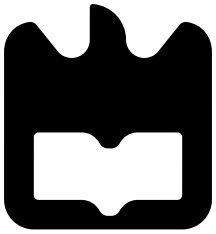
Security in Communications Networks

First Project Report

João Gaspar (107708)

Departamento de Eletrónica, Telecomunicações e Informática

Universidade de Aveiro



Contents

List of Figures

List of Tables

1 Introduction

This report documents my design, deployment, configuration, and testing of a secure communications network incorporating redundant load-balancers and firewalls. It covers six key implementation points:

- Firewall and load-balancers deployment
- Network routing and connectivity
- Device state synchronization
- Zones definition based on security policies
- Inter-zone rules based on security policies
- Report structure and findings

2 Firewall and Load Balancers Deployment

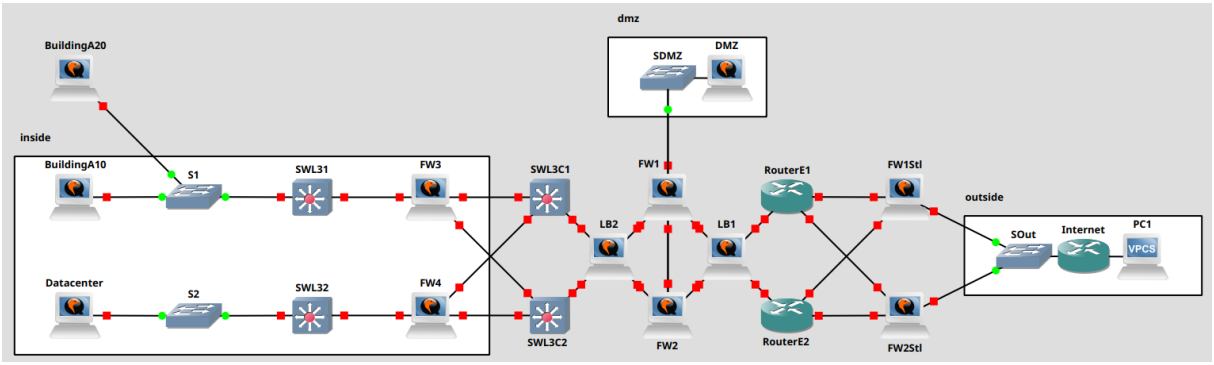


Figure 1: Project topology with firewalls and load-balancers

2.1 Topology Overview

The network is divided into three security zones: *Outside* (Internet), *DMZ* (public-facing services), and *Inside* (internal network). I deployed six VyOS firewalls—two stateless at the Internet edge and four stateful internally and at the core—plus two VyOS load-balancers for redundancy.

2.2 IPv4 Addressing Summary

Table 1: IPv4 addressing of all devices

Device	Interface	IPv4 Private	IPv4 Public
Internet	Fa0/0	100.0.0.1/29	–
	Fa0/1	100.0.0.13/30	–
FWStl1	eth1	10.0.1.1/30	–
	eth2	10.0.1.5/30	–
	eth3	–	100.0.0.2/29
FWStl2	eth1	10.0.1.9/30	–
	eth2	10.0.1.13/30	–

Device	Interface	IPv4 Private	IPv4 Public
	eth3	–	100.0.0.3/29
RouterE1	Fa0/0	10.0.1.2/30	–
	Fa0/1	10.0.1.14/30	–
	Fa1/0	10.0.2.1/30	–
RouterE2	Fa0/0	10.0.1.10/30	–
	Fa0/1	10.0.1.6/30	–
	Fa1/0	10.0.2.5/30	–
LB1	eth1	10.0.2.6/30	–
	eth2	10.0.2.9/30	–
	eth3	10.0.2.13/30	–
	eth8	10.0.2.2/30	–
FW1	eth1	10.0.2.10/30	–
	eth2	200.0.0.2/24	–
	eth5	192.168.250.1/30	–
	eth5v10v4	–	–
	eth8	10.0.2.17/30	–
DMZ Server	ens3	200.0.0.4/24	–
FW2	eth1	10.0.2.25/30	–
	eth2	200.0.0.3/24	–
	eth5	192.168.250.2/30	–
	eth5v10v4	192.168.100.1/24	–
	eth8	10.0.2.14/30	–
LB2	eth1	10.0.2.26/30	–
	eth2	10.0.2.33/30	–
	eth3	10.0.2.37/30	–
	eth8	10.0.2.18/30	–
SWL3C1	Fa0/0	10.0.2.34/30	–
	Fa1/0	10.0.2.41/30	–
	Fa1/1	10.0.2.45/30	–
SWL3C2	Fa0/0	10.0.2.38/30	–
	Fa1/0	10.0.2.49/30	–
	Fa1/1	10.0.2.53/30	–
FW3	eth1	10.0.2.54/30	–
	eth2	10.0.2.57/30	–
	eth8	10.0.2.42/30	–
FW4	eth1	10.0.2.5/30	–
	eth2	10.0.2.65/30	–
	eth8	10.0.2.50/30	–
SWL31	Fa1/0	10.0.2.58/30	–
	Fa1/1	VLAN10:10.10.0.1 & VLAN20:10.20.0.1	–
SWL32	Fa1/0	10.0.2.66/30	–
	Fa1/1	10.100.0.2/24	–
BuildingA10	ens3	10.10.0.10/24	–
BuildingA20	ens3	10.20.0.10/24	–
Datacenter	ens3	10.100.0.1/16	–

3 Network Routing and Connectivity

3.1 OSPF Configuration

All routers and Layer-3 switches run OSPF process 1. For example, on RouterE1:

```
router ospf 1
  network 10.0.0.0 0.0.255.255 area 0
  network 10.10.0.0 0.0.0.255 area 0
  network 10.20.0.0 0.0.0.255 area 0
  network 10.100.0.0 0.0.255.255 area 0
  network 200.0.0.0 0.0.0.255 area 0
```

Below is the equivalent configuration snippet on FW1:

```
protocols {
  ospf {
    area 0 {
      network 10.0.0.0/16
      network 10.100.0.0/16
      network 200.0.0.0/24
      network 100.0.0.0/29
      network 10.10.0.0/24
      network 10.20.0.0/24
    }
  }
}
```

3.2 OSPF Neighbors and Routes

```
RouterE1#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.0.2.13         1   FULL/BDR        00:00:37    10.0.2.2        FastEthernet1/0
100.0.0.3         1   FULL/BDR        00:00:38    10.0.1.13       FastEthernet0/1
100.0.0.2         1   FULL/BDR        00:00:38    10.0.1.1        FastEthernet0/0
...
```

```
vyos@vyos:~$ show ip route ospf
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, ...
O   10.0.1.0/30 [110/1] is directly connected, eth1, weight 1, 00:01:34
O   10.0.1.4/30 [110/1] is directly connected, eth2, weight 1, 00:01:47
...
```

3.3 Ping Tests

```
vyos@FW2:~$ ping 100.0.0.1
PING 100.0.0.1 (100.0.0.1) 56(84) bytes of data.
64 bytes from 100.0.0.1: icmp_seq=1 ttl=252 time=22.7 ms
64 bytes from 100.0.0.1: icmp_seq=2 ttl=252 time=23.5 ms
64 bytes from 100.0.0.1: icmp_seq=3 ttl=252 time=22.5 ms
64 bytes from 100.0.0.1: icmp_seq=4 ttl=252 time=30.1 ms
^C
--- 100.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
```

Figure 2: Ping from FW2 to the Internet router

```
labcom@LabComServer:~$ ping 10.10.0.1
PING 10.10.0.1 (10.10.0.1) 56(84) bytes of data.
64 bytes from 10.10.0.1: icmp_seq=1 ttl=251 time=28.8 ms
64 bytes from 10.10.0.1: icmp_seq=2 ttl=251 time=26.2 ms
64 bytes from 10.10.0.1: icmp_seq=3 ttl=251 time=21.8 ms
64 bytes from 10.10.0.1: icmp_seq=4 ttl=251 time=26.8 ms
64 bytes from 10.10.0.1: icmp_seq=5 ttl=251 time=12.9 ms
64 bytes from 10.10.0.1: icmp_seq=6 ttl=251 time=28.3 ms
^C
--- 10.10.0.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 14ms
rtt min/avg/max/mdev = 12.922/24.119/28.758/5.500 ms
```

Figure 3: Ping from DMZ to BuildingA10

4 Devices State Synchronization

4.1 VRRP

On both FW1 and FW2:

```
high-availability {
  vrrp {
    group DMZCluster vrid 20 {
      interface eth2
      virtual-address 200.0.0.1/24
    }
    group FWCluster vrid 10 {
      interface eth5
      virtual-address 192.168.100.1/24
      rfc3768-compatibility
```

```
    }
    sync-group DMZGroup member DMZCluster
    sync-group FWCluster member FWCluster
  }
}
```

4.2 Conntrack-Sync

```
service {
  conntrack-sync {
    accept-protocol 'tcp,udp,icmp'
    failover-mechanism vrrp sync-group FWCluster
    interface eth5
    mcast-group 225.0.0.50
    disable-external-cache
  }
}
```

4.3 State Sync Verification

```
vyos@FW2:~$ show conntrack-sync cache internal
Main Table Entries:
Source          Destination          Protocol
192.168.250.2:46788     225.0.0.50:3780     udp
...
```

Failover Test Before shutting down FW1's `eth5`:

vyos@FW2# *run show vrrp*
...

After shutting down FW1's `eth5`, FW2 becomes MASTER:

vyos@FW2# *run show vrrp*
...

5 Zones Definition Based on Security Policies

5.1 Security Policies

1. DDoS resilience
2. Internal → Internet: only TCP/UDP 80, 443
3. DMZ services accessible from Internet and Inside
4. Intranet/Storage internal DNS: only VLAN 10/20

5. Databases: only VLAN 20
6. VLAN 1 device: SSH/ICMP console access
7. VLAN 10–20: VoIP only (UDP 5060)

5.2 VyOS Zone Configuration

On FW1 and FW2:

```
zone DMZ {
  description "DMZ Servers"
  from INSIDE firewall name INSIDE-to-DMZ
  from OUTSIDE firewall name OUTSIDE-to-DMZ
  interface eth2
}
zone INSIDE {
  description "Internal Network"
  from DMZ firewall name DMZ-to-INSIDE
  interface eth1
}
zone OUTSIDE {
  description "Internet Zone"
  from DMZ firewall name DMZ-to-OUTSIDE
  interface eth8
}
```

On FW3 and FW4:

```
zone CORE {
  description "Core Backbone"
  from INSIDE firewall name INSIDE-to-CORE
  interface eth0
  interface eth8
}
zone INSIDE {
  description "Internal Zone"
  from CORE firewall name CORE-to-INSIDE
  interface eth2
}
```

6 Inter-Zone Rules Based on Security Policies

6.1 Example on FW1

```
name DMZ-to-INSIDE {
  default-action drop
  rule 10 action accept state established related
  rule 20 action accept protocol icmp state new
}
name DMZ-to-OUTSIDE {
  default-action drop
  rule 10 action accept state established related
  rule 20 action accept protocol icmp state new
```

```
}
name INSIDE-to-DMZ {
  default-action drop
  rule 10 action accept state established related
  rule 20 action accept protocol icmp state new
}
name OUTSIDE-to-DMZ {
  default-action drop
  rule 10 action accept protocol udp destination port 53
  rule 20 action accept protocol tcp destination port 443
  rule 30 action accept protocol tcp destination port 993
  rule 40 action accept protocol tcp destination port 25
  rule 50 action accept protocol icmp state new
}
```

6.2 Traffic Validation Tests

To validate the security policies, I executed tailored tests from each source zone to its permitted destinations, observing packet behavior via Wireshark captures and CLI utilities.

Policy 1 – DDoS Resilience via Load Balancers

To mitigate high-rate Distributed Denial of Service (DDoS) attacks, I deployed two redundant VyOS load-balancers (LB1, LB2). These load-balancers distribute incoming connection requests across multiple stateful firewalls (FW1, FW2), preventing any single device from becoming a bottleneck under surge traffic. In a full-scale deployment, the load-balancers could also perform health checks and automatically remove unresponsive backends, further improving overall resilience. Due to lab performance constraints, I was unable to generate realistic DDoS traffic volumes; however, the complete load-balancer configuration is in place, and I validated normal HTTP/HTTPS flows to ensure the distribution logic functions as expected.

Policy 2 – Inside to Internet (TCP/UDP 80, 443)

I verified that internal hosts (e.g. RouterE1) can connect to ports 80 and 443 on the Internet edge successfully, while connections to other ports are dropped by the stateless firewall. Stateful firewalls FW1/FW2 maintain session state and allow return traffic only on established flows.

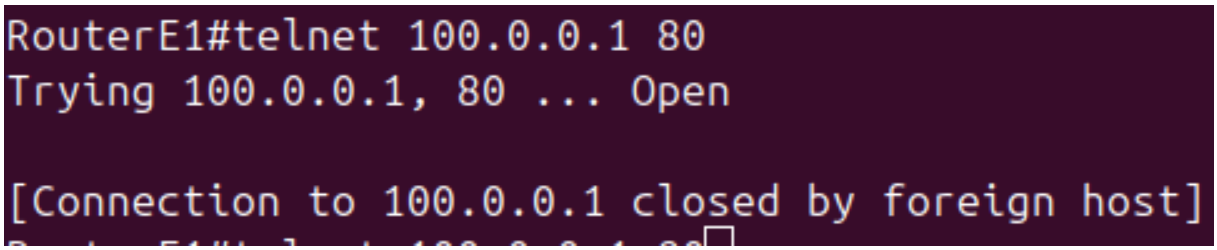


Figure 4: Test of TCP port 80

```
RouterE1#telnet 100.0.0.1 443
Trying 100.0.0.1, 443 ... Open
```

Figure 5: Test of TCP port 443

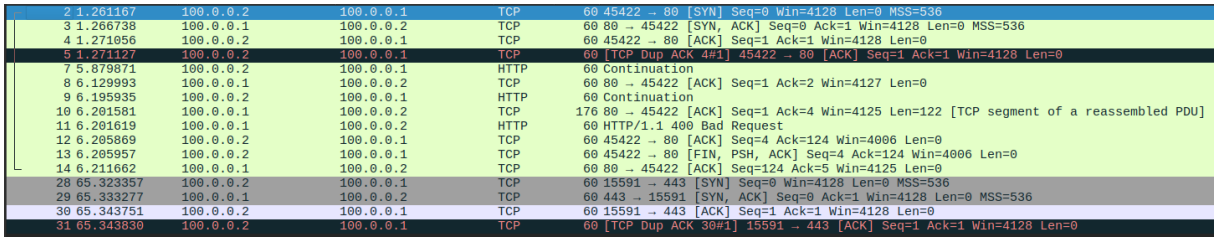


Figure 6: Wireshark capture on link between FWStl1 and Internet

Policy 3 – DMZ Access from Inside and Outside

I confirmed that ICMP traffic from both the Internet edge and the core network reaches the DMZ server (200.0.0.4) successfully, demonstrating bi-directional reachability for monitoring and management purposes. Any protocol not explicitly allowed is dropped at the firewall.

```
Internet#ping 200.0.0.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.0.0.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/50/52 ms
```

Figure 7: Ping from the Internet to DMZ

```
SWL3C1#ping 200.0.0.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.0.0.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/10/12 ms
```

Figure 8: Ping from the core to DMZ

Policy 4 – Intranet/DNS Accessible from VLAN10/20 Only

This policy ensures that only hosts in VLAN10 (10.10.0.0/24) and VLAN20 (10.20.0.0/24) can reach internal intranet/storage services and the internal DNS server. Stateful firewalls FW3 and FW4 enforce this by matching source IP subnets and dropping all other traffic, thus isolating sensitive services within the trusted network segments.

Policy 5 – Database Access Only from VLAN20

I ensured that MySQL (port 3306) on the database server is reachable exclusively from VLAN20. FW3 and FW4 inspect the source IP of incoming connections to port 3306 and allow

only those from 10.20.0.0/24. All other attempts are dropped, preventing unauthorized database access.

Policy 6 – VLAN 1 Device Console Access

I granted ICMP and SSH access only to a single management host in VLAN1 (10.0.1.10). FW1 and FW2 permit traffic from this IP to the console interfaces of all network devices, while blocking all other sources. This approach confines administrative access to a trusted segment.

Policy 7 – VLAN10 - VLAN20 VoIP Only (UDP 5060)

To enable VoIP communications, I restricted traffic between VLAN10 and VLAN20 to UDP port 5060. In testing, SIP traffic passed successfully on the trunk link, whereas ICMP and TCP traffic were dropped, ensuring that only voice calls are permitted between these VLANs.

```
labcom@LabComServer:~$ ping 10.20.0.10
PING 10.20.0.10 (10.20.0.10) 56(84) bytes of data.
From 10.10.0.1 icmp_seq=1 Packet filtered
From 10.10.0.1 icmp_seq=2 Packet filtered
From 10.10.0.1 icmp_seq=3 Packet filtered
From 10.10.0.1 icmp_seq=4 Packet filtered
From 10.10.0.1 icmp_seq=5 Packet filtered
^C
--- 10.20.0.10 ping statistics ---
5 packets transmitted, 0 received, +5 errors, 100% packet loss, time 10ms

labcom@LabComServer:~$ echo "hello" | nc -u 10.20.0.10 5060
```

Figure 9: VoIP between VLAN10 and VLAN20

icmp or udp.port == 5060

No.	Time	Source	Destination	Protocol	Length	Info
156	68.435050	10.10.0.10	10.20.0.10	ICMP	102	Echo (ping) request id=0x03c6, seq=1/256, ttl=64 (no response found!)
157	68.442081	10.10.0.1	10.10.0.10	ICMP	74	Destination unreachable (Communication administratively filtered)
158	69.436777	10.10.0.10	10.20.0.10	ICMP	102	Echo (ping) request id=0x03c6, seq=2/512, ttl=64 (no response found!)
159	69.438956	10.10.0.1	10.10.0.10	ICMP	74	Destination unreachable (Communication administratively filtered)
164	70.438793	10.10.0.10	10.20.0.10	ICMP	102	Echo (ping) request id=0x03c6, seq=3/768, ttl=64 (no response found!)
165	70.443755	10.10.0.1	10.10.0.10	ICMP	74	Destination unreachable (Communication administratively filtered)
166	71.440475	10.10.0.10	10.20.0.10	ICMP	102	Echo (ping) request id=0x03c6, seq=4/1024, ttl=64 (no response found!)
167	71.450486	10.10.0.1	10.10.0.10	ICMP	74	Destination unreachable (Communication administratively filtered)
172	72.441785	10.10.0.10	10.20.0.10	ICMP	102	Echo (ping) request id=0x03c6, seq=5/1280, ttl=64 (no response found!)
173	72.447193	10.10.0.1	10.10.0.10	ICMP	74	Destination unreachable (Communication administratively filtered)
275	117.771934	10.10.0.10	10.20.0.10	UDP	64	41038 → 5060 Len=6

Figure 10: Wireshark capture of SIP packets

7 Conclusion

I successfully deployed and tested a multi-layer secure network featuring redundant firewalls and load-balancers, OSPF routing, VRRP & conntrack-sync state synchronization, and precise inter-zone firewall rules. All tests confirmed the correct enforcement of the security policies. Future improvements could include automated DDoS mitigation and advanced load-balancing algorithms.