YAML is the program that is read by Ansible

DVWA is the web application to test vulnerabilities and for penetration testing

KUBERNETES is an open-source container-orchestration system for automating computer application deployment, scaling, and management

DOCKER is a set of platforms as a service product that use OS-level virtualization to deliver software in packages called containers.

ANSIBLE is an open-source software provisioning, configuration management, and application-deployment tool enabling infrastructure as code.

ACTIVITY : INSTALL yml in a container and enable and run the webserver to access port 80

root@c1e0a059c0b0:/etc/ansible# ansible.cfg

remote\_user : sysadmin

root@c1e0a059c0b0:/etc/ansible# vi hosts (or nano hosts)

[webservers]

## alpha.example.org

## beta.example.org

## 192.168.1.100

## 192.168.1.110

10.0.0.6 ansible\_python\_interpreter=/usr/bin/python3

10.0.0.5 ansible\_python\_interpreter=/usr/bin/python3

Where ‘webserver’ is the cname of 10.0.0.6 and 10.0.0.5

root@c1e0a059c0b0:~# nano my-playbook1.yml

---

- name: Config Web VM with Docker

hosts: webservers

become: true

tasks:

- name: docker.io

apt:

name: docker.io

state: present

- name: Install pip

apt:

name: python3-pip

state: present

- name: Install Docker python module

pip:

name: docker

state: present

- name: download and launch a docker web container

docker\_container:

name: dvwa

image: cyberxsecurity/dvwa

state: started

published\_ports: 80:80

Where :

pip is a de facto standard package-management system used to install and manage software packages written in Python.

DVWA is a PHP/MySQL web application, whose main goal is to be an aid for security professionals to test their skills and tools in a legal environment.

hosts: webservers – is the cname of the hosts inside the webservers located in etc/ansible/hosts

cyberxsecurity/dvwa – is the image repository from the Docker hub

docker.io – is the package name to run docker images in linux

root@c1e0a059c0b0:~# ansible-playbook my-playbook1.yml

PLAY [Config Web VM with Docker] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

TASK [Gathering Facts] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ok: [10.0.0.6]

ok: [10.0.0.5]

TASK [docker.io] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ok: [10.0.0.6]

ok: [10.0.0.5]

TASK [Install pip] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ok: [10.0.0.6]

ok: [10.0.0.5]

TASK [Install Docker python module] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ok: [10.0.0.5]

ok: [10.0.0.6]

TASK [download and launch a docker web container] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ok: [10.0.0.6]

ok: [10.0.0.5]

PLAY RECAP \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

10.0.0.5 : ok=5 changed=0 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0

10.0.0.6 : ok=5 changed=0 unreachable=0 failed=0 skipped=0 rescued=0

TEST and PUBLISH port 80 on Both Web1 and Web2 server

First, login to jumpbox where the ansible is rooted

ssh -i id\_rsa [sysadmin@52.242.18.55](mailto:sysadmin@52.242.18.55)

root@c1e0a059c0b0:~# ssh sysadmin@10.0.0.6

sysadmin@Web1:~$ curl localhost/setup.php

root@c1e0a059c0b0:~# ssh sysadmin@10.0.0.5

sysadmin@Web2:~$ curl localhost/setup.php

CREATE A LOAD BALANCER AND CREATE A RULE

1. CREATE : FROM AZURE WEB APPLICATION > GO TO HOME > LOAD BALANCERS > make sure it is dynamic and public.

FIGURE showing the structure on creating load balancer

JUMP BOX SEVER with

ANSIBLE ROOT

WEB 1

WEB 2

Load Balancer

Cache

Cache

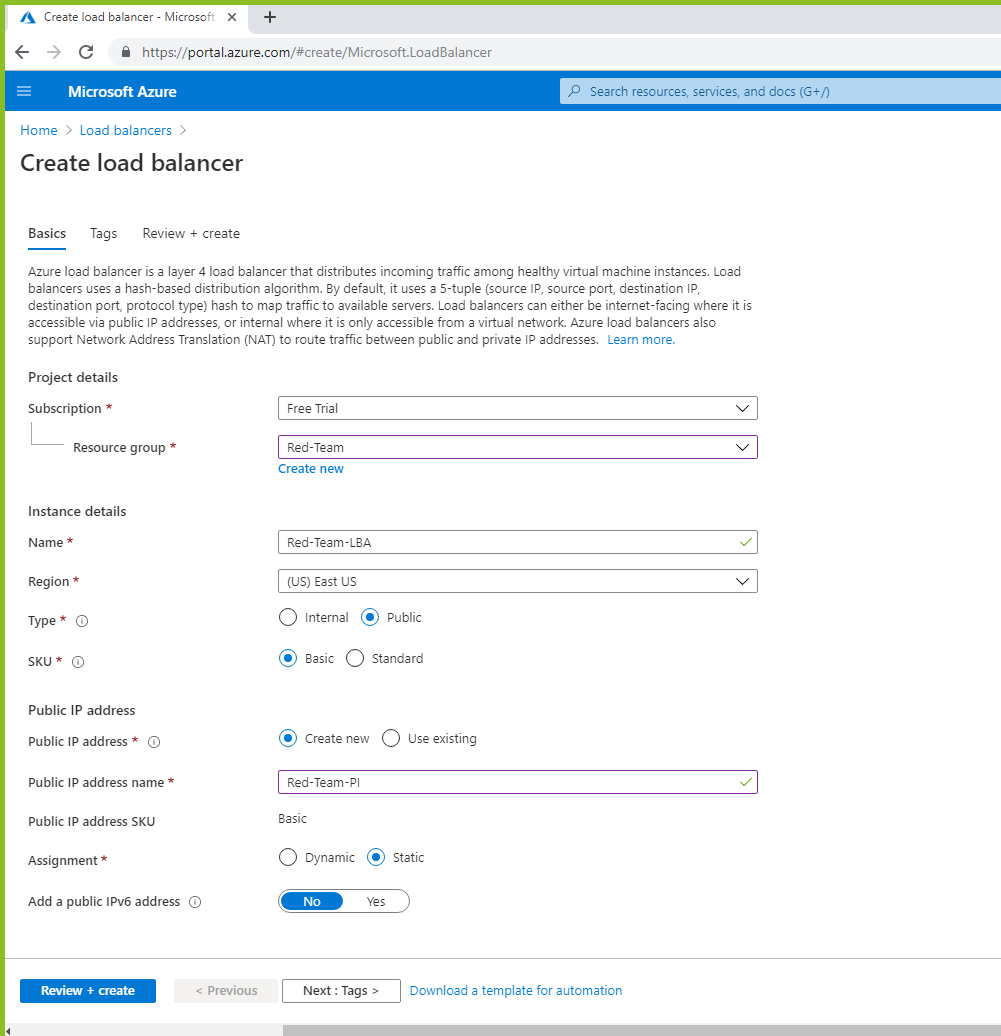
Load Balancer

Web Application Firewall (WAF)

ssh

Public IP

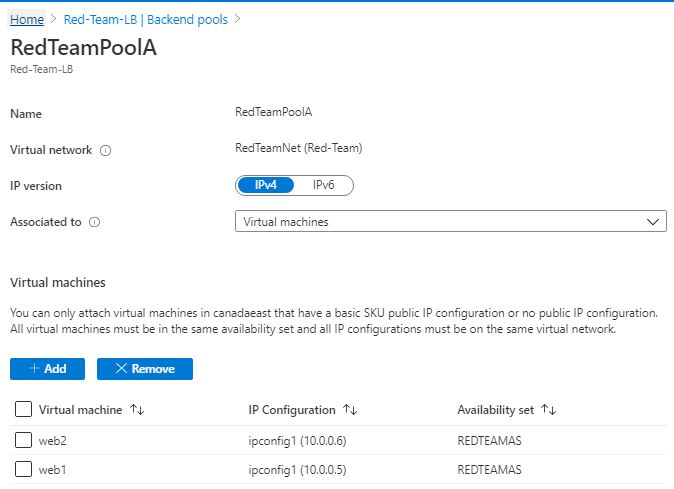
12



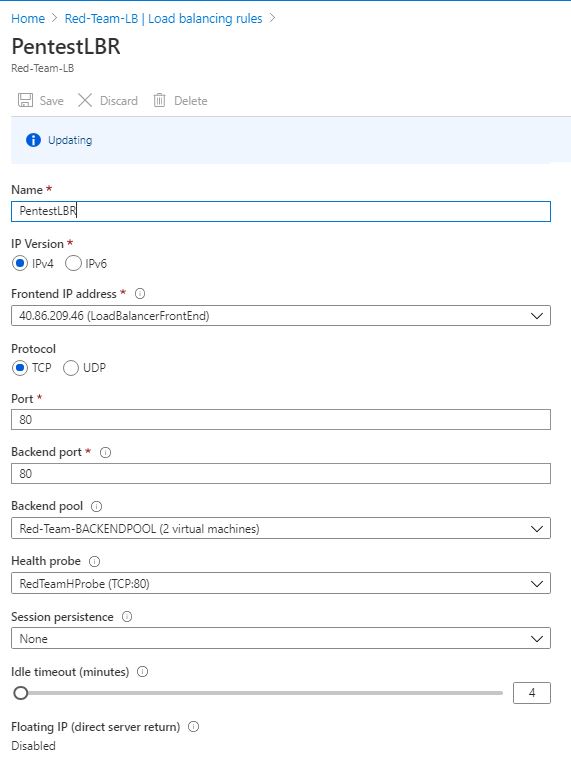
2. ADD HEALTH PROBE

AZURE > RED-TEAM-LB > Health Probe



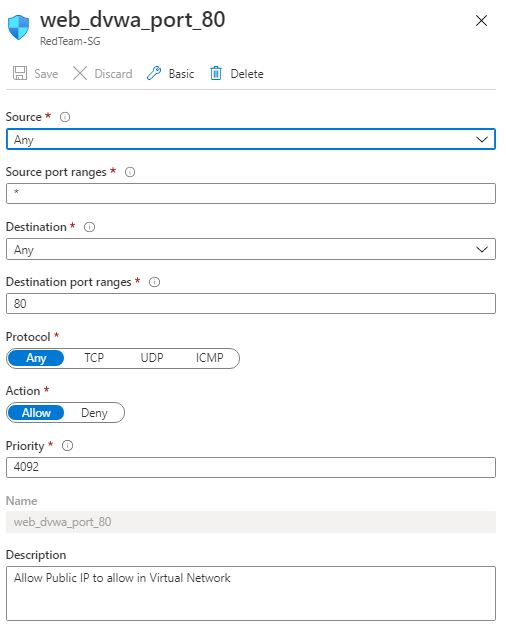
3. ADD BACKEND POOL

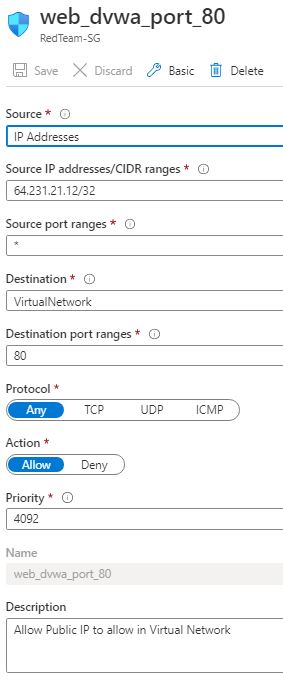
4. ADD LOAD BALANCING RULE



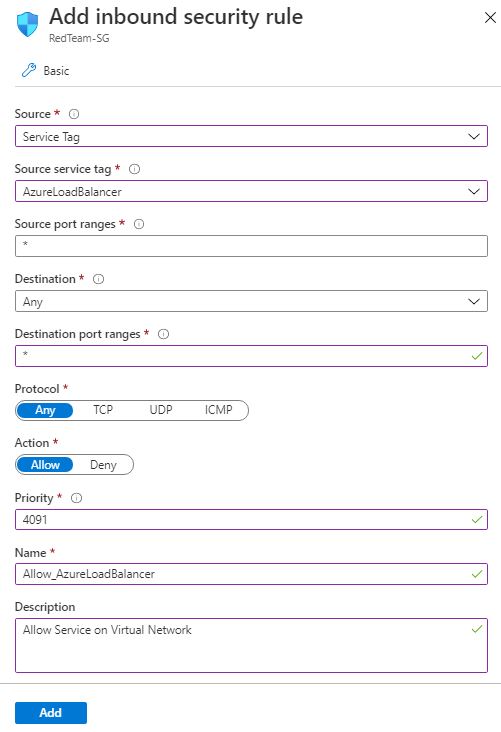
NOTE: This figure is the Cloudfare CIDR IPV4 and IPV6 List for PUBLIC IPs in cloud

5 . CREATE A FIREWALL FOR TESTING

 PRODUCTION TESTING



ALLOW AZURLOADBALANCER SERVICE

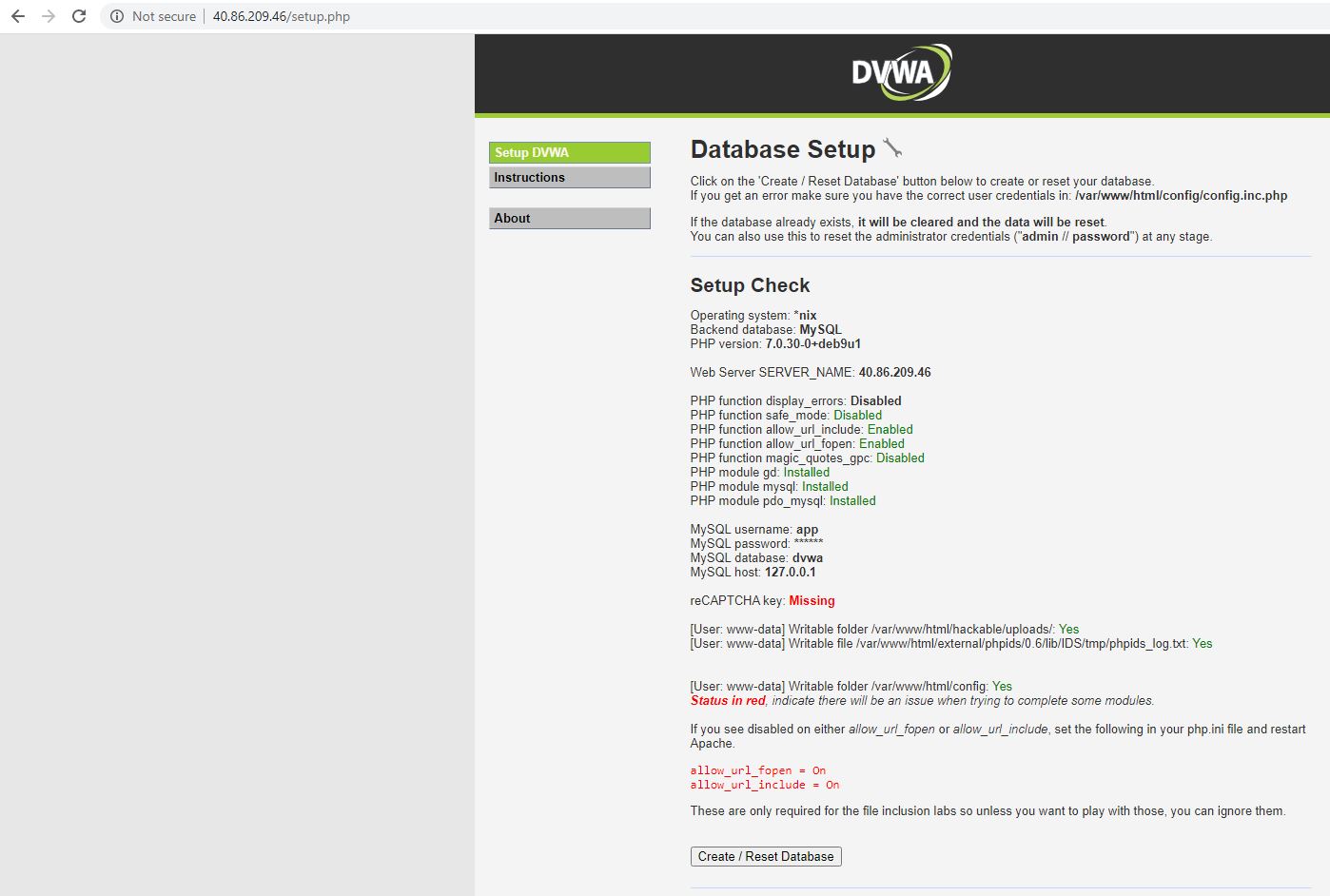


Change the Destination to VirtualNetwork .

Just change the Destination Port Range : 80 and 443 in separate rule.

6. Test the DVWA on Load Balancer Public IP address

<http://40.86.209.46/setup.php>

  
THIS IS THE RESULT FOR SETTING TESTING it WONT WORK IN PRODUCTION SETTING (MEANS SAFE)