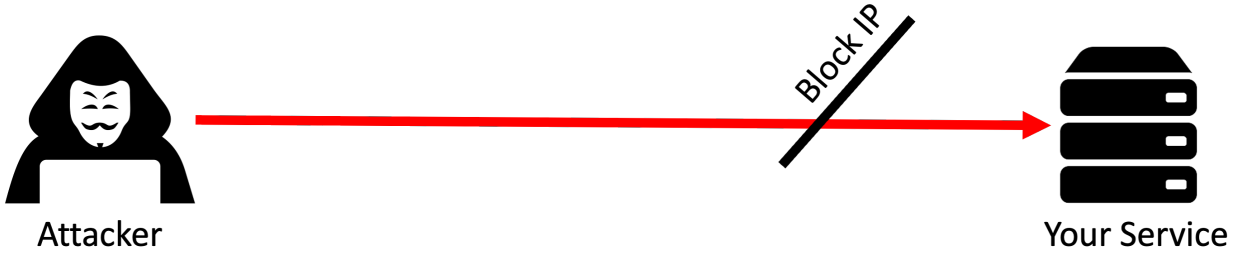
- Tour the DDoS protection tiers Azure offers
- Create a virtual network
- Apply a DDoS protection to the virtual network

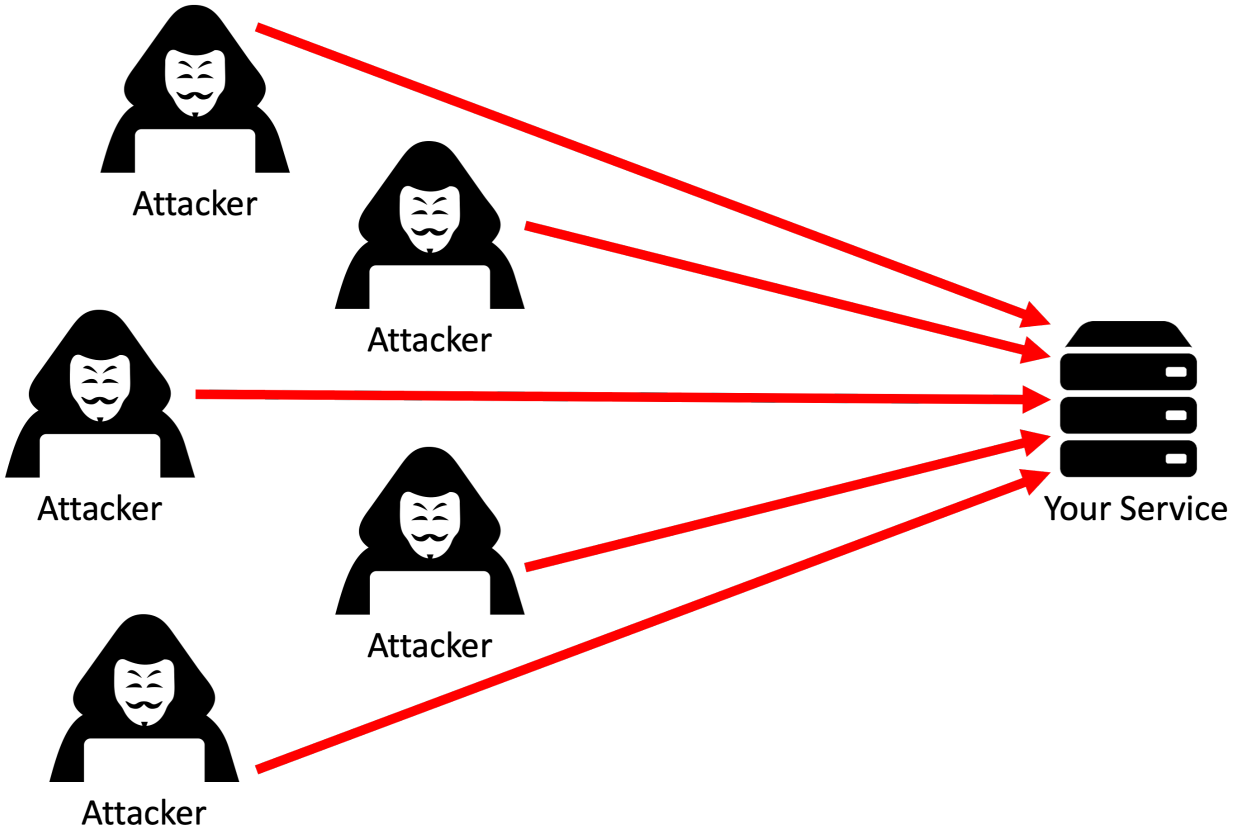
Step 2 - DDoS Overview

Let's say a bad actor decides they want to take your web service down and choose direct denial of service (DDoS) as their best attack tool. The motives could be economic, political, or social, but regardless it is unauthorized and illegal in many countries. DDoS is illegal in the United States under the Federal Computer Fraud and Abuse Act, and can lead to up to 10 years in prison and a $500,000 fine. The crime penalty does not stop malicious hackers, so you have to rely on your own defenses. Thankfully Microsoft Azure provides these.

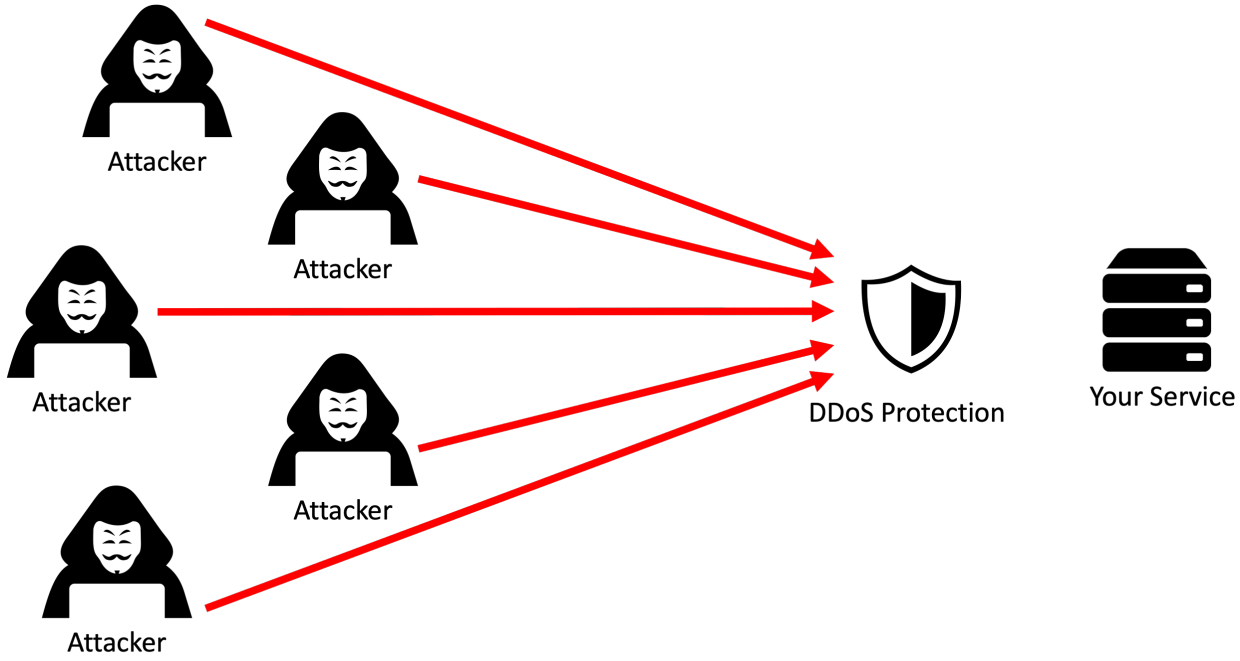
Let's briefly discuss how DDoS works. An amateur hacker could overwhelm your website by running requests in a scripted loop. No big deal. You would see this IP address repeatedly hitting your service and just block it.



But what if the hacker has colleagues to help them? Or have taken over many machines and IP addresses to repeatedly send requests? Your service would get so overwhelmed, not discerning malicious requests from legitimate ones, that your service may ultimately shut down. It would also drive up your cloud costs because the services unnecessarily burn energy and data processing.



Microsoft Azure's Basic DDoS protection is enabled by default. It will discern between legitimate requests and malicious requests based on pattern recognition algorithms. You may choose to upgrade to Standard DDoS protection for further monitoring and mitigation, which will provide DDoS protection not just on a regional level, but on the application level. It will also prevent more sophisticated attacks that are layer-specific and provide DDoS monitoring tools. That's what we are going to use here.



Step 3 - Creating DDoS Protection

Let's create the DDoS protection service. We will call it `MyDDoSProtection` service:

```
az network ddos-protection create \
    --resource-group $resource \
    --name MyDDoSProtection
```

Apply a DDoS on the the virtual network level by setting the `--ddos-protection` argument to `true` and providing the `DDoSProtection` plan that we just created:

```
az network vnet create \
    --name myVN \
    --location eastus \
    --resource-group $resource \
    --ddos-protection true \
```

```
    --ddos-protection-plan MyDDoSProtection
```

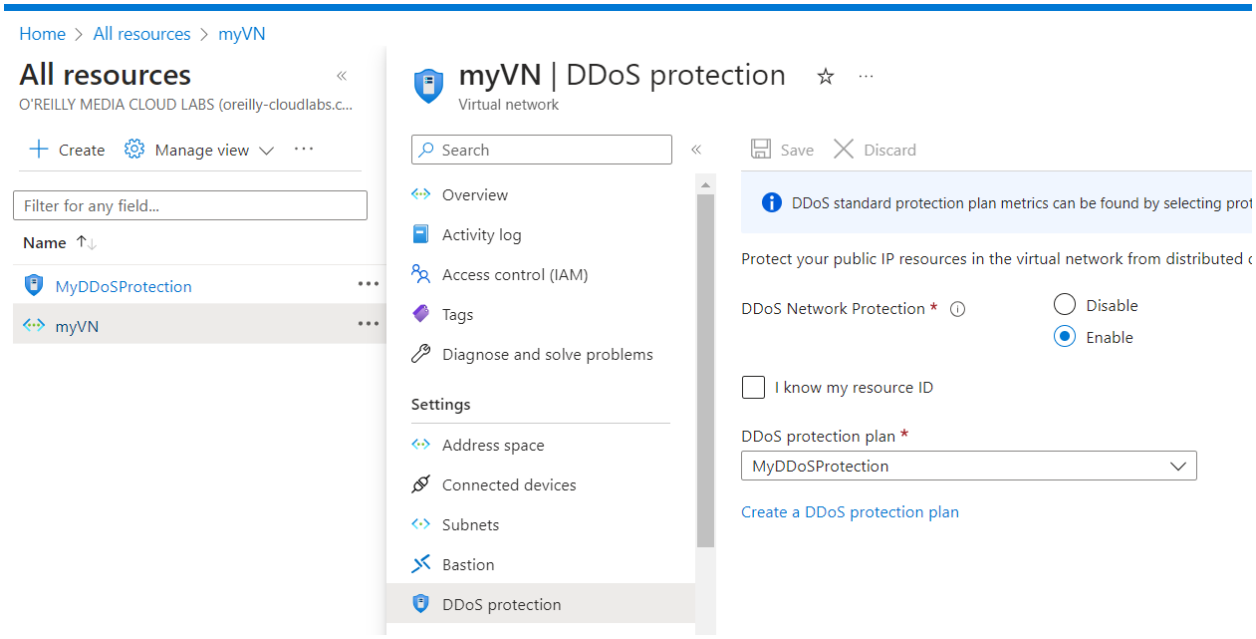
Just for future reference, if you already have a virtual network, you can apply the DDoS service using the `az network vnet update` command. This block is not runnable because it is for reference only:

```
az network vnet update \
    --resource-group $resource \
    --name myVN \
    --ddos-protection true \
    --ddos-protection-plan MyDDoSProtection
```

Step 4 - Displaying the DDoS Protection

You can see that the DDoS service is now up and running:

```
az network ddos-protection show \
    --resource-group $resource \
    --name MyDDoSProtection
```



Step 2 - Setup
The Microsoft Defender for Cloud is a one-stop service to evaluate the health and security configurations of all your resources. It is natively embedded in all the services you create, but presents them all in a centralized and unified fashion. It also will feed recommendations to the Azure Advisor service, which is covered in a separate lab. Here we will explore the security center and its scoring metrics.

When you spin up resources on Azure, Microsoft will automatically apply security initiatives, which are a set of security policies. A security policy is a rule dictating security specifications you want controlled. While many policies are provided, you also have the ability to create your own. The default initiative applied to every resource by default is the Azure Security Benchmark and contains common policies like not exposing storage to outside networks.

Azure will regularly scan your resources and determine what is out of compliance and then provide a score across different categories. It will then provide recommendations on how to remedy these compliance issues.

First we need a resource group.

```
az group create --name $resource --location eastus
```
Let's then create a virtual machine:

```
az vm create --name 'MyVM' \
   --image UbuntuLTS \
   --location eastus \
   --resource-group $resource \
   --admin-username azureuser \
   --public-ip-sku Basic
```

Step 3 - Security Score Definitions
To see all the definitions of what drives our Secure Score in Azure, you can run this command. I recommend outputting this as a table first:

```
az security secure-score-control-definitions list --output table
```
Notice you will see different categories, from multifactor authentication (MFA) to encryption and port security. All of these categories drive your Secure Score in Azure, and note also the MaxScore each of these categories get.

When you run the full JSON output of this command, note you get some more details, particularly the IDs of definitions:

```
az security secure-score-control-definitions list
```

Azure will not have a chance to run its security scans in this lab, so we are not going to get any results with these commands. Regardless, here is the command that would return the Secure Scores. It would detail the results and the current state:

az security secure-scores list
You could also list each of the controls individually with their current status:

az security secure-score-controls list
Step 4 - Viewing Alerts
To view current alerts, you would run the following command. This would show actions that need to be taken based the security initiatives and definitions:

az security alert list
You could also provide a resource group to restrict scope to that resource group:

az security alert list --resource-group $resource
As you can see if you run these, we do not have any alerts because we have not done much other than create a VM in this lab. Over time, security will monitor for vulnerabilities, and if we took insecure actions, like opening up the VM ports to liberally, it should pop up here as an alert.

This wraps up our tour of the security center and the commands to retrieve Secure Scores.