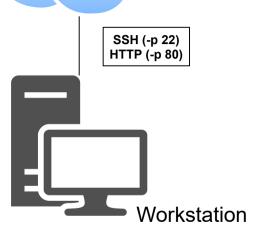
Red Team (Resource Group) Red Team (Virtual Network): 10.0.0.0/16 Red Team (Virtual Subnet): 10.0.0.0/24 TCP (-p 9200, 5601) Elk Virtual Network: 10.1.0.0/16 SSH (-p 22) Elk Virtual Subnet: Load Balancer Backend Pool 10.1.0.0/24 Elk Server: Peering (Elk-jumpMachine)
Elk Container: Web-1 Web-2 10.0.0.5 10.0.0.6 20.65.57.242 10.1.0.4 Jump-Box VM DVWA Ansible Containers Kibana Metricbeat SSH Public Key SSH Public Key Filebeat 10.0.04 (20.119.32.190) SSH Private Key TCP (-p 5601) Red Team Load Balancer (redteamLB1) 13.82.120.227 (static) ELK-jumpMachine-nsg **Security Group** SSH (-p 22) HTTP (-p 80) TCP (-p 5601) Internet



Security Rules:

- 1. Deny All Inbound Traffic
- 2. Allow Azure Load Balancer inbound
- 3. Allow VNET inbound
- 4. SSH: Allow SSH from my IPv4
- 5. SSH Jumpbox: Allow SSH from Jump-box IP
- 6. Port 5601: Allow TCP traffic over port 5601 to access

Kibana from ELK machine server

7. Port 80: Allow TCP Traffic over port 80