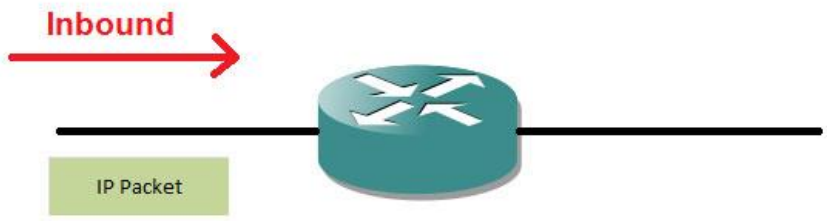
Overview:
A new instance is created, but is not placed into the correct security group. This instance may not be directly added to the default security group. Due to the fact that world inbound access from anywhere is a very bad practice. When a security group is created, the group should set up a way to disallow access. If the instance becomes discoverable on the network, the security group would help to diminish these risks. Connectivity should be **predictable** for each instance.



Discovery:
In the Virtual Private Cloud (VPC) Console, make sure to view the security groups and determine if the instances are correctly being restricted. Rules can be added to each security group to distinguish the differences for each instance and allow traffic to and from its associated instances. These rules can be modified at anytime.

Connection Tracking

- Security groups use connection tracking to track all the information to and from the instances. The rules are applied depending on the state of the connection of the traffic. The rules allow and deny the traffic from entering and leaving the instance.

For more information about VPC:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

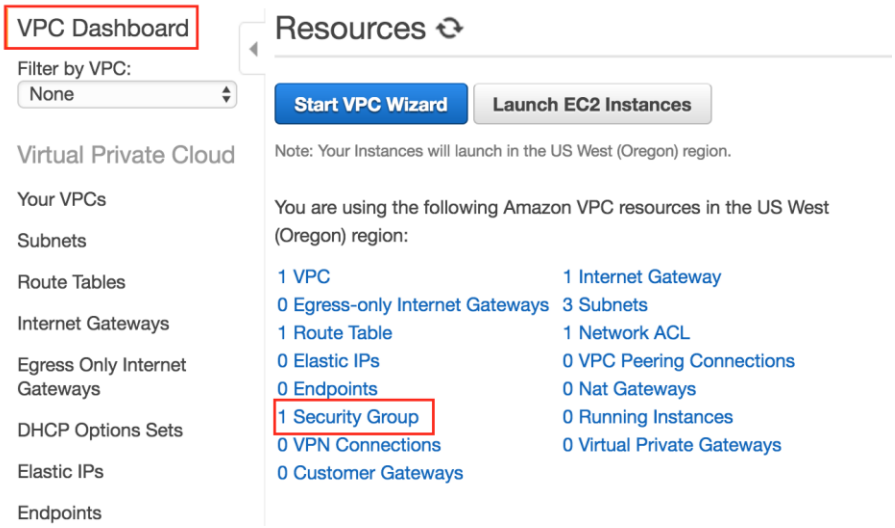
For more information about Connection Tracking:
http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html#security-group-connection-tracking

Remediation:

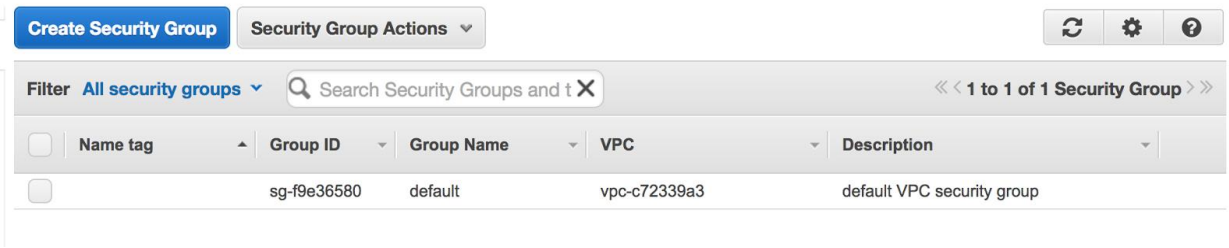
To remediate security group world inbound access attacks, go to the VPC Console in the Amazon Web Services Console. Visit all of the security groups and assign strict rules using the inbound rules tab. Set the access rules that will disallow the instance from being attacked again.

Shown in the images below is the VPC dashboard and the Security Groups Dashboard

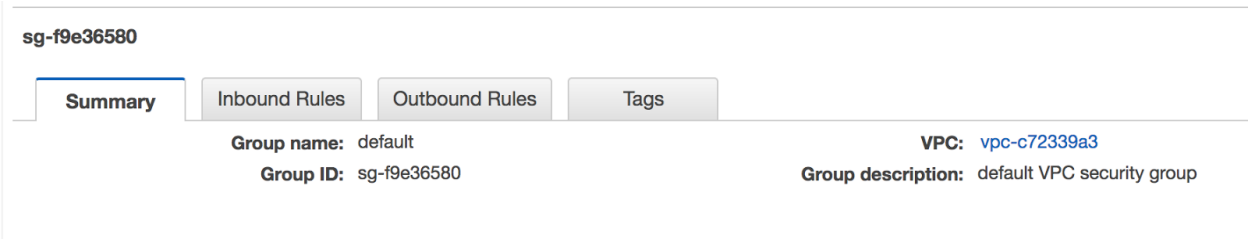
VPC



Security Groups



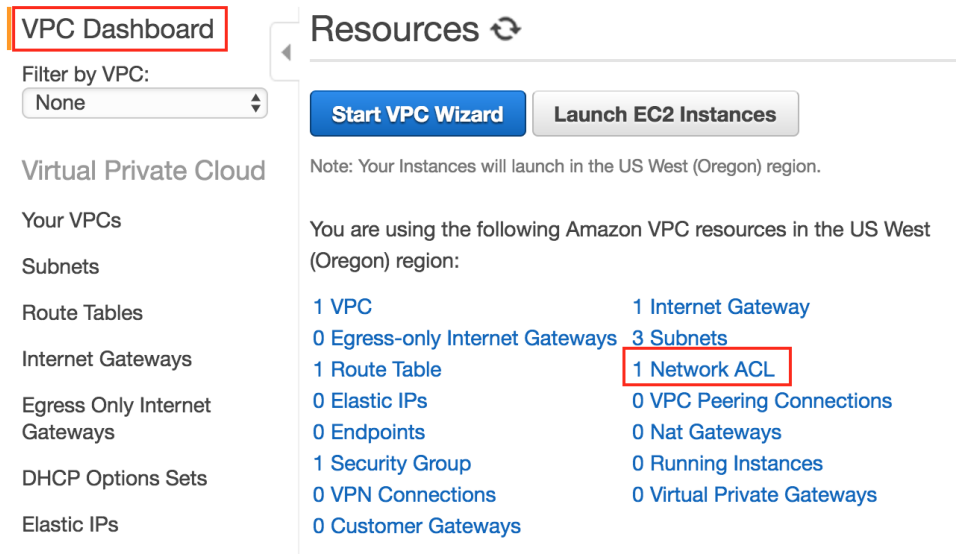
At the bottom of the page you can see the summary for each of the security groups and the inbound and outbound rules, as seen below.



Prevention:

Amazon S3 Access Control Lists (ACLs) enables you to manage access to the buckets and objects. Each bucket and object has an ACL attached to its subresources. When a request is received against a resource, Amazon S3 checks the corresponding ACL to verify the requester has the necessary access permissions. ACLs limit the amount of people with capabilities to edit security groups and stand up instances on a network. The security groups will restrict permissions and capabilities of each of the instances.

In the AWS Dashboard go to the VPC Dashboard and then Network ACL



Network ACL: Here you can view all of the Inbound and Outbound Rules as well as the Subnet Associations with the Individual Network ACL