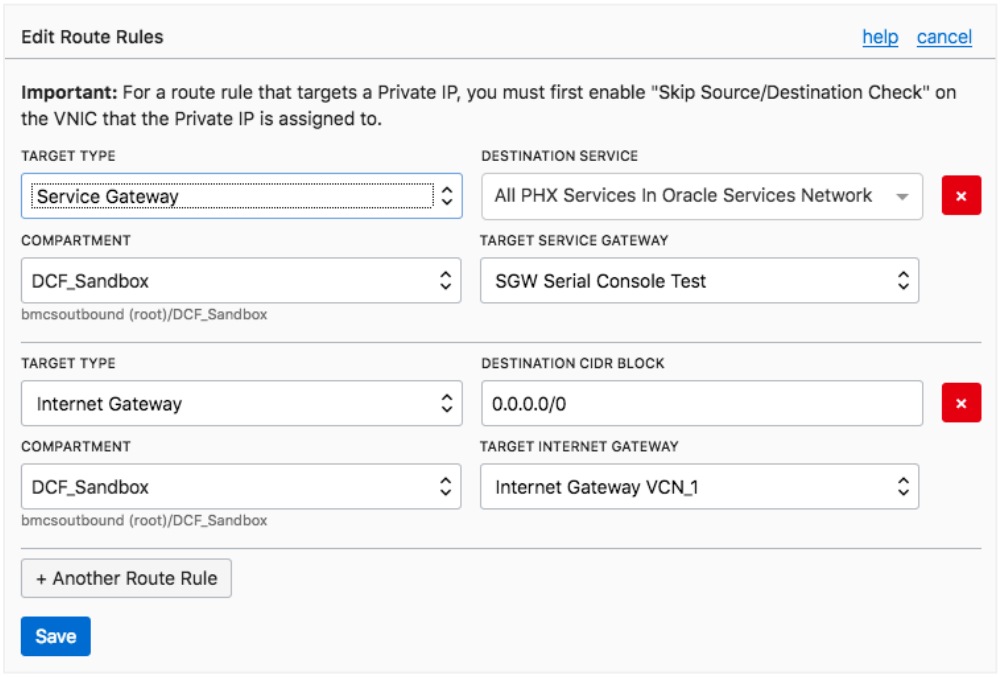
For traffic to be routed correctly from the VCN to the private subnet, you must add some rules and routes. If you want to access the tenancy from the internet, add the normal internet gateway to the internet route of 0.0.0.0/0 to your VCN.

Note: You can also configure a dynamic routing gateway for your external connection. The internet gateway is not required.

Configuring the Route Table

To use the service gateway, you must create a route to it.

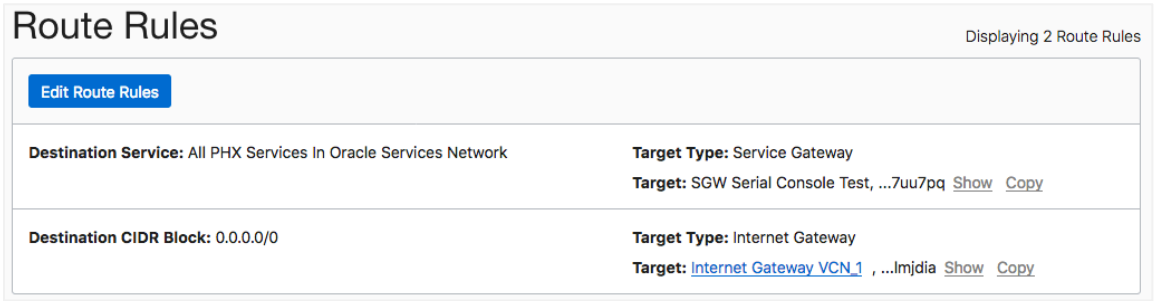
1. Under **Resources** on the VCN's details page, click **Route Tables**.
2. Select the route table and then click **Edit Route Rules**.
3. Add the service route, and then associate the private subnet with this route table.
   A. Select **Service Gateway** as the target type.
   B. Select the compartment.
   C. Select **All PHX Services in Oracle Services Network** as the destination service.
   D. Select the service gateway that you created as the target.



4. Click **Save**.

   Following is an example of what the VCN's route table rules should look like when completed.

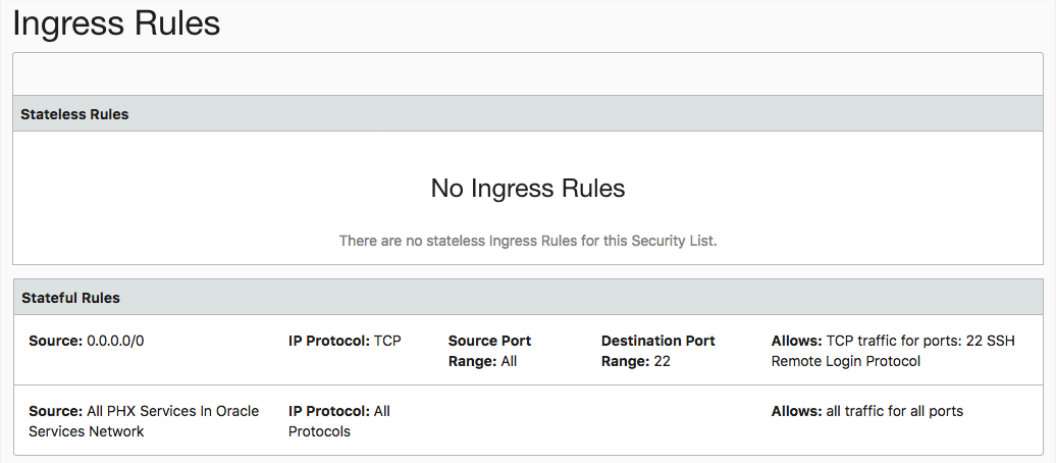
   - **Destination Service:** All PHX Services in Oracle Services Network
   - **Target Type:** Service Gateway
   - **Target:** SGW Serial Console



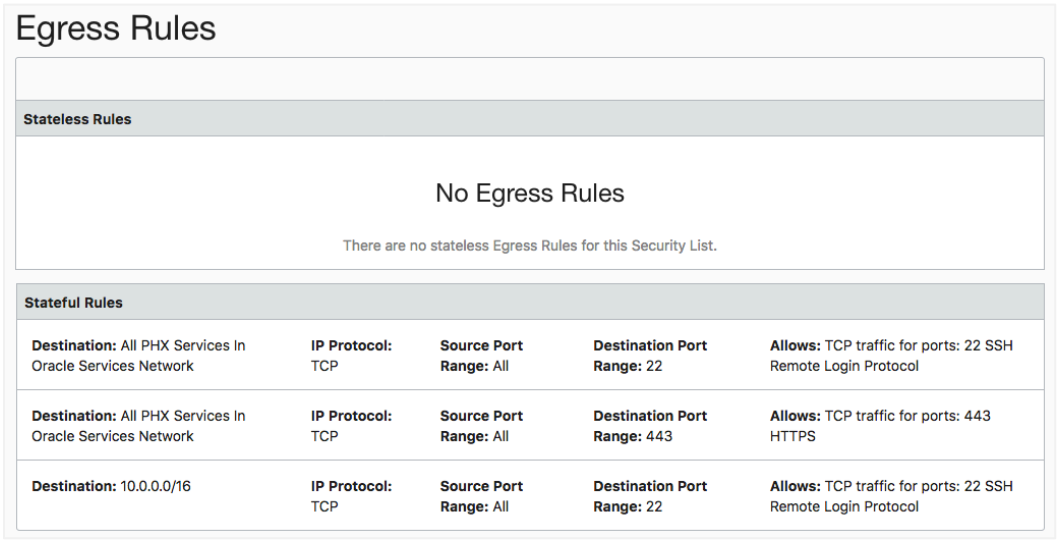
Configuring the Security Lists

Security lists are a common set of firewall rules associated with a subnet. They are applied to all instances launched inside the subnet and provide ingress rules and egress rules that specify the types of traffic allowed in and out of the instances. When configuring the service gateway, you need to ensure that the security lists for the subnets that use the service gateway have the correct ports open. For example, the serial console uses port 22 (SSH). Note that this port might already be open for use by other instances.

1. Determine which subnets need to communicate with the service gateway.
2. Under **Resources** on the VCN's details page, click **Security Lists**.
3. Click the security list and click **Edit All Rules**.
4. Add a stateful ingress rule with the following values:
   - **Source:** All PHX Services in Oracle Services Network
   - **IP Protocols:** All Protocols (can be restricted to select protocols)
   - **Allows:** all traffic for all ports (can be restricted to select ports)

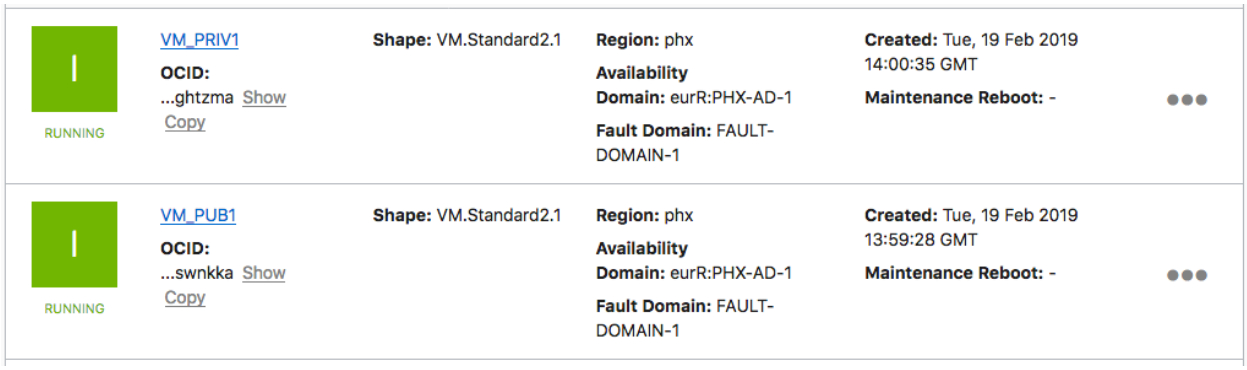


5. Add egress rules with the following values:
   - **Destination:** All PHX Services in Oracle Services Network
   - **IP Protocol:** TCP
   - **Source Port:** ALL (can be restricted to select ports)
   - **Destination Port:** 22, 443 (can be restricted to select ports)



Creating Public and Private Instances

This use case connects a VM instance on a public subnet to the serial console of a VM instance on a private subnet. Ensure that both of the instances use the route table and security lists that you have modified.



Configuring the Serial Console

In this use case, the service gateway destination is the serial console of the private VM instance.

1. In the Oracle Cloud Infrastructure Console, navigate to the details page of the private VM instance to which you want to connect.
2. Under **Resources**, click **Console Connections**.
3. Click **Create Console Connection**.

4. In the dialog box, enter your SSH key (paste or choose a file), and then click **Create Console Connection**.

5. On the page that lists all the instances in the compartment, click the Actions menu (three dots) for the instance to which you want to connect, and then select **Connect with SSH**.

6. In the Connect with SSH dialog box, select the platform from which you are connecting. The connection string that is required to connect to the private instance is generated.

7. Copy the connection string to a text file. You will use it in the next section.

Connecting to the Private Instance's Serial Console

You must first test and set up connectivity between the public and private VM instances.

1. Use SSH to connect from the public instance to the private instance.

```
[opc@vm-pub1 ~]$ ssh -i ~/.ssh/oci -l opc 10.0.3.2

Warning: Identity file /home/opc/.ssh/oci not accessible: No such file or
directory.

The authenticity of host '10.0.3.2 (10.0.3.2)' can't be established.

ECDSA key fingerprint is
SHA256:qzbMWEY2ENdh0oZqHGrMHCDdJKGMitHl2nQ8KJuyqjs.

ECDSA key fingerprint is
MD5:0c:c4:11:13:83:d1:09:0c:3f:77:3b:65:5d:0c:8d:58.

Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added '10.0.3.2' (ECDSA) to the list of known hosts.
```

2. Edit the SSH key file and add the source private key file of the person that requires connectivity.

```
[opc@vm_priv1 ~]$ vi ~/.ssh/oci (add in the private key file)
```

3. Change the permissions of the SSH key file for security.

```
[opc@vm_priv1 ~]$ chmod 400 ~/.ssh/oci
```

4. Exit the private instance connection session.

5. Using the connection string that you copied in the previous section, connect from the public instance to the private serial console. Replace the text highlighted in blue (`-i ~/.ssh/oci`) with the directory path specific to the instance.

```
[opc@vm-pub1 ~]$ ssh -i ~/.ssh/oci -o ProxyCommand='ssh -i ~/.ssh/oci -W
%h:%p -p 443
ocid1.instanceconsoleconnection.oc1.phx.abyhqljsjfhketfyf73rz7c6jcpbjpvlaj
ewog4dyvbj3ueukjolsfrpjskq@instance-console.us-phoenix-1.oraclecloud.com'
ocid1.instance.oc1.phx.abyhqljsjfw4hzv3dnduacasvri2juvolznhoqias4dwqbyi6xe
e3vghtzma

Warning: Identity file /home/opc/.ssh/oci not accessible: No such file or
directory.

Warning: Identity file /home/opc/.ssh/oci not accessible: No such file or
directory.

The authenticity of host '[instance-console.us-phoenix-
1.oraclecloud.com]:443 ([129.146.14.188]:443)' can't be established.

RSA key fingerprint is SHA256:Ghg/XkZv4W42u0xaqNhN7LMQcxrYuRTE+IYBD+kBxxx.

RSA key fingerprint is
MD5:29:5e:e8:be:3c:8c:39:5c:29:d3:3a:9d:78:e9:7f:d3.

Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[instance-console.us-phoenix-
1.oraclecloud.com]:443,[129.146.14.188]:443' (RSA) to the list of known
hosts.

The authenticity of host
'ocid1.instance.oc1.phx.abyhqljsjfw4hzv3dnduacasvri2juvolznhoqias4dwqbyi6x
ee3vghtzma (<no hostip for proxy command>)' can't be established.

RSA key fingerprint is SHA256:PhpxXIeD9OuKmi0ntmhePLW4Br8PRpu4oYMmuNvRAKk.

RSA key fingerprint is
MD5:xx:xx:1c:dd:30:54:3f:68:bd:58:22:e4:65:64:9b:xx.
```

```
Are you sure you want to continue connecting (yes/no)? yes

Warning: Permanently added
'ocid1.instance.oc1.phx.abyhqljsjfw4hzv3dnduacasvri2juvolznhoqias4dwqbyi6x
ee3vghtzma' (RSA) to the list of known hosts.
```

You then receive confirmation of the console connection:

```
Oracle Linux Server 7.6
Kernel 4.14.35-1844.1.3.el7uek.x86_64 on an x86_64
```

Testing the Private Instance's Serial Console Connection

To test the serial console connection, perform a reboot on the private VM instance console and see if the connection is maintained. At this point, you can either log in to the private VM instance or via the console to issue the reboot command. While still connected to the private instance's serial console, you should be able to watch the entire reboot process.

```
vm_priv1 login: [  OK  ] Stopped Dump dmesg to /var/log/dmesg.
         Stopping RPC bind service...
[  OK  ] Closed LVM2 poll daemon socket.
[  OK  ] Stopped target rpc_pipefs.target.
[  OK  ] Stopped target Multi-User System.
[  OK  ] Stopped Resets System Activity Logs.

Private VM instance rebooting……

Welcome to Oracle Linux Server 7.6 dracut-033-554.0.3.el7 (Initramfs)!

[  OK  ] Reached target Swap.
[  OK  ] Started Dispatch Password Requests to Console Directory Watch.
[  OK  ] Reached target Timers.
[  OK  ] Reached target Local Encrypted Volumes.
[  OK  ] Reached target Paths.
```

Conclusion

This paper describes how to create a private serial console connection from a public source point that uses a service gateway to remain isolated and secure on the Oracle Services Network.

ORACLE

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services

Connecting to a Private IP Serial Console Through a Service Gateway
March 2019
Author: David Foster