

# Azure - RedTeam Resource Group

RedTeam - Virtual Network: 10.1.0.0/16

Web Server: dvwa - Load Balancer Pool

Region: Australia South East

Subnet: 10.1.0.0/24

## Availability Set - WebSet

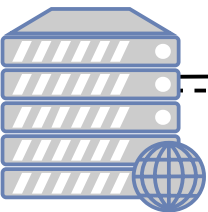
VM Web-1

NIC: web-1140

private IP: 10.1.0.5

dvwa - docker

container@37ab570b216b



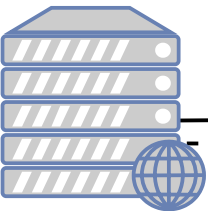
VM Web-2

NIC: web-2142

private IP: 10.1.0.6

dvwa - docker

container@38a7af4ca6d4



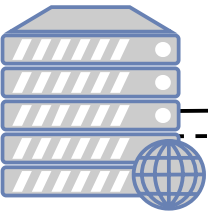
VM Web-3

NIC: web-361

private IP: 10.1.0.7

dvwa - docker

container @61eba526dbab



Allow - http (tcp port 80)

Allow - http (tcp port 80)

Allow - http (tcp port 80)

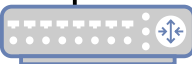
Load Balancer

RedTeam-LB

Public IP:

40.115.66.139

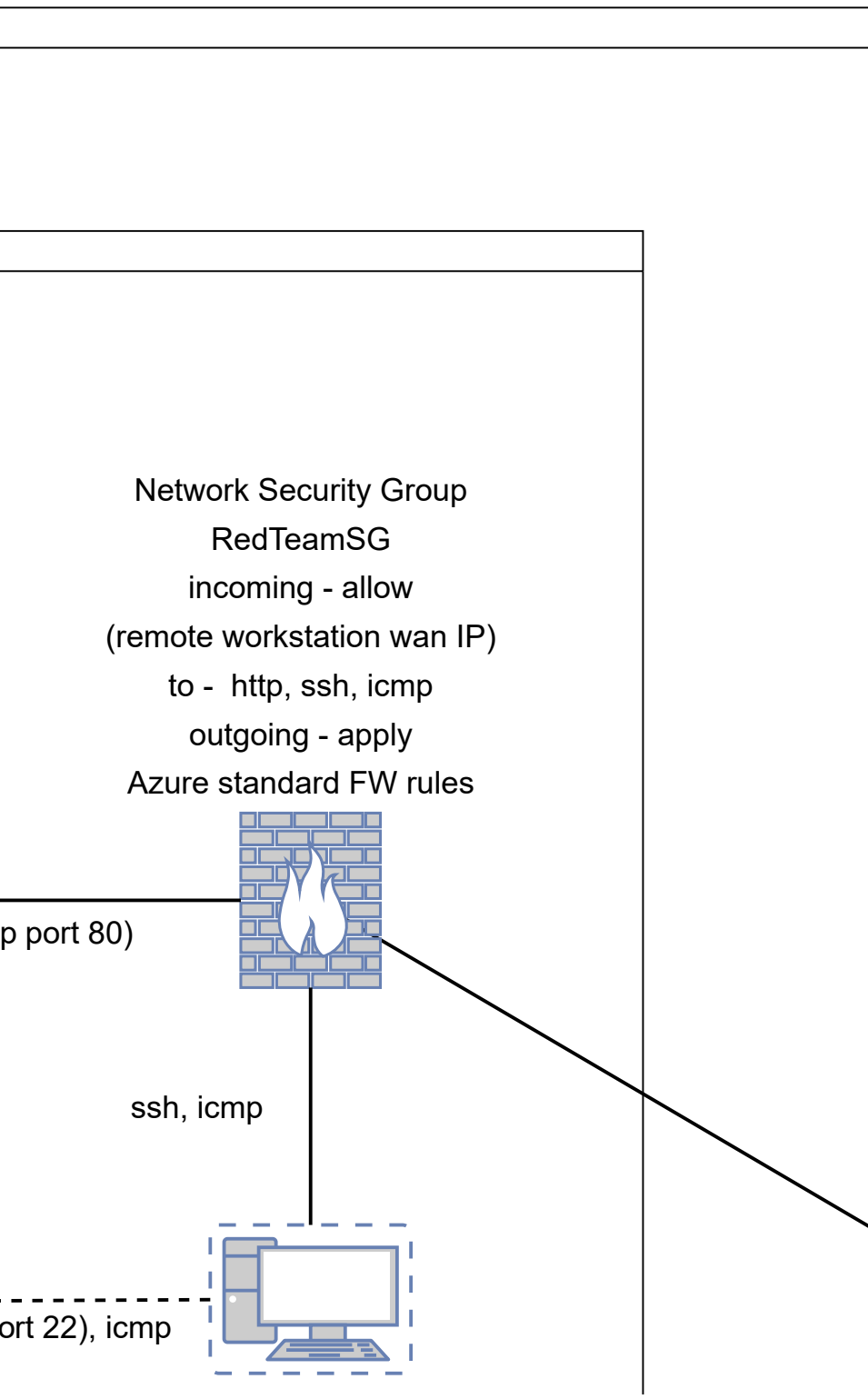
Allow - tcp 80 & icmp



Health Probe

Allow - http (tcp port 80)

Allow - ssh (tcp port 22)

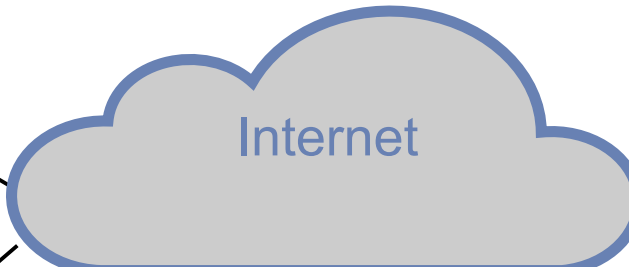


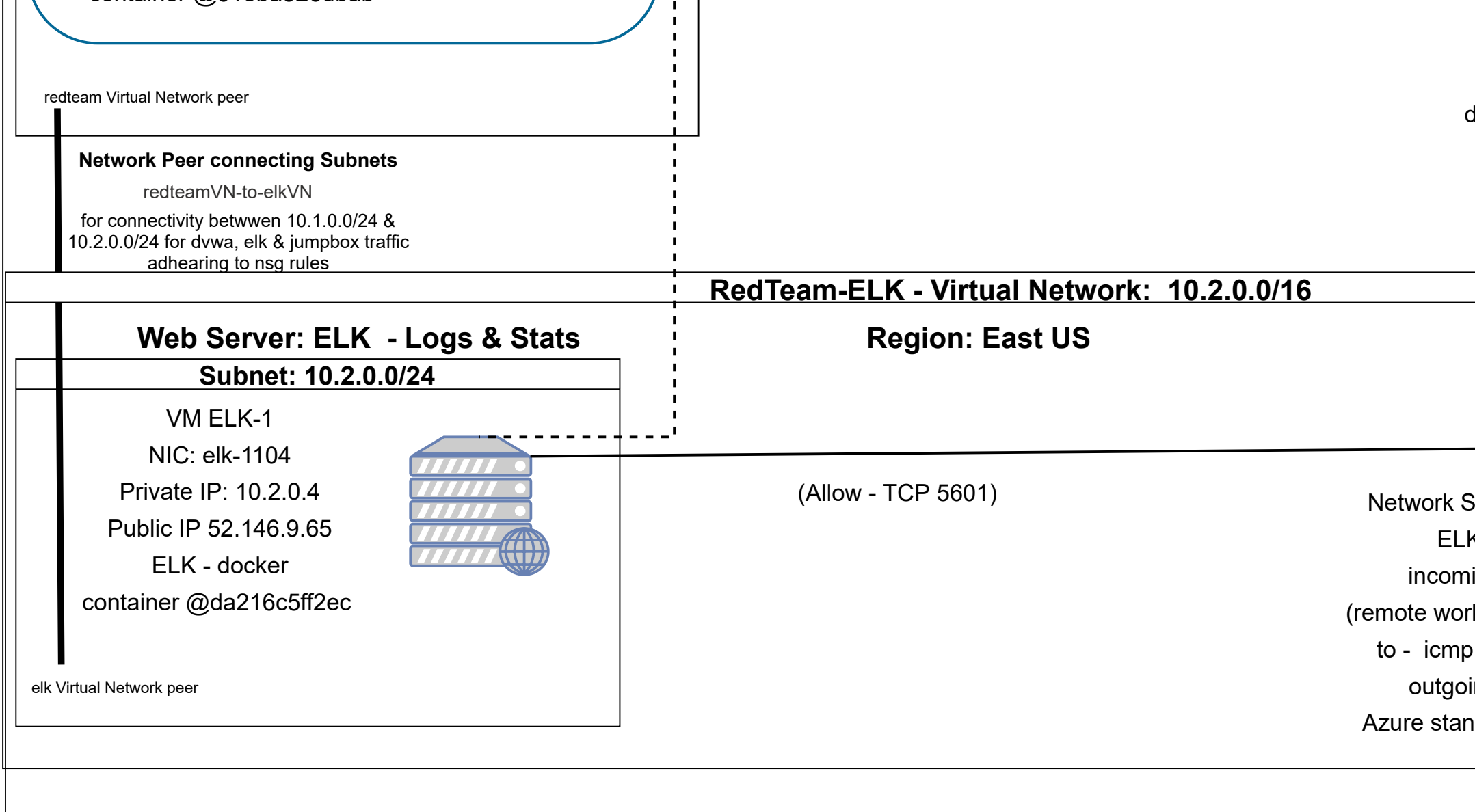
## Remote Workstation



Remote Modem  
wan link  
Public IP: Dynamic

Workstation connectivity  
Allow - ssh (tcp port 22)  
Allow - http (tcp port 80)  
Allow - tcp 5601  
Allow - ping (icmp)





#### Notes:

##### 1. Login access

1.1 JumpBox - UserID - azadmin - Password - Public key (remote work station)

##### 1.2 All RedTeam devices

docker - UserID - azadmin - Password - Public key (JumpBox)

ansible - UserID - ansible - Password - Public key (JumpBox (container @927333067dd3 (ansible)))

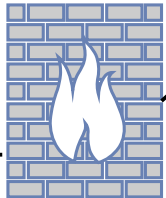
##### 2. RedTeamSG - NSG

Incoming rule - all incoming rules have source address of Remote work stations wan IP address.

##### 3. ELK-1\_-nsg - NSG

Incoming rule - all incoming rules have source address of Remote work stations wan IP address.

VM- Jump Box - Provisioner  
Private IP: 10.1.0.4 Static  
Public IP 40.115.65.102 Static  
locker container - @927333067dd3  
ansible  
Admin User: azadmin  
auto shutdown - every midnight



Security Group  
K-1-nsg  
ng - allow  
kstation wan IP)  
& TCP 5601  
ng - apply  
dard FW rules



**08/03/2021  
Martin Hills  
Home Work 14  
Monash Cyber Security boot camp  
Final V1.0**

**Peer Review Sign off  
Name:  
Date:**

Incoming rule - all incoming rules have source address of Remote work stations wan IP address.

### 3. Servers/PC's

**Jump-Box-Provisioner**, Web1, 2 &3

**hdw size: Standard\_B1s** (Standard B1s (1 vcpus, 1 GiB memory)

**sfw os:** Linux (ubuntu 18.04) all boxes

**Docker** - 19.03.06

**Ansible** - 2.9.2

