Purpose of Each Device

Layer 2 Switch

- Configured within virtual box network settings, not a VM.
- Allows communication/data transmission within the network.

Firewall

- Configured with OPNsense VM.
- Similar to a router, allows data transmission within different networks and uses IDS/IPS to make sure only permitted data transmission is allowed and block malicious activity.

Virtual Servers (Run as VMs)

- **Splunk/Elastic Monitoring -** SIEM tools that use log analysis from the device to capture any unauthorized activity and analyze possible vulnerabilities and threats.

- **Active Directory -** A database that maintains users, computers, groups, etc. Allowing experimentation with user permissions, policies, the traditional organization set up

- **Ubuntu** - Linux distribution OS, used in servers and security environments. Allows for comfortability with linux which is critical because most eneterprise servers run on Linux not windows.
    - You can use ubuntu to do anything from installing IDS/IPS (Suricata, Snort, Zeek)
    - Forwarding logs to a SIEM tool (Splunk)

    - Host webservers (Apache, Ngimx)
    - etc.

- **Email - Running a email server VM simulates the environment allowing monitoring, studying, and defending email traffic.**
    - Email is one of the biggest attack vectors in the real world (phishing, malware delivery, business email compromise...)

Virtual Clients (Run as VMs)

- **Windows** - The traditional windows operating system that can allow me to use it as a target machine do deploy malware for analysis, input logs through SIEM tools, and experiment attack results as a normal machine.
- **Kali Linux** - Operating System that offers preinstalled cybersecurity tools, a good recourse for learning through hands-on experiments.