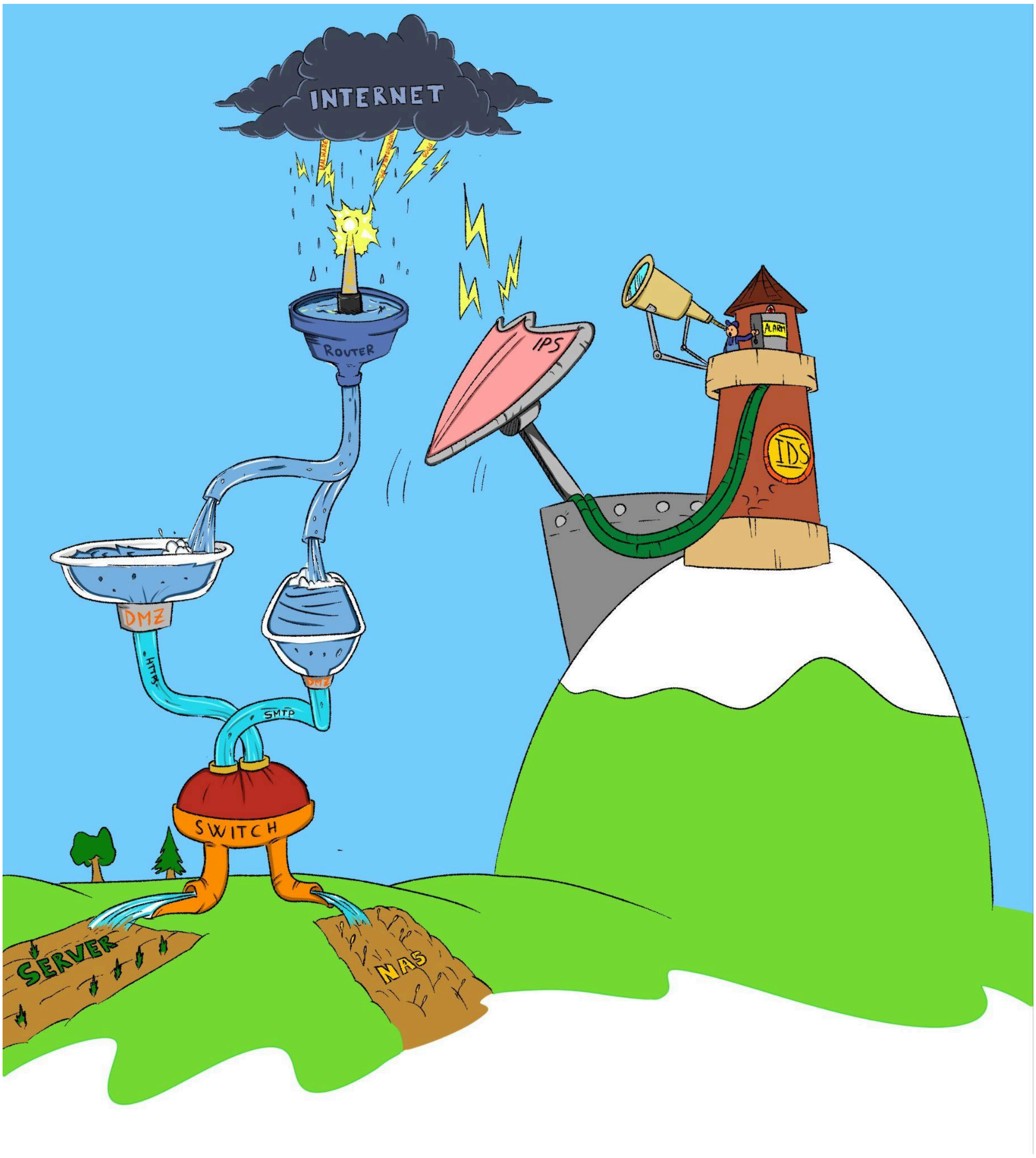
Project S3L5 - Visual Representation of a Network:

Today’s project asked us to provide a visual representation of a Network protected by a Firewall and IPS and IDS: the Network must include a DMZ as well, and at least a server or a NAS in an intranet. As I struggled to visualize these concepts myself, I decided to create an intuitive and metaphorical illustration to help the reader, who might be someone who’s completely unaware of how a network works, figure out more easily the concepts and parts of a protected Network. Here’s the illustration:



In my illustration, as requested, I represented the Internet as a cloud, but in this case it's an actual cloud: from global Internet we can request, through our router, connection for safe reception of useful and pertinent data, represented by the rain coming from the stormy cloud. By connecting ourselves though, we also expose ourselves to the numerous risks coming from the worldwide web: these can be represented by undesirable IPs, hidden malware in the downloaded data, DDoS attacks, and numerous more: the Firewall, after being configured to only let a certain range of IPs in, or to read PDU's to detect unusual activity, blocks these following the rules previously given. This is represented in my illustration with a lightning rod, catching all of the lightning bolts (which represent the malwares) before they reach our network.

As great of a safety measure the firewall is, it's not unfailable, as the rules for a firewall may lead to undetected threats: for this exact reason IPS (Intrusion Prevention System) and IDS (Intrusion Detection System) serve as an additional barrier between our network and any malevolent activity coming our way. IDS, by reading the traffic and the logs, detects at a deeper level the unusual activity that wasn't caught by the firewall and alerts the IPS which proceeds to receive the alert by blocking them further. I decided to represent them as an additional control tower handled by a security IDS officer alerting the IPS shield by raising it against potential threats. It's worth noting that the IPS can also act independently from the IDS, but generally this is how it works on most systems.

Once the information from the global web has been filtered by the firewall and the IDS and IPS, it gets transferred to the router: as previously mentioned, in our metaphor the safe data will be the rain. The rain flows through the router which correctly routes it as it would with the information to the second stage of our network: the DMZ. The DMZ acts as an intermediary part between the router and the intranet, and is isolated both for safety measures (as we already said in previous projects, a segmented network will always be more secure than a non-segmented one). In this case we have an HTTPS and an SMTP protocol working in the DMZ area, which will encrypt the data respectively from HTTPS websites (could be with an additional firewall or with proxy techniques) and from email messages (by using filtered and secure connections), and send it through a switch to our end-devices. This way, any public traffic is well isolated in the DMZ before being sent out to the intranet with the needed encrypting and filtered connections. Here it's represented by two additional tubs, gathering the water coming from the router; at the end of the tubs is a DMZ "filter" encrypting the messages and securing the desirable emails, clearing the water even further as evidenced by the colour of it, representing the clean data being transmitted to our end-devices.

The final part, after the DMZ, is our intranet composed of a switch and finally the end devices, the server and the NAS: the switch, with the aid of both ICMP and ARP requests we saw in previous modules, ensures that the information gets sent only to the correct devices by associating the IP address and the MAC address with the information contained in the received PDU's. Here it's visually represented by a final tank, collecting all of the clean "water data" received by the DMZ and routing it to the respective end devices, which in my illustration are two fields getting fed with the information they need to bear fruit, one being the NAS (which is mostly employed to store data, useful for file sharing) and the server (which can be employed for multiple reasons, such as hosting websites, web-apps etc.).