# Application Security:

## AWS WAF: (Amazon web services – Web Application Firewall)

This service works as a robust firewall for web application to protect the resources used in web application when HTTP and HTTPs requests are being forwarded. It provides comprehensive protection for a range of resource types, including Amazon CloudFront, API Gateway, Application Load Balancer, AWS AppSync, Amazon Cognito, AWS App Runner, and AWS Verified Access instances. AWS WAF allows for efficient management of content access through the definition of specific conditions, such as source IP addresses or query string values.

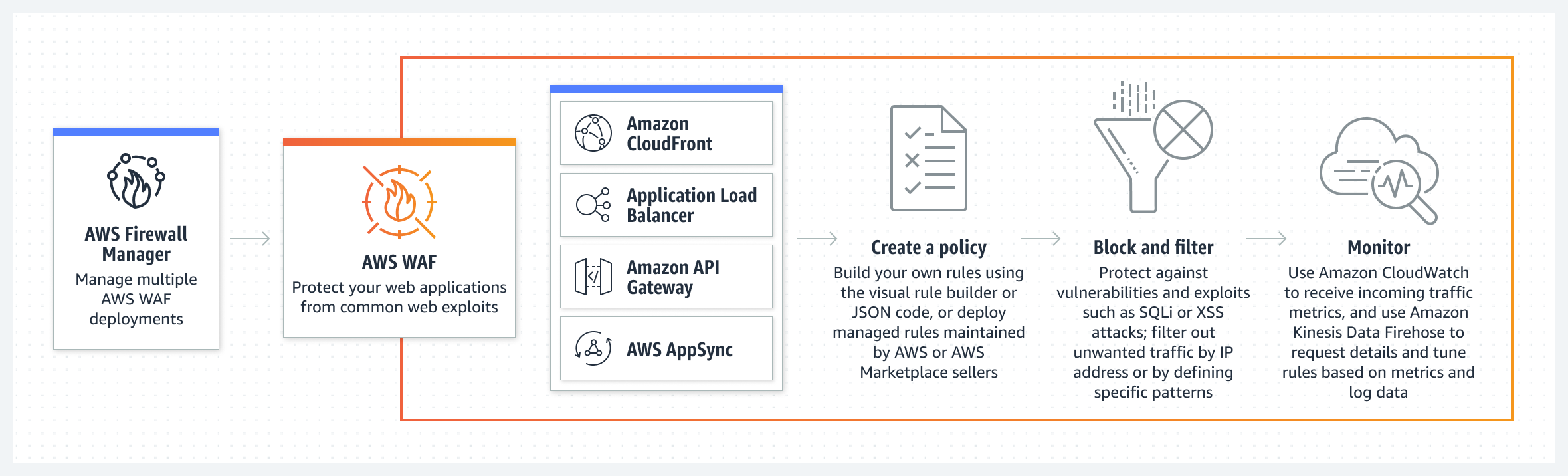


Figure: how AWS WAF works? Opted from :

Amazon. (2023). *How AWS WAF works* [image]. https://aws.amazon.com/waf/. <https://d1.awsstatic.com/Product-Page-Diagram_AWS-Web-Application-Firewall%402x.5f24d1b519ed1a88b7278c5d4cf7e4eeaf9b75cf.png>

Procedure: Here are the steps involved:

1. Configure AWS WAF Setup.

2. Establish a Web Application Firewall (WebACL).

3. Incorporate a string match rule.

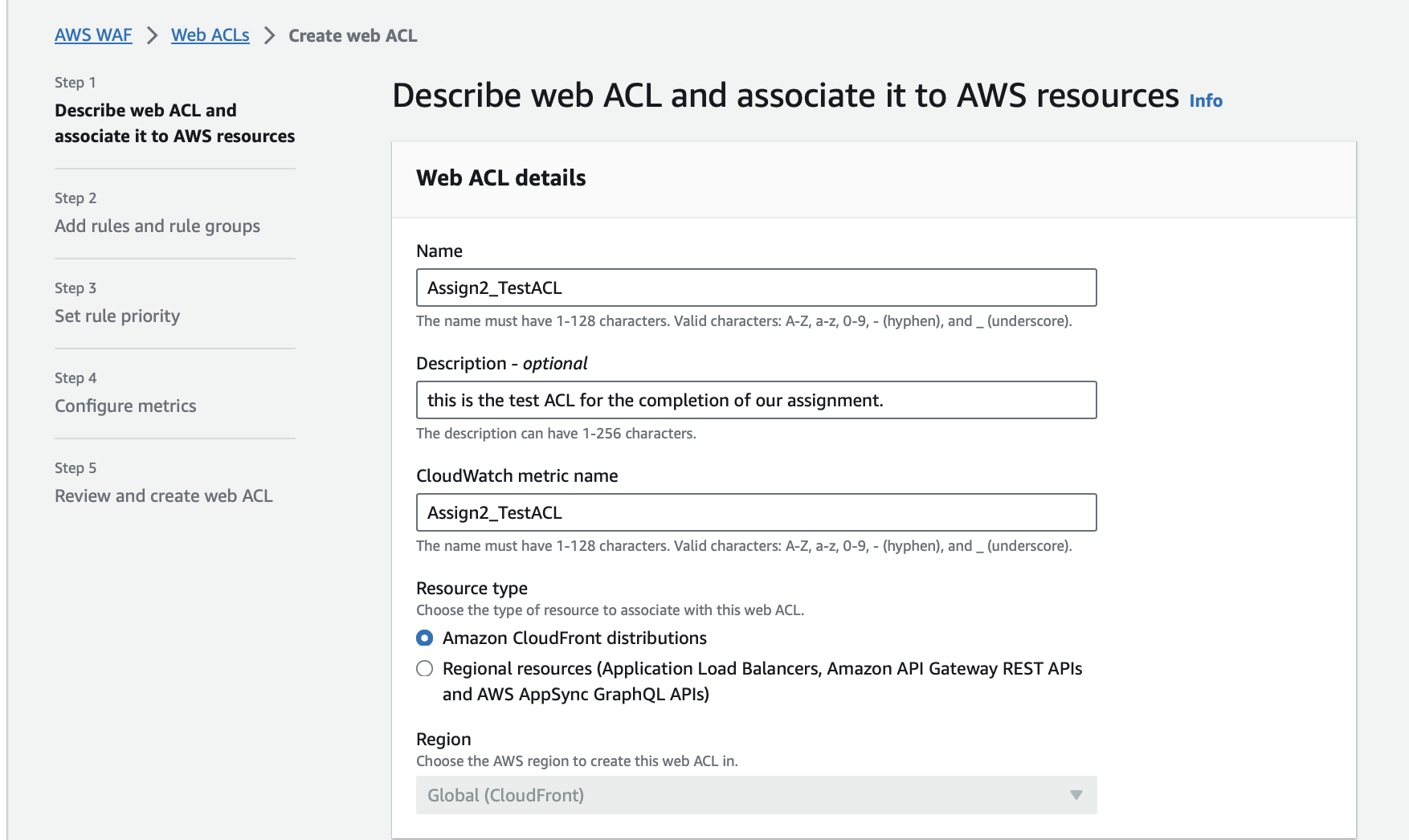
4. Integrate an AWS Managed Rules rule group.

5. Conclude the configuration of your WebACL.

6. Perform resource cleanup.

#### Procedure 1 and 2:

* AWS Console-> Security -> AWS WAF
* Then select create web ACL. Provide the details as mentioned in below snippet:



A screenshot of a web page

Description automatically generated

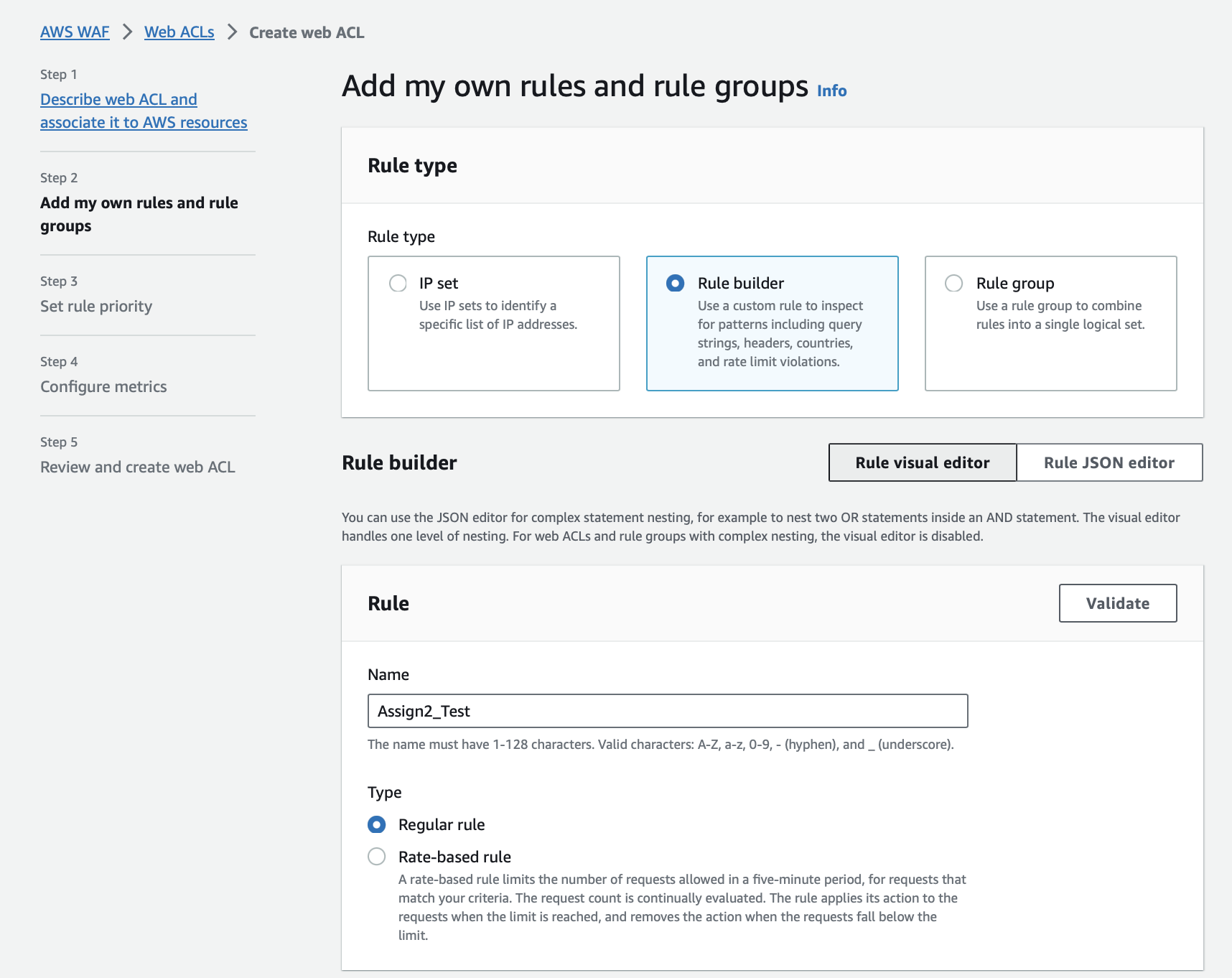
* Then hit Next: to add rules and rule group -> select Add rule dropdown and select add my own rules and rule group:

A screenshot of a computer

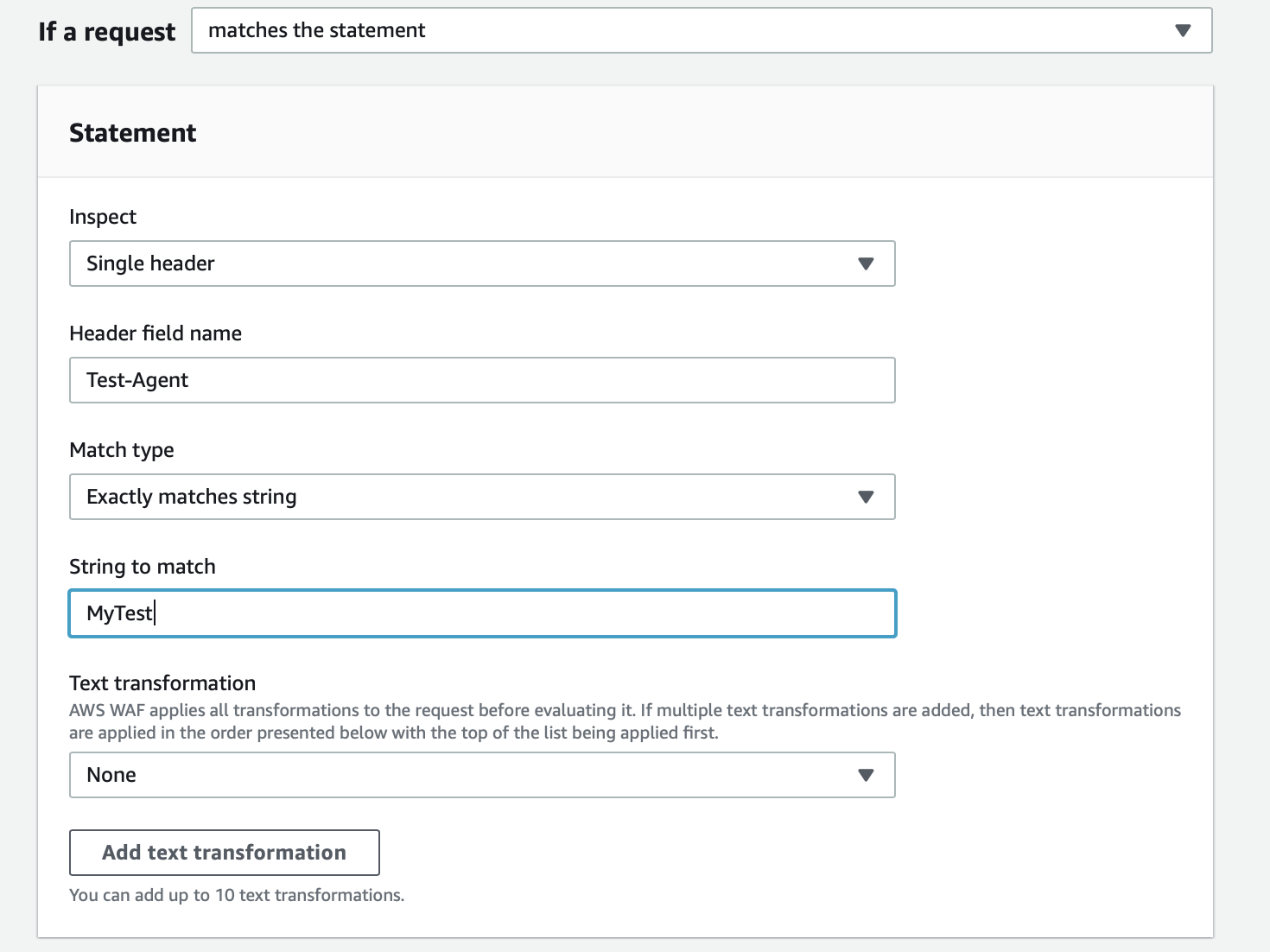
Description automatically generated

#### Procedure 3:

* Then provide the rule name and select the type as Regular Rule.



* Under the "Statement" section, within the "Inspect" category, access the dropdown menu, and select the web request element you desire AWS WAF to examine. In this illustration, opt for "Single Header." Leave rest as default or change as per the requirement and click on add rule.
* Upon selecting "Single Header," you will additionally define the specific header for AWS WAF to analyse. Input "Test-Agent" as the chosen header. It's important to note that letter casing is not relevant in this context.
* After that provide the match type and string to match for example “exactly matches string” and “MyTest”. Leave the text transformation to none and others to default or modify them according to needs.

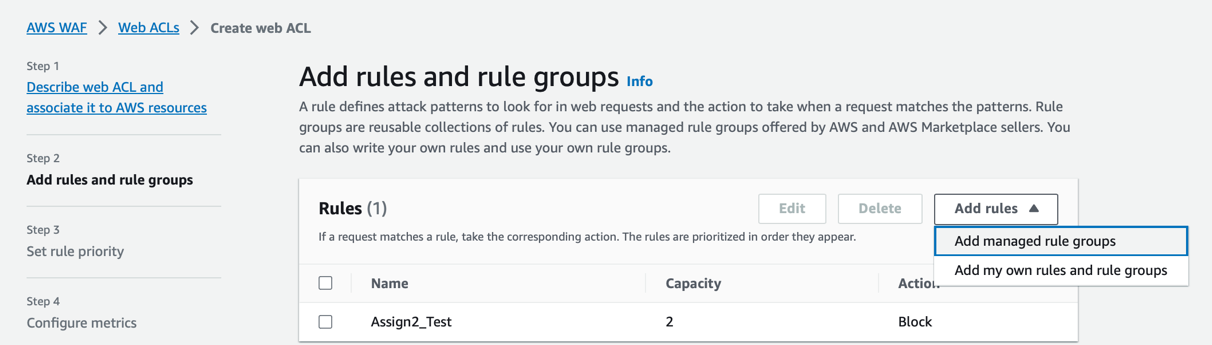


A screenshot of a computer

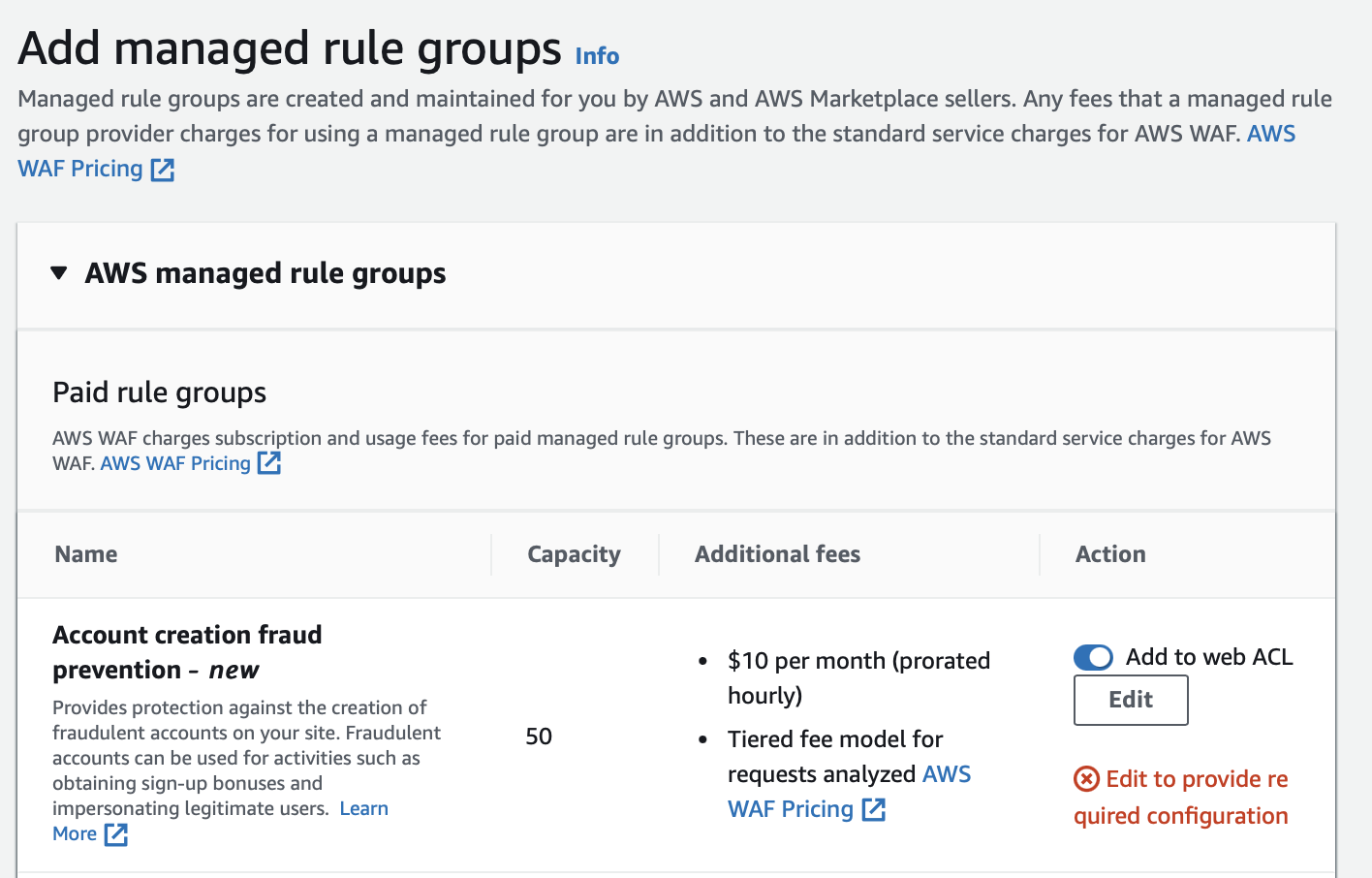
Description automatically generated

#### Procedure 4:

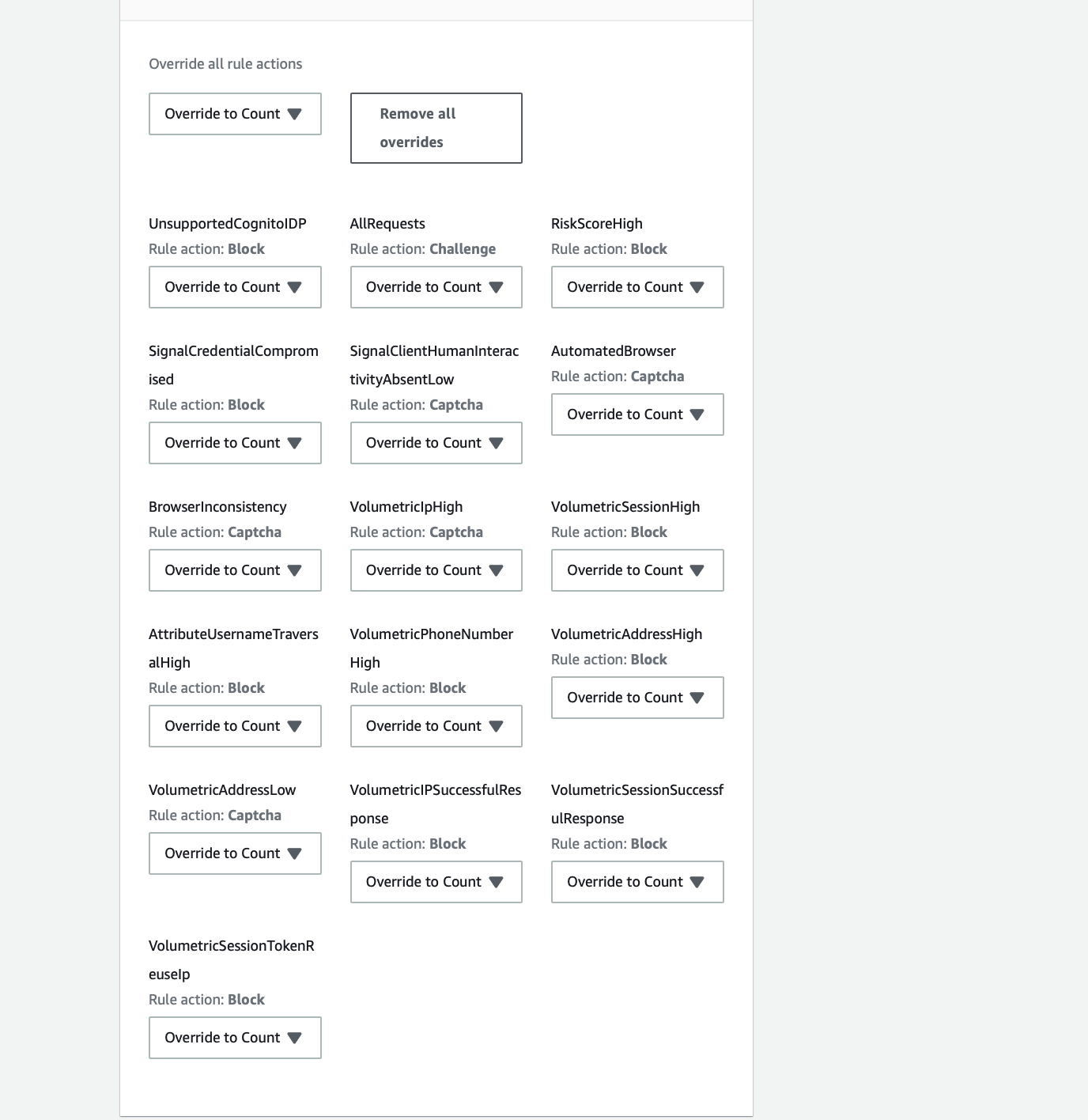
* Then click Add rule and Navigate to the "Add rules and rule groups" section and select "Add rules." Subsequently, opt for "Add managed rule groups."



* Within the "Add managed rule groups" section, expand the AWS managed rule groups listing. To add the desired rule group, follow these steps:
* Enable the "Add to web ACL" option in the Action column.



* Click "Edit," and within the rule group's Rules list, access the "Override all rule actions" dropdown. Choose "Count" to set all rules in the group to count-only mode.
* Save the rule.



A screenshot of a group action

Description automatically generated

* On the "Add managed rule groups" page, select "Add rules," which will take you back to the "Add rules and rule groups" page.

A screenshot of a web page

Description automatically generated

#### Procedure 5:

* Click on next and navigate to set rule priority.

A screenshot of a computer program

Description automatically generated

* Then click on next to go to the page for metrics configuration:

A screenshot of a computer

Description automatically generated

* At the last hit next again to Review and create the web ACL:

A screenshot of a web survey

Description automatically generated

A screenshot of a web page

Description automatically generated

A screenshot of a computer

Description automatically generated

Step 6:

To avoid additional AWS WAF charges, clean up AWS WAF objects or adjust the configuration for desired web request management.

## AWS Shield:

AWS Shield Standard and AWS Shield Advanced offer safeguards against Distributed Denial of Service (DDoS) assaults for AWS assets at both the network and transport layers (layer 3 and 4) as well as the application layer (layer 7). Shield's detection and mitigation capabilities are formulated to safeguard against threats, even if they haven't been previously identified by the service at the time of detection.

### Procedure:

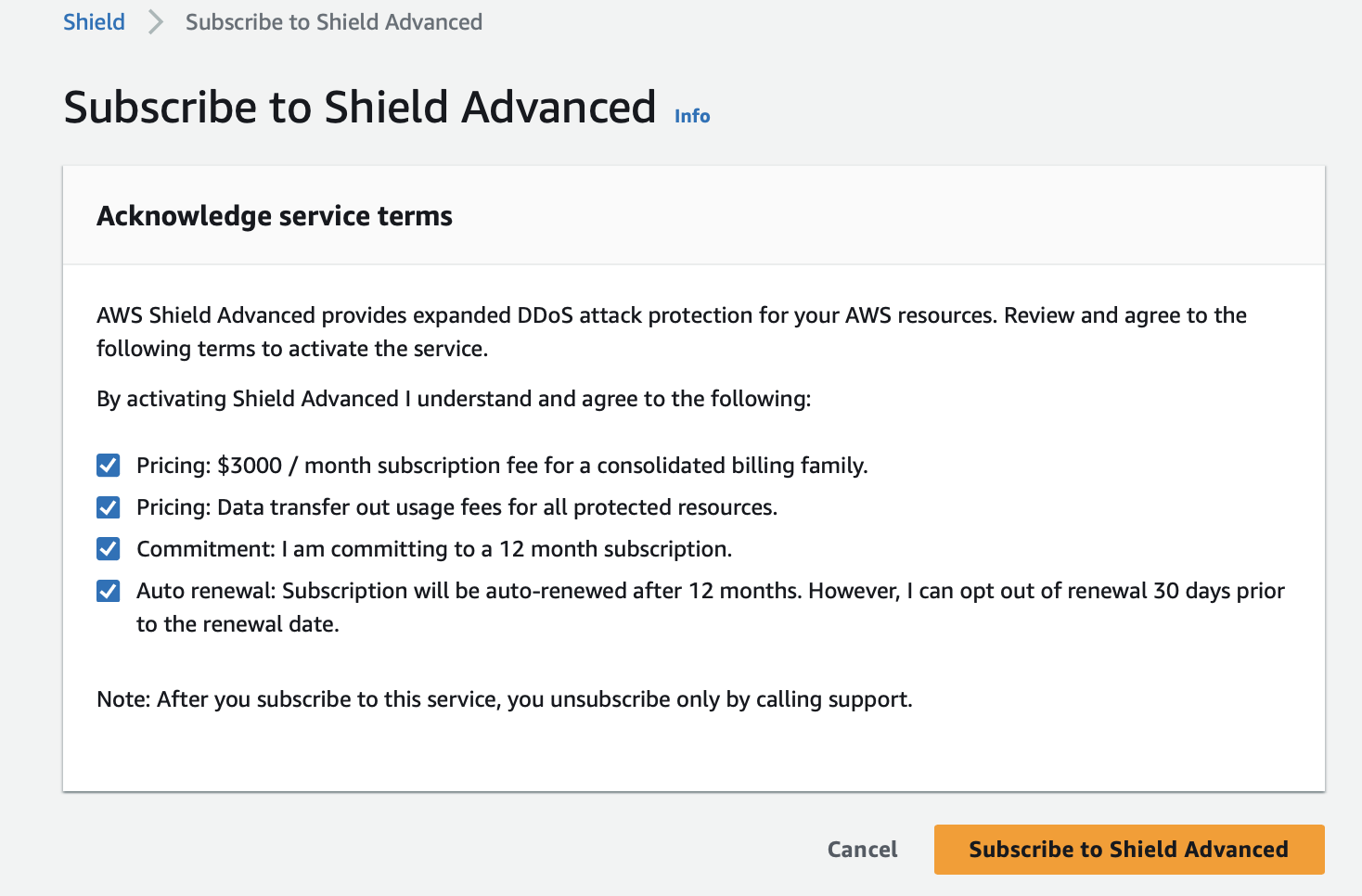
1. Start with shield Advance by subscribing it.
2. Employ protection to resources by configuring the safeguard.
3. Set up protection on application layer (layer 7) against distributed denial of service using AWS WAF.
4. Establish health-based detection for protections.
5. Customize notification and alarm.
6. Complete and Review protection step.
7. Deploy AWS SRT Assistance
8. Generate a dashboard for DDOS under CloudWatch and its configuration.

#### Procedure 1:

* Singin to Console then goto-> Security-> WAF&Sheild
* In the navigation bar-> select getting started-> click the subscribe to shield advance



* On the page read each term of the agreement-> select check box to accept the agreement.



* Click on Subscribe to shield advance.

#### Procedure 2:

* Select add resources-> On the "Select Resources to Safeguard with Shield Advanced" page, within the "Specify the Region and resource types" section, input the Region and resource type details for the resources you intend to secure.
* Pick the resources you need to safeguard. Shield Advanced populates the "Select Resources" section with AWS resources that meet your criteria, allowing you to filter the list by entering a search string.
* Add tags in tag section.
* Select protection as protect with shield advance.

#### Procedure 3,4, 5, 6, 7 and 8:

* For DDOS protection configuration create Web ACL as described above under AWS WAF procedures.
* To implement automatic DDOS mitigation opt for "Enable" and then specify the AWS WAF rule action you wish Shield Advanced to employ in its custom rules.
* For health-based detection, input the ID in the associate health check section and proceed to the notification page by clicking "Next."
* Select the topic to create the alert and notification and then hit next for review as well as to complete the process.
* Under console page of AWS shield service-> select configure shield response time (SRT) option-> edit the SRT rule as per the requirement-> then hit save.

A screenshot of a computer

Description automatically generated

Note: I cannot perform the activities to provide screenshots for procedures (2,3,4,5,6,7,8) on AWS console because of limited access issue.

A screenshot of a computer

Description automatically generated

## AWS Firewall Manager:

AWS Firewall Manager serves as a security management solution, facilitating the central setup and regulation of firewall regulations throughout AWS accounts and applications within AWS Organizations. It streamlines the process of enforcing consistent security rules, ensuring compliance for newly created applications and resources.

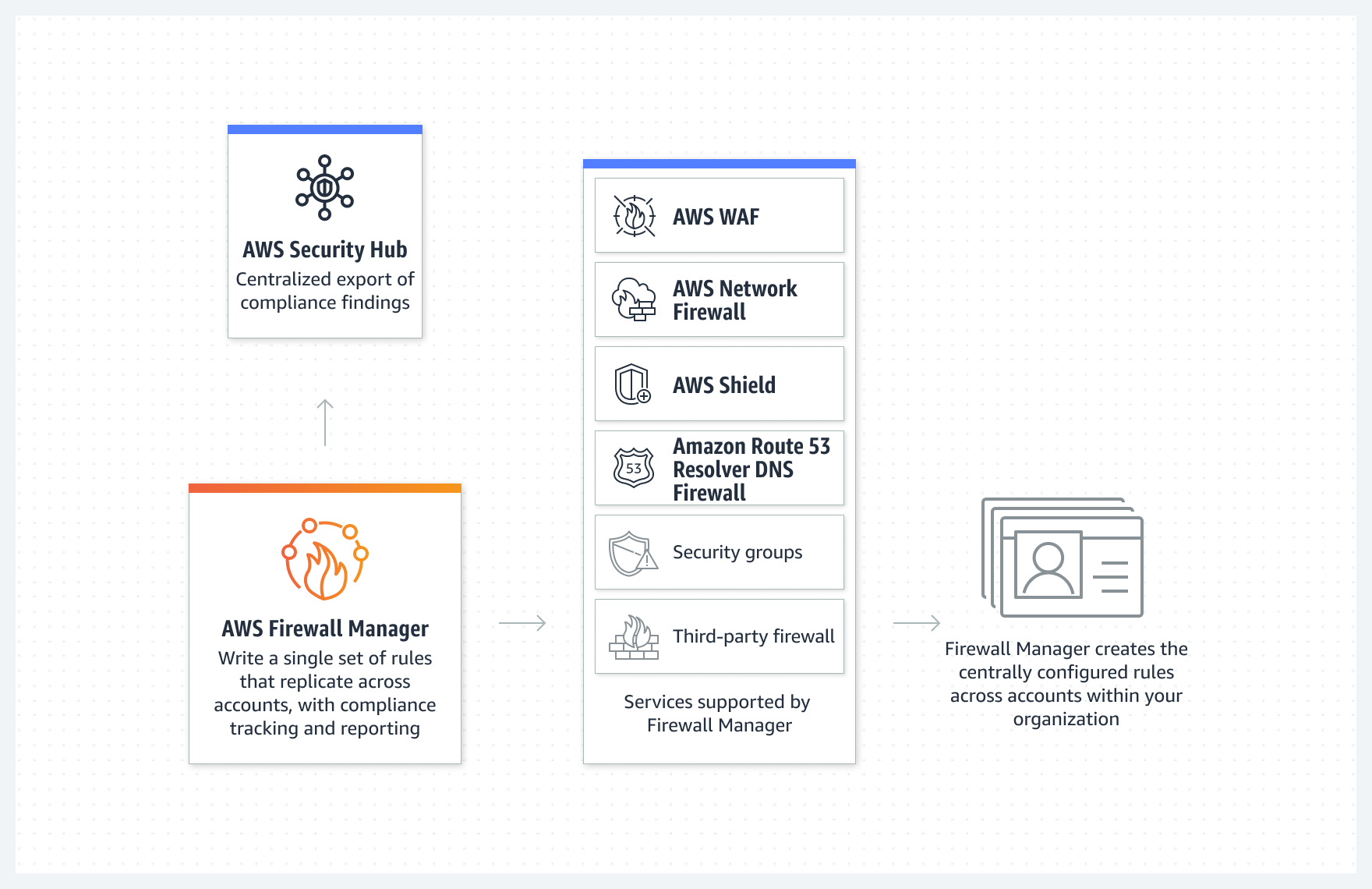


Figure : How AWS firewall manager works derived from: Amazon. (2023). How AWS firewall manager works. <https://d1.awsstatic.com/products/firewall-manager/product-page-diagram_AWS-Firewall-Manager%402x%20(1)1.ad6bf5281dc2c33c0493e9988e3504dd1590eaa2.png>

# Reference:

Amazon. (2023). AWS WAF, AWS Firewall Manager, and AWS Shield Advanced Developer Guide. <https://docs.aws.amazon.com/pdfs/waf/latest/developerguide/waf-dg.pdf>

Amazon. (2023). AWS firewall manager. Amazon Web Services, Inc. <https://aws.amazon.com/firewall-manager/>