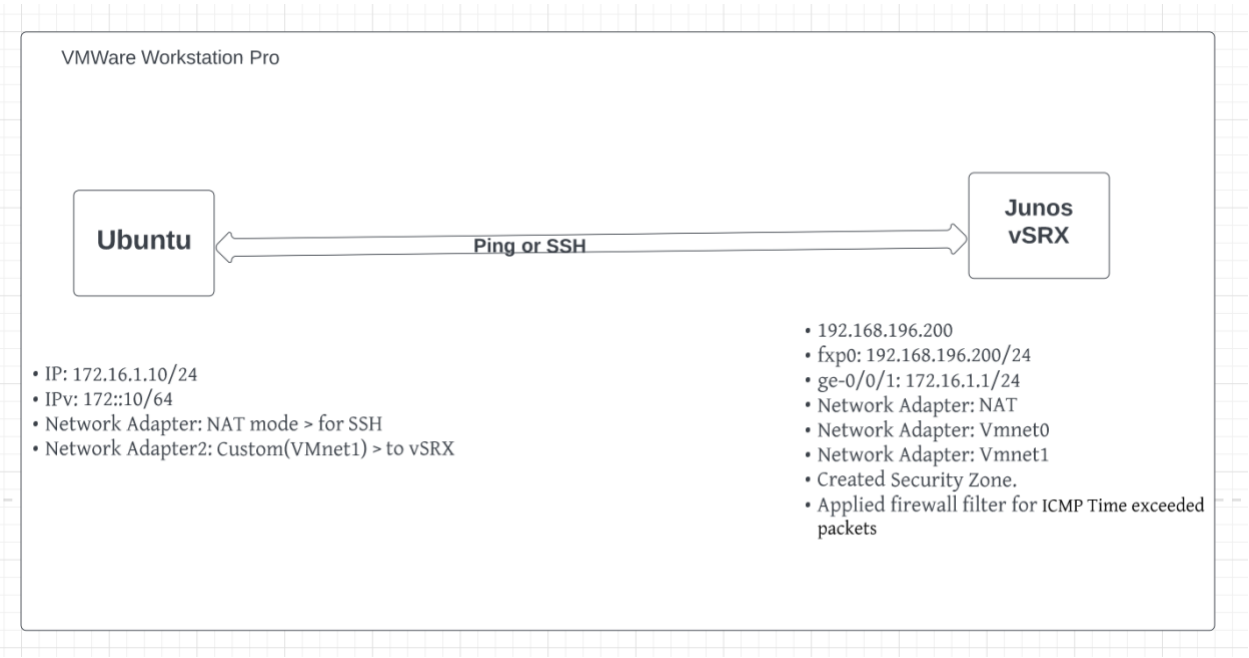
Juniper SIRT PSE Internship 2023 – Round 1 (vSRX Challenge)

Name: Harsha SG
Email: harshasiddapura98@gmail.com
Phone: 316-734-7836

Lab Topology:



1. **show system license.**

```
root> show system license
License usage:
                                 Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  logical-system                        1            3           0    permanent
  Virtual Appliance                     1            1           0    59 days
  remote-access-ipsec-vpn-client        0            2           0    permanent
  remote-access-juniper-std             0            2           0    permanent

Licenses installed:
  License identifier: E420588955
  License version: 4
  Software Serial Number: 20150625
  Customer ID: vSRX-JuniperEval
  Features:
    Virtual Appliance - Virtual Appliance
      count-down, Original validity: 60 days

root>
```

2. **show chassis hardware.**

```
root> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                3ef320cabc0f      VSRX
Midplane
System IO
Routing Engine                                           VSRX-2CPU-4G memory
FPC 0                     BUILTIN      BUILTIN           FPC
  PIC 0                                                  VSRX DPDK GE
Power Supply 0

root>
```

3. **Show chassis fpc pic-status.**

```
root> show chassis fpc pic-status
Slot 0   Online       FPC
  PIC 0  Online       VSRX DPDK GE

root>
```

4. **show interfaces.**

```
root> show interfaces terse ge-0/0/1
Interface               Admin Link Proto    Local                 Remote
ge-0/0/1                up    up
ge-0/0/1.0              up    up   inet     172.16.1.1/24
                                   inet6    172::1/64
                                            fe80::20c:29ff:feca:bc23/64

root> show interfaces terse fxp0
Interface               Admin Link Proto    Local                 Remote
fxp0                    up    up
fxp0.0                  up    up   inet     192.168.196.200/24

root>
```

5. (Optional) Ping and/or SSH between the hosts

- Ping and SSH both working from Ubuntu server to vSRX on 192.168.196.200.

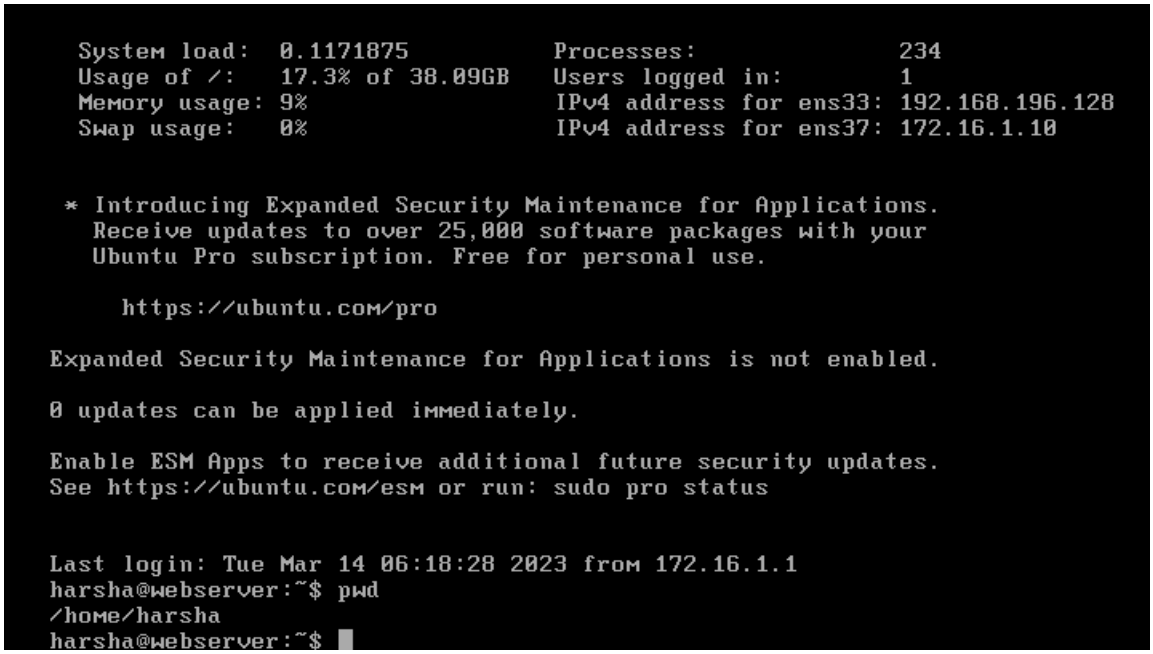
```
root@webserver:~# ping 192.168.196.200
PING 192.168.196.200 (192.168.196.200) 56(84) bytes of data.
64 bytes from 192.168.196.200: icmp_seq=1 ttl=64 time=3.51 ms
64 bytes from 192.168.196.200: icmp_seq=2 ttl=64 time=0.522 ms
64 bytes from 192.168.196.200: icmp_seq=3 ttl=64 time=0.597 ms
64 bytes from 192.168.196.200: icmp_seq=4 ttl=64 time=2.79 ms
64 bytes from 192.168.196.200: icmp_seq=5 ttl=64 time=0.614 ms
64 bytes from 192.168.196.200: icmp_seq=6 ttl=64 time=0.567 ms
64 bytes from 192.168.196.200: icmp_seq=7 ttl=64 time=0.887 ms
64 bytes from 192.168.196.200: icmp_seq=8 ttl=64 time=0.537 ms
^C
--- 192.168.196.200 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7081ms
rtt min/avg/max/mdev = 0.522/1.252/3.506/1.113 ms
root@webserver:~# ssh root@192.168.196.200
(root@192.168.196.200) Password:
Last login: Mon Mar 13 21:43:41 2023 from 192.168.196.128
--- JUNOS 20.3R1.8 Kernel 64-bit XEN JNPR-11.0-20200908.87c9d89_buil
root@:~ # cli
root> show version | match :
Model: vSRX
Junos: 20.3R1.8

root> configure
Entering configuration mode

[edit]
root# _
```

- Ping and SSH both working from vSRX to Ubuntu server on 172.16.1.10.

```
root@:~ # ping 172.16.1.10
PING 172.16.1.10 (172.16.1.10): 56 data bytes
64 bytes from 172.16.1.10: icmp_seq=0 ttl=64 time=1.960 ms
64 bytes from 172.16.1.10: icmp_seq=1 ttl=64 time=1.032 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=64 time=0.715 ms
64 bytes from 172.16.1.10: icmp_seq=3 ttl=64 time=1.337 ms
^C
--- 172.16.1.10 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.715/1.261/1.960/0.460 ms
root@:~ #
```



1. **Apply and share the configuration for a firewall filter on an vSRX interface for ICMP Time exceeded packets. What kind of traffic will be affected from this filter? Please explain.**

- set firewall family inet filter allow-icmp-term term allow-icmp from protocol icmp
- set firewall family inet filter allow-icmp-term term allow-icmp from icmp-type time-exceeded
- set firewall family inet filter allow-icmp-term term allow-icmp then accept

This firewall filter will allow ICMP Time Exceeded packets to pass through the vSRX interface. ICMP Time Exceeded packets are generated by routers when they cannot forward an IP datagram because the time-to-live (TTL) field has reached zero. These packets are part of the ICMP protocol and are used to signal network errors to the source host.

By allowing ICMP Time Exceeded packets, this firewall filter will allow traceroute (also known as tracert) packets to pass through the vSRX interface. Traceroute is a tool that uses ICMP Time Exceeded packets to discover the path taken by packets across an IP network.

Additionally, other types of ICMP packets such as echo-request (ping) and destination-unreachable will be blocked by this firewall filter, as they are not explicitly allowed in the configuration.

Overall, this firewall filter will only affect traffic that uses ICMP Time Exceeded packets, which includes traceroute packets. All other traffic will be unaffected.

Bonus Q – Please capture an example of transit traffic passing through vSRX and share a pcap for the same.

fx01.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.196.1	192.168.196.254	BOOTP	364	[Packet size limited during capture]
2	0.000016	192.168.196.254	192.168.196.1	BOOTP	364	Boot Reply[Packet size limited during capture]
3	0.000380	VMware_ca:bc:0f	Broadcast	ARP	64	Who has 192.168.196.254? Tell 192.168.196.200
4	0.000902	VMware_ca:bc:0f	Broadcast	ARP	64	Who has 192.168.196.1? Tell 192.168.196.200
5	0.001330	VMware_f8:ec:33	VMware_ca:bc:0f	ARP	82	192.168.196.254 is at 00:50:56:f8:ec:33
6	0.001337	VMware_c0:00:08	VMware_ca:bc:0f	ARP	82	192.168.196.1 is at 00:50:56:c0:00:08
7	0.001348	192.168.196.1	192.168.196.254	BOOTP	364	[Packet size limited during capture]
8	0.001559	192.168.196.200	192.168.196.254	ICMP	92	Redirect (Redirect for host)
9	0.002160	192.168.196.200	192.168.196.1	ICMP	92	Redirect (Redirect for host)
10	0.002905	192.168.196.254	192.168.196.1	BOOTP	364	Boot Reply[Packet size limited during capture]
11	0.003199	192.168.196.254	192.168.196.1	BOOTP	364	Boot Reply[Packet size limited during capture]
12	0.003361	192.168.196.200	192.168.196.254	ICMP	92	Redirect (Redirect for host)
13	0.013014	192.168.196.254	192.168.196.1	BOOTP	364	Boot Reply[Packet size limited during capture]
14	0.018336	fe80::342a:ceaa:4e3…	ff02::16	ICMPv6	112	Multicast Listener Report Message v2[Packet size limited during capture]
15	0.018340	192.168.196.1	224.0.0.22	IGMPv3	82	Membership Report / Leave group 224.0.0.252
16	0.055180	fe80::342a:ceaa:4e3…	ff02::16	ICMPv6	112	Multicast Listener Report Message v2[Packet size limited during capture]
17	0.055187	192.168.196.1	224.0.0.22	IGMPv3	82	Membership Report / Join group 224.0.0.252 for any sources
18	0.056738	fe80::342a:ceaa:4e3…	ff02::16	ICMPv6	112	Multicast Listener Report Message v2[Packet size limited during capture]
19	0.056744	192.168.196.1	224.0.0.22	IGMPv3	82	Membership Report / Leave group 224.0.0.252
20	0.056750	fe80::342a:ceaa:4e3…	ff02::16	ICMPv6	112	Multicast Listener Report Message v2[Packet size limited during capture]
21	0.056751	192.168.196.1	224.0.0.22	IGMPv3	82	Membership Report / Join group 224.0.0.252 for any sources
22	0.058743	192.168.196.1	224.0.0.251	MDNS	94	Standard query 0x0000 ANY harsha.local, "QM" question
23	0.059412	fe80::342a:ceaa:4e3…	ff02::fb	MDNS	114	Standard query 0x0000[Packet size limited during capture]
24	0.059712	fe80::342a:ceaa:4e3…	ff02::fb	MDNS	152	Standard query response 0x0000[Packet size limited during capture]
25	0.059866	192.168.196.1	224.0.0.251	MDNS	132	Standard query response 0x0000[Packet size limited during capture]
26	0.340665	192.168.196.1	224.0.0.22	IGMPv3	82	Membership Report / Join group 224.0.0.252 for any sources
27	0.340673	fe80::342a:ceaa:4e3…	ff02::16	ICMPv6	112	Multicast Listener Report Message v2[Packet size limited during capture]

- Monitoring the ICMP packets receiving from Ubuntu to vSRX.

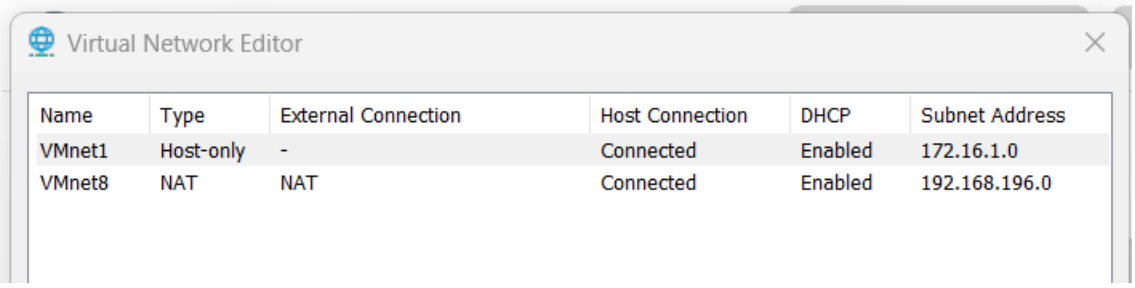
```
root> monitor traffic interface fxp0 matching "icmp"
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is ON. Use <no-resolve> to avoid any reverse lookup delay.
Address resolution timeout is 4s.
Listening on fxp0, capture size 96 bytes

Reverse lookup for 192.168.196.128 failed (check DNS reachability).
Other reverse lookup failures will not be reported.
Use <no-resolve> to avoid reverse lookups on IP addresses.

09:58:37.458193  In IP truncated-ip - 24 bytes missing! 192.168.196.128 > 192.16
8.196.200: ICMP echo request, id 6, seq 40, length 64
09:58:37.458207 Out IP truncated-ip - 24 bytes missing! 192.168.196.200 > 192.16
8.196.128: ICMP echo reply, id 6, seq 40, length 64
09:58:38.482268  In IP truncated-ip - 24 bytes missing! 192.168.196.128 > 192.16
8.196.200: ICMP echo request, id 6, seq 41, length 64
09:58:38.482294 Out IP truncated-ip - 24 bytes missing! 192.168.196.200 > 192.16
8.196.128: ICMP echo reply, id 6, seq 41, length 64
^C
6 packets received by filter
0 packets dropped by kernel
```

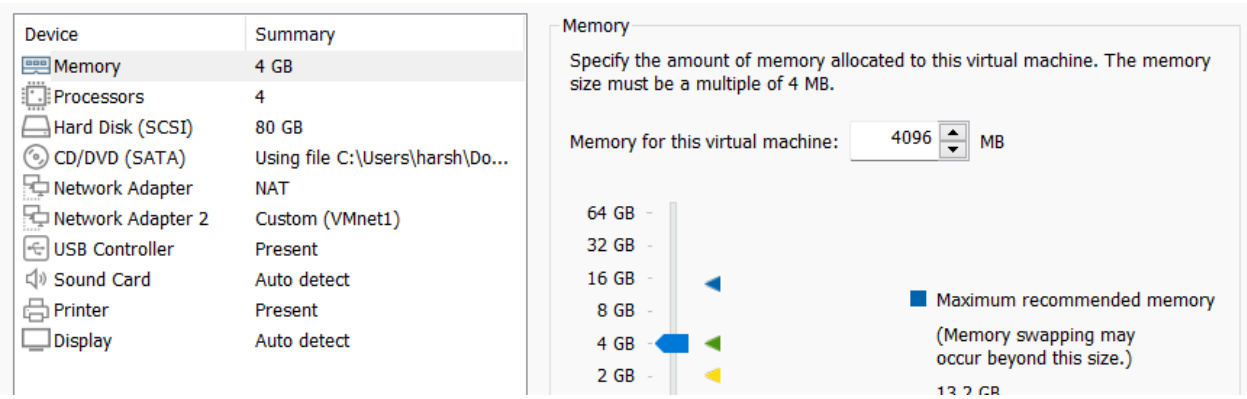
Networks setup snapshots:

VMware workstation pro



Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	Enabled	172.16.1.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.196.0

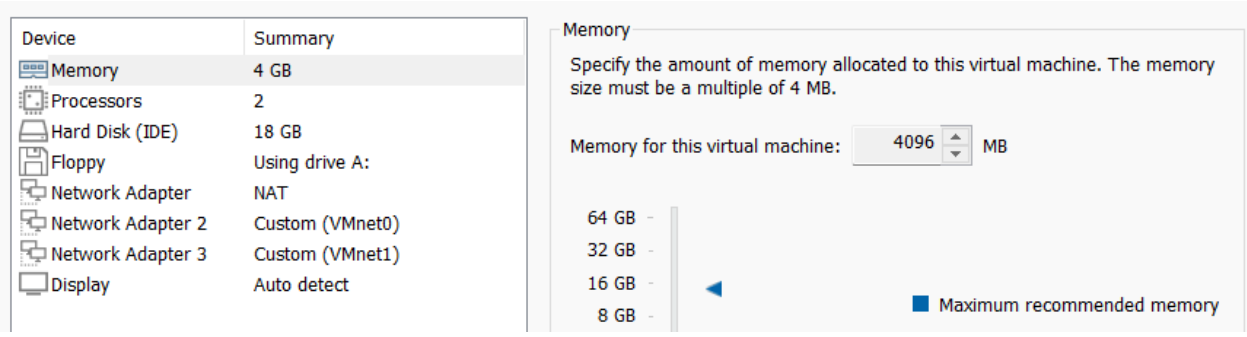
Network setup Ubuntu:




```
root@webserver:~# ip a show ens33
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:85:31:75 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.196.128/24 metric 100 brd 192.168.196.255 scope global dynamic ens33
       valid_lft 1533sec preferred_lft 1533sec
    inet6 fe80::20c:29ff:fe85:3175/64 scope link
       valid_lft forever preferred_lft forever
root@webserver:~# ip a show ens37
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:85:31:7f brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet 172.16.1.10/24 brd 172.16.1.255 scope global ens37
       valid_lft forever preferred_lft forever
    inet6 172::1/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe85:317f/64 scope link
       valid_lft forever preferred_lft forever
root@webserver:~#
```

```
root@webserver:~# ip r
default via 172.16.1.1 dev ens37 proto static
default via 192.168.196.2 dev ens33 proto dhcp src 192.168.196.128 metric 100
172.16.1.0/24 dev ens37 proto kernel scope link src 172.16.1.10
192.168.196.0/24 dev ens33 proto kernel scope link src 192.168.196.128 metric 100
192.168.196.2 dev ens33 proto dhcp scope link src 192.168.196.128 metric 100
root@webserver:~# ip -6 r
::1 dev lo proto kernel metric 256 pref medium
172::/64 dev ens37 proto kernel metric 256 pref medium
fe80::/64 dev ens37 proto kernel metric 256 pref medium
fe80::/64 dev ens33 proto kernel metric 256 pref medium
root@webserver:~# _
```

Network setup -vSRX




```
root@:~ # cli
root> show interfaces terse ge-0/0/1
Interface               Admin Link Proto    Local                 Remote
ge-0/0/1                up    up
ge-0/0/1.0              up    up   inet     172.16.1.1/24
                                  inet6    172::1/64
                                           fe80::20c:29ff:feca:bc23/64

root>
```

This is an automated email. Please do not reply to this email.
Please see instructions at the bottom of this message to communicate with Juniper Networks, Inc.

Dear HARSHA SIDDAPURA GNANESHWARA,

Thank you for purchasing products from Juniper Networks. This email is a confirmation of your registration and may be printed for your personal records.

Your Account Information

User ID : harshabidrae97@gmail.com
Email Address : harshabidrae97@gmail.com
First Name : HARSHA
Last Name : SIDDAPURA GNANESHWARA
Company : WICHITA STATE UNIVERSITY
