

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):

Compute > Instances > Instance details

Wordpress Blog

[Start](#) [Stop](#) [Reboot](#) [Terminate](#) [More actions](#)

Instance information [Shielded instance](#) [Oracle Cloud Agent](#) [Notifications](#) [Tags](#)

General information

Availability domain: AD-2
Fault domain: FD-1
Region: uk-london-1
OCID: ...dobr5q [Show](#) [Copy](#)
Launched: Thu, Oct 19, 2023, 09:41:51 UTC
Compartment: ...
Capacity type: On-demand

Instance details

Virtual cloud network: ...
Maintenance reboot: -
Image: [Canonical-Ubuntu-22.04-Minimal-aarch64-2023.09.28-0](#)
Launch mode: PARAVIRTUALIZED
Instance metadata service: Versions 1 and 2 [Edit](#) ⓘ
Live migration: Enabled
Maintenance recovery action: Restore instance

Shape configuration

Shape: VM.Standard.A1.Flex
OCPU count: 4
Network bandwidth (Gbps): 4
Memory (GB): 24
Local disk: Block storage only

Instance access

You [connect to a running Linux instance](#) using a Secure Shell (SSH) connection. You'll need the private key from the SSH key pair that was used to create the instance.

Public IP address: ... [Copy](#)
Username: ubuntu

Primary VNIC

Public IPv4 address: ...
Private IPv4 address: ...
Network security groups: None [Edit](#) ⓘ
Subnet: [Wordpress Server Subnet](#)
Private DNS record: Enable
Hostname: ...
Internal FQDN: ... [Show](#) [Copy](#)

Launch options

NIC attachment type: PARAVIRTUALIZED
Remote data volume: PARAVIRTUALIZED
Firmware: UEFI_64
Boot volume type: PARAVIRTUALIZED
In-transit encryption: Disabled
Secure Boot: Disabled
Measured Boot: Disabled
Trusted Platform Module: Disabled
Confidential computing: Disabled

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

Networking > Virtual cloud networks > vcn-20231019-1038 > Subnet Details

Wordpress Server Subnet

[Edit](#) [Move resource](#) [Add tags](#) [Create path analysis](#) [Terminate](#)

Subnet Information [Tags](#)

OCID: ...bwywua [Show](#) [Copy](#)
IPv4 CIDR Block: 10.0.0.0/24
IPv6 Prefix: -
Virtual Router MAC Address: ...
Subnet Type: Regional

Compartment: ...
DNS Domain Name: ... [Show](#) [Copy](#)
Subnet Access: Public Subnet
DHCP Options: [Default DHCP Options for vcn-20231019-1038](#)
Route Table: [Default Route Table for vcn-20231019-1038](#)

Security Lists

[Add Security List](#)

Name	State	Compartment	Created
Default Security List for vcn-20231019-1038	Available	...	Thu, Oct 19, 2023, 09:41:45 UTC

Showing 1 item < 1 of 1 >

Now you can define your rules:



AVAILABLE

Default Security List for

Instance traffic is controlled by firewall rules on each Instance in addition to this Security List

[Move resource](#) [Add tags](#) [Terminate](#)

Security List Information Tags

OCID: ...ezk75q [Show](#) [Copy](#) **Compartment:** movielad76 (root)
Created: Thu, Oct 19, 2023, 09:41:45 UTC

Resources

Ingress Rules (19)
[Egress Rules \(1\)](#)

Ingress Rules

Add Ingress Rules Edit Remove								
<input type="checkbox"/>	Stateless ▾	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	Description
<input type="checkbox"/>	No		TCP	All	22		TCP traffic for ports: 22 SSH Remote Login Protocol	
<input type="checkbox"/>	No	0.0.0.0/0	ICMP			3, 4	ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set	
<input type="checkbox"/>	No	10.0.0.0/16	ICMP			3	ICMP traffic for: 3 Destination Unreachable	
<input type="checkbox"/>	No	103.21.244.0/22	TCP	All	443		TCP traffic for ports: 443 HTTPS	Cloudflare
<input type="checkbox"/>	No	103.22.200.0/22	TCP	All	443		TCP traffic for ports: 443 HTTPS	Cloudflare
<input type="checkbox"/>	No	103.31.4.0/22	TCP	All	443		TCP traffic for ports: 443 HTTPS	Cloudflare
<input type="checkbox"/>	No	104.16.0.0/13	TCP	All	443		TCP traffic for ports: 443 HTTPS	Cloudflare
<input type="checkbox"/>	No	104.24.0.0/14	TCP	All	443		TCP traffic for ports: 443 HTTPS	Cloudflare
<input type="checkbox"/>	No	108.162.192.0/18	TCP	All	443		TCP traffic for ports: 443 HTTPS	Cloudflare
<input type="checkbox"/>	No	131.0.72.0/22	TCP	All	443		TCP traffic for ports: 443 HTTPS	Cloudflare
<input type="checkbox"/>	No	141.101.64.0/18	TCP	All	443		TCP traffic for ports: 443 HTTPS	Cloudflare
<input type="checkbox"/>	No	162.158.0.0/15	TCP	All	443		TCP traffic for ports: 443 HTTPS	Cloudflare