



Universidade de Aveiro

Mestrado em Cibersegurança

Código: 41782 - Segurança em Redes de Comunicações

Responsível: Paulo Jorge Salvador Serra Ferreira

Report 1

Monday 8th April, 2024

Ricardo Covelo (102668) - Telmo Sauce (104428)

Contents

1	Exercise 9	1
1.1	Q1 - Explain why the synchronization of the load-balancers allows the nonexistence of a firewall synchronization.	1
1.2	Q2 - Which load-balancing algorithm may also allow the nonexistence of load-balancer synchronization?	1
1.3	Q3 - Explain why device/connection states synchronization may be detrimental during a DDoS attack.	1
2	Exercise 10	2
2.1	Policies	2
2.1.1	Good Practice	2
2.1.2	Preventing DDOS	3
3	Implementaion	3
3.1	Load-Balancing	3
3.2	Synchronization	4
3.3	NAT	5
3.4	Firewall policies	5

1 Exercice 9

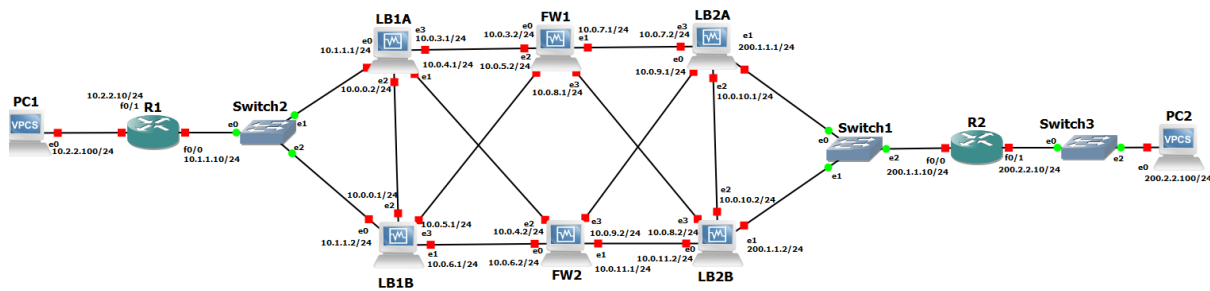


Figure 1: Network

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

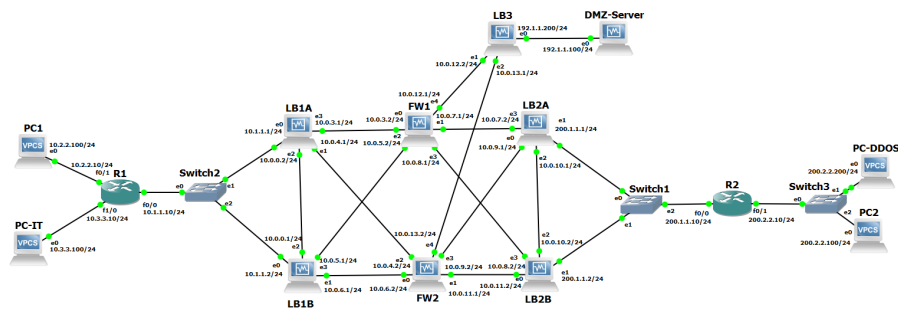


Figure 2: Network

2.1 Policies

2.1.1 Good Practice

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

- Restrict 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.
- Restrict communications that are started from the outside and trying to communicate with our internal network.
- Restrict 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 Vlan's 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-Availability-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.

No.	Time	Source	Destination	Protocol	Length	Info
176	268.882853	10.3.3.100	192.1.1.100	TCP	74	53285 → 22 [SYN] Seq=
177	268.885922	192.1.1.100	10.3.3.100	TCP	60	22 → 53285 [RST, ACK] Seq=
178	261.901152	10.3.3.100	192.1.1.100	TCP	74	[TCP Port numbers reversed]
179	261.905556	192.1.1.100	10.3.3.100	TCP	60	22 → 53285 [RST, ACK] Seq=

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: Synchronization conf

No.	Time	Source	Destination	Protocol	Length	Info
183	58.053755	10.0.0.1	224.0.0.18	VRRP	60	Announcement (v2)
184	58.141323	10.0.0.1	225.0.0.50	UDP	60	60254 → 3780 Len=16
185	58.446921	10.0.0.2	225.0.0.50	UDP	60	42427 → 3780 Len=16
186	59.464911	10.0.0.1	224.0.0.18	VRRP	60	Announcement (v2)
187	59.142528	10.0.0.1	225.0.0.50	UDP	60	60254 → 3780 Len=16
188	59.447434	10.0.0.2	225.0.0.50	UDP	60	42427 → 3780 Len=16
189	60.950419	10.0.0.1	224.0.0.18	VRRP	60	Announcement (v2)
190	60.143474	10.0.0.1	225.0.0.50	UDP	60	60254 → 3780 Len=16
191	60.448346	10.0.0.2	225.0.0.50	UDP	60	42427 → 3780 Len=16
192	61.055042	10.0.0.1	224.0.0.18	VRRP	60	Announcement (v2)
193	61.143574	10.0.0.1	225.0.0.50	UDP	60	60254 → 3780 Len=16
194	61.449408	10.0.0.2	225.0.0.50	UDP	60	42427 → 3780 Len=16
195	62.000888	10.0.0.1	224.0.0.18	VRRP	60	Announcement (v2)
196	62.144468	10.0.0.1	225.0.0.50	UDP	60	60254 → 3780 Len=16
197	62.449670	10.0.0.2	225.0.0.50	UDP	60	42427 → 3780 Len=16
198	63.008756	10.0.0.1	224.0.0.18	VRRP	60	Announcement (v2)
199	63.145739	10.0.0.1	225.0.0.50	UDP	60	60254 → 3780 Len=16
200	63.458320	10.0.0.2	225.0.0.50	UDP	60	42427 → 3780 Len=16
201	64.055641	10.0.0.1	224.0.0.18	VRRP	60	Announcement (v2)
202	64.146689	10.0.0.1	225.0.0.50	UDP	60	60254 → 3780 Len=16
203	64.451438	10.0.0.2	225.0.0.50	UDP	60	42427 → 3780 Len=16
204	65.000886	10.0.0.1	224.0.0.18	VRRP	60	Announcement (v2)
205	65.147623	10.0.0.1	225.0.0.50	UDP	60	60254 → 3780 Len=16
206	65.452179	10.0.0.2	225.0.0.50	UDP	60	42427 → 3780 Len=16
207	66.001631	10.0.0.1	224.0.0.18	VRRP	60	Announcement (v2)
208	66.149219	10.0.0.1	225.0.0.50	UDP	60	60254 → 3780 Len=16
209	66.452732	10.0.0.2	225.0.0.50	UDP	60	42427 → 3780 Len=16
210	67.002706	10.0.0.1	224.0.0.18	VRRP	60	Announcement (v2)
211	67.149624	10.0.0.1	225.0.0.50	UDP	60	60254 → 3780 Len=16
212	67.453661	10.0.0.2	225.0.0.50	UDP	60	42427 → 3780 Len=16
213	68.004048	10.0.0.1	224.0.0.18	VRRP	60	Announcement (v2)
214	68.158773	10.0.0.1	225.0.0.50	UDP	60	60254 → 3780 Len=16

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

The figure displays three Wireshark packet capture windows, each showing a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info.

Window 1: [LB2A Ethernet0 to FW2 Ethernet3]

No.	Time	Source	Destination	Protocol	Length	Info
139	221.222744	192.1.0.20	200.2.2.100	UDP	98	15983 → 2001 Len=56
140	223.222611	192.1.0.20	200.2.2.100	UDP	98	15983 → 2001 Len=56
141	224.242437	200.2.2.100	192.1.0.20	UDP	98	2001 → 15983 Len=56
142	224.252584	200.2.2.100	192.1.0.20	UDP	98	2001 → 15983 Len=56
143	225.220836	192.1.0.20	200.2.2.100	UDP	98	15983 → 2001 Len=56

Window 2: [FW1 Ethernet3 to LB2B Ethernet3]

No.	Time	Source	Destination	Protocol	Length	Info
97	164.874880	192.1.0.10	200.2.2.100	UDP	98	59811 → 2012 Len=56
100	165.913397	192.1.0.10	200.2.2.100	UDP	98	59811 → 2012 Len=56
101	166.941141	192.1.0.10	200.2.2.100	UDP	98	59811 → 2012 Len=56
102	167.982622	192.1.0.10	200.2.2.100	UDP	98	59811 → 2012 Len=56
103	169.023410	192.1.0.10	200.2.2.100	UDP	98	59811 → 2012 Len=56

Window 3: [LB1B Ethernet1 to FW2 Ethernet0]

No.	Time	Source	Destination
55	96.219747	10.3.3.100	200.2.2.100
56	98.219649	10.3.3.100	200.2.2.100
59	100.218073	10.3.3.100	200.2.2.100
62	101.259786	10.3.3.100	200.2.2.100
63	102.303427	10.3.3.100	200.2.2.100

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


```

4> 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

4> 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

4> ping 200.2.2.200
200.2.2.200 icmp_seq=1 timeout
200.2.2.200 icmp_seq=2 timeout
200.2.2.200 icmp_seq=3 timeout
200.2.2.200 icmp_seq=4 timeout
200.2.2.200 icmp_seq=5 timeout

```

Figure 13: Failed pings

The image shows three Wireshark packet capture windows. The top window shows a list of five ping requests from 10.3.3.100 to 200.2.2.100, all marked as 'timeout'. The middle window shows a detailed view of one of these ping requests, displaying the ICMP Echo (ping) request packet structure. The bottom window shows a packet capture of a ping request from 10.3.3.100 to 200.2.2.200, also marked as 'timeout'.

No.	Time	Source	Destination	Protocol	Length	Info
6	0.35.342486	10.3.3.100	200.2.2.100	ICMP	56	Echo (ping) request [length=56]
7	0.35.342490	10.3.3.100	200.2.2.100	ICMP	56	Echo (ping) request [length=56]
8	0.35.342494	10.3.3.100	200.2.2.100	ICMP	56	Echo (ping) request [length=56]
9	0.35.342498	10.3.3.100	200.2.2.100	ICMP	56	Echo (ping) request [length=56]
10	0.35.342502	10.3.3.100	200.2.2.100	ICMP	56	Echo (ping) request [length=56]

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 Personnel 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

The figure consists of two Wireshark packet capture windows. The top window is titled '*- [LB2A Ethernet0 to FW2 Ethernet3]' and the bottom window is titled '*- [LB2A Ethernet3 to FW1 Ethernet1]'. Both windows show a packet list table with columns: No., Time, Source, Destination, Protocol, Length, and Info. The filter in both windows is 'ip.addr==192.1.1.100 || ip.addr==200.2.2.100 || ip.addr==200.2.2.200'.

No.	Time	Source	Destination	Protocol	Length	Info
363	630.590873	200.2.2.100	10.2.2.100	UDP	98	28458 → 2001 Len=56
368	632.601264	200.2.2.100	10.2.2.100	UDP	98	28458 → 2001 Len=56

No.	Time	Source	Destination	Protocol	Length	Info
345	639.609338	200.2.2.100	10.2.2.100	UDP	98	28458 → 2001 Len=56
348	641.608184	200.2.2.100	10.2.2.100	UDP	98	28458 → 2001 Len=56
349	643.607008	200.2.2.100	10.2.2.100	UDP	98	28458 → 2001 Len=56

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