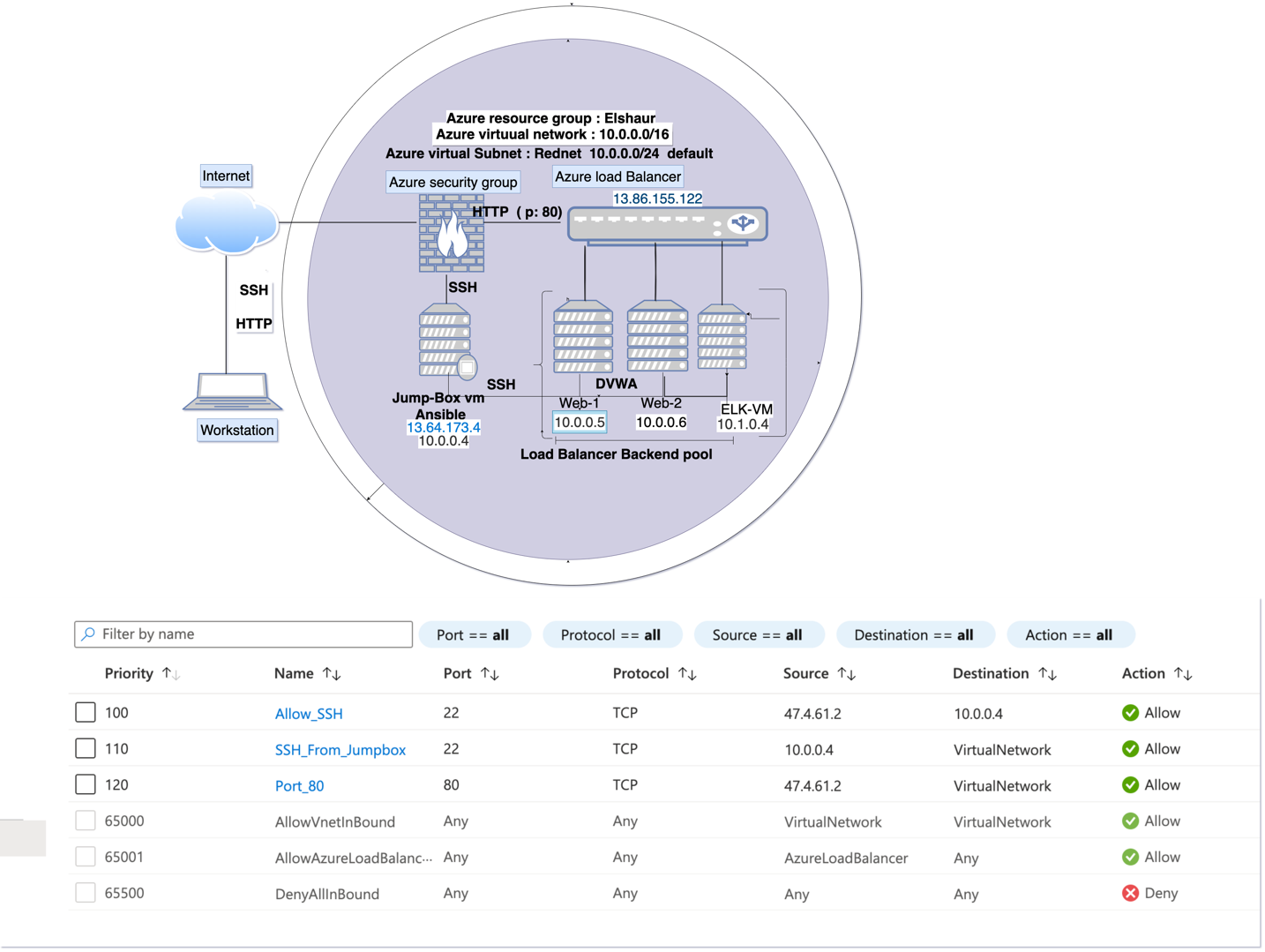
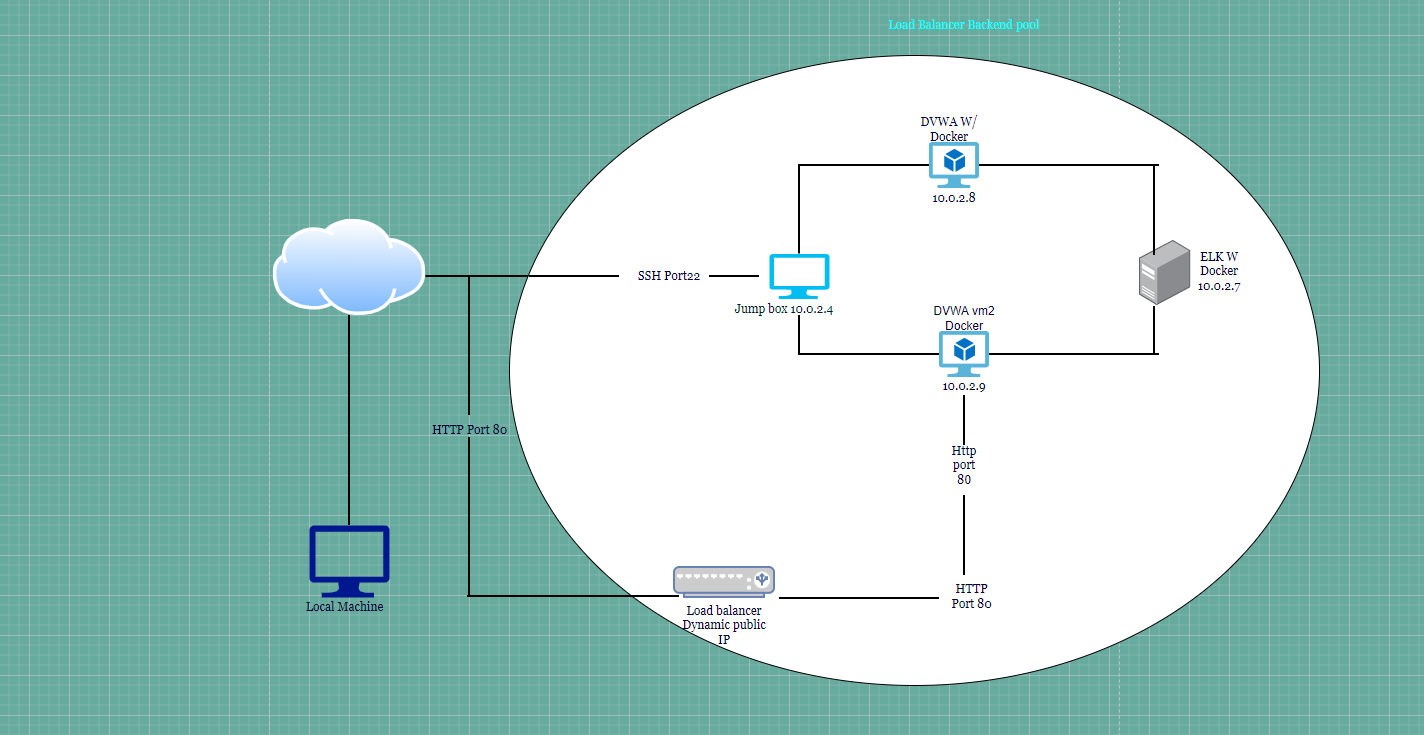
## Automated ELK Stack Deployment



These files have been tested and used to generate a live ELK deployment on Azure. Alternatively, select portions of the playbook file may be used to install only certain pieces of it, such as Filebeat.

FIlebeat

Filebeat-playbook.yml

---

- name: installing and launching filebeat

hosts: webservers

become: yes

tasks:

- name: download filebeat deb

command: curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.1-amd64.deb

- name: install filebeat deb

command: dpkg -i filebeat-7.6.1-amd64.deb

- name: drop in filebeat.yml

copy:

src: /etc/ansible/files/filebeat-config.yml

dest: /etc/filebeat/filebeat.yml

- name: enable and configure system module

command: filebeat modules enable system

- name: setup filebeat

command: filebeat setup

- name: start filebeat service

command: service filebeat start

- name: enable service filebeat on boot

systemd:

name: filebeat

enabled: yes

### Description of the Topology

The main purpose of this network is to expose a load-balanced and monitored instance of DVWA, the D\*mn Vulnerable Web Application.

Load balancing ensures that the application will be highly available, in addition to restricting access to the network.

* Load balancers play a very important role in cybersecurity. The load balancer has an off-loading function which defends an organization against distributed denial of service also known as (DDoS). The benefit of using a jump box is that your virtual machines are protected from the outside world. Meaning that you are not exposed to everyone.

Integrating an ELK server allows users to easily monitor the vulnerable VMs for changes to the log files and system perfomance.

According to a source named Elastic, the writer states “Filebeat is a lightweight shipper for forwarding and centralizing log data. Installed as an agent on your servers, Filebeat monitors the log files or locations that you specify, collects log events, and forwards them either to Elasticsearch or Logstash for indexing”.

Metrobeat helps with monitoring your servers by collecting metrics from the system.

The configuration details of each machine may be found below.

\_Note: Use the [Markdown Table Generator](http://www.tablesgenerator.com/markdown\_tables) to add/remove values from the table\_.

| Name | Function | IP Address | Operating System |

|----------|----------|------------|------------------|

| Jump Box | Gateway | 10.0.0.4. | Linux ubuntu 18.4|

| Web-1 | VM | 10.0.0.5 | Linux ubuntu 18.4|

| Web-2 | VM | 10.0.0.6 | Linux ubuntu 18.4|

| ELK-VM | VM | 10.1.0.4 | Linux ubuntu 18.4|

### Access Policies

The machines on the internal network are not exposed to the public Internet.

Only the Jumpbox machine can accept connections from the Internet. Access to this machine is only allowed from the following IP addresses:

* [13.64.173.4](https://portal.azure.com/#blade/HubsExtension/ResourceMenuBlade/id/%2Fsubscriptions%2Fd5b4fcb6-4eee-4b1b-8ff0-3ca440a963af%2FresourceGroups%2FElshaur-RG%2Fproviders%2FMicrosoft.Network%2FpublicIPAddresses%2FJump-Box-Provisioner-ip/menuid/configuration)

Machines within the network can only be accessed by port 22.

A summary of the access policies in place can be found in the table below.

| Name | Publicly Accessible | Allowed IP Addresses |

|----------|---------------------|----------------------|

| Jump Box | No | 10.0.0.4 |

|vm-1&vm-2 | No | |

|ELK vm | No | |

### Elk Configuration

Ansible was used to automate configuration of the ELK machine. No configuration was performed manually, which is advantageous because...

* Ansible simplifies your work, it is flexible which means it can be ran everywhere and more importantly ensures that provisioning scripts run the same.

The playbook implements the following tasks:

* Change the memory on the ELK VM
* Install docker.io
* Install python-pip
* Install docker python module
* Download and launch a docker elk stack

The following screenshot displays the result of running `docker ps` after successfully configuring the ELK instance.

Text

Description automatically generated

### Target Machines & Beats

This ELK server is configured to monitor the following machines:

* 10.0.0.4
* 10.0.0.5
* 10.0.0.6
* 10.1.0.4

We have installed the following Beats on these machines:

* Filebeat-7.6.1-amd64.deb

These Beats allow us to collect the following information from each machine:

* FIlebeat sends logs to Kibana. Furthermore, it collects and monitors log events on specific servers.

### Using the Playbook

In order to use the playbook, you will need to have an Ansible control node already configured. Assuming you have such a control node provisioned:

SSH into the control node and follow the steps below:

- Copy the Filebeat-configuration file to ELK VM.

- Update the hosts file to include webservers, 10.0.0.5, 10.0.0.6, 10.1.0.4

- Run the playbook, and navigate to Kibana to check that the installation worked as expected.

The specific commands the user will need to run to download the playbook, update the files, etc.\_

$ansible-playbook filebeat-playbook.yml

Graphical user interface, text, application

Description automatically generated