Universidade de Aveiro
Mestrado em Cibersegurança
Código: 41782 - Segurança em Redes de Comunicações
Responsible: Paulo Jorge Salvador Serra Ferreira

Report 1

Monday 8th April, 2024
Ricardo Covelo (102668) - Telmo Sauce (104428)

Contents

1 Exercice 9

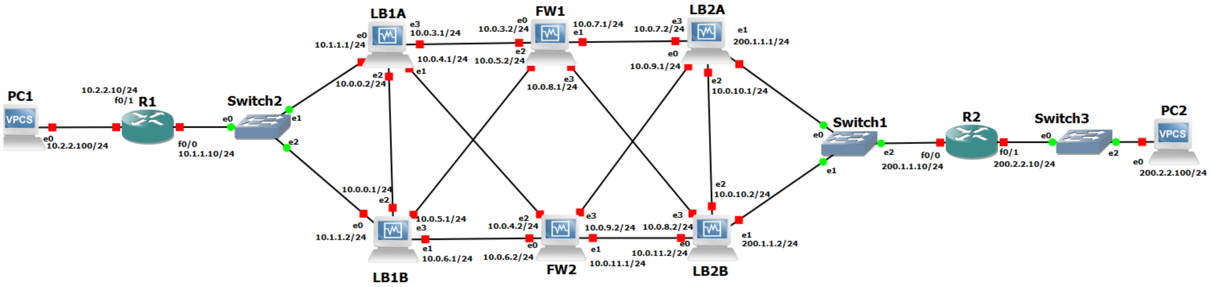

Figure 1: Network

1.1 Q1 - Explain why the synchronization of the load-balancers allows the nonexistence of a firewall synchronization.

The nonexistence of firewall synchronization is due to the lack of need for both firewalls to have the same NAT/PAT table since every pair request/response will be routed through the same Firewall. This is possible due to the sticky connections that ensure that the response packet is sent to the same Firewall that was sent from. The Synchronization of the load balancers makes it so the table with the Packet-Firewall table would be shared between both load balancers and even if a response packet ends up on a different load balancer it would end up on the same Firewall.

1.2 Q2 - Which load-balancing algorithm may also allow the nonexistence of load-balancer synchronization?

The algorithm that would be useful so that we wouldn't have to set up Load-balancer synchronization is IP Hash since the IP of the client will be the only selecting factor on where the packet will be sent.

1.3 Q3 - Explain why device/connection states synchronization may be detrimental during a DDoS attack.

With a DDOS attack, an attacker floods the network with a very high number of packets, this may lead to the overload of the Load-Balancers because of the additional need for synchronization of all those new packets and the overload of the communication channel they use to synchronize all those new packets.

2 Exercice 10

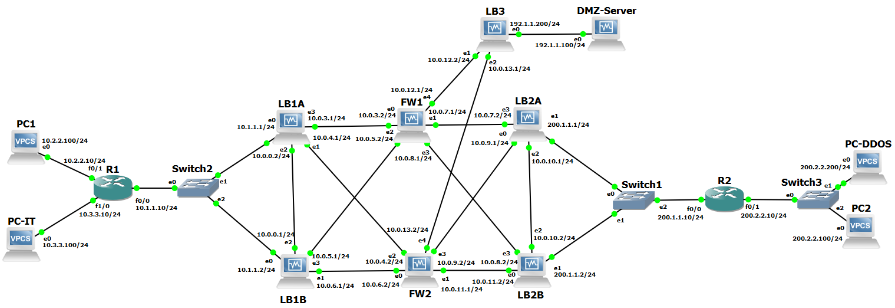

Figure 2: Network

2.1 Policies

2.1.1 Good Practice

Several good practices can be applied to our network to make it more resilient and secure:

- Restric access to IP addresses that:
  - Comes from outside with an IP Address of our public IP address pool.
  - Comes from inside with an IP address that isn't part of our private IP address pool.
  - Comes from outside with an IP address of our private IP address pool.
- By **default** no protocol should be allowed.
- Restric communications that are started from the outside and trying to communicate with our internal network.
- Restric communications from the DMZ to other zones.
- Allow only SSH to all PCs to users that need them, for example only IT personnel.
- Allow HTTP and HTTPS to all users from the INSIDE zone and only to a specific machine.
- Allow DNS from Inside the Network.
- Allow HTTPS to all users from the OUTSIDE zone and only to a specific machine.
- Implement redundancy for communication, especially in critical communications (In our case for example the synchronization of the LB, because if they don't sync properly the whole network may stop functioning)
- Compartmentalize with the help of Vlans or DMZ's

- Only allow ports that are necessary to the scope, unnecessary ports may be used by an attacker.

2.1.2 Preventing DDOS

- Implementing a mechanism of detecting a continuous high flow of packets to the internal network and then blocking such IP.
- Define a maximum amount of pings per minute and block every IP that goes above that threshold such as shown on 3

```
# set firewall name <name> rule <1-999999> recent count <1-255>
# set firewall ipv6-name <name> rule <1-999999> recent count <1-255>
# set firewall name <name> rule <1-999999> recent time <second | minute | hour>
# set firewall ipv6-name <name> rule <1-999999> recent time <second | minute | hour>
```

Match when 'count' amount of connections are seen within 'time'. These matching criteria can be used to block brute-force attempts.

Figure 3: Command to block brute-force attempts

3 Implementaion

The full implementation of the devices can be found at High-Avaliability-Network.

3.1 Load-Balancing

We configured all the Load-Balancer similarly just adjusting the interfaces and the IP addresses maintaining the weight of the connections keeping sticky connections and disabling source-nat, this is an example of how it is configured in LB1A

```
set load-balancing wan interface-health eth1 nexthop
10.0.3.2
set load-balancing wan interface-health eth3 nexthop
10.0.4.2
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 eth3 weight 1
set load-balancing wan sticky-connections inbound
set load-balancing wan disable-source-nat
```

Figure 4: LB1A Configuration

To show this working we pinged from PC1-PC2 and (as these pings go always to LB1A) set a Wireshark capture between LB1A and both firewalls. As seen below 3 packets went through FW1 and the rest to FW2.

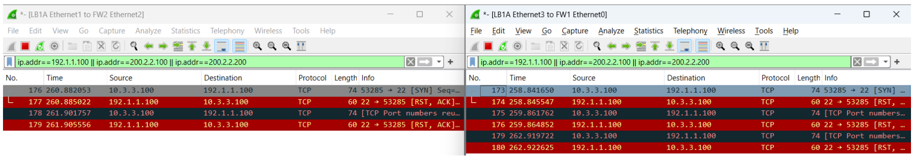

Figure 5: Capture between LB1A and firewalls

We needed to introduce a third load balancer within the DMZ. The reason behind this addition was that the packets arriving from the DMZ, routed through a router, were being directed to a firewall that was not initiating the requests. Consequently, this firewall could not determine the appropriate destination for the responses. To address this, we deployed the load balancer to consistently route the replies back to the firewall that made the request.

3.2 Synchronization

As we can see on the following figures there is a synchronization between the Load balancers.

```
set high-availability vrrp group LBCluster vrid 10
set high-availability vrrp group LBCluster interface eth2
set high-availability vrrp group LBCluster virtual-address 192.168.100.1/24
set high-availability vrrp sync-group LBCluster member LBCluster
set high-availability vrrp group LBCluster rfc3768-compatibility

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

Figure 6: Syncronization conf

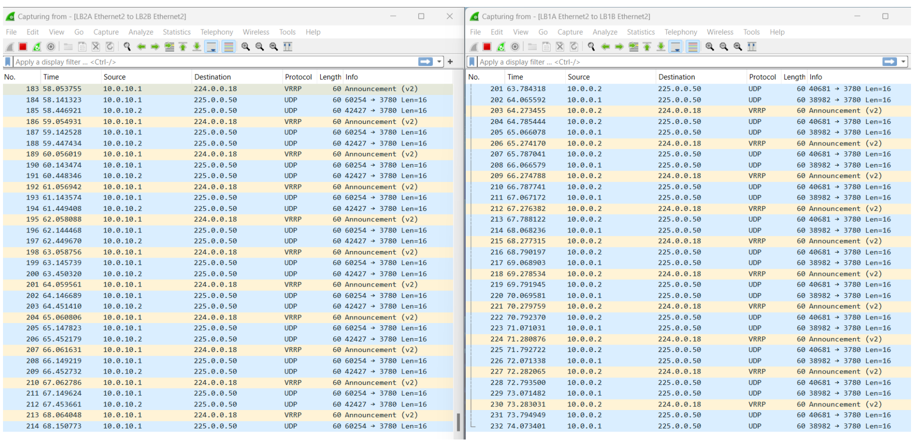

Figure 7: Packets Passing between LB

3.3 NAT

Our NAT translation is being done separately on both firewalls, each having a distinct table and different public IP address pool (FW1: 192.1.0.1-192.1.0.10, FW2:192.1.0.11-192.1.0.20) so it is easier to debug.

```
set nat source rule 10 outbound-interface eth3
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 eth1
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
```

Figure 8: Nat config for FW2

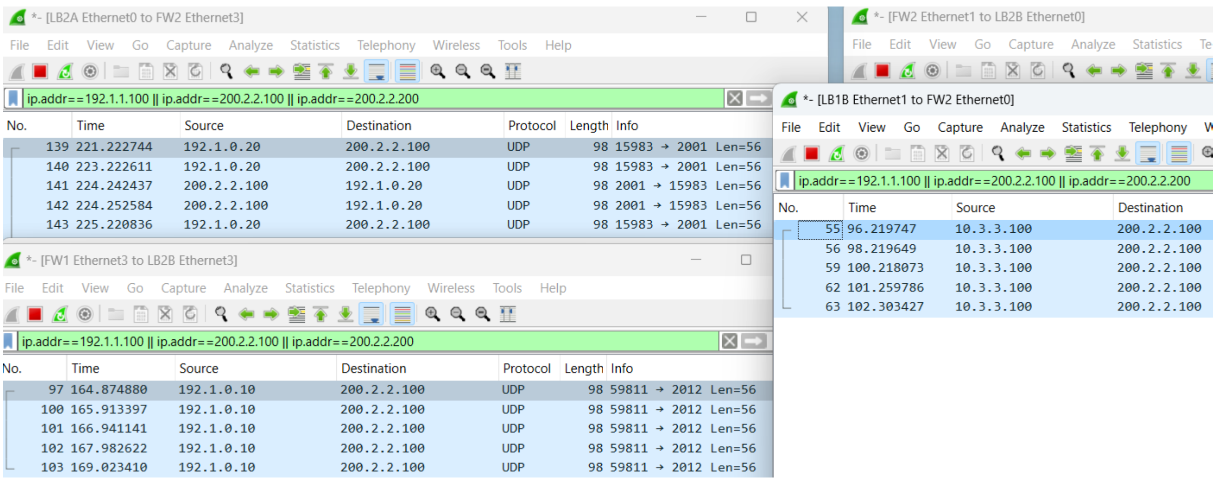

Figure 9: NAT traduction example

3.4 Firewall policies

The firewall is equipped with several policies to prevent attacks such as DDOS attacks and unauthorized access. By default, it drops all traffic and only allows what has been explicitly implemented and approved.

```
set zone-policy zone INSIDE description "Inside (Internal Network)"
set zone-policy zone INSIDE interface eth0
set zone-policy zone INSIDE interface eth2
set zone-policy zone INSIDE default-action drop
set zone-policy zone OUTSIDE description "Outside (Internet)"
set zone-policy zone OUTSIDE default-action drop
set zone-policy zone OUTSIDE interface eth1
set zone-policy zone OUTSIDE interface eth3
set zone-policy zone DMZ description "DMZ (Server Farm)"
set zone-policy zone DMZ interface eth4
set zone-policy zone DMZ default-action drop
```

Figure 10: Drop Packets Config

DDOS

With the expectation that some external mechanism to prevent DDOS would give us the IP 200.2.2.200 to block we blocked it in both firewalls.

```
set firewall group address-group BLOCKED_IPS address 200.2.2.200
set firewall name FROM-OUTSIDE-TO-DMZ rule 10 action drop
set firewall name FROM-OUTSIDE-TO-DMZ rule 10 protocol all
set firewall name FROM-OUTSIDE-TO-DMZ rule 10 source group address-group 'BLOCKED_IPS'
```

Figure 11: Blocking Ip

DMZ

The DMZ is unable to ping any device however if a device tries to ping it can respond either to the Inside or outside of the network. The DMZ contains only one device that other devices from different networks can ping which is 192.1.1.100/24. We considered that this device has the DNS and website of the enterprise.

```
set firewall name FROM-DMZ-TO-OUTSIDE rule 10 description "Accept Established-Related Connections"
set firewall name FROM-DMZ-TO-OUTSIDE rule 10 action accept
set firewall name FROM-DMZ-TO-OUTSIDE rule 10 state established enable
set firewall name FROM-DMZ-TO-OUTSIDE rule 10 state related enable
```

Figure 12: DMZ Config

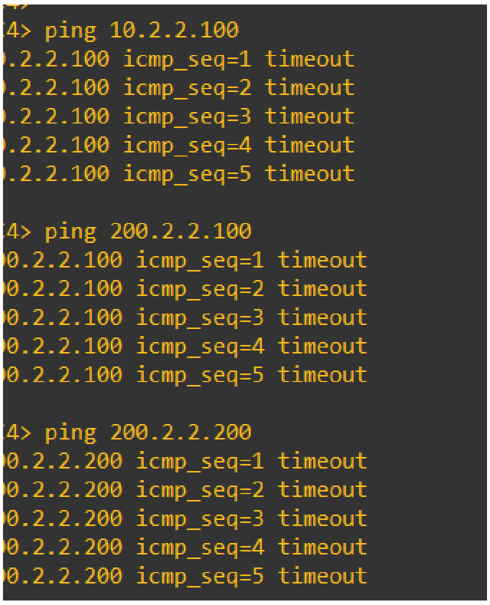

Figure 13: Failled pings

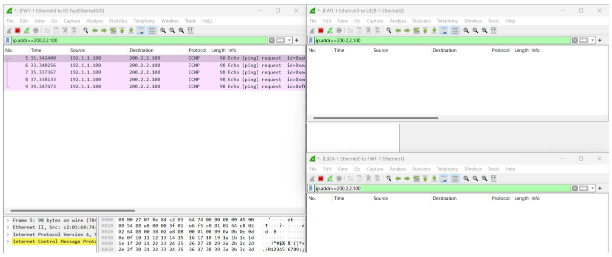

Figure 14: Ping doesn't go through the FW1

Inside

The inside of the network can ping the device 192.1.1.100 on the DMZ or the Outside, however no device outside of it can connect to it. As stated previously some policies were implemented. The IT personnel(10.3.3.0/24) can connect via SSH to the DMZ and finally, all users located on the Inside can connect to the DMZ with HTTP, HTTPS, and DNS.

```
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 description "Accept UDP Echo Request"
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 action accept
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 protocol udp
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 destination port 2000-4000

set firewall name TO-INSIDE rule 10 description "Accept Established-Related Connections"
set firewall name TO-INSIDE rule 10 action accept
set firewall name TO-INSIDE rule 10 state established enable
set firewall name TO-INSIDE rule 10 state related enable

set firewall name FROM-INSIDE-TO-DMZ rule 10 description "Accept UDP Echo Request"
set firewall name FROM-INSIDE-TO-DMZ rule 10 action accept
set firewall name FROM-INSIDE-TO-DMZ rule 10 protocol udp
set firewall name FROM-INSIDE-TO-DMZ rule 10 destination port 2000-4000
set firewall name FROM-INSIDE-TO-DMZ rule 10 destination address 192.1.1.0/24

set firewall name FROM-INSIDE-TO-DMZ rule 20 description "Accept SSH from IT Personel Only"
set firewall name FROM-INSIDE-TO-DMZ rule 20 action accept
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
set firewall name FROM-INSIDE-TO-DMZ rule 20 protocol tcp
set firewall name FROM-INSIDE-TO-DMZ rule 20 source address 10.3.3.0/24


set firewall name FROM-INSIDE-TO-DMZ rule 30 description "Accept DNS access"
set firewall name FROM-INSIDE-TO-DMZ rule 30 action accept
set firewall name FROM-INSIDE-TO-DMZ rule 30 destination address 192.1.1.100/24
set firewall name FROM-INSIDE-TO-DMZ rule 30 destination port 53
set firewall name FROM-INSIDE-TO-DMZ rule 30 protocol tcp_udp

set firewall name FROM-INSIDE-TO-DMZ rule 40 description "Accept HTTP, HTTPS"
set firewall name FROM-INSIDE-TO-DMZ rule 40 action accept
set firewall name FROM-INSIDE-TO-DMZ rule 40 destination address 192.1.1.100/24
set firewall name FROM-INSIDE-TO-DMZ rule 40 destination port 80,443
set firewall name FROM-INSIDE-TO-DMZ rule 40 protocol tcp
set firewall name FROM-INSIDE-TO-DMZ rule 40 source address 10.0.0.0/8
```

Figure 15: Inside Config

```
PC2> ping 10.2.2.100 -P 17 -p 2001
10.2.2.100 udp_seq=1 timeout
10.2.2.100 udp_seq=2 timeout
10.2.2.100 udp_seq=3 timeout
10.2.2.100 udp_seq=4 timeout
10.2.2.100 udp_seq=5 timeout
```

Figure 16: Outside PC can’t ping inside PC’s

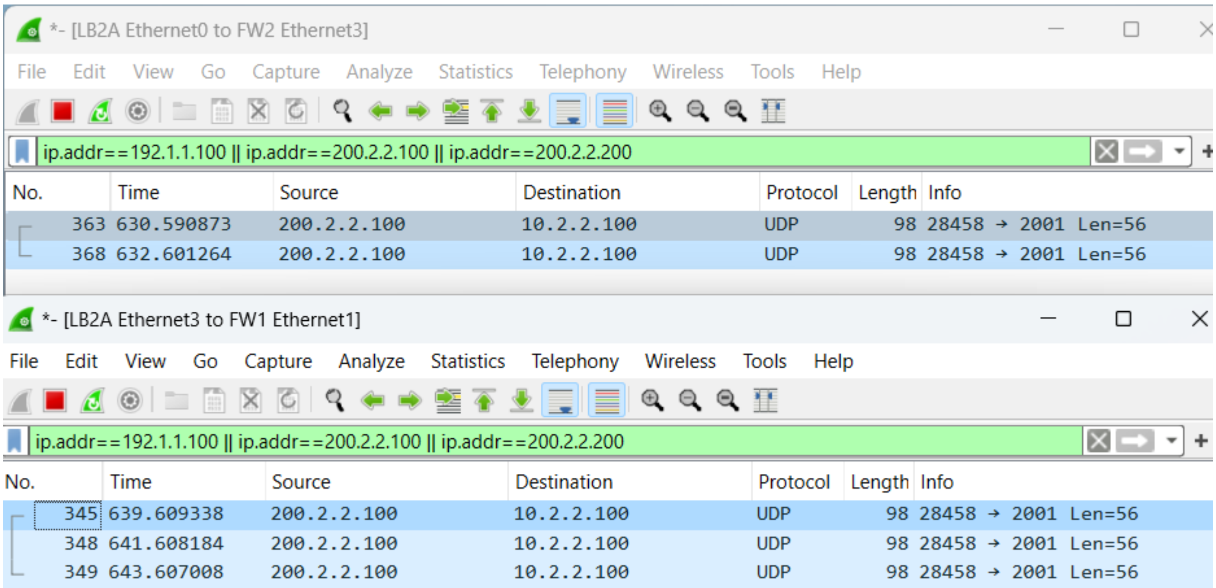

Figure 17: Pings Don't go through Firewall

Outside

The devices Outside the network can connect only to the DMZ using UDP packages on ports 2000-4000, and the packets are incoming from the address of the internal network and addresses that are in the NAT pool of our infrastructure. Finally, we allowed HTTPS to outside users connecting the device 192.1.1.100 of the DMZ.

```
set firewall name FROM-OUTSIDE-TO-DMZ rule 20 description "Accept UDP Echo Request"
set firewall name FROM-OUTSIDE-TO-DMZ rule 20 action accept
set firewall name FROM-OUTSIDE-TO-DMZ rule 20 protocol udp
set firewall name FROM-OUTSIDE-TO-DMZ rule 20 destination port 2000-4000
set firewall name FROM-OUTSIDE-TO-DMZ rule 20 destination address 192.1.1.100/24
set firewall name FROM-OUTSIDE-TO-DMZ rule 20 source address !10.0.0.0/8
set firewall name FROM-OUTSIDE-TO-DMZ rule 20 source address !192.1.0.0/28

set firewall name FROM-OUTSIDE-TO-DMZ rule 40 description "Accept HTTPS"
set firewall name FROM-OUTSIDE-TO-DMZ rule 40 action accept
set firewall name FROM-OUTSIDE-TO-DMZ rule 40 destination address 192.1.1.100/24
set firewall name FROM-OUTSIDE-TO-DMZ rule 40 destination port 443
set firewall name FROM-OUTSIDE-TO-DMZ rule 40 protocol tcp
set firewall name FROM-OUTSIDE-TO-DMZ rule 40 source address !10.0.0.0/8
set firewall name FROM-OUTSIDE-TO-DMZ rule 40 source address !192.1.0.0/28
```

Figure 18: Outside config

```
PC2> ping 192.1.1.100 -T 10000
84 bytes from 192.1.1.100 icmp_seq=1 ttl=60 time=34.315 ms
84 bytes from 192.1.1.100 icmp_seq=2 ttl=60 time=38.862 ms
84 bytes from 192.1.1.100 icmp_seq=3 ttl=60 time=40.469 ms
84 bytes from 192.1.1.100 icmp_seq=4 ttl=60 time=32.280 ms
84 bytes from 192.1.1.100 icmp_seq=5 ttl=60 time=38.993 ms
```

Figure 19: Outside PC's(200.2.2.100) can ping DMZ