

20181109_caixabank_portforwarding

Goal

Permitir tráfico del puerto entrante al puerto 8158 del servidor local pasar a otro servidor en una red privada por el puerto 11580

Steps

- 1.- Create Instance in Public Subnet
- 2.- Add VNIC in Private Subnet
- 3.- Launch OS script to configure second interface
- 4.- Install rinetd package
- 5.- Configure rinetd
- 6.- Open local firewall
- 7.- Open destination local firewall
- 8.- Start rinetd service

Details

Create Instance in Public Subnet

Create Compute Instance

Oracle Cloud Infrastructure Compute lets you provision and manage compute hosts, known as instances. You can launch instances as needed to meet your compute and application requirements.


Name your instance

PFW2a

Select an availability domain for your instance

AD 1 CpyX:EU-FRANKFURT-1-AD-1	AD 2 CpyX:EU-FRANKFURT-1-AD-2 ✓	AD 3 CpyX:EU-FRANKFURT-1-AD-3
----------------------------------	------------------------------------	----------------------------------

Choose an operating system or image source



Oracle Linux 7.5
Image Build: 2018.10.16-0

The Unbreakable Enterprise Kernel (UEK) is Oracle's optimized operating system kernel for demanding Oracle workloads. GPU shapes are supported with this image.

Change Image Source

Choose instance type

Virtual Machine A virtual machine is an independent computing environment that runs on top of physical bare metal hardware. ✓	Bare Metal Machine A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation.
--	--

Choose instance shape

VM.Standard1.1

1 Core OCPU, 7 GB Memory

Change Shape

Configure boot volume

Default boot volume size: 46.6 GB

☐ Custom boot volume size (in GB)

☐ Choose a key from Key Management to encrypt this volume

Add SSH key

☐ Choose SSH key file ☒ Paste SSH keys

SSH key

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAC74zPR43mGkwK+w9Azu/UsHdaGGFL9BsyLRj+nFjLyzsO03ED+jF43GfYk4ipafE2ndjzPRT3laetYALg3rr

+

Configure networking

Virtual cloud network compartment

OEMM

caixamarzo18 (root)/OEMM

Virtual cloud network

OEMM_VCN

Subnet compartment

OEMM

caixamarzo18 (root)/OEMM

Subnet

Public_2_OEMM

[Show Advanced Options](#)

Create

Add VNIC in Private Subnet

Create VNIC

[cancel](#)

VNIC Information

If the Virtual Cloud Network, or Subnet is in a different Compartment than the VNIC, enable Compartment selection for those resources: [Click here](#).

NAME (Optional)

PFW2a

VIRTUAL CLOUD NETWORK

OEMM_VCN

SUBNET

Private_2_OEMM



☒ Skip Source/Destination Check

The source/destination check causes this VNIC to drop any network traffic whose source or destination is not this VNIC. Only check the checkbox if you want this VNIC to skip the check and forward that traffic (for example, to perform Network Address Translation).

Attached VNICs

Displaying 2 Attached VNICs

[Create VNIC](#)

	<p>PFW2a <small>(Primary VNIC)</small></p> <p>OCID: ...ji67va Show Copy</p> <p>Attached: Fri, 09 Nov 2018 15:14:24 GMT</p> <p>Compartment: OEMM</p>	<p>Private IP Address: 10.0.12.6</p> <p>Fully Qualified Domain Name: pfw2a... Show Copy</p> <p>Public IP Address: 130.61.57.93</p>	<p>Subnet: Public_2_OEMM</p> <p>Skip Source/Destination Check: No</p> <p>MAC Address: 02:00:17:02:89:47</p> <p>VLAN Tag: 1823</p>
	<p>PFW2a</p> <p>OCID: ...qbpkoq Show Copy</p> <p>Attached: Fri, 09 Nov 2018 15:17:40 GMT</p> <p>Compartment: OEMM</p>	<p>Private IP Address: 10.0.22.6</p> <p>Fully Qualified Domain Name: <i>Unavailable</i></p> <p>Public IP Address:</p>	<p>Subnet: Private_2_OEMM</p> <p>Skip Source/Destination Check: Yes</p> <p>MAC Address: 02:00:17:02:72:37</p> <p>VLAN Tag: 1825</p>

Launch OS script to configure second interface

```
/usr/local/bin/secondary_vnic_all_configure.sh -c
ifconfig
ip route
```

```

[opc@pfw2a ~]$ sudo -s
[root@pfw2a opc]# cd /usr/local/bin
[root@pfw2a bin]# vi secondary_vnic_all_configure.sh
[root@pfw2a bin]# chmod u+x secondary_vnic_all_configure.sh
[root@pfw2a bin]# ./secondary_vnic_all_configure.sh -c
Info: adding IP config for VNIC MAC 02:00:17:02:72:37 with id ocid1.vnic.oc1.eu-frankfurt-1.abtheljt4bzfmplxbrfj2d3qrbwx3gcq47y73niawzmp34i2u347jmqbpkoq
Info: added IP address 10.0.22.6 on interface ens4 with MTU 9000
Info: added rule for routing from 10.0.22.6 lookup ort1 with default via 10.0.22.1
Info: added rule for routing from 10.0.12.6 lookup ort0 with default via 10.0.12.1
[root@pfw2a bin]# ifconfig
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9000
    inet 10.0.12.6 netmask 255.255.255.0 broadcast 10.0.12.255
    ether 02:00:17:02:89:47 txqueuelen 1000 (Ethernet)
    RX packets 50492 bytes 306871197 (292.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 57344 bytes 282030166 (268.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

ens4: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9000
    inet 10.0.22.6 netmask 255.255.255.0 broadcast 0.0.0.0
    ether 02:00:17:02:72:37 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    loop txqueuelen 1000 (Local Loopback)
    RX packets 10 bytes 692 (692.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 10 bytes 692 (692.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@pfw2a bin]# ip route
default via 10.0.12.1 dev ens3
10.0.12.0/24 dev ens3 proto kernel scope link src 10.0.12.6
10.0.22.0/24 dev ens4 proto kernel scope link src 10.0.22.6
169.254.0.0/16 dev ens3 proto static scope link
169.254.0.0/16 dev ens3 scope link metric 1002
[root@pfw2a bin]#

```

Install rinetd package

wget http://li.nux.ro/download/nux/misc/el6/x86_64//rinetd-0.62-9.el6.nux.x86_64.rpm
rpm -i rinetd-0.62-9.el6.nux.x86_64.rpm

```

[root@pfw2a bin]# wget http://li.nux.ro/download/nux/misc/el6/x86_64//rinetd-0.62-9.el6.nux.x86_64.rpm
--2018-11-09 15:20:04-- http://li.nux.ro/download/nux/misc/el6/x86_64//rinetd-0.62-9.el6.nux.x86_64.rpm
Resolving li.nux.ro (li.nux.ro)... 217.19.15.108
Connecting to li.nux.ro (li.nux.ro)|217.19.15.108|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 24664 (24K) [application/x-rpm]
Saving to: 'rinetd-0.62-9.el6.nux.x86_64.rpm'

100%[=====>] 24,664 --.-K/s in 0.03s

2018-11-09 15:20:05 (774 KB/s) - 'rinetd-0.62-9.el6.nux.x86_64.rpm' saved [24664/24664]

[root@pfw2a bin]# rpm -i rinetd-0.62-9.el6.nux.x86_64.rpm
warning: rinetd-0.62-9.el6.nux.x86_64.rpm: Header V4 RSA/SHA1 Signature, key ID 85c6cd8a: NOKEY
[root@pfw2a bin]#

```

Configure rinetd

```
[root@pfw2a bin]# cat /etc/rinetd.conf
# example configuration file for rinetd
#
#
# to forward connections to port 80 on 10.10.10.2 to port 80 on 192.168.0.2
# 10.10.10.2 80 192.168.0.2 80
#
# to forward connections to port 80 on all addresses to port 80 on 192.168.0.2
# 0.0.0.0 80 192.168.0.2 80
#
# access controls can be set with allow and deny rules
# allow and deny before the first forwarding rule are global
# allow and deny after a specific rule apply to it only
#
# this rule allows hosts from 172.16.32.0/24 netblock
# allow 172.16.32.*
#
# this rule denies the host 192.168.32.12
# deny 192.168.32.12
#
# rinetd supports logging - to enable, uncomment the following
logfile /var/log/rinetd.log
#
# by default, logs are in a tab-delimited format. Web common-log format
# is available by uncommenting the following
logcommon
#
# redirect from public to private OEMM
10.0.12.6 8158 10.0.22.3 11580
```

Open local firewall

```
iptables -A IN_public_allow -p tcp --dport 8158 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
iptables -n -L
```

```
[root@pfw2a bin]# iptables -A IN_public_allow -p tcp --dport 8158 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
[root@pfw2a bin]# iptables -n -L IN_public_allow
Chain IN_public_allow (1 references)
target      prot opt source                destination           tcp dpt:22 ctstate NEW
ACCEPT      tcp  --  0.0.0.0/0              0.0.0.0/0             tcp dpt:8158 ctstate NEW,ESTABLISHED
```

Open destination local firewall

```
iptables -A IN_public_allow -p tcp --sport 11580 -m conntrack --ctstate NEW,ESTABLISHED -j
ACCEPT
```

```
iptables -A IN_public_allow -p tcp --dport 11580 -m conntrack NEW,ESTABLISHED -j ACCEPT
[root@oem2 ope]# iptables -n -L IN_public_allow
Chain IN_public_allow (1 references)
target    prot opt source                destination           tcp dpt:22 ctstate NEW
ACCEPT    tcp  --  0.0.0.0/0              0.0.0.0/0             tcp dpt:5902
ACCEPT    tcp  --  0.0.0.0/0              0.0.0.0/0             tcp dpt:80
ACCEPT    tcp  --  0.0.0.0/0              0.0.0.0/0             tcp dpt:11580 ctstate NEW,ESTABLISHED
```

Start rinetd service

```
systemctl start rinetd.service
systemctl status rinetd.service
```

```
[root@pfw2a bin]# systemctl start rinetd.service
[root@pfw2a bin]# systemctl status rinetd.service
• rinetd.service - SYSV: rinetd is a TCP redirection server
  Loaded: loaded (/etc/rc.d/init.d/rinetd; bad; vendor preset: disabled)
  Active: active (running) since Fri 2018-11-09 15:32:26 GMT; 6s ago
    Docs: man:systemd-sysv-generator(8)
  Process: 13718 ExecStart=/etc/rc.d/init.d/rinetd start (code=exited, status=0/SUCCESS)
  CGroup: /system.slice/rinetd.service
          └─13727 /usr/sbin/rinetd

Nov 09 15:32:26 pfw2a systemd[1]: Starting SYSV: rinetd is a TCP redirection server...
Nov 09 15:32:26 pfw2a rinetd[13718]: Starting rinetd: [ OK ]
Nov 09 15:32:26 pfw2a systemd[1]: Started SYSV: rinetd is a TCP redirection server.
```

```
systemctl enable rinetd
systemctl check rinetd
```

```
[root@pfw2a ope]# systemctl enable rinetd
rinetd.service is not a native service, redirecting to /sbin/chkconfig.
Executing /sbin/chkconfig rinetd on
[root@pfw2a ope]# systemctl check rinetd
active
```