Configure AWS Config Rules Based on your security policies

1. Evaluate your security policies to understand what type of AWS Config rule will be necessary for your organization.
2. For example, “Remote Access Policy” indicates that you will need to open SSH only to a specific IP address used by the companies network administrators.
3. Open AWS Config and select “Rules” from the left
4. Click add rule and select the “restricted ssh” rule and add the rule to this region.
5. This rule will detect any security group that has port 22 open to 0.0.0.0/0 and mark as non-compliant.