Goal

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

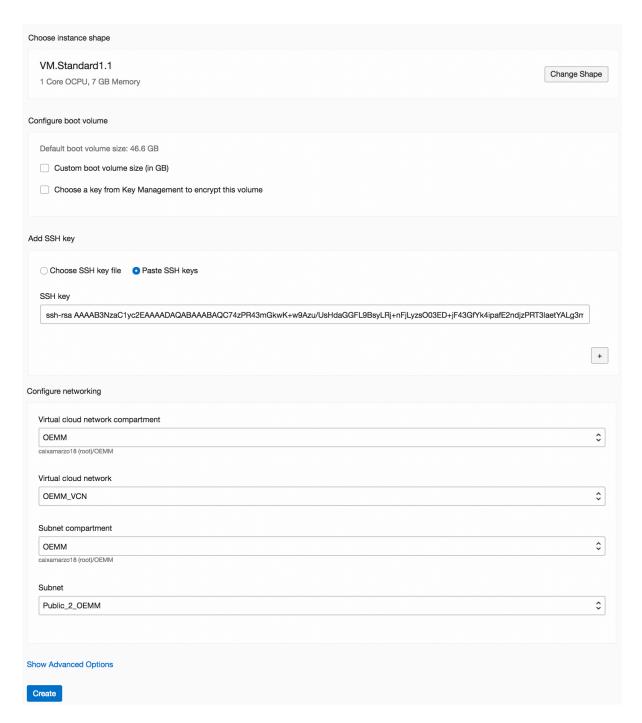
Steps

- 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

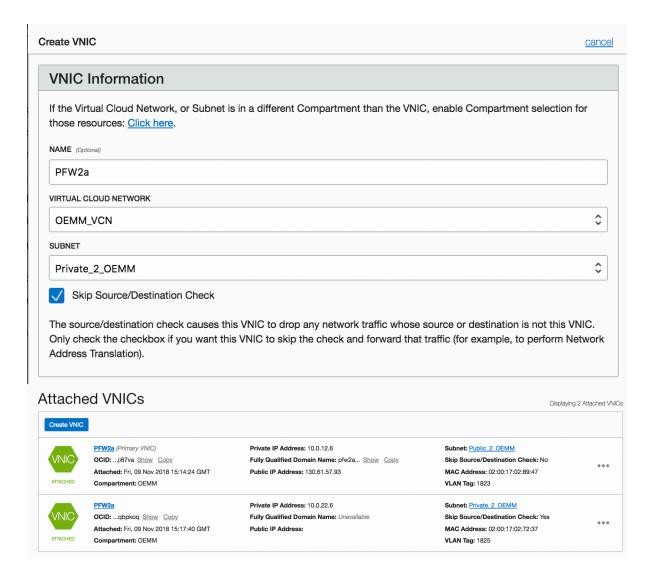
Details

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 applica Name your instance PFW2a Select an availability domain for your instance AD 1 AD 2 AD 3 CpyX:EU-FRANKFURT-1-AD-1 CpyX:EU-FRANKFURT-1-AD-2 CpyX:EU-FRANKFURT-1-AD-3 Choose an operating system or image source Oracle Linux 7.5 ORACLE Image Build: 2018.10.16-0 Change Image Source The Unbreakable Enterprise Kernel (UEK) is Oracle's optimized operating system kernel for demanding Oracle workloads. GPU shapes are supported with this image. Choose instance type Virtual Machine Bare Metal Machine A virtual machine is an independent computing environment that runs on A bare metal compute instance gives you dedicated physical server top of physical bare metal hardware. access for highest performance and strong isolation.



Add VNIC in Private Subnet



Launch OS script to configure second interface

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

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

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

Open destination local firewall

iptables -A IN public allow -p tcp —sport 11580 -m contract NEW,ESTABLISHED -j ACCEPT

```
[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
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 ctstate NEW
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:8158 ctstate NEW,ESTABLISHED
```

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

systematl start rinetd.service systematl status rinetd.service

systemctl enable rinetd systemctl check rinetd

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