Cloud Security Azure Deployment:

The below deployment implements multiple cloud approaches to deliver in a system implementation targeting to show case the below key system design approaches:

1. Use of Jump-box-provisioner, main purpose is managed and provision devices in different zones of security which hardens the management process.
2. Deploy of containers using ansible for multiple devices showing management technique with potential to scale at minimum management and provisioning effort.

Gliffy / ***Project_01_Cloud_Azure_Deployment, v6**

Azure Resource Group: Red-Team

Address Space IPV4: 10.0.0.0/16
RedTeamvNet:
Location: region1
Subnets: 10.0.0.0/24

Address Space IPV4: 10.1.0.0/16
Red-Team-2:
Location: region2
Subnets: 10.1.0.0/24

RedTeam-NSG
SSH:p22
ANY:p80

Internet

Azure Load Balancer
RedTeam-LB: 20.92.112.140 Fix IP
Public IP

52.243.75.218 Dynamic IP Public IP
ELK-Server

20.248.168.124 Dynamic IP Public IP

Public IP

jump-Box-Provisioner

docker

10.0.0.4 Fix IP Private
SSH:p22

On-Premise Workstation [Local Computer]

Ansible Control Node

Web-1 Web-2 Web-3

Elk-to-Red
Red-to-Elk

Private 10.1.0.4 Fix IP
SSH:p22

ELK Stack Container

DVWA Container | DVWA Container | DVWA Container
10.0.0.5 Fix IP Private | 10.0.0.6 Fix IP Private | 10.0.0.X Fix IP Private | **SSH:**p22

Elk-to-Red
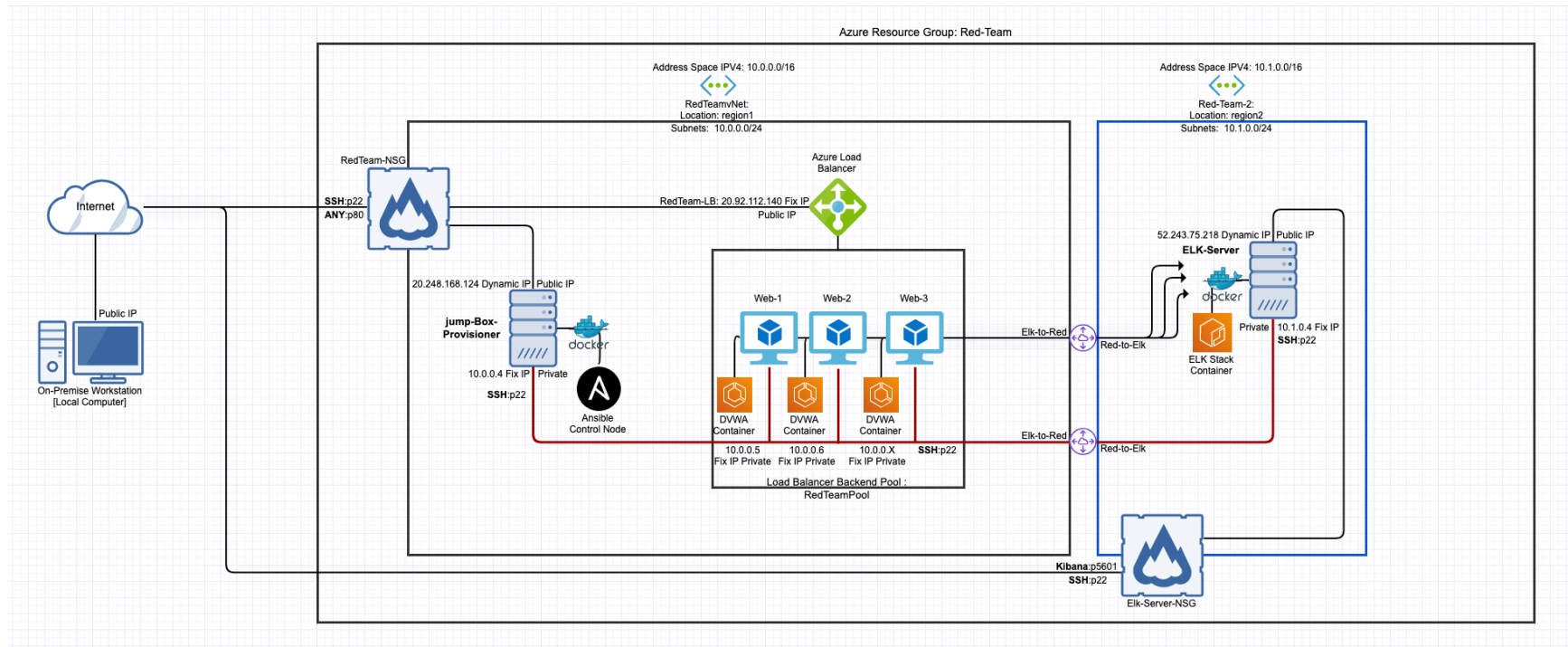Red-to-Elk

Load Balancer Backend Pool : RedTeamPool

Kibana:p5601
SSH:p22

Elk-Server-NSG

Figure 1 Security Cloud Azure Cloud