SECURITY GROUPS

WHAT WE'LL COVER

In this lab we will learn about **Security Groups.**

WHAT IS SECURITY GROUP

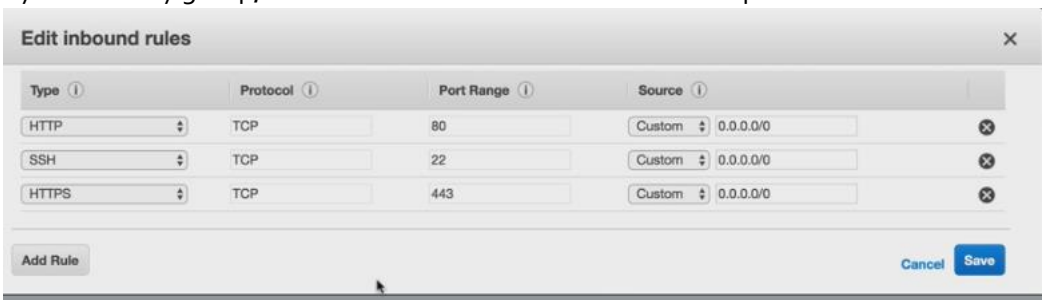
A **Security Group** is a Virtual Firewall. And instance can belong to more than one security groups. Each security group has rules that allow or deny traffic. A security group is the first line of defense against hackers. With security groups you can only add rules that allow, not rules that deny. For that there is another tool that is called **Network ACL** (**Network Access Control List)**. This lecture is about security groups only.

- All inbound Traffic is Blocked by default
- All outbound Traffic is allowed by default
- Changes to Security Groups take effect immediately
- You can have any number of EC2 instances within a security group
- You can have multiple security groups attached to EC2 instances.
- Security groups are STATEFUL
    - If you create an inbound rule allowing traffic in, that traffic is automatically allowed back out again
- You cannot block specific IP addresses using Security Groups.
- You can specify allow rules, but not deny rules

LAB

EXERCISE

1. Make sure you have an EC2 instance from the last lab. If not then create one.
2. Go to security group settings and delete the inbound rule of http
3. Go to your security group, edit and delete the **inbound rule** for http

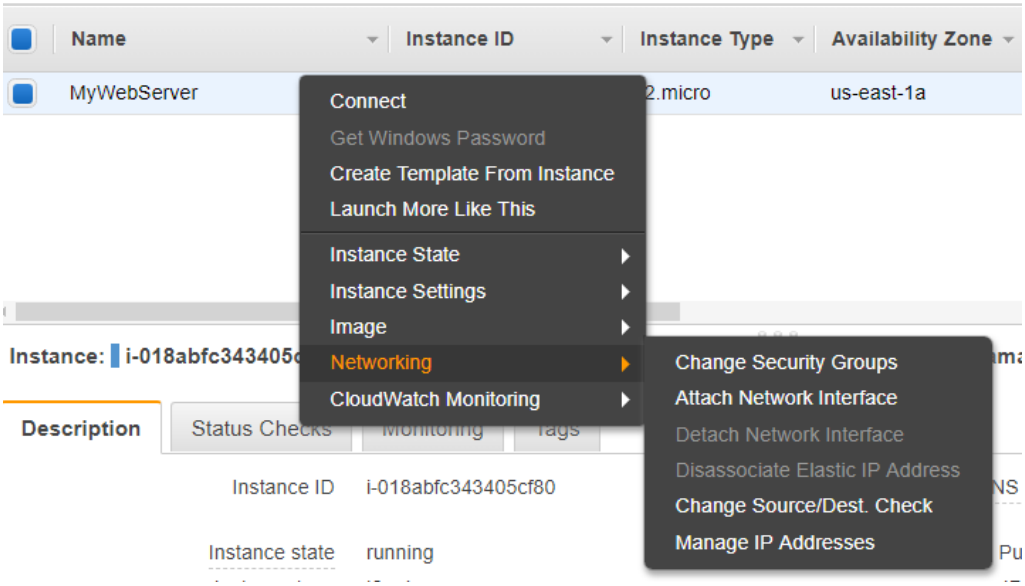


4. Refresh your webpage and check if it's working
5. Now add the rule back and refresh the webpage again.

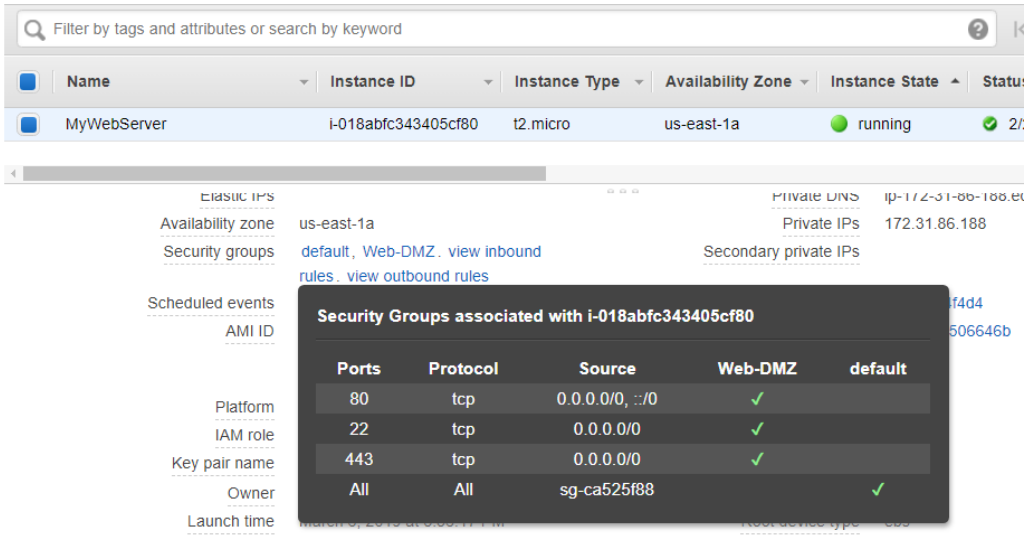
EXERCISE

Now try to add more than one security group to your instance.

Hint:



When you're done view them in the instance details pane



SUMMARY

In the lab we learned about **Security Groups**.