FIT9137 Assignment 3 - 27030768

Task A: Routing

Subnets which are directly connected to a router are connected via their link number, via "ip route add <subnet_address> dev <link interface>". The most direct routes are chosen for routers R1, R2, R3 and R4; R3-R4 is connected via R1 following the faster propagation delay, ignoring the slower link speed. The node "Internet" has no default route as it directs traffic from each side to the other, there is no logical default route for it and a default route would create a routing loop. The routing tables for R1-R4 and all static routing configs required are as follows:

R1 config:

R1:R1
R4:R4
R2:R2
default: R3

```
ip route add 159.187.69.0/24 dev eth0
ip route add 159.187.192.0/24 via 159.187.132.2
ip route add 159.187.53.0/24 via 159.187.44.2
ip route add default via 159.187.67.2
```

R4 config:

R4:R4
R1:R1
R2:R2
default: R3

```
ip route add 159.187.192.0/24 dev eth0
ip route add 159.187.69.0/24 via 159.187.132.1
ip route add 159.187.53.0/24 via 159.187.128.2
ip route add default via 159.187.132.1
```

R2 config:

R2:R2
R1:R1
R4:R4
default: R3

```
ip route add 159.187.53.0/24 dev eth0
ip route add 159.187.69.0/24 via 159.187.44.1
ip route add 159.187.192.0/24 via 159.187.128.1
ip route add default via 159.187.113.1
```

R3 config:

```
R1:R1
R2:R2
R4:R1
default: Internet

ip route add 159.187.69.0/24 via 159.187.67.1
ip route add 159.187.53.0/24 via 159.187.113.2
ip route add 159.187.192.0/24 via 159.187.67.1
default Internet via 21.72.125.2/24
```

minerva config:

```
default: Internet
ip route add 140.119.40.0/24 dev eth1
ip route add 140.119.235.0/24 dev eth2
ip route add default via 113.131.151.1
```

Internet config:

```
ip route add 89.182.31.10/24 dev eth2
ip route add 159.187.0.0/16 via 21.72.125.1
ip route add 140.119.0.0/16 via 113.131.151.2
```

Task B: DHCP Server

Following the format of R1, the subnet we are assigning IP addresses to is 140.119.40.0, and the domain name server is the node artemis with an IP address of 140.119.235.11/24. As static IPs override dynamic IPs, the static IP on extClient1 and extClient2 were removed to be reassigned dynamic IPs from the DHCP server. This leads to the following DHCP config on the node minerva:

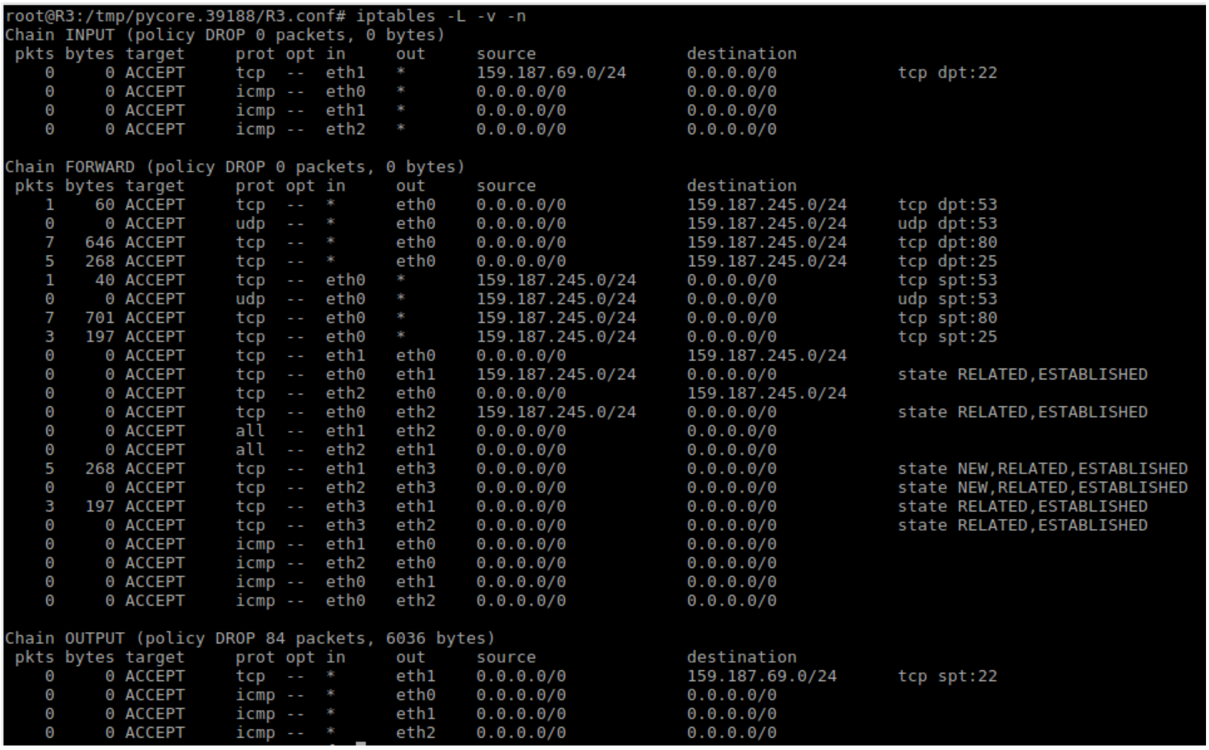
Node minerva:

DHCP:

```
log-facility local6;

default-lease-time 36000;
max-lease-time 72000;

ddns-update-style none;

subnet 140.119.40.0 netmask 255.255.255.0 {
  pool {
    range 140.119.40.127 140.119.40.254;
    default-lease-time 36000;
    option routers 140.119.40.1;
    option domain-name-servers 140.119.235.11;
    option domain-name “delos.edu”;
  }
}
```

Task C: Firewall

By default, traffic is dropped, and only allowed to pass through if it matches a rule. “FORWARD” entries refer to allowing the corresponding traffic to pass through the firewall, and “INPUT”/”OUTPUT” entries refer to allowing request/responses to the firewall router itself. Stateful inspection refers to the latter traffic only being allowed to the former if it is in response to a request from the former.
DNS is on port 53, HTTP on port 80, STMP on port 25, SSH on port 22.
The requirements and corresponding rules for the R3 firewall are as follows:

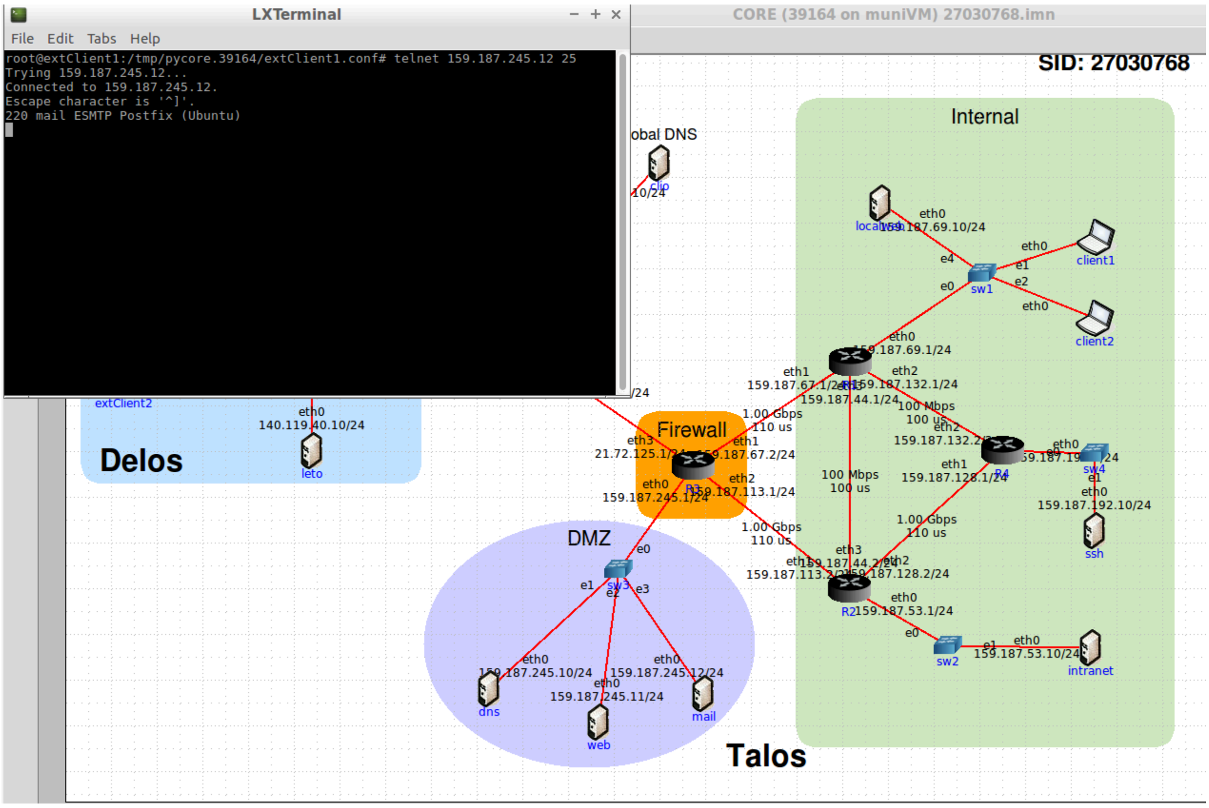


```
root@R3:/tmp/pycore.39188/R3.conf# iptables -L -v -n
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  eth1   *       159.187.69.0/24      0.0.0.0/0            tcp dpt:22
    0     0 ACCEPT     icmp --  eth0   *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     icmp --  eth1   *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     icmp --  eth2   *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    1    60 ACCEPT     tcp  --  *      eth0    0.0.0.0/0            159.187.245.0/24     tcp dpt:53
    0     0 ACCEPT     udp  --  *      eth0    0.0.0.0/0            159.187.245.0/24     udp dpt:53
    7   646 ACCEPT     tcp  --  *      eth0    0.0.0.0/0            159.187.245.0/24     tcp dpt:80
    5   268 ACCEPT     tcp  --  *      eth0    0.0.0.0/0            159.187.245.0/24     tcp dpt:25
    1    40 ACCEPT     tcp  --  eth0   *       159.187.245.0/24     0.0.0.0/0            tcp spt:53
    0     0 ACCEPT     udp  --  eth0   *       159.187.245.0/24     0.0.0.0/0            udp spt:53
    7   701 ACCEPT     tcp  --  eth0   *       159.187.245.0/24     0.0.0.0/0            tcp spt:80
    3   197 ACCEPT     tcp  --  eth0   *       159.187.245.0/24     0.0.0.0/0            tcp spt:25
    0     0 ACCEPT     tcp  --  eth1   eth0    0.0.0.0/0            159.187.245.0/24
    0     0 ACCEPT     tcp  --  eth0   eth1    159.187.245.0/24     0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  eth2   eth0    0.0.0.0/0            159.187.245.0/24
    0     0 ACCEPT     tcp  --  eth0   eth2    159.187.245.0/24     0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 ACCEPT     all  --  eth1   eth2    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     all  --  eth2   eth1    0.0.0.0/0            0.0.0.0/0
    5   268 ACCEPT     tcp  --  eth1   eth3    0.0.0.0/0            0.0.0.0/0            state NEW,RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  eth2   eth3    0.0.0.0/0            0.0.0.0/0            state NEW,RELATED,ESTABLISHED
    3   197 ACCEPT     tcp  --  eth3   eth1    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  eth3   eth2    0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 ACCEPT     icmp --  eth1   eth0    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     icmp --  eth2   eth0    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     icmp --  eth0   eth1    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     icmp --  eth0   eth2    0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy DROP 84 packets, 6036 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     tcp  --  *      eth1    0.0.0.0/0            159.187.69.0/24      tcp spt:22
    0     0 ACCEPT     icmp --  *      eth0    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     icmp --  *      eth1    0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     icmp --  *      eth2    0.0.0.0/0            0.0.0.0/0
```

Requirement #1:

Allow traffic from anywhere to DMZ for the provided service by each server. In the DMZ, DNS is on port 53 and on both TCP and UDP at 159.187.245.10, HTTP (web service) is on port 80 at 159.187.245.11, and SMTP (mail service) is on port 25 at 159.187.245.12.

```
iptables -A FORWARD -o eth0 -d 159.187.245.10/24 -p tcp --dport 53 -j ACCEPT
iptables -A FORWARD -o eth0 -d 159.187.245.10/24 -p udp --dport 53 -j ACCEPT
iptables -A FORWARD -o eth0 -d 159.187.245.11/24 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -o eth0 -d 159.187.245.12/24 -p tcp --dport 25 -j ACCEPT
```



```
root@extClient1:/tmp/pycore.39164/extClient1.conf# telnet 159.187.245.12 25
Trying 159.187.245.12...
Connected to 159.187.245.12.
Escape character is '^]'.
220 mail ESMTP Postfix (Ubuntu)
```

Requirement #2:

Allow servers in DMZ to initiate a connection if it is required by the service, stateful inspection DMZ -> External. This is the mirror of rule #1. The return connection is covered by rule #1.

```
iptables -A FORWARD -i eth0 -s 159.187.245.10/24 -p tcp --sport 53 -j ACCEPT
iptables -A FORWARD -i eth0 -s 159.187.245.10/24 -p udp --sport 53 -j ACCEPT
iptables -A FORWARD -i eth0 -s 159.187.245.11/24 -p tcp --sport 80 -j ACCEPT
iptables -A FORWARD -i eth0 -s 159.187.245.12/24 -p tcp --sport 25 -j ACCEPT
```

Requirement #3:

Allow internal hosts to access all DMZ services, stateful inspection Internal -> DMZ. All internal hosts are connected to the firewall on either eth1 or eth2, and the DMZ is connected to the firewall on eth0 with a subnet IP address of 159.187.245.0/24. As we do not care where in the internal network the internal hosts are, there is no need to check for the internal host IP address beyond checking their link direction.

```
iptables -A FORWARD -i eth1 -o eth0 -d 159.187.245.0/24 -p tcp -j ACCEPT
iptables -A FORWARD -i eth0 -o eth1 -s 159.187.245.0/24 -p tcp -m state –state
RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth2 -o eth0 -d 159.187.245.0/24 -p tcp -j ACCEPT
iptables -A FORWARD -i eth0 -o eth2 -s 159.187.245.0/24 -p tcp -m state –state
RELATED,ESTABLISHED -j ACCEPT
```

Requirement #4:

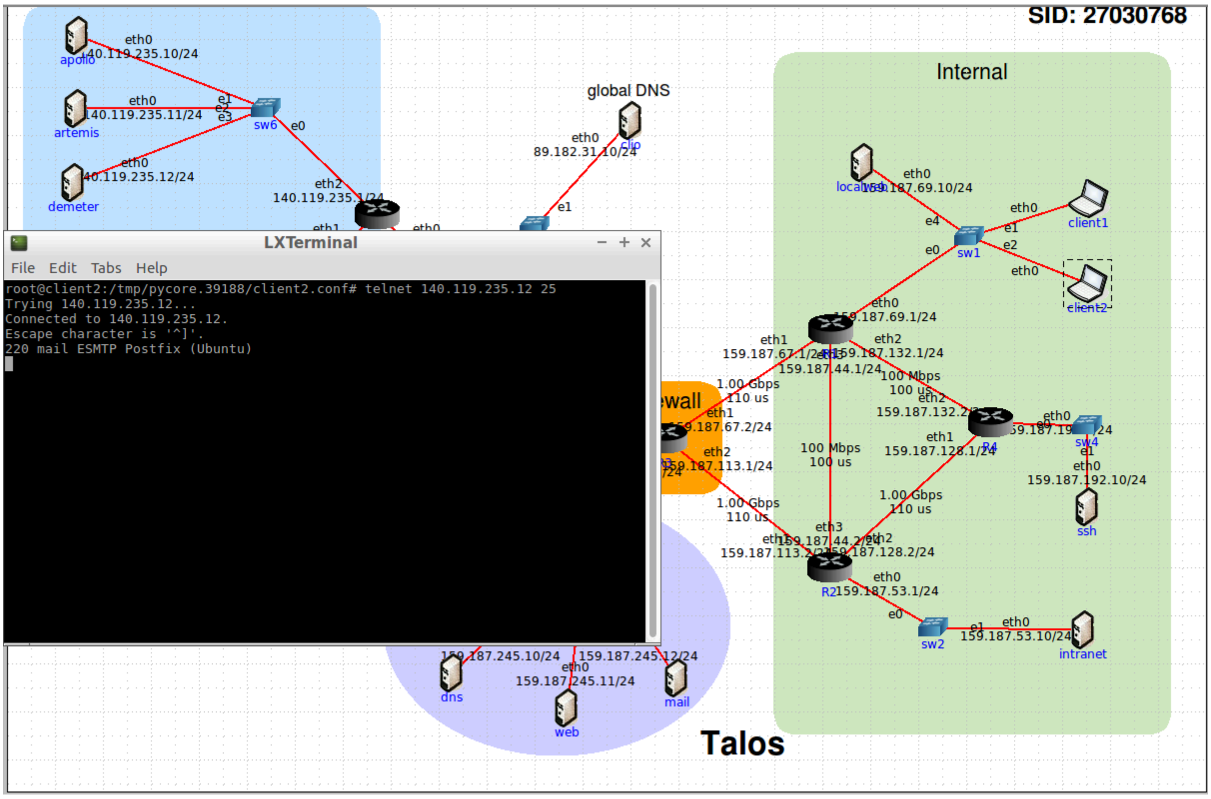
Allow all Internal traffic to other Internal hosts. These correspond to data interchanging between links eth1 and eth2.

```
iptables -A FORWARD -i eth1 -o eth2 -j ACCEPT
iptables -A FORWARD -i eth2 -o eth1 -j ACCEPT
```

Requirement #5:

Allow internal nodes to access external servers, stateful inspection Internal -> External. Internal nodes are on link eth1 and eth2, and external servers are on link eth3. Responses to requests are tracked by “RELATED” or “ESTABLISHED” states.

iptables -A FORWARD -i eth1 -o eth3 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth2 -o eth3 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth3 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth3 -o eth2 -m state --state RELATED,ESTABLISHED -j ACCEPT

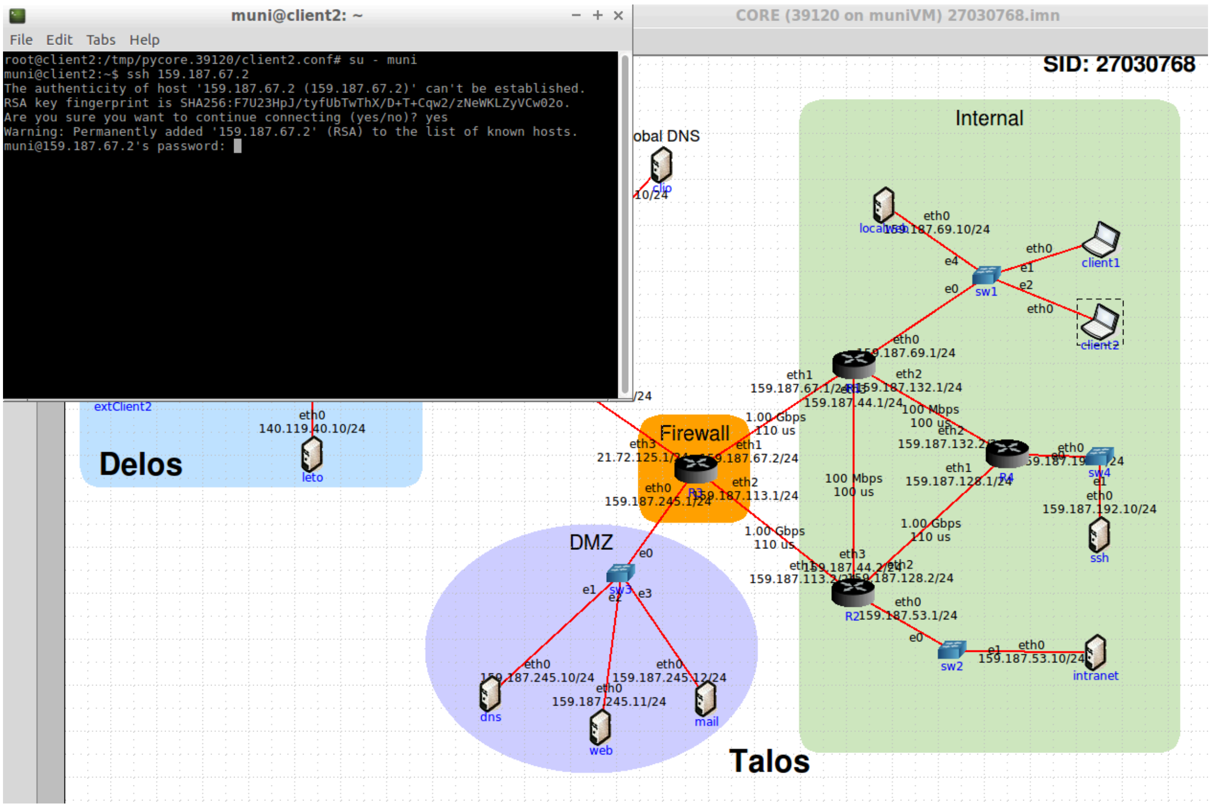


```
root@client2:/tmp/pycore.39188/client2.conf# telnet 140.119.235.12 25
Trying 140.119.235.12...
Connected to 140.119.235.12.
Escape character is '^]'.
220 mail ESMTP Postfix (Ubuntu)
```

Requirement #6:

Allow Talos clients to ssh to R3 firewall. Talos clients are any host connected to R1.eth0 subnet. The Talos client subnet is 159.187.69.0/24, and it enters the R3 firewall through the eth1 link on R3.

```
iptables -A INPUT -i eth1 -s 159.187.69.0/24 -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -o eth1 -d 159.187.69.0/24 -p tcp --sport 22 -j ACCEPT
```

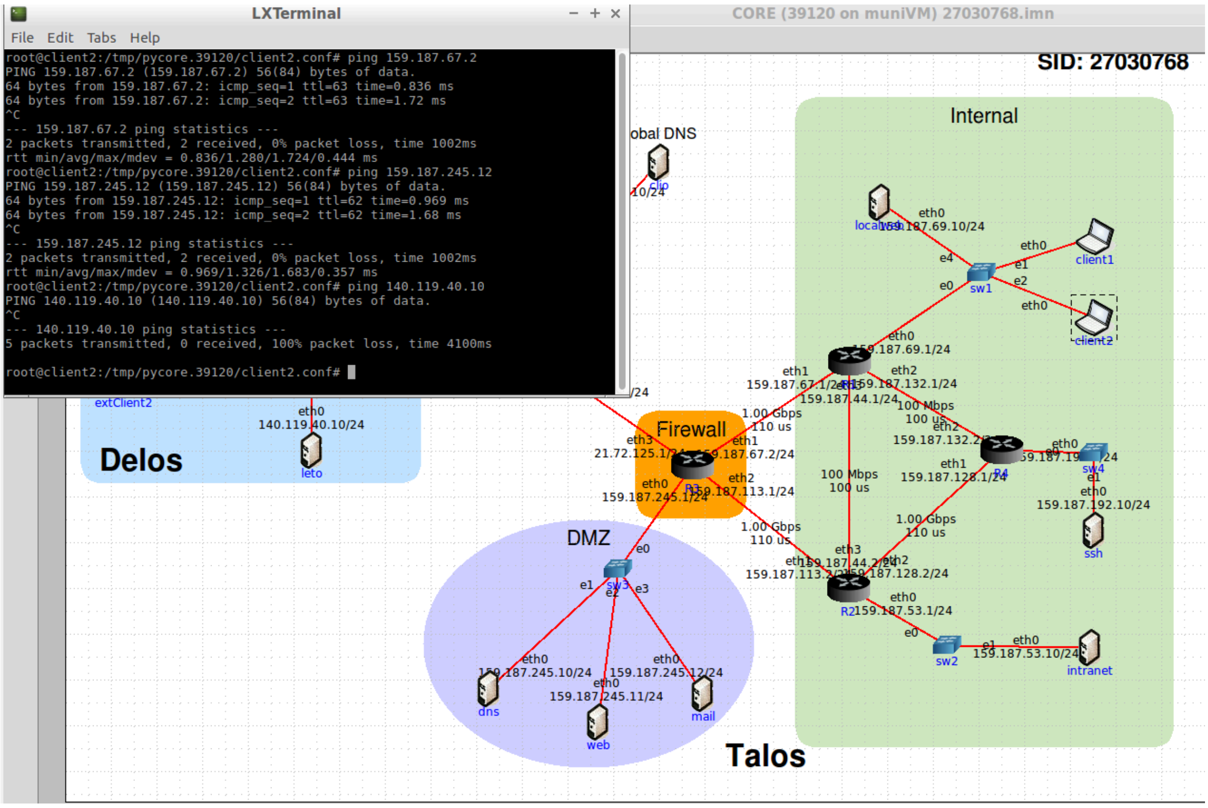


```
root@client2:/tmp/pycore.39120/client2.conf# su - muni
muni@client2:~$ ssh 159.187.67.2
The authenticity of host '159.187.67.2 (159.187.67.2)' can't be established.
RSA key fingerprint is SHA256:F7U23HpJ/tyfUbTwThX/D+T+Cqw2/zNeWKLZyVCw02o.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '159.187.67.2' (RSA) to the list of known hosts.
muni@159.187.67.2's password: █
```

Requirement #7:

Allow R3 firewall to send and receive ICMP echo requests and replies to internal Talos nodes and all DMZ servers. The firewall itself needs to be able to send and receive ICMP, and also forward it between Talos and DMZ. Talos is on links eth1 and eth2, and DMZ is on link eth0.

```
iptables -A FORWARD -i eth1 -o eth0 -p icmp -j ACCEPT
iptables -A FORWARD -i eth2 -o eth0 -p icmp -j ACCEPT
iptables -A FORWARD -i eth0 -o eth1 -p icmp -j ACCEPT
iptables -A FORWARD -i eth0 -o eth2 -p icmp -j ACCEPT
iptables -A INPUT -i eth0 -p icmp -j ACCEPT
iptables -A INPUT -i eth1 -p icmp -j ACCEPT
iptables -A INPUT -i eth2 -p icmp -j ACCEPT
iptables -A OUTPUT -o eth0 -p icmp -j ACCEPT
iptables -A OUTPUT -o eth1 -p icmp -j ACCEPT
iptables -A OUTPUT -o eth2 -p icmp -j ACCEPT
```

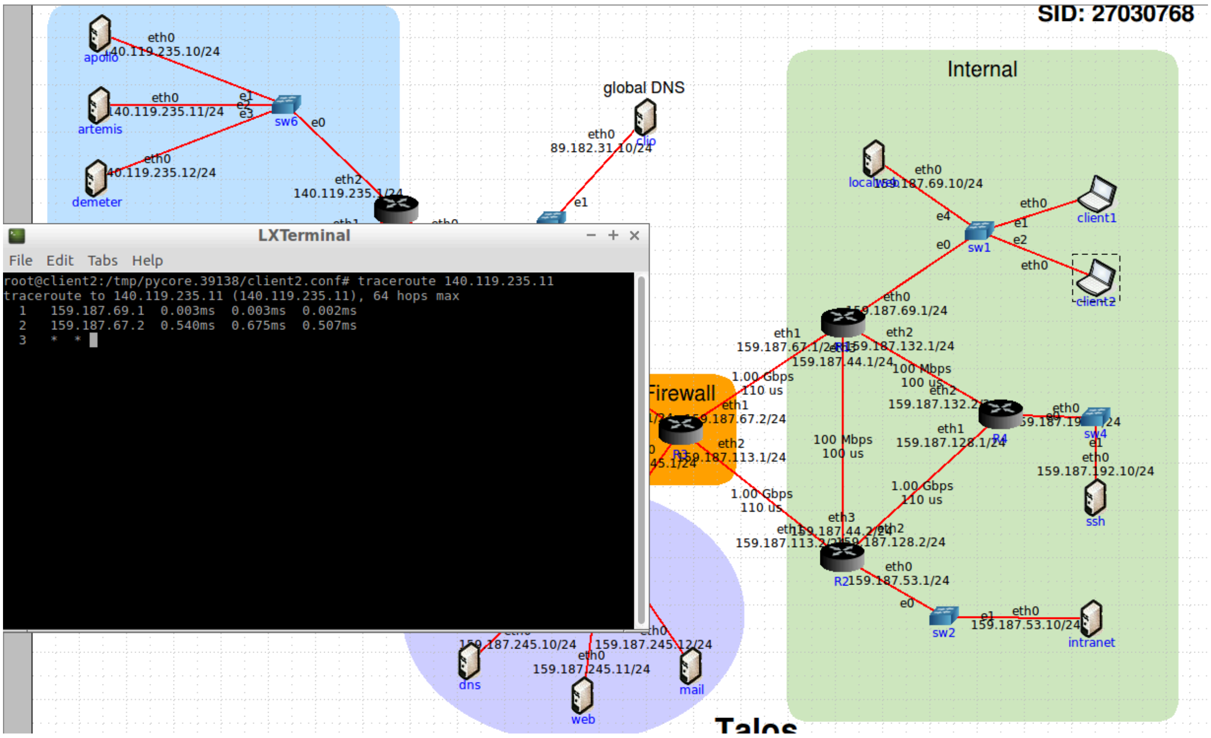


```
root@client2:/tmp/pycore.39120/client2.conf# ping 159.187.67.2
PING 159.187.67.2 (159.187.67.2) 56(84) bytes of data.
64 bytes from 159.187.67.2: icmp_seq=1 ttl=63 time=0.836 ms
64 bytes from 159.187.67.2: icmp_seq=2 ttl=63 time=1.72 ms
^C
--- 159.187.67.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.836/1.280/1.724/0.444 ms
root@client2:/tmp/pycore.39120/client2.conf# ping 159.187.245.12
PING 159.187.245.12 (159.187.245.12) 56(84) bytes of data.
64 bytes from 159.187.245.12: icmp_seq=1 ttl=62 time=0.969 ms
64 bytes from 159.187.245.12: icmp_seq=2 ttl=62 time=1.68 ms
^C
--- 159.187.245.12 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.969/1.326/1.683/0.357 ms
root@client2:/tmp/pycore.39120/client2.conf# ping 140.119.40.10
PING 140.119.40.10 (140.119.40.10) 56(84) bytes of data.
^C
--- 140.119.40.10 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4100ms

root@client2:/tmp/pycore.39120/client2.conf# 
```

Requirement #8:

Drop all traffic by default. Since this is the default, it is put at the very top of the config file.

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```



```
root@client2:/tmp/pycore.39138/client2.conf# traceroute 140.119.235.11
traceroute to 140.119.235.11 (140.119.235.11), 64 hops max
  1   159.187.69.1  0.003ms  0.003ms  0.002ms
  2   159.187.67.2  0.540ms  0.675ms  0.507ms
  3   *  *
```