Penta SECURITY

Cloudbric Managed Rules for AWS WAF Setting Guide v1.6

For End User (Public)

2026.06

Revision History

Date	Author	Revisions	Page	Notes
Dec 2022	Jay Park	Initial documentation		V1.0
May 2023	Jay Park	Description for Rule overrides using labels added.		V1.1
Jun 2023	Jay Park	Description for Tor IP Detection Rule Set added. Description for Rule Set versioning and update notification settings added.		V1.2
Aug 2023	Jay Park	Description for Bot Protection Rule Set added.		V1.3
Jun 2024	Jay Park	Name of the company changed to “Penta Security Inc.” Customer support email address changed. Description for Anonymous IP Protection added. Name of the product line changed to “Cloudbric Managed Rules.” Name of all managed rule groups changed following the change in the name of product line. Document updated in accordance with the most recent version of AWS console		V1.4
Dec 2024	Jay Park	Description for API Protection added		V1.5
Jun 2026	Dave Han	Description for Protocol Validity Protection Rule Set added.		V1.6

CONTENTS

1. Overview....4

1.1 What are “Cloudbric Managed Rules?”.... 4

1.2 Cloudbric Managed Rules Products.... 4

2. Setting Up Cloudbric Managed Rules....5

2.1 Subscribing to Cloudbric Managed Rules....5

2.2 Implementing Cloudbric Managed Rules....7

2.3 Selecting the Version of Cloudbric Managed Rules....12

2.4 Setting Up Notifications for Cloudbric Managed Rules....14

3. Canceling Cloudbric Managed Rules Subscription.... 17

3.1 Canceling Cloudbric Managed Rules Subscription....17

3.2 Deleting Cloudbric Managed Rules.... 19

3.3 Canceling Notifications for Cloudbric Managed Rules....21

4. Optimizing Cloudbric Managed Rules....23

4.1 Configuring Rule Action to “Count”....23

4.2 Adding Override Rules Based on Labels....26

5. Appendix.... 30

5.1 Frequently Asked Questions....30

1. Overview

This document was made to explain how an Amazon Web Services Web Application Firewall (AWS WAF) user can adopt Cloudbric Managed Rules (CMR) through subscribing to the service and implementing the service on AWS WAF. CMR is provided by Penta Security Inc. and is currently available for subscription in the AWS Marketplace.

1.1 What are "Cloudbric Managed Rules?"

Cloudbric Managed Rules for AWS WAF is a managed rule groups[1)] service developed and provided by Penta Security, an Independent Software Vendor (ISV) of AWS Marketplace and an official partner of AWS. CMR was developed by the security experts of Penta Security, based on the core technology that has provided security for its customers for nearly three decades. Penta Security is currently one of only seven ISVs to provide managed rule groups within AWS WAF, and CMR is continuously updated and managed by Penta Security to maintain a stable level of security while boosting the AWS WAF experience for the users.

1) Managed rule groups are collections of predefined, ready-to-use rules that AWS and AWS Marketplace sellers (such as Penta Security) write for AWS WAF users. Managed rule groups are available by subscription through AWS Marketplace. By subscribing to and implementing the managed rule groups with AWS WAF, users can immediately start protecting their web applications and APIs from general threats without having to define the security rules themselves.

1.2 Cloudbric Managed Rules Products

Name	Description
OWASP Top 10 Rule Set *Go to Subscribe*	Provides security against threats from OWASP Top 10 Web Application Security Risks such as SQL Injection and Cross-Site Scripting (XSS).
Malicious IP Protection *Go to Subscribe*	Provides security against Malicious IP traffic based on the Malicious IP Reputation List created using the ThreatDB, collected and analyzed by Cloudbric Labs[2)].
API Protection *Go to Subscribe*	Provides security against the OWASP API Security Top 10 Risk by establishing a defense system against known API attacks and providing validation and protection for XML, JSON, and YAML data.
Bot Protection *Go to Subscribe*	Provides security against malicious bots that negatively impact and damage websites and web applications through repetitive behaviors.
Anonymous IP Protection *Go to Subscribe*	Provides integrated security against Anonymous IPs originating from various sources including VPNs, Data Centers, DNS Proxies, Tor Networks, Relays, P2P Networks, etc.
Tor IP Protection *Go to Subscribe*	Provides security against Anonymous IP traffic, specifically originating from Tor network, which can be difficult to detect using an ordinary IP Risk Index.
Protocol Validity Protection *Go to Subscribe*	Provides security against any web request that breaks HTTP rules before it can reach your site.

2) Cloudbric Labs is Penta Security's proprietary Cyber Threat Intelligence (CTI) platform.

2. Setting Up Cloudbric Managed Rules

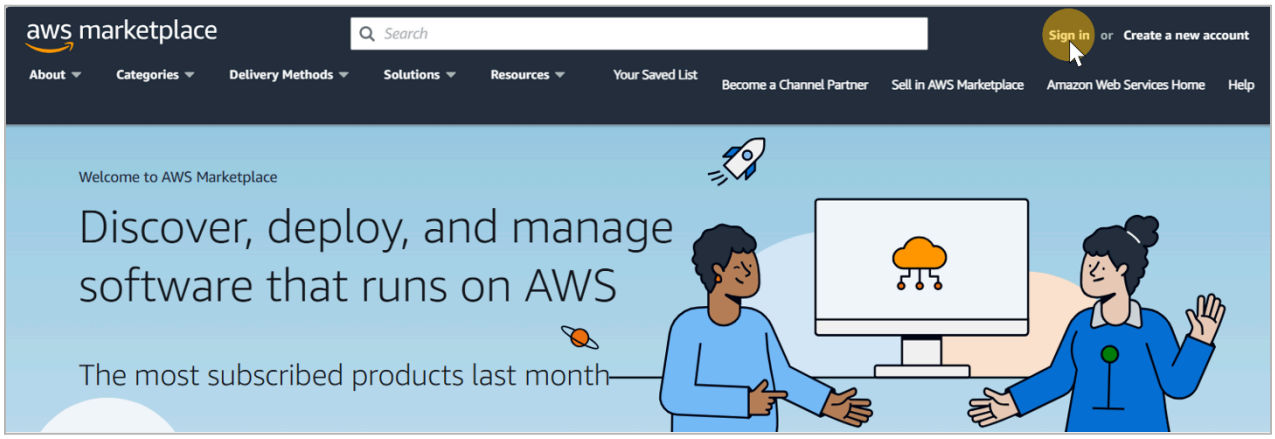
To set up CMR on your AWS WAF, you must first subscribe to the product. After subscribing to CMR, you can associate the managed rule groups with the web ACLs that you would create from the AWS WAF console and configure the detailed options, such as versions and notifications.

2.1 Subscribing to Cloudbric Managed Rules

- **Step 1**

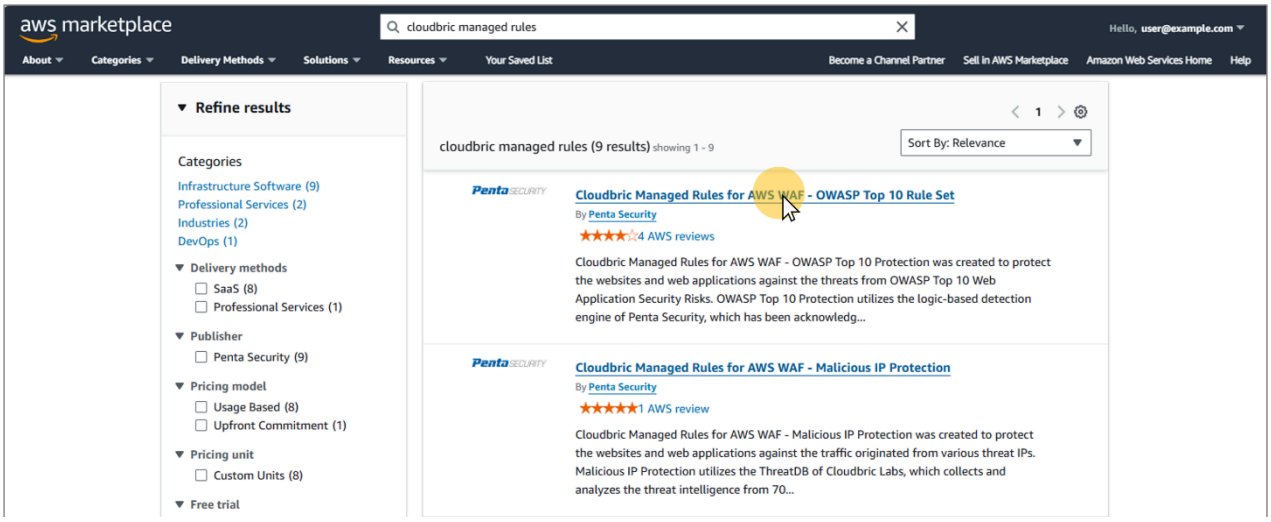
Login to AWS Marketplace with your AWS Account.

*AWS Marketplace Link: https://aws.amazon.com/marketplace



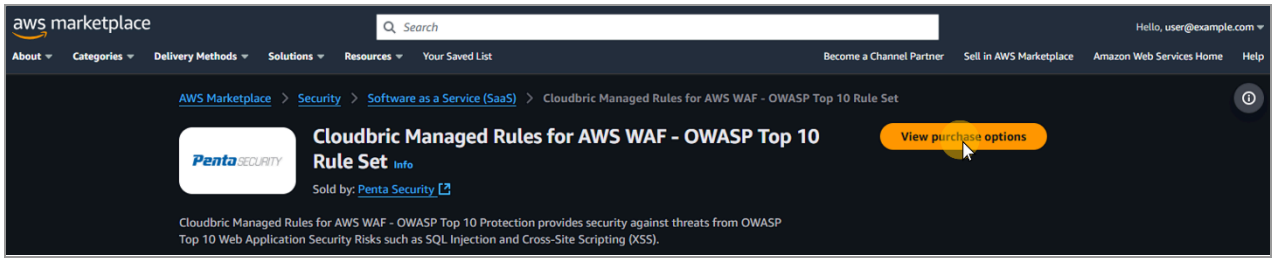
- **Step 2**

Search for "**Cloudbric Managed Rules"** and click the name of the managed rule group you wish to adopt.



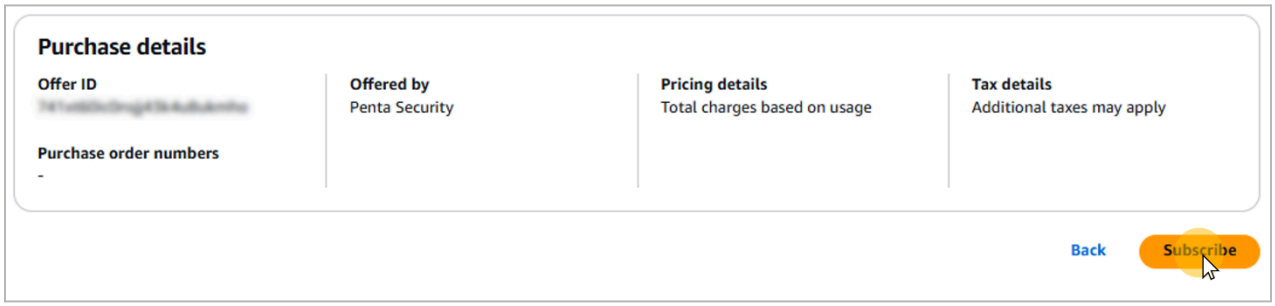
- **Step 3**

Please go over the description of the selected managed rule group, then select **[View purchase options]**.



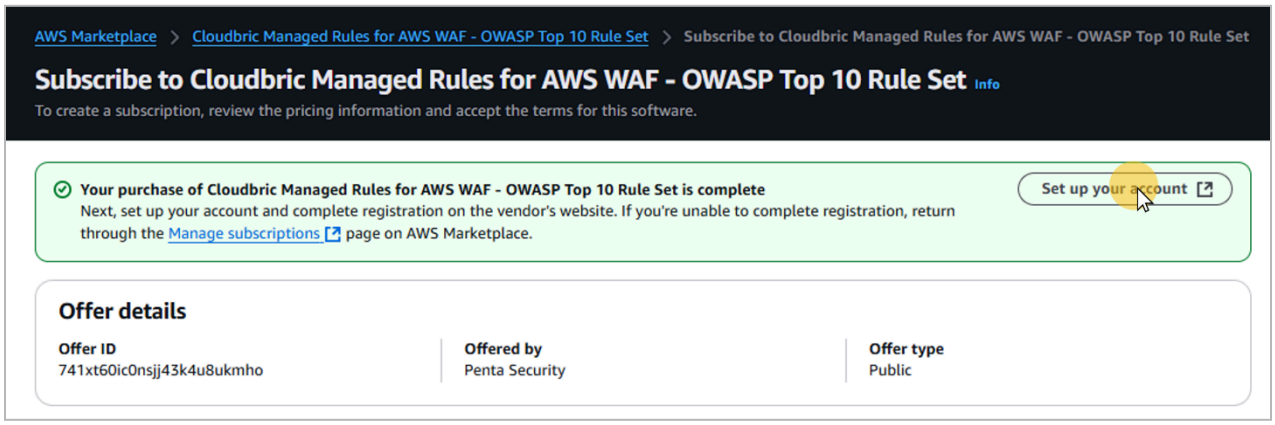
- **Step 4**

Review the terms and pricing information, then select **[Subscribe]**.



- **Step 5**

You are now subscribed to the managed rule group. To implement the subscribed managed rule group, click **[Set up your account]** and access the AWS WAF console.

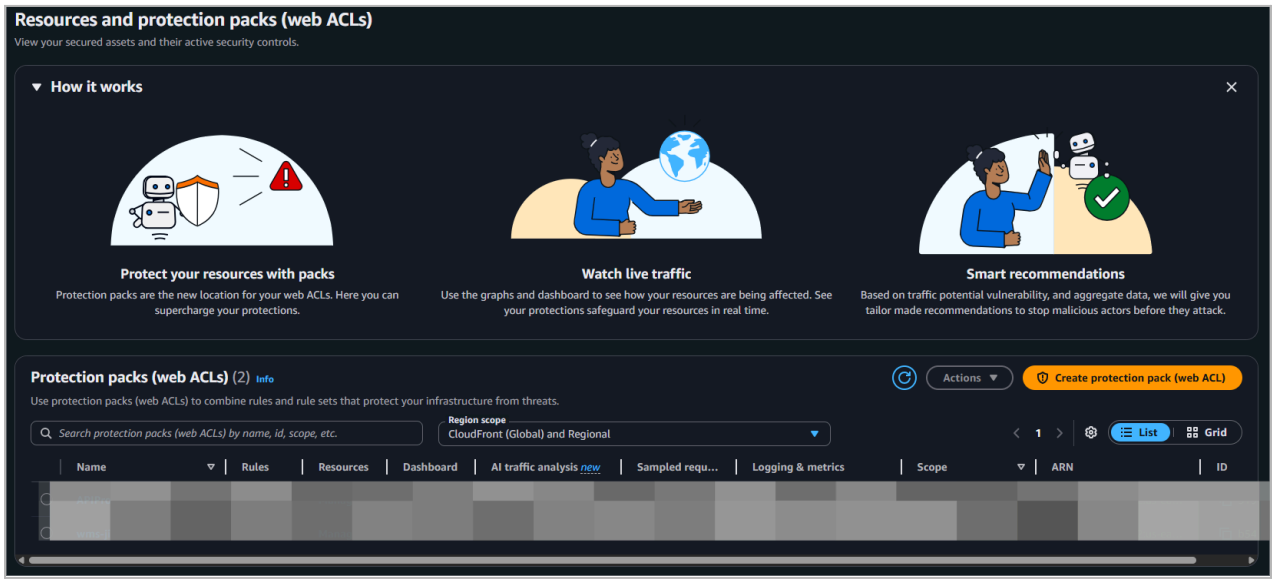


2.2 Implementing Cloudbric Managed Rules

- **Step 1**

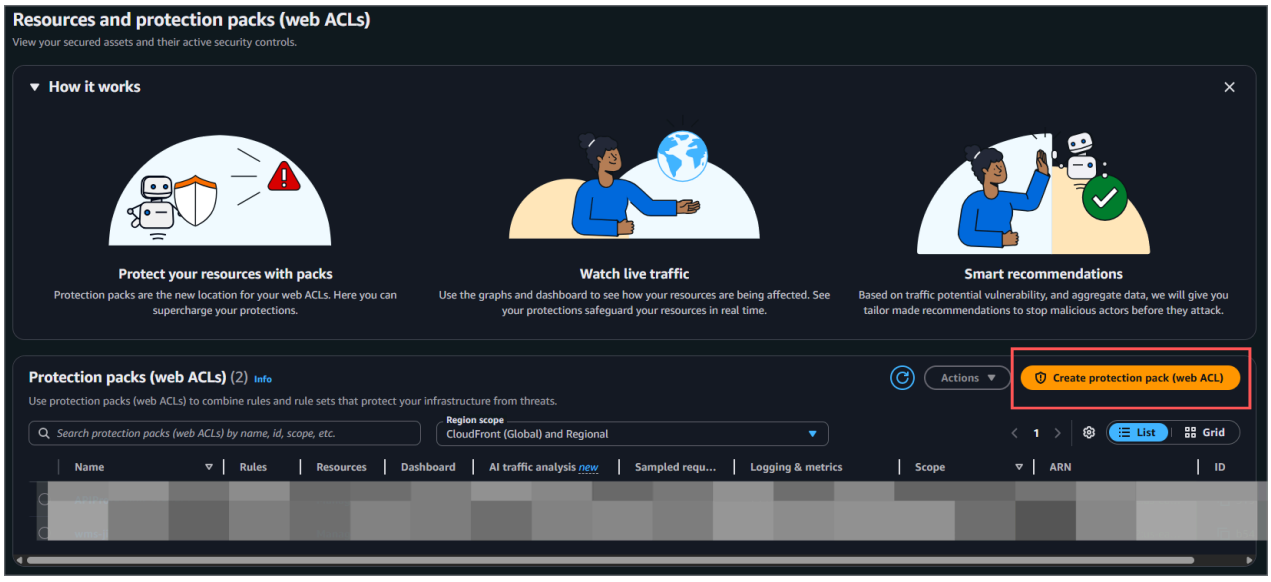
Sign in to the new AWS Management Console and open the AWS WAF console

*AWS WAF console: https://console.aws.amazon.com/wafv2-pro



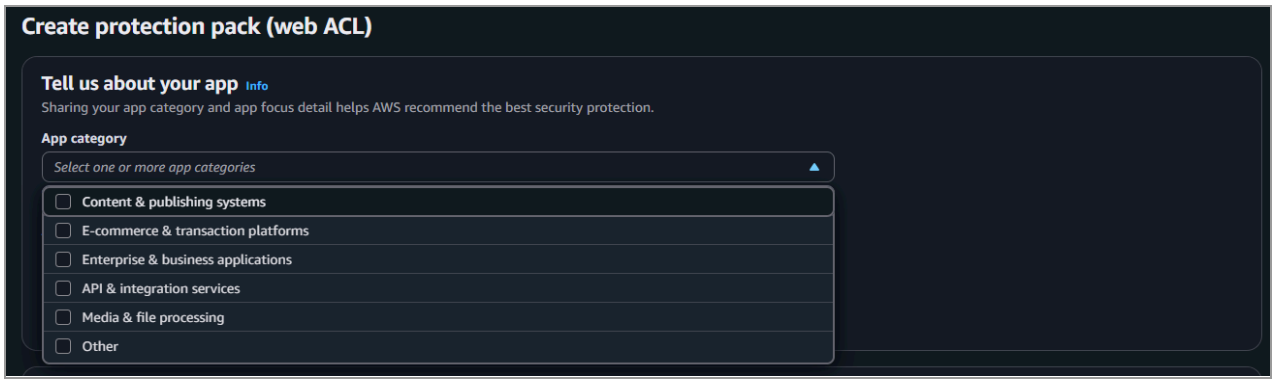
- **Step 2**

In the navigation pane, choose Resources & protection packs (web ACLs).



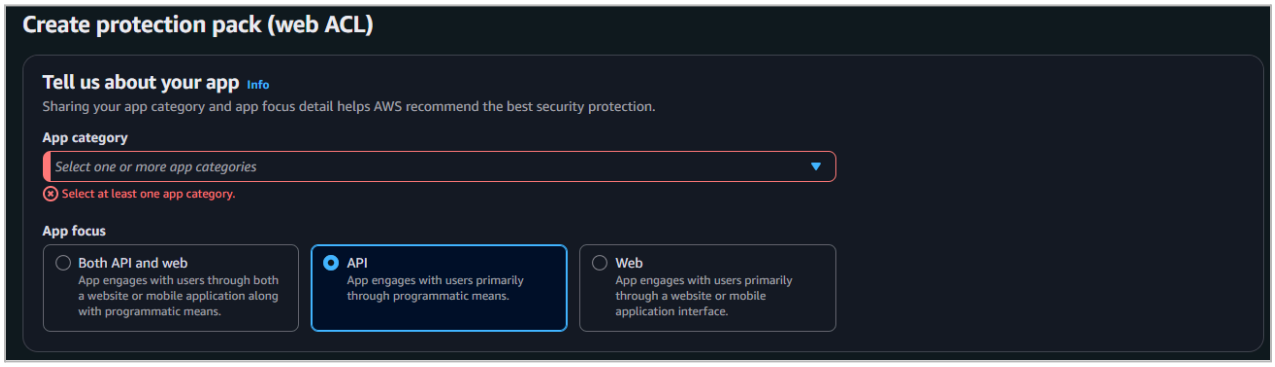
- **Step 3**

Under Tell us about your app, for App category, select one or more app categories.



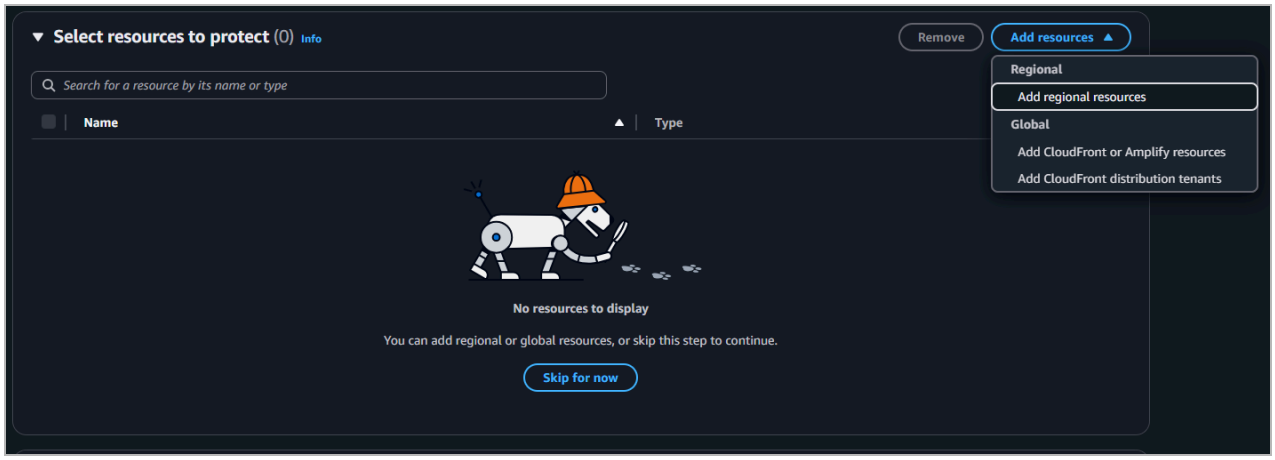
- **Step 4**

For Traffic source, choose the type of traffic the application engages with; API, Web, or Both API and Web.



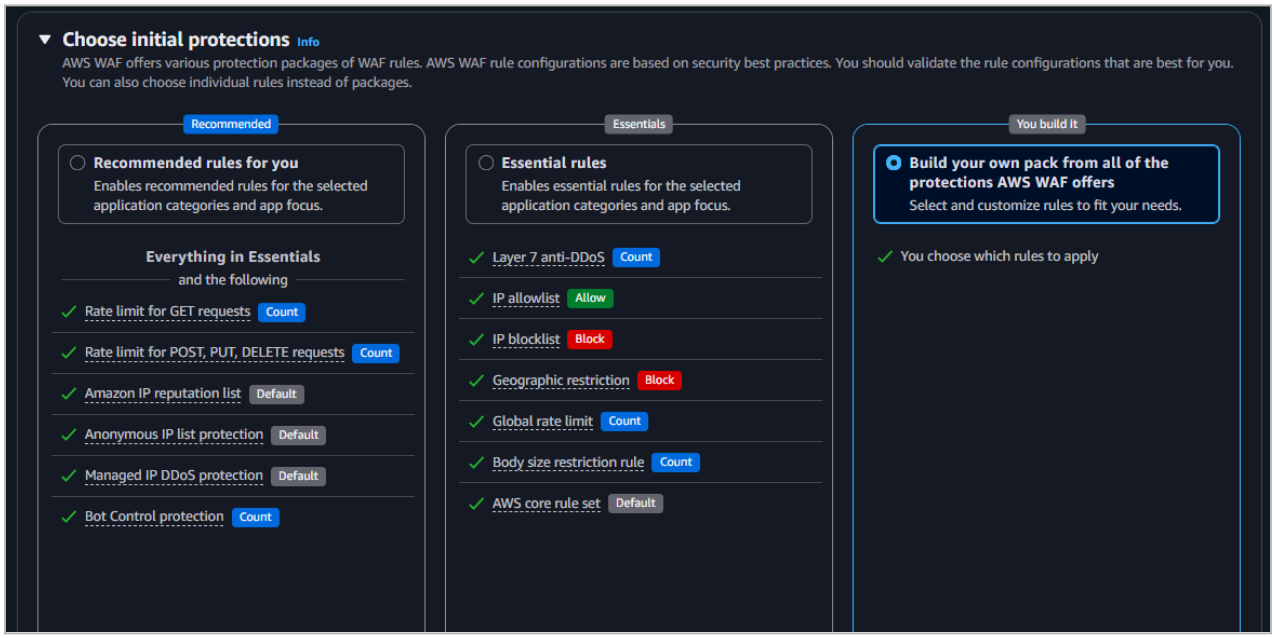
- **Step 5**

Under Resources to protect, choose Add resources.Choose the category of AWS resource that you want to associate with this protection pack (web ACL), either Amazon CloudFront distributions or Regional resources. For more information, see [Associating or disassociating protection with an AWS resource](#).



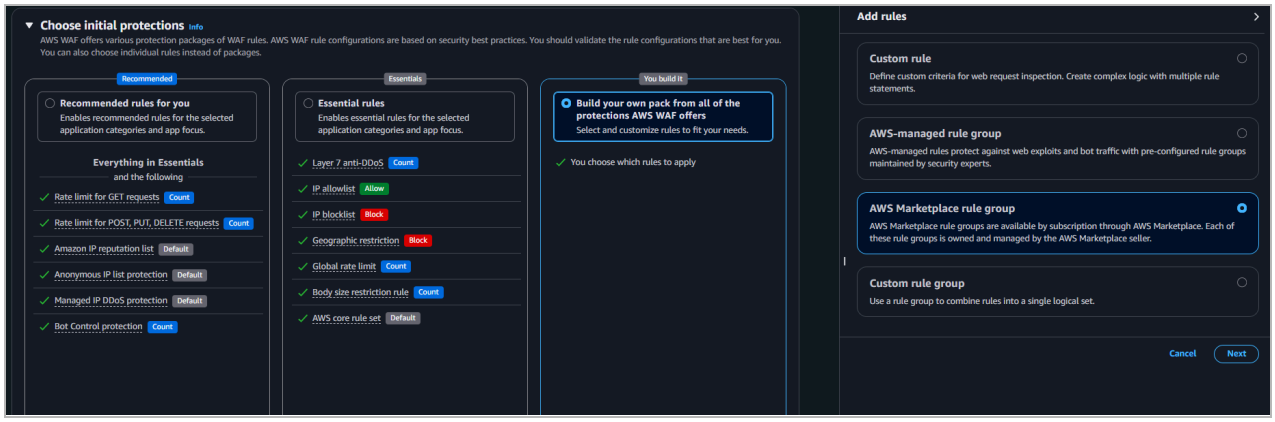
- **Step 6**

Under Choose initial protections, select ‘You build it’ protection level



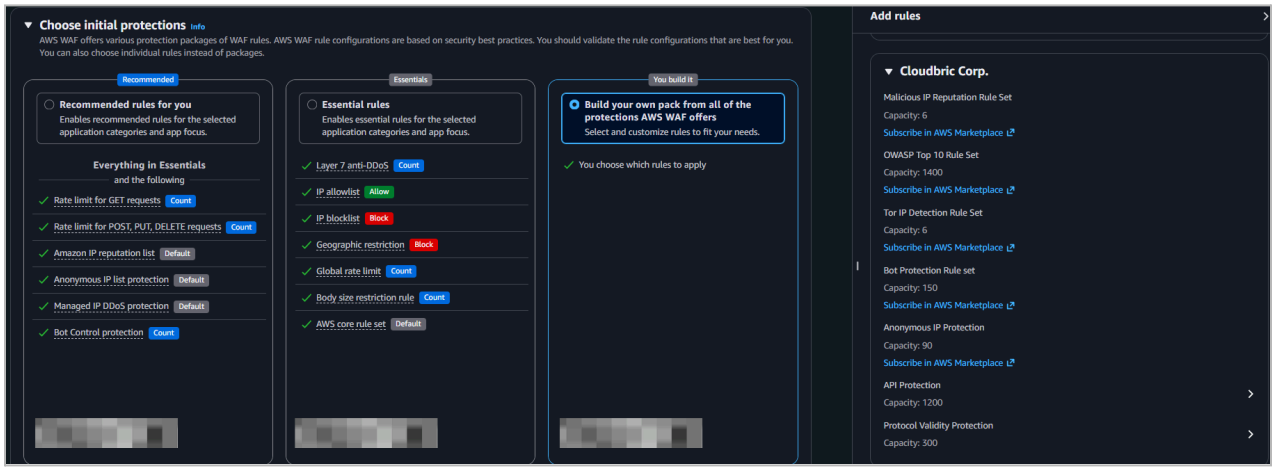
- **Step 7**

Click AWS Marketplace rule group and then choose Next.



- **Step 8**

On the Add rules page, expand the listing for Cloudbric Corp. Choose the version of the rule group. Choose Next.

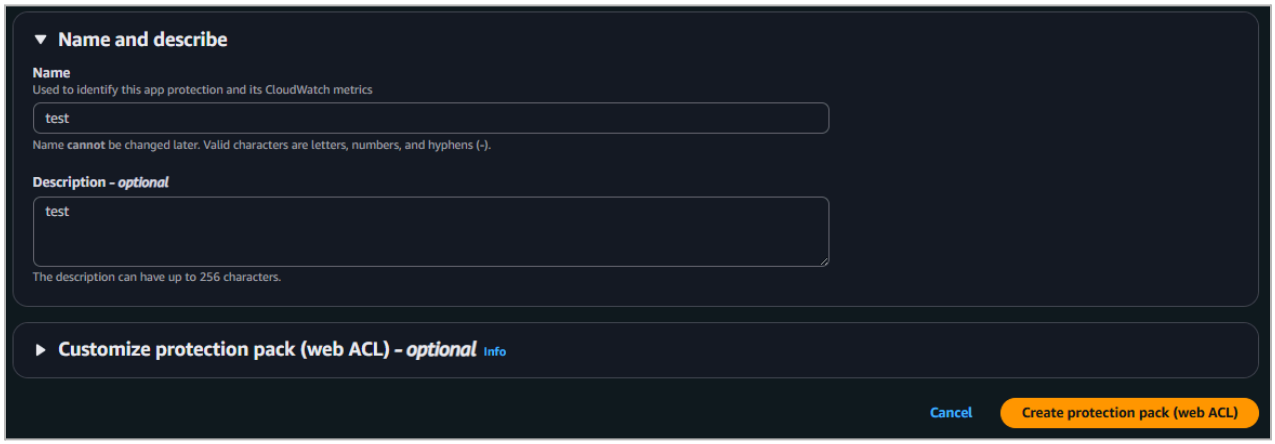


- **Step 9**

Under Name and description, enter a name for your protection pack (web ACL). Optionally, enter a description.

- **Step 10**

Review your settings and choose Add protection pack (web ACL).

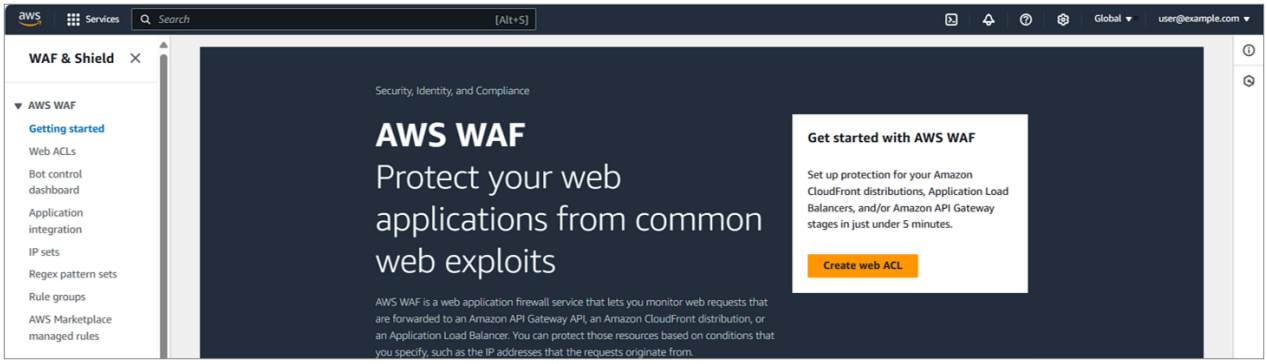


2.3 Selecting the Version of Cloudbric Managed Rules

- **Step 1**

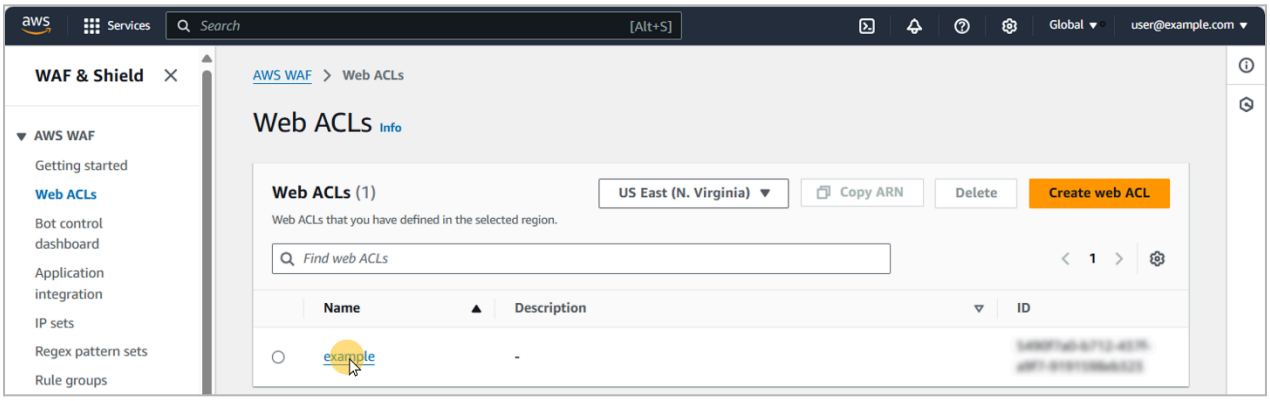
Go to AWS WAF console

*AWS WAF console: https://console.aws.amazon.com/wafv2/



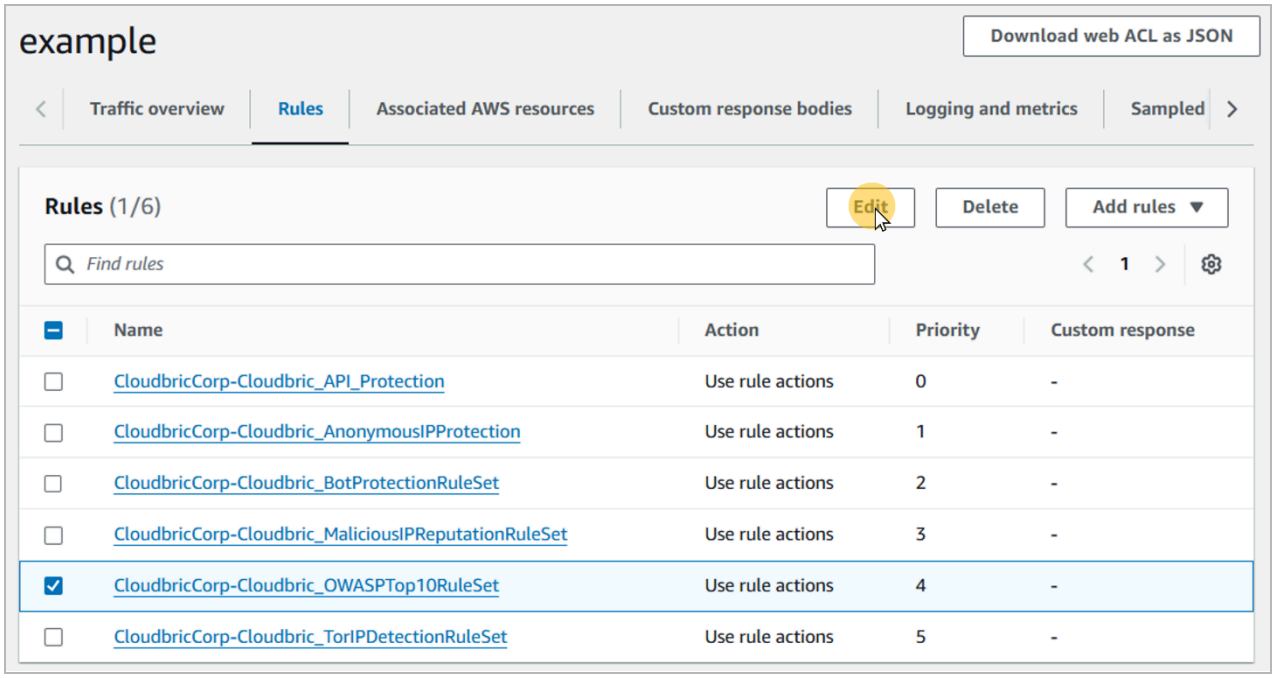
- **Step 2**

Go to the web ACLs menu and select the web ACL that you wish to implement a different version of Cloudbric Managed Rule Group.



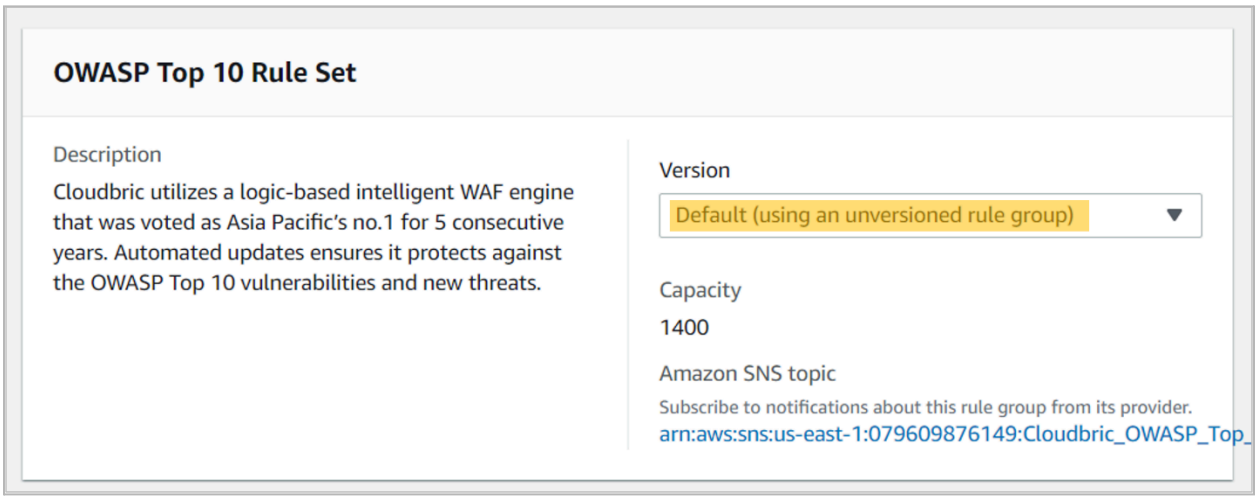
- **Step 3**

Select the **[Rules]** tab of the web ACL, select the managed rule group, and click **[Edit]**.



- **Step 4**

Select the version of the managed rule group and click **[Save rule]** to apply the changes.



*As the managed rule group is updated, new versions of the managed rule group will be available to be associated with the web ACL.

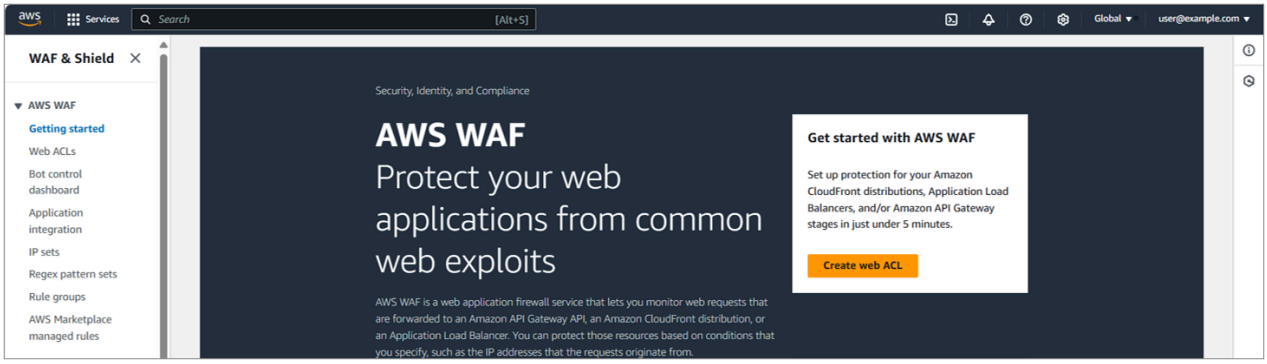
*The new versions of the managed rule group will not be automatically updated on your web ACL. If you wish to associate the new version of Cloudbric Managed Rule Group, you will have to change the version of the managed rule group manually.

2.4 Setting Up Notifications for Cloudbric Managed Rules

- **Step 1**

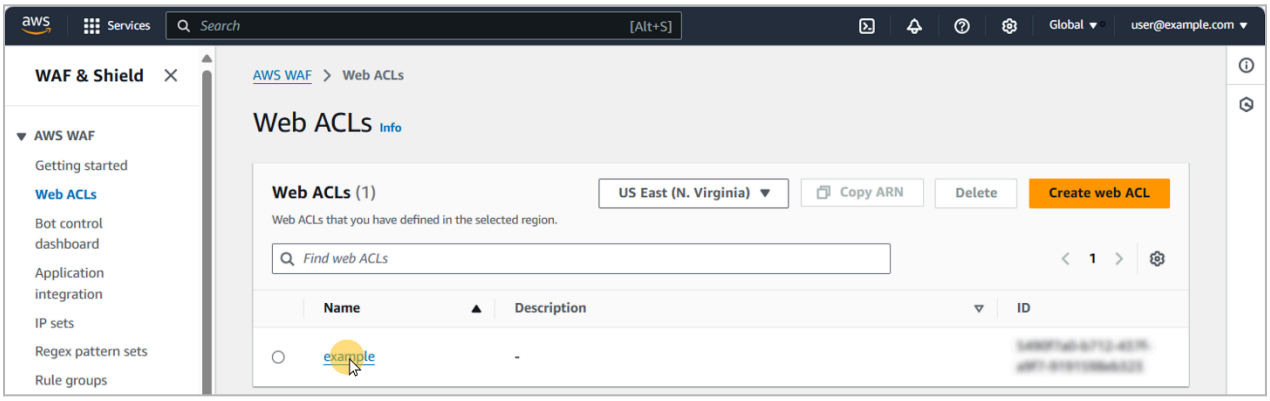
Go to AWS WAF console

*AWS WAF console: https://console.aws.amazon.com/wafv2/



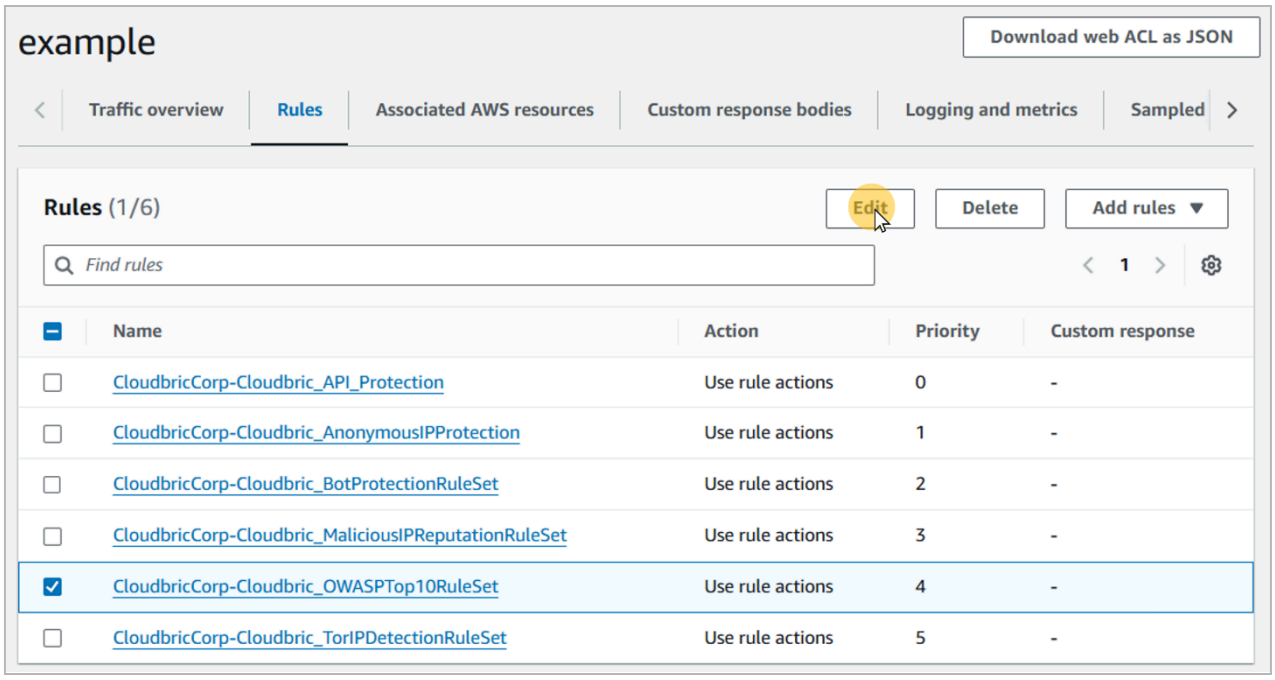
- **Step 2**

Go to the web ACLs menu and select the web ACL you associated with Cloudbric Managed Rule Group.



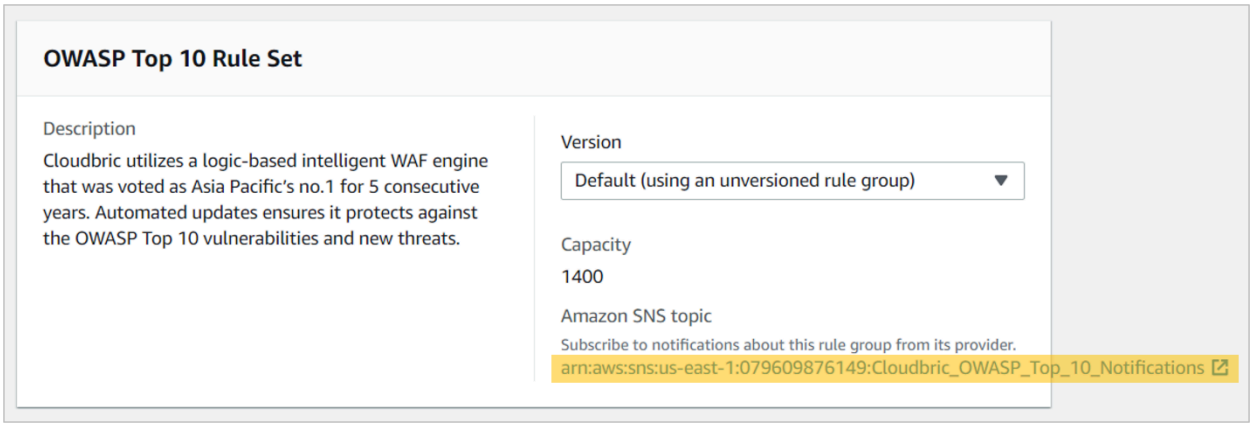
- **Step 3**

Select the **[Rules]** tab of the Web ACL, select the managed rule group, and click **[Edit]**.



- **Step 4**

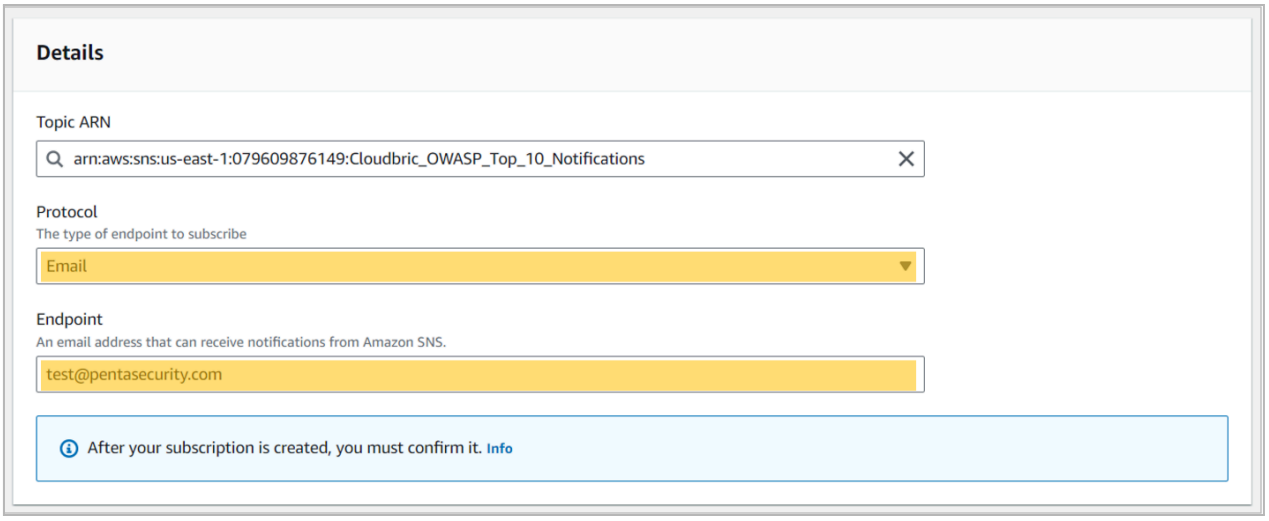
Copy the Amazon Resource Name (ARN) of the Amazon Simple Notification Service (SNS) topic for the selected Cloudbric Managed Rule Group and click on the ARN to configure the update notifications of Amazon SNS.



- **Step 5**

Enter the Protocol and Endpoint to receive the notifications of the updates.

- Topic ARN: ARN of the Amazon SNS topic copied from the previous step.
- Protocol: Select “Email.”
- Endpoint: Email address to receive the update notifications.



*If you wish to receive update notifications through protocols other than email, enter the endpoint that matches the protocol.

- **Step 6**

Complete the process of configuring the update notifications by clicking the “**Create subscription”** from the email sent to the email address you entered for the Endpoint in the previous step.

3. Canceling Cloudbric Managed Rules Subscription

If you wish to cancel the subscription for Cloudbric Managed Rules, Cloudbric Managed Rule Groups must be deleted from all web ACLs created in the AWS WAF console before canceling the subscription from the AWS Marketplace. Additionally, if you are subscribed to the Amazon SNS topic for Cloudbric Managed Rule Group, you may continue to be charged for the update notifications.

*You will continue to be charged for Cloudbric Managed Rule Group usage if it has not been deleted from the web ACLs, even after you canceled the subscription.

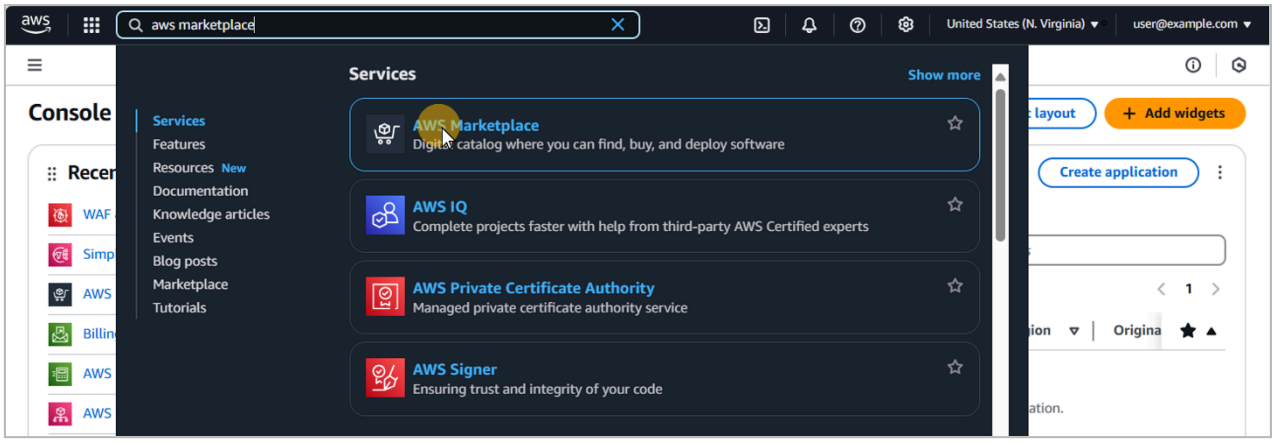
*You may also be charged for the update notifications of Cloudbric Managed Rule Groups if the subscription for Amazon SNS has not been canceled.

3.1 Canceling Cloudbric Managed Rules Subscription

- **Step 1**

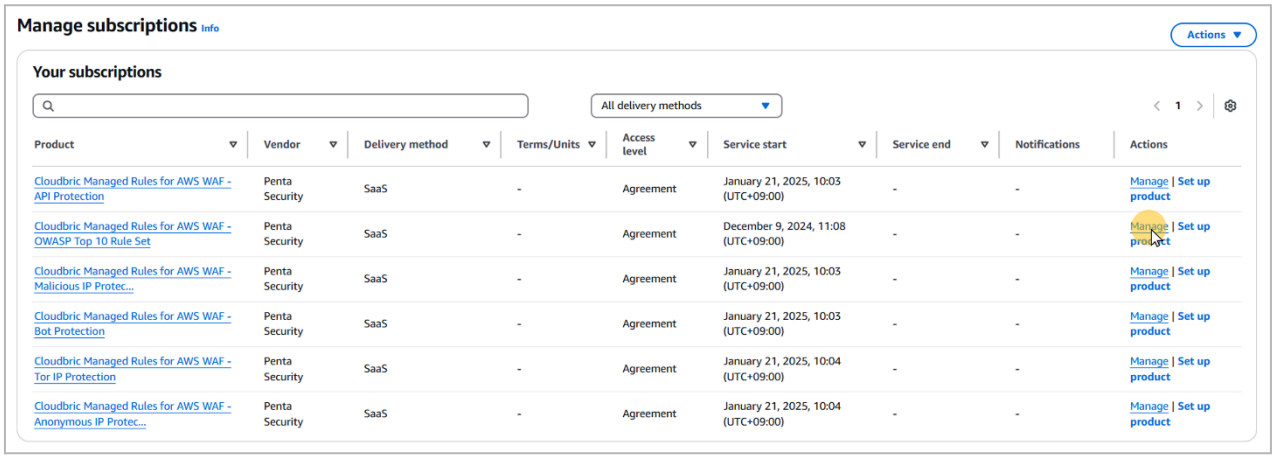
  Go to AWS Marketplace Subscriptions management console.

  *AWS WAF console: https://console.aws.amazon.com/marketplace/home#/subscriptions



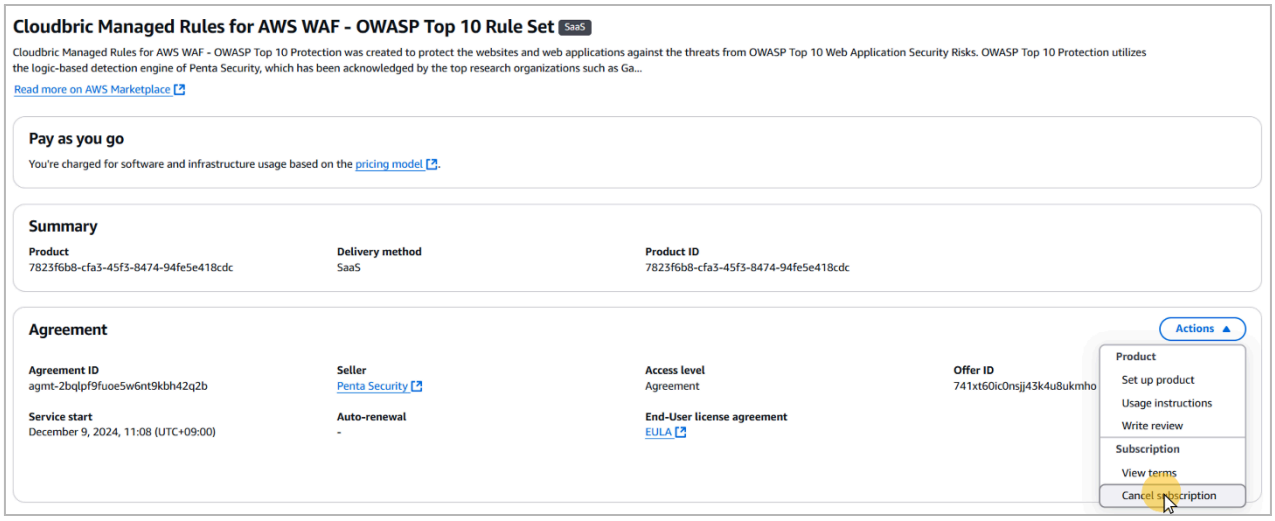
- **Step 2**

  Go to **[Manage subscriptions]** menu and click **[Manage]** for the Cloudbric Managed Rule Group you wish cancel the subscription.



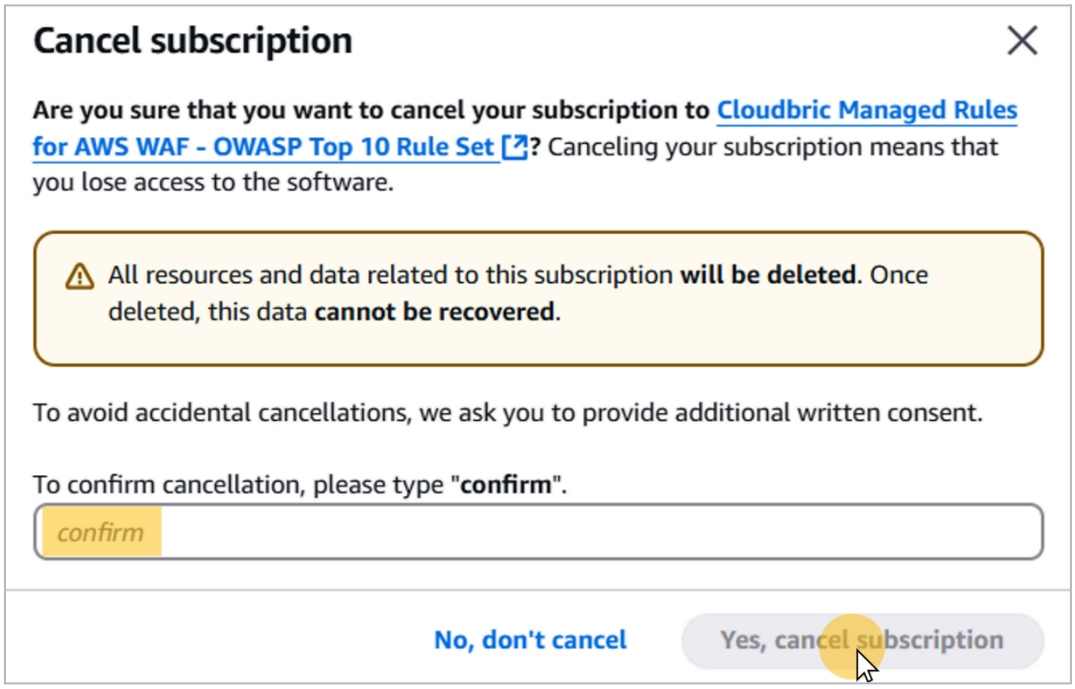
- **Step 3**

  Select **[Cancel subscription]** from the **[Actions]** drop down menu in **'Agreement.'**



- **Step 4**

  When the '**Cancel subscription**' pop-up appears, type **'confirm'** in the input box and click **[Yes, cancel subscription]** to complete the cancellation process.

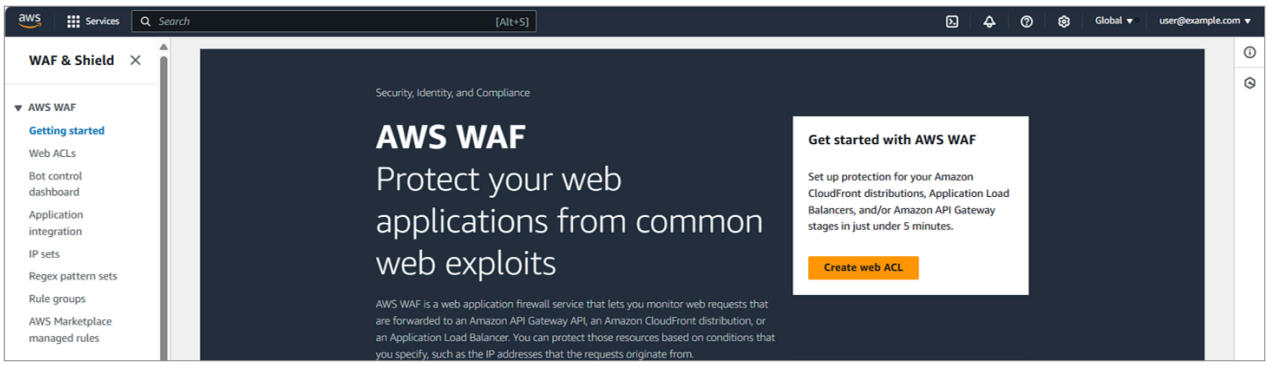


3.2 Deleting Cloudbric Managed Rules

- **Step 1**

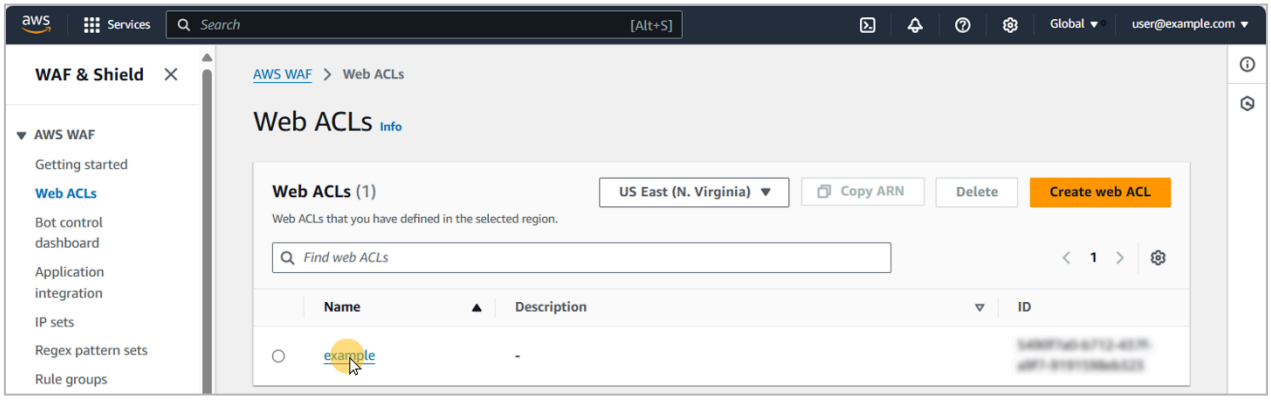
  Go to AWS WAF console

  *AWS WAF console: https://console.aws.amazon.com/wafv2/



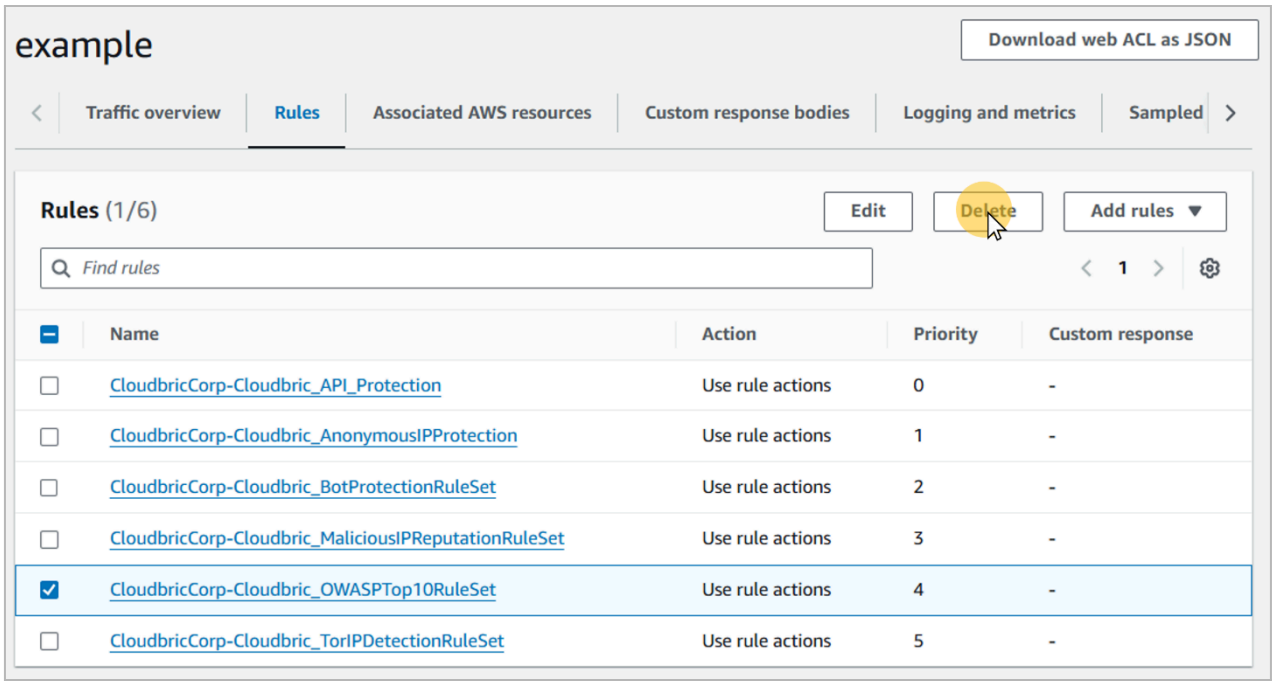
- **Step 2**

  Go to the web ACLs menu and select the web ACL you associated with Cloudbric Managed Rule Group.



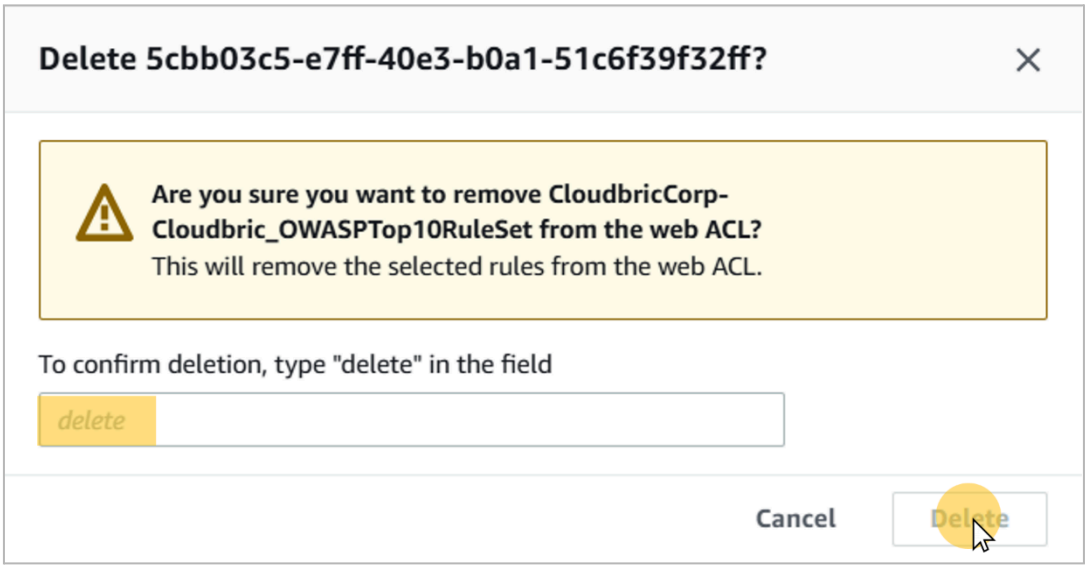
- **Step 3**

  Go to the **[Rules]** tab and select the Cloudbric managed rule group you wish to delete. Then click **[Delete]**.



- **Step 4**

  When the '**Delete**' pop-up appears, type '**delete**' in the input box and click **[Delete]** to complete the cancellation process.

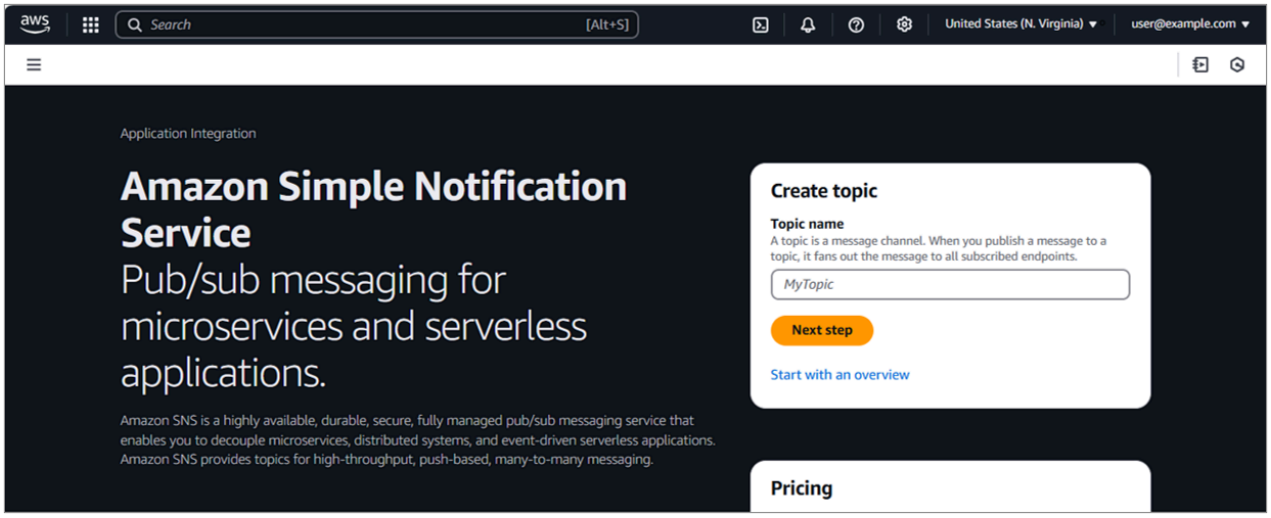


3.3 Canceling Notifications for Cloudbric Managed Rules

- **Step 1**

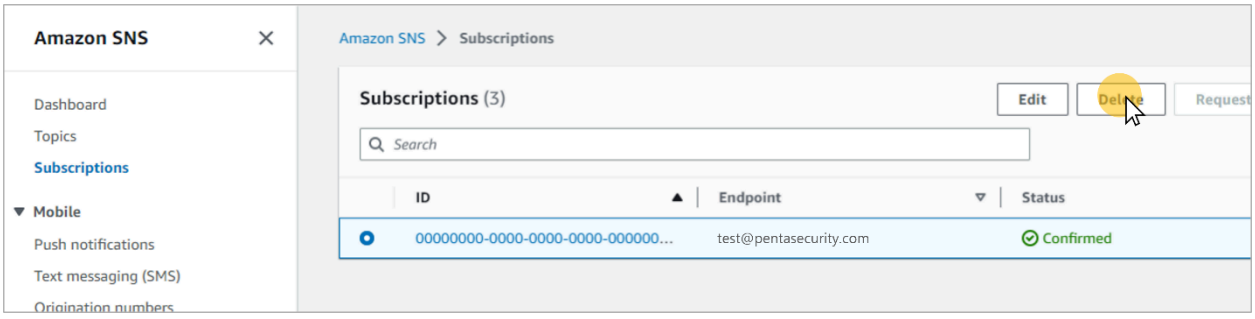
  Go to Amazon Simple Notification Service (SNS) console.

  *Amazon SNS console: https://console.aws.amazon.com/sns/home



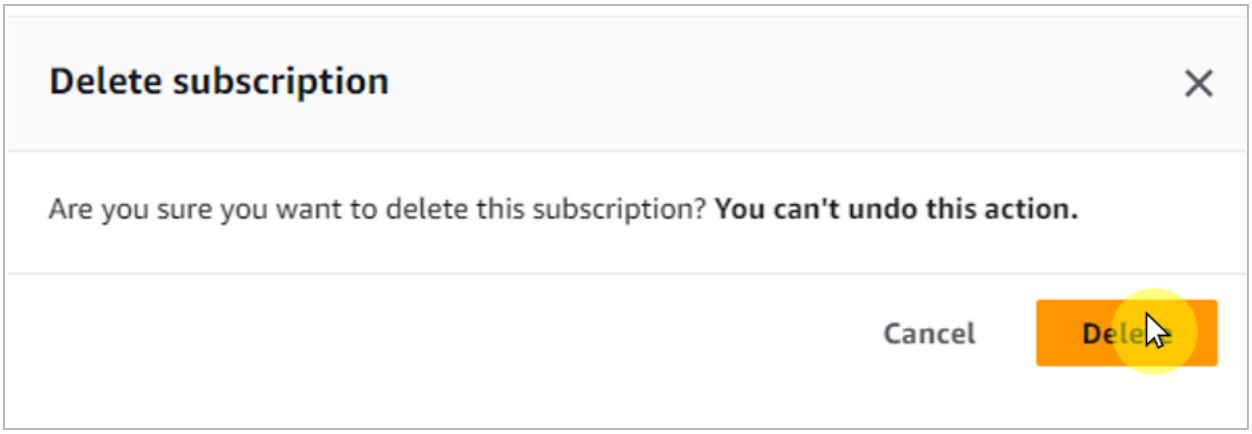
- **Step 2**

  Select the ID that is currently receiving the update notifications for the Cloudbric managed rule group from the '**Subscriptions**' menu and click **[Delete]**.



- **Step 3**

  Click **[Delete]** to confirm. Please note that this action cannot be undone.



4. Optimizing Cloudbric Managed Rules

When first implemented, all rule actions for individual rules in Cloudbric Managed Rule Groups are set to ‘Block’ by default. However, for certain rules, the rule action must be changed to ‘Count’ as soon as the managed rule groups are implemented. This adjustment is necessary because Cloudbric Managed Rules, unlike other managed rule groups that provide minimal security configurations and require users to add user-defined rules as needed, initially offer maximum security configurations. The setup allows users to override individual rules as needed, streamlining the process of rule optimization. The rules requiring their rule actions to be changed to ‘Count’ when initially associating the managed rule groups with the web ACL are as follows:

API Protection	Cloudbric_JSON_Protection_Check_Body_1 Cloudbric_JSON_Protection_Check_Body_2 Cloudbric_YAML_Protection_Check_Body Cloudbric_XML_Protection_Body_1
Anonymous IP Protection	ProxyIP_Medium VPNIP_Medium CSPIP_Medium IDCIP_Medium CDNIP_Medium RelayIP_Medium

After the initial rule optimization, false positives may occur when using Cloudbric Managed Rule Groups, where a legitimate request is falsely blocked by a rule, depending on the user’s unique environment. In such cases, the rule action for the rule causing the false positives must also be overridden to ‘Count.’ To maintain the performance of Cloudbric Managed Rules, overrides should only be applied to the rules that caused the false positives, apart from the rules initially changed to have the rule action set to ‘Count,’ in associating the managed rule groups to the web ACL. These overrides can also be implemented by adding a label-based, user-defined rule.

*All rules in Cloudbric Managed Rules for AWS WAF – OWASP Top 10 Rule Set are preconfigured with labels.

*The IP-based Cloudbric managed rule groups are not configured with any labels due to the dynamic tendency of the IP list. If you need to override a specific IP, you must create an additional rule, allowing the IP.

4.1 Configuring Rule Action to “Count”

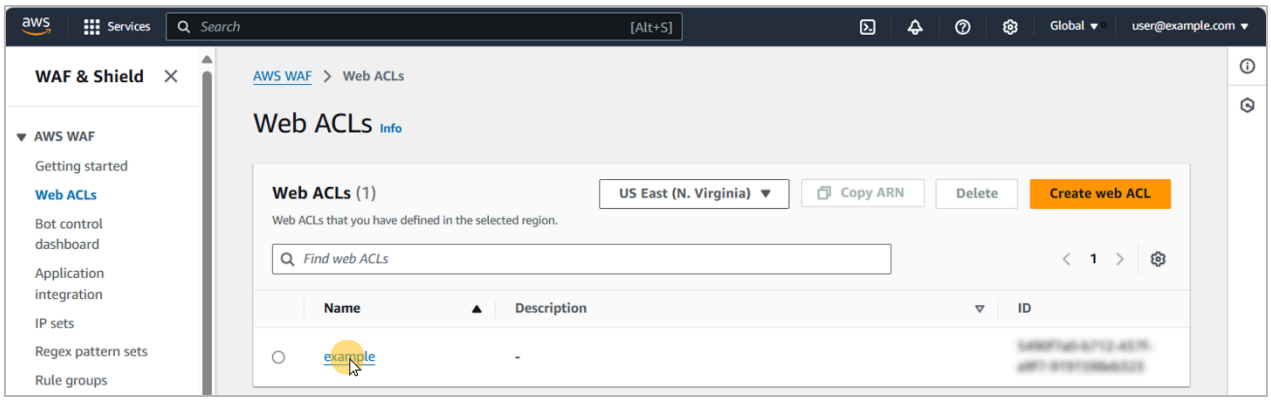
- **Step 1**

  Go to AWS WAF console

  *AWS WAF console: https://console.aws.amazon.com/wafv2/

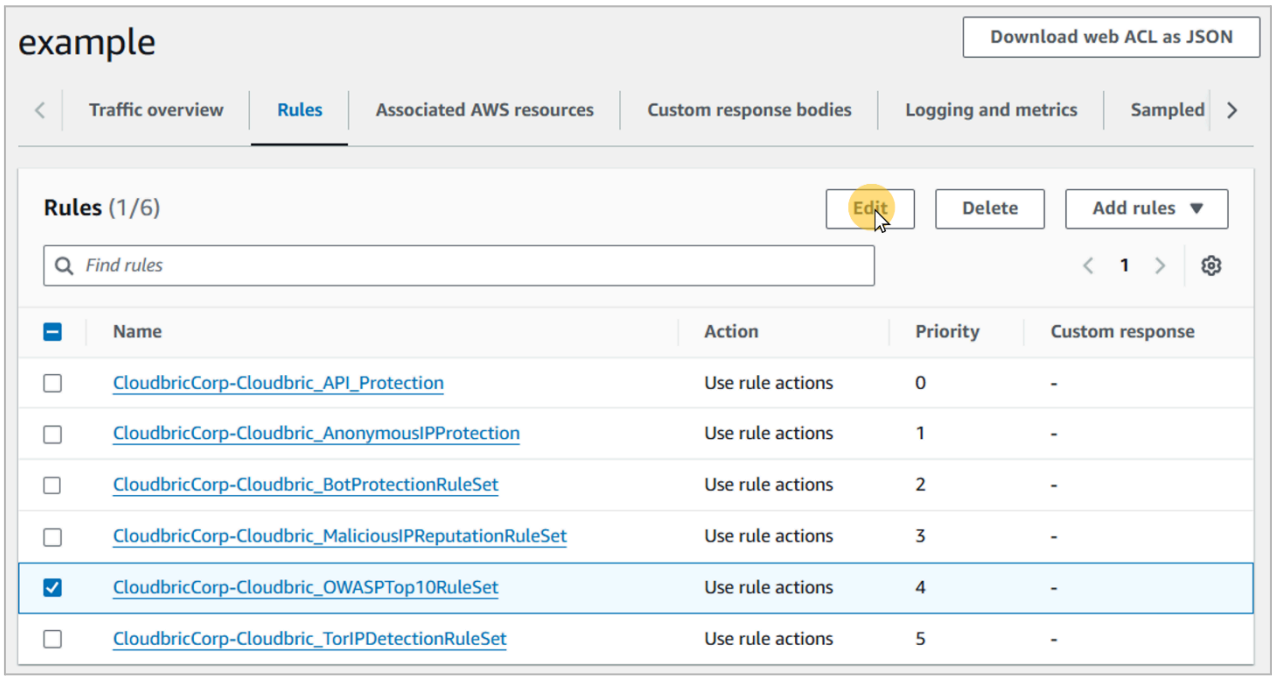
- **Step 2**

  Go to the web ACL menu and select the web ACL associated with a Cloudbric managed rule group.



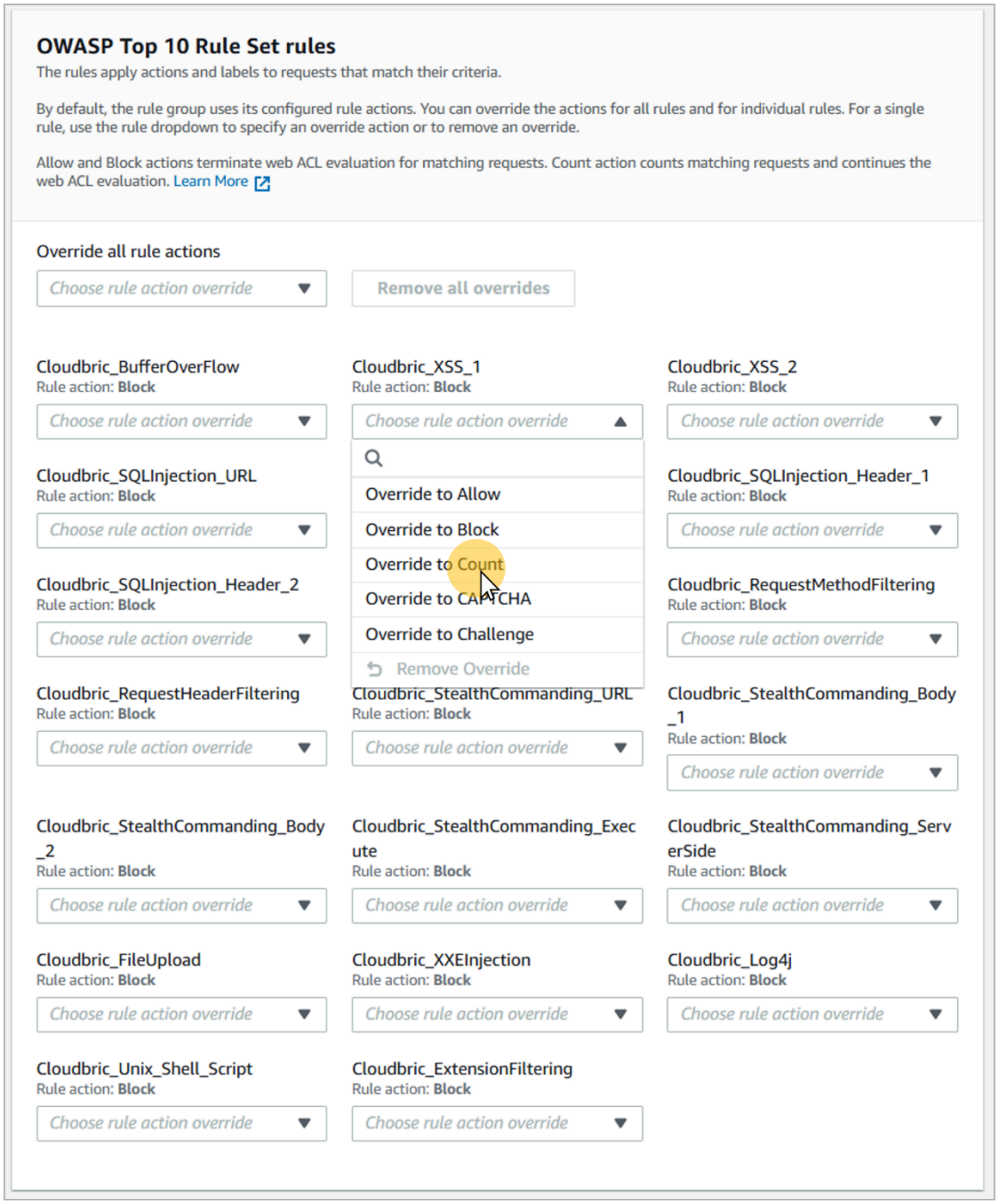
- **Step 3**

  Go to the **[Rules]** tab, then select the checkboxes for all the Cloudbric managed rule group to override and select **[Edit]**.



- **Step 4**

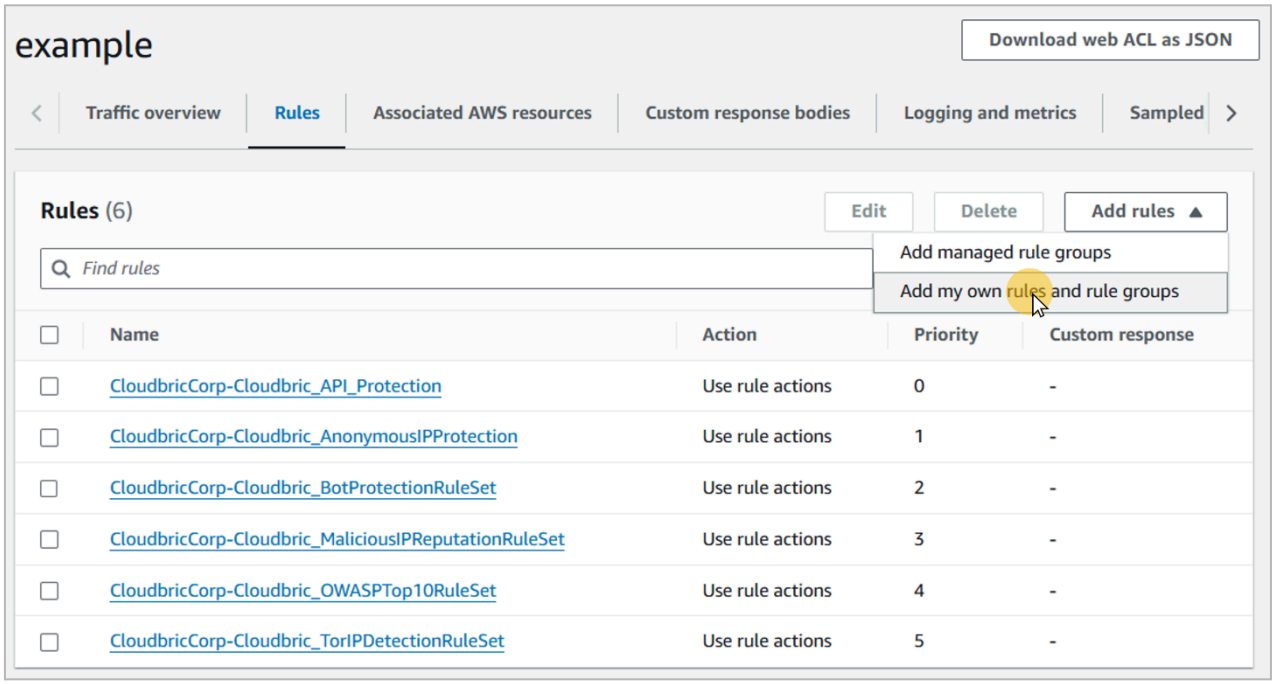
  Change the rule action of the rule to override to '**Count**' and click **[Save rule]** to complete the process.



4.2 Adding Override Rules Based on Labels

- **Step 1**

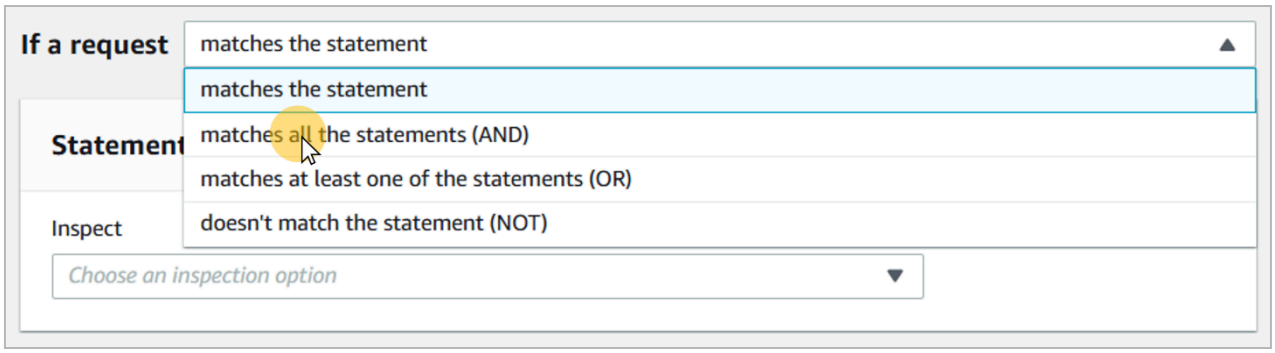
  Go to the **[Rules]** tab from the web ACL, click **[Add rules]** and select **[Add my own rules and rule groups]** from the drop-down menu to create a new rule.



- **Step 2**

  Select the overlapping '**AND**' option for the request to match the rule if it fulfills 2 statements.

  -If a request: matches all the statements (AND)

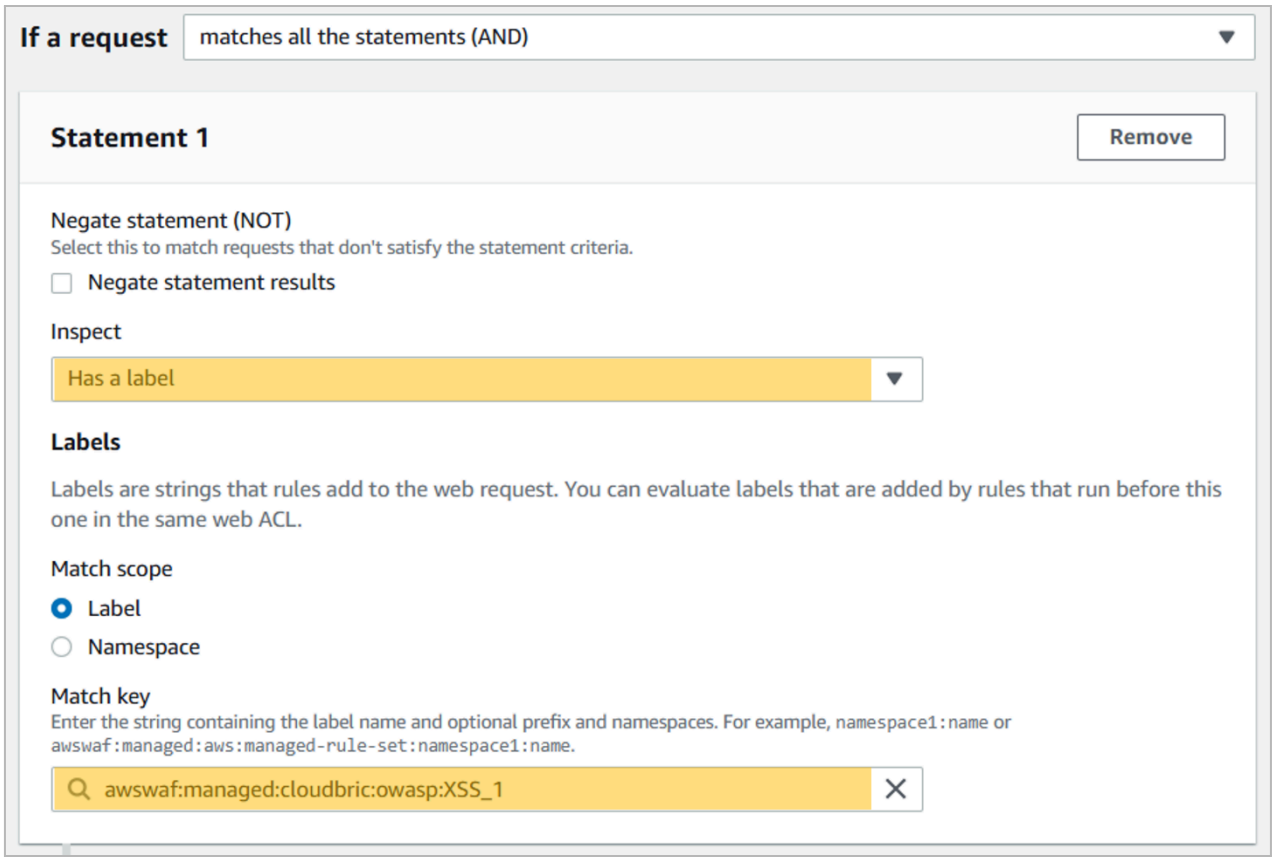


- **Step 3**

  Statement 1 is defined to inspect the request that matches the rule configured to override in section 4.1.

  -Inspect: Has a label

  -Match key: Enter ‘Label name’ for the rule you wish to override



*The structure of Label name for Cloudbric Managed Rules – OWASP Top 10 Rule Set:

awswaf:managed:cloudbric:owasp:**[Rule Name]**

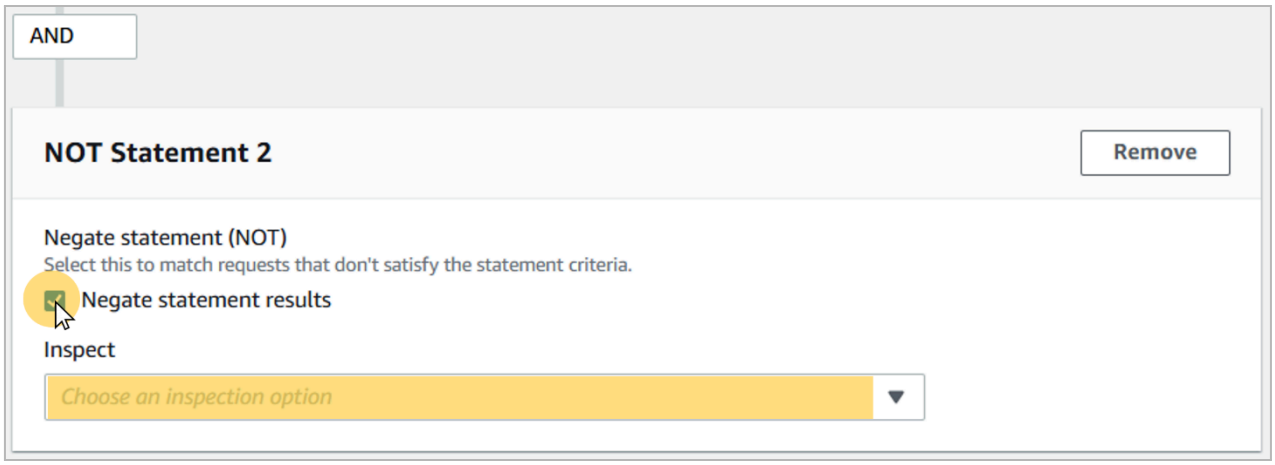
-e.g., If the rule name is ‘Cloudbric_XXS_1,’ the label is created as: ‘awswaf:managed:cloudbric:owasp:**XSS_1’**

- **Step 4**

  Statement 2 is defined to override the inspection option for the request with the false positive occurrence from the rule configured to override in section 4.1.

  -Negate statement results: Configured to check to override the detection option defined in the statement.

  -Inspect: Configures the inspection option with the false positive occurrences.

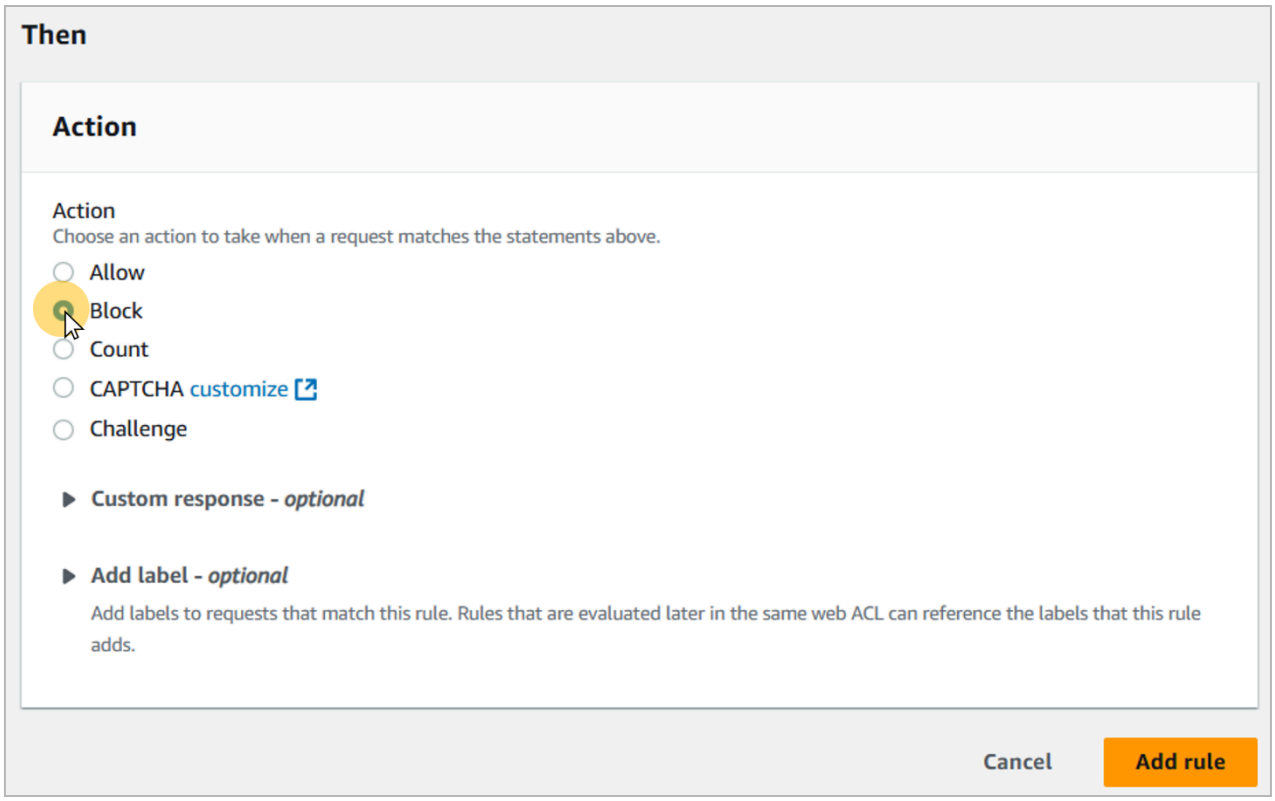


*The inspection option that matches with the request can be viewed from AWS WAF ‘ ruleMatchDetails’ log field, limited to the rules that detect SQL Injections and Cross Site Scripting (XSS) attacks.

*Please contact awsmkp@pentasecurity.com and provide the log information if any false positives occurred in rules.

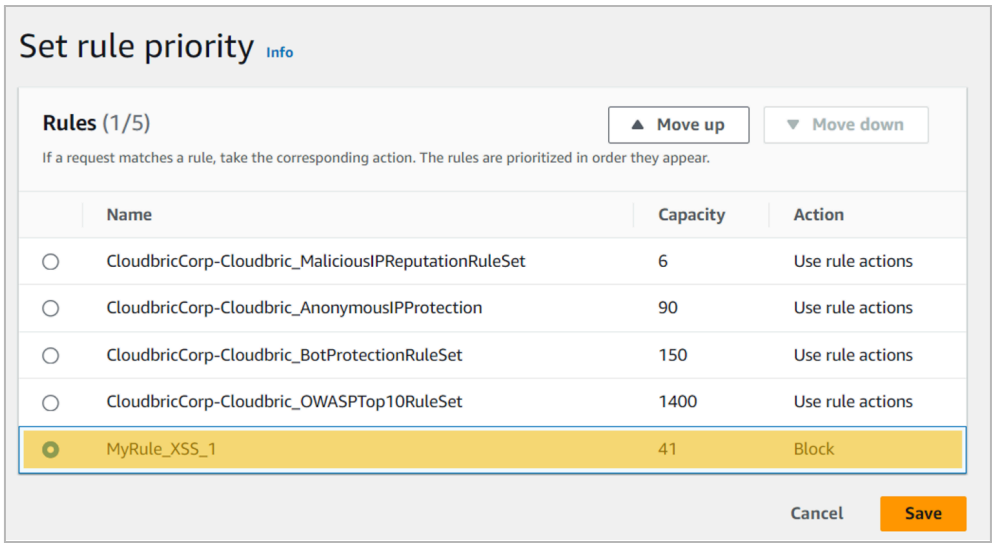
- **Step 5**

  Select the rule action as ‘Block’ to block the requests when it matches the rule and click **[Add rule]** to add the rule.



- **Step 6**

  Set the priority of the created rule to come after the override rule configured in section 4.1, and click **[Save]** to complete the configuration of the override rule.



5. APPENDIX

5.1 Frequently Asked Questions

Q. How much would I be billed for using Cloudbric Managed Rules?

The cost of using Cloudbric managed rule groups can be estimated by combining the following pricing dimensions:

1. **Region**: Number of Regions with web ACL deployed.
2. **Requests**: Number of Requests received by web ACLs per region by the units of 1 million requests.

Example of estimating the cost for Cloudbric OWASP Top 10 Protection is as follows:

- Current pricing for OWASP Top 10 Protection:

Units	Cost
Charge per month in each available region (pro-rated by the hour)	$25.00
Charge per million requests in each available region	$1.00

- Case A:

1 web ACL associated with Cloudbric managed rule group, OWASP Top 10 Protection, created for a single region (e.g., us-east-1), with a total number of web requests the web ACL received was 10 million for a month.

us-east-1 region

① Region cost: $25.00 * 1 = $25.00

② Requests cost: $1.00 (per million) * 10 units = $10.00

= Total cost: (①+②): $35.00

- Case B:

  1 web ACL associated with Cloudbric managed rule group, OWASP Top 10 Protection, created for 2 regions (e.g., us-east-1, us-west-1), with a total number of web requests each web ACL received was 10 million for a month.

  us-east-1 region

  ① Region cost: $25.00 * 1 = $25.00

  ② Requests cost: $1.00 (per million) * 10 units = $10.00

  us-west-1 region

  ③ Region cost: $25.00 * 1 = $25.00

  ④ Requests cost: $1.00 (per million) * 10 units = $10.00

  = Total Cost: (①+②+③+④)= $70.00

Q. Can I view the statement details of Cloudbric Managed Rules?

The statement details of the rules are an intellectual property of the Independent Software Vendors (ISVs). Due to AWS policy the statement details such as, not limited to, regex patterns, IP list, or inspection criteria cannot be disclosed to the subscribers.
If the statement details need to be changed due to reasons including false positives or negatives, it is recommended that the subscriber adopt Cloudbric WMS (WAF Managed Service), a security rule operation and management service for AWS WAF users.

- Cloudbric WMS (Professional Services model): Link
- Cloudbric WMS (PAYG model): Link

Q. How are the inspection criteria for the IP-based rules managed?

The IP-based rules of Cloudbric Managed Rules, such as Malicious IP Protection, Anonymous IP Protection, and Tor IP Protection, are all managed and operated by Penta Security's proprietary threat intelligence, Cloudbric Labs. The database of Cloudbric Labs, ThreatDB, regularly collects and analyzes the malicious IP data and scores the IP by its threat level. The data is then updated for the IP-based rules. Additionally, by adding inspection criteria for X-Forwarded-For (XFF) headers, the IP-based rules of Cloudbric Managed Rules can not only detect malicious IPs based on its source IPs, but also origin IPs.

Q. How can I be notified of any updates made to Cloudbric Managed Rules?

Since Nov 12th, 2021, any changes or updates made to Cloudbric Managed Rules are notified on Cloudbric's official homepage. However, if you would like to receive notifications of updates, it is recommended that you subscribe to the SNS topic of Cloudbric managed rule group. If you have any questions, please contact: awsmkp@pentasecurity.com.

*Due to the variability of the IP-list, changes and updates made to the IP-based rules are not notified through Cloudbric official homepage.

*The release notes for Cloudbric Managed Rules for AWS WAF can be found at the following address: https://www.cloudbric.com/cloudbric-managed-rules-for-aws-waf-release-notes/