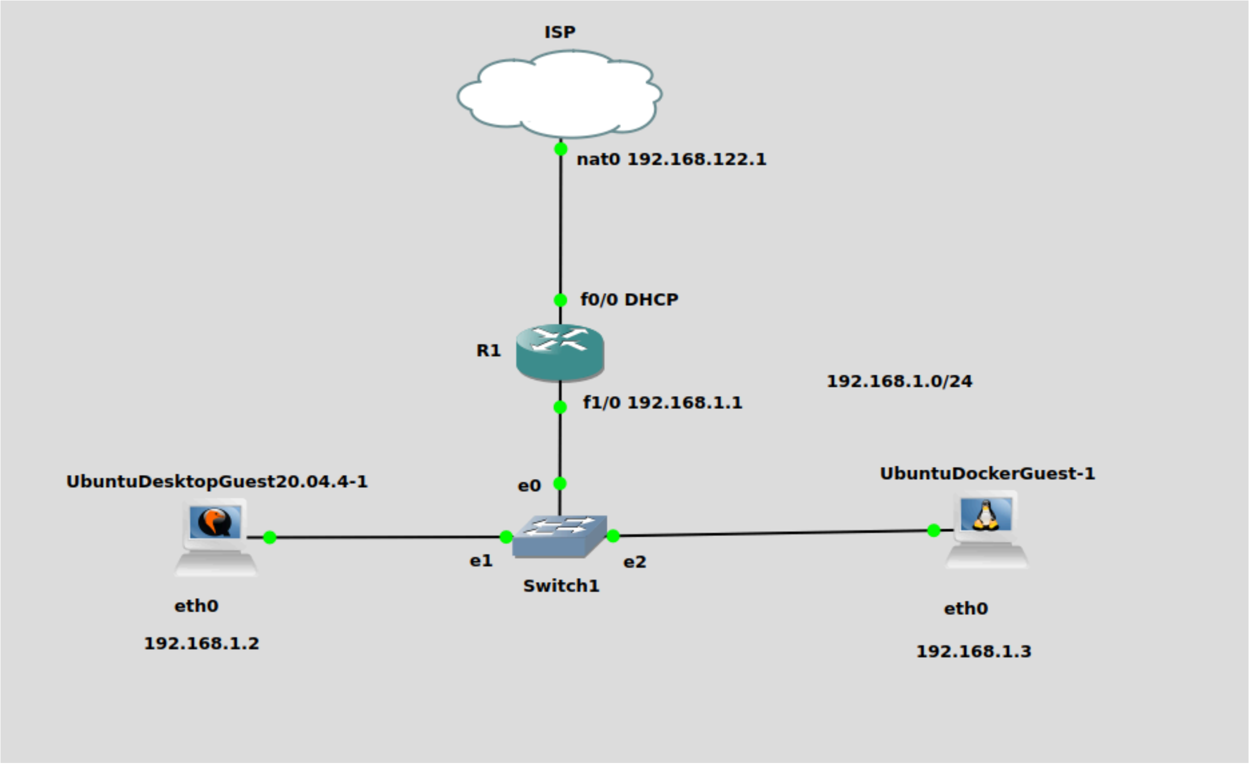
1.
Tarek Chaalan
Mason Chiang
Wayne Muse
Haron Taher
Bryan Corona

2.

-Screenshot of Topology:

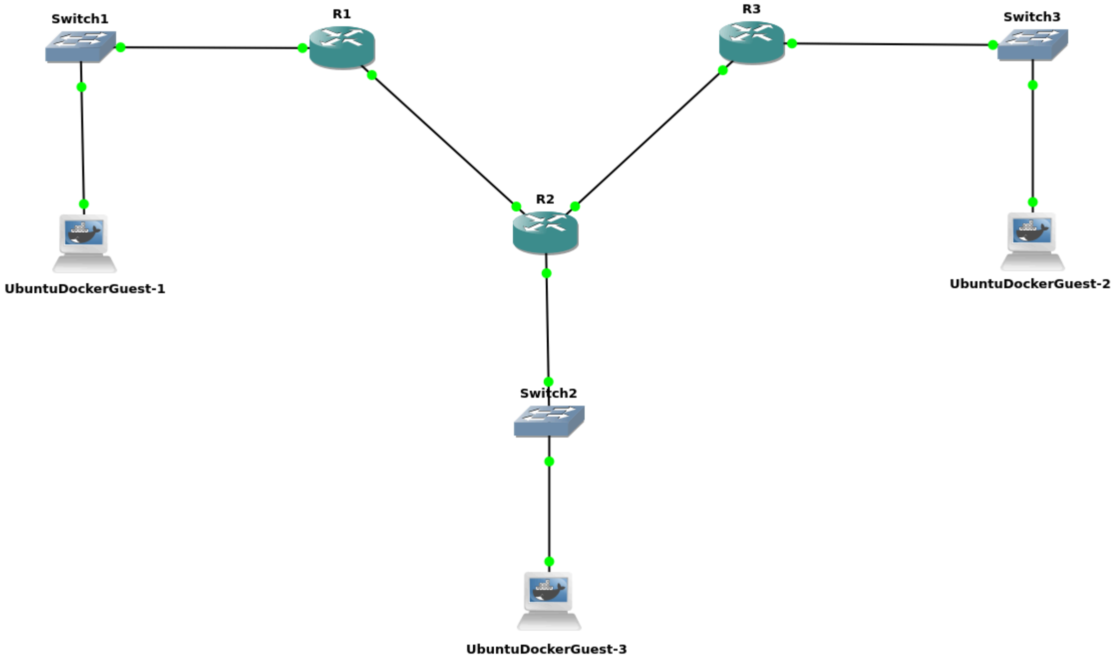


Config for router- uploaded on canvas for q2

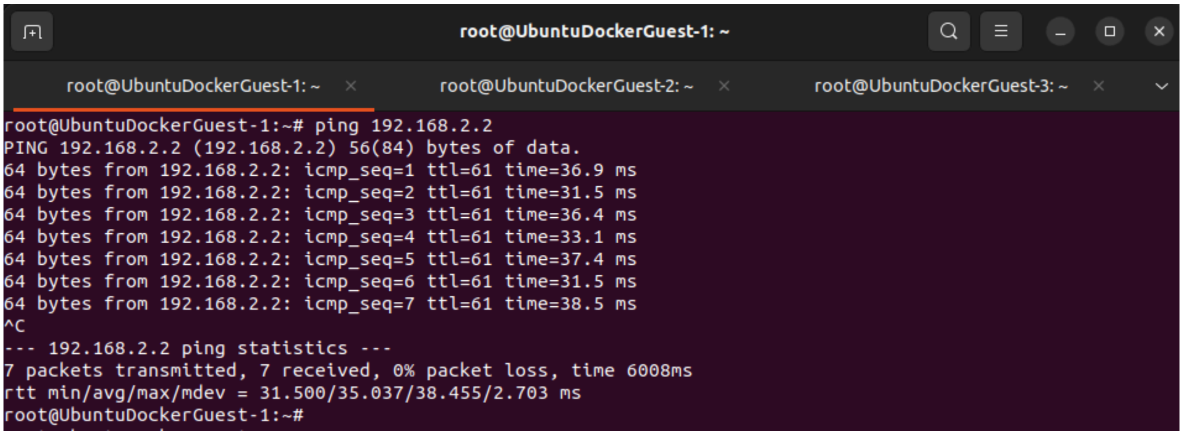
Config Files (Q2)

3.

- **Screenshot of Topology:**

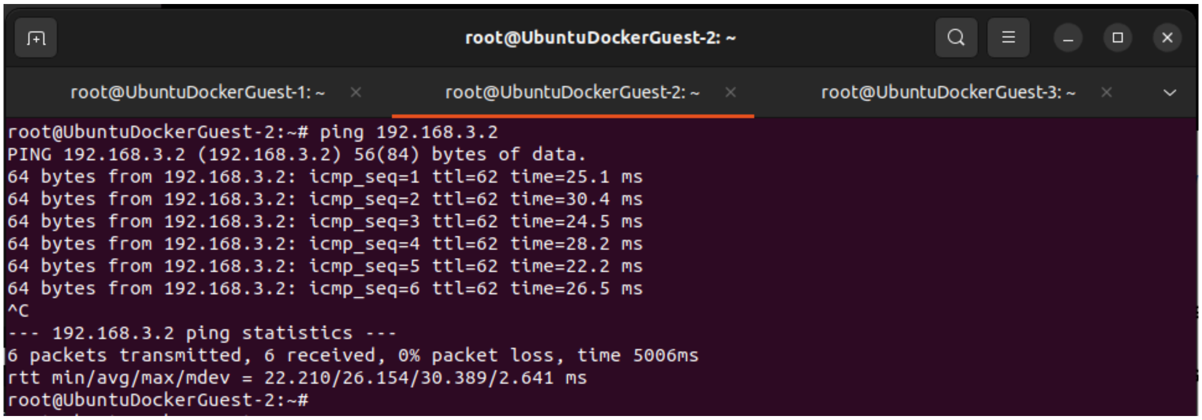


- **Screenshots of pings illustrating that each host can ping any other host:**
  - UbuntuDockerGuest-1 PINGING UbuntuDockerGuest-2


root@UbuntuDockerGuest-1: ~
root@UbuntuDockerGuest-1: ~
root@UbuntuDockerGuest-2: ~
root@UbuntuDockerGuest-3: ~

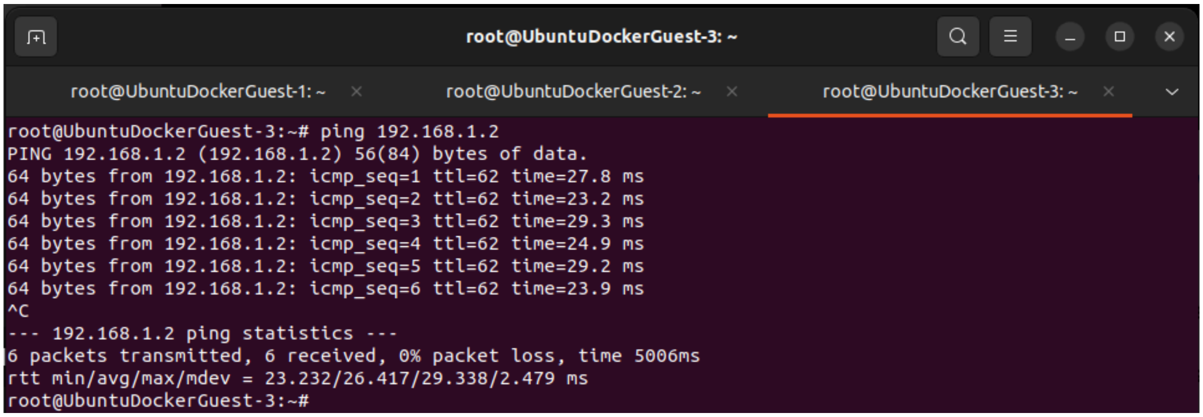
```
root@UbuntuDockerGuest-1:~# ping 192.168.2.2
PING 192.168.2.2 (192.168.2.2) 56(84) bytes of data.
64 bytes from 192.168.2.2: icmp_seq=1 ttl=61 time=36.9 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=61 time=31.5 ms
64 bytes from 192.168.2.2: icmp_seq=3 ttl=61 time=36.4 ms
64 bytes from 192.168.2.2: icmp_seq=4 ttl=61 time=33.1 ms
64 bytes from 192.168.2.2: icmp_seq=5 ttl=61 time=37.4 ms
64 bytes from 192.168.2.2: icmp_seq=6 ttl=61 time=31.5 ms
64 bytes from 192.168.2.2: icmp_seq=7 ttl=61 time=38.5 ms
^C
--- 192.168.2.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 31.500/35.037/38.455/2.703 ms
root@UbuntuDockerGuest-1:~#
```

  - UbuntuDockerGuest-2 PINGING UbuntuDockerGuest-3


root@UbuntuDockerGuest-2: ~
root@UbuntuDockerGuest-1: ~
root@UbuntuDockerGuest-2: ~
root@UbuntuDockerGuest-3: ~

```
root@UbuntuDockerGuest-2:~# ping 192.168.3.2
PING 192.168.3.2 (192.168.3.2) 56(84) bytes of data.
64 bytes from 192.168.3.2: icmp_seq=1 ttl=62 time=25.1 ms
64 bytes from 192.168.3.2: icmp_seq=2 ttl=62 time=30.4 ms
64 bytes from 192.168.3.2: icmp_seq=3 ttl=62 time=24.5 ms
64 bytes from 192.168.3.2: icmp_seq=4 ttl=62 time=28.2 ms
64 bytes from 192.168.3.2: icmp_seq=5 ttl=62 time=22.2 ms
64 bytes from 192.168.3.2: icmp_seq=6 ttl=62 time=26.5 ms
^C
--- 192.168.3.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 22.210/26.154/30.389/2.641 ms
root@UbuntuDockerGuest-2:~#
```

- UbuntuDockerGuest-3 PINGING UbuntuDockerGuest-1

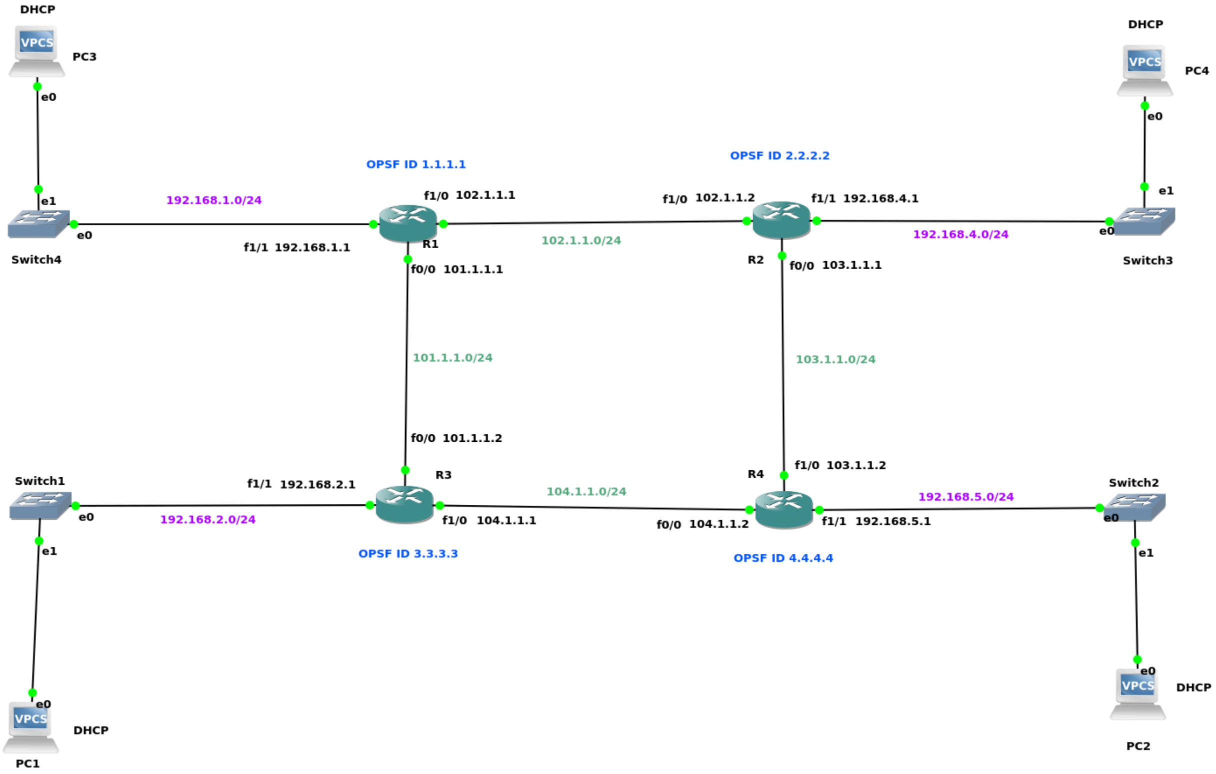

root@UbuntuDockerGuest-3: ~
root@UbuntuDockerGuest-1: ~
root@UbuntuDockerGuest-2: ~
root@UbuntuDockerGuest-3: ~

```
root@UbuntuDockerGuest-3:~# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=62 time=27.8 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=62 time=23.2 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=62 time=29.3 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=62 time=24.9 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=62 time=29.2 ms
64 bytes from 192.168.1.2: icmp_seq=6 ttl=62 time=23.9 ms
^C
--- 192.168.1.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5006ms
rtt min/avg/max/mdev = 23.232/26.417/29.338/2.479 ms
root@UbuntuDockerGuest-3:~#
```

- **Configuration files for each Router:**

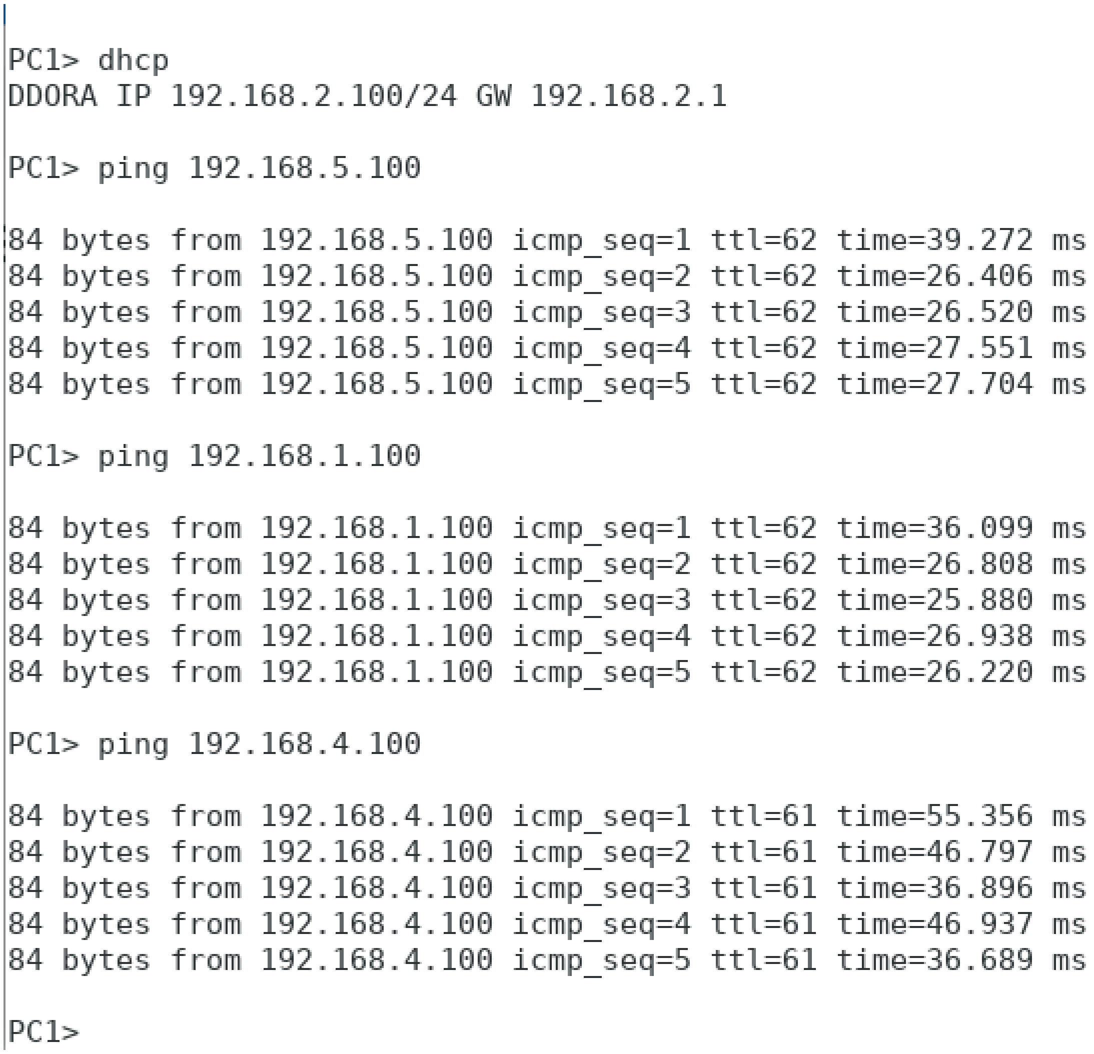
  Config Files (Q3)

4.



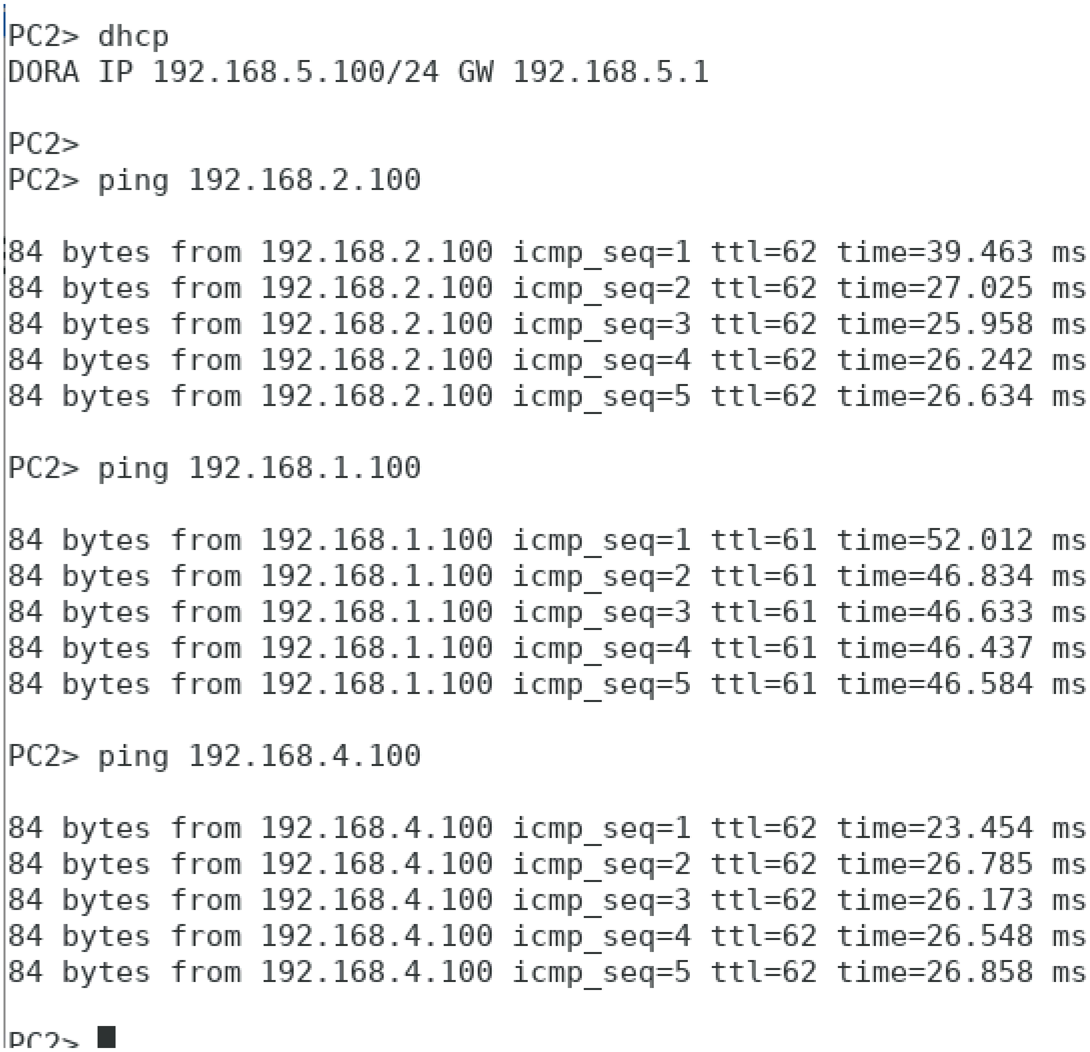
Pings

PC1 to PC2,PC3,PC4



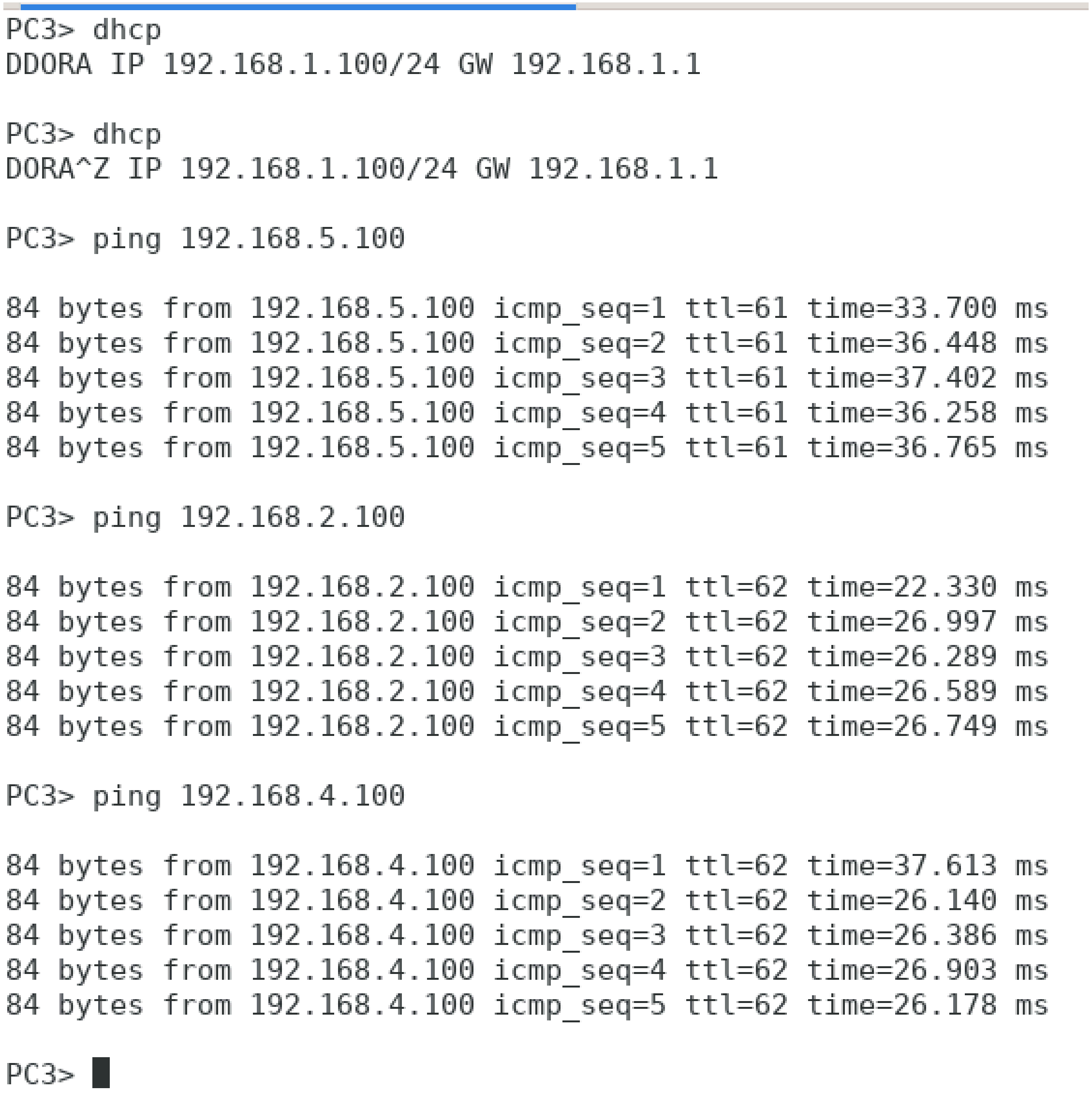
```
PC1> dhcp
DDORA IP 192.168.2.100/24 GW 192.168.2.1

PC1> ping 192.168.5.100

84 bytes from 192.168.5.100 icmp_seq=1 ttl=62 time=39.272 ms
84 bytes from 192.168.5.100 icmp_seq=2 ttl=62 time=26.406 ms
84 bytes from 192.168.5.100 icmp_seq=3 ttl=62 time=26.520 ms
84 bytes from 192.168.5.100 icmp_seq=4 ttl=62 time=27.551 ms
84 bytes from 192.168.5.100 icmp_seq=5 ttl=62 time=27.704 ms

PC1> ping 192.168.1.100

84 bytes from 192.168.1.100 icmp_seq=1 ttl=62 time=36.099 ms
84 bytes from 192.168.1.100 icmp_seq=2 ttl=62 time=26.808 ms
84 bytes from 192.168.1.100 icmp_seq=3 ttl=62 time=25.880 ms
84 bytes from 192.168.1.100 icmp_seq=4 ttl=62 time=26.938 ms
84 bytes from 192.168.1.100 icmp_seq=5 ttl=62 time=26.220 ms

PC1> ping 192.168.4.100

84 bytes from 192.168.4.100 icmp_seq=1 ttl=61 time=55.356 ms
84 bytes from 192.168.4.100 icmp_seq=2 ttl=61 time=46.797 ms
84 bytes from 192.168.4.100 icmp_seq=3 ttl=61 time=36.896 ms
84 bytes from 192.168.4.100 icmp_seq=4 ttl=61 time=46.937 ms
84 bytes from 192.168.4.100 icmp_seq=5 ttl=61 time=36.689 ms

PC1>
```

PC2



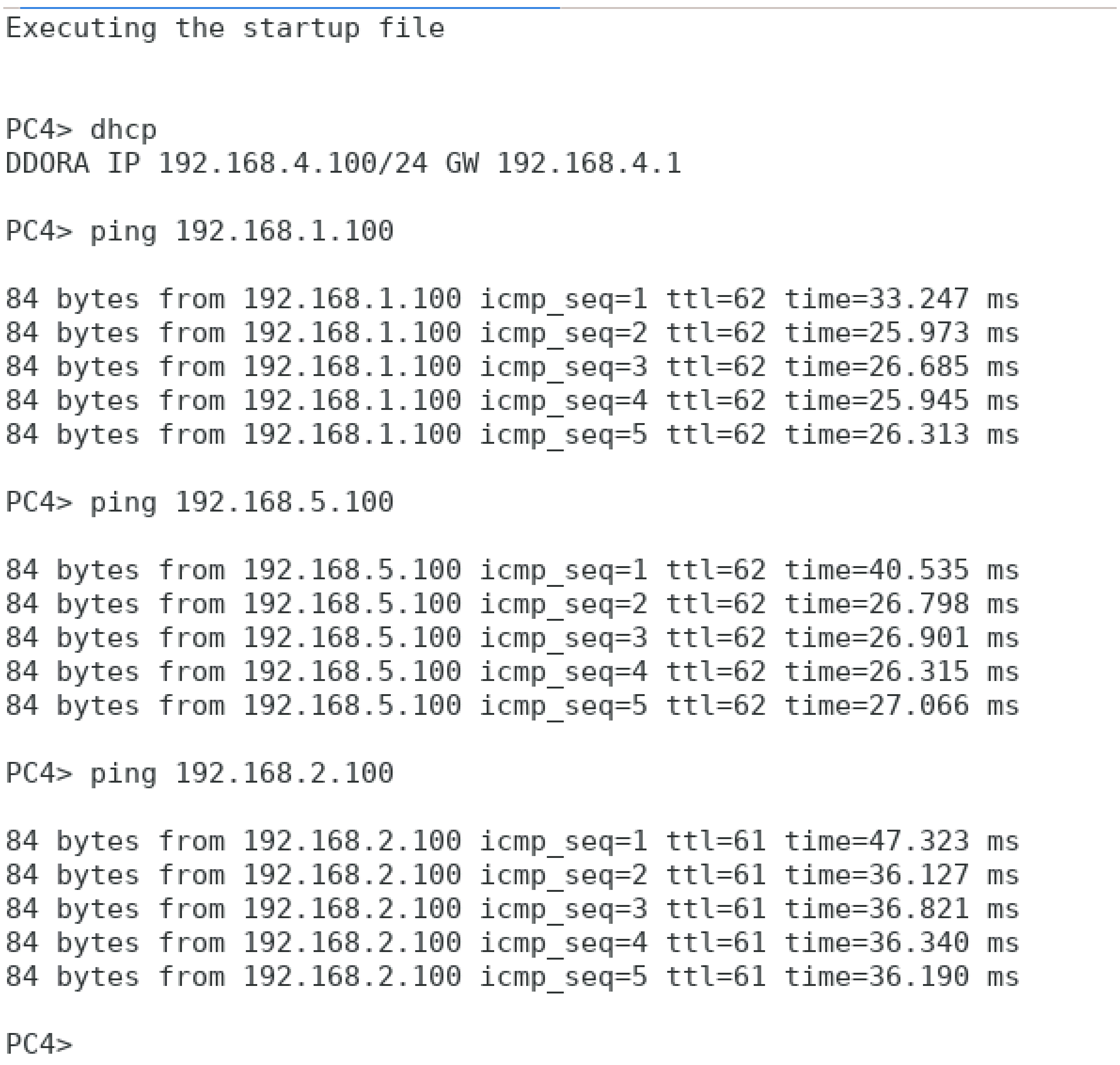
```
PC2> dhcp
DORA IP 192.168.5.100/24 GW 192.168.5.1

PC2>
PC2> ping 192.168.2.100

84 bytes from 192.168.2.100 icmp_seq=1 ttl=62 time=39.463 ms
84 bytes from 192.168.2.100 icmp_seq=2 ttl=62 time=27.025 ms
84 bytes from 192.168.2.100 icmp_seq=3 ttl=62 time=25.958 ms
84 bytes from 192.168.2.100 icmp_seq=4 ttl=62 time=26.242 ms
84 bytes from 192.168.2.100 icmp_seq=5 ttl=62 time=26.634 ms

PC2> ping 192.168.1.100

84 bytes from 192.168.1.100 icmp_seq=1 ttl=61 time=52.012 ms
84 bytes from 192.168.1.100 icmp_seq=2 ttl=61 time=46.834 ms
84 bytes from 192.168.1.100 icmp_seq=3 ttl=61 time=46.633 ms
84 bytes from 192.168.1.100 icmp_seq=4 ttl=61 time=46.437 ms
84 bytes from 192.168.1.100 icmp_seq=5 ttl=61 time=46.584 ms

PC2> ping 192.168.4.100

84 bytes from 192.168.4.100 icmp_seq=1 ttl=62 time=23.454 ms
84 bytes from 192.168.4.100 icmp_seq=2 ttl=62 time=26.785 ms
84 bytes from 192.168.4.100 icmp_seq=3 ttl=62 time=26.173 ms
84 bytes from 192.168.4.100 icmp_seq=4 ttl=62 time=26.548 ms
84 bytes from 192.168.4.100 icmp_seq=5 ttl=62 time=26.858 ms

PC2> █
```

PC3



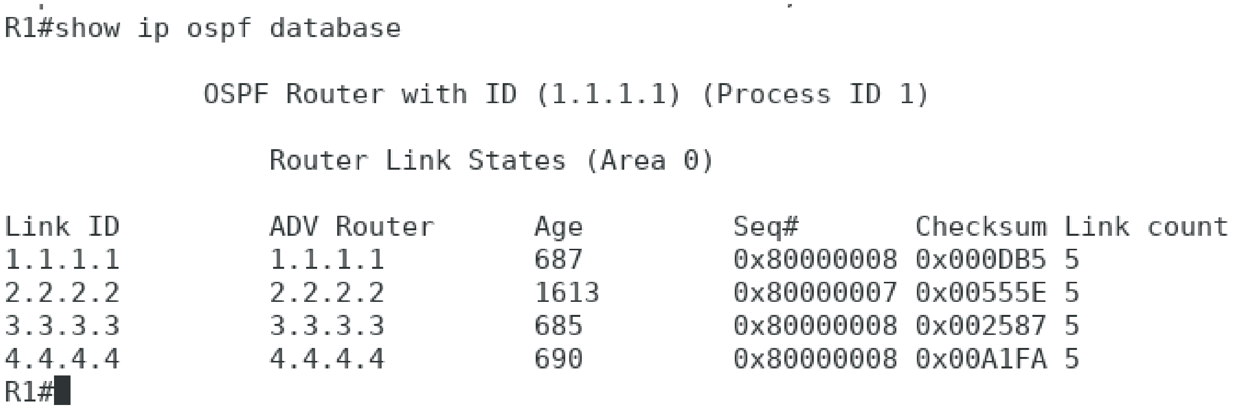
```
PC3> dhcp
DDORA IP 192.168.1.100/24 GW 192.168.1.1

PC3> dhcp
DORA^Z IP 192.168.1.100/24 GW 192.168.1.1

PC3> ping 192.168.5.100

84 bytes from 192.168.5.100 icmp_seq=1 ttl=61 time=33.700 ms
84 bytes from 192.168.5.100 icmp_seq=2 ttl=61 time=36.448 ms
84 bytes from 192.168.5.100 icmp_seq=3 ttl=61 time=37.402 ms
84 bytes from 192.168.5.100 icmp_seq=4 ttl=61 time=36.258 ms
84 bytes from 192.168.5.100 icmp_seq=5 ttl=61 time=36.765 ms

PC3> ping 192.168.2.100

84 bytes from 192.168.2.100 icmp_seq=1 ttl=62 time=22.330 ms
84 bytes from 192.168.2.100 icmp_seq=2 ttl=62 time=26.997 ms
84 bytes from 192.168.2.100 icmp_seq=3 ttl=62 time=26.289 ms
84 bytes from 192.168.2.100 icmp_seq=4 ttl=62 time=26.589 ms
84 bytes from 192.168.2.100 icmp_seq=5 ttl=62 time=26.749 ms

PC3> ping 192.168.4.100

84 bytes from 192.168.4.100 icmp_seq=1 ttl=62 time=37.613 ms
84 bytes from 192.168.4.100 icmp_seq=2 ttl=62 time=26.140 ms
84 bytes from 192.168.4.100 icmp_seq=3 ttl=62 time=26.386 ms
84 bytes from 192.168.4.100 icmp_seq=4 ttl=62 time=26.903 ms
84 bytes from 192.168.4.100 icmp_seq=5 ttl=62 time=26.178 ms

PC3> █
```

PC4



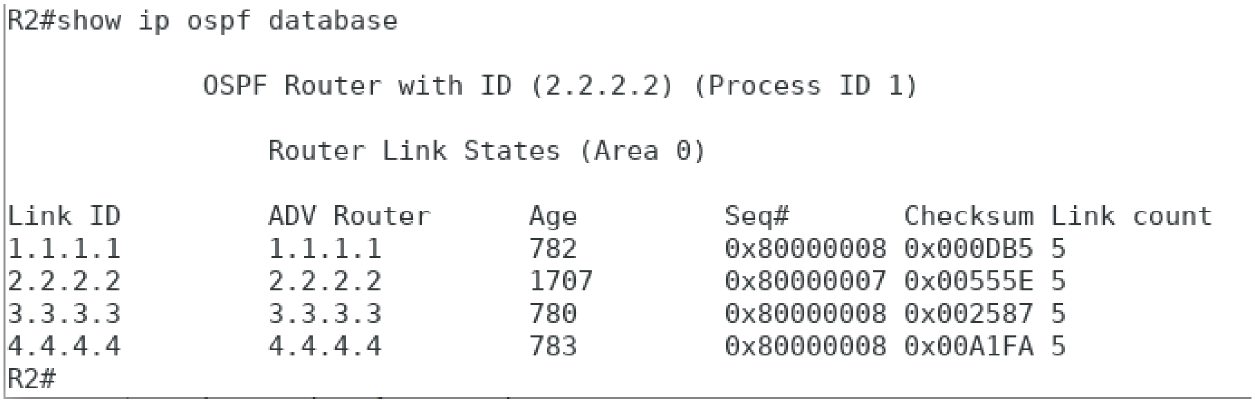
```
Executing the startup file


PC4> dhcp
DDORA IP 192.168.4.100/24 GW 192.168.4.1

PC4> ping 192.168.1.100

84 bytes from 192.168.1.100 icmp_seq=1 ttl=62 time=33.247 ms
84 bytes from 192.168.1.100 icmp_seq=2 ttl=62 time=25.973 ms
84 bytes from 192.168.1.100 icmp_seq=3 ttl=62 time=26.685 ms
84 bytes from 192.168.1.100 icmp_seq=4 ttl=62 time=25.945 ms
84 bytes from 192.168.1.100 icmp_seq=5 ttl=62 time=26.313 ms

PC4> ping 192.168.5.100

84 bytes from 192.168.5.100 icmp_seq=1 ttl=62 time=40.535 ms
84 bytes from 192.168.5.100 icmp_seq=2 ttl=62 time=26.798 ms
84 bytes from 192.168.5.100 icmp_seq=3 ttl=62 time=26.901 ms
84 bytes from 192.168.5.100 icmp_seq=4 ttl=62 time=26.315 ms
84 bytes from 192.168.5.100 icmp_seq=5 ttl=62 time=27.066 ms

PC4> ping 192.168.2.100

84 bytes from 192.168.2.100 icmp_seq=1 ttl=61 time=47.323 ms
84 bytes from 192.168.2.100 icmp_seq=2 ttl=61 time=36.127 ms
84 bytes from 192.168.2.100 icmp_seq=3 ttl=61 time=36.821 ms
84 bytes from 192.168.2.100 icmp_seq=4 ttl=61 time=36.340 ms
84 bytes from 192.168.2.100 icmp_seq=5 ttl=61 time=36.190 ms

PC4>
```

Router1



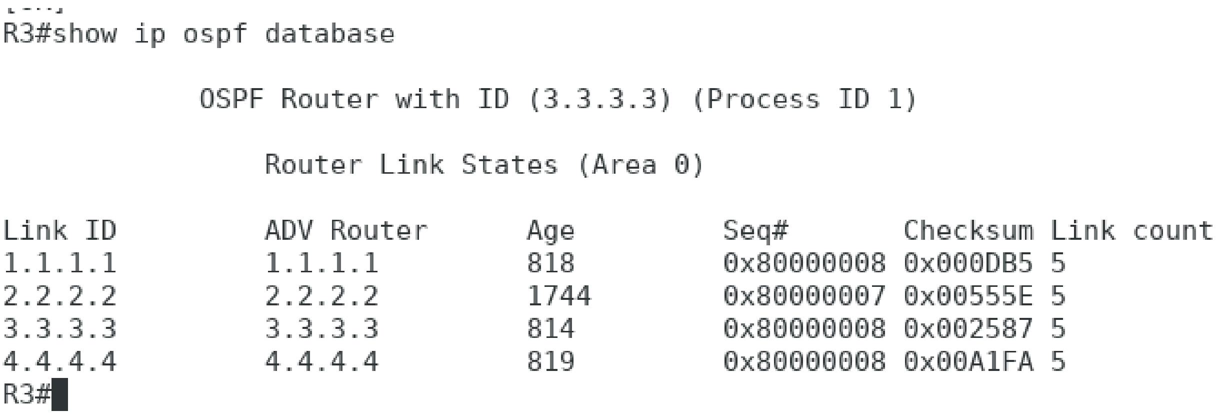
```
R1#show ip ospf database

            OSPF Router with ID (1.1.1.1) (Process ID 1)

                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         687         0x80000008 0x000DB5 5
2.2.2.2         2.2.2.2         1613        0x80000007 0x00555E 5
3.3.3.3         3.3.3.3         685         0x80000008 0x002587 5
4.4.4.4         4.4.4.4         690         0x80000008 0x00A1FA 5
R1#
```

Router2



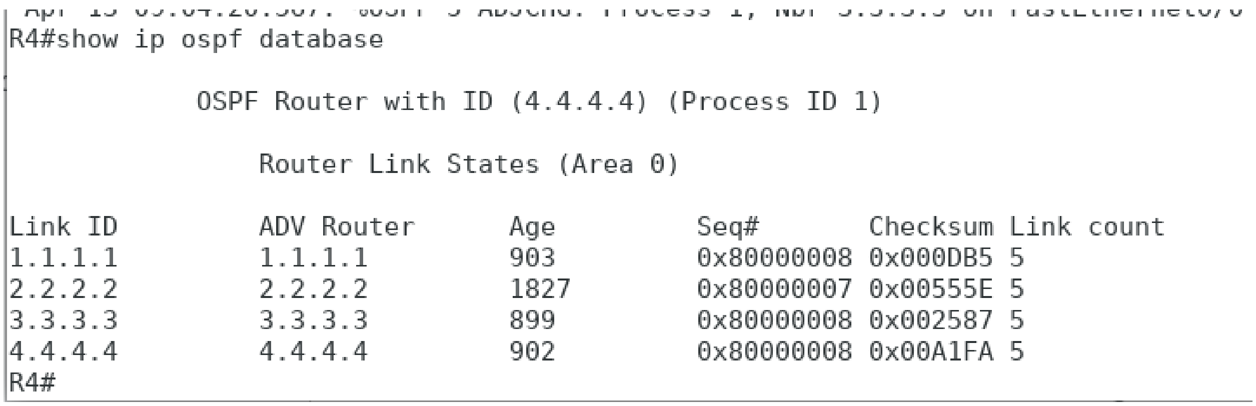
```
R2#show ip ospf database

              OSPF Router with ID (2.2.2.2) (Process ID 1)

                  Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         782         0x80000008 0x000DB5 5
2.2.2.2         2.2.2.2         1707        0x80000007 0x00555E 5
3.3.3.3         3.3.3.3         780         0x80000008 0x002587 5
4.4.4.4         4.4.4.4         783         0x80000008 0x00A1FA 5
R2#
```

Router3



```
R3#show ip ospf database

              OSPF Router with ID (3.3.3.3) (Process ID 1)

                  Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         818         0x80000008 0x000DB5 5
2.2.2.2         2.2.2.2         1744        0x80000007 0x00555E 5
3.3.3.3         3.3.3.3         814         0x80000008 0x002587 5
4.4.4.4         4.4.4.4         819         0x80000008 0x00A1FA 5
R3#
```

Router4



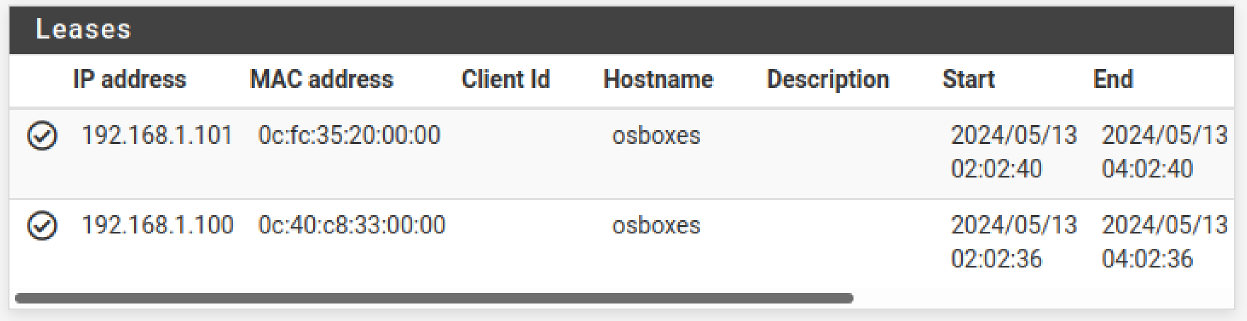
```
 Apr 15 09:04:20.507: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on FastEthernet0/0
R4#show ip ospf database

              OSPF Router with ID (4.4.4.4) (Process ID 1)

                  Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         903         0x80000008 0x000DB5 5
2.2.2.2         2.2.2.2         1827        0x80000007 0x00555E 5
3.3.3.3         3.3.3.3         899         0x80000008 0x002587 5
4.4.4.4         4.4.4.4         902         0x80000008 0x00A1FA 5
R4#
```

Config Files (Q4)

Firewalling

Followed the pfSense guide from start to finish, set up the topology and all configurations:

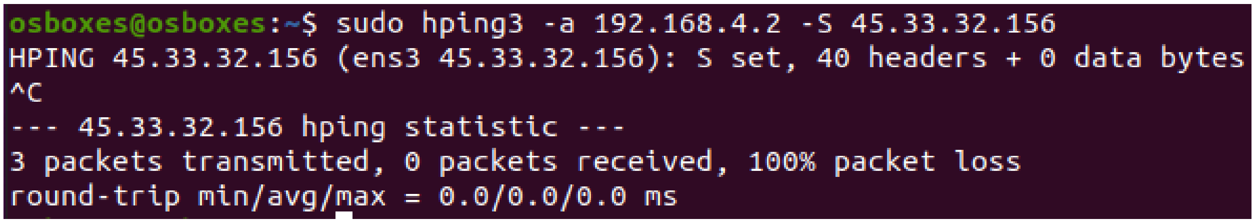
1. IP Address Assignment
   The pfSense DHCP server assigned the following IP addresses within the internal network:
   a. UbuntuDesktopGuest20.04.4-1: 192.168.1.100
   b. UbuntuDesktopGuest20.04.4-2: 192.168.1.101



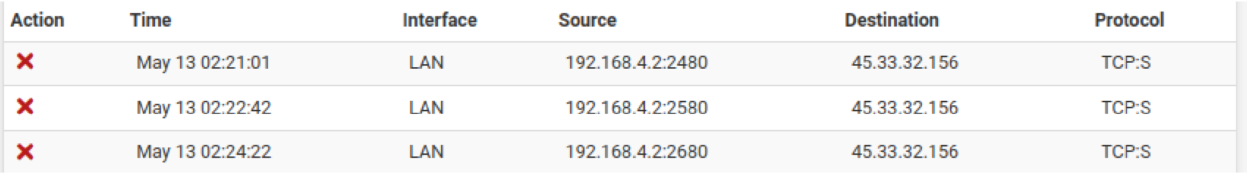
Leases

	IP address	MAC address	Client Id	Hostname	Description	Start	End
✓	192.168.1.101	0c:fc:35:20:00:00		osboxes		2024/05/13 02:02:40	2024/05/13 04:02:40
✓	192.168.1.100	0c:40:c8:33:00:00		osboxes		2024/05/13 02:02:36	2024/05/13 04:02:36

2. Anti-Spoofing Test Using hping3
   Command run on UbuntuDesktopGuest20.04.4-1:
   sudo hping3 -a 192.168.4.2 -S 45.33.32.156

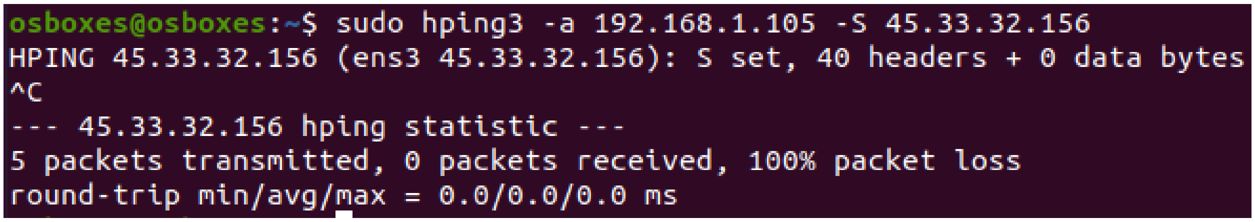


```
osboxes@osboxes:~$ sudo hping3 -a 192.168.4.2 -S 45.33.32.156
HPING 45.33.32.156 (ens3 45.33.32.156): S set, 40 headers + 0 data bytes
^C
--- 45.33.32.156 hping statistic ---
3 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

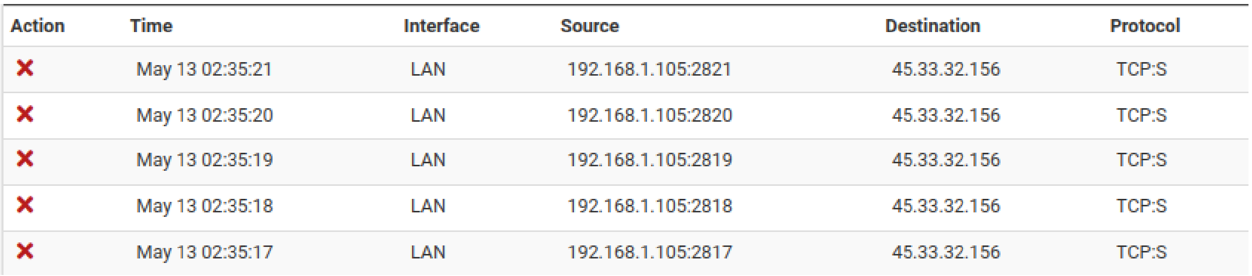


Action	Time	Interface	Source	Destination	Protocol
✗	May 13 02:21:01	LAN	192.168.4.2:2480	45.33.32.156	TCP:S
✗	May 13 02:22:42	LAN	192.168.4.2:2580	45.33.32.156	TCP:S
✗	May 13 02:24:22	LAN	192.168.4.2:2680	45.33.32.156	TCP:S

3. Spoofing Test from Internal Network
   Command run on UbuntuDesktopGuest20.04.4-1:
   sudo hping3 -a 192.168.1.105 -S 45.33.32.156

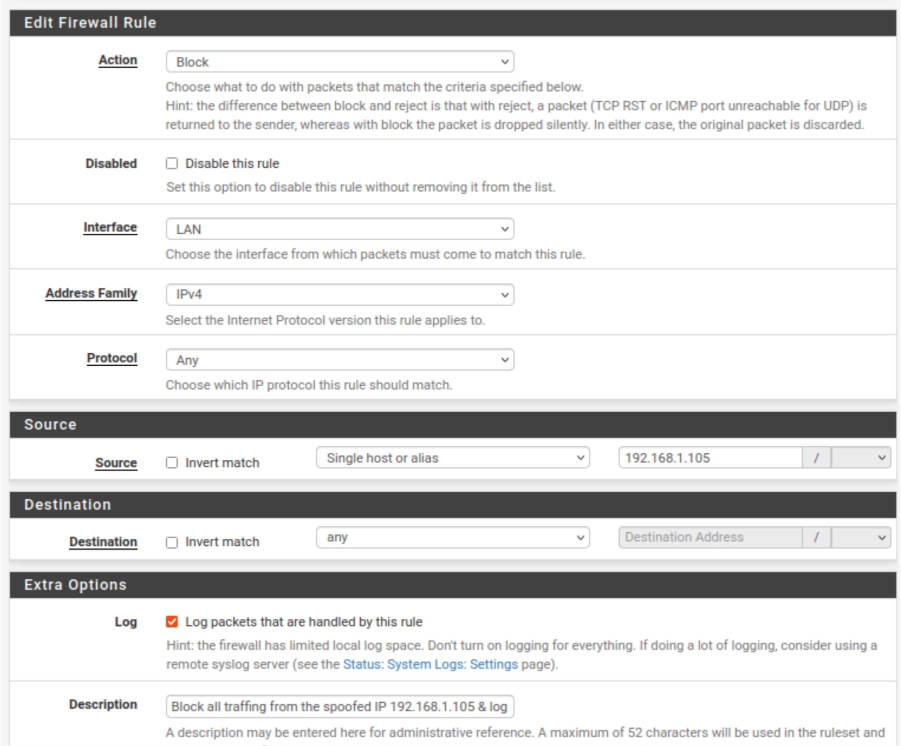


```
osboxes@osboxes:~$ sudo hping3 -a 192.168.1.105 -S 45.33.32.156
HPING 45.33.32.156 (ens3 45.33.32.156): S set, 40 headers + 0 data bytes
^C
--- 45.33.32.156 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```



Action	Time	Interface	Source	Destination	Protocol
✕	May 13 02:35:21	LAN	192.168.1.105:2821	45.33.32.156	TCP:S
✕	May 13 02:35:20	LAN	192.168.1.105:2820	45.33.32.156	TCP:S
✕	May 13 02:35:19	LAN	192.168.1.105:2819	45.33.32.156	TCP:S
✕	May 13 02:35:18	LAN	192.168.1.105:2818	45.33.32.156	TCP:S
✕	May 13 02:35:17	LAN	192.168.1.105:2817	45.33.32.156	TCP:S

4. Configuring a blocking rule
   Create a firewall rule to block all traffic originating from the IP address 192.168.1.105 within the LAN and log the blocked packets



Edit Firewall Rule

Action: Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: □ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: LAN
Choose the interface from which packets must come to match this rule.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: Any
Choose which IP protocol this rule should match.

Source

Source: □ Invert match | Single host or alias | 192.168.1.105 /

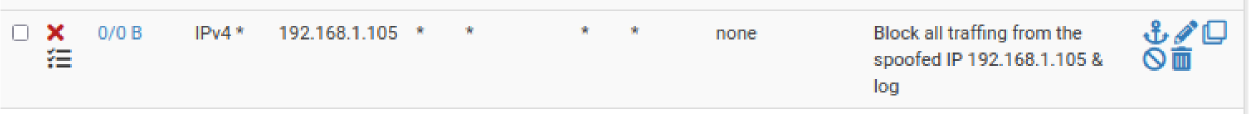
Destination

Destination: □ Invert match | any | Destination Address /

Extra Options

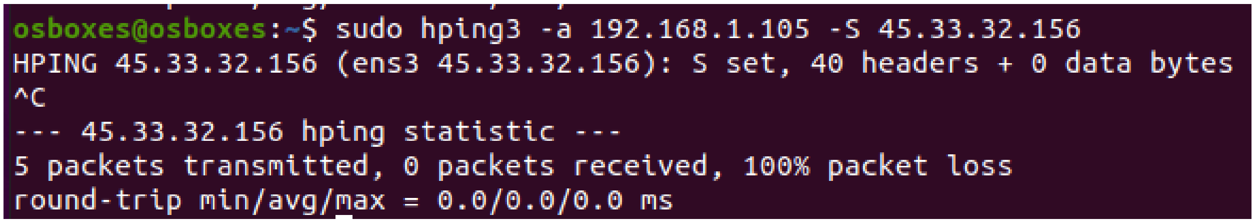
Log: ☑ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description: Block all traffing from the spoofed IP 192.168.1.105 & log
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and

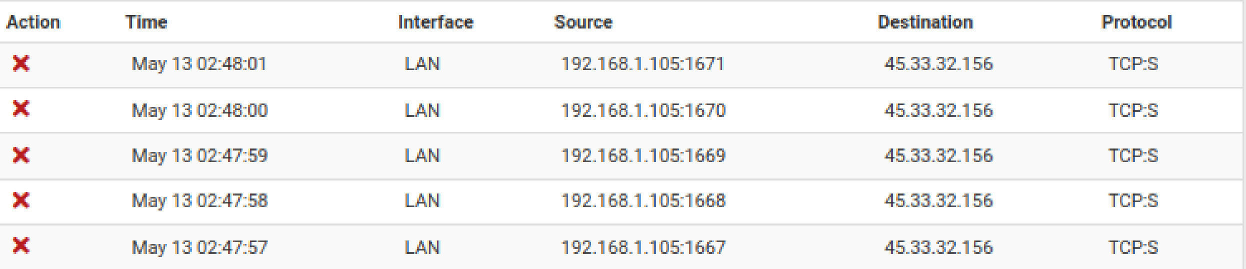


□	✕ ☰	0/0 B	IPv4 *	192.168.1.105	*	*	*	*	none	Block all traffing from the spoofed IP 192.168.1.105 & log	⚓ ✎ ❐ ⊘ 🗑

Repeating the experiment from the previous question

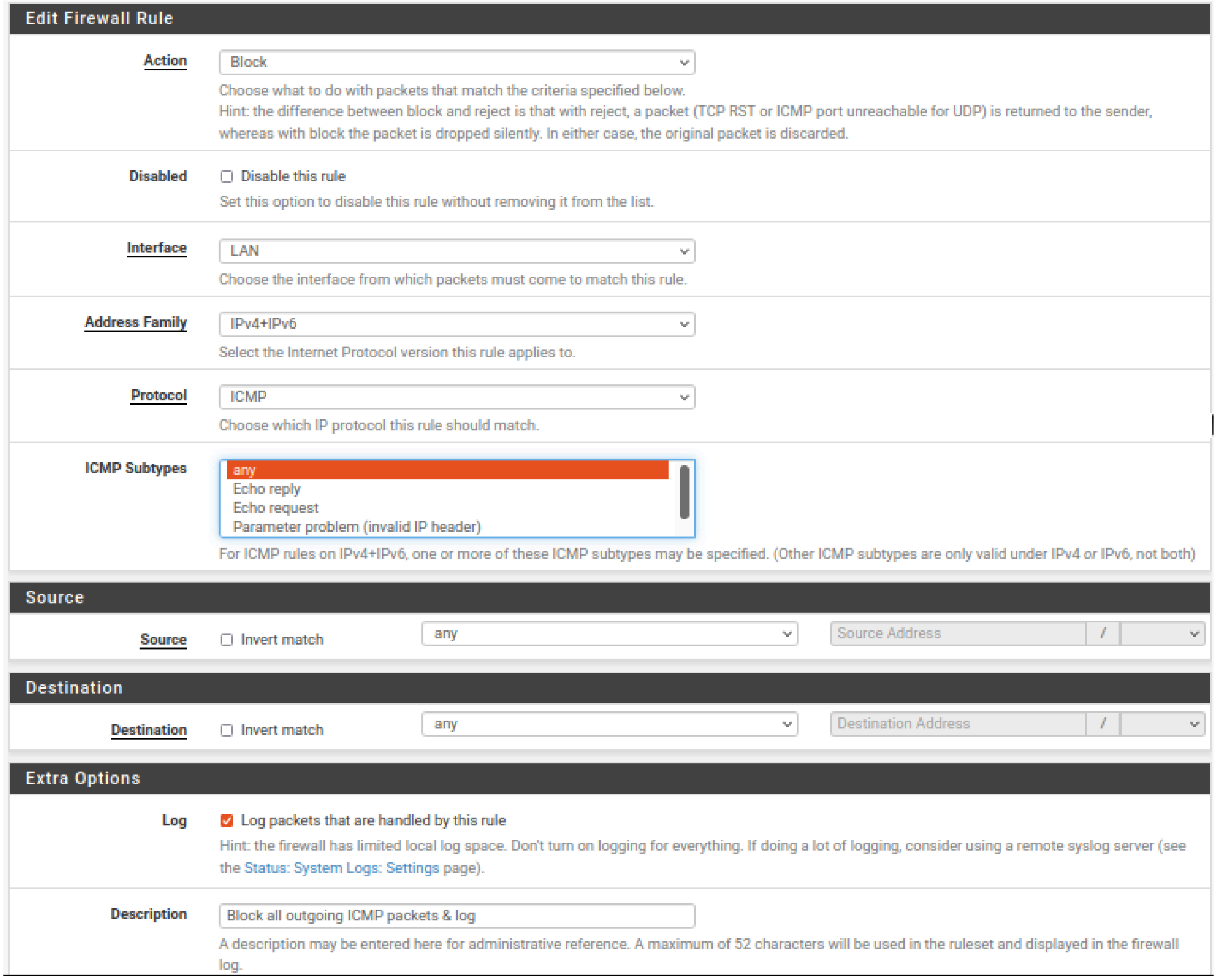


```
osboxes@osboxes:~$ sudo hping3 -a 192.168.1.105 -S 45.33.32.156
HPING 45.33.32.156 (ens3 45.33.32.156): S set, 40 headers + 0 data bytes
^C
--- 45.33.32.156 hping statistic ---
5 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```



Action	Time	Interface	Source	Destination	Protocol
✗	May 13 02:48:01	LAN	192.168.1.105:1671	45.33.32.156	TCP:S
✗	May 13 02:48:00	LAN	192.168.1.105:1670	45.33.32.156	TCP:S
✗	May 13 02:47:59	LAN	192.168.1.105:1669	45.33.32.156	TCP:S
✗	May 13 02:47:58	LAN	192.168.1.105:1668	45.33.32.156	TCP:S
✗	May 13 02:47:57	LAN	192.168.1.105:1667	45.33.32.156	TCP:S

5. Block All Outgoing ICMP Packets
Create a firewall rule to block all all outgoing ICMP packets within the LAN and log the



Edit Firewall Rule

Action: Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: LAN
Choose the interface from which packets must come to match this rule.

Address Family: IPv4+IPv6
Select the Internet Protocol version this rule applies to.

Protocol: ICMP
Choose which IP protocol this rule should match.

ICMP Subtypes: any (selected), Echo reply, Echo request, Parameter problem (invalid IP header)
For ICMP rules on IPv4+IPv6, one or more of these ICMP subtypes may be specified. (Other ICMP subtypes are only valid under IPv4 or IPv6, not both)

Source

Source: ☐ Invert match any Source Address /

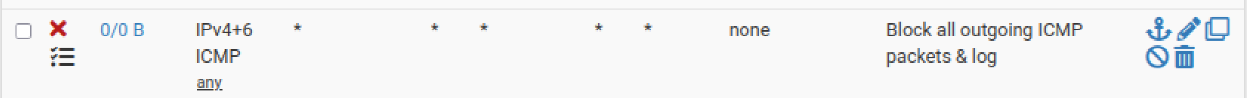
Destination

Destination: ☐ Invert match any Destination Address /

Extra Options

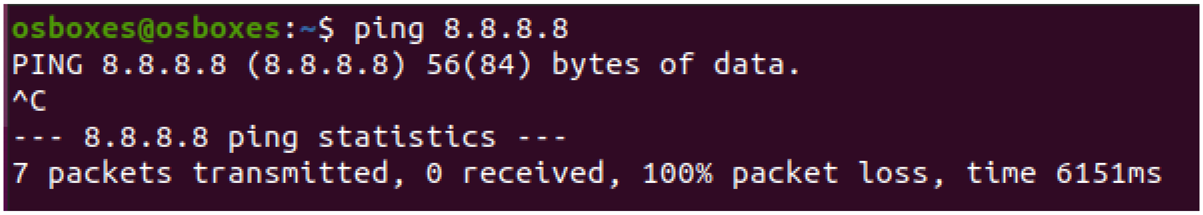
Log: ☑ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description: Block all outgoing ICMP packets & log
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

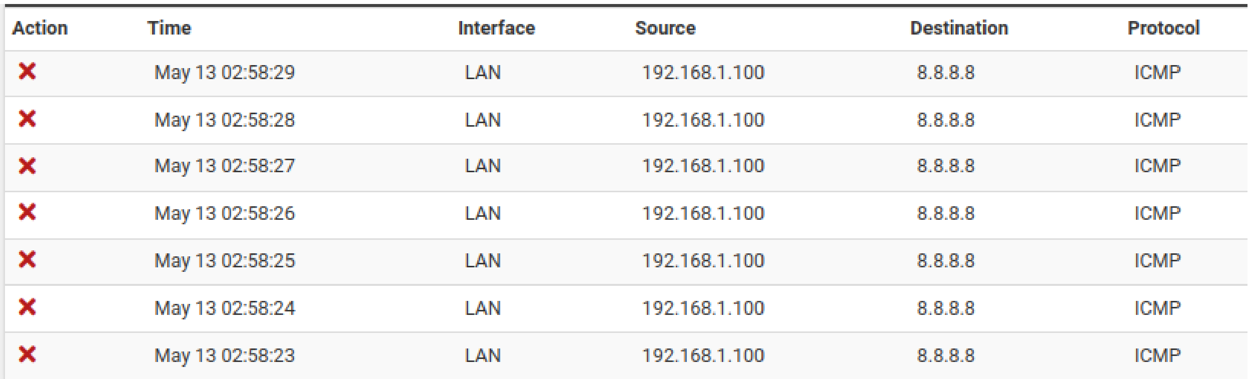


☐	✖	0/0 B	IPv4+6 ICMP any	*	*	*	*	*	none	Block all outgoing ICMP packets & log	

Tested functionality of the firewall rule blocking all outgoing ICMP packets by pinging 8.8.8.8 from UbuntuDesktopGuest20.04.4-1

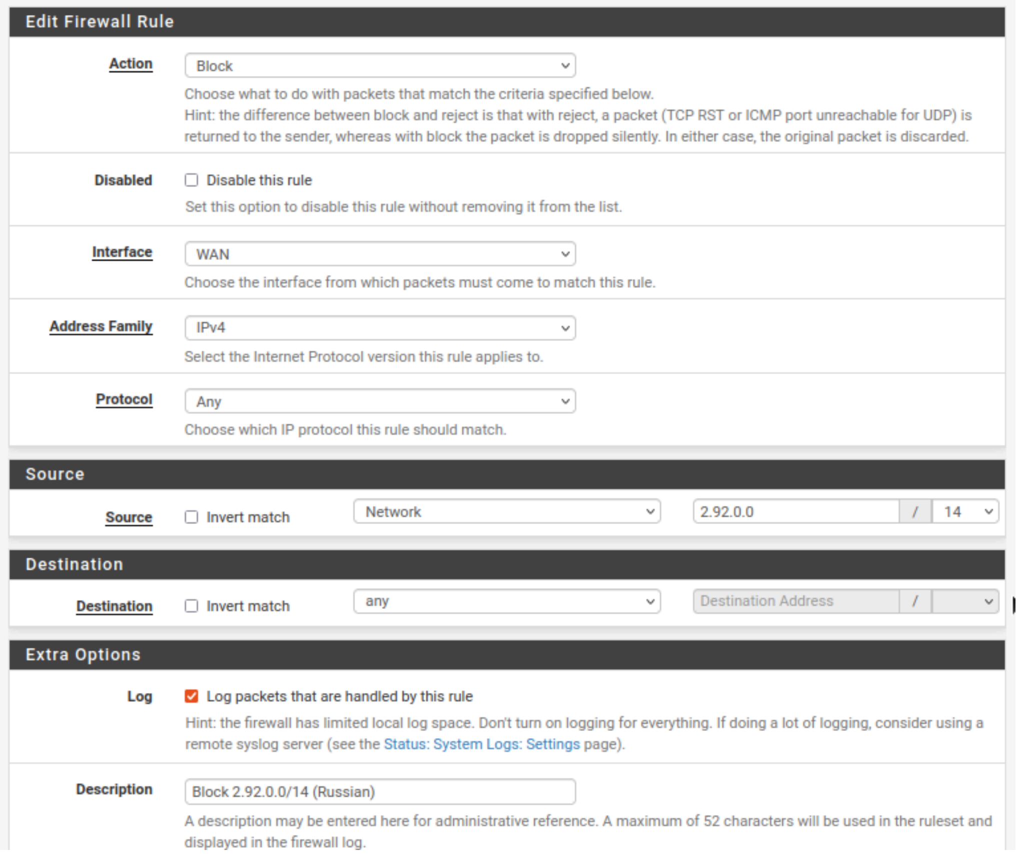


```
osboxes@osboxes:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 0 received, 100% packet loss, time 6151ms
```



Action	Time	Interface	Source	Destination	Protocol
✖	May 13 02:58:29	LAN	192.168.1.100	8.8.8.8	ICMP
✖	May 13 02:58:28	LAN	192.168.1.100	8.8.8.8	ICMP
✖	May 13 02:58:27	LAN	192.168.1.100	8.8.8.8	ICMP
✖	May 13 02:58:26	LAN	192.168.1.100	8.8.8.8	ICMP
✖	May 13 02:58:25	LAN	192.168.1.100	8.8.8.8	ICMP
✖	May 13 02:58:24	LAN	192.168.1.100	8.8.8.8	ICMP
✖	May 13 02:58:23	LAN	192.168.1.100	8.8.8.8	ICMP

6. Ban traffic from specific IP address blocks from Russia & China
Example rule (applied the same for all IP's just used different source IP



Edit Firewall Rule

Action: Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: WAN
Choose the interface from which packets must come to match this rule.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: Any
Choose which IP protocol this rule should match.

Source

Source: ☐ Invert match | Network | 2.92.0.0 / 14

Destination

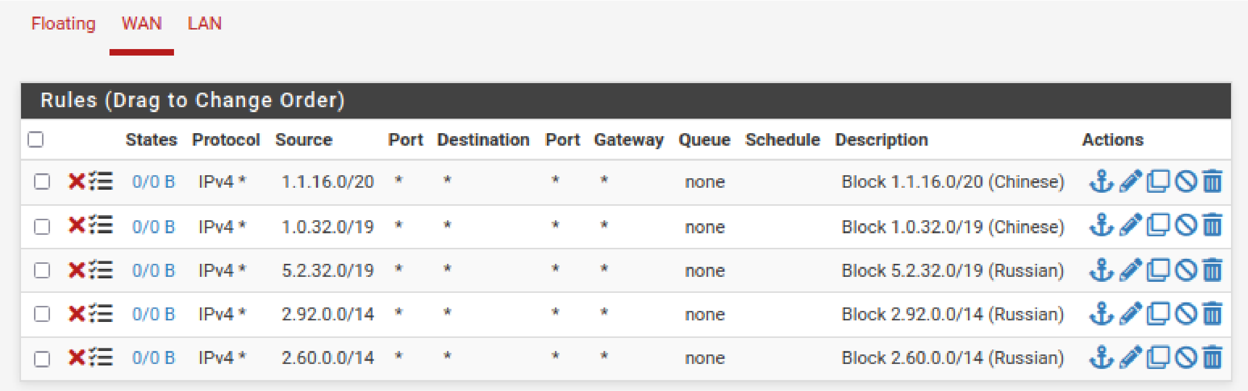
Destination: ☐ Invert match | any | Destination Address /

Extra Options

Log: ☑ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description: Block 2.92.0.0/14 (Russian)
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

All rules (3 Russian, 2 Chinese)



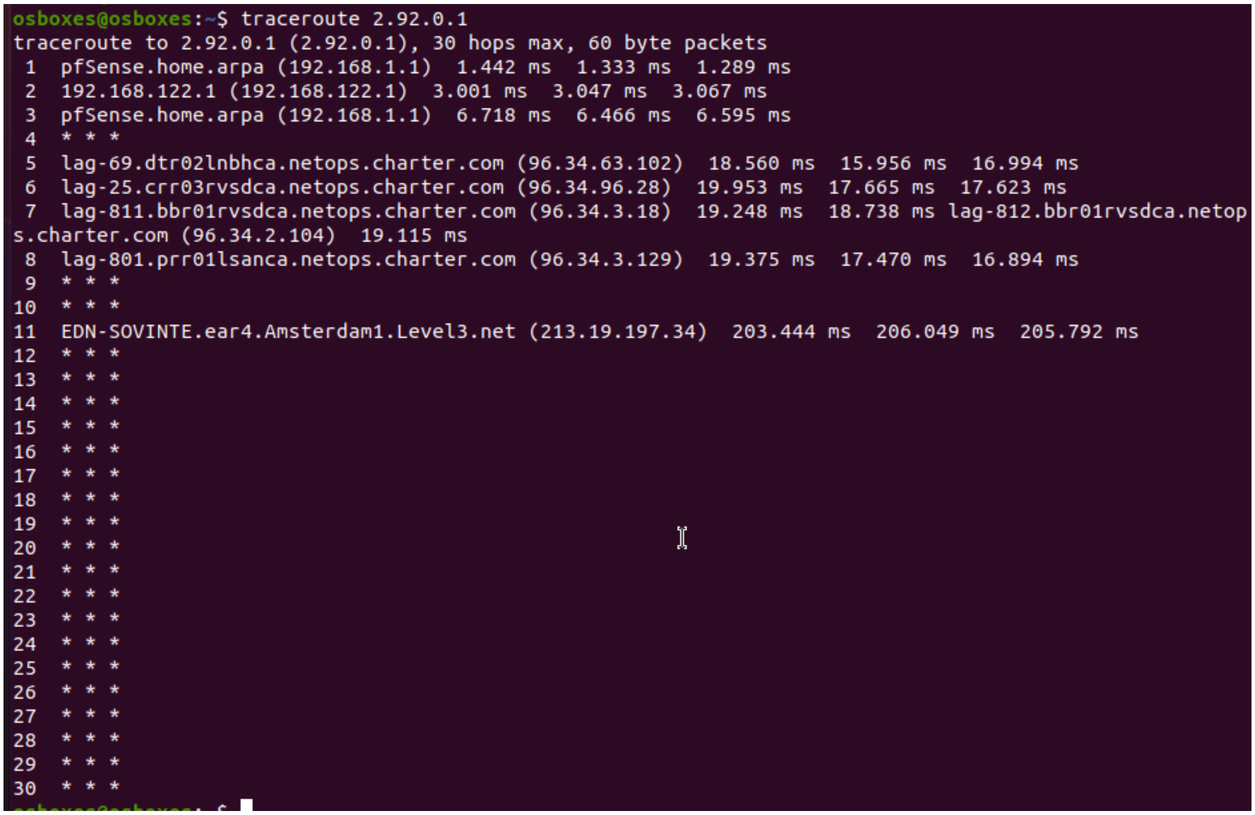
Rules (Drag to Change Order)

☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✕ ☰	0/0 B	IPv4 *	1.1.16.0/20	*	*	*	*	none		Block 1.1.16.0/20 (Chinese)	⚓ ✎ ❐ ⊘ 🗑
☐	✕ ☰	0/0 B	IPv4 *	1.0.32.0/19	*	*	*	*	none		Block 1.0.32.0/19 (Chinese)	⚓ ✎ ❐ ⊘ 🗑
☐	✕ ☰	0/0 B	IPv4 *	5.2.32.0/19	*	*	*	*	none		Block 5.2.32.0/19 (Russian)	⚓ ✎ ❐ ⊘ 🗑
☐	✕ ☰	0/0 B	IPv4 *	2.92.0.0/14	*	*	*	*	none		Block 2.92.0.0/14 (Russian)	⚓ ✎ ❐ ⊘ 🗑
☐	✕ ☰	0/0 B	IPv4 *	2.60.0.0/14	*	*	*	*	none		Block 2.60.0.0/14 (Russian)	⚓ ✎ ❐ ⊘ 🗑

Test:

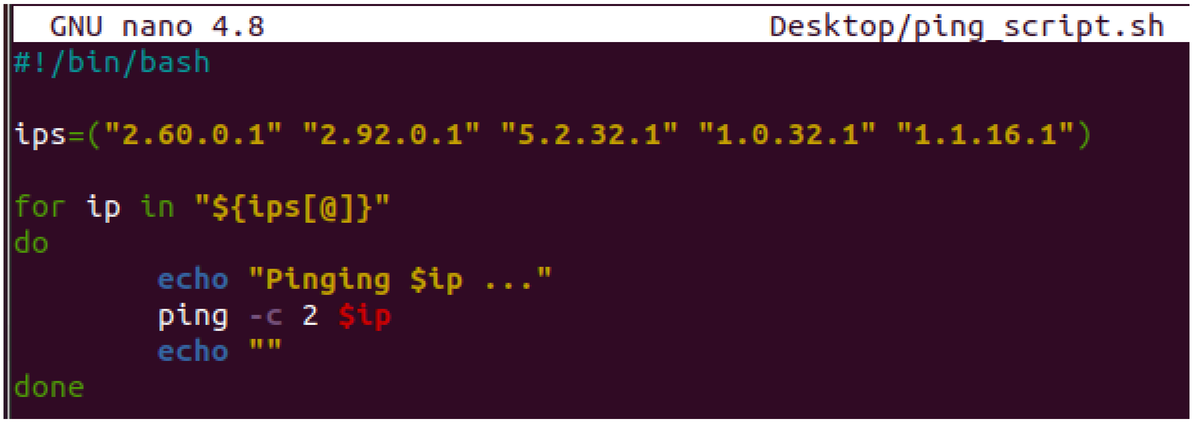
Used traceroute to see the path it takes and when it gets blocked (doesn't get a reply)

This is to a Russian IP



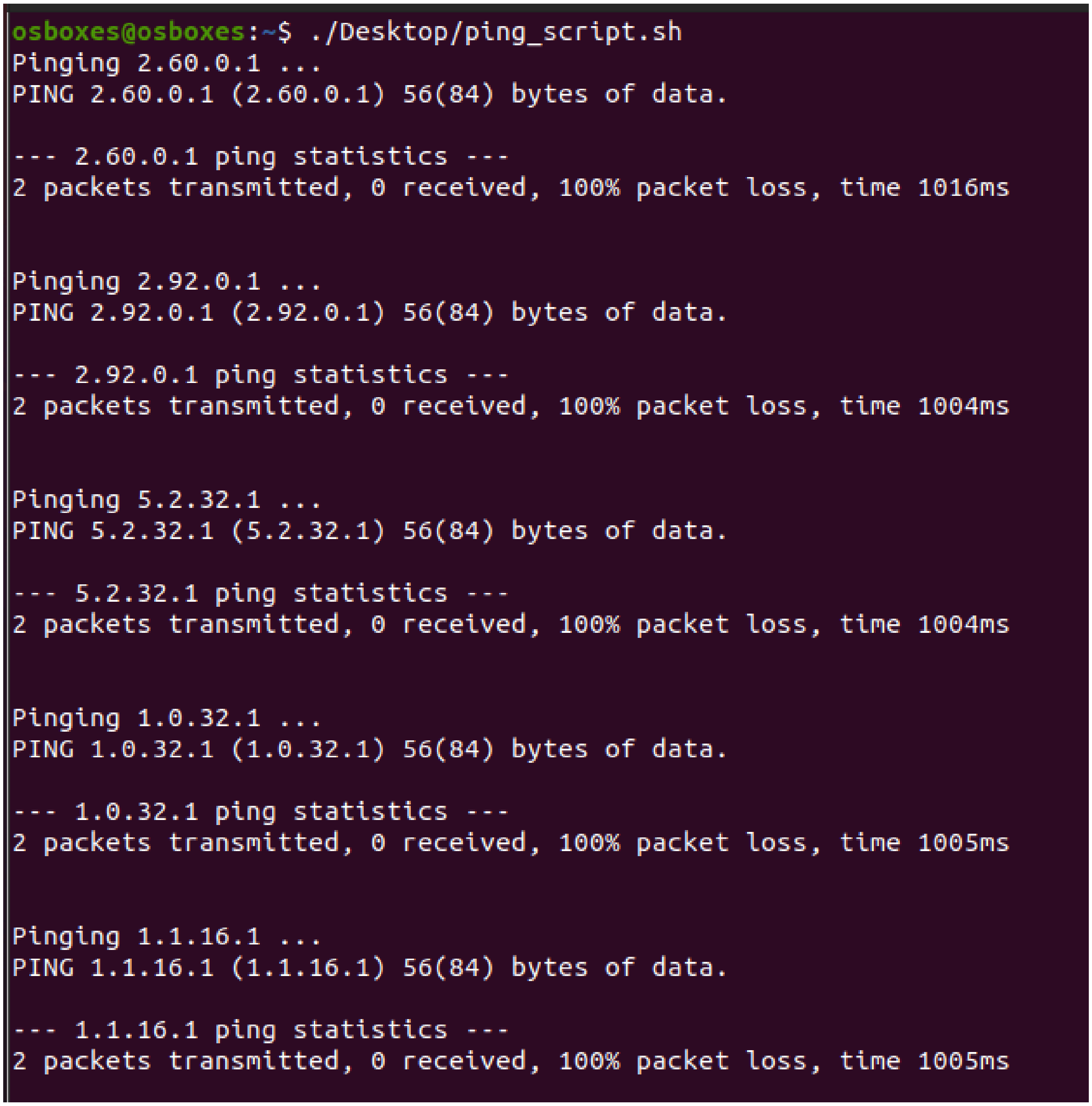
```
osboxes@osboxes:~$ traceroute 2.92.0.1
traceroute to 2.92.0.1 (2.92.0.1), 30 hops max, 60 byte packets
 1  pfSense.home.arpa (192.168.1.1)  1.442 ms  1.333 ms  1.289 ms
 2  192.168.122.1 (192.168.122.1)  3.001 ms  3.047 ms  3.067 ms
 3  pfSense.home.arpa (192.168.1.1)  6.718 ms  6.466 ms  6.595 ms
 4  * * *
 5  lag-69.dtr02lnbhca.netops.charter.com (96.34.63.102)  18.560 ms  15.956 ms  16.994 ms
 6  lag-25.crr03rvsdca.netops.charter.com (96.34.96.28)  19.953 ms  17.665 ms  17.623 ms
 7  lag-811.bbr01rvsdca.netops.charter.com (96.34.3.18)  19.248 ms  18.738 ms lag-812.bbr01rvsdca.netop
s.charter.com (96.34.2.104)  19.115 ms
 8  lag-801.prr01lsanca.netops.charter.com (96.34.3.129)  19.375 ms  17.470 ms  16.894 ms
 9  * * *
10  * * *
11  EDN-SOVINTE.ear4.Amsterdam1.Level3.net (213.19.197.34)  203.444 ms  206.049 ms  205.792 ms
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
osboxes@osboxes:~$
```

Using ping on all of them:



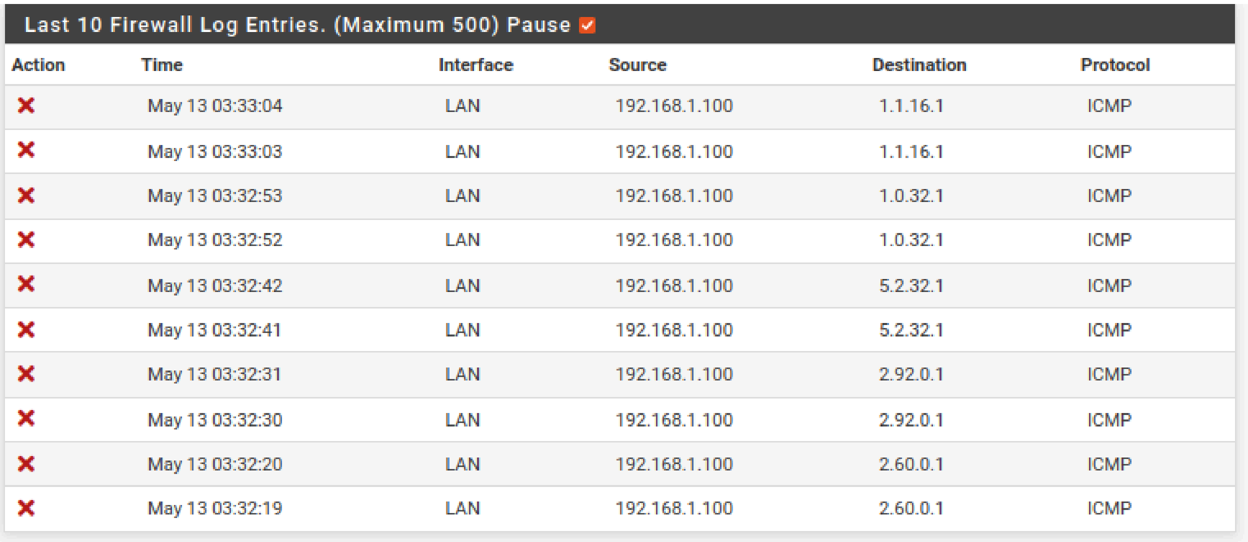
```
  GNU nano 4.8                                 Desktop/ping_script.sh
#!/bin/bash

ips=("2.60.0.1" "2.92.0.1" "5.2.32.1" "1.0.32.1" "1.1.16.1")

for ip in "${ips[@]}"
do
        echo "Pinging $ip ..."
        ping -c 2 $ip
        echo ""
done
```

Running the ping script:



```
osboxes@osboxes:~$ ./Desktop/ping_script.sh
Pinging 2.60.0.1 ...
PING 2.60.0.1 (2.60.0.1) 56(84) bytes of data.

--- 2.60.0.1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1016ms


Pinging 2.92.0.1 ...
PING 2.92.0.1 (2.92.0.1) 56(84) bytes of data.

--- 2.92.0.1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1004ms


Pinging 5.2.32.1 ...
PING 5.2.32.1 (5.2.32.1) 56(84) bytes of data.

--- 5.2.32.1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1004ms


Pinging 1.0.32.1 ...
PING 1.0.32.1 (1.0.32.1) 56(84) bytes of data.

--- 1.0.32.1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1005ms


Pinging 1.1.16.1 ...
PING 1.1.16.1 (1.1.16.1) 56(84) bytes of data.

--- 1.1.16.1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1005ms
```

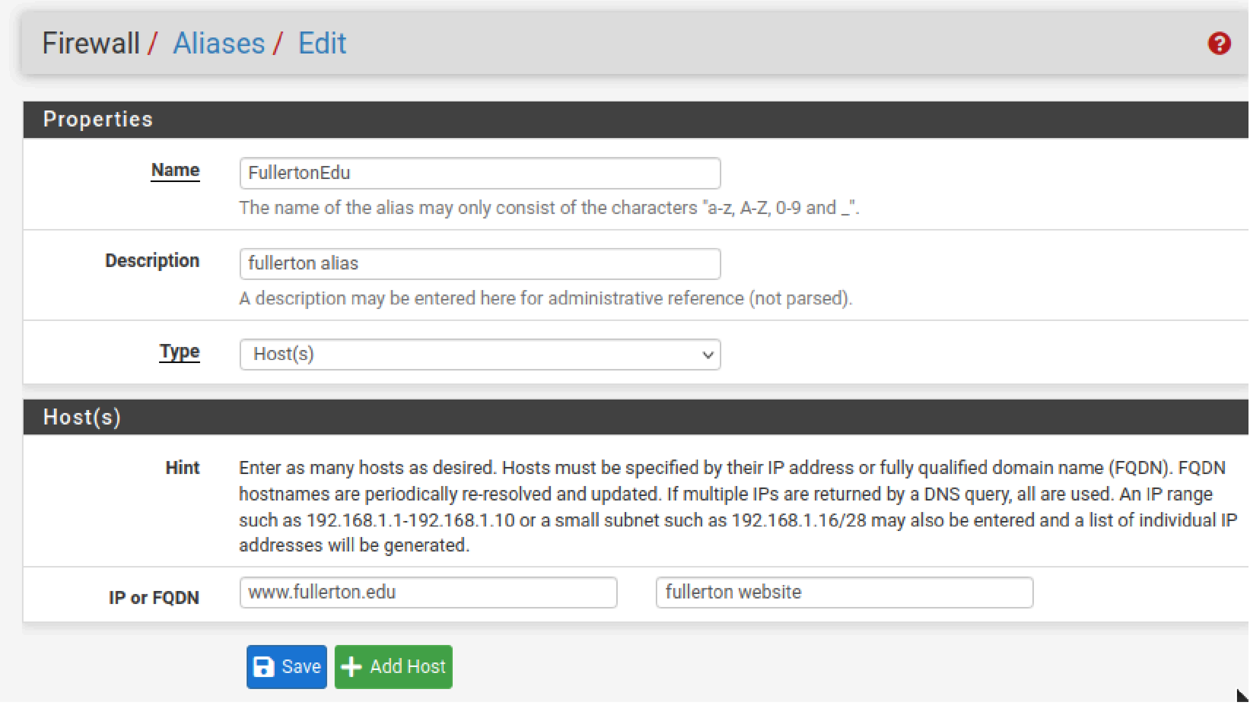
Logs:



Last 10 Firewall Log Entries. (Maximum 500) Pause ☑

Action	Time	Interface	Source	Destination	Protocol
✗	May 13 03:33:04	LAN	192.168.1.100	1.1.16.1	ICMP
✗	May 13 03:33:03	LAN	192.168.1.100	1.1.16.1	ICMP
✗	May 13 03:32:53	LAN	192.168.1.100	1.0.32.1	ICMP
✗	May 13 03:32:52	LAN	192.168.1.100	1.0.32.1	ICMP
✗	May 13 03:32:42	LAN	192.168.1.100	5.2.32.1	ICMP
✗	May 13 03:32:41	LAN	192.168.1.100	5.2.32.1	ICMP
✗	May 13 03:32:31	LAN	192.168.1.100	2.92.0.1	ICMP
✗	May 13 03:32:30	LAN	192.168.1.100	2.92.0.1	ICMP
✗	May 13 03:32:20	LAN	192.168.1.100	2.60.0.1	ICMP
✗	May 13 03:32:19	LAN	192.168.1.100	2.60.0.1	ICMP

7. Only allow HTTPS sessions with www.fullerton.edu & Block all other HTTPS traffic
Create an alias for www.fullerton.edu



Firewall / Aliases / Edit

Properties

Name: FullertonEdu
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description: fullerton alias
A description may be entered here for administrative reference (not parsed).

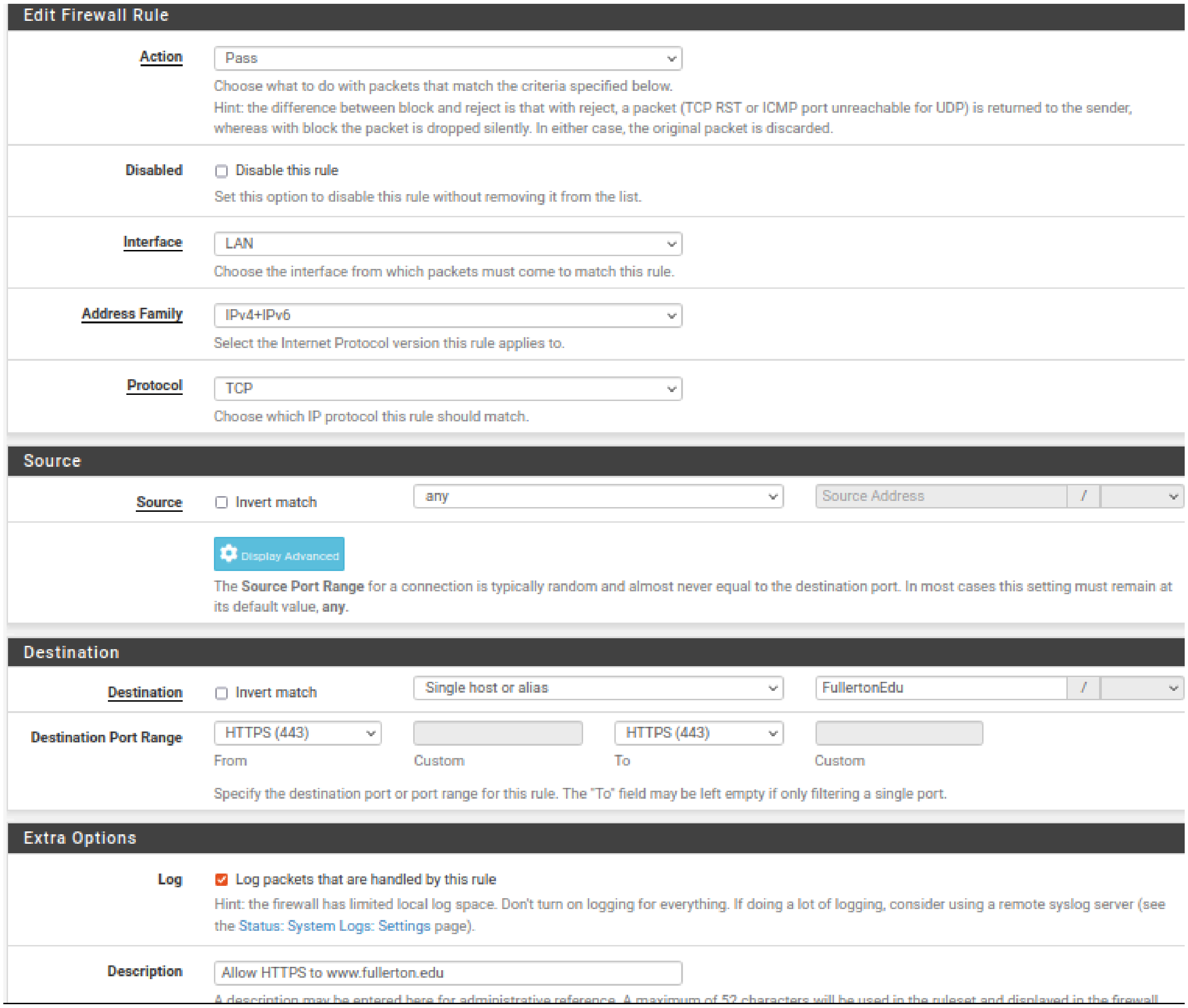
Type: Host(s)

Host(s)

Hint: Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN: www.fullerton.edu | fullerton website

Rule to only allow HTTPS sessions with www.fullerton.edu:



Edit Firewall Rule

Action Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface LAN

Choose the interface from which packets must come to match this rule.

Address Family IPv4+IPv6

Select the Internet Protocol version this rule applies to.

Protocol TCP

Choose which IP protocol this rule should match.

Source

Source ☐ Invert match any Source Address /

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match Single host or alias FullertonEdu /

Destination Port Range HTTPS (443) From Custom HTTPS (443) To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

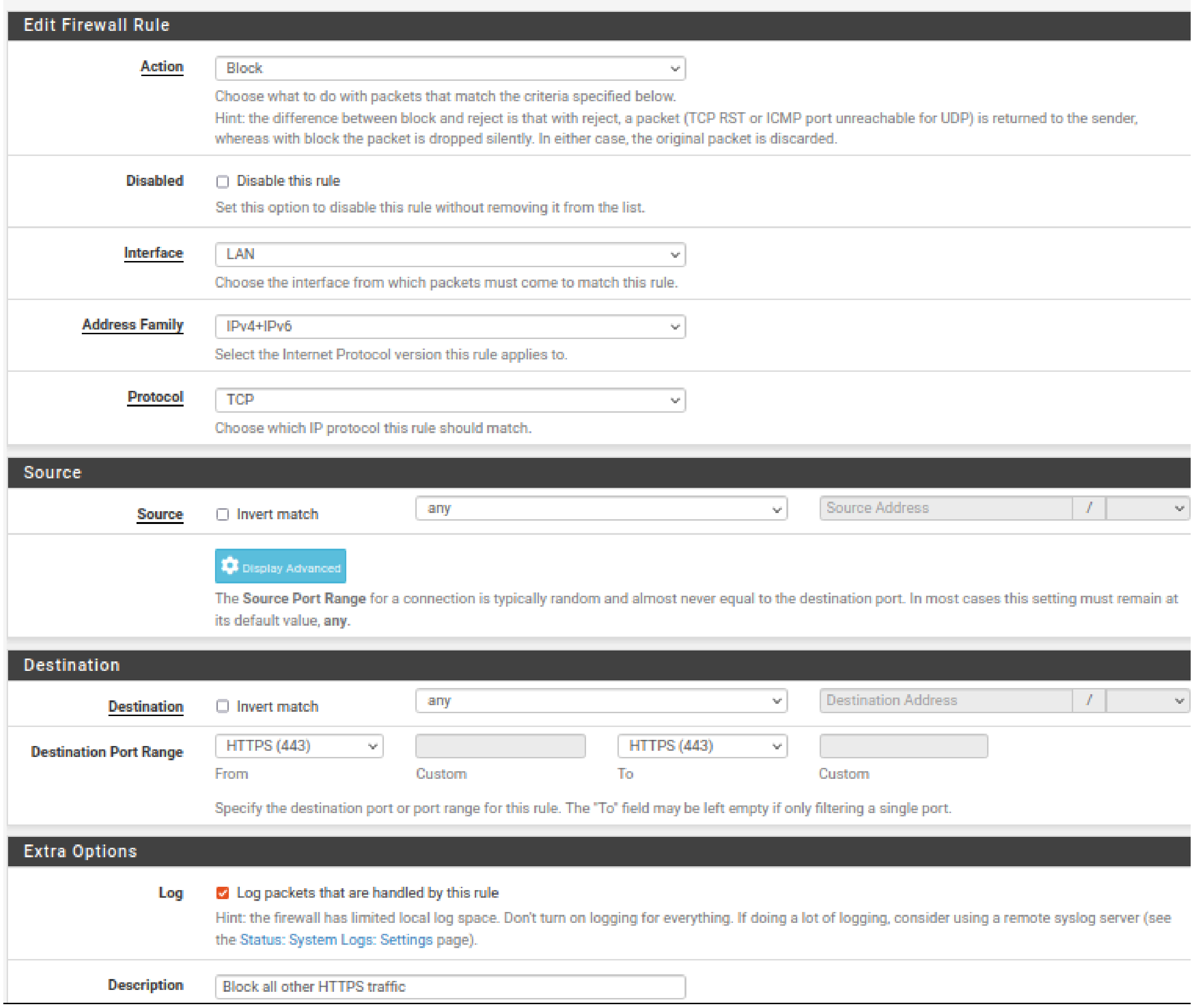
Log ☑ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description Allow HTTPS to www.fullerton.edu

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall

Rule to Block all other HTTPS sessions:



Edit Firewall Rule

Action Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled □ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface LAN
Choose the interface from which packets must come to match this rule.

Address Family IPv4+IPv6
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which IP protocol this rule should match.

Source

Source □ Invert match any Source Address /

Display Advanced
The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination □ Invert match any Destination Address /

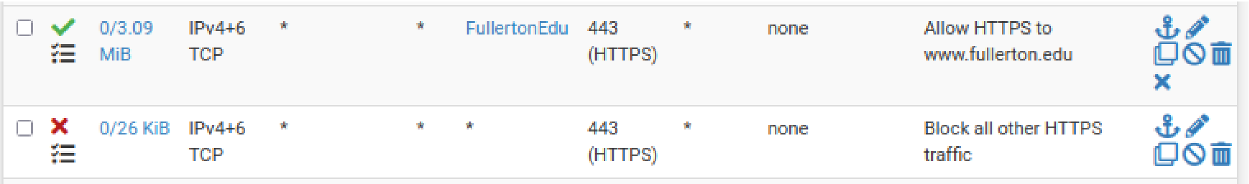
Destination Port Range HTTPS (443) From; Custom; HTTPS (443) To; Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☑ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description Block all other HTTPS traffic

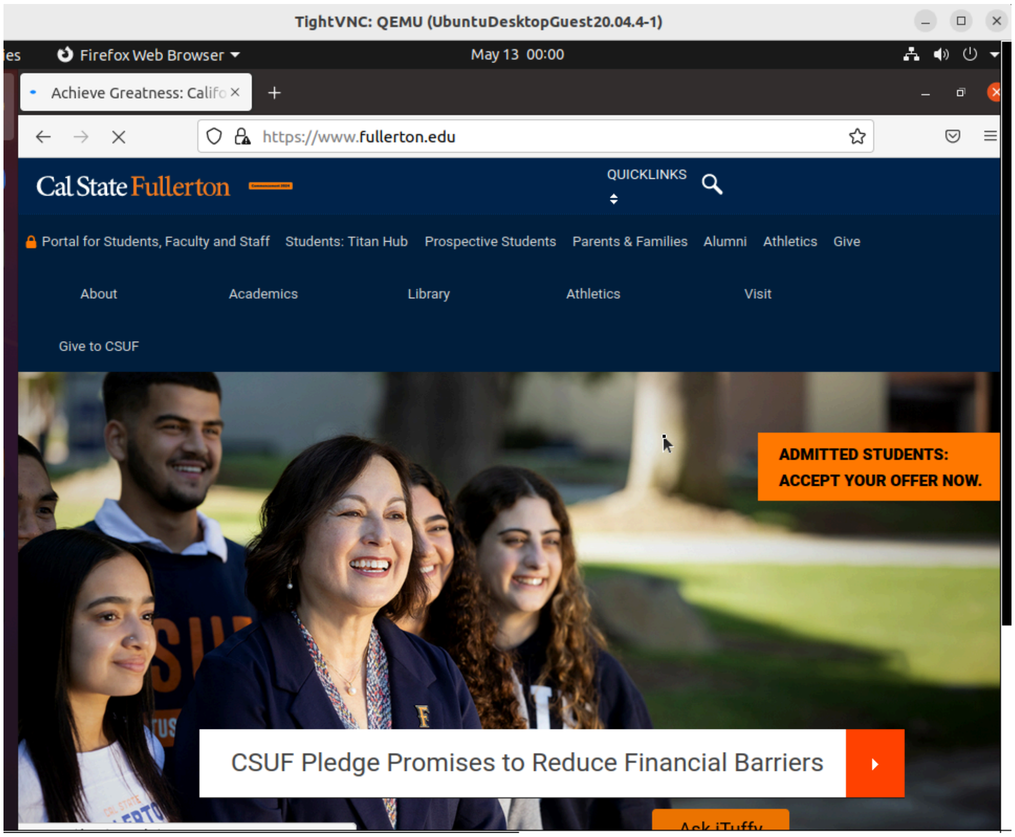
Rules (pass needs to be above block for it to work):



□	✓	0/3.09 MiB	IPv4+6 TCP	*	*	FullertonEdu	443 (HTTPS)	*	none	Allow HTTPS to www.fullerton.edu	
□	✗	0/26 KiB	IPv4+6 TCP	*	*	*	443 (HTTPS)	*	none	Block all other HTTPS traffic	

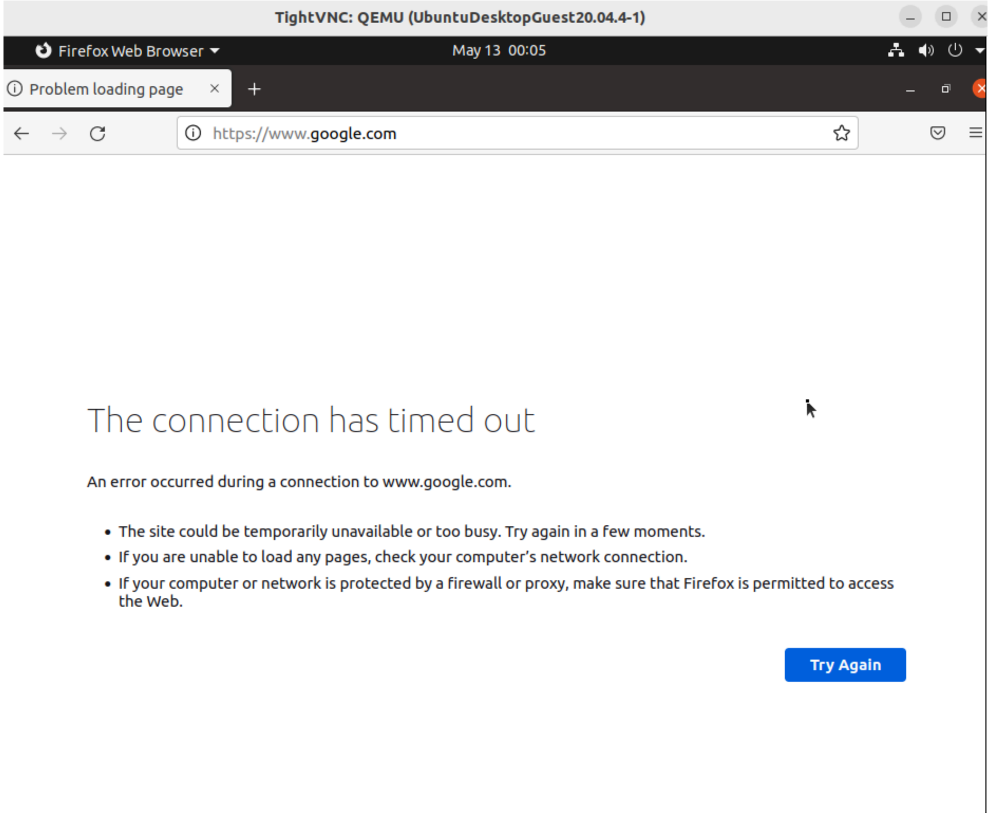
Testing:

Opening www.fullerton.edu:


TightVNC: QEMU (UbuntuDesktopGuest20.04.4-1)
Firefox Web Browser
May 13 00:00
Achieve Greatness: Califo
https://www.fullerton.edu
Cal State Fullerton
QUICKLINKS
Portal for Students, Faculty and Staff
Students: Titan Hub
Prospective Students
Parents & Families
Alumni
Athletics
Give
About
Academics
Library
Athletics
Visit
Give to CSUF
ADMITTED STUDENTS: ACCEPT YOUR OFFER NOW.
CSUF Pledge Promises to Reduce Financial Barriers
Ask iTuffy

Opening www.google.com:

Doesn’t load



The connection has timed out

An error occurred during a connection to www.google.com.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer’s network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.