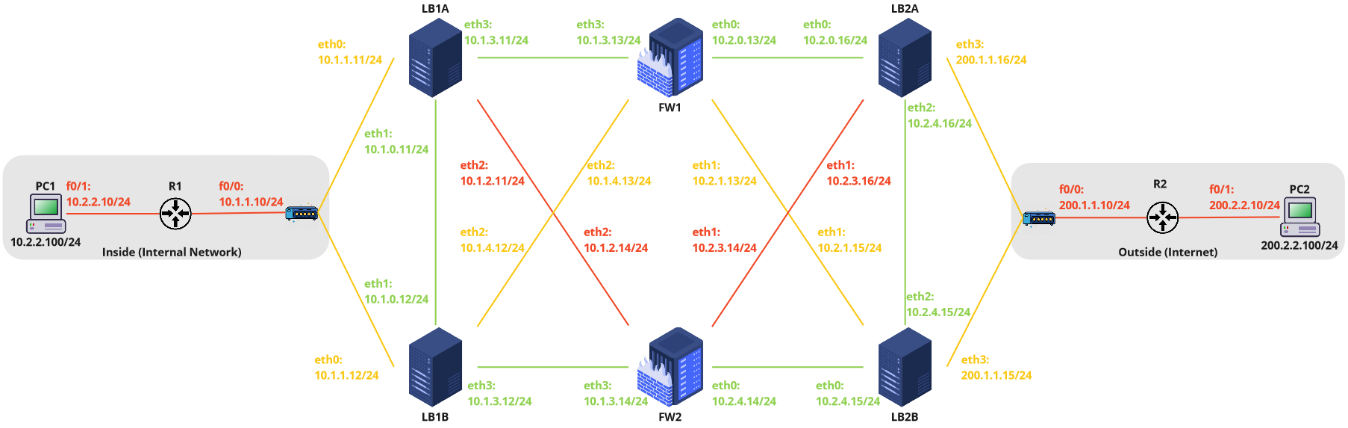
Authors: Camila Fonseca (nmec: 97880), Rodrigo Lima (nmec: 98457)

Introduction

This report details the design and implementation of a simple network configuration, while employing load-balancing with redundancy and state synchronization, as well as policy definition and integrated deployment. The aim is to create a resilient, high-performance network infrastructure that ensures availability, security, and scalability.

Load-Balancing Scenario [Exercise 9]

The network configuration follows the following network diagram:



The network is configured with redundancy and state synchronization, which can be seen in the following configurations:

Load Balancer Template Configuration

VRRP (Virtual Router Redundancy Protocol)

This configuration enables redundancy, allowing multiple devices to work together as a group and share a virtual IP address

```
# vrrp
set high-availability vrrp group LB1Cluster vrid 10
set high-availability vrrp group LB1Cluster interface eth1
set high-availability vrrp group LB1Cluster virtual-address 192.168.100.1/24
set high-availability vrrp sync-group LB1Cluster member LB1Cluster
set high-availability vrrp group LB1Cluster rfc3768-compatibility
```

This configuration enables state synchronization between the load balancers, which ensures a seamless failover in case of device failure.

```
# conntrack sync
set service conntrack-sync accept-protocol 'tcp,udp,icmp'
set service conntrack-sync failover-mechanism vrrp sync-group LB1Cluster
set service conntrack-sync interface eth1
set service conntrack-sync mcast-group 225.0.0.50
set service conntrack-sync disable-external-cache
```

This configuration enables load balancing, in order to distribute traffic across multiple devices.

```
# load balancing
set load-balancing wan interface-health eth3 nexthop 10.1.3.13
set load-balancing wan interface-health eth2 nexthop 10.1.2.14
set load-balancing wan rule 1 inbound-interface eth0
set load-balancing wan rule 1 interface eth3 weight 1
set load-balancing wan rule 1 interface eth2 weight 1
set load-balancing wan sticky-connections inbound
set load-balancing wan disable-source-nat
```

Note

In this scenario, the firewalls are not directly involved in load balancing or VRRP failover. The load balancing and failover are managed by the two load balancers LB1A and LB1B, which are configured to synchronize the connection state information between them using the conntrack-sync mechanism.

Since both LB1A and LB1B are in the same VRRP group and are members of the same sync-group, they are aware of the state of connections handled by each other. When a failover occurs, the new active load balancer can continue handling the existing connections without dropping them.

The firewalls, on the other hand, are not involved in connection tracking or load balancing, and they do not need to synchronize their state with the load balancers. They simply need to have their default gateway set to the IP address of the active load balancer in the VRRP cluster so that they can forward the non-dropped traffic to the next load balancer.

Note

In this project sticky connections are enabled, which means that once a client is connected to a specific device behind the load-balancer, subsequent requests from that client will be sent to the same device. Other load balancing algorithms that may allow the nonexistence of load-balancers synchronization are:

1. Round Robin: This algorithm distributes incoming requests sequentially among backend servers in a circular manner. As there is no need to maintain any state, there is no need for load-balancer synchronization.

2. Least Connections: This algorithm directs incoming requests to the backend server with the fewest active connections. In scenarios where the servers have similar capacity, this algorithm can work effectively without load-balancer synchronization.

3. Random: This algorithm selects a backend server randomly for each incoming request, and hence, no state is maintained. However, this method may not provide the best load distribution, especially in cases where the backend servers have varying capacities.

Note

During a Distributed Denial of Service (DDoS) attack, the attacker aims to overwhelm a target network or device with a flood of traffic, making it unreachable or unusable. In response, network administrators may employ various mitigation techniques to filter out the malicious traffic and keep the network functioning.

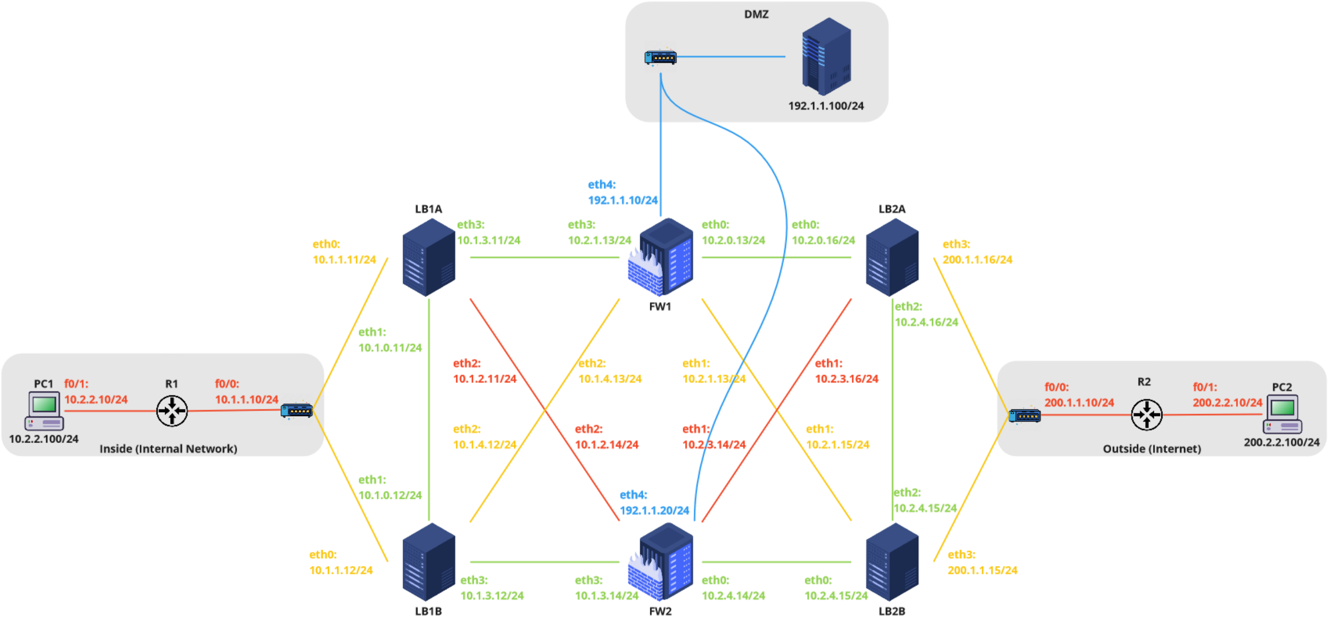
One such technique is to distribute the traffic across multiple servers or devices using load balancing, so that no single device becomes overwhelmed. However, if the load balancers are synchronizing their device/connection states, this can create a problem during a DDoS attack.

If the load balancers are synchronized, then when one load balancer detects a flood of traffic, it will direct traffic away from the affected device to another device. However, since all the load balancers are synchronized, they will direct all traffic away from the affected device, leaving only a single device to handle all the traffic. This can cause the overwhelmed device to crash or become unusable, defeating the purpose of load balancing.

Therefore, it is often better to have independent load balancers that do not synchronize their device/connection states during a DDoS attack. This allows each load balancer to make its own decisions about where to direct traffic, based on its own view of the network and the devices that it is managing. This approach helps to ensure that the network remains available and functional during a DDoS attack.

Policies Definition and Integrated Deployment [Exercise 10]

The network configuration follows the following network diagram:



Firewall Template Configuration

Control policies

Zone definition

The project was divided into three distinct zones: DMZ, Inside (Internal Network) and Outside (Internet), using the following zone policy configuration:

```
# Set Zone Policies
set zone-policy zone INSIDE description "Inside (Internal Network)"
set zone-policy zone INSIDE interface eth2
set zone-policy zone INSIDE interface eth3
set zone-policy zone DMZ description "DMZ"
set zone-policy zone DMZ interface eth4
set zone-policy zone OUTSIDE description "Outside (Internet)"
set zone-policy zone OUTSIDE interface eth0
set zone-policy zone OUTSIDE interface eth1
```

ACL definition

To limit the access through the network, the following ACLs were created:

```
# Access Control Lists
set firewall name RESTRICTED default-action drop
set firewall name ESTABLISHED default-action drop
```

Established connetions

This rule is used to accept established and related connections, which have been previously initiated.

```
# Accept estabelished
set firewall name ESTABLISHED rule 1 description "Accept Established-Related
Connections"
set firewall name ESTABLISHED rule 1 action accept
set firewall name ESTABLISHED rule 1 state established enable
set firewall name ESTABLISHED rule 1 state related enable
```

Restricted

To better restrict access through the network only some ports and protocols were allowed through it.

HTTP

```
# HTTP
set firewall name RESTRICTED rule 10 description "Accept HTTP"
set firewall name RESTRICTED rule 10 action accept
set firewall name RESTRICTED rule 10 protocol tcp
set firewall name RESTRICTED rule 10 destination address 0.0.0.0/0
set firewall name RESTRICTED rule 10 destination port 80
```

HTTPS

```
# HTTPS
set firewall name RESTRICTED rule 20 description "Accept HTTPS"
set firewall name RESTRICTED rule 20 action accept
set firewall name RESTRICTED rule 20 protocol tcp
set firewall name RESTRICTED rule 20 destination address 0.0.0.0/0
set firewall name RESTRICTED rule 20 destination port 443
```

SSH

```
# SSH
set firewall name RESTRICTED rule 30 description "Accept SSH"
set firewall name RESTRICTED rule 30 action accept
set firewall name RESTRICTED rule 30 protocol tcp
set firewall name RESTRICTED rule 30 destination address 0.0.0.0/0
set firewall name RESTRICTED rule 30 destination port 22
```

DNS

```
# DNS
set firewall name RESTRICTED rule 40 description "Accept DNS TCP"
set firewall name RESTRICTED rule 40 action accept
set firewall name RESTRICTED rule 40 protocol tcp
set firewall name RESTRICTED rule 40 destination address 0.0.0.0/0
set firewall name RESTRICTED rule 40 destination port 53

set firewall name RESTRICTED rule 50 description "Accept DNS UDP"
set firewall name RESTRICTED rule 50 action accept
set firewall name RESTRICTED rule 50 protocol udp
set firewall name RESTRICTED rule 50 destination address 0.0.0.0/0
set firewall name RESTRICTED rule 50 destination port 53
```

ICMP

```
# ICMP
set firewall name RESTRICTED rule 60 description "Accept ICMP"
set firewall name RESTRICTED rule 60 action accept
set firewall name RESTRICTED rule 60 protocol icmp
set firewall name RESTRICTED rule 60 destination address 0.0.0.0/0
```

ACL Application

The application of these ACLs were applied as follows:

```
# Apply ACLs to Zone Policies
set zone-policy zone DMZ from INSIDE firewall name RESTRICTED
set zone-policy zone DMZ from OUTSIDE firewall name RESTRICTED
set zone-policy zone OUTSIDE from INSIDE firewall name RESTRICTED
set zone-policy zone OUTSIDE from DMZ firewall name ESTABLISHED
set zone-policy zone INSIDE from OUTSIDE firewall name ESTABLISHED
set zone-policy zone INSIDE from DMZ firewall name ESTABLISHED
```

As it stands, devices in the DMZ may not initiate connections to either Inside or Outside zones, but can receive connections from either, given they're in an approved protocol/port as detailed in the Restricted ACL. Traffic is allowed to the outside of the DMZ after the connection has been initiated from outside.

Devices in the Inside zone can send and receive Restricted traffic from either DMZ and Outside.

Devices in the Outside zone (Internet) can initiate connections with the DMZ but not with the Inside zone, also under the Restricted ACL. After a connection is established from Inside, traffic may flow Outside → Inside.

Rate Limiting

To better mitigate possible DDoS attacks, a rate-limiting traffic policy to shape the outbound traffic on the eth4 interface was applied. The rate limit is set to 10 Mbps and was configured as follows:

```
# Rate limiting
set traffic-policy shaper RATE-LIMIT-10Mbps bandwidth 10mbit
set traffic-policy shaper RATE-LIMIT-10Mbps default bandwidth 100%

set interfaces ethernet eth4 traffic-policy out RATE-LIMIT-10Mbps
```

Block List

To better mitigate DDoS attacks, it was also implemented a firewall rule named "BLOCKED" to block traffic from specific IP addresses that belong to a group called "ddos_blocklist":

```
# BlockList
set firewall name BLOCKED rule 70 description "Block IPs"
set firewall name BLOCKED rule 70 action drop
set firewall name BLOCKED 70 source group address-group ddos_blocklist
```

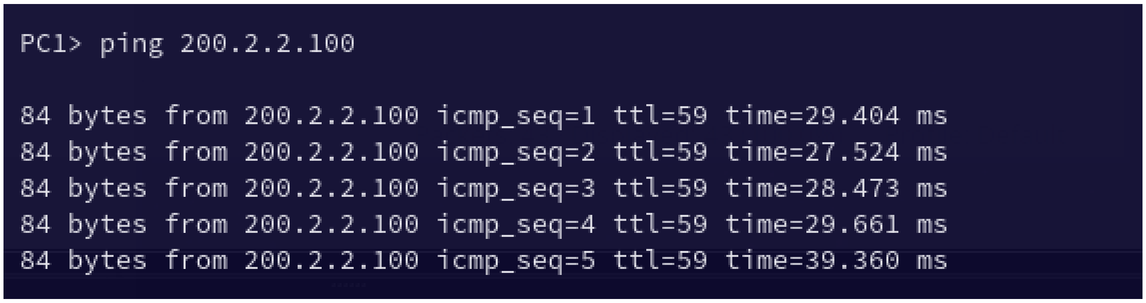
It is assumed that an external monitoring system exists and will identify the external IP address of the DDoS participants, dynamically providing an updated list.
One such possible implementation of this is the following bash script, with the help of a file containing said list that should be imported:

```
#!/bin/bash

# Define the path to the blocklist file and the firewall group name
BLOCKLIST_FILE="/path/to/blocklist.txt"
FIREWALL_GROUP_NAME="ddos_blocklist"

# Configure VyOS to apply the updated rules
sudo vtysh -c "configure terminal"

# Remove the existing firewall group, if it exists
sudo vtysh -c "delete firewall group address-group $FIREWALL_GROUP_NAME"

# Create a new firewall group and add the IP addresses from the blocklist file
while read -r ip; do
  sudo vtysh -c "set firewall group address-group $FIREWALL_GROUP_NAME address $ip"
done < "$BLOCKLIST_FILE"

# Commit and save the changes
sudo vtysh -c "commit"
sudo vtysh -c "save"
sudo vtysh -c "exit"
```

Connectivity Demo

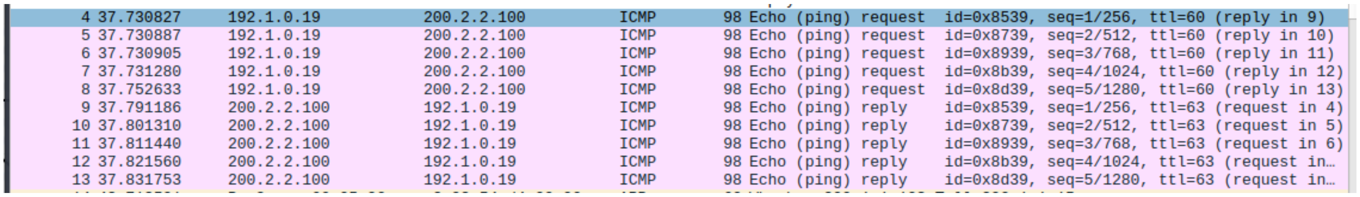
There is full connectivity from PC1 to PC2:

PC1→PC2



```
PC1> ping 200.2.2.100

84 bytes from 200.2.2.100 icmp_seq=1 ttl=59 time=29.404 ms
84 bytes from 200.2.2.100 icmp_seq=2 ttl=59 time=27.524 ms
84 bytes from 200.2.2.100 icmp_seq=3 ttl=59 time=28.473 ms
84 bytes from 200.2.2.100 icmp_seq=4 ttl=59 time=29.661 ms
84 bytes from 200.2.2.100 icmp_seq=5 ttl=59 time=39.360 ms
```

(Captured in between R2 and Switch2)

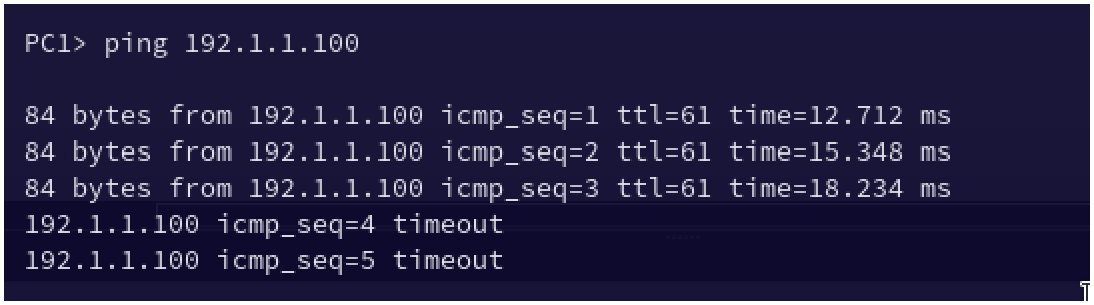


```
 4 37.730827   192.1.0.19    200.2.2.100   ICMP   98 Echo (ping) request  id=0x8539, seq=1/256, ttl=60 (reply in 9)
 5 37.730887   192.1.0.19    200.2.2.100   ICMP   98 Echo (ping) request  id=0x8739, seq=2/512, ttl=60 (reply in 10)
 6 37.730905   192.1.0.19    200.2.2.100   ICMP   98 Echo (ping) request  id=0x8939, seq=3/768, ttl=60 (reply in 11)
 7 37.731280   192.1.0.19    200.2.2.100   ICMP   98 Echo (ping) request  id=0x8b39, seq=4/1024, ttl=60 (reply in 12)
 8 37.752633   192.1.0.19    200.2.2.100   ICMP   98 Echo (ping) request  id=0x8d39, seq=5/1280, ttl=60 (reply in 13)
 9 37.791186   200.2.2.100   192.1.0.19    ICMP   98 Echo (ping) reply    id=0x8539, seq=1/256, ttl=63 (request in 4)
10 37.801310   200.2.2.100   192.1.0.19    ICMP   98 Echo (ping) reply    id=0x8739, seq=2/512, ttl=63 (request in 5)
11 37.811440   200.2.2.100   192.1.0.19    ICMP   98 Echo (ping) reply    id=0x8939, seq=3/768, ttl=63 (request in 6)
12 37.821560   200.2.2.100   192.1.0.19    ICMP   98 Echo (ping) reply    id=0x8b39, seq=4/1024, ttl=63 (request in…
13 37.831753   200.2.2.100   192.1.0.19    ICMP   98 Echo (ping) reply    id=0x8d39, seq=5/1280, ttl=63 (request in…
```

There is connectivity from PC1 to PC3, however there is a problem - PC3 has its' gateway set to FW1.
When the pings go through FW2, their replies come back through FW1, which drops

them, since it is set to drop packets incoming from the DMZ that aren't in previously established connections. This results in roughly half the ICMP requests timing out.

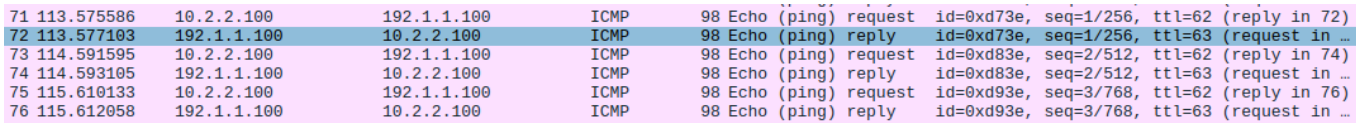
PC1→PC3



```
PC1> ping 192.1.1.100

84 bytes from 192.1.1.100 icmp_seq=1 ttl=61 time=12.712 ms
84 bytes from 192.1.1.100 icmp_seq=2 ttl=61 time=15.348 ms
84 bytes from 192.1.1.100 icmp_seq=3 ttl=61 time=18.234 ms
192.1.1.100 icmp_seq=4 timeout
192.1.1.100 icmp_seq=5 timeout
```

This can be verified by the following Wireshark captures:

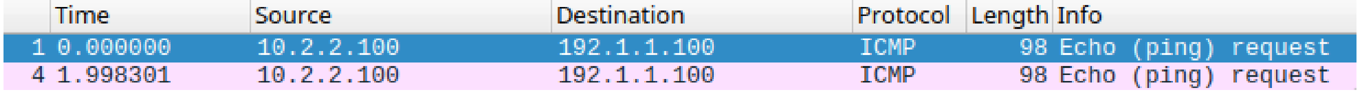
Between LB1A and FW1



```
71 113.575586   10.2.2.100    192.1.1.100   ICMP   98 Echo (ping) request  id=0xd73e, seq=1/256, ttl=62 (reply in 72)
72 113.577103   192.1.1.100   10.2.2.100    ICMP   98 Echo (ping) reply    id=0xd73e, seq=1/256, ttl=63 (request in …
73 114.591595   10.2.2.100    192.1.1.100   ICMP   98 Echo (ping) request  id=0xd83e, seq=2/512, ttl=62 (reply in 74)
74 114.593105   192.1.1.100   10.2.2.100    ICMP   98 Echo (ping) reply    id=0xd83e, seq=2/512, ttl=63 (request in …
75 115.610133   10.2.2.100    192.1.1.100   ICMP   98 Echo (ping) request  id=0xd93e, seq=3/768, ttl=62 (reply in 76)
76 115.612058   192.1.1.100   10.2.2.100    ICMP   98 Echo (ping) reply    id=0xd93e, seq=3/768, ttl=63 (request in …
```

(Replies are present.)

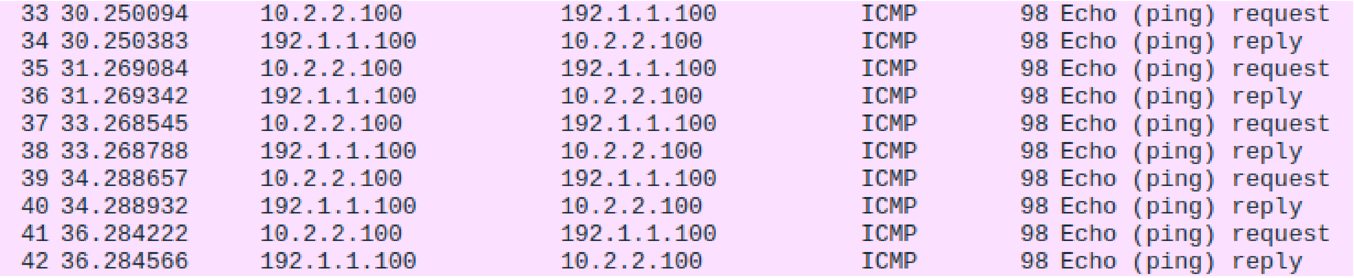
Between LB1A and FW2



```
   Time          Source        Destination   Protocol Length Info
 1 0.000000      10.2.2.100    192.1.1.100   ICMP      98 Echo (ping) request
 4 1.998301      10.2.2.100    192.1.1.100   ICMP      98 Echo (ping) request
```

(No replies.)

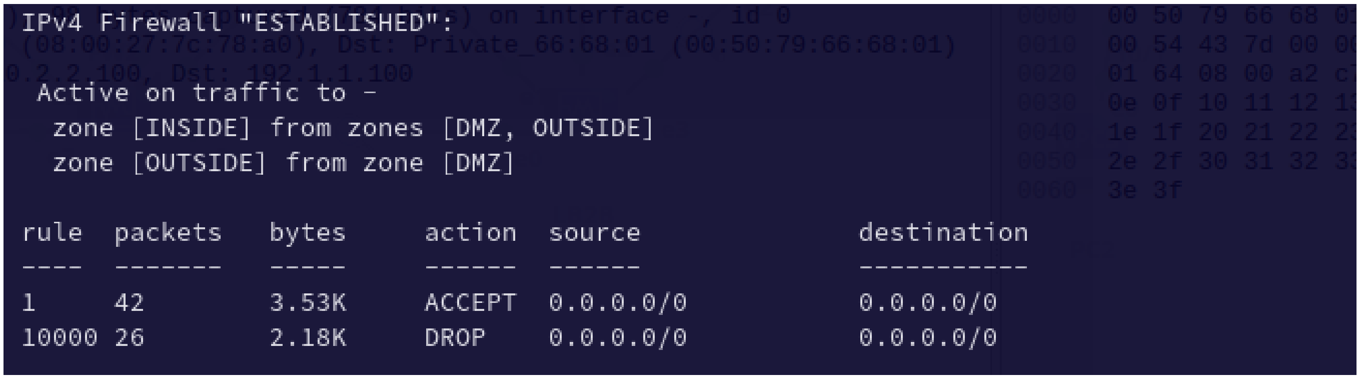
Between Switch3 and PC3(DMZ)



```
33 30.250094   10.2.2.100    192.1.1.100   ICMP   98 Echo (ping) request
34 30.250383   192.1.1.100   10.2.2.100    ICMP   98 Echo (ping) reply
35 31.269084   10.2.2.100    192.1.1.100   ICMP   98 Echo (ping) request
36 31.269342   192.1.1.100   10.2.2.100    ICMP   98 Echo (ping) reply
37 33.268545   10.2.2.100    192.1.1.100   ICMP   98 Echo (ping) request
38 33.268788   192.1.1.100   10.2.2.100    ICMP   98 Echo (ping) reply
39 34.288657   10.2.2.100    192.1.1.100   ICMP   98 Echo (ping) request
40 34.288932   192.1.1.100   10.2.2.100    ICMP   98 Echo (ping) reply
41 36.284222   10.2.2.100    192.1.1.100   ICMP   98 Echo (ping) request
42 36.284566   192.1.1.100   10.2.2.100    ICMP   98 Echo (ping) reply
```

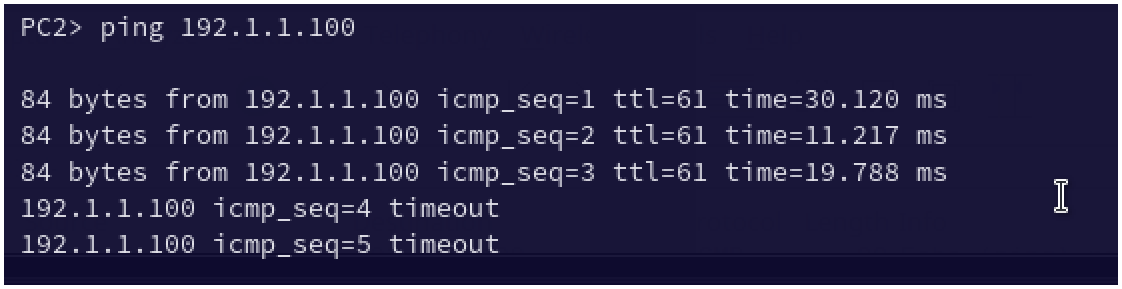
(All replies are present)

Furthermore, by looking at FW1's firewall statistics we can see it is indeed dropping packets.



```
IPv4 Firewall "ESTABLISHED":

 Active on traffic to -
  zone [INSIDE] from zones [DMZ, OUTSIDE]
  zone [OUTSIDE] from zone [DMZ]

rule  packets   bytes    action  source             destination
----  -------   -----    ------  ------             -----------
1     42        3.53K    ACCEPT  0.0.0.0/0          0.0.0.0/0
10000 26        2.18K    DROP    0.0.0.0/0          0.0.0.0/0
```

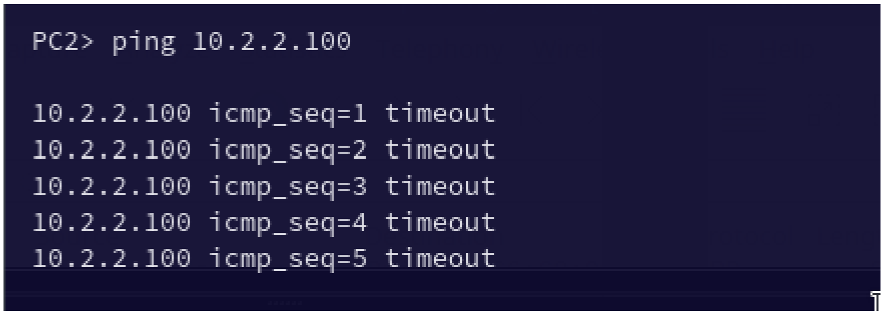
PC2 → PC3



```
PC2> ping 192.1.1.100

84 bytes from 192.1.1.100 icmp_seq=1 ttl=61 time=30.120 ms
84 bytes from 192.1.1.100 icmp_seq=2 ttl=61 time=11.217 ms
84 bytes from 192.1.1.100 icmp_seq=3 ttl=61 time=19.788 ms
192.1.1.100 icmp_seq=4 timeout
192.1.1.100 icmp_seq=5 timeout
```

Due to the same issue as before, half the ICMP requests get replies.

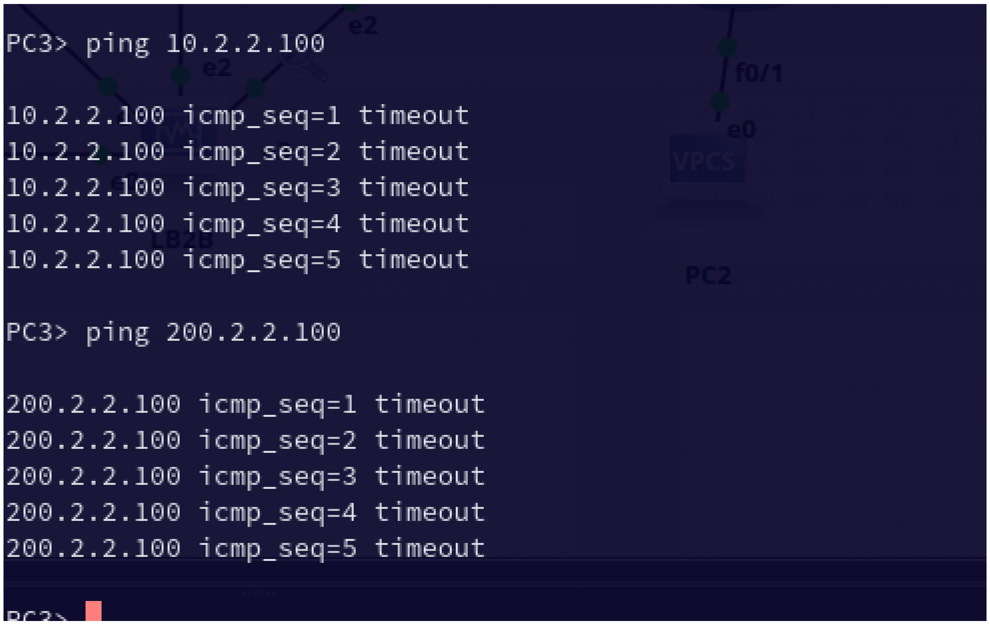
PC2→PC1



```
PC2> ping 10.2.2.100

10.2.2.100 icmp_seq=1 timeout
10.2.2.100 icmp_seq=2 timeout
10.2.2.100 icmp_seq=3 timeout
10.2.2.100 icmp_seq=4 timeout
10.2.2.100 icmp_seq=5 timeout
```

As intended, a device in the Outside zone cannot initiate connections with one in the Inside zone.

PC3→PC1 and PC3→PC2



```
PC3> ping 10.2.2.100

10.2.2.100 icmp_seq=1 timeout
10.2.2.100 icmp_seq=2 timeout
10.2.2.100 icmp_seq=3 timeout
10.2.2.100 icmp_seq=4 timeout
10.2.2.100 icmp_seq=5 timeout

PC3> ping 200.2.2.100

200.2.2.100 icmp_seq=1 timeout
200.2.2.100 icmp_seq=2 timeout
200.2.2.100 icmp_seq=3 timeout
200.2.2.100 icmp_seq=4 timeout
200.2.2.100 icmp_seq=5 timeout

PC3>
```

In a similar manner, the DMZ PC can't ping devices in either Inside or Outside zones.

Full configuration (Appendix)

PC1 (Computer)

```
ip 10.2.2.100/24 10.2.2.10
```

PC2 (Computer)

```
ip 200.2.2.100/24 200.2.2.10
```

PC3 (Computer DMZ)

```
ip 192.1.1.100/24 192.1.1.10
```

R1 (Router)

```
conf t
int f0/0
ip addr 10.1.1.10 255.255.255.0
no shut
int f0/1
ip addr 10.2.2.10 255.255.255.0
no shut

# Static Routes
## Internet
ip route 0.0.0.0 0.0.0.0 10.1.1.11
## DMZ
ip route 192.1.1.0 255.255.255.0 10.1.1.11

end
write
```

R2 (Router)

```
conf t
int f0/0
ip addr 200.1.1.10 255.255.255.0
no shut
int f0/1
ip addr 200.2.2.10 255.255.255.0
no shut

# Static Routes
## Internal
ip route 0.0.0.0 0.0.0.0 200.1.1.15
```

```
end
write
```

LB1A (Load Balancer)

```
configure
set system host-name LB1A
set interfaces ethernet eth0 address 10.1.1.11/24
set interfaces ethernet eth1 address 10.1.0.11/24
set interfaces ethernet eth2 address 10.1.2.11/24
set interfaces ethernet eth3 address 10.1.3.11/24

# Static routes
## Intranet
set protocols static route 10.2.2.0/24 next-hop 10.1.1.10
## Internet
set protocols static route 0.0.0.0/0 next-hop 10.1.3.13
set protocols static route 0.0.0.0/0 next-hop 10.1.2.14
## DMZ
set protocols static route 192.1.1.0/24 next-hop 10.1.3.13
set protocols static route 192.1.1.0/24 next-hop 10.1.2.14


set protocols static route 192.1.1.0/24 next-hop 10.1.1.13 disable

# vrrp
set high-availability vrrp group LB1Cluster vrid 10
set high-availability vrrp group LB1Cluster interface eth1
set high-availability vrrp group LB1Cluster virtual-address 192.168.100.1/24
set high-availability vrrp sync-group LB1Cluster member LB1Cluster
set high-availability vrrp group LB1Cluster rfc3768-compatibility

# conntrack sync
set service conntrack-sync accept-protocol 'tcp,udp,icmp'
set service conntrack-sync failover-mechanism vrrp sync-group LB1Cluster
set service conntrack-sync interface eth1
set service conntrack-sync mcast-group 225.0.0.50
set service conntrack-sync disable-external-cache
```

```
# load balancing
set load-balancing wan interface-health eth3 nexthop 10.1.3.13
set load-balancing wan interface-health eth2 nexthop 10.1.2.14
set load-balancing wan rule 1 inbound-interface eth0
set load-balancing wan rule 1 interface eth3 weight 1
set load-balancing wan rule 1 interface eth2 weight 1
set load-balancing wan sticky-connections inbound
set load-balancing wan disable-source-nat
commit
save
exit
```

LB1B (Load Balancer)

```
configure
set system host-name LB1B
set interfaces ethernet eth0 address 10.1.1.12/24
set interfaces ethernet eth1 address 10.1.0.12/24
set interfaces ethernet eth2 address 10.1.4.12/24
set interfaces ethernet eth3 address 10.1.3.12/24

# Static routes
## Intranet
set protocols static route 10.2.2.0/24 next-hop 10.1.1.10
## Internet
set protocols static route 0.0.0.0/0 next-hop 10.1.4.13
set protocols static route 0.0.0.0/0 next-hop 10.1.3.14
## DMZ
set protocols static route 192.1.1.0/24 next-hop 10.1.4.13
set protocols static route 192.1.1.0/24 next-hop 10.1.3.14
# vrrp
set high-availability vrrp group LB1Cluster vrid 10
set high-availability vrrp group LB1Cluster interface eth1
set high-availability vrrp group LB1Cluster virtual-address 192.168.100.1/24
set high-availability vrrp sync-group LB1Cluster member LB1Cluster
set high-availability vrrp group LB1Cluster rfc3768-compatibility

# conntrack sinc
set service conntrack-sync accept-protocol 'tcp,udp,icmp'
set service conntrack-sync failover-mechanism vrrp sync-group LB1Cluster
set service conntrack-sync interface eth1
set service conntrack-sync mcast-group 225.0.0.50
set service conntrack-sync disable-external-cache

# load balancing
set load-balancing wan interface-health eth3 nexthop 10.1.3.14
set load-balancing wan interface-health eth2 nexthop 10.1.4.13
set load-balancing wan rule 1 inbound-interface eth0
set load-balancing wan rule 1 interface eth3 weight 1
set load-balancing wan rule 1 interface eth2 weight 1
set load-balancing wan sticky-connections inbound
set load-balancing wan disable-source-nat
commit
save
exit
```

LB2A (Load Balancer)

```
configure
set system host-name LB2A
set interfaces ethernet eth0 address 10.2.0.16/24
set interfaces ethernet eth1 address 10.2.3.16/24
set interfaces ethernet eth2 address 10.2.4.16/24
set interfaces ethernet eth3 address 200.1.1.16/24

# Static routes
## Internet
set protocols static route 0.0.0.0/0 next-hop 200.1.1.10
## Intranet
set protocols static route 192.1.0.0/28 next-hop 10.2.0.13
set protocols static route 192.1.0.0/28 next-hop 10.2.3.14
## DMZ
set protocols static route 192.1.1.0/24 next-hop 10.2.0.13
set protocols static route 192.1.1.0/24 next-hop 10.2.3.14

# vrrp
set high-availability vrrp group LB2Cluster vrid 10
set high-availability vrrp group LB2Cluster interface eth2
set high-availability vrrp group LB2Cluster virtual-address 192.168.100.2/24
set high-availability vrrp sync-group LB2Cluster member LB2Cluster
set high-availability vrrp group LB2Cluster rfc3768-compatibility

# conntrack sync
set service conntrack-sync accept-protocol 'tcp,udp,icmp'
set service conntrack-sync failover-mechanism vrrp sync-group LB2Cluster
set service conntrack-sync interface eth2
set service conntrack-sync mcast-group 225.0.0.50
set service conntrack-sync disable-external-cache

# load balancing
set load-balancing wan interface-health eth0 nexthop 10.2.0.13
set load-balancing wan interface-health eth1 nexthop 10.2.3.14
set load-balancing wan rule 1 inbound-interface eth3
set load-balancing wan rule 1 interface eth0 weight 1
set load-balancing wan rule 1 interface eth1 weight 1
set load-balancing wan sticky-connections inbound
set load-balancing wan disable-source-nat

commit
save
exit
```

LB2B (Load Balancer)

```
configure
set system host-name LB2B
set interfaces ethernet eth0 address 10.2.4.15/24
set interfaces ethernet eth1 address 10.2.1.15/24
set interfaces ethernet eth2 address 10.2.4.15/24
set interfaces ethernet eth3 address 200.1.1.15/24

# Static routes
## Internet
set protocols static route 0.0.0.0/0 next-hop 200.1.1.10
## Intranet
set protocols static route 192.1.0.0/28 next-hop 10.2.4.14
set protocols static route 192.1.0.0/28 next-hop 10.2.1.13
## DMZ
set protocols static route 192.1.1.0/24 next-hop 10.2.4.14
set protocols static route 192.1.1.0/24 next-hop 10.2.1.13
```

```
# vrrp
set high-availability vrrp group LB2Cluster vrid 10
set high-availability vrrp group LB2Cluster interface eth2
set high-availability vrrp group LB2Cluster virtual-address 192.168.100.2/24
set high-availability vrrp sync-group LB2Cluster member LB2Cluster
set high-availability vrrp group LB2Cluster rfc3768-compatibility

# conntrack sync
set service conntrack-sync accept-protocol 'tcp,udp,icmp'
set service conntrack-sync failover-mechanism vrrp sync-group LB2Cluster
set service conntrack-sync interface eth2
set service conntrack-sync mcast-group 225.0.0.50
set service conntrack-sync disable-external-cache

# load balancing
set load-balancing wan interface-health eth0 nexthop 10.2.4.14
set load-balancing wan interface-health eth1 nexthop 10.2.1.13
set load-balancing wan rule 1 inbound-interface eth3
set load-balancing wan rule 1 interface eth0 weight 1
set load-balancing wan rule 1 interface eth1 weight 1
set load-balancing wan sticky-connections inbound
set load-balancing wan disable-source-nat

commit
save
exit
```

FW1 (Firewall)

```
configure
set system host-name FW1
set interfaces ethernet eth0 address 10.2.0.13/24
set interfaces ethernet eth1 address 10.2.1.13/24
set interfaces ethernet eth2 address 10.1.4.13/24
set interfaces ethernet eth3 address 10.1.3.13/24
set interfaces ethernet eth4 address 192.1.1.10/24

# Static routes
## Internet
```

```
set protocols static route 0.0.0.0/0 next-hop 10.2.0.16
## Intranet
set protocols static route 10.2.2.0/24 next-hop 10.1.3.11

# Nat/pat
set nat source rule 10 outbound-interface eth0
set nat source rule 10 source address 10.2.2.0/24
set nat source rule 10 translation address 192.1.0.1-192.1.0.15

# Set Zone Policies
set zone-policy zone INSIDE description "Inside (Internal Network)"
set zone-policy zone INSIDE interface eth2
set zone-policy zone INSIDE interface eth3
set zone-policy zone DMZ description "DMZ"
set zone-policy zone DMZ interface eth4
set zone-policy zone OUTSIDE description "Outside (Internet)"
set zone-policy zone OUTSIDE interface eth0
set zone-policy zone OUTSIDE interface eth1

# Access Control Lists
set firewall name RESTRICTED default-action drop
set firewall name ESTABLISHED default-action drop

# Accept estabelished
set firewall name ESTABLISHED rule 1 description "Accept Established-Related Connections"
set firewall name ESTABLISHED rule 1 action accept
set firewall name ESTABLISHED rule 1 state established enable
set firewall name ESTABLISHED rule 1 state related enable

# HTTP
set firewall name RESTRICTED rule 10 description "Accept HTTP"
set firewall name RESTRICTED rule 10 action accept
set firewall name RESTRICTED rule 10 protocol tcp
set firewall name RESTRICTED rule 10 destination address 0.0.0.0/0
set firewall name RESTRICTED rule 10 destination port 80

# HTTPS
set firewall name RESTRICTED rule 20 description "Accept HTTPS"
set firewall name RESTRICTED rule 20 action accept
set firewall name RESTRICTED rule 20 protocol tcp
set firewall name RESTRICTED rule 20 destination address 0.0.0.0/0
set firewall name RESTRICTED rule 20 destination port 443

# SSH
set firewall name RESTRICTED rule 30 description "Accept SSH"
set firewall name RESTRICTED rule 30 action accept
set firewall name RESTRICTED rule 30 protocol tcp
set firewall name RESTRICTED rule 30 destination address 0.0.0.0/0
set firewall name RESTRICTED rule 30 destination port 22

# DNS
set firewall name RESTRICTED rule 40 description "Accept DNS TCP"
set firewall name RESTRICTED rule 40 action accept
set firewall name RESTRICTED rule 40 protocol tcp
set firewall name RESTRICTED rule 40 destination address 0.0.0.0/0
set firewall name RESTRICTED rule 40 destination port 53

set firewall name RESTRICTED rule 50 description "Accept DNS UDP"
set firewall name RESTRICTED rule 50 action accept
set firewall name RESTRICTED rule 50 protocol udp
set firewall name RESTRICTED rule 50 destination address 0.0.0.0/0
set firewall name RESTRICTED rule 50 destination port 53

# ICMP
set firewall name RESTRICTED rule 60 description "Accept ICMP"
set firewall name RESTRICTED rule 60 action accept
set firewall name RESTRICTED rule 60 protocol icmp
set firewall name RESTRICTED rule 60 destination address 0.0.0.0/0

# BlockList
# set firewall name RESTRICTED rule 70 description "Block IPs"
# set firewall name RESTRICTED rule 70 action drop
# set firewall name RESTRICTED 70 source group address-group ddos_blocklist

# Apply ACLs to Zone Policies
set zone-policy zone DMZ from INSIDE firewall name RESTRICTED
set zone-policy zone DMZ from OUTSIDE firewall name RESTRICTED
set zone-policy zone OUTSIDE from INSIDE firewall name RESTRICTED
set zone-policy zone OUTSIDE from DMZ firewall name ESTABLISHED
set zone-policy zone INSIDE from OUTSIDE firewall name ESTABLISHED
set zone-policy zone INSIDE from DMZ firewall name ESTABLISHED

# Rate limiting
set traffic-policy shaper RATE-LIMIT-10Mbps bandwidth 10mbit
set traffic-policy shaper RATE-LIMIT-10Mbps default bandwidth 100%

set interfaces ethernet eth4 traffic-policy out RATE-LIMIT-10Mbps

commit
save
exit
```

FW2 (Firewall)

```
configure
set system host-name FW2
set interfaces ethernet eth0 address 10.2.4.14/24
set interfaces ethernet eth1 address 10.2.3.14/24
set interfaces ethernet eth2 address 10.1.2.14/24
set interfaces ethernet eth3 address 10.1.3.14/24
set interfaces ethernet eth4 address 192.1.1.20/24

# Static route
## Internet
set protocols static route 0.0.0.0/0 next-hop 10.2.4.15
## Intranet
set protocols static route 10.2.2.0/24 next-hop 10.1.3.12

# Nat/pat
set nat source rule 10 outbound-interface eth0
set nat source rule 10 source address 10.2.2.0/24
set nat source rule 10 translation address 192.1.0.16-192.1.0.31

# Set Zone Policies
set zone-policy zone INSIDE description "Inside (Internal Network)"
set zone-policy zone INSIDE interface eth2
set zone-policy zone INSIDE interface eth3
set zone-policy zone DMZ description "DMZ"
set zone-policy zone DMZ interface eth4
set zone-policy zone OUTSIDE description "Outside (Internet)"
set zone-policy zone OUTSIDE interface eth0
set zone-policy zone OUTSIDE interface eth1

# Access Control Lists
set firewall name RESTRICTED default-action drop
set firewall name ESTABLISHED default-action drop

# Accept estabelished
set firewall name ESTABLISHED rule 1 description "Accept Established-Related Connections"
set firewall name ESTABLISHED rule 1 action accept
set firewall name ESTABLISHED rule 1 state established enable
set firewall name ESTABLISHED rule 1 state related enable

# HTTP
set firewall name RESTRICTED rule 10 description "Accept HTTP"
set firewall name RESTRICTED rule 10 action accept
set firewall name RESTRICTED rule 10 protocol tcp
set firewall name RESTRICTED rule 10 destination address 0.0.0.0/0
set firewall name RESTRICTED rule 10 destination port 80

# HTTPS
set firewall name RESTRICTED rule 20 description "Accept HTTPS"
set firewall name RESTRICTED rule 20 action accept
set firewall name RESTRICTED rule 20 protocol tcp
set firewall name RESTRICTED rule 20 destination address 0.0.0.0/0
set firewall name RESTRICTED rule 20 destination port 443

# SSH
set firewall name RESTRICTED rule 30 description "Accept SSH"
set firewall name RESTRICTED rule 30 action accept
set firewall name RESTRICTED rule 30 protocol tcp
set firewall name RESTRICTED rule 30 destination address 0.0.0.0/0
set firewall name RESTRICTED rule 30 destination port 22

# DNS
set firewall name RESTRICTED rule 40 description "Accept DNS TCP"
set firewall name RESTRICTED rule 40 action accept
set firewall name RESTRICTED rule 40 protocol tcp
set firewall name RESTRICTED rule 40 destination address 0.0.0.0/0
set firewall name RESTRICTED rule 40 destination port 53

set firewall name RESTRICTED rule 50 description "Accept DNS UDP"
set firewall name RESTRICTED rule 50 action accept
set firewall name RESTRICTED rule 50 protocol udp
set firewall name RESTRICTED rule 50 destination address 0.0.0.0/0
set firewall name RESTRICTED rule 50 destination port 53

# ICMP
set firewall name RESTRICTED rule 60 description "Accept ICMP"
set firewall name RESTRICTED rule 60 action accept
set firewall name RESTRICTED rule 60 protocol icmp
set firewall name RESTRICTED rule 60 destination address 0.0.0.0/0

# BlockList
# set firewall name RESTRICTED rule 70 description "Block IPs"
# set firewall name RESTRICTED rule 70 action drop
# set firewall name RESTRICTED 70 source group address-group ddos_blocklist

# Apply ACLs to Zone Policies
set zone-policy zone DMZ from INSIDE firewall name RESTRICTED
set zone-policy zone DMZ from OUTSIDE firewall name RESTRICTED
set zone-policy zone OUTSIDE from INSIDE firewall name RESTRICTED
set zone-policy zone OUTSIDE from DMZ firewall name ESTABLISHED
set zone-policy zone INSIDE from OUTSIDE firewall name ESTABLISHED
set zone-policy zone INSIDE from DMZ firewall name ESTABLISHED

# Rate limiting
set traffic-policy shaper RATE-LIMIT-10Mbps bandwidth 10mbit
set traffic-policy shaper RATE-LIMIT-10Mbps default bandwidth 100%

set interfaces ethernet eth4 traffic-policy out RATE-LIMIT-10Mbps

commit
save
exit
```

Import script

```
#!/bin/bash

# Define the path to the blocklist file and the firewall group name
BLOCKLIST_FILE="/path/to/blocklist.txt"
FIREWALL_GROUP_NAME="ddos_blocklist"

# Configure VyOS to apply the updated rules
sudo vtysh -c "configure terminal"

# Remove the existing firewall group, if it exists
sudo vtysh -c "delete firewall group address-group $FIREWALL_GROUP_NAME"

# Create a new firewall group and add the IP addresses from the blocklist file
while read -r ip; do
  sudo vtysh -c "set firewall group address-group $FIREWALL_GROUP_NAME address $ip"
done < "$BLOCKLIST_FILE"

# Commit and save the changes
sudo vtysh -c "commit"
sudo vtysh -c "save"
sudo vtysh -c "exit"
```