INFO-0045: Introduction to Computer Security

Project 1 - Firewalls
Part 1 - Drawing of the Network

Maxime Goffart
180521

Olivier Joris
182113

Academic year 2021 - 2022

1 Drawing of the network

We can represent the described network by the following diagram:

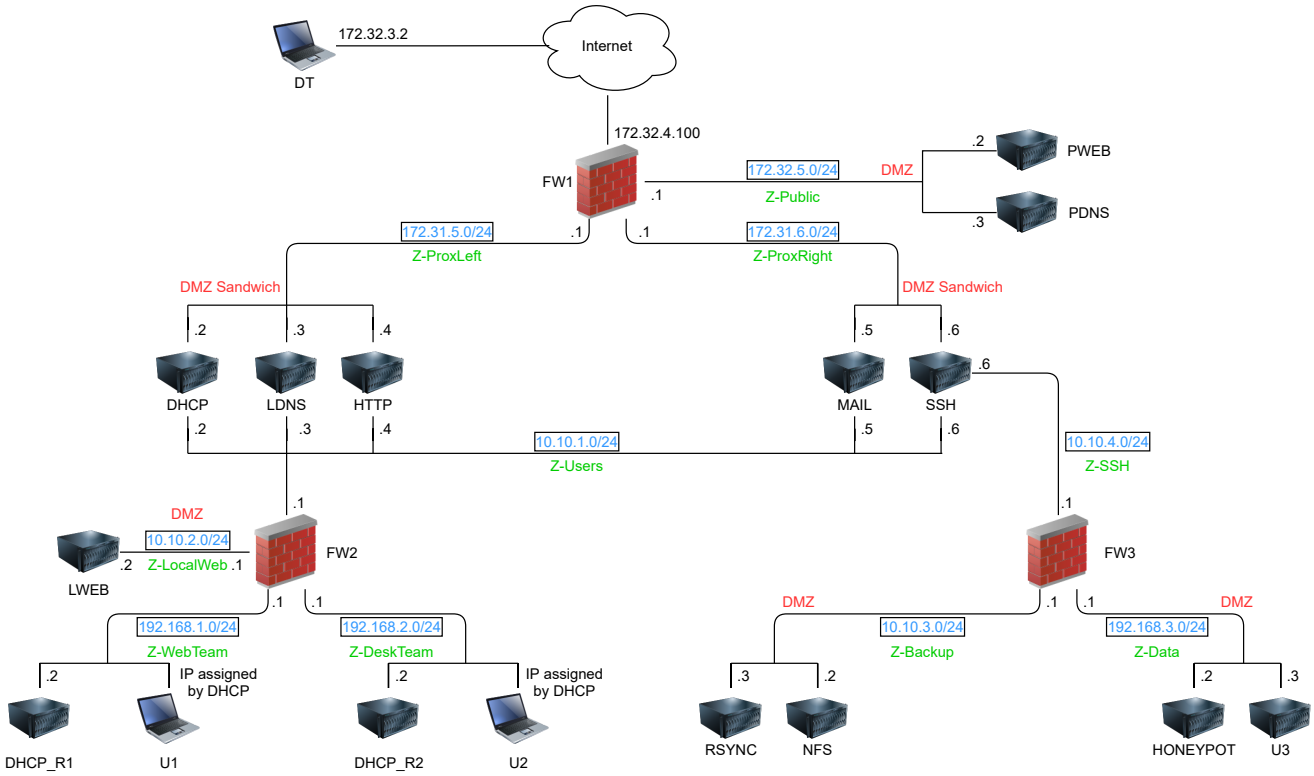

Figure 1: Network topology

2 Zones and their order per firewall

2.1 Zones

We have the following zones:

- `Z-Public` is the zone associated to devices that can be reach from the Internet. It corresponds to the subnet 172.32.5.0/24.
- `Z-ProxLeft` is the zone associated to the DHCP, LDNS, and HTTP(S) services. It corresponds to the subnet 172.31.5.0/24.
- `Z-ProxRight` is the zone associated to the mail (IMAP and SMTP) and SSH services. It corresponds to the subnet 172.31.6.0/24.

- `Z-Users` is the zone associated to the users of the network. It corresponds to the subnet 10.10.1.0/24.
- `Z-LocalWeb` is the zone associated to the local web server. It corresponds to the subnet 10.10.2.0/24.
- `Z-WebTeam` is the zone associated to the web team. It corresponds to the subnet 192.168.1.0/24.
- `Z-DeskTeam` is the zone associated to the desk team. It corresponds to the subnet 192.168.2.0/24.
- `Z-SSH` is the zone associated to the SSH relay. It corresponds to the subnet 10.10.4.0/24.
- `Z-Backup` is the zone associated to the backup servers. It corresponds to the subnet 10.10.3.0/24.
- `Z-Data` is the zone associated to the data servers. It corresponds to the subnet 192.168.3.0/24.

2.2 Order of zones per firewall

For firewall `FW1`, we have the following order of zones based on decreasing security level:

1) `Z-ProxLeft` because these services should not be reachable from outside except for the replies of HTTP(S) and DNS protocols.
2) `Z-ProxRight` because the mail server and ssh relay should receive connections from outside.
3) `Z-Public` because the servers inside this zone are intended for public use.

For firewall `FW2`, we have the following order of zones based on decreasing security level:

1) `Z-DeskTeam` because it should have the highest level of security.
2) `Z-WebTeam` because it should have the same restrictions as `Z-DeskTeam`. Yet, it also need access to the RSYNC server to backup web data and they need access to the FTP server of LWEB to modify web pages.
3) `Z-LocalWeb` because it should be accessible only by people from `Z-WebTeam` and `Z-DeskTeam`.
4) `Z-Users` because it should be accessible by anyone from `Z-WebTeam` and `Z-DeskTeam` because they need to access the proxies, the mail server, and the SSH relay.

For firewall `FW3`, we have the following order of zones based on decreasing security level:

1) `Z-Backup` because it is highly sensible. We definitely do not want anyone without proper permissions to access the servers inside it.
2) `Z-Data` because it should be accessible only by a few people or a few servers.
3) `Z-SSH` because it is under less restrictions than the previous zones.