Security Groups

Introduction

Within a VPC, there are a few mechanisms to control access to your EC2 instances. In this session, we are going to review Security Groups. Security groups can be thought of as a virtual firewall, which allow you to control the inbound and outbound traffic your EC2 instance can receive or send. By default, when you create a new security group it does not allow any inbound traffic. Just like any other firewall policy, you want to limit the traffic allowed as much as possible. Let's review the default security group created for your EDGE instance deployment, which may look something like this.

- As you can see, we only have one Inbound rule in this group currently.
- It allows SSH traffic, via the TCP protocol over port 22 from Anywhere (0.0.0.0/0).
- Our goal is to further restrict the source address or addresses that we will allow communication from.
- When we edit the security group, we are presented with a dialog of information we need to provide.

Step 1:

- We start with identifying the Type of traffic.
- In the drop down, some common protocols are provided which you can select.
- For example HTTP, HTTPS, and RDP.
- If your specific requirements aren't listed, you can do a custom Rule and input the specific Port/Protocol requirements for your application.
- You can also select to allow All traffic.
- In our example, we will choose SSH. This will populate the Protocol (TCP) and Port Range fields (22) for us.

Step 2:

- Now we need to edit the Source which has three options in the dropdown.
- Anywhere means just that. It is represented as series of zeroes and this rule will allow traffic from any Source Address via the configured protocol.
- MyIP - When selected, this will check what your current Public IP address is and input into that the field.
- CustomIP - This is the option we will select. Here is where we can provide the specific IP address or network of addresses you will be connecting from.

Step 3:

- If necessary, check with your Network Administrator to determine which Public address(es) will need to be input into this rule.
- In our example we will input 192.168.1.100/32 which is one specific IP address.
- When we hit Save, this change will take an immediate effect.

Any EC2 instance which has this security group assigned will now only allow SSH traffic from 192.168.1.100. Anything other connections will be denied.