😊 AWS Firewall Manager

AWS Firewall Manager is a security management service provided by Amazon Web Services (AWS) that makes it easier for you to centrally configure and manage firewall rules across your AWS accounts and applications. It allows you to set up and enforce firewall rules, including AWS WAF rules, across your entire AWS infrastructure or specific accounts and resources within your organization.

With AWS Firewall Manager, you can create and manage firewall rules for AWS WAF, AWS Shield Advanced, and VPC security groups. This centralized management helps ensure consistent security across all your AWS resources and accounts, simplifying the process of maintaining security and compliance standards.

Key features of AWS Firewall Manager include:

1. **Centralized Management:** You can centrally configure and manage firewall rules across multiple AWS accounts and resources from a single management console.
2. **Policy Enforcement:** AWS Firewall Manager allows you to enforce security policies consistently across your organization, ensuring compliance with security requirements and industry standards.
3. **Integration with AWS WAF and Shield Advanced:** You can create and manage AWS WAF rules and AWS Shield Advanced protections across your accounts and resources using Firewall Manager.
4. **Automated Remediation:** Firewall Manager can automatically remediate non-compliant resources by applying the necessary firewall rules, helping to maintain a secure environment.
5. **Customizable Rules:** You can create custom firewall rules tailored to your organization's specific security needs and requirements.

😄 Use Case of Firewall Manager:

AWS Firewall Manager offers several use cases for organizations looking to manage and enforce security policies across their AWS infrastructure:

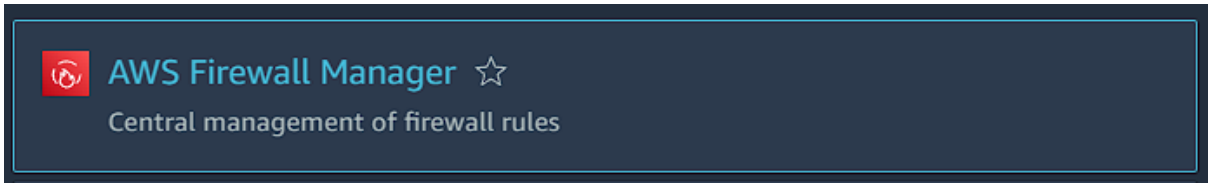
1. **Centralized Security Management:** Organizations with multiple AWS accounts can use AWS Firewall Manager to manage and enforce security policies centrally, ensuring consistent protection across all accounts and resources.
2. **Compliance and Governance:** AWS Firewall Manager helps organizations enforce compliance with security standards and regulatory requirements by centrally configuring and enforcing firewall rules, including AWS WAF rules and AWS Shield Advanced protections.
3. **Protection from DDoS Attacks:** By integrating with AWS Shield Advanced, Firewall Manager enables organizations to protect their applications and resources from Distributed Denial of Service (DDoS) attacks across multiple AWS accounts.

4. **Application Security:** With AWS WAF integration, Firewall Manager allows organizations to define and enforce web application firewall rules to protect their applications from common web exploits and attacks.
5. **Multi-Tiered Applications:** Organizations deploying multi-tiered applications on AWS can use Firewall Manager to manage security rules across different tiers, ensuring appropriate access controls and protection for each component.
6. **Automated Remediation:** Firewall Manager can automatically remediate non-compliant resources by applying the necessary firewall rules, reducing the manual effort required to maintain a secure environment and improving operational efficiency.
7. **Custom Security Policies:** Organizations can create custom firewall rules tailored to their specific security needs and requirements, allowing them to address unique security challenges and threats.
8. **Managed Security Services:** Managed Security Service Providers (MSSPs) can use AWS Firewall Manager to offer centralized security management and compliance services to their customers, providing added value and peace of mind.

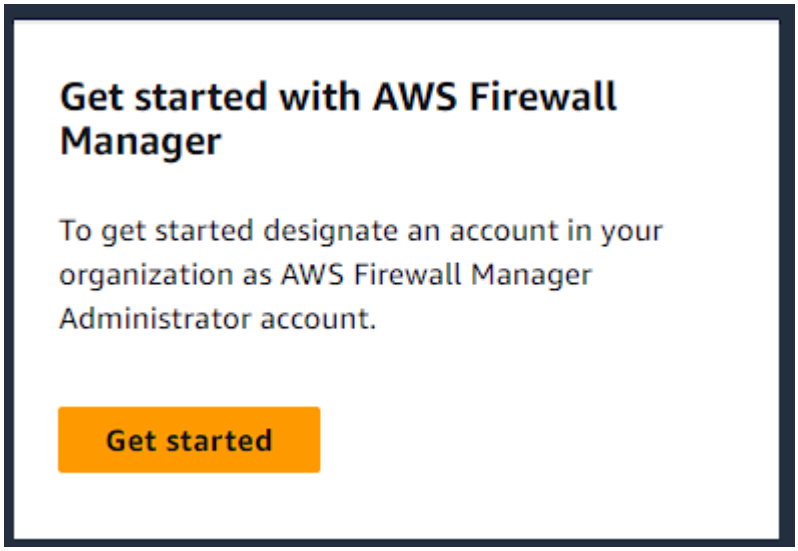
In this lab, we are setting up intentionally insecure security groups in a slave AWS account to test AWS Firewall Manager's auditing capabilities. The end goal is to evaluate whether Firewall Manager can accurately identify and report non-compliant resources, such as instances with insecure security group configurations, and demonstrate its ability to enforce security policies across AWS accounts.

😄 To begin with the Lab:

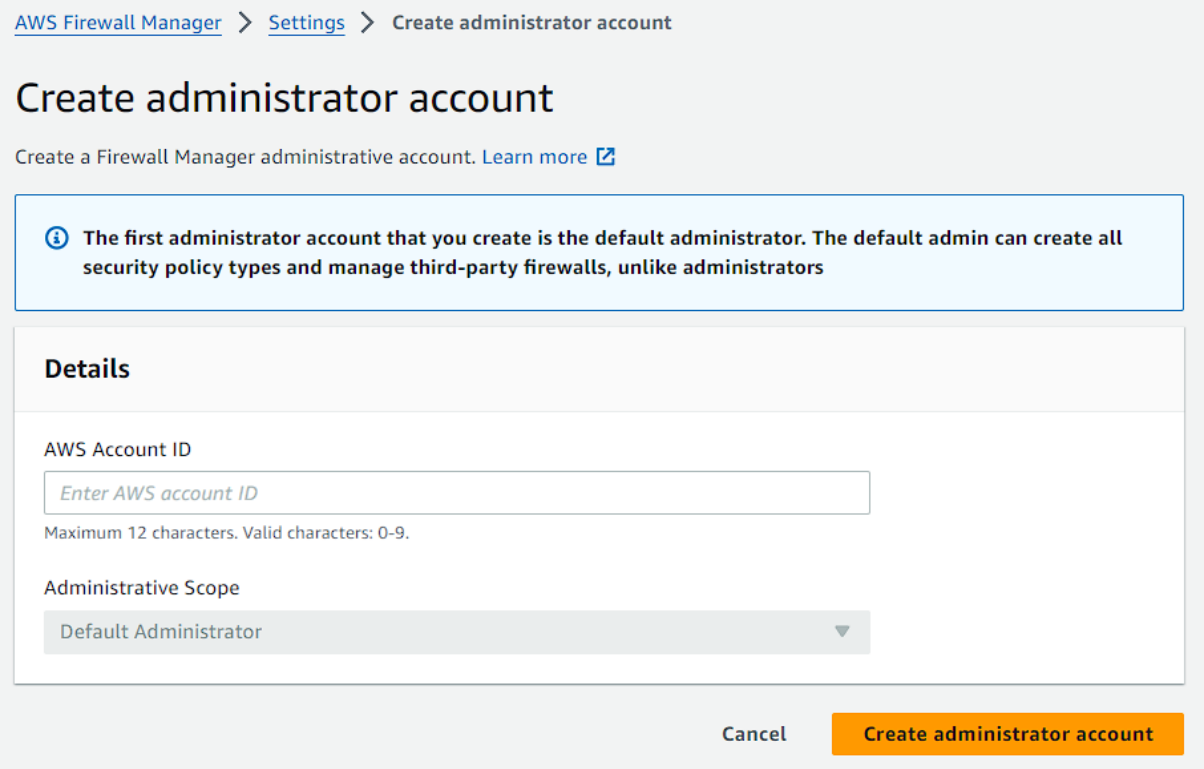
1. So, the pre-requisites for this lab are, first you should have two AWS Accounts and you should have enabled AWS Organizations in your account which should be your master account as well.
2. Then you must add the second account as your slave account in the master account using AWS Organization.
3. Now from your master account navigate to Firewall Manager. Choose this service accordingly.



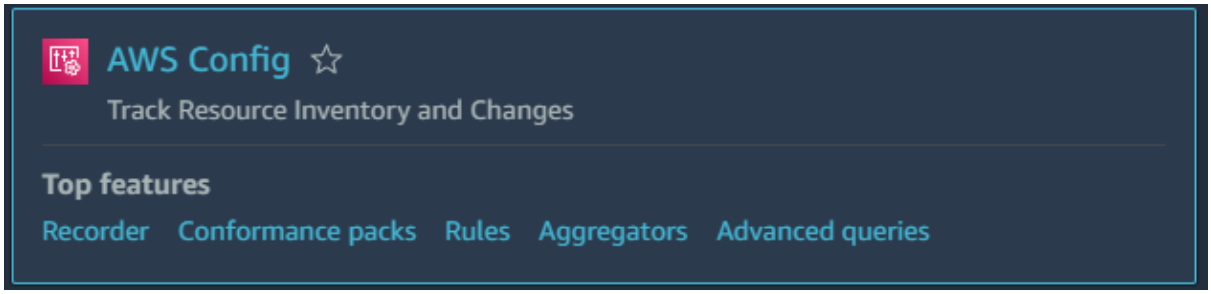
4. Now from the dashboard of firewall manager click on Get Started.



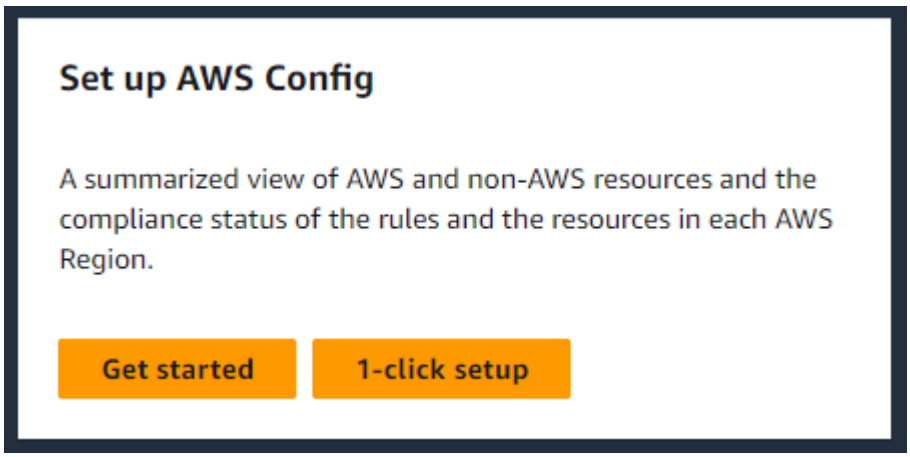
5. Here you have to create an administration account which is your master account. So, here you have to add the account ID of your master account and click on Create.



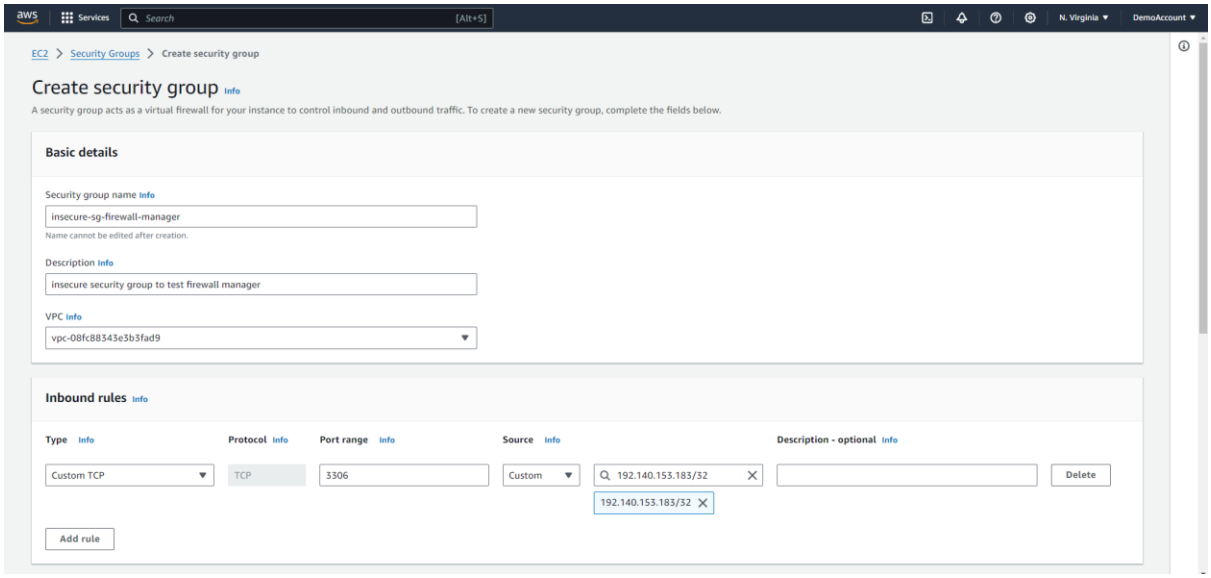
6. Now we will go to the member account or slave account and demonstrate the setup of security groups in EC2 instances from that account so that we can see how the firewall manager created in this master account can be used to control or audit the configurations in one of your member accounts.
7. So, the very first thing you have to do in your slave account is that you have to enable AWS Config on it. Choose this service accordingly.



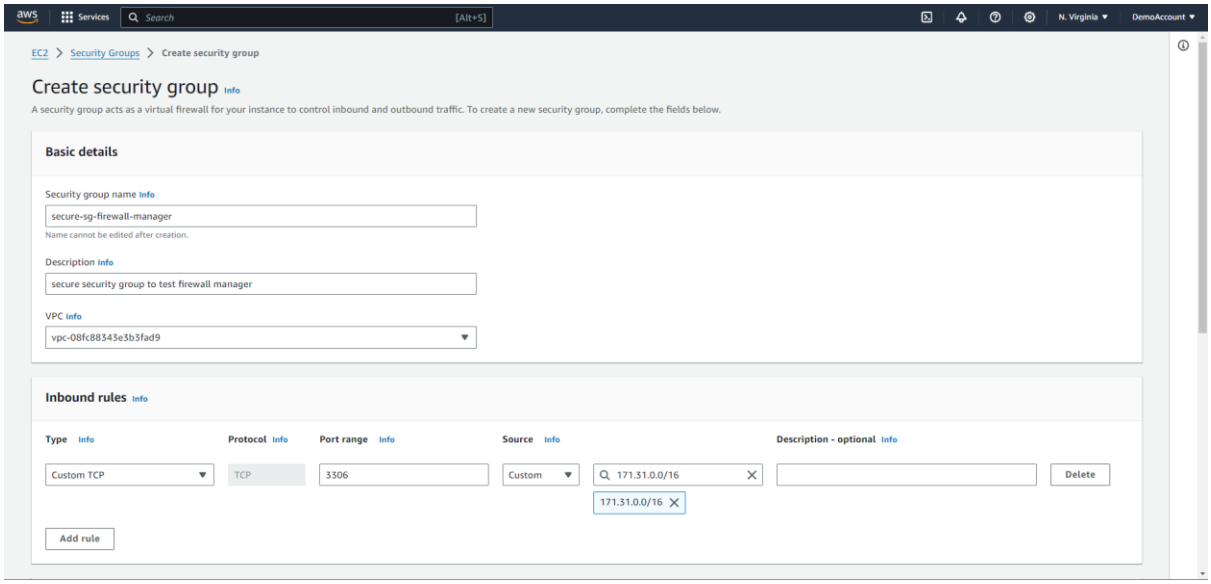
8. Now from the dashboard of AWS Config you have to click on get started if you have not enabled it.



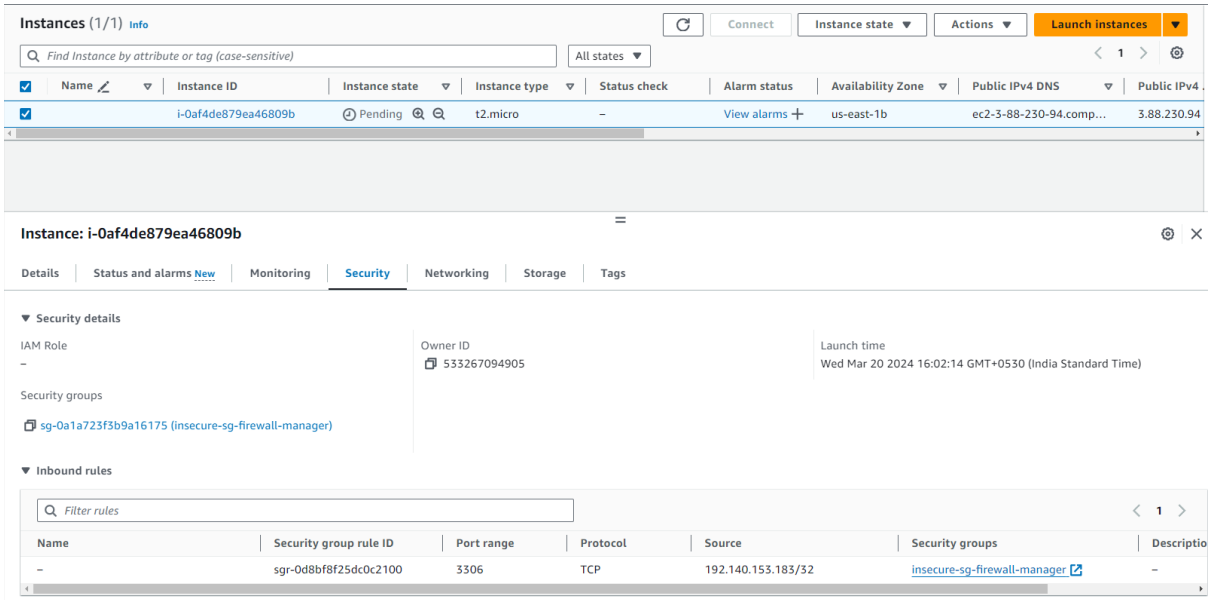
9. You have to keep everything to default and just start your AWS config.
10. Now config is a configuration management tool in AWS. It stores the configuration changes for all your resources over time and it is also the resource that's used by the firewall manager to track the different configurations of your security groups. So, it's in effect the auditing tool that's firewall manager uses to figure out if the configuration of the security group is different from what we have defined in the firewall management policy.
11. Now you are going to EC2 and there you are going to create security groups.
12. Through this we will do the testing for AWS Firewall Manager with intentionally insecure security groups to evaluate its auditing functionality. And you have to create these security groups in your slave account.
13. Now you are going to create a security group which should insecure in nature. You can use your public IP of your local machine.



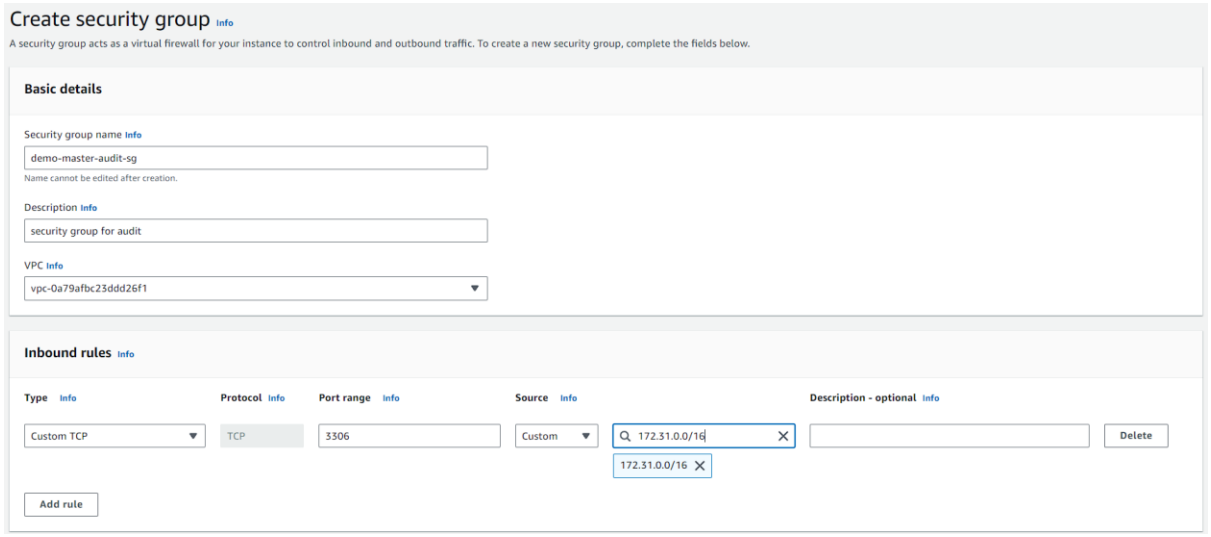
14. Then again you have to create a security group which is secure in nature. You can use the IP address of your VPC.



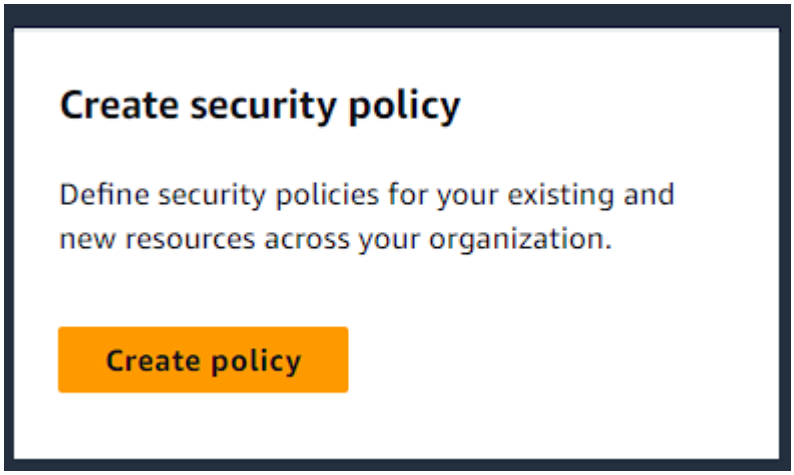
15. Then you are going to launch an instance in your insecure security group.



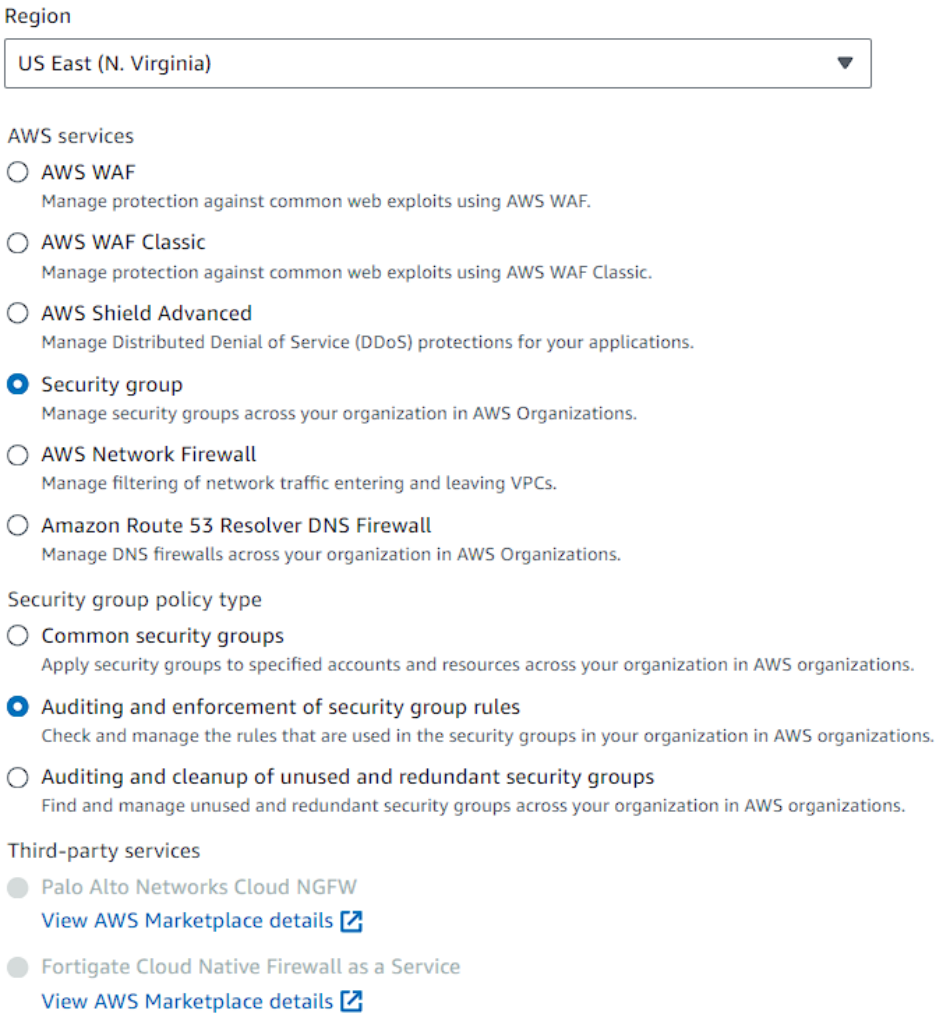
16. Now you should navigate to your master account and create policy for you firewall manager.
17. But first we also need to create a security group rule and this can be called an audit security group because it's essentially going to be your ideal or the most secure configuration that you want and then what the firewall manager would do is that for SS or audit all of the other security groups concerning this configuration.
18. So, navigate to EC2 go to security groups in your master account, and create a security group rule.
19. Here in the inbound rules again you can add the port 3306 and for IP address give your VPC private IP.



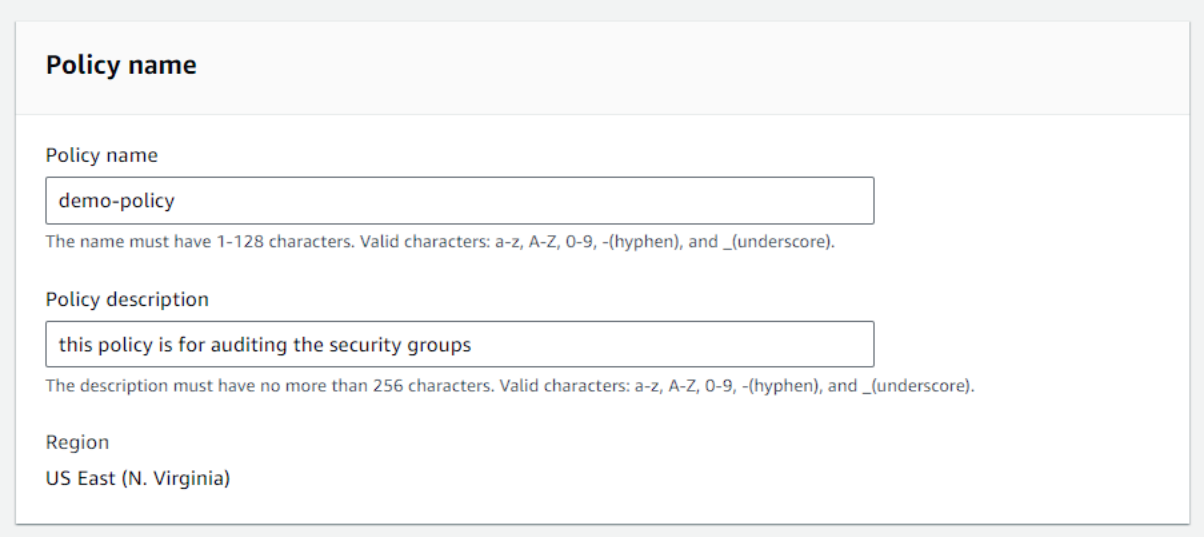
20. Now go back to firewall manager and from its dashboard click on create policy.



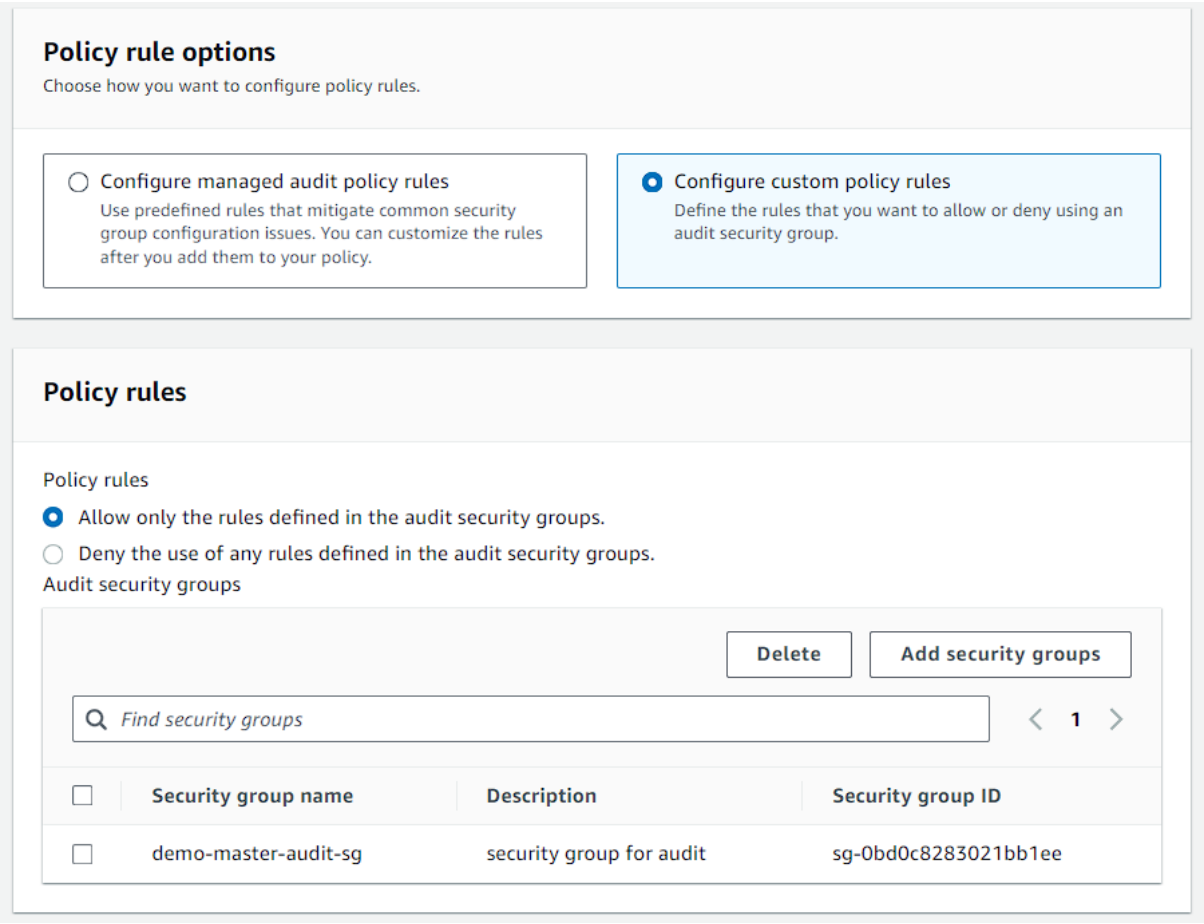
21. Now you have to select the region where you are working with firewall manager. Then select security group.
22. After that the policy type is auditing and enforcement.



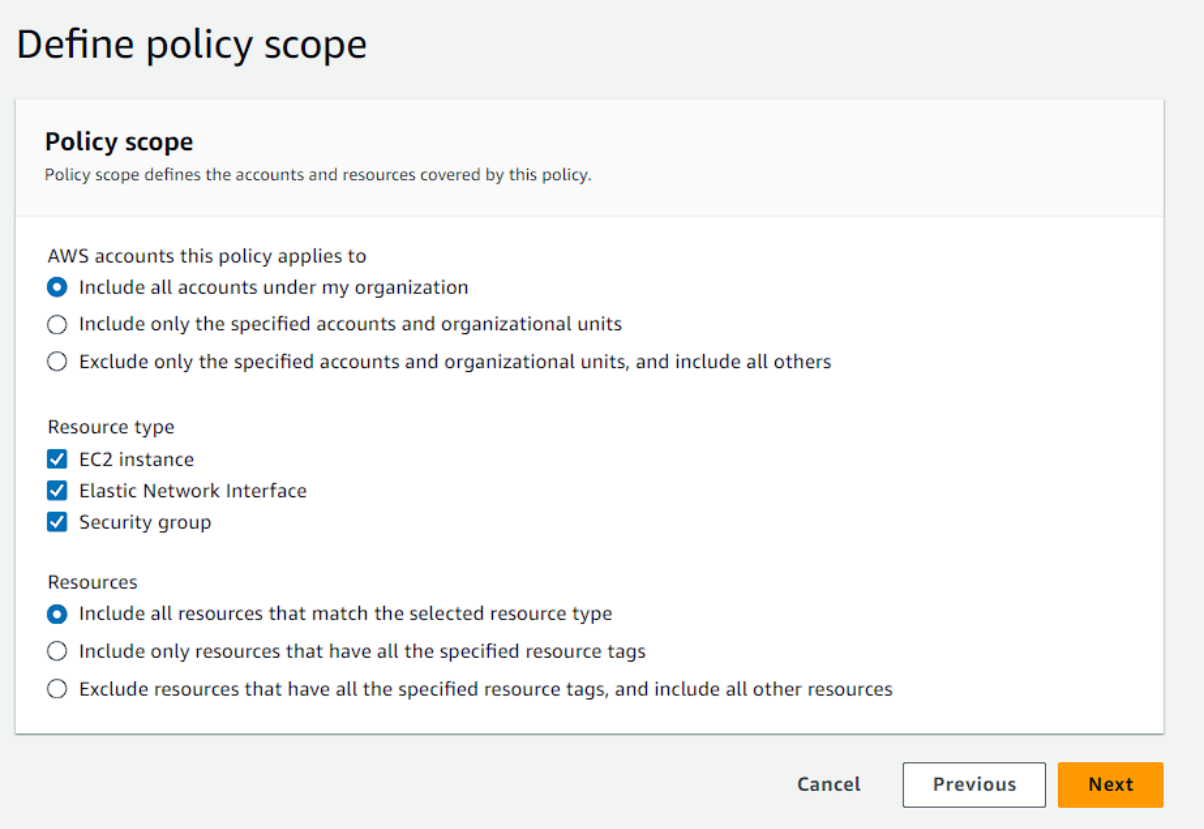
23. After that you have to name your policy and give it a description.



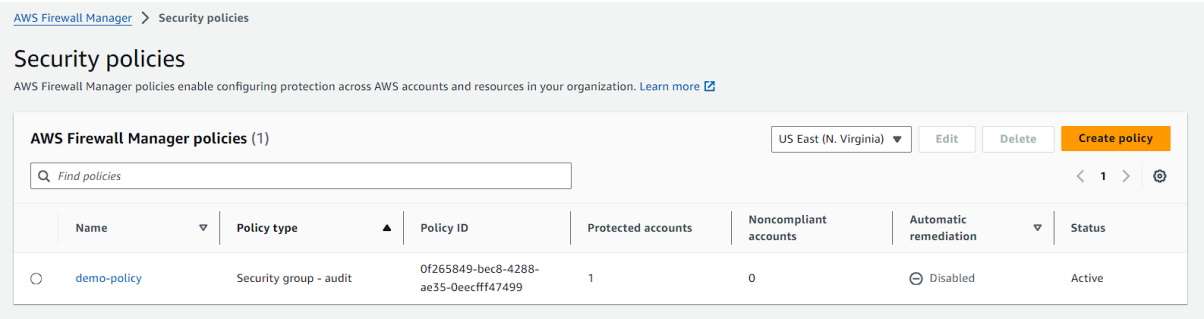
24. Then choose to configure custom policy rules and select your security which you just created. Then just click on next and move to next page.



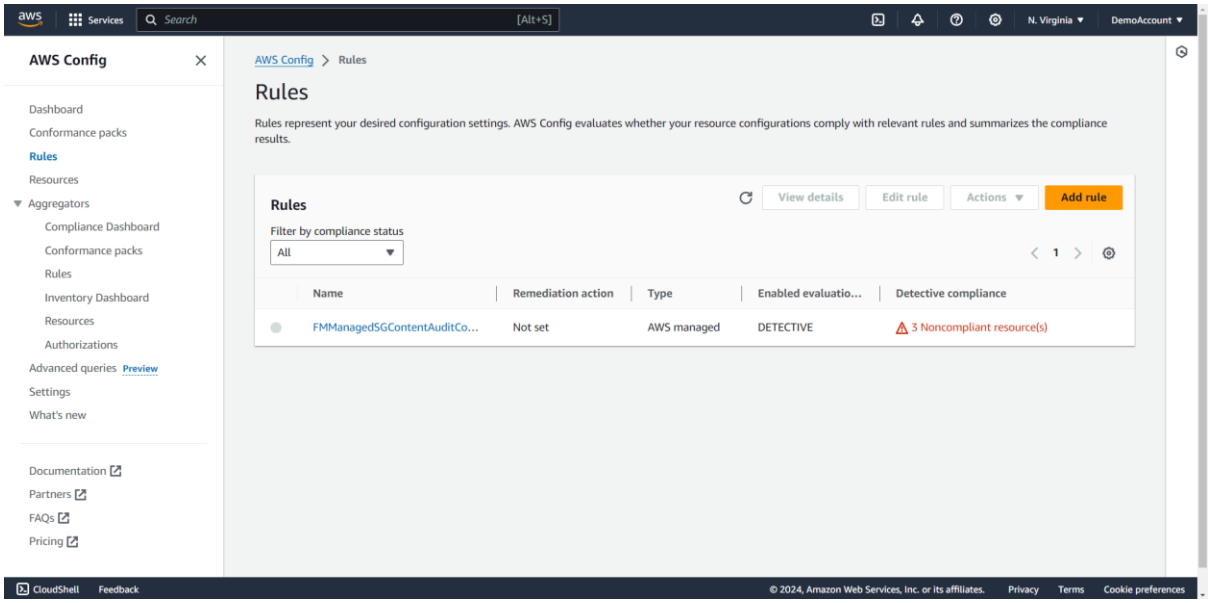
25. Now you have to choose these options shown below.
26. And move to the review page and create your policy.



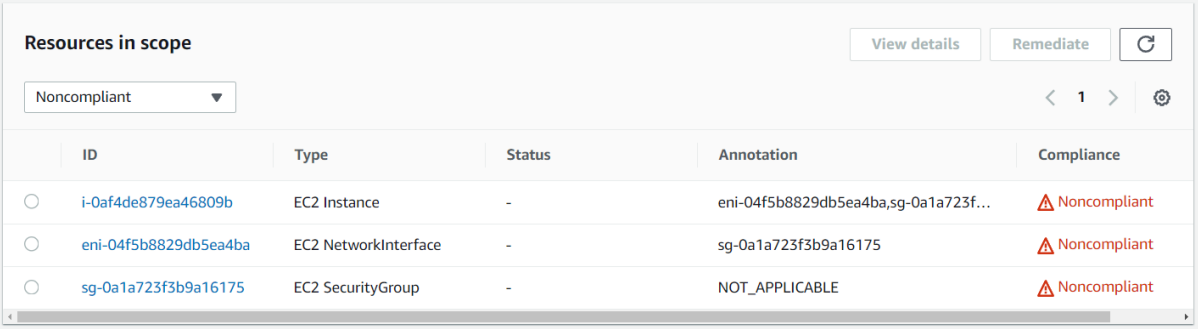
27. Below you can see your policy. So, generally it takes up to 5 minutes so the things can get ready.



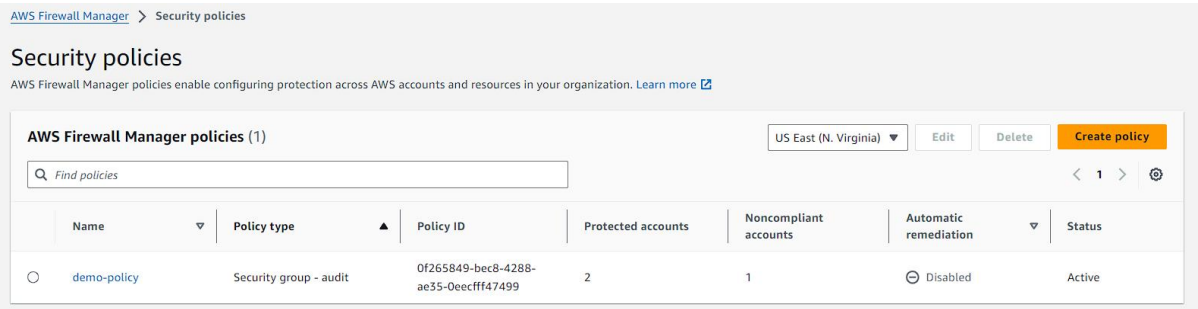
28. Now you have to navigate to AWS config in your slave account. There you have to go to rules and you will see that the firewall manager has created a rule which shows the non-compliant resources. Currently you will see there are 3 anomalies.
29. These 3 noncompliant resources are the insure one.



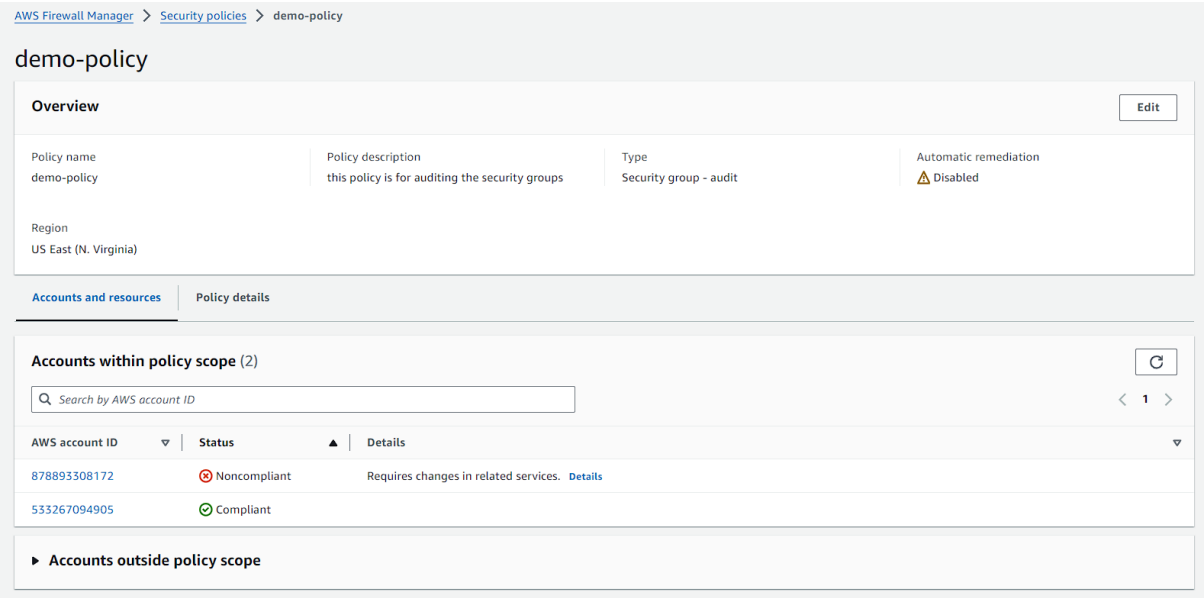
30. If you go inside of it and scroll down to the bottom you can see the noncompliant resources.
31. Here we have the security group, the instance on that we launched on the insecure security group and the ENI that got attached to this instance.



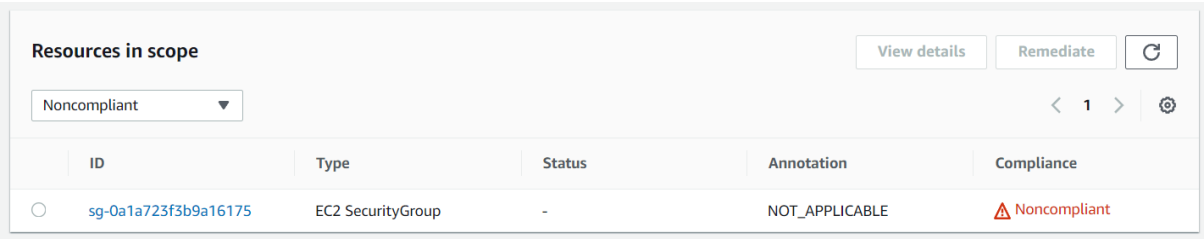
32. Now if you go back to the firewall manager in the master account and in the policies you can see that is showing the noncompliant account.



33. If you go inside of it you can see the account ids which are compliant and noncompliant.



34. Now you are going to the slave account and there you are going to change the security group of the EC2 instance to see whether the firewall manager changes the report.
35. Once you have changed the security group from insecure to secure then you have to wait for 5-10 minutes to look at the changes.
36. Here you can see the change the EC2 instance and the ENI attached to it are gone. Which means that they are of secure nature now.
37. But the security groups still remains.



38. Once you have done this practical terminate your instance and turn off the recording for AWS Config for the accounts.