SAND PMA

Student ID or IDs for group work	2126529
Module Date	7th - 11th November 2022

Date set	10th Nov 2022
Submission date (excluding extensions)	12th Dec 2022
Submission guidance	Several files of several types to be submitted via tabula (See Assignment Specification supplied separately) Also viva / demo
Marks return date (excluding extensions)	18th Jan 2023
Late submission policy	If work is submitted late, penalties will be applied at the rate of **5 marks per University working day** after the due date, up to a **maximum of 10 working days** late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). "Late" means **after the submission deadline time as well as the date** – work submitted after the given time even on the same day is counted as 1 day late. For **Postgraduate** students only, who started their **current course before 1 August 2019**, the daily penalty is **3 marks** rather than 5.
Resubmission policy	If you fail this assignment or module, please be aware that the University allows students to remedy such failure (within certain limits). Decisions to authorise such resubmissions are made by Exam Boards. Normally these will be issued at specific times of the year, depending on your programme of study. More information can be found from your programme office if you are concerned.

Module title & code	ES94P-15 Security Architecture and Network Defence (SAND)
Module owner	Peter Norris
Module tutor	Peter Norris
Module marker	Peter Norris
Assessment type	Technical securing of organisation's assets (design, implement, test) in emulated environment, evaluation of proposal, with demo/viva. All to be consistent with each other.
Weighting of mark	100%

Phase1:

1.1 Clearly represent the zones of trust, the network topology and ip addressing used in the network diagram in the pdf[1]
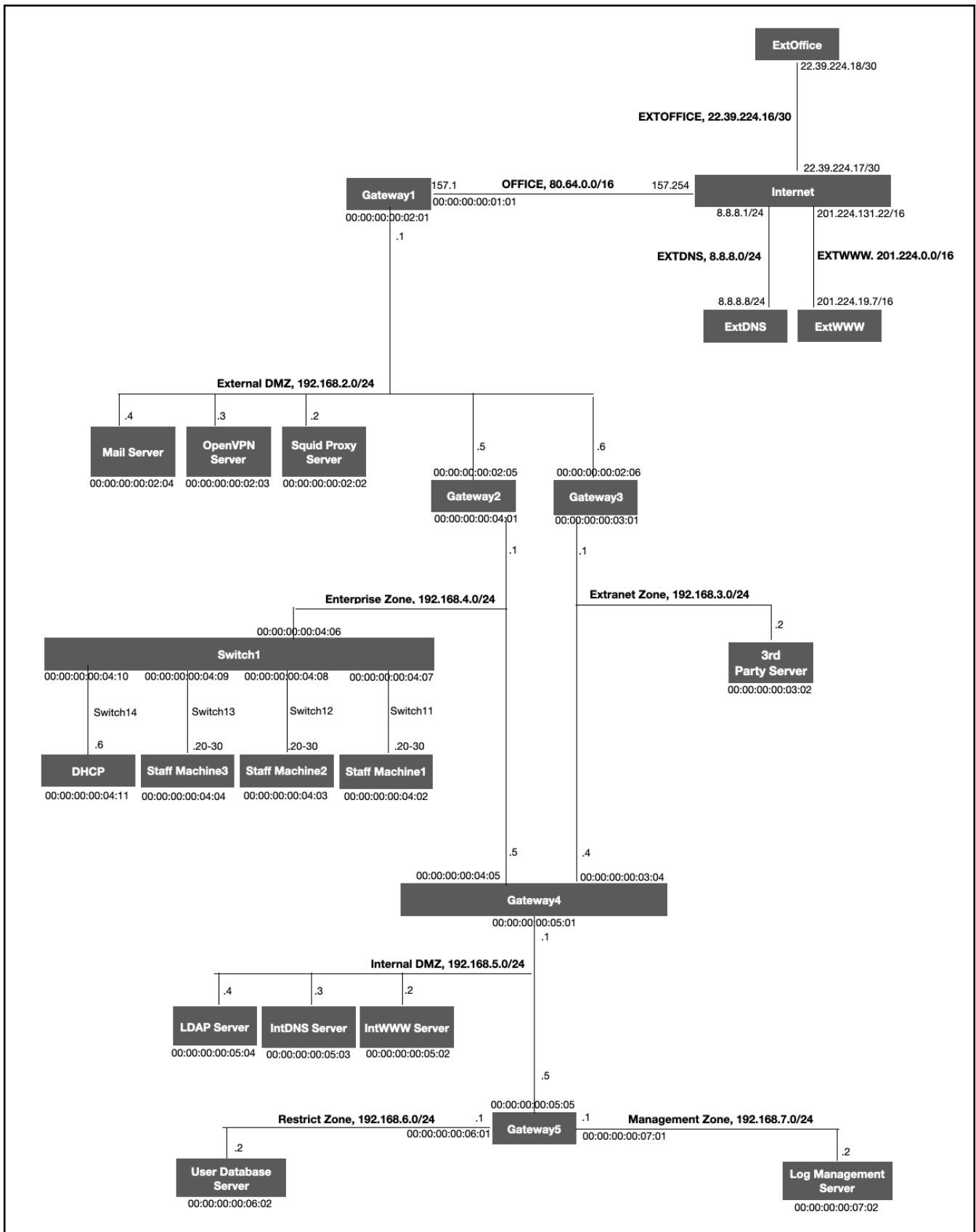
1.2 Define and implement credible zones of trust and re-organised IP addressing[1]

• Internet Zone (No Trust):

	IP Address	Mac Address
ExtOffice	22.39.224.18/30	X
ExtDNS	8.8.8.8/24	X
ExtWWW	201.224.19.7/16	X

• External DMZ (Low Trust):

	IP Address	Mac Address
Squid Proxy Server	192.168.2.2/24	00:00:00:00:02:02
OpenVPN Server	192.168.2.3/24	00:00:00:00:02:03
Mail Server	192.168.2.4/24	00:00:00:00:02:04

• Enterprise Zone (Medium Trust):

	IP Address	Mac Address
Staff Machine1	192.168.4.20-30/24	00:00:00:00:04:02
Staff Machine2	192.168.4.20-30/24	00:00:00:00:04:03
Staff Machine3	192.168.4.20-30/24	00:00:00:00:04:04

• Extranet Zone (Medium Trust):

	IP Address	Mac Address
3rd Party Server	192.168.3.2/24	00:00:00:00:03:02

• Internal DMZ (High Trust):

	IP Address	Mac Address
IntWWW Server	192.168.5.2/24	00:00:00:00:05:02
IntDNS Server	192.168.5.3/24	00:00:00:00:05:03
LDAP Server	192.168.5.4/24	00:00:00:00:05:04

• Restrict Zone (Highest Trust):

	IP Address	Mac Address
User Database Server	192.168.6.2/24	00:00:00:00:06:02

• Management Zone (Highest Trust):

	IP Address	Mac Address
Log Management Server	192.168.7.2/24	00:00:00:00:07:02

1.3 Define and implement filters between zones of trust (All use TCP protocol)

- External DMZ (Low Trust) - Enterprise Zone (Medium Trust)

	IP Address:Port	IP Address:Port
Squid Server → All Staff	192.168.2.2/24:Any	192.168.4.0/24:5000
OpenVPN Server → All Staff	192.168.2.3/24:Any	192.168.4.0/24:5000
Mail Server → All Staff	192.168.2.4/24:Any	192.168.4.0/24:5000

- Enterprise Zone (Medium Trust) - Extranet Zone (Medium Trust)

	IP Address:Port	IP Address:Port
All Staff → 3rd Party Server	192.168.4.0/24:Any	192.168.3.2/24:6000
3rd Party Server → All Staff	192.168.3.2/24:Any	192.168.4.0/24:5000

- Enterprise Zone (Medium Trust) - Internal DMZ (High Trust)

	IP Address:Port	IP Address:Port
All Staff → IntWWW Server	192.168.4.0/24:Any	192.168.5.2/24:8080
All Staff → IntDNS Server	192.168.4.0/24:Any	192.168.5.3/24:53
All Staff → LDAP Server	192.168.4.0/24:Any	192.168.5.4/24:389

- Internal DMZ (High Trust) - Restrict Zone (Highest Trust)

	IP Address:Port	IP Address:Port
IntWWW Server → User DB Server	192.168.5.2/24:Any	192.168.6.2/24:1433
LDAP Server → User DB Server	192.168.5.4/24:Any	192.168.6.2/24:1433

- Management Zone (Highest Trust) - All Zone

	IP Address:Port	IP Address:Port
Log Management → External DMZ	192.168.7.2/24:Any	192.168.2.0/24:Any
Log Management → Enterprise Zone	192.168.7.2/24:Any	192.168.3.0/24:Any
Log Management → Extranet Zone	192.168.7.2/24:Any	192.168.4.0/24:Any
Log Management → Internal DMZ	192.168.7.2/24:Any	192.168.5.0/24:Any
Log Management → Restrict Zone	192.168.7.2/24:Any	192.168.6.0/24:Any
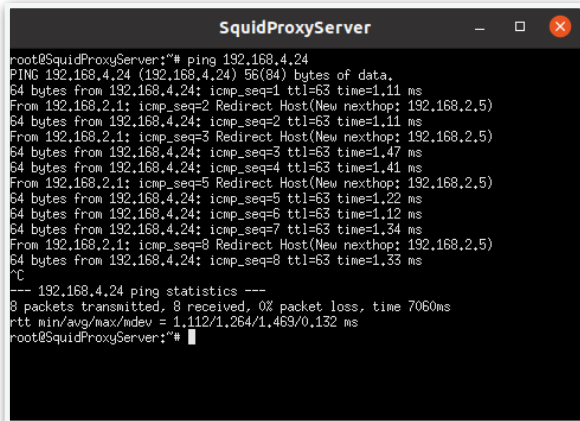
1.4 Partially verify that connectivity is achieved / prevented as appropriate between clients and services

1.4.1 Ping(ICMP) devices between zones to ensure the ip routes we set are correct

To simplify, we select one machine in each zone to ensure ip routes we set are achieved below

External DMZ (Low Trust) - Enterprise Zone (Medium Trust)
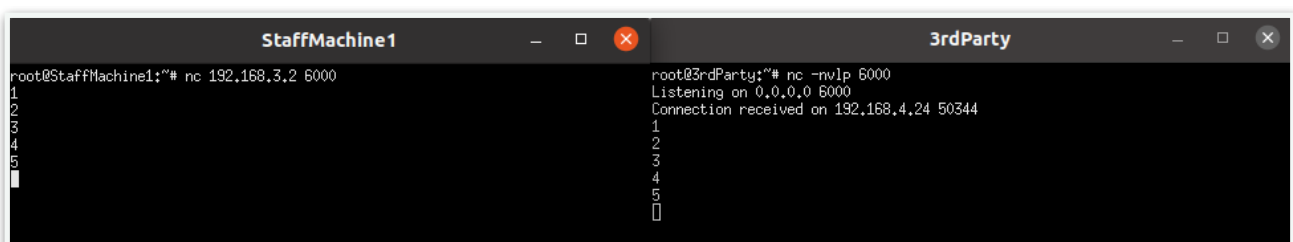- Squid Server - Staff Machine1 (/hostlab/shared/1_4_1_1.pcap)

• External DMZ (Low Trust) - Extranet Zone (Medium Trust)
- Squid Server - 3rd Party Server (/hostlab/shared/1_4_1_2.pcap)
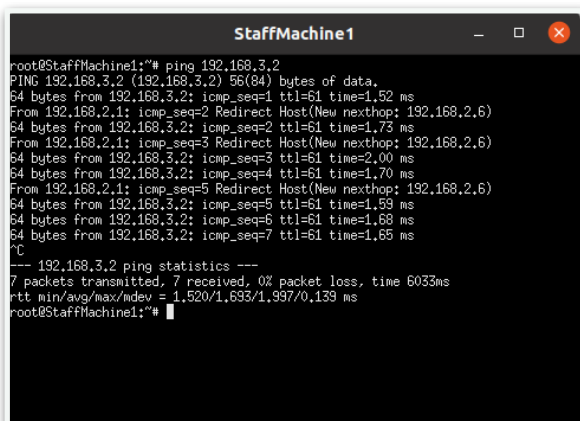
• Enterprise Zone (Medium Trust) - Extranet Zone (Medium Trust)
- Staff Machine1 - 3rd Party Server (/hostlab/shared/1_4_1_3.pcap)

- Enterprise Zone (Medium Trust) - Internal DMZ (High Trust)
- Staff Machine1 - IntWWW Server (/hostlab/shared/1_4_1_4.pcap)

- Extranet Zone (Medium Trust) - Internal DMZ (High Trust)
- 3rd Party Server - IntWWW Server (/hostlab/shared/1_4_1_5.pcap)

- Internal DMZ (High Trust) - Restrict Zone (Highest Trust)
- IntWWW Server - User DB Server (/hostlab/shared/1_4_1_6.pcap)

- Management Zone (Highest Trust) - All Zone
- Log Management Server - Squid Server (/hostlab/shared/1_4_1_7.pcap)

- Log Management Server- Staff Machine1 (/hostlab/shared/1_4_1_8.pcap)
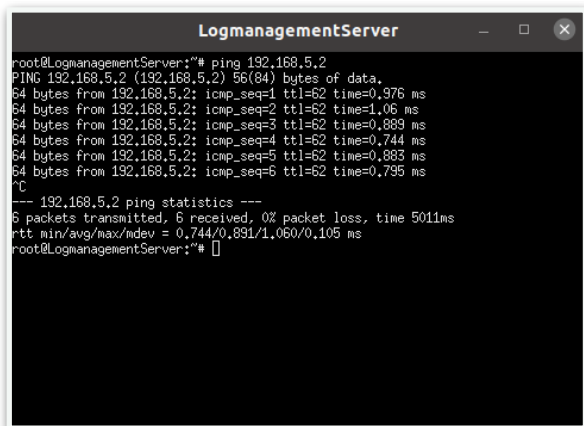
- Log Management Server - 3rd Party Server (/hostlab/shared/1_4_1_9.pcap)

- Log Management Server - IntWWW Server (/hostlab/shared/1_4_1_10.pcap)


```
root@LogmanagementServer:~# ping 192.168.5.2
PING 192.168.5.2 (192.168.5.2) 56(84) bytes of data.
64 bytes from 192.168.5.2: icmp_seq=1 ttl=62 time=0.976 ms
64 bytes from 192.168.5.2: icmp_seq=2 ttl=62 time=1.06 ms
64 bytes from 192.168.5.2: icmp_seq=3 ttl=62 time=0.889 ms
64 bytes from 192.168.5.2: icmp_seq=4 ttl=62 time=0.744 ms
64 bytes from 192.168.5.2: icmp_seq=5 ttl=62 time=0.883 ms
64 bytes from 192.168.5.2: icmp_seq=6 ttl=62 time=0.795 ms
^C
--- 192.168.5.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5011ms
rtt min/avg/max/mdev = 0.744/0.891/1.060/0.105 ms
root@LogmanagementServer:~# []
```

- Log Management Server - User DB Server (/hostlab/shared/1_4_1_11.pcap)


```
root@LogmanagementServer:~# ping 192.168.6.2
PING 192.168.6.2 (192.168.6.2) 56(84) bytes of data.
64 bytes from 192.168.6.2: icmp_seq=1 ttl=63 time=0.589 ms
64 bytes from 192.168.6.2: icmp_seq=2 ttl=63 time=0.857 ms
64 bytes from 192.168.6.2: icmp_seq=3 ttl=63 time=0.722 ms
64 bytes from 192.168.6.2: icmp_seq=4 ttl=63 time=0.670 ms
64 bytes from 192.168.6.2: icmp_seq=5 ttl=63 time=0.588 ms
64 bytes from 192.168.6.2: icmp_seq=6 ttl=63 time=0.681 ms
^C
--- 192.168.6.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5117ms
rtt min/avg/max/mdev = 0.588/0.684/0.857/0.091 ms
root@LogmanagementServer:~# █
```

1.4.2 Netcat ports of devices that we set in the iptables filter

We verify connectivity is prevented by setting default input/forward/output DROP in all firewalls
In the following, we verify that the connectivity we set in the iptables filter is achieved

- External DMZ (Low Trust) - Enterprise Zone (Medium Trust)
- Squid Server → Staff Machine1(5000) (/hostlab/shared/1_4_2_1.pcap)
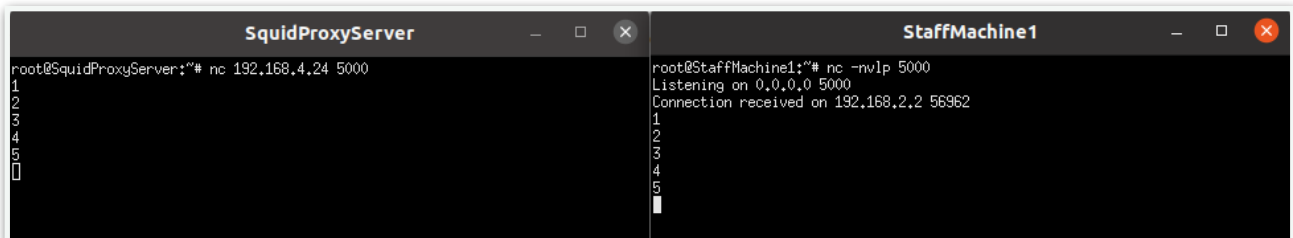
- OpenVPN Server → Staff Machine1(5000) (/hostlab/shared/1_4_2_2.pcap)
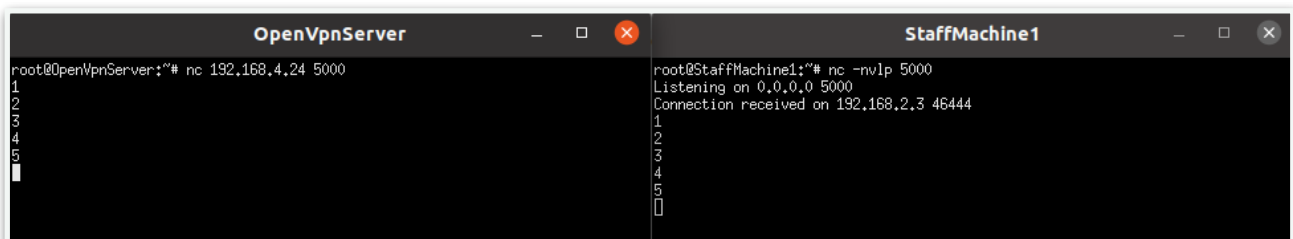
- Mail Server → Staff Machine1(5000) (/hostlab/shared/1_4_2_3.pcap)
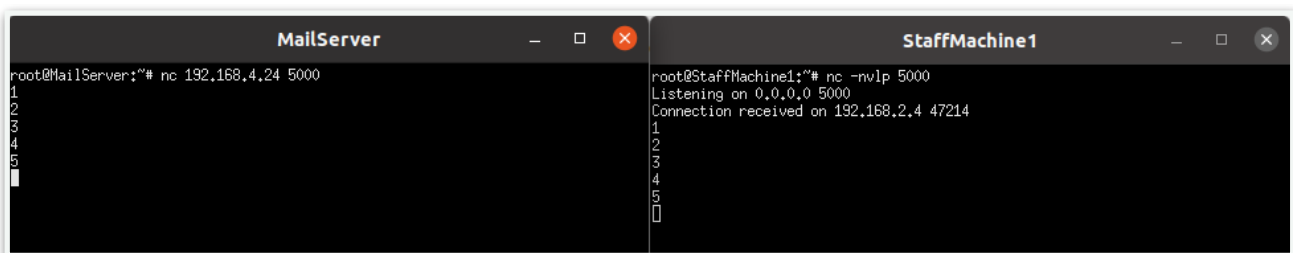
- Enterprise Zone (Medium Trust) - Extranet Zone (Medium Trust)
- Staff Machine1 → 3rd Party Server(6000) (/hostlab/shared/1_4_2_4.pcap)

- 3rd Party Server → Staff Machine1(5000) (/hostlab/shared/1_4_2_5.pcap)
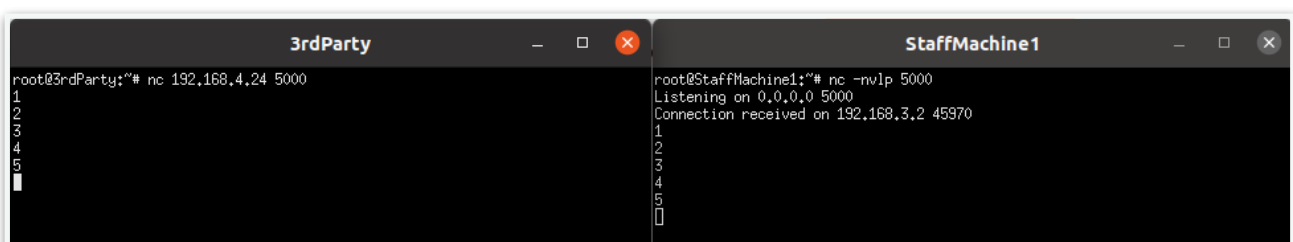
- Enterprise Zone (Medium Trust) - Internal DMZ (High Trust)
- Staff Machine1 → IntWWW Server(8080) (/hostlab/shared/1_4_2_6.pcap)

- Staff Machine1 → IntDNS Server(53) (/hostlab/shared/1_4_2_7.pcap)

- Staff Machine1 → LDAP Server(389) (/hostlab/shared/1_4_2_8.pcap)

- Internal DMZ (High Trust) - Restrict Zone (Highest Trust)
- IntWWW Server → User DB Server(1433) (/hostlab/shared/1_4_2_9.pcap)

- LDAP Server → User DB Server(1433) (/hostlab/shared/1_4_2_10.pcap)

- Management Zone (Highest Trust) - All Zone
- Log Management → Squid Server(8080) (/hostlab/shared/1_4_2_11.pcap)

- Log Management → Staff Machine1(5000) (/hostlab/shared/1_4_2_12.pcap)

- Log Management → 3rd Party Server(6000) (/hostlab/shared/1_4_2_13.pcap)

- Log Management → IntWWW Server(8080) (/hostlab/shared/1_4_2_14.pcap)

- Log Management → User DB Server(1433) (/hostlab/shared/1_4_2_15.pcap)

Phase2:

2.1 Fully implement NAT / port-forwarding(All use TCP protocol)

Internet Zone (No Trust) - External DMZ (Low Trust)

	IP Address:Port	IP Address:Port
Internet → Squid Server	80.64.157.1/16:Any	192.168.2.2/24:8080
Internet → OpenVPN Server	80.64.157.1/16:Any	192.168.2.3/24:487
Internet → Mail Server	80.64.157.1/16:Any	192.168.2.4/24:587
Squid Server → Internet	192.168.2.2/24:Any	80.64.157.254/16:Any
OpenVPN Server → Internet	192.168.2.3/24:Any	80.64.157.254/16:Any
Mail Server → Internet	192.168.2.4/24:Any	80.64.157.254/16:Any

2.2 Robustly verify that connectivity is achieved / prevented as appropriate between clients and services

In this part, we can combine Phase1.4 and will add the NAT part in the following
Netcat ports of devices that we set in the iptables filter

• Internet Zone (No Trust) - External DMZ (Low Trust)
- Internet → Squid Server (8080) (/hostlab/shared/2_2_1.pcap)

- Internet → OpenVPN Server (487) (/hostlab/shared/2_2_2.pcap)

- Internet → Mail Server (587) (/hostlab/shared/2_2_3.pcap)

- Squid Server → Internet (1234) (/hostlab/shared/2_2_4.pcap)


```
SquidProxyServer
root@SquidProxyServer:~# nc 80.64.157.254 1234
1
2
3
4
5
```

```
Internet
root@Internet:~# nc -nvlp 1234
Listening on 0.0.0.0 1234
Connection received on 80.64.157.1 60618
1
2
3
4
5
```

- OpenVPN Server → Internet (4321) (/hostlab/shared/2_2_5.pcap)


```
OpenVpnServer
root@OpenVpnServer:~# nc 80.64.157.254 4321
1
2
3
4
5
```

```
Internet
root@Internet:~# nc -nvlp 4321
Listening on 0.0.0.0 4321
Connection received on 80.64.157.1 42348
1
2
3
4
5
```

- Mail Server → Internet (1111) (/hostlab/shared/2_2_6.pcap)


```
MailServer
root@MailServer:~# nc 80.64.157.254 1111
1
2
3
4
5
```

```
Internet
root@Internet:~# nc -nvlp 1111
Listening on 0.0.0.0 1111
Connection received on 80.64.157.1 46324
1
2
3
4
5
```

2.3 make a compelling case for your design and implementation of one augmented feature

- Load Balance: We divide the network traffic with 2 Gateways (Gateway2 and Gateway3) to avoid massive network traffic to Enterprise Zone
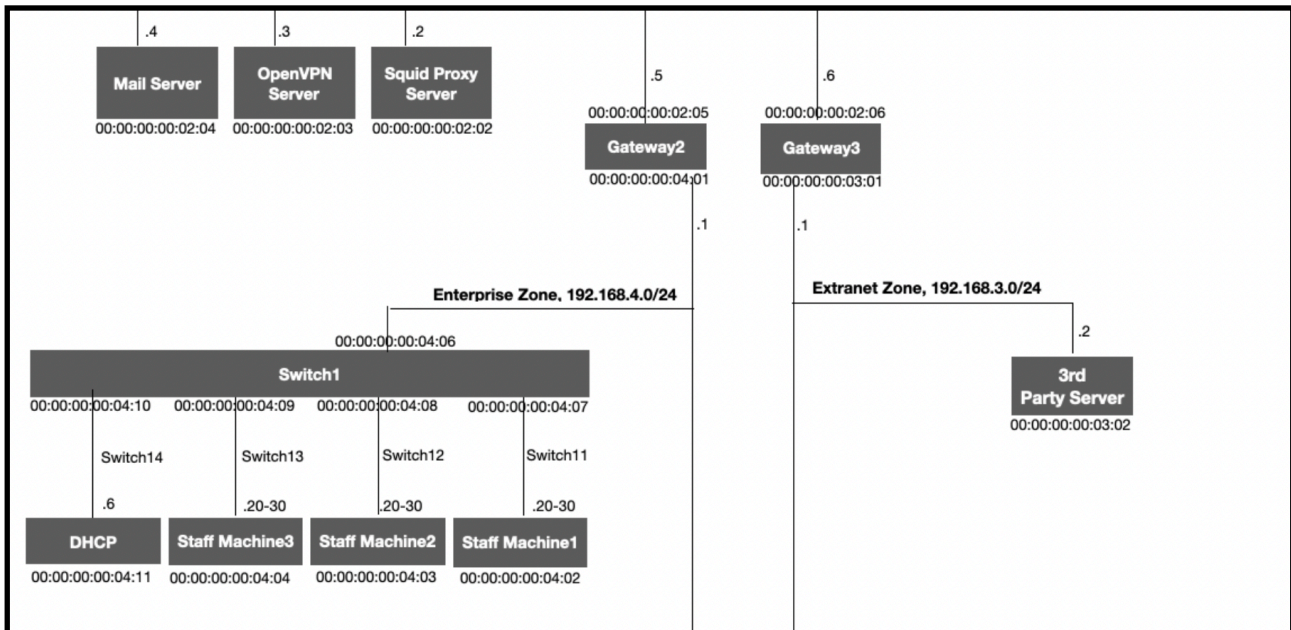
- DHCP: We can avoid manually setting IP addresses errors by using DHCP to enhance the security posture

3. Identifying the further work that is needed but that you were unable to realise

• Utilise VLANs to good effect
• Implement well-organised DNS using zone files

4. Reference

[1] Luciana Obregon. (2021) Infrastructure Security Architecture for Effective Security Monitoring