18.10.2024

Traccia per il progetto
Esercizio Segmentazione di rete
Disegnare una rete con i seguenti componenti:

- Una zona di Internet (rappresentata da un cloud o un simbolo di Internet).
- Una zona DMZ con almeno un server web HTTP e un server di posta elettronica SMTP.
- Una rete interna con almeno un server o nas.
- Un firewall perimetrale posizionato tra le tre zone.
- Spiegare le scelte

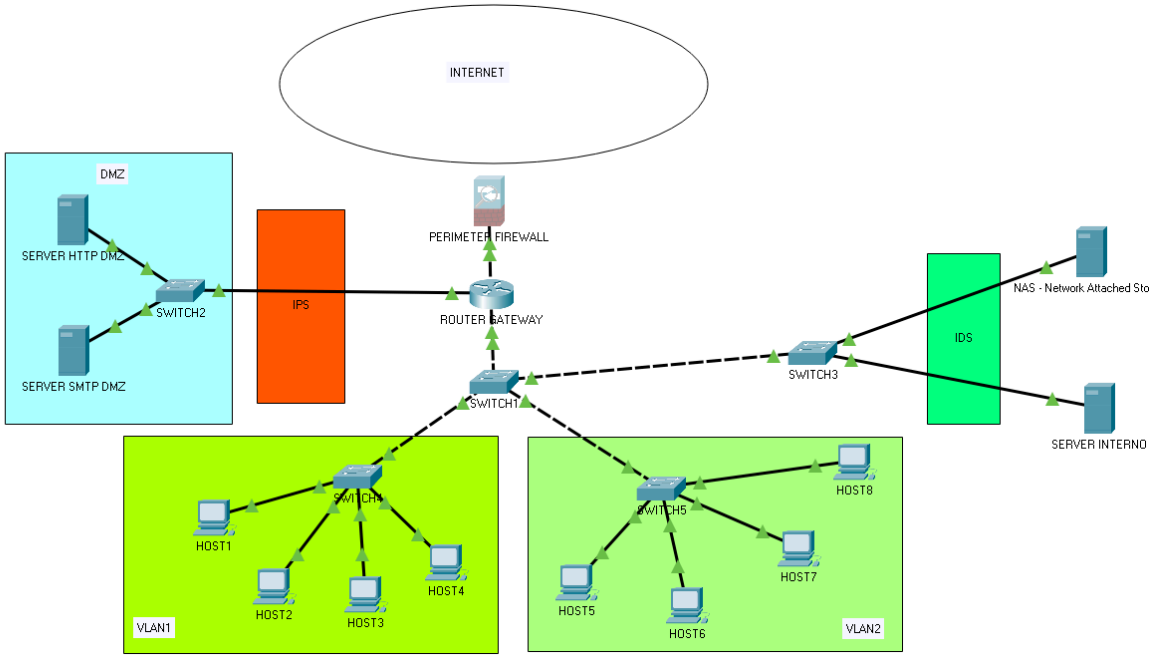
Project
Please segment a network with the following inputs:

- Internet zone;
- DMZ zone with web HTTP and SMTP servers
- “local” network with 1 NAS and 1 Server
- perimeter Firewall
- give a reason for your choices

Cyber Security is nowadays a must for every company which wishes to make business all over the world or easily to be connected with the external world (let’s think about companies with many spread locations - they need to communicate among them) and attacks are more and more frequent as, looks like utopian, data have much more value than money.

Security is, for sure, one **key factor** when it comes to “health company” and we’re gonna setup a company network with few features to prevent attacks and keep the “working space” safe.

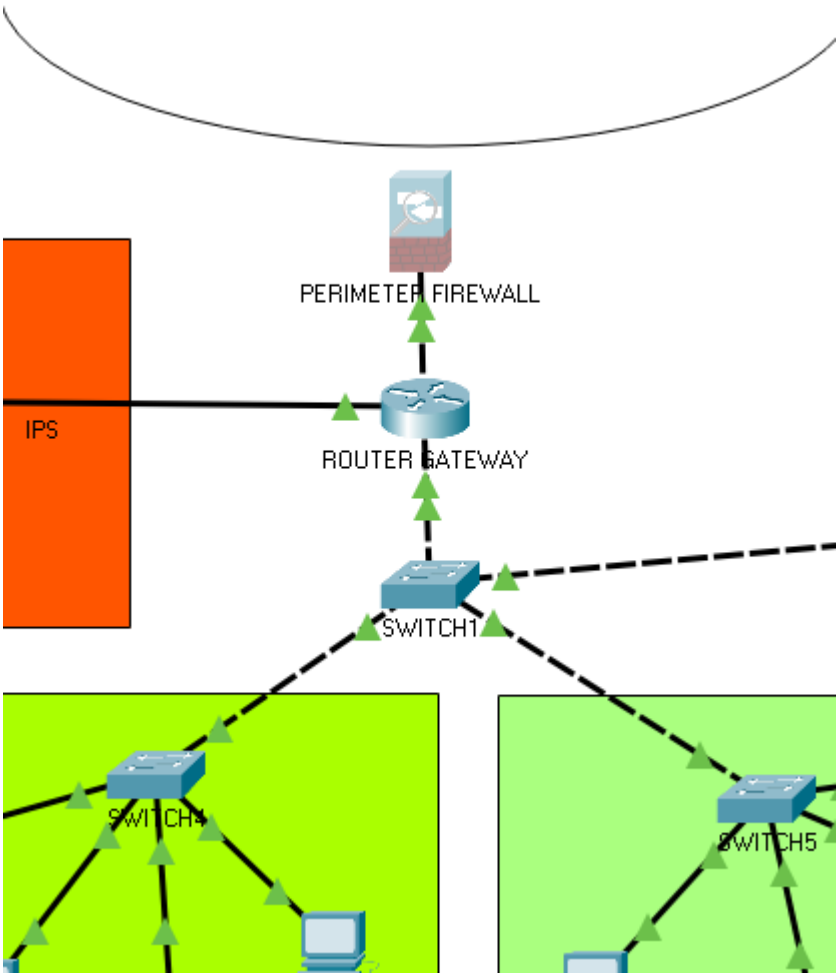
According to the requested project request I've created a network as show below:



As we can see I've been using the following devices:

- **Perimeter Firewall** - this allows to protect the network from the "outside" and it's the first obstacle that an intruder will face;
- **Router Gateway** - it allows to split the network among all the devices;
- Switches - as the word says itself they are used to "switch" the network among all the hosts;
- **IDS/IPS** (Intruction Detection System/Intruction Prevention System) - they will eventually give more protection to the Servers
- **DMZ** zone with:
    - Server SMTP;
    - Server web HTTP/S
- "**local management area**" with
    a. NAS Server - to store all the data
    b. Internal Server

Now let’s analyse everything better:

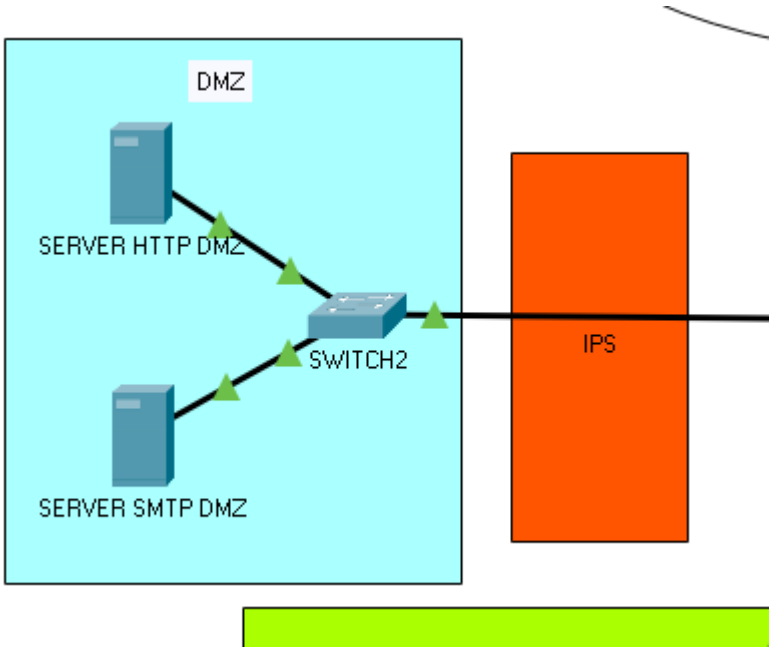


The first filter between us and the outside is the Perimeter Firewall.

As the word explains itself, this device is gonna **protect** “**ALL THE VIRTUAL PERIMETER**” of the network between our working space (**LAN**) and the outside space(**WAN**).

This device can also do the job of the Router, it depends on the infrastructural needs of the company (of course we will have a different setup according to the size of the company, size of the data we need to protect, kind of business).

In this case I decided to split the network in “private access” and “public access”.

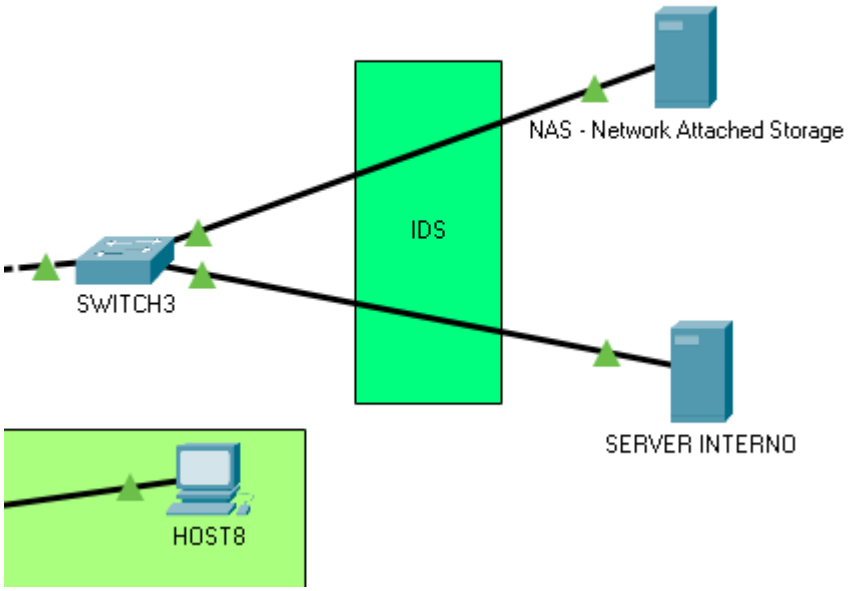


Here we have the so called **DMZ zone** (De-Militarized Zone).

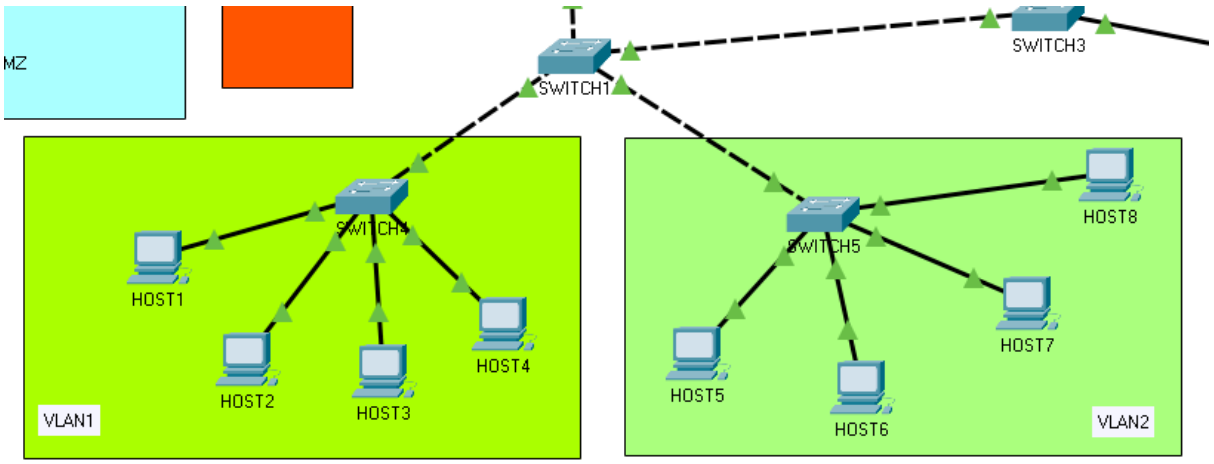
This area is accessible from the outside as it's public - the front end of all the jobs of the company - and it's the area where we find the HTTP Server and the SMTP server that allow, as we want, communication with the outside world.

Beyond the perimeter firewall here we can add an **IPS** (Intruction Prevention System) that is gonna send an alert to the security administrator and block the packet that it recognises as unsure.

There's the option to also use a **WAF**(Web Application Firewall) filtering the incoming requests. WAF is not only checking for IP addresses and ports, but it's also checking the data(packets) itself; it means it's gonna literally read all the code that is being received. Thanks to WAF we're gonna cover all the **7 layers of the ISO OSI protocol**.



The “private” network is already secured by the perimeter firewall and in this case we’re gonna add an **IDS**(Intrusion Detection System) - in this case the security administrator will receive only an alert when a packet is “suspicious”.
We don’t use an IPS because, in case, it will block the packet and since this area of the network is used by the “back end team” they always need to have access to the NAS and the main Server.
Ps - it may happen to get a “false positive” alert - that’s why we get only an alert.



Since safety is never enough I would also split the working network into **two different VLAN** (one can be used for the front end and one for the back end, for example) because, as we’ve learnt, the more we segment a network, the more it’s difficult to be attacked.

Antonio Bevilacqua