Architecture

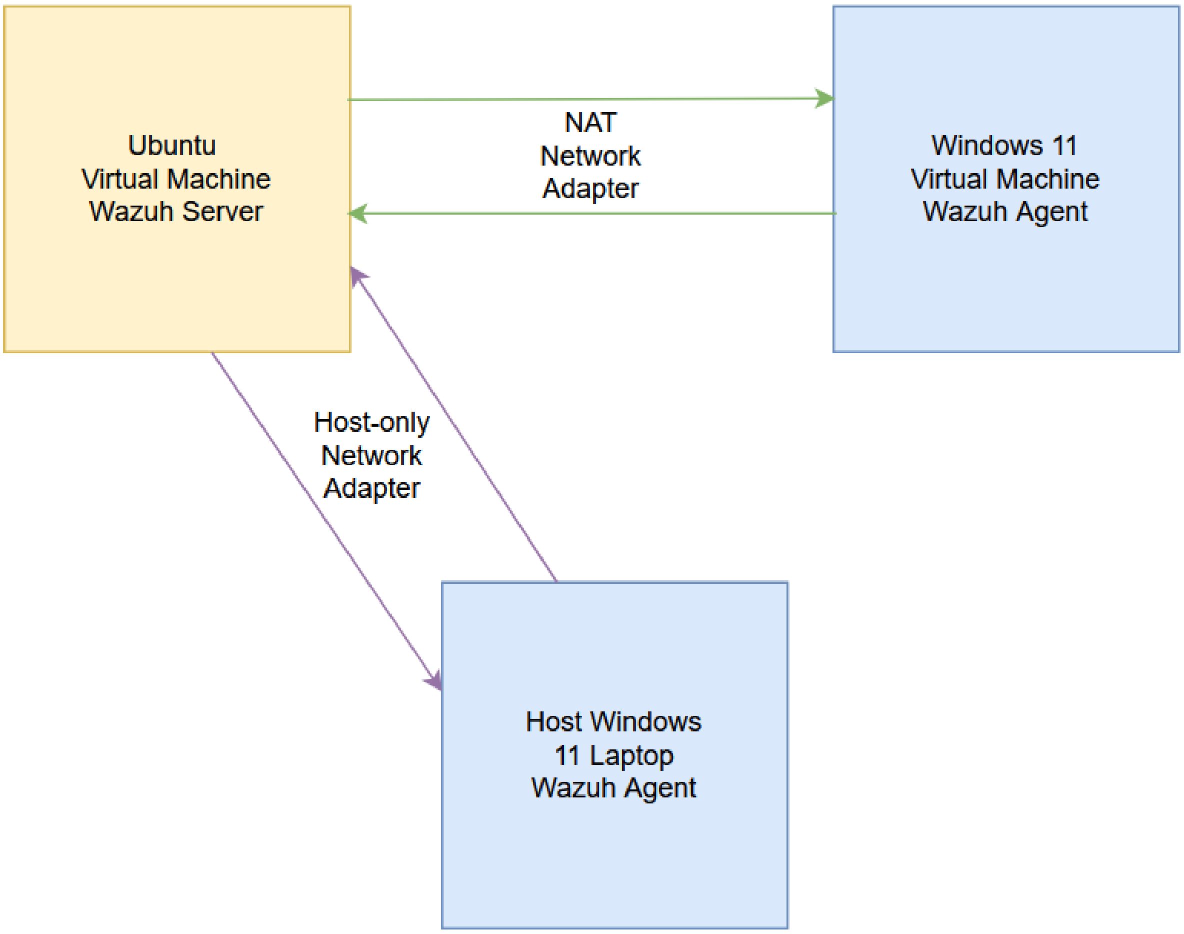

Figure 1: SIEM Environment Architecture

NAT Network Adapter- Used on both the Ubuntu and Windows 11 VM to allow for two-way communication between the two of them on their own network.

Host-only Network Adapter- Normally only allows for one-way communication from the host side, however using a firewall rule for inbound connections on the host for the VMs IP address allow for this to become a two-way connection. Used on the Ubuntu server VM

Two-way connections are required for the Wazuh server to enrol agents and communicate. The easiest solution to this would be using bridged adapters, which treats each VM as being on the same home network as the host machine as separate machines with different IP addresses. I started with this approach initially, however I had issues with the connections working consistently so I had to use alternative solutions.