



## 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:

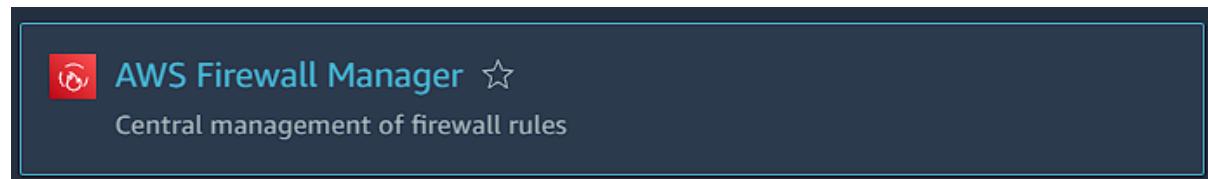
1. **Centralized Security Management:** Organizations with multiple AWS accounts can use AWS Firewall Manager to manage and enforce security policies centrally, ensuring consistent protection across all accounts and resources.
2. **Compliance and Governance:** AWS Firewall Manager helps organizations 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.

## Get started with AWS Firewall Manager

To get started designate an account in your organization as AWS Firewall Manager Administrator account.

[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.

[AWS Firewall Manager](#) > [Settings](#) > [Create administrator account](#)

### Create administrator account

Create a Firewall Manager administrative account. [Learn more](#)

**(i) The first administrator account that you create is the default administrator. The default admin can create all security policy types and manage third-party firewalls, unlike administrators**

#### Details

AWS Account ID

Enter AWS account ID

Maximum 12 characters. Valid characters: 0-9.

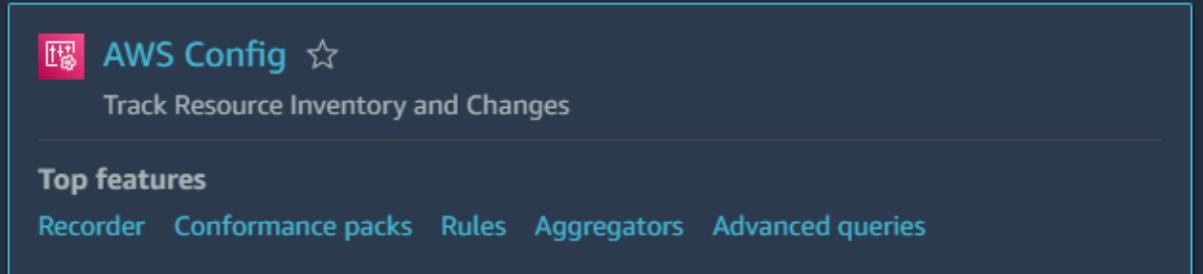
Administrative Scope

Default Administrator

[Cancel](#)

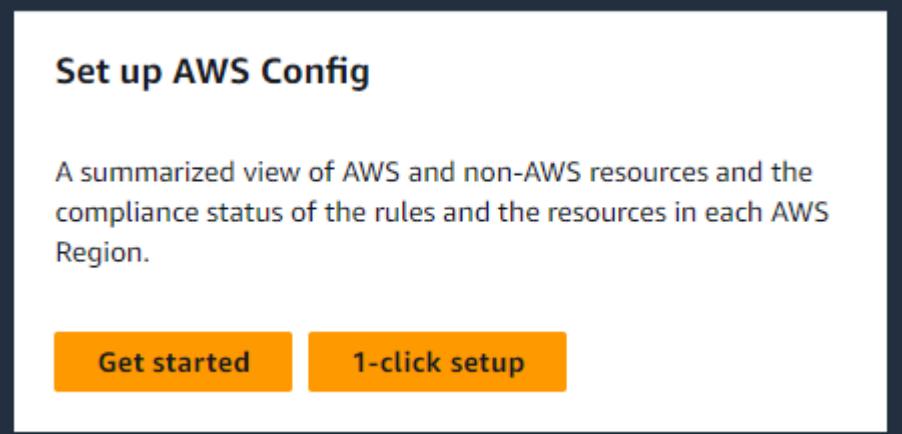
[Create administrator account](#)

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.



AWS Config ☆  
Track Resource Inventory and Changes  
**Top features**  
Recorder Conformance packs Rules Aggregators Advanced queries

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



## Set up AWS Config

A summarized view of AWS and non-AWS resources and the compliance status of the rules and the resources in each AWS Region.

**Get started**   **1-click setup**

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.

Screenshot of the AWS EC2 Create security group interface. The 'Basic details' section shows a security group name 'insecure-sg-firewall-manager' and a description 'insecure security group to test firewall manager'. The 'VPC Info' dropdown is set to 'vpc-08fc88545e3b3fad9'. In the 'Inbound rules' section, there is one rule: a Custom TCP rule on port 3306 from source 192.140.153.183/32.

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

Screenshot of the AWS EC2 Create security group interface. The 'Basic details' section shows a security group name 'secure-sg-firewall-manager' and a description 'secure security group to test firewall manager'. The 'VPC Info' dropdown is set to 'vpc-08fc88545e3b3fad9'. In the 'Inbound rules' section, there is one rule: a Custom TCP rule on port 3306 from source 171.31.0.0/16.

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

Instances (1/1) [Info](#)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4
<input checked="" type="checkbox"/> i-0af4de879ea46809b	i-0af4de879ea46809b	Pending	t2.micro	-	<a href="#">View alarms</a> +	us-east-1b	ec2-3-88-230-94.comp...	3.88.230.94

Instance: i-0af4de879ea46809b

Details | Status and alarms [New](#) | Monitoring | **Security** | Networking | Storage | Tags

**Security details**

IAM Role	Owner ID	Launch time
-	553267094905	Wed Mar 20 2024 16:02:14 GMT+0530 (India Standard Time)
Security groups		
<a href="#">sg-0a1a723f3b9a16175 (insecure-sg-firewall-manager)</a>		

**Inbound rules**

Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
-	sgr-0d8bf8f25dc0c2100	3306	TCP	192.140.153.183/32	<a href="#">insecure-sg-firewall-manager</a>	-

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.

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

**Basic details**

Security group name [Info](#)  
demo-master-audit-sg  
Name cannot be edited after creation.

Description [Info](#)  
security group for audit

VPC [Info](#)  
vpc-0a79afbc23ddd26f1

**Inbound rules** [Info](#)

Type	Protocol	Port range	Source	Description - optional
Custom TCP	TCP	3306	Custom	<input type="text" value="172.31.0.0/16"/> <a href="#">Delete</a>
<a href="#">Add rule</a>				

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

## Create security policy

Define security policies for your existing and new resources across your organization.

**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.

Region

US East (N. Virginia)



AWS services

- AWS WAF  
Manage protection against common web exploits using AWS WAF.
- AWS WAF Classic  
Manage protection against common web exploits using AWS WAF Classic.
- AWS Shield Advanced  
Manage Distributed Denial of Service (DDoS) protections for your applications.
- Security group  
Manage security groups across your organization in AWS Organizations.
- AWS Network Firewall  
Manage filtering of network traffic entering and leaving VPCs.
- Amazon Route 53 Resolver DNS Firewall  
Manage DNS firewalls across your organization in AWS Organizations.

Security group policy type

- Common security groups  
Apply security groups to specified accounts and resources across your organization in AWS organizations.
- Auditing and enforcement of security group rules  
Check and manage the rules that are used in the security groups in your organization in AWS organizations.
- Auditing and cleanup of unused and redundant security groups  
Find and manage unused and redundant security groups across your organization in AWS organizations.

Third-party services

- Palo Alto Networks Cloud NGFW  
[View AWS Marketplace details](#)
- Fortigate Cloud Native Firewall as a Service  
[View AWS Marketplace details](#)

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

**Policy name**

Policy name  
demo-policy

The name must have 1-128 characters. Valid characters: a-z, A-Z, 0-9, -(hyphen), and \_(underscore).

Policy description  
this policy is for auditing the security groups

The description must have no more than 256 characters. Valid characters: a-z, A-Z, 0-9, -(hyphen), and \_(underscore).

Region  
US East (N. Virginia)

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.

**Policy rule options**

Choose how you want to configure policy rules.

Configure managed audit policy rules  
Use predefined rules that mitigate common security group configuration issues. You can customize the rules after you add them to your policy.

Configure custom policy rules  
Define the rules that you want to allow or deny using an audit security group.

**Policy rules**

Policy rules

Allow only the rules defined in the audit security groups.  
 Deny the use of any rules defined in the audit security groups.

Audit security groups

	Security group name	Description	Security group ID
<input type="checkbox"/>	demo-master-audit-sg	security group for audit	sg-0bd0c8283021bb1ee

25. Now you have to choose these options shown below.

26. And move to the review page and create your policy.

## Define policy scope

### Policy scope

Policy scope defines the accounts and resources covered by this policy.

AWS accounts this policy applies to

- Include all accounts under my organization
- Include only the specified accounts and organizational units
- Exclude only the specified accounts and organizational units, and include all others

Resource type

- EC2 instance
- Elastic Network Interface
- Security group

Resources

- Include all resources that match the selected resource type
- Include only resources that have all the specified resource tags
- Exclude resources that have all the specified resource tags, and include all other resources

Cancel

Previous

Next

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

AWS Firewall Manager policies (1)						
<input type="text"/> Find policies						
Name		Policy type	Policy ID	Protected accounts	Noncompliant accounts	Automatic remediation
<input type="radio"/>	demo-policy	Security group - audit	0f265849-bec8-4288-ae35-0eecfff47499	1	0	<input type="radio"/> Disabled

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.

The screenshot shows the AWS Config Rules interface. On the left, there's a sidebar with navigation links like Dashboard, Conformance packs, Rules, Resources, Aggregators, and Documentation. The main area is titled 'Rules' and contains a table with one row. The table columns are Name, Remediation action, Type, Enabled evaluation, and Detective compliance. The row shows 'FMMManagedSGContentAuditCo...' with 'Not set' under Remediation action, 'AWS managed' under Type, and 'DETECTIVE' under Enabled evaluation. Under Detective compliance, it says '3 Noncompliant resource(s)' with a warning icon.

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.

The screenshot shows the 'Resources in scope' section of AWS Firewall Manager. It lists three noncompliant resources: an EC2 Instance (ID: i-0af4de879ea46809b), an EC2 NetworkInterface (ID: eni-04f5b8829db5ea4ba), and an EC2 SecurityGroup (ID: sg-0a1a723f3b9a16175). Each resource is shown with its ID, Type, Status, Annotation, and Compliance status (Noncompliant).

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.

The screenshot shows the 'AWS Firewall Manager policies' page. It displays a single policy named 'demo-policy' with a Policy type of 'Security group - audit'. The policy has a Policy ID of '0f265849-bee8-4288-ae55-0ecffff47499', 2 Protected accounts, 1 Noncompliant accounts, and Automatic remediation is set to 'Disabled'. The status is 'Active'.

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

AWS Firewall Manager > Security policies > demo-policy

## demo-policy

**Overview**

Policy name demo-policy	Policy description this policy is for auditing the security groups	Type Security group - audit	Automatic remediation <span style="color: orange;">⚠️</span> Disabled
Region US East (N. Virginia)			

**Accounts and resources** | Policy details

**Accounts within policy scope (2)**

AWS account ID	Status	Details
878893308172	<span style="color: red;">☒</span> Noncompliant	Requires changes in related services. <a href="#">Details</a>
533267094905	<span style="color: green;">☑</span> Compliant	

**▶ Accounts outside policy scope**

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.

**Resources in scope**

Noncompliant
<span style="color: red;">☒</span> sg-0a1a723f3b9a16175 EC2 SecurityGroup - NOT_APPLICABLE <span style="color: orange;">⚠️</span> Noncompliant

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