Azure Virtual Network Monitored VM Machines behind load balancer Е 10.0.0.7 DVWA Ubuntu 18.04 С VM 1 G w Docker Allow 99.26.181.143 to SSH В Jump Box into 52.188.65.605 Ubuntu 18.04 Α (jump box) Ansible Control Node 104.214.68.93 on Port 22 10.0.0.8 10.2.0.4 Whitelisted logs and Computer system metrics Internet Firewall ELK VM Azure NSG DVWA Ubuntu 18.04 Ubuntu 18.04 Allow 99.36.181.143 w Docker В VM 2 access to 40.117.158.16 w Docker via load balancer TCP on port 80 port 80 10.0.0.9 Firewall D Azure NSG Load Balancer DVWA Ubuntu 18.04 Allow 99.36.181.143 access to VM 3 http://104.214.68.93:5601/app/kibana#/home w Docker (ELK VM) F Firewall Azure NSG

Components A - E are part of the RedTeam Virtual Network
Components F-G are part of ELKStack Virtual network. The two communicate through
peerings that allow communication between the two virtual networks

- **A.** Whitelisted Computer with public IP 99.26.181.143
- 1. allowed access to the jump box via SSH @52.188.65.205 (public key stored on jumpbox)
- 2. allowed access to http://104.214.68.93:5601/app/kibana#/home via port 80
- 3. allowed access to http://40.117.158.16 via port 80

B. Red Team Firewall

Controls access to the red team virtual network with a load balancer with 3 DVWA VM machines

- 1. firewall rule to limit ssh access to jump box from 99.26.181.143 with public-private key verification
- 2. firewall rule to allow only 99.26.181.143 access to http://40.117.158.16 via port 80
- **C.** Jumpbox with Docker and Ansible installed used to update and install the 3 DVWA VM machines and ELK VM machine via ssh using private IP addresses and public-private key verification.
- **D.** Load Balancer provides redundancy and load balancing via the 3 DVWA VM machines. The three machines are provided the same Public IP address (40.117.158.16)
- E. 3 DVWA VM machines behind Load Balancer
- **F.** ELK Stack Firewall restricts ELKStack Vnet with ELK VM to only allow whitelisted computer to access http://104.214.68.93:5601/app/kibana#/home via port 80
- **G**. ELK Stack VM
- 1. access allowed via ssh through the jump box
- 2. access granted to whitelisted computer to

access http://104.214.68.93:5601/app/kibana#/home via port 80