**Day1: Creating a Logical Network Diagram using Draw.io**

One of the most important aspects of doing a security project is understanding the network one will be working with. To accomplish this, one of the foundational and most important steps is to create a diagram of the network.

**What is a Network Diagram?**

Simply put, a network diagram is a visual representation that shows the layout of a network, including devices, connections, and paths, to illustrate how data flows and communicates.

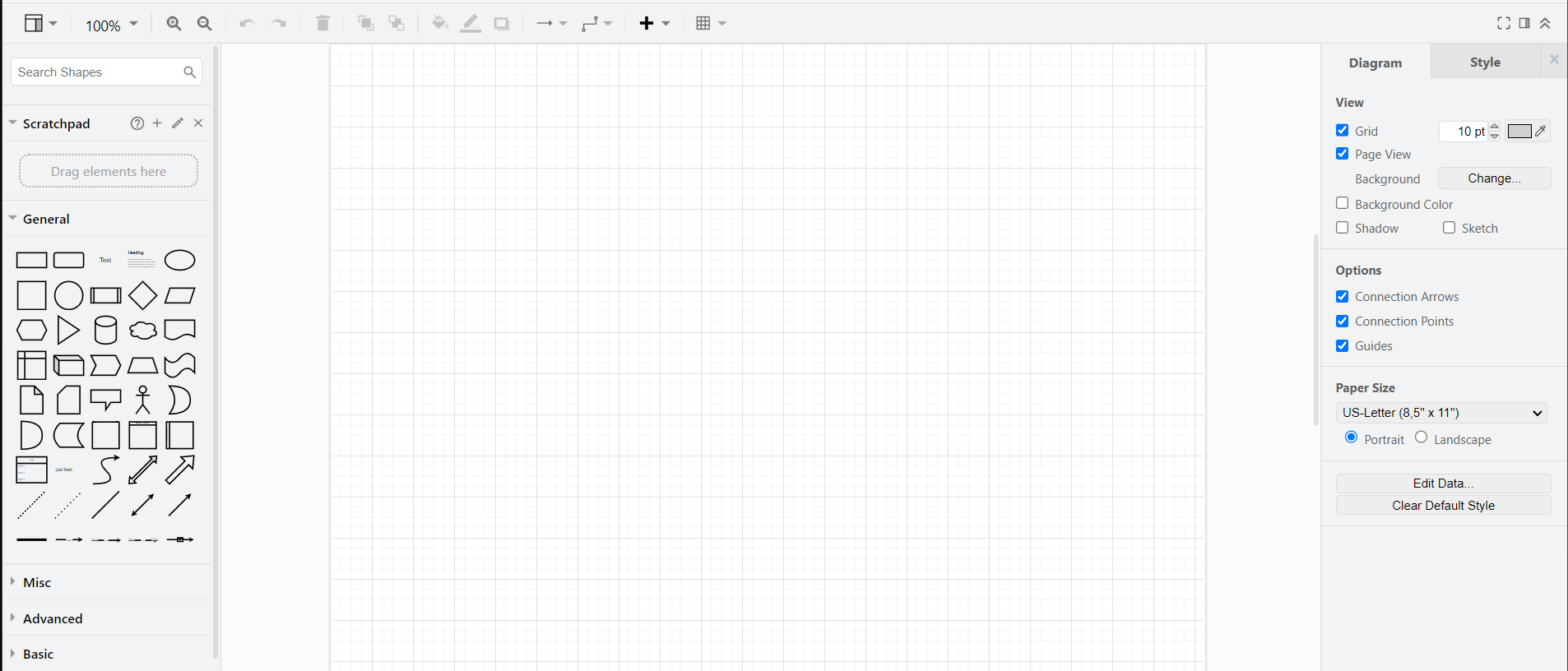
**Advantages of making a network diagram**

* **Visual Clarity**: Simplifies complex network structures, making them easier to understand.
* **Efficient Troubleshooting**: Helps quickly identify and resolve network issues.
* **Improved Planning**: Aids in designing and scaling networks effectively.
* **Documentation**: Serves as a valuable reference for network configurations and updates.
* **Enhanced Communication**: Facilitates clear communication among team members and stakeholders.
* **Security Management**: Helps identify vulnerabilities and plan security measures.
* **Resource Allocation**: Optimizes the use of network resources and hardware.

**Creating a Network Diagram for the 30-day SOC Challenge Draw.io**

Accessing Draw.io

draw.io is a free, web-based tool for creating diagrams, including network layouts and flowcharts. I navigated to their website at <https://app.diagrams.net/> and created a blank document:

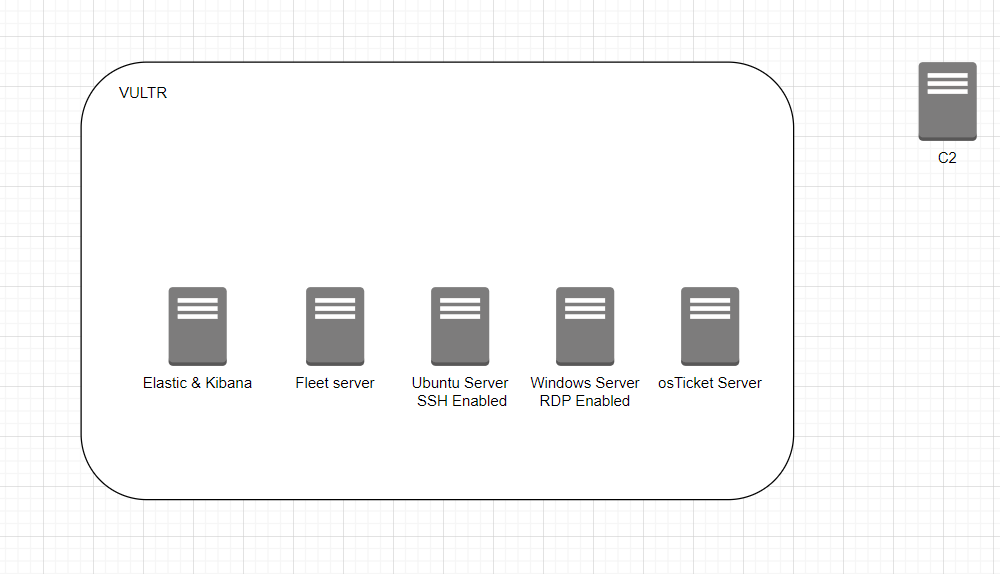


**Adding Servers**

On searching for servers on the left hand side, I picked one and duplicated them to create 6 servers, named as follows:

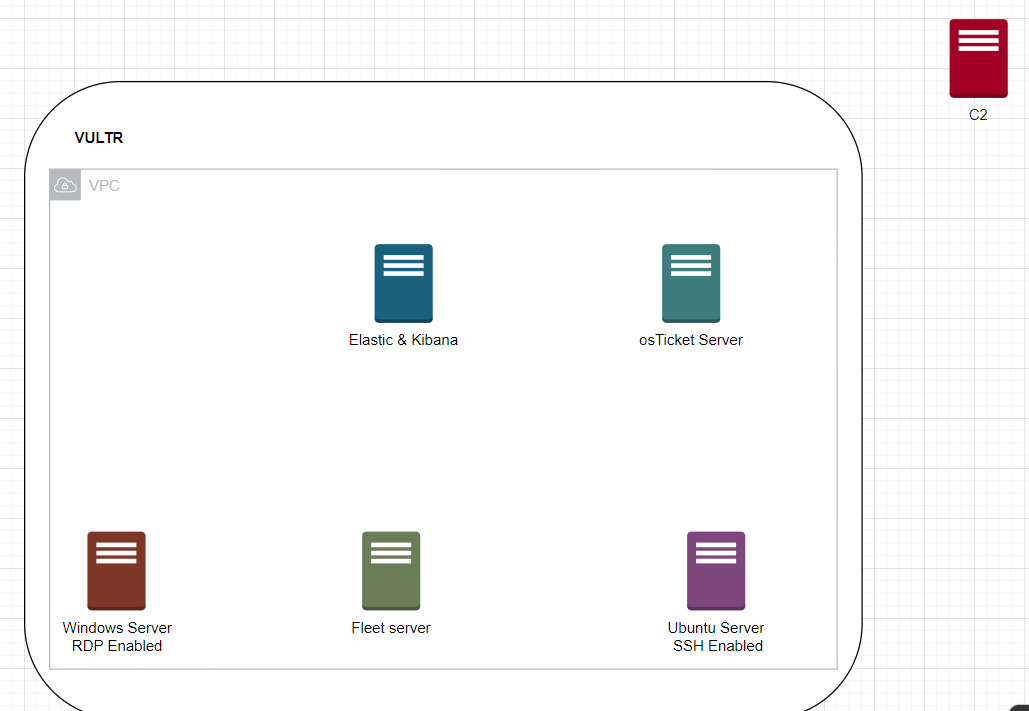
1. **Elastic & Kibana -** Elastic SIEM with Kibana for visualization.
2. **Windows Server -** Windows server 2022.
3. **Ubuntu Server -** Ubuntu Linux.
4. **Fleet Server -** A centralized management system for Elastic Agents.
5. **osTicket Server** - To generate and manage tickets.
6. **C2 (Command and Control) Server** - to be used by attacker machine to remotely manage and control compromised systems or networks. It is represented by red.

The roles of these servers will further be understood as the project goes on.



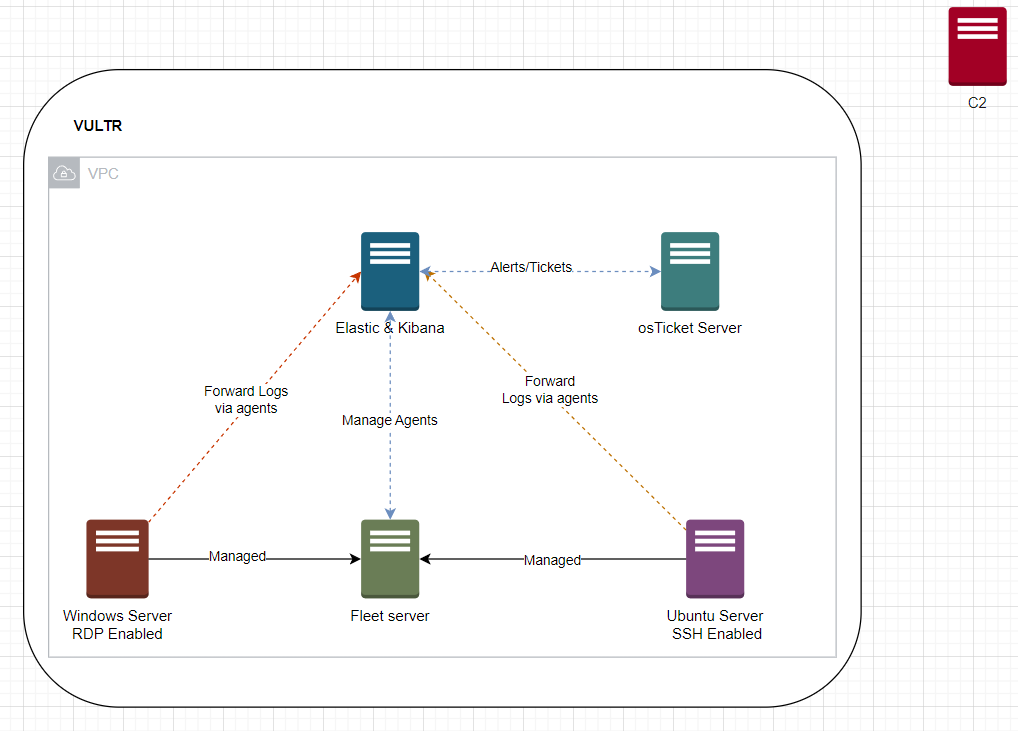
**Adding Servers to Virtual Private Cloud**

Since all the servers will be **Virtual Machines** (VMs) hosted on VULTR cloud, I added them to a **Virtual Private Cloud** (VPC). A VPC ensures that the servers will be part of the same private network while also being connected to the internet. I also formatted the layout and colors for better visual understanding.



**Establishing Network Relationships via Logical Flow Directions**

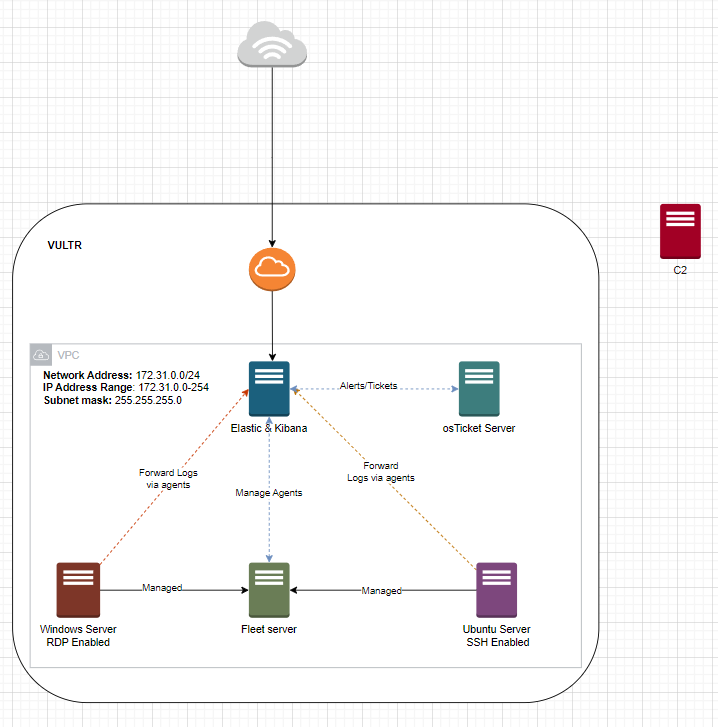
Using the arrows around every element of the network, flow relationships are specified and labelled as follows:



**Adding Internet Access and Network Details**

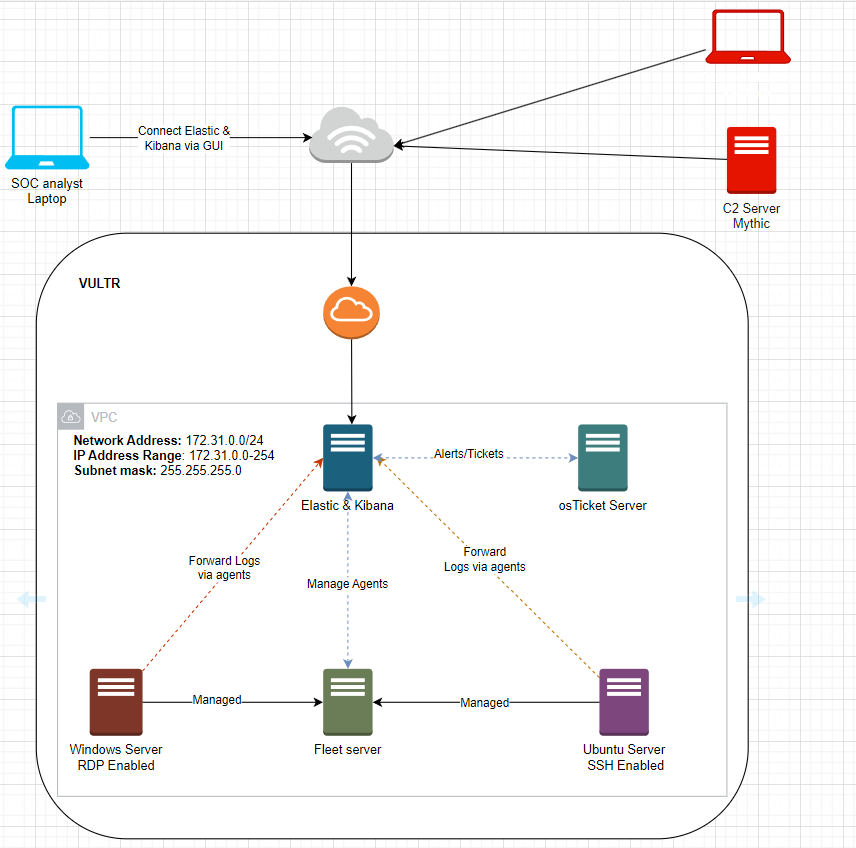
Once the internal relationships are established, a **Network Gateway** is added to the network to bridge its connection to the internet. An IP Address range is also specified with a corresponding subnet mask as follows:

* **Network Address:** 172.31.0.0/24
* **IP Address Range:** 172.31.0.1-254
* **Subnet Mask:** 255.255.255.0



**Adding Analyst and Attacker Machines**

As the final component, the project requires a machine to simulate a SOC Analyst as well as another machine to simulate the attacker. To achieve this, I added 2 laptops and labeled them accordingly. The machines will communicate with the network over the internet via Web GUI:



**Conclusion**

A Network Diagram was successfully created outlining the network component and the relationships between them. Day 1 of the SOC Analyst challenge is completed.