Load Balancing
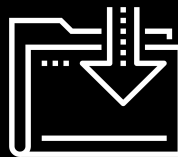
Class Objectives

By the end of today's class, you will be able to:
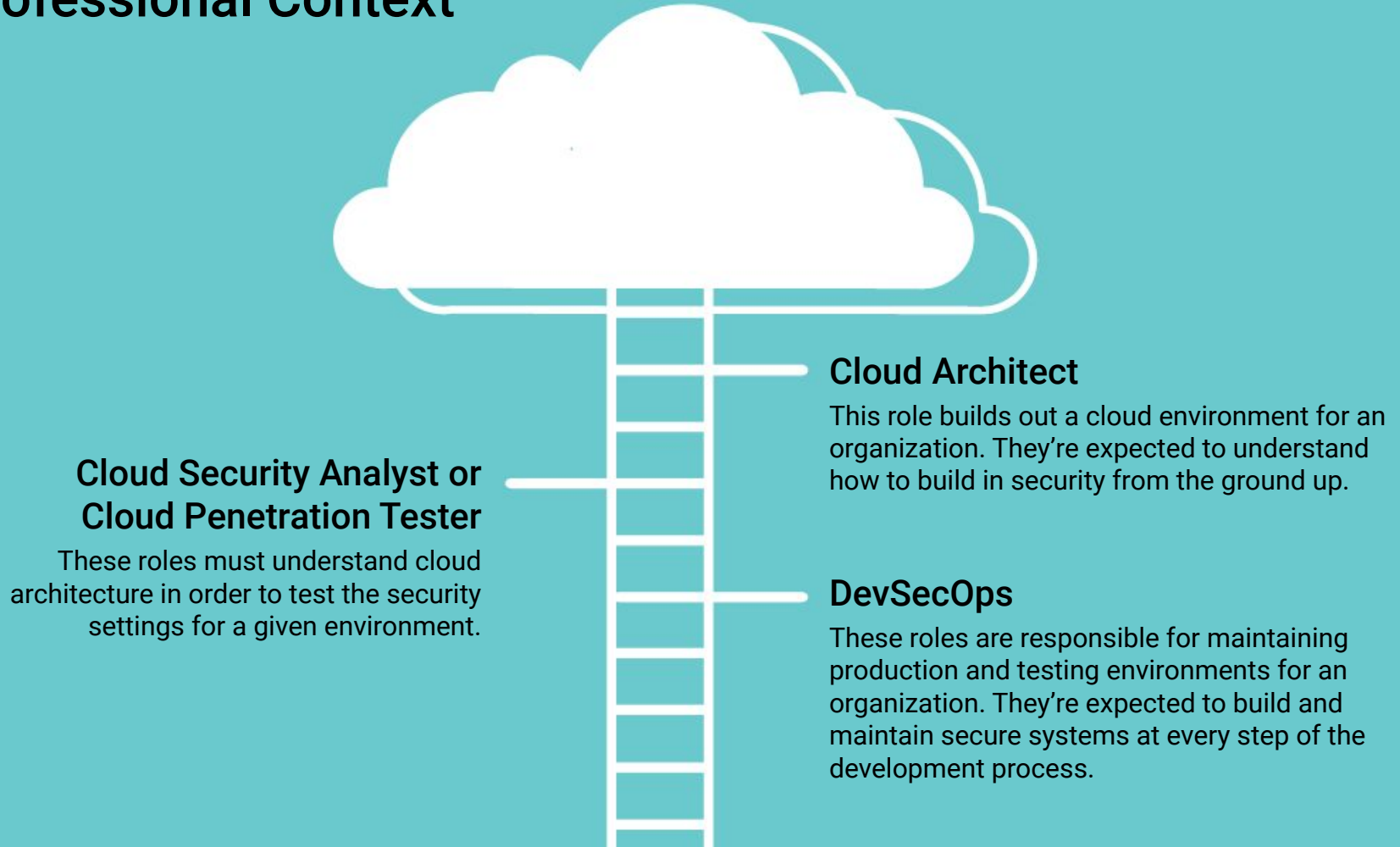
Create an Ansible Playbook to configure VMs.

Create a load balancer on the Azure platform.

Create firewall and load balancer rules to allow traffic to the correct VMs.

Professional Context

Cloud Architect

This role builds out a cloud environment for an organization. They're expected to understand how to build in security from the ground up.

Cloud Security Analyst or Cloud Penetration Tester

These roles must understand cloud architecture in order to test the security settings for a given environment.

DevSecOps

These roles are responsible for maintaining production and testing environments for an organization. They're expected to build and maintain secure systems at every step of the development process.

Ansible Playbooks

We have implemented a jump box that is running an Ansible container.

The Ansible container has full access to our VNet and can connect with our new VM. Now we will write code that will be "infrastructure as code" for this vulnerable web server.

Ansible reads YAML code.

stands for

YAML **A**in't **M**arkup **L**anguage

and is designed to be readable and simple to use.

YAML

Today, we'll start with a guided tour of YAML.

```yaml
---
  - name: My first playbook
    hosts: webservers
    become: true
    tasks:

    - name: Install apache httpd  (state=present is optional)
      apt:
        name: apache2
       state: present
```

Instructor Demonstration

YAML Guided Tour

Activity: Ansible Playbooks

In this activity, you will create an Ansible playbook that installs Docker and configures a VM with the DVWA web app.

Suggested Time:

25 Minutes

Time's Up! Let's Review.

Questions?

Load Balancing

Load Balancing

So far, we have:

Created a Vnet.

Deployed a jump box running an Ansible Docker container.

Used that container to configure another VM running a DVWA container.
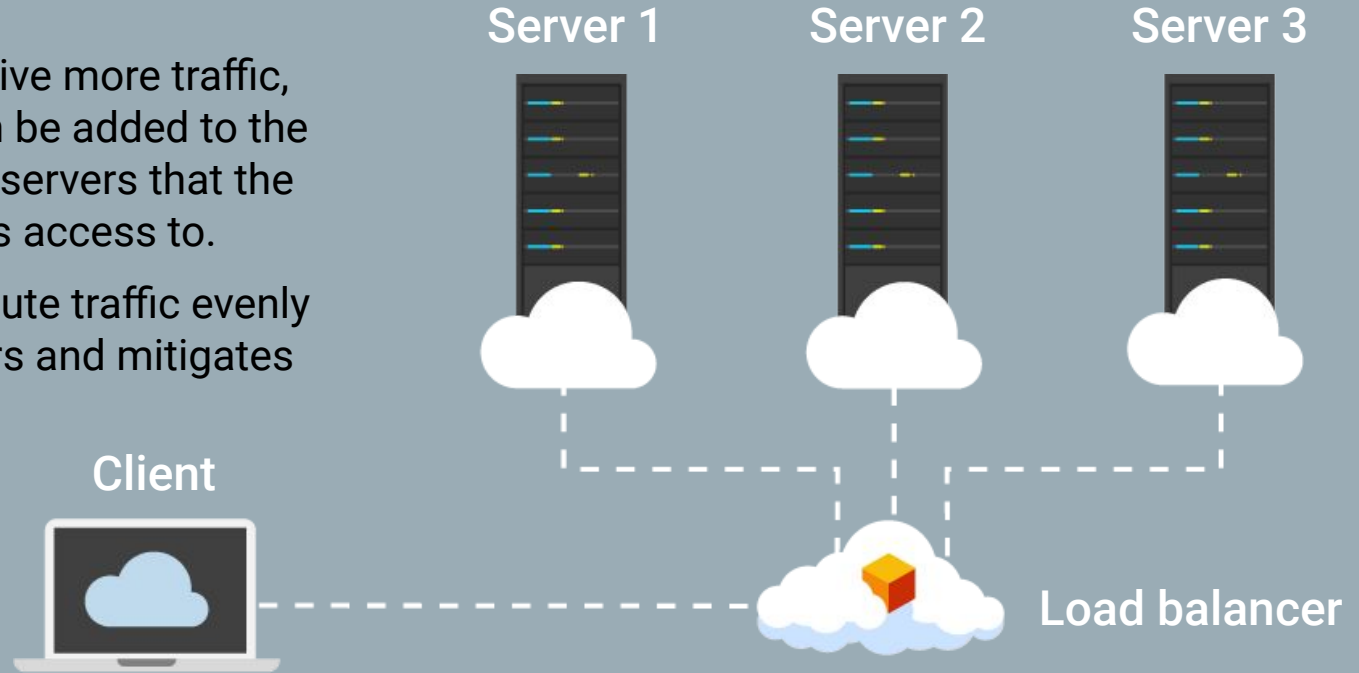
Load Balancing

If the Red Team attacks this DVWA container with enough traffic, they may be able to trigger a Denial of Service (DoS) on the machine.
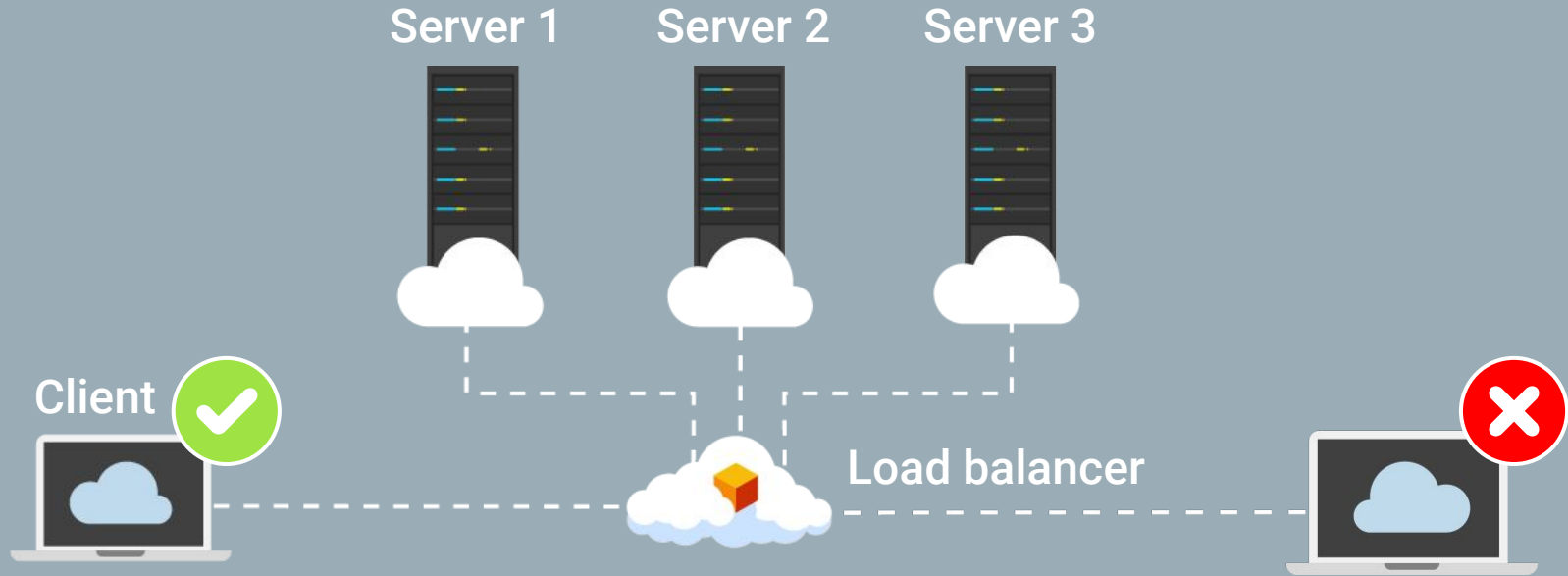
Load Balancers

A **load balancer** provides the external IP address that the rest of the internet can access. Then, it receives traffic that comes into the website and distributes it across multiple servers.

- As websites receive more traffic, more servers can be added to the group ("pool") of servers that the load balancer has access to.

- This helps distribute traffic evenly across the servers and mitigates DoS attacks.

Server 1

Server 2

Server 3

Client

Load balancer

Load Balancers

Load balancers offer a **health probe** function to regularly check all the machines behind the load balancer. Machines with issues are reported, and the load balancers stop sending traffic to those machines.

Server 1　　　Server 2　　　Server 3

Client
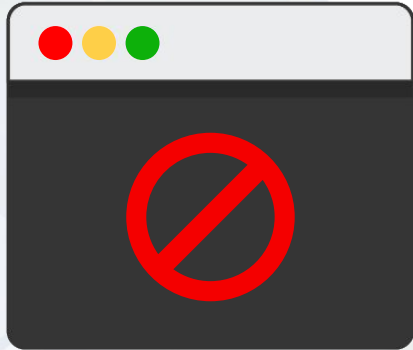
Load balancer

The DVWA VM we set up is not accessible from the internet at this time. This is intentional.

The next step is to set up a load balancer that has an external IP and point it to the VM.

Instructor Demonstration

Setting Up a Load Balancer

Activity: Load Balancing

In this activity, you will install a load balancer in front of the VM to distribute the traffic across more than one VM.
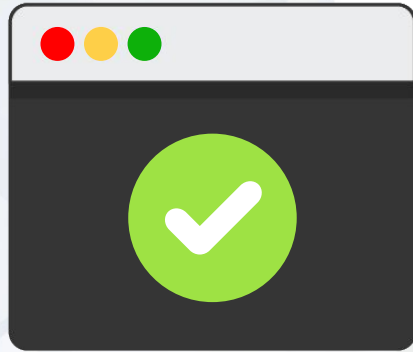
Suggested Time:

20 Minutes

Time's Up! Let's Review.

Questions?

Firewall Configuration

Now that we have a load balancer running, we want to make sure it is configured properly to allow traffic to the VM back-end pool.

By the end of the next activity, we will be able to reach the DVWA website from the internet.

Firewall Configuration

We need to configure a security group to allow web traffic into the VNet from the load balancer. In the following guided tour, we'll create a load balancing rule.
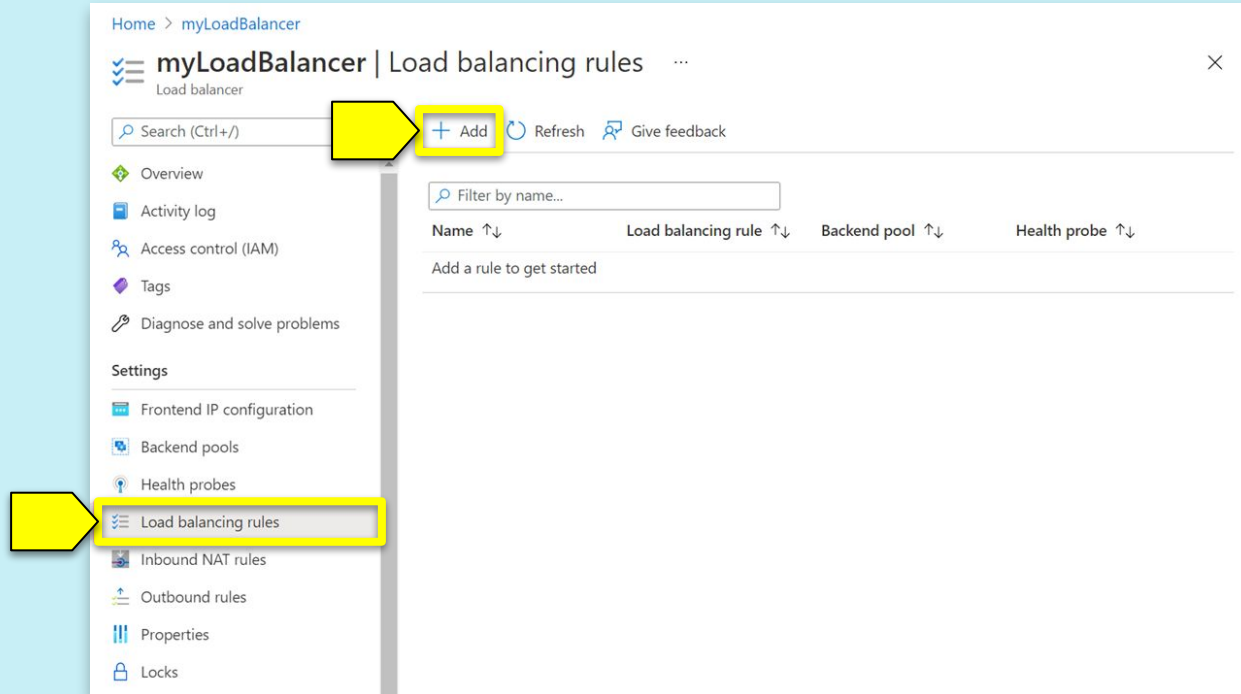
Instructor Demonstration

Load Balancing Rule

Activity: Security Configuration

In this activity, you will configure the load balancer and security group to work together to expose port 80 of the VM to the internet.

Suggested Time:

20 Minutes

Time's Up! Let's Review.

Questions?

Daily Checklist

By the end of today, you should have completed the following critical tasks:

An Ansible playbook has been created that configures Docker and downloads a container.

The Ansible playbook is able to be run on the web VMs.

The web VMs are running a DVWA Docker container.

A load balancer has been created and at least two web VMs placed behind it.

The DVWA site is able to be accessed through the load balancer from the internet.

⚠️ **Shut Down Your Machines** ⚠️

Don't forget to power off your machine!