University of Liège

Securing network with firewalls and NATs

Step 1: drawing the network

Maxime Meurisse
Valentin Vermeylen

Master in Civil Engineering
Academic year 2020-2021

1 Drawing of the network

The representation of the network topology is shown in Figure 1. This figure is in vector format: it is possible to zoom in on it for better reading without loss of quality.

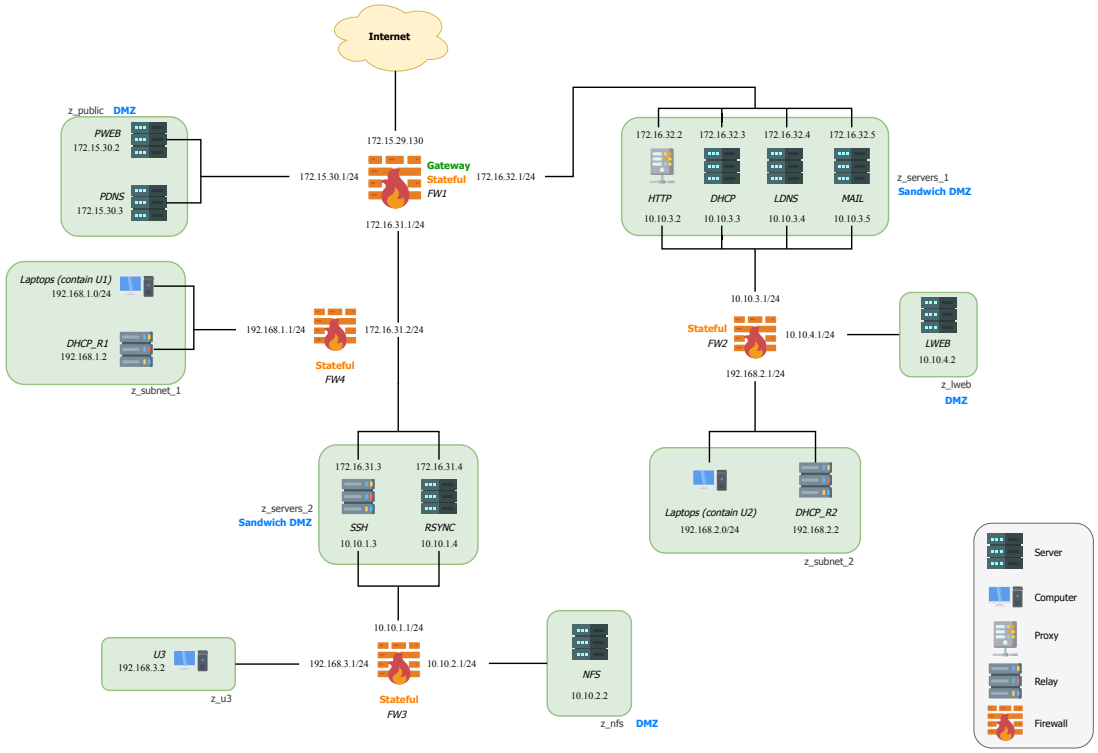

Figure 1: Topology of the network.

2 Details of the network

This network is composed of 4 firewalls, 8 zones and several types of machines (servers, proxies, computers and relays).

2.1 Firewalls

The 4 firewalls present in the network are *stateful* firewalls.

The firewall *FW1* is a gateway: it acts as a link between the Internet and the company's internal network. A NAT configuration will be necessary on this firewall. The NAT interfaces are: `172.15.29.130`, `172.16.32.1/24`, `172.16.31.1/24` and `172.15.30.1/24`.

The other firewalls (*FW2*, *FW3* and *FW4*) are "classical" firewalls that do not act as NATs.

2.2 Zones

The network is composed of 8 zones: *z_public*, *z_servers_1*, *z_servers_2*, *z_lweb*, *z_subnet_1*, *z_subnet_2*, *z_u3* and *z_nfs*. Each zone has been defined by grouping together devices that have the same IP address prefix.

The *z_public*, *z_lweb* and *z_nfs* zones are *DMZ*. The *z_servers_1* and *z_servers_2* zones are *sandwich DMZ* (because zones are between 2 firewalls). These zones are considered are DMZ because they are connected neither to the Internet, or the internel network. The internal network is represented by *z_subnet_1*, *z_subnet_2* and *z_u3* zones.

2.2.1 Zone classification

For each firewall, zones are classified from more secured to less secured.

- *FW1*
  - *z_servers_1*
  - *z_public*
- *FW2*
  - *z_subnet_2*
  - *z_lweb*
- *FW3*
  - *z_nfs*
  - *z_u3*
- *FW4*
  - *z_subnet_1*
  - *z_servers_2*

We have considered that the deeper a zone is in the network (*i.e.* behind more firewalls), the more secure it is.

2.3 Devices

The network is composed of several devices. The type of each device is represented by its icon. Note that in zones *z_subnet_1* and *z_subnet_2*, company computers ("Laptops") cannot have the same IP address as the DHCP relay in the same zone.