First Report
Load-Balancing Scenario (with redundancy and state synchronization)

Segurança em Redes de Comunicações

Universidade de Aveiro
DETI

Adalberto Jr. Vaz do Rosário, (105589)

Contents

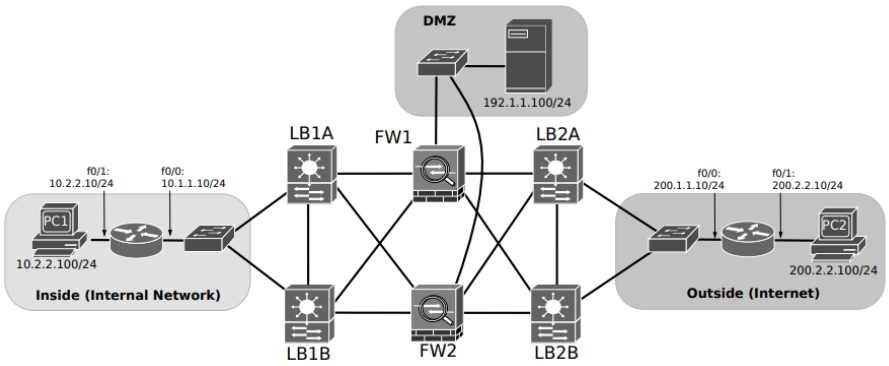

Figure 1: Load-Balancing Scenario (with redundancy and state synchronization)

1 Task 9

1.1 Task 9.a.

Explain why the synchronization of the load-balancers allows the nonexistence of firewall synchronization.

In this scenario, as all traffic has to pass through load-balancers before reaching the firewalls, and as both those that have access to the internal network and those that are connected to the external network are synchronized via VRRP, this allows a "implicit synchronization" between firewalls. This means that in the case of address translation (NAT/PAT) the load-balancers direct traffic to the corresponding firewall that translated the IP, thus overcoming the need for firewalls to synchronize their NAT/PAT translation tables.

1.1.1 Task 9.b

Which load balancing algorithm may also allow the nonexistence of load-balancers synchronization?

IP Hash

In the IP Hash algorithm, load balancers combine the source and destination IP addresses of incoming traffic and using a mathematical function convert this combination into a hash. This hash is used to limit the connection to a specific server, this means that all requests from the same client will always be directed consistently to the same server and traffic will be balanced equally, as there is a consistent hashing function across all the operating systems. servers. And this means there is no need for synchronization.

1.1.2 Task 9.c

Explain why device/connection states synchronization may be detrimental during a DDoS attack.

DDoS attacks overload systems with a massive connection influx. Synchronizing device/connection states adds another layer of processing to already overloaded systems. This can consume valuable resources needed to handle legitimate connections or identify and mitigate the attack itself. Furthermore, there may be potential inconsistency in the network, because it may be difficult for synchronization protocols to keep up with rapid changes, leading to outdated data or inaccurate information about the states of the devices.

2 Task 10

Policies Definition and Integrated Deployment

2.0.1 Topology

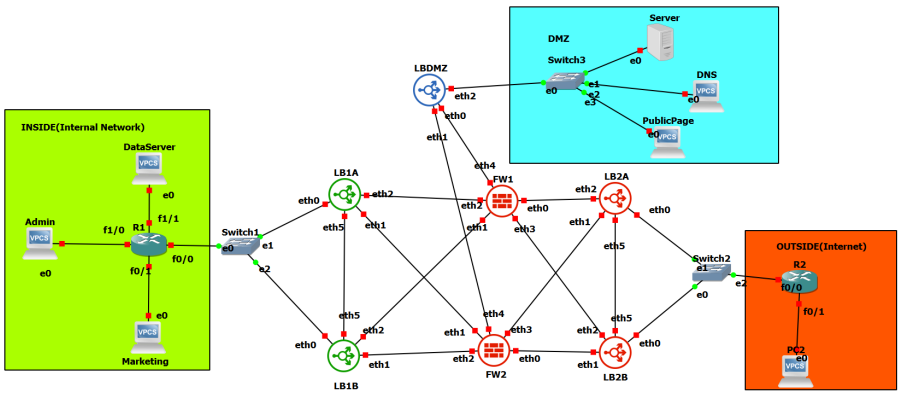

Figure 2: Network Architecture

IPS:

```
Fw1:                  FW2:                  LB1A
eth0: 10.0.3.1/24 | eth0: 10.0.5.1/24 |
eth1: 10.0.2.1/24 | eth1: 10.0.6.1/24 |
eth2: 10.0.1.1/24 | eth2: 10.0.7.1/24 |
eth3: 10.0.4.1/24 | eth3: 10.0.8.1/24 |
eth4: 10.0.9.1/24 | eth4: 10.0.11.1/24|

LB1A:                  LB1B:
eth0: 10.1.1.1/24  | eth0: 10.1.1.2/24
eth1: 10.0.6.10/24 | eth1: 10.0.7.10/24
eth2: 10.0.1.10/24 | eth2: 10.0.2.10/24
eth5: 10.0.0.1/24  | eth5: 10.0.0.2/24

LB2A:                  LB2B:
eth0: 200.1.1.1/24 | eth0: 200.1.1.2/24
eth1: 10.0.8.10/24 | eth1: 10.0.5.10/24
eth2: 10.0.3.10/24 | eth2: 10.0.4.10/24
eth5: 10.0.10.1/24 | eth5: 10.0.10.2/24
LBDMZ:                     R2:
eth0: 10.0.9.2/24   | F0/0: 200.1.1.10/24
eth1: 10.0.11.2/24  | F0/1: 200.2.2.10/24
eth2: 192.1.1.10/24 |

R1:
F0/0: 10.1.1.10/24
F0/1: 10.2.2.10/24
F1/0: 10.3.3.10/24
F1/1: 10.4.4.10/24

Marketing: 10.2.2.100/24  | Admin: 10.3.3.5/24
Desing: 10.4.4.100/24     | PC2: 200.2.2.100/24
PC3: 192.1.1.101/24       | Sever: 192.1.1.100/24
Public Page: 192.1.1.150/24
```

The network is made up of three zones: INSIDE, OUTSIDE and DMZ. In the INSIDE zone (internal network), there are 3 subnets. The 10.2.2.0/24 network, which I called Marketing Network, which contains a VPCS with IP address 10.2.2.100, the 10.3.3.0/24 network, which I called Admin Network, contains a VPCS with IP 10.3.3.5 and the Network 10.4.4.0/24, called the Data Server Network, contains a VPCS with the IP address 10.4.4.100. The remaining IPs in the 10.0.0.0/8 network are assigned to the remaining company terminals.

The OUTSIDE(Internet) zone consists of the 200.2.2.0/24 subnet with a VPCS to simulate an external device.

Finally, the DMZ zone includes the subnet 192.1.1.0/24 with three IP addresses, being: 192.1.1.100 which is the IP of the (DMZ)Server and is only accessible internally, 192.1.1.150 server of the company's public page and o 192.1.1.200 which will simulate a DNS server.

2.1 Configurations (The relevant points)

2.1.1 INSIDE and OUTSIDE

On the internal router (R1) I defined static routes for LB1A and LB1B, while on the external router (R2) I configured static routes for LB2A and LB2B.

2.1.2 Load Balancers (LBs)

All LBs, with the exception of LBDMZ, have conntrack-sync configured on eth5, and load balancing on their eth1 and eth2 interfaces with equal weights, this means that the probability of forwarding a packet to an interface is 50%. In LB1 I created static routes forwarding the internal department networks to the Inside router interface and in LB2 there is a static route directing traffic to the 200.2.2.0/24 network through the Outside router.

2.1.3 Firewall (FW)

For the Firewalls (FWs), I configured static routes from INSIDE to OUTSIDE and from OUTSIDE to INSIDE. Traffic destined for the 10.0.0.0/8 network is routed through the near hops connected to the eth1 and eth2 interfaces, while traffic destined for the 200.2.2.0/24 network is routed through the near hops connected to the eth0 and eth3 interfaces. I also activated the SSH service on port 22, giving access control to the standard user (vyos) and only devices connected to the eth4 interface can access it through SSH. (For extra part) The NAT pool between FWs is the same, using a pool that ranges from 192.168.1.0 to 192.168.1.10.

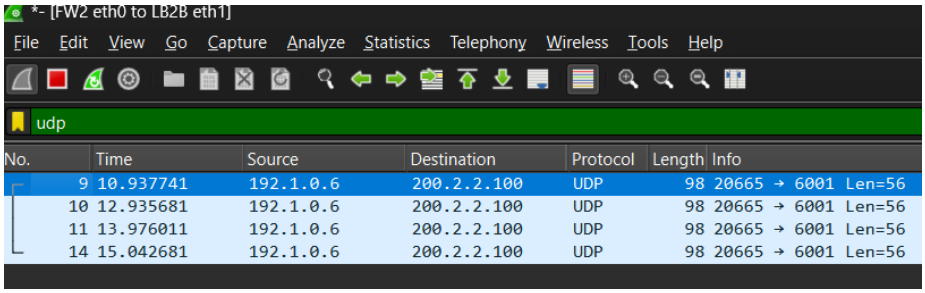

Figure 3: NAT Translations

2.2 Policies (Services)

Define some services for networks. The Inside network can only communicate with the Outside network using UDP on ports 6000 to 7000. The Outside cannot initiate communication with the Inside. It can be confirmed in the figure 4

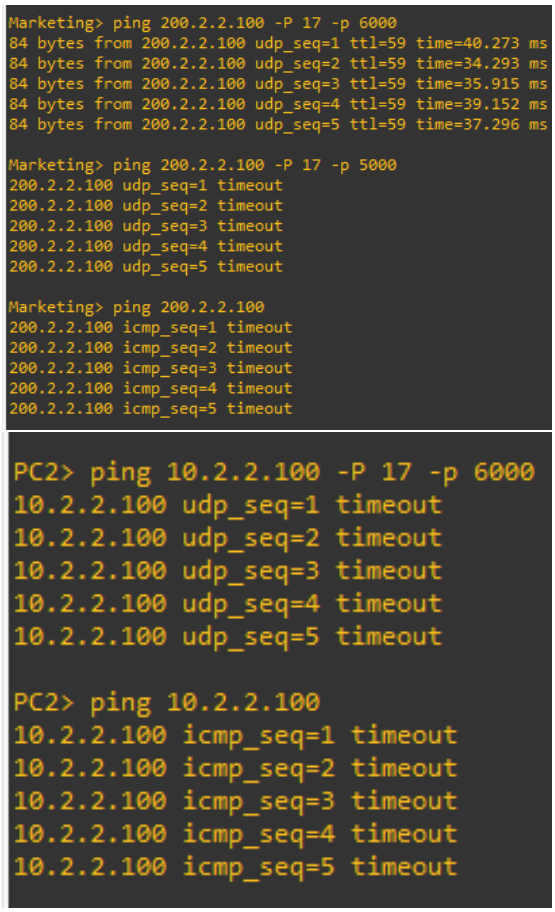

Figure 4: Rules of INSIDE to OUTSIDE communication.

Another service was Inside's access to the DMZ. All internal devices can ping devices on the DMZ network, communicate via UDP on port 53 (to simulate DNS communication) and also communicate via TCP on ports 80 and 443, allowing them to access web services via HTTP and HTTPS. See figure 5.

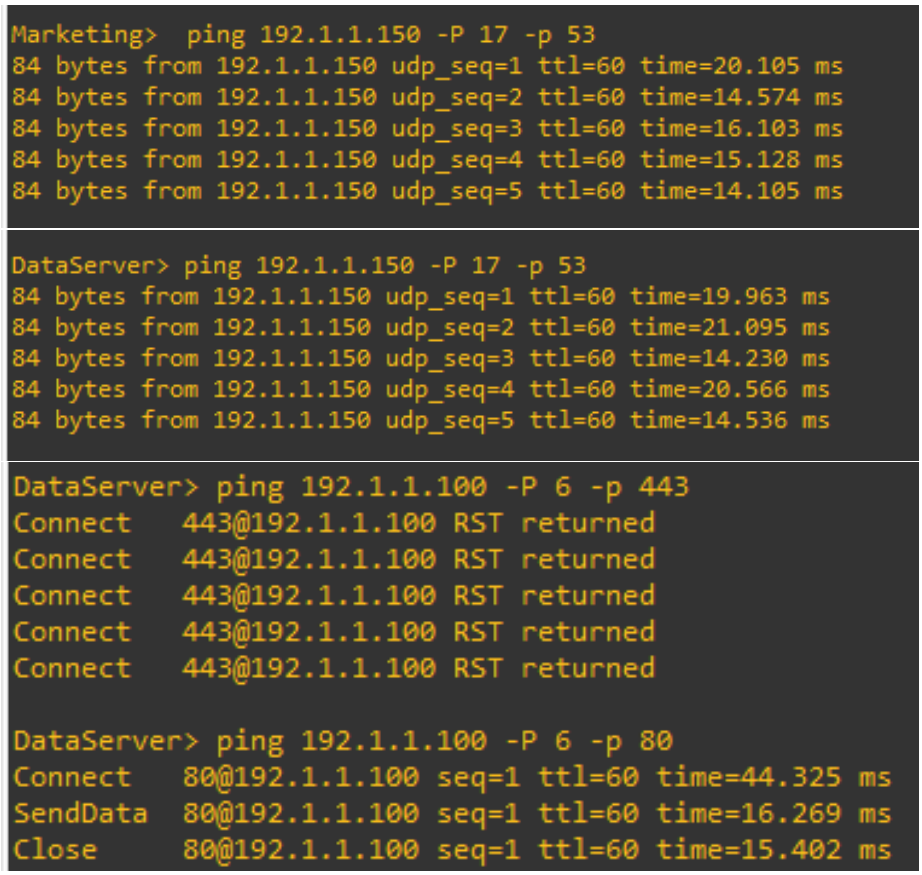

Figure 5: Communication on port 53, 80 and 443.

Furthermore, only the administrative network (10.3.3.0/24), for now only IP 10.3.3.5/24 can communicate with the DMZ through TCP on port 22, which means that only administrators can establish SSH connections with those inside the DMZ terminals.

For some reason the service on port 22 is not working, even configured in the firewall, see the attachment 4, it always gives a timeout and in the capture it says that "A new tcp session is started with the same ports as a previous session in this trace". See the figure 6

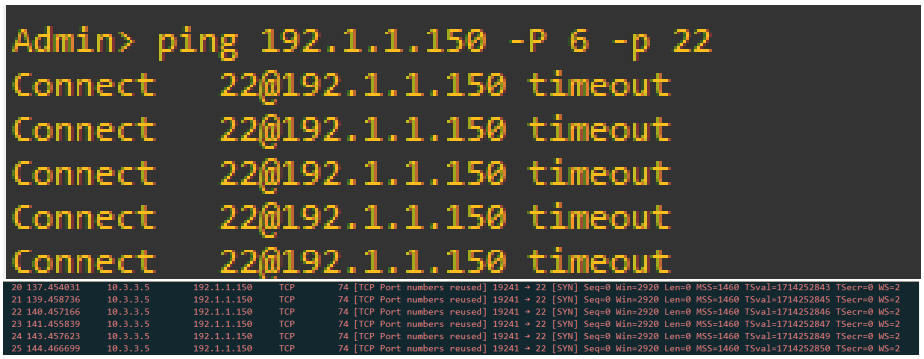

Figure 6: Communication on port 22 by the Admin

Only the Data Server network (10.4.4.0/24) can communicate with the DMZ via TCP on port 21,57 and 587 to simulate FTP, MTP and SMTP services respectively and via UDP on port 18 to simulate SMP(Message Send Protocol). Figure 7

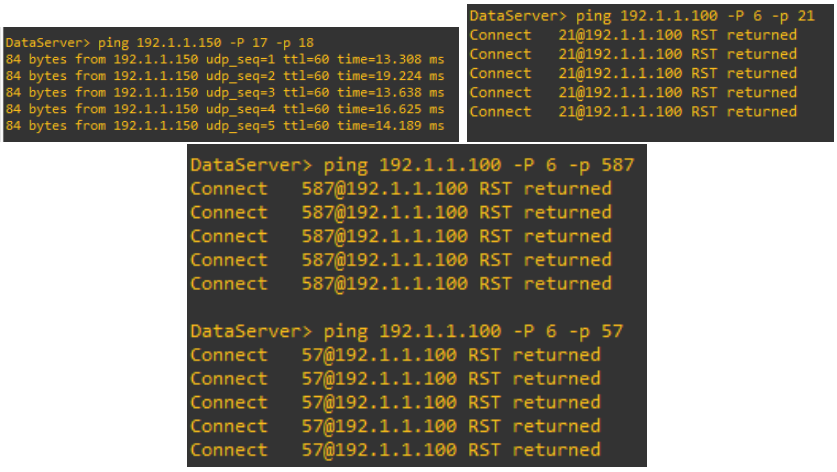

Figure 7: Communication on port 18,21,57 and 587

I noticed that some ports do not work on all VPCS even though they have permission and most pings on these ports only work when done to the virtual machine's PC (192.1.1.100).

Maybe it's package formatting issues. See figure 8

331	2406.195890	10.4.4.100	192.1.1.150	DNS	98 Unknown operation (15) 0x0050[Malformed Packet]
332	2406.196965	192.1.1.150	10.4.4.100	DNS	98 Unknown operation (15) 0x0050[Malformed Packet]
333	2411.338842	10.4.4.100	192.1.1.150	DNS	98 Unknown operation (15) 0x0050[Malformed Packet]
334	2411.338842	192.1.1.150	10.4.4.100	DNS	98 Unknown operation (15) 0x0050[Malformed Packet]
335	2412.361555	10.4.4.100	192.1.1.150	DNS	98 Unknown operation (15) 0x0050[Malformed Packet]
336	2412.362563	192.1.1.150	10.4.4.100	DNS	98 Unknown operation (15) 0x0050[Malformed Packet]
337	2413.377697	10.4.4.100	192.1.1.150	DNS	98 Unknown operation (15) 0x0050[Malformed Packet]
338	2413.377697	192.1.1.150	10.4.4.100	DNS	98 Unknown operation (15) 0x0050[Malformed Packet]
339	2414.399787	10.4.4.100	192.1.1.150	DNS	98 Unknown operation (15) 0x0050[Malformed Packet]
340	2414.399787	192.1.1.150	10.4.4.100	DNS	98 Unknown operation (15) 0x0050[Malformed Packet]
341	2415.415001	10.4.4.100	192.1.1.150	DNS	98 Unknown operation (15) 0x0050[Malformed Packet]
342	2415.415001	192.1.1.150	10.4.4.100	DNS	98 Unknown operation (15) 0x0050[Malformed Packet]

Figure 8: Capture of packets with false negatives

For the OUTSIDE network, I defined a service in which devices can only communicate with the IP address 192.1.1.150 (public page). The allowed communication methods are through pings or via TCP on port 443, which allows access via HTTPS. See figure 9.

```
PC2> ping 192.1.1.150
84 bytes from 192.1.1.150 icmp_seq=1 ttl=60 time=19.502 ms
84 bytes from 192.1.1.150 icmp_seq=2 ttl=60 time=37.041 ms
84 bytes from 192.1.1.150 icmp_seq=3 ttl=60 time=13.659 ms
84 bytes from 192.1.1.150 icmp_seq=4 ttl=60 time=14.158 ms
84 bytes from 192.1.1.150 icmp_seq=5 ttl=60 time=11.770 ms

PC2> ping 192.1.1.150 -P 6 -p 443
Connect   443@192.1.1.150 timeout
Connect   443@192.1.1.150 timeout
Connect   443@192.1.1.150 timeout
Connect   443@192.1.1.150 timeout
Connect   443@192.1.1.150 timeout
```

```
PC2> ping 192.1.1.100
192.1.1.100 icmp_seq=1 timeout
192.1.1.100 icmp_seq=2 timeout
192.1.1.100 icmp_seq=3 timeout
192.1.1.100 icmp_seq=4 timeout
192.1.1.100 icmp_seq=5 timeout
```

Figure 9: Communication from Outsite to DMZ(only with the public page)

Communication from Outside to DMZ via TCP on port 443 should work but for some reason it doesn't. I was unable to understand the reason for the non-operation.

The DMZ is not allowed to initiate communication, neither to Inside nor to Outside.

3 conclusion

During the project I came across some problems that I had not been able to resolve until then. For some reason, after closing gns3, the vyos become inaccessible in virtualbox, and I can't open the project again. I can only open the project if I create the machines again with my project names and consequently, I lose the data. For some reason services implemented via ports do not work and those that work are those made for a virtual machine and not for VPCS. To carry out the project, I used the group's report (André Clérigo (98485), Pedro Rocha (98256)) students from the previous year as a basis. I used some configurations they used, added some and also updated some that didn't make sense for my network.

4 Attachment

4.1 Firewall

4.1.1 FW1

```
configure

set system host-name FW1

set interfaces ethernet eth0 address 10.0.3.1/24
set interfaces ethernet eth1 address 10.0.2.1/24
set interfaces ethernet eth2 address 10.0.1.1/24
set interfaces ethernet eth3 address 10.0.4.1/24
set interfaces ethernet eth4 address 10.0.9.1/24

set nat source rule 10 outbound-interface eth0
set nat source rule 10 source address 10.0.0.0/8
set nat source rule 10 translation address
    192.1.0.1-192.1.0.10

set nat source rule 20 outbound-interface eth3
set nat source rule 20 source address 10.0.0.0/8
set nat source rule 20 translation address
    192.1.0.1-192.1.0.10

set protocols static route 0.0.0.0/0 next-hop
    10.0.3.10
set protocols static route 0.0.0.0/0 next-hop
    10.0.4.10
set protocols static route 10.2.2.0/24 next-hop
    10.0.1.10
set protocols static route 10.2.2.0/24 next-hop
    10.0.2.10
set protocols static route 10.3.3.0/24 next-hop
    10.0.1.10
set protocols static route 10.3.3.0/24 next-hop
    10.0.2.10
set protocols static route 10.4.4.0/24 next-hop
    10.0.1.10
set protocols static route 10.4.4.0/24 next-hop
    10.0.2.10
set protocols static route 192.1.1.0/24 next-hop
    10.0.9.2

set service ssh access-control allow user vyos
```

```
set service ssh listen-address 10.0.9.1
set service ssh port 22

set firewall name FROM-DMZ-TO-INSIDE rule 10 action
    accept
set firewall name FROM-DMZ-TO-INSIDE rule 10
    description "Accept Established-related connections
    "
set firewall name FROM-DMZ-TO-INSIDE rule 10 state
    established enable
set firewall name FROM-DMZ-TO-INSIDE rule 10 state
    related enable
set firewall name FROM-DMZ-TO-OUTSIDE rule 10 action
    accept
set firewall name FROM-DMZ-TO-OUTSIDE rule 10
    description "Accept Established-related connections
    "
set firewall name FROM-DMZ-TO-OUTSIDE rule 10 state
    established enable
set firewall name FROM-DMZ-TO-OUTSIDE rule 10 state
    related enable
set firewall name FROM-INSIDE-TO-DMZ rule 10 action
    accept
set firewall name FROM-INSIDE-TO-DMZ rule 10
    description "Accept ICMP Echo Request to DMZ"
set firewall name FROM-INSIDE-TO-DMZ rule 10
    destination address 192.1.1.0/24
set firewall name FROM-INSIDE-TO-DMZ rule 10 icmp type
     8
set firewall name FROM-INSIDE-TO-DMZ rule 10 protocol
    icmp
set firewall name FROM-INSIDE-TO-DMZ rule 20 action
    accept
set firewall name FROM-INSIDE-TO-DMZ rule 20
    description "Accept HTTP, HTTPS and SSH from Admin
    to DMZ"
set firewall name FROM-INSIDE-TO-DMZ rule 20
    destination address 192.1.1.0/24
set firewall name FROM-INSIDE-TO-DMZ rule 20
    destination port 22,80,443
set firewall name FROM-INSIDE-TO-DMZ rule 20 protocol
    tcp
set firewall name FROM-INSIDE-TO-DMZ rule 20 source
    address 10.3.3.5/24
set firewall name FROM-INSIDE-TO-DMZ rule 20 action
    accept
```

```
set firewall name FROM-INSIDE-TO-DMZ rule 20
   description "Accept HTTP and HTTPS from Inside to
   DMZ"
set firewall name FROM-INSIDE-TO-DMZ rule 20
   destination address 192.1.1.0/24
set firewall name FROM-INSIDE-TO-DMZ rule 20
   destination port 80,443
set firewall name FROM-INSIDE-TO-DMZ rule 20 protocol
   tcp
set firewall name FROM-INSIDE-TO-DMZ rule 20 source
   address 10.2.2.0/24
set firewall name FROM-INSIDE-TO-DMZ rule 20 source
   address 10.4.4.0/24
set firewall name FROM-INSIDE-TO-DMZ rule 30 action
   accept
set firewall name FROM-INSIDE-TO-DMZ rule 30
   description "Allow DNS access to DMZ"
set firewall name FROM-INSIDE-TO-DMZ rule 30
   destination address 192.1.1.0/24
set firewall name FROM-INSIDE-TO-DMZ rule 30
   destination port 53
set firewall name FROM-INSIDE-TO-DMZ rule 30 protocol
   udp
set firewall name FROM-INSIDE-TO-DMZ rule 40 action
   accept
set firewall name FROM-INSIDE-TO-DMZ rule 40
   description "Accept FTP, MTP and SMTP from Data
   Server to DMZ"
set firewall name FROM-INSIDE-TO-DMZ rule 40
   destination address 192.1.1.0/24
set firewall name FROM-INSIDE-TO-DMZ rule 40
   destination port 21,57,587
set firewall name FROM-INSIDE-TO-DMZ rule 40 protocol
   tcp
set firewall name FROM-INSIDE-TO-DMZ rule 40 source
   address 10.4.4.100/32
set firewall name FROM-INSIDE-TO-DMZ rule 41 action
   accept
set firewall name FROM-INSIDE-TO-DMZ rule 41
   description "Accept SMP(Message Send Protocol) from
    Data Server to DMZ"
set firewall name FROM-INSIDE-TO-DMZ rule 41
   destination address 192.1.1.0/24
set firewall name FROM-INSIDE-TO-DMZ rule 41
   destination port 18
```

```
set firewall name FROM-INSIDE-TO-DMZ rule 41 protocol
   udp
set firewall name FROM-INSIDE-TO-DMZ rule 41 source
   address 10.4.4.100/32
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10
   action accept
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10
   description "Accept UDP from ports 6000-7000"
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10
   destination port 6000-7000
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10
   protocol udp
set firewall name FROM-OUTSIDE-TO-DMZ rule 10 action
   accept
set firewall name FROM-OUTSIDE-TO-DMZ rule 10
   description "Accept ICMP Echo Request to DMZ Public
    Page"
set firewall name FROM-OUTSIDE-TO-DMZ rule 10
   destination address 192.1.1.150/32
set firewall name FROM-OUTSIDE-TO-DMZ rule 10 icmp
   type 8
set firewall name FROM-OUTSIDE-TO-DMZ rule 10 protocol
    icmp
set firewall name FROM-OUTSIDE-TO-DMZ rule 20 action
   accept
set firewall name FROM-OUTSIDE-TO-DMZ rule 20
   description "Accept HTTPS to Public Page"
set firewall name FROM-OUTSIDE-TO-DMZ rule 20
   destination address 192.1.1.150/32
set firewall name FROM-OUTSIDE-TO-DMZ rule 20
   destination port 443
set firewall name FROM-OUTSIDE-TO-DMZ rule 20 protocol
    tcp
set firewall name FROM-OUTSIDE-TO-DMZ rule 30 action
   accept
set firewall name FROM-OUTSIDE-TO-DMZ rule 30
   description "Accept SMTP to Public Page"
set firewall name FROM-OUTSIDE-TO-DMZ rule 30
   destination address 192.1.1.150/32
set firewall name FROM-OUTSIDE-TO-DMZ rule 30
   destination port 465
set firewall name FROM-OUTSIDE-TO-DMZ rule 30 protocol
    tcp
set firewall name FROM-OUTSIDE-TO-INSIDE rule 10
   action accept
```

```
set firewall name FROM-OUTSIDE-TO-INSIDE rule 10
   description "Accept Established-related connections
   "
set firewall name FROM-OUTSIDE-TO-INSIDE rule 10 state
    established enable
set firewall name FROM-OUTSIDE-TO-INSIDE rule 10 state
    related enable

set zone-policy zone INSIDE description "Inside (
   Internal Network)"
set zone-policy zone INSIDE interface eth1
set zone-policy zone INSIDE interface eth2
set zone-policy zone DMZ description "DMZ (Server Farm
   )"
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 eth3
set zone-policy zone INSIDE from DMZ firewall name
   FROM-DMZ-TO-INSIDE
set zone-policy zone INSIDE from OUTSIDE firewall name
    FROM-OUTSIDE-TO-INSIDE
set zone-policy zone DMZ from INSIDE firewall name
   FROM-INSIDE-TO-DMZ
set zone-policy zone DMZ from OUTSIDE firewall name
   FROM-OUTSIDE-TO-DMZ
set zone-policy zone OUTSIDE from DMZ firewall name
   FROM-DMZ-TO-OUTSIDE
set zone-policy zone OUTSIDE from INSIDE firewall name
    FROM-INSIDE-TO-OUTSIDE
```

The firewall configurations are similar, only the IPs differ, with the same policies and zones.

4.2 Load Balancers

4.2.1 LB1A

```
configure
set system host-name LB1A
set interfaces ethernet eth0 address 10.1.1.1/24
set interfaces ethernet eth1 address 10.0.6.10/24
set interfaces ethernet eth2 address 10.0.1.10/24
set interfaces ethernet eth5 address 10.0.0.1/24
set protocols static route 10.2.2.0/24 next-hop
    10.1.1.10
set protocols static route 10.3.3.0/24 next-hop
    10.1.1.10
set protocols static route 10.4.4.0/24 next-hop
    10.1.1.10
set load-balancing wan interface-health eth1 nexthop
    10.0.6.1
set load-balancing wan interface-health eth2 nexthop
    10.0.1.1
set load-balancing wan rule 1 inbound-interface eth0
set load-balancing wan rule 1 interface eth1 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
set high-availability vrrp group LB1Cluster vrid 1
set high-availability vrrp group LB1Cluster interface
    eth5
set high-availability vrrp group LB1Cluster virtual-
    address 10.0.0.1/24
set high-availability vrrp sync-group LB1Cluster
    member LB1Cluster
set high-availability vrrp group LB1Cluster rfc3768-
    compatibility
set service conntrack-sync accept-protocol 'tcp,udp,
    icmp'
set service conntrack-sync failover-mechanism vrrp
    sync-group LB1Cluster
set service conntrack-sync interface eth5
set service conntrack-sync mcast-group 225.0.0.50
set service conntrack-sync disable-external-cache
commit
save
```

The Load Balancers configurations are similar, only the IPs differ.

4.2.2 LBDMZ

```
configure

set system host-name LBDMZ

set interfaces ethernet eth0 address 10.0.9.2/24
set interfaces ethernet eth1 address 10.0.11.2/24
set interfaces ethernet eth2 address 192.1.1.10/24

set load-balancing wan disable-source-nat
set load-balancing wan interface-health eth0 nexthop
   10.0.9.1
set load-balancing wan interface-health eth1 nexthop
   10.0.11.1
set load-balancing wan rule 1 inbound-interface eth2
set load-balancing wan rule 1 interface eth0 weight 1
set load-balancing wan rule 1 interface eth1 weight 1
set load-balancing wan rule 1 protocol all
set load-balancing wan sticky-connections inbound
commit
save
```