Oracle Cloud Hosting: Configuring default IPTables on a Virtual Machine

> Applies to Ubuntu 22.04 LTS ARM64 VMs on Oracle Cloud. May also apply to x86_64 VMs and other Linux distributions too.

Despite OCI (Oracle Cloud Infrastructure) having a firewall in-front of your VM in the form of security lists, the VM itself runs its own set of iptables rules, as defined by Oracle. I **came across this article** which saved my sanity as I initially couldn't figure out why, despite defining the ingress rules within the OCI Security List, connections weren't going through. Turns out that they weren't defined in iptables!

Updating IPTables rules on an Oracle VM

I edited `/etc/iptables/rules.v4` and added the following lines:

```
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
```

which appear at lines 12 and 13 in the snippet of the full `rules.v4` file below:

```
# Generated by iptables-save v1.8.7 on Thu Oct 19 15:25:17 2023
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [328577:1494721704]
:InstanceServices - [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p udp -m udp --sport 123 -j ACCEPT
```

-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
-A OUTPUT -d 169.254.0.0/16 -j InstanceServices
-A InstanceServices -d 169.254.0.2/32 -p tcp -m owner --uid-owner 0 -m tcp --dport 3260 -m comment --comment "See the Oracle-Provided Images section in the Oracle Cloud Infrastructure documentation for security impact of modifying or removing this rule" -j ACCEPT
-A InstanceServices -d 169.254.2.0/24 -p tcp -m owner --uid-owner 0 -m tcp --dport 3260 -m comment --comment "See the Oracle-Provided Images section in the Oracle Cloud Infrastructure documentation for security impact of modifying or removing this rule" -j ACCEPT
-A InstanceServices -d 169.254.4.0/24 -p tcp -m owner --uid-owner 0 -m tcp --dport 3260 -m comment --comment "See the Oracle-Provided Images section in the Oracle Cloud Infrastructure documentation for security impact of modifying or removing this rule" -j ACCEPT
-A InstanceServices -d 169.254.5.0/24 -p tcp -m owner --uid-owner 0 -m tcp --dport 3260 -m comment --comment "See the Oracle-Provided Images section in the Oracle Cloud Infrastructure documentation for security impact of modifying or removing this rule" -j ACCEPT
-A InstanceServices -d 169.254.0.2/32 -p tcp -m tcp --dport 80 -m comment --comment "See the Oracle-Provided Images section in the Oracle Cloud Infrastructure documentation for security impact of modifying or removing this rule" -j ACCEPT
-A InstanceServices -d 169.254.169.254/32 -p udp -m udp --dport 53 -m comment --comment "See the Oracle-Provided Images section in the Oracle Cloud Infrastructure documentation for security impact of modifying or removing this rule" -j ACCEPT
-A InstanceServices -d 169.254.169.254/32 -p tcp -m tcp --dport 53 -m comment --comment "See the Oracle-Provided Images section in the Oracle Cloud Infrastructure documentation for security impact of modifying or removing this rule" -j ACCEPT
-A InstanceServices -d 169.254.0.3/32 -p tcp -m owner --uid-owner 0 -m tcp --dport 80 -m comment --comment "See the Oracle-Provided Images section in the Oracle Cloud Infrastructure documentation for security impact of modifying or removing this rule" -j ACCEPT
-A InstanceServices -d 169.254.0.4/32 -p tcp -m tcp --dport 80 -m comment --comment "See the Oracle-Provided Images section in the Oracle Cloud Infrastructure documentation for security impact of modifying or removing this rule" -j ACCEPT
-A InstanceServices -d 169.254.169.254/32 -p tcp -m tcp --dport 80 -m comment --comment "See the Oracle-Provided Images section in the Oracle Cloud Infrastructure documentation for security impact of modifying or removing this rule" -j ACCEPT
-A InstanceServices -d 169.254.169.254/32 -p udp -m udp --dport 67 -m comment --comment "See the Oracle-Provided Images section in the Oracle Cloud Infrastructure documentation for security impact of modifying or removing this rule" -j ACCEPT
-A InstanceServices -d 169.254.169.254/32 -p udp -m udp --dport 69 -m comment --comment "See the Oracle-

```
Provided Images section in the Oracle Cloud Infrastructure documentation for security impact of modifying or removing this rule" -j ACCEPT
-A InstanceServices -d 169.254.169.254/32 -p udp -m udp --dport 123 -m comment --comment "See the Oracle-Provided Images section in the Oracle Cloud Infrastructure documentation for security impact of modifying or removing this rule" -j ACCEPT
-A InstanceServices -d 169.254.0.0/16 -p tcp -m tcp -m comment --comment "See the Oracle-Provided Images section in the Oracle Cloud Infrastructure documentation for security impact of modifying or removing this rule" -j REJECT --reject-with tcp-reset
-A InstanceServices -d 169.254.0.0/16 -p udp -m udp -m comment --comment "See the Oracle-Provided Images section in the Oracle Cloud Infrastructure documentation for security impact of modifying or removing this rule" -j REJECT --reject-with icmp-port-unreachable
COMMIT
# Completed on Thu Oct 19 15:25:17 2023
```

and once saved, I simply restarted iptables:

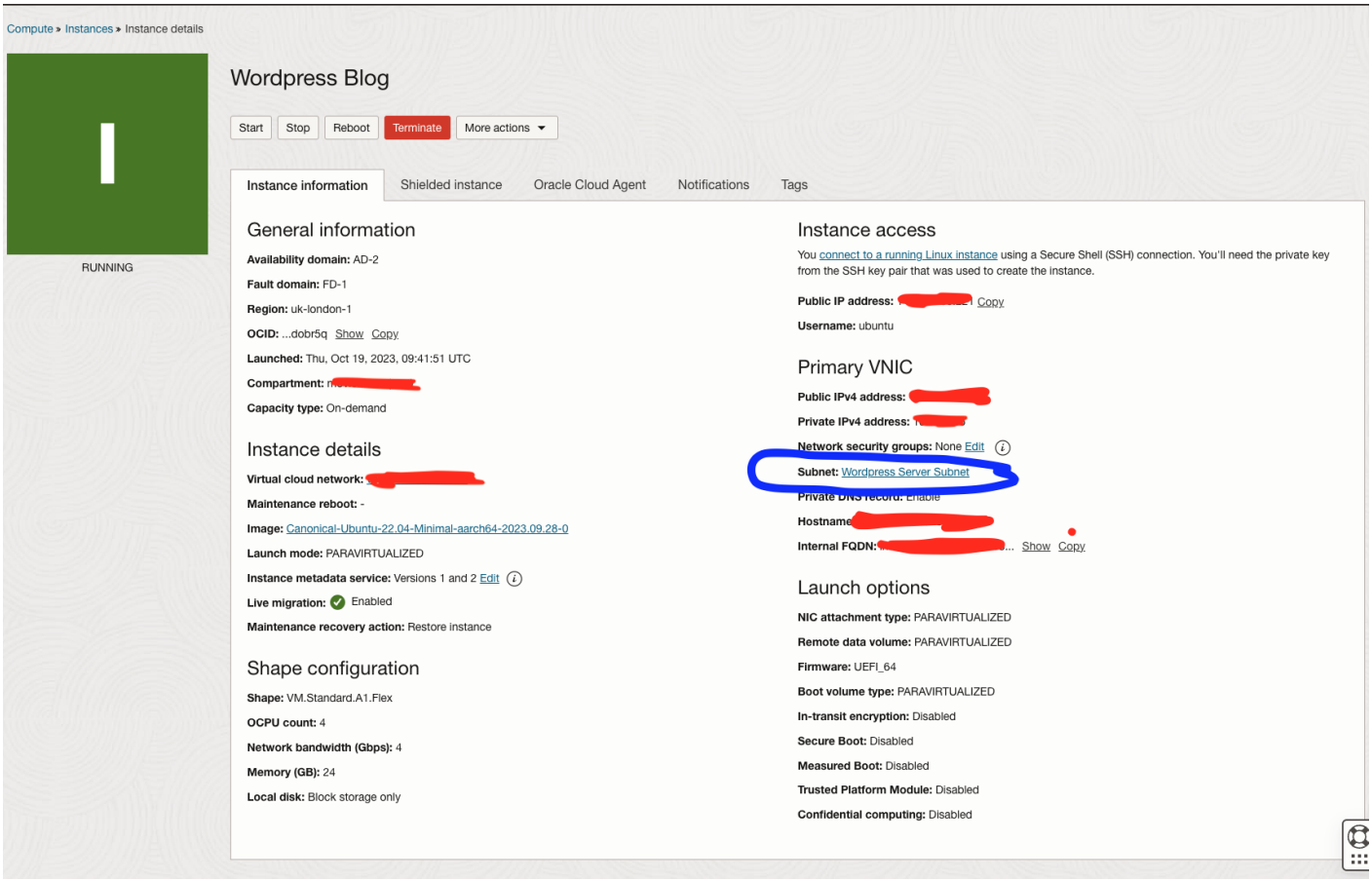
```
systemctl restart iptables
```

And everything worked!

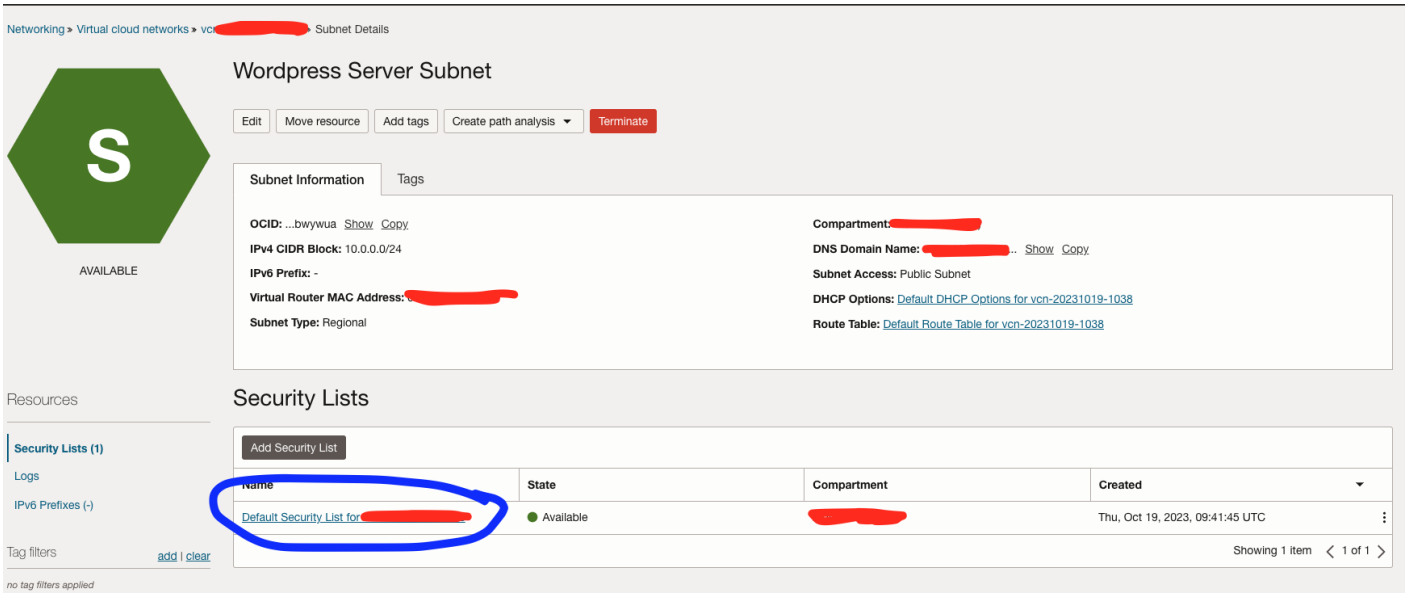
Setting up the Security Lists (firewall ingress/egress rules) for your Oracle VM

In this example, I only allow incoming SSH connections to a limited number of IP addresses, and all TLS traffic is allowed from Cloudflare IP address ranges.

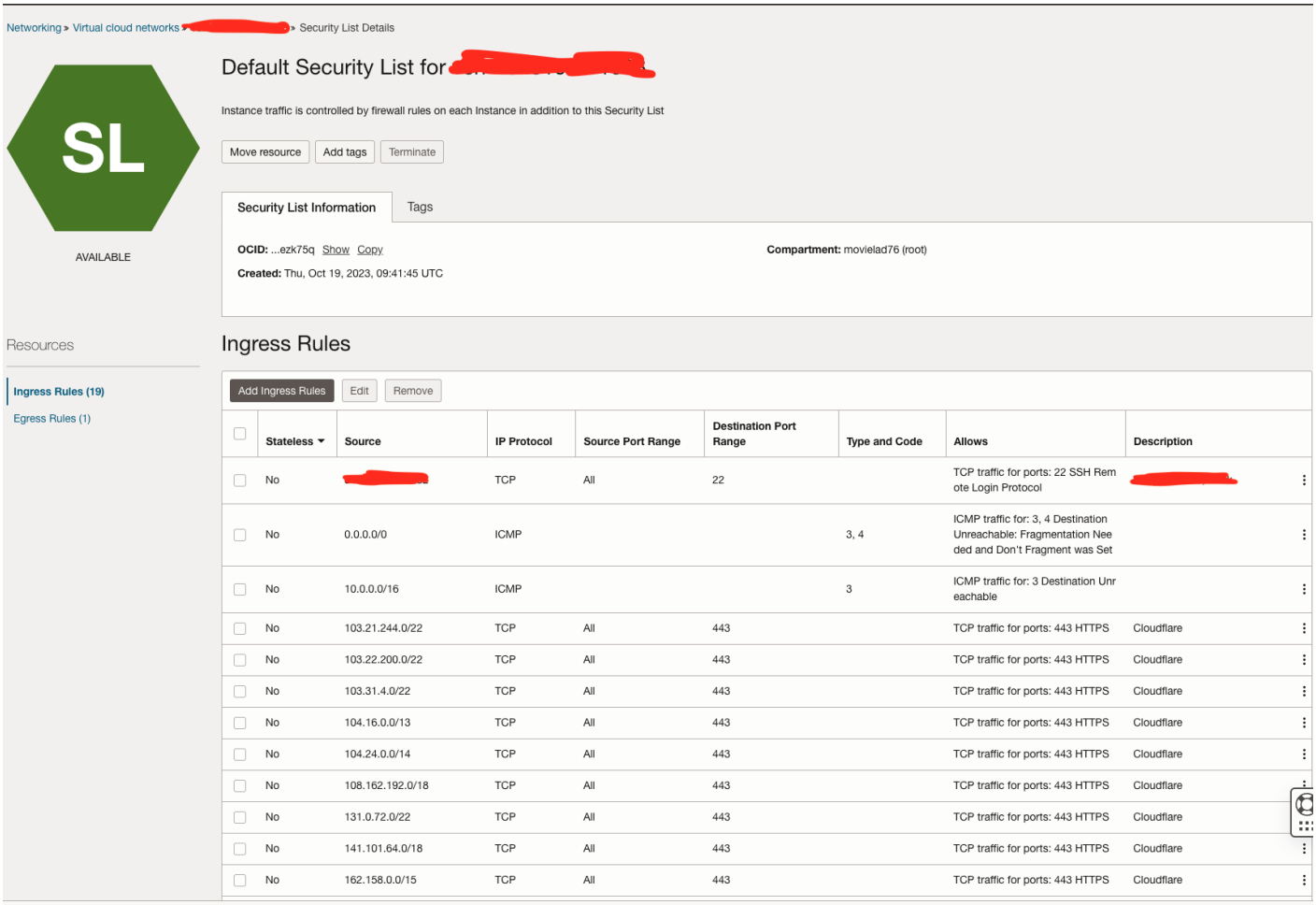
From the Instance page, click on the Subnet link (as shown in below circle):



Then click the Security List name associated with it (again, in blue circle):



Now you can define your rules:



Revision #9
Created 8 December 2023 13:46:07 by Martyn Drake
Updated 9 December 2023 04:32:37 by Martyn Drake