Penta SECURITY

Cloudbric Managed Rules

Cloudbric Managed Rules for AWS WAF Setting Guide v1.4 2024.06

FOR ENDUSER(PUBLIC)

CHANGE HISTORY

Date	Author	Revision Description	Page no.	Comment
2022.12	Park. Junhyung	Initial documentation		v 1.0
2023.05	Park. Junhyung	Added details regarding the Rule override using Labels.	15, 17, 22, 26	v 1.1
2023.06	Park. Junhyung	Added description for Tor IP Detection Rule Set Added details for Rule Set versioning and update notifications settings	4, 10-14, 19, 20	v 1.2
2023.08	Park. Junhyung	Added description for Bot Protection Rule Set	4	v 1.3
2024.06	Park. Junhyung	Changed the name of the company to Penta Security Inc. Changed the customer support e-mail address Added description for Anonymous IP Protection Changed the product line name to Cloudbric Managed Rules Changed the name of all managed rule groups due to rebranding of Cloudbric Managed Rules Updated the document in accordance with the latest version of AWS console	3-30	v 1.4

CONTENTS

1. Overview

This document was made to explain how an AWS Web Application Firewall (WAF) user can subscribe and implement「Cloudbric Managed Rules」for AWS WAF, provided by Penta Security Inc., currently available in AWS Marketplace.

1.1 What are 'Cloudbric Managed Rules?':

Cloudbric Managed Rules for AWS WAF is a product line of managed rule groups developed by Penta Security, an official AWS WAF Ready Program Launch Partner of Amazon Web Services (AWS). Cloudbric Managed Rules were developed by security experts with over 20 years of experience, based on Penta Security's core technology. Penta Security is currently one of only seven Independent Software Vendors (ISV) to provide managed rule group products within AWS WAF. Cloudbric Managed Rules are continuously updated and managed by Penta Security to maintain a stable level of security and boost the AWS WAF experience for the users.

What are Managed Rule Groups in AWS Marketplace?
Managed rule groups are collections of predefined, ready-to-use rules that AWS and AWS Marketplace sellers 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 rules themselves.

1.2 Cloudbric Managed Rules Products:

Name	Details
OWASP Top 10 Protection *Go to Subscribe*	Provides security against threats from OWASP Top 10 Web Application Security Risks, such as SQL Injection and Cross Site Scripting (XSS) utilizing the logic-based detection engine recognized by world-renowned research organizations such as Gartner and Frost & Sullivan.
Malicious IP Protection *Go to Subscribe*	Provides security against malicious IP traffic based on the Malicious IP Reputation list created using ThreatDB, which is collected and analyzed from 700,000 websites in 148 countries worldwide by Cloudbric labs, Penta Security's own Cyber Threat Intelligence (CTI).
Bot Protection *Go to Subscribe*	Provides security against malicious bots, such as scrapers, scanners, and crawlers, which negatively impact and damage websites and web applications through repetitive behavior, based on the malicious bot patterns collected and analyzed by Penta Security.
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, and P2P Networks, responding to threats such as geo-location frauds, DDoS, and license and copyright infringement.
Tor IP Protection *Go to Subscribe*	Provides security against Anonymous IP traffic, specifically originating from the Tor network, which can be difficult to detect using an ordinary IP Risk Index, utilizing the Tor IP list managed and updated by Cloudbric Labs.

2. Setting Up Cloudbric Managed Rules

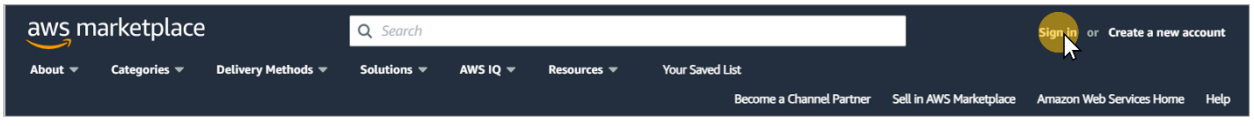
To set up Cloudbric Managed Rules for your AWS WAF, you must first subscribe to the Cloudbric Managed Rules for AWS WAF. After subscribing to the Cloudbric Managed Rules, the rule groups can be associated with the web ACL from the AWS WAF console, and you can configure the specifics of the rule groups, such as versions and update notifications, which you will receive through Amazon Simple Notification Service (Amazon SNS).

2.1 Subscribing to Cloudbric Managed Rules

- **Step 1**

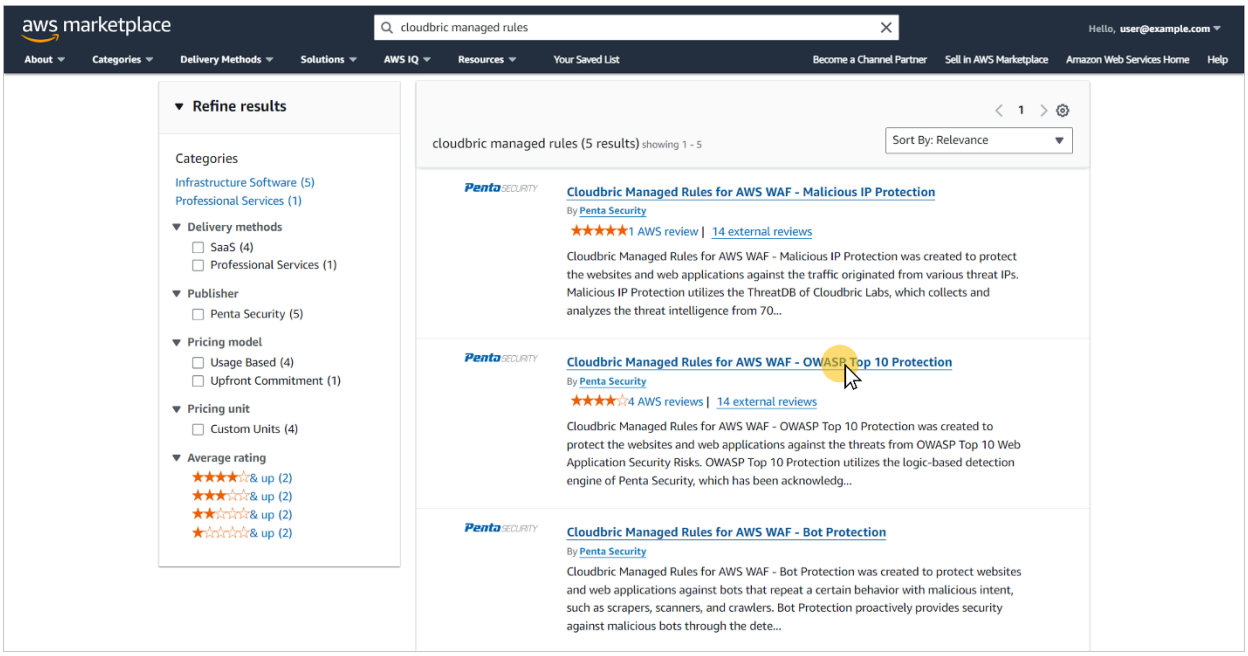
  Log in to AWS Marketplace with your AWS Account.

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



- **Step 2**

  Search for **'Cloudbric Managed Rules'** and select the name of the rule group you wish to subscribe.

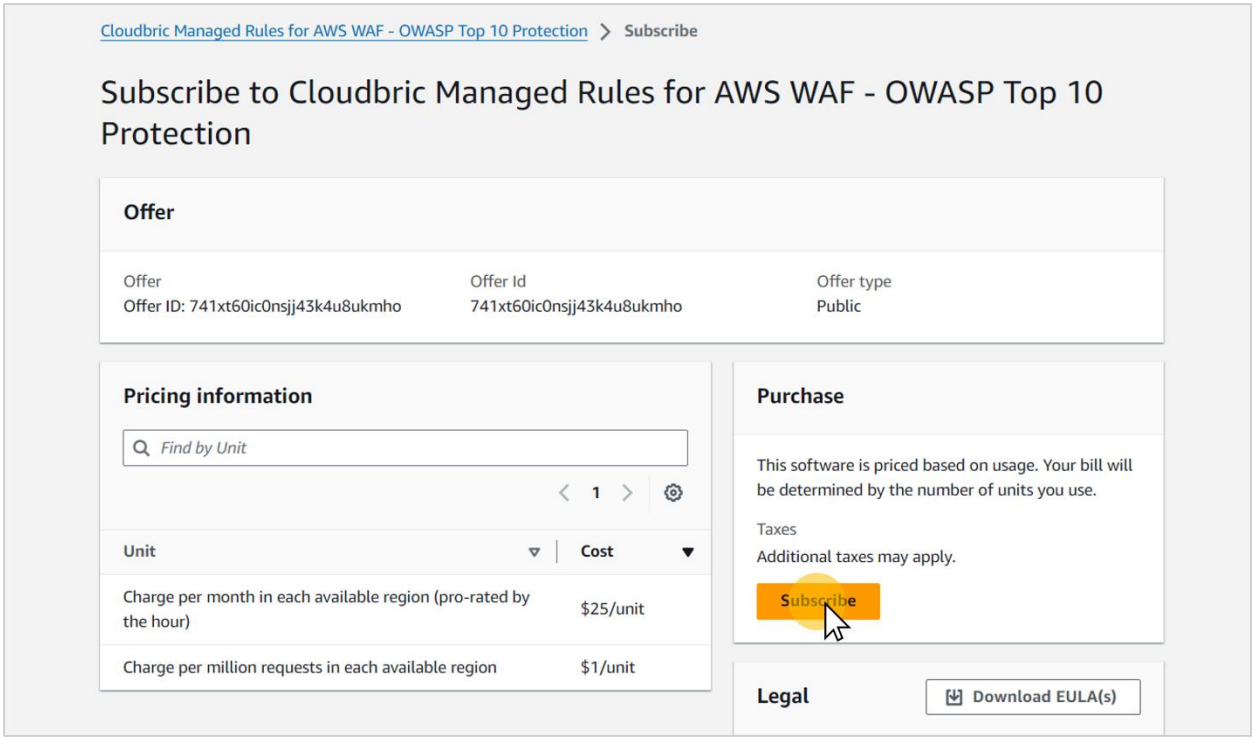


- **Step 3**

  Make sure to read the details of the selected rule group, then select **[View purchase options]**.

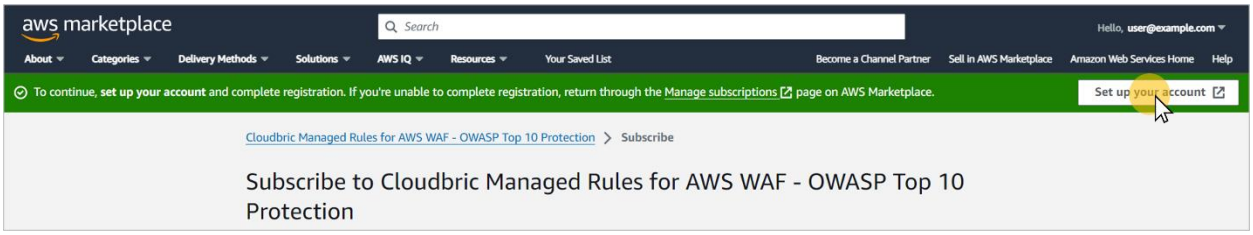
- **Step 4**

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



- **Step 5**

  You are now subscribed to the rule group. Select **[Set up your account]** to go to your AWS WAF console and implement Cloudbric Managed Rules.

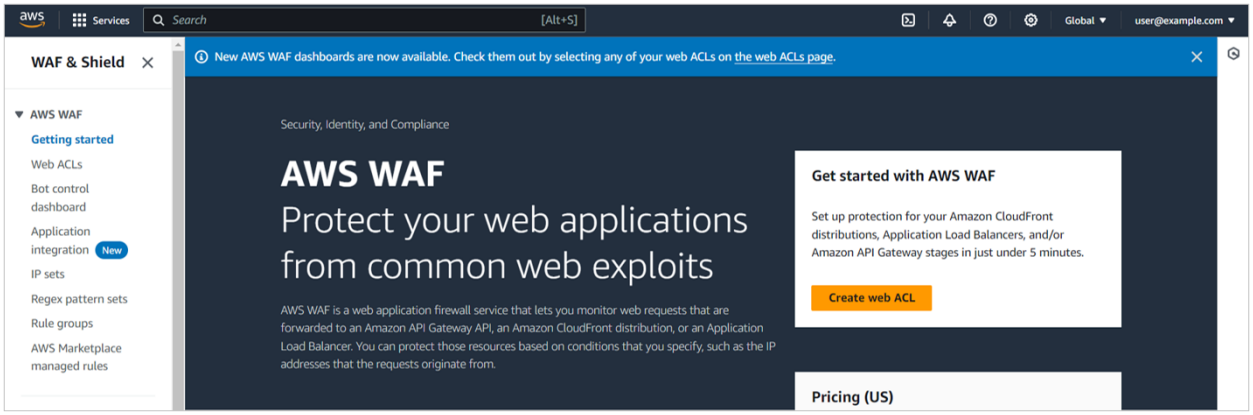


2.2 Implementing Cloudbric Managed Rules

- **Step 1**

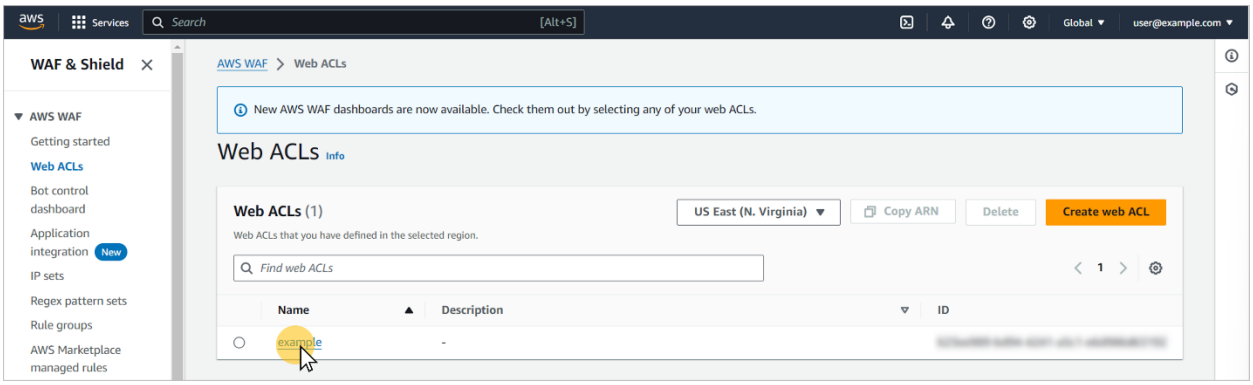
  Go to AWS WAF console.

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



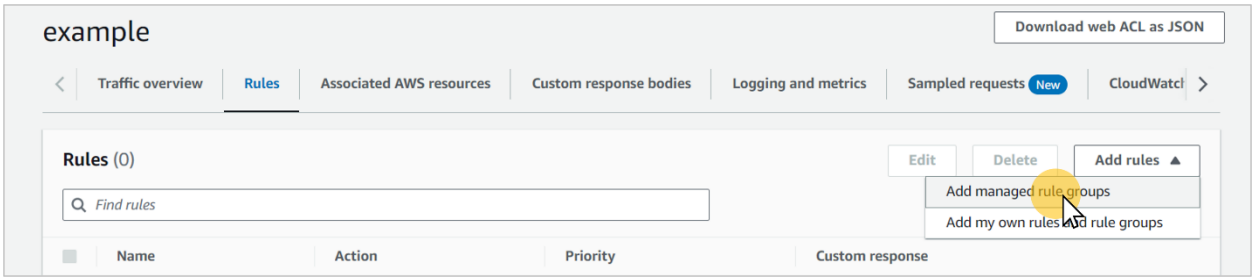
- **Step 2**

  Go to the Web ACLs menu and select the Web ACL you wish to associate with Cloudbric Managed Rules.



- **Step 3**

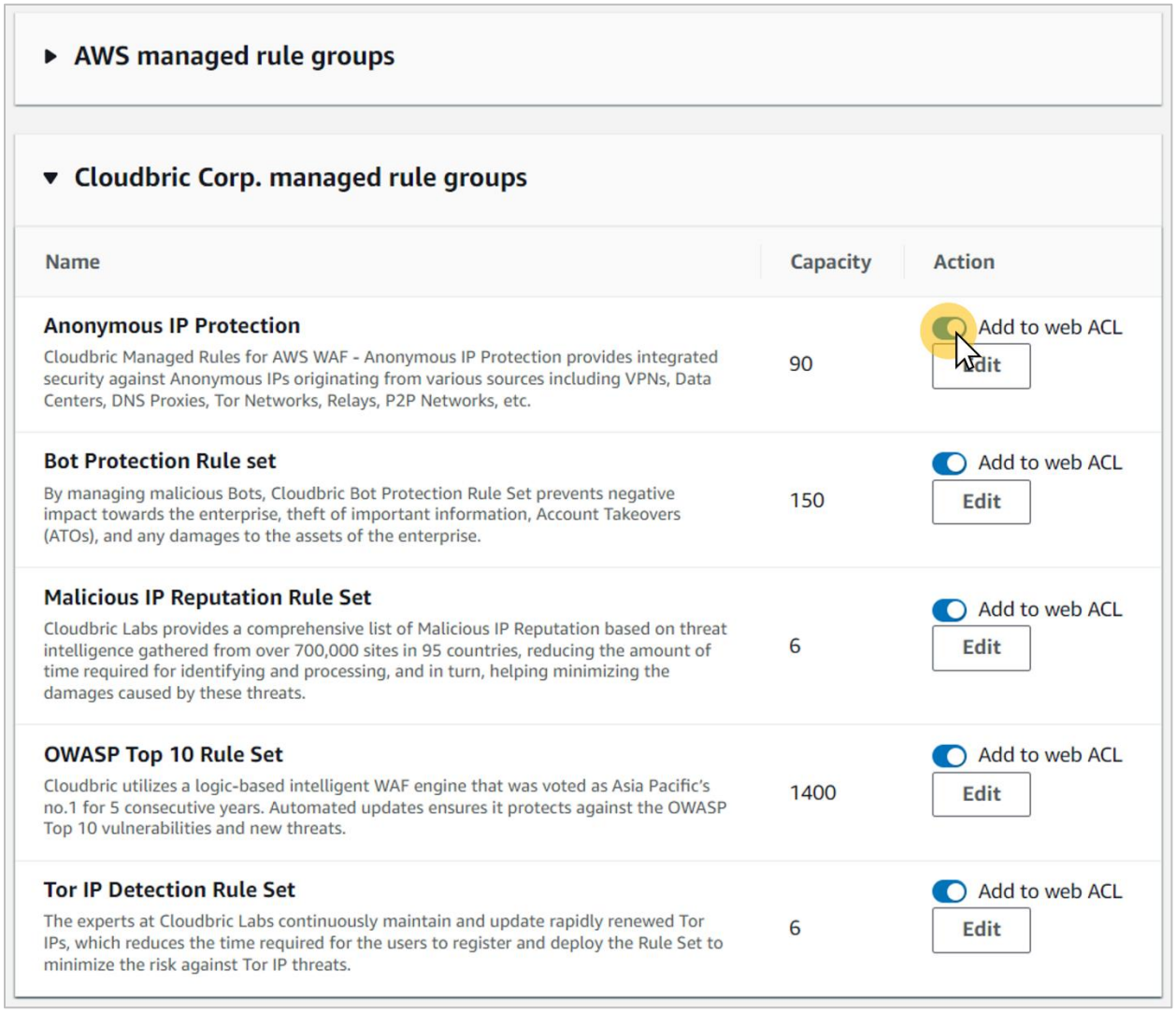
  Select the **[Rules]** tab and select **[Add managed rule group]** from the **[Add rules]** drop down menu.



- **Step 4**

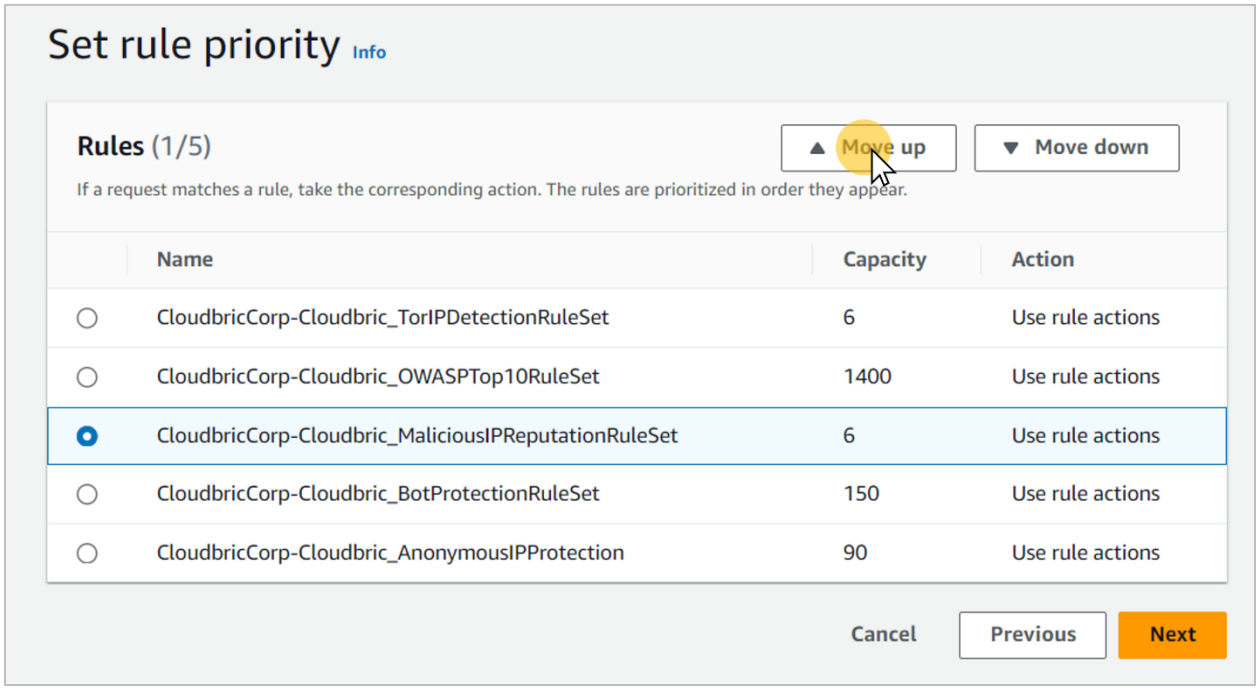
  Enable ‘Add to web ACL’ for the rule group you wish to associate with the web ACL, then select **[Add rules]**.

  ※To test the Rules Set first, select [Edit] and change the Action to ‘count’.



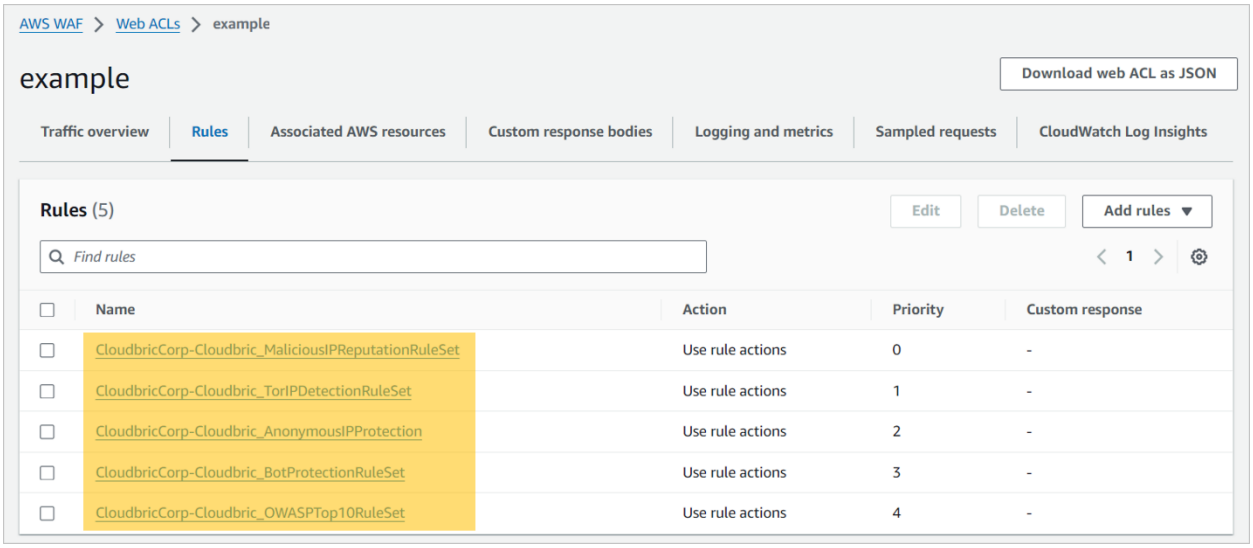
- **Step 5**

  If you wish to implement multiple Cloudbric managed rule groups for your web ACL, we recommend configuring the priority of each rule group for maximum performance. It is recommended that the IP-based rules, such as Malicious IP Protection and Anonymous IP Protection be configured with the highest priority, and the OWASP Top 10 Protection be configured with the lowest priority. The managed rule groups are implemented in order of highest priority to lowest. If you have any inquiries regarding how to configure the priority of Cloudbric managed rule groups, please contact awsmkp@pentasecurity.com.



- **Step 6**

  Review the **[Rules]** tab of the web ACLs menu to see if Cloudbric managed rule groups has been properly implemented.

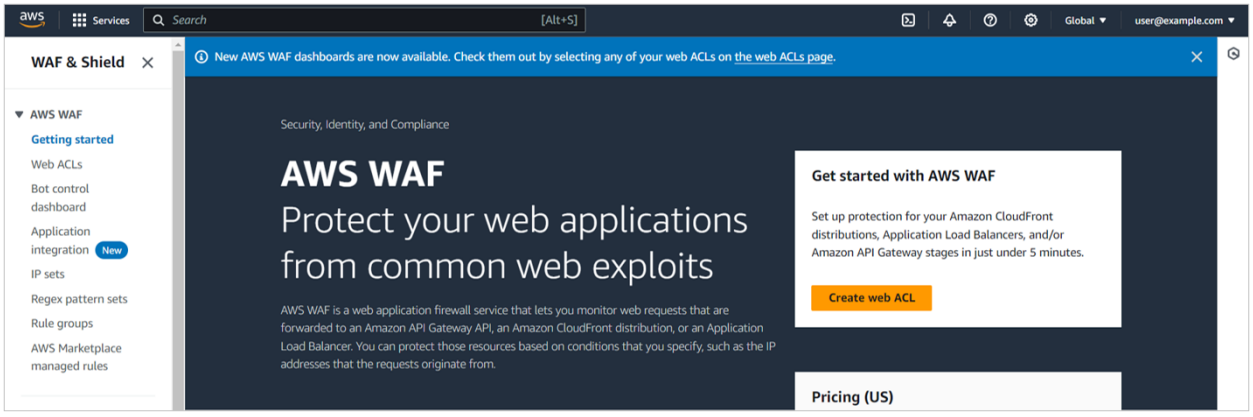


2.3 Selecting the Version of Cloudbric Managed Rules

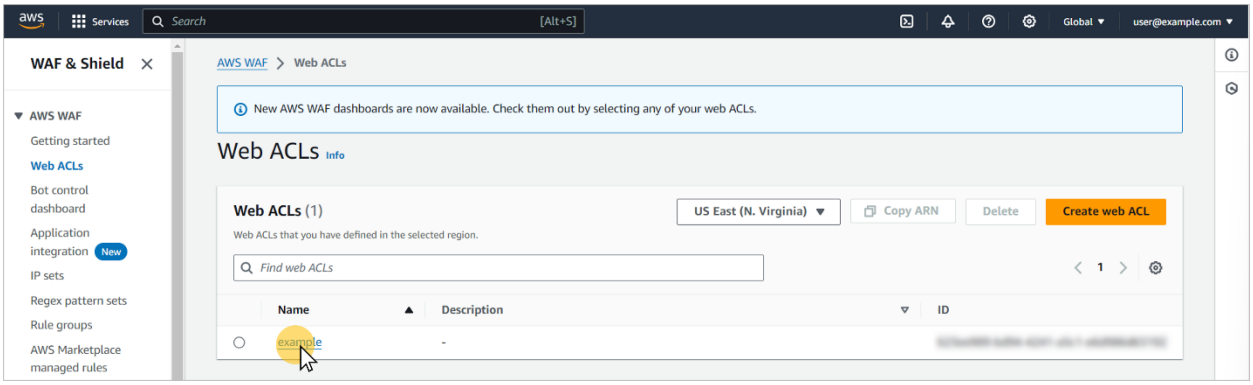
- **Step 1**

  Go to AWS WAF console.

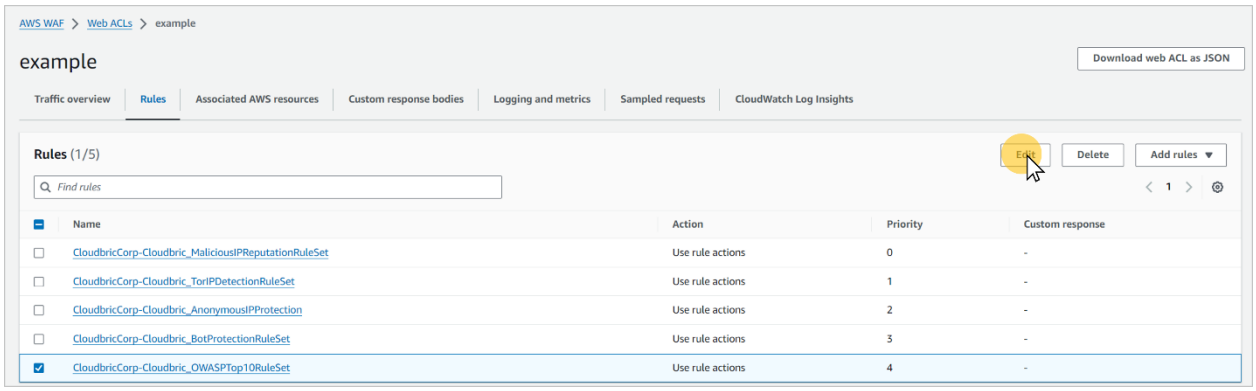
  ※*AWS WAF console :* https://console.aws.amazon.com/wafv2/



- **Step 2**
  Go to the web ACLs menu and select the web ACL that requires a different version of the Cloudbric managed rule group.

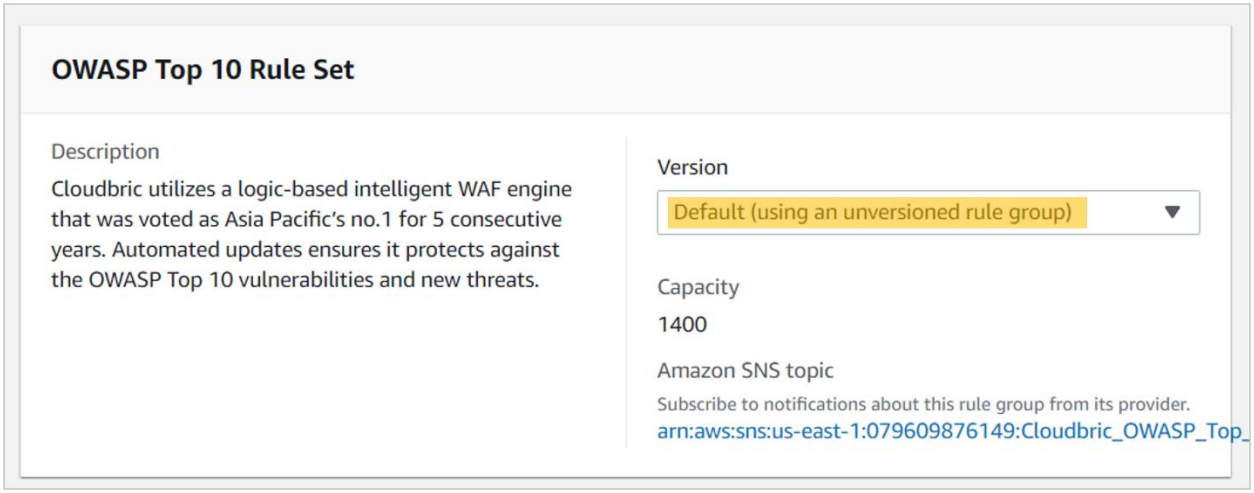


- **Step 3**
  Select the **[Rules]** tab of the Web ACL, select the managed rule group, and click **[Edit]**.



※*Versioning is currently only available for OWASP Top 10 Protection.*

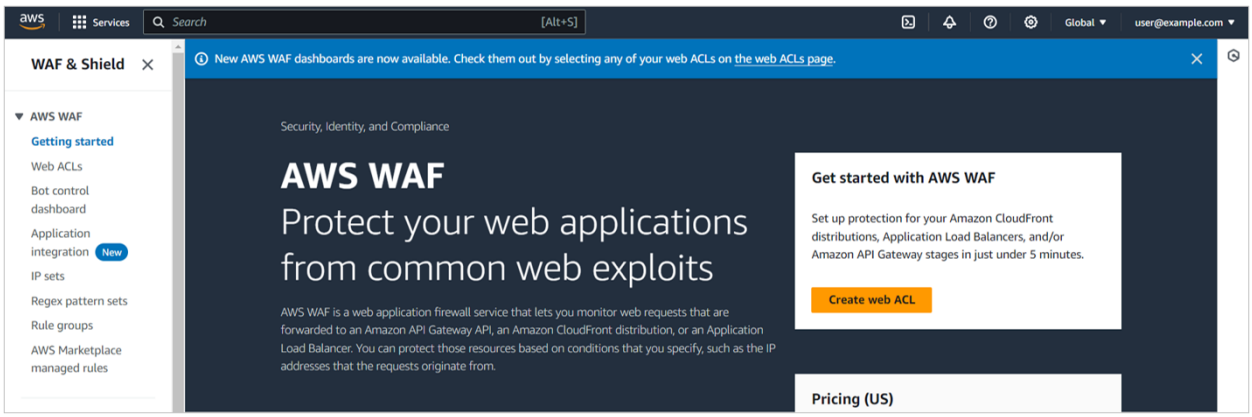
- **Step 4**
  Select the version of the managed rule group and click **[Save rule]** to associate with the web ACL.



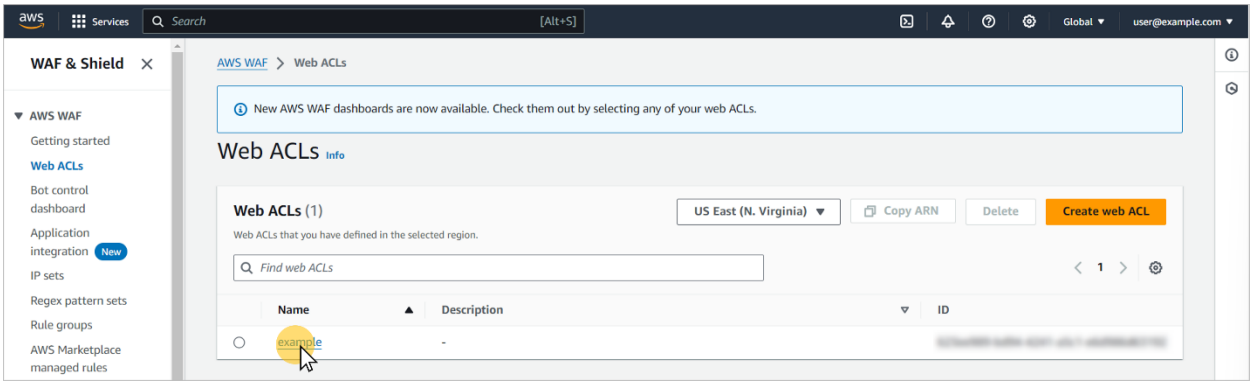
※As the managed rule group is updated, new versions of the managed rule group will be available to be associated with the web ACL.

2.4 Setting Up Notifications for Cloudbric Managed Rules

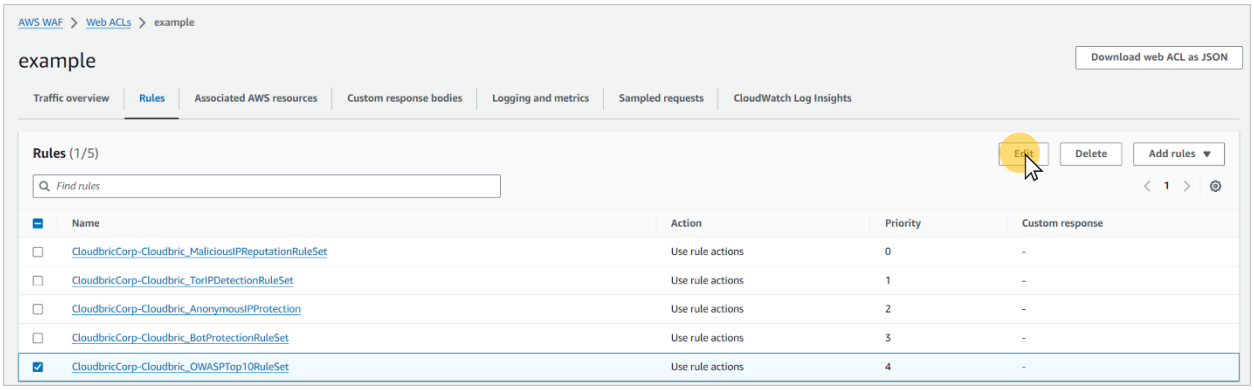
- **Step 1**
  Go to AWS WAF console.
  ※AWS WAF console : https://console.aws.amazon.com/wafv2/



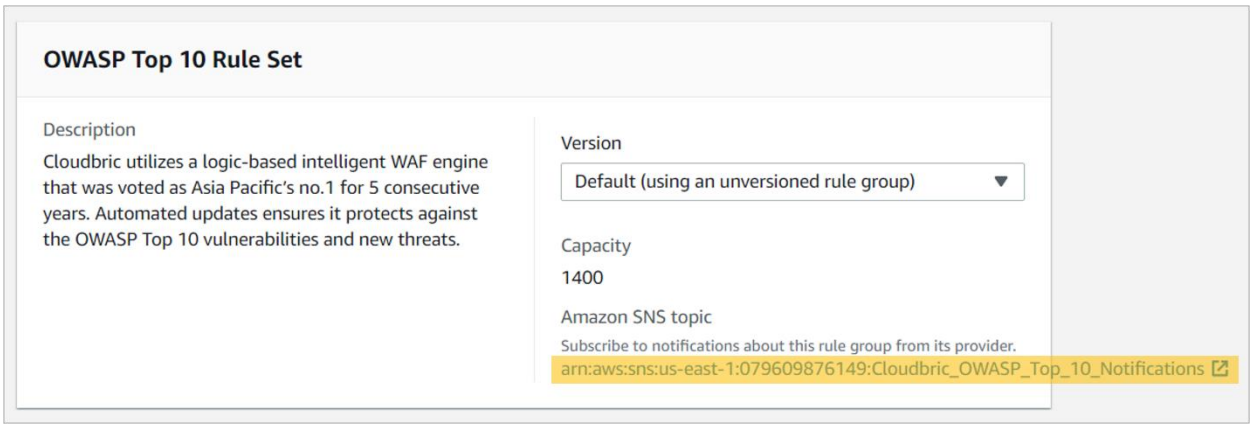
- **Step 2**
  Go to the web ACLs menu and select the web ACL that requires a different version of the Cloudbric managed rule group.



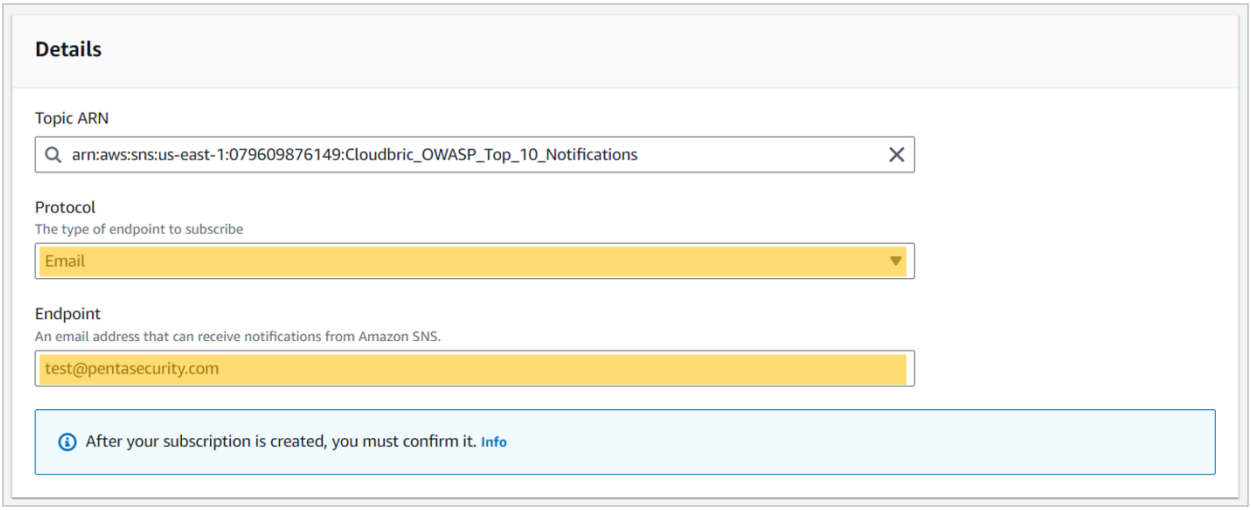
- **Step 3**
  Select the **[Rules]** tab of the Web ACL, select the managed rule group, and click **[Edit]**.



- **Step 4**
  Copy 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 the 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 be continued to be billed for the Cloudbric managed rule group if it has not been deleted from the Web ACLs, even after you canceled the subscription.*

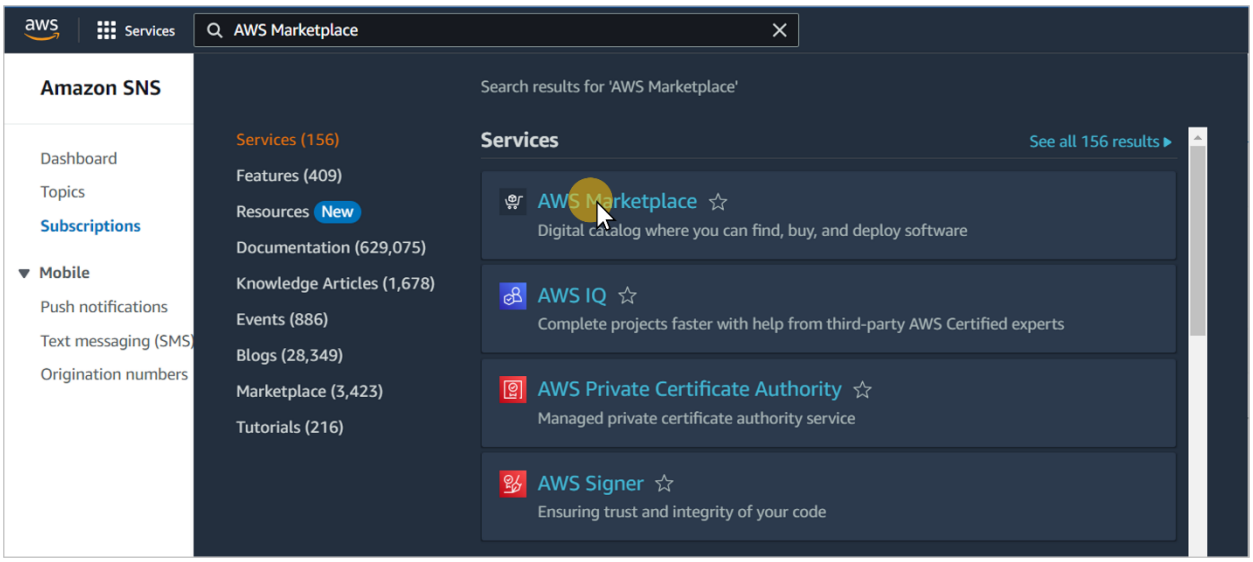
※*You may also be billed for the update notifications of Cloudbric managed rule groups if the subscription for Amazon SNS has not been canceled.*

3.1 Canceling Cloudbric Managed Rules Subscription

- **Step 1**

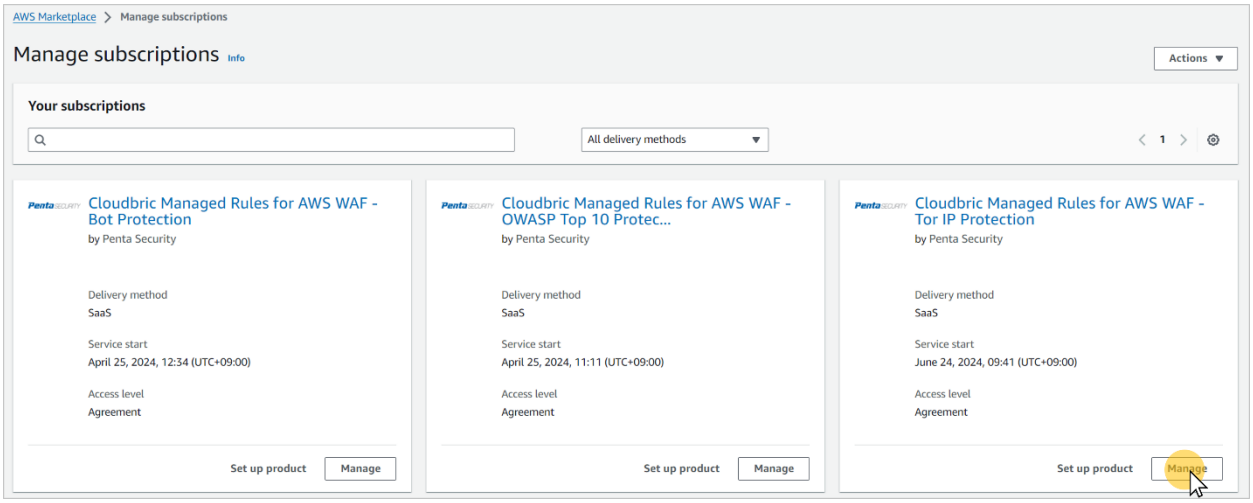
  Go to AWS Marketplace Subscriptions management console.

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



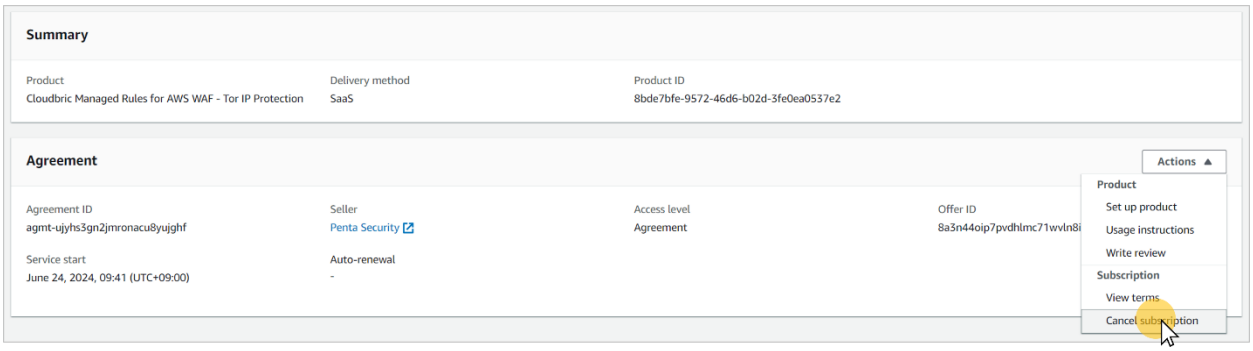
- **Step 2**

  Go to the **[Manage subscriptions]** menu and click **[Manage]** for the Cloudbric managed rule group you wish to cancel the subscription.



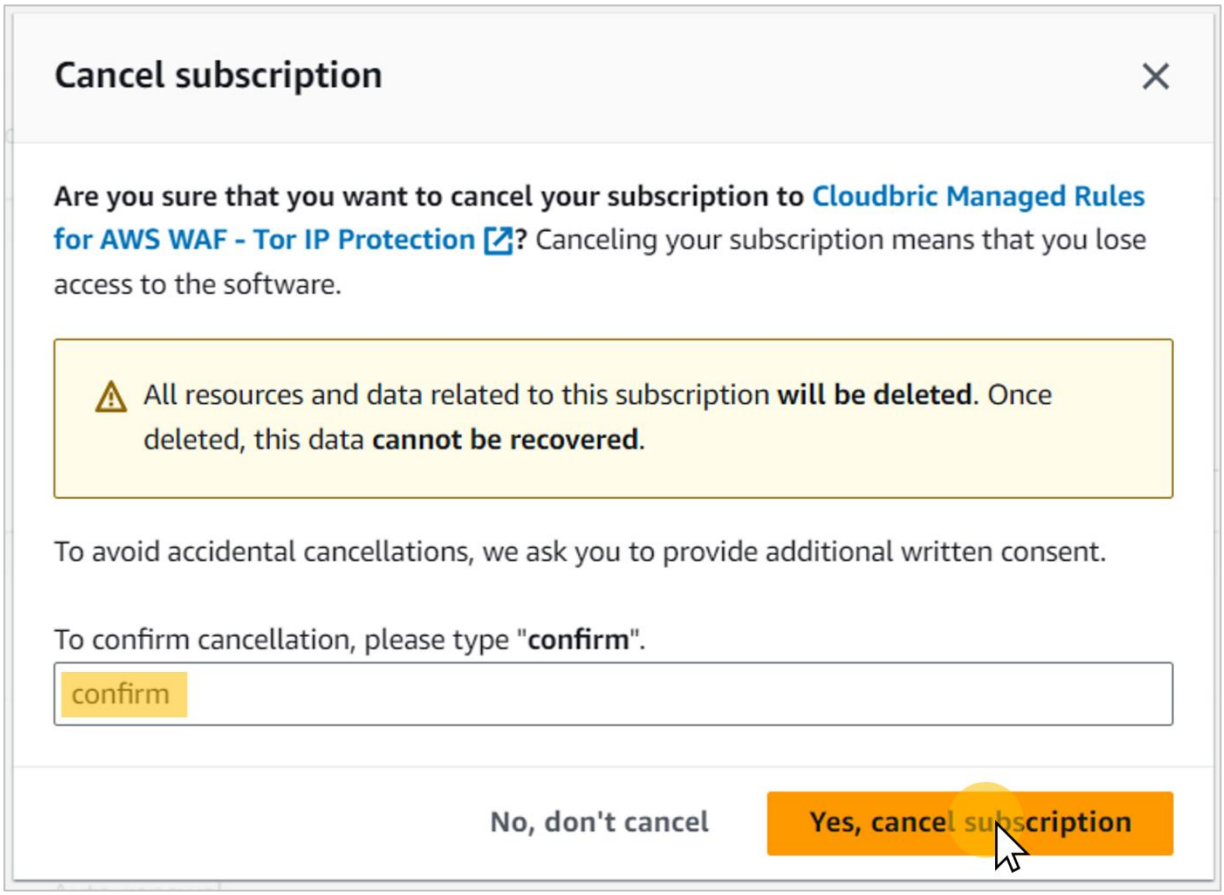
- **Step 3**

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



- **Step 4**

  Complete the cancellation of subscription by typing **"confirm"** in the input box and selecting **[Yes, cancel subscription].**

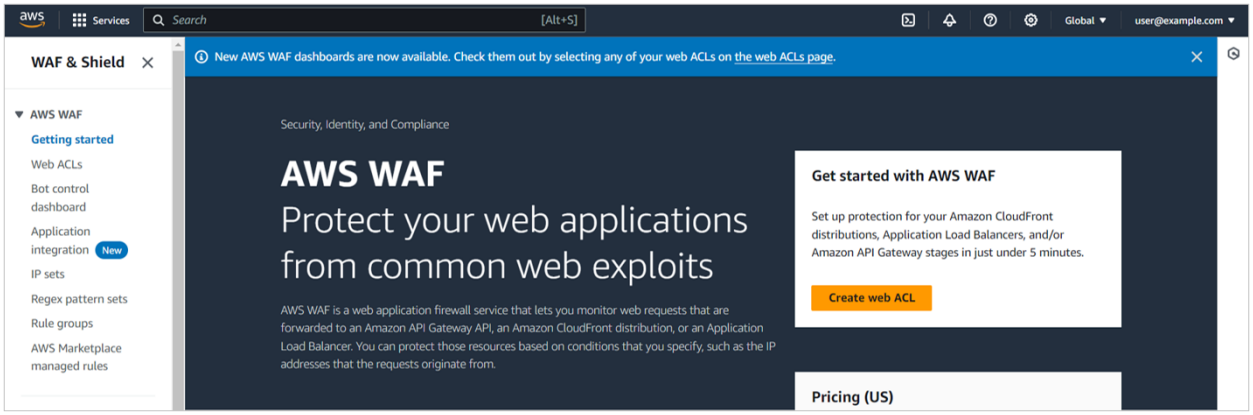


3.2 Deleting Cloudbric Managed Rules

- **Step 1**

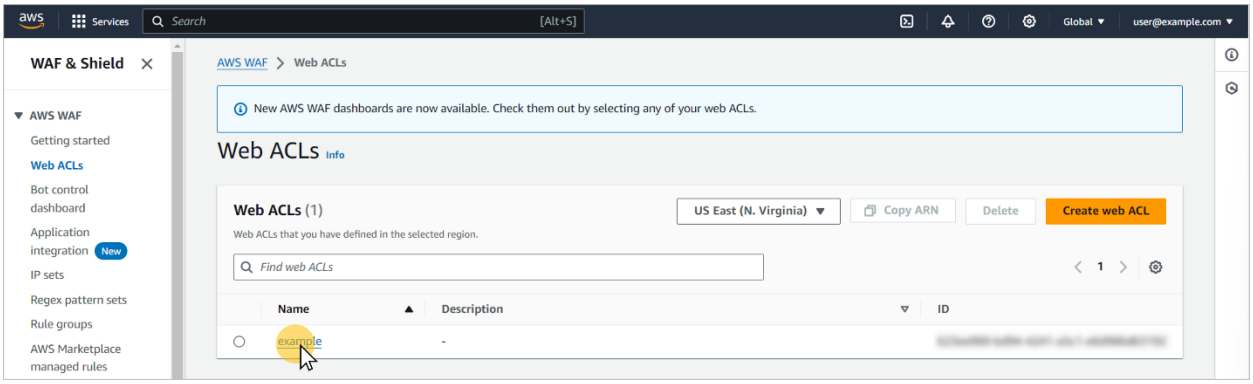
  Go to AWS WAF console.

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



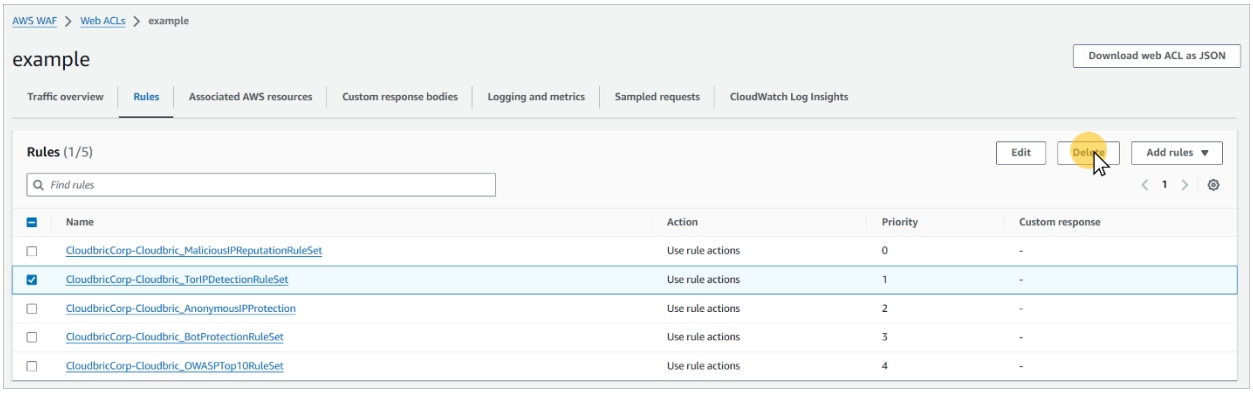
- **Step 2**

  Go to the Web ACLs menu and select the web ACL to delete the Cloudbric managed rule group.

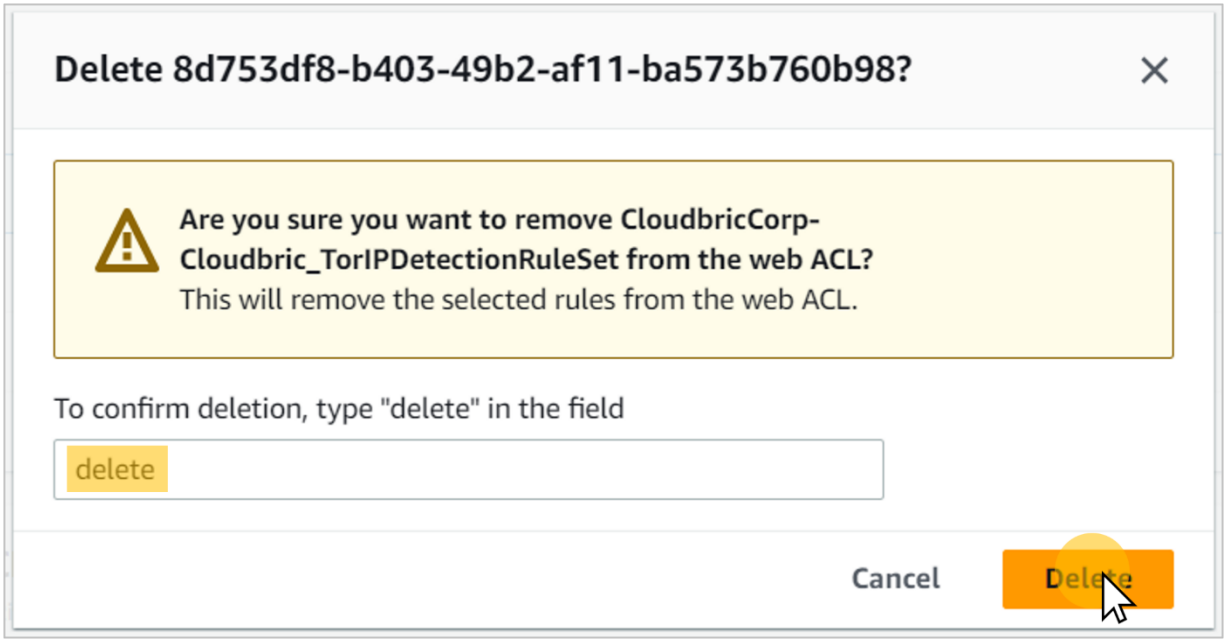


- **Step 3**

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



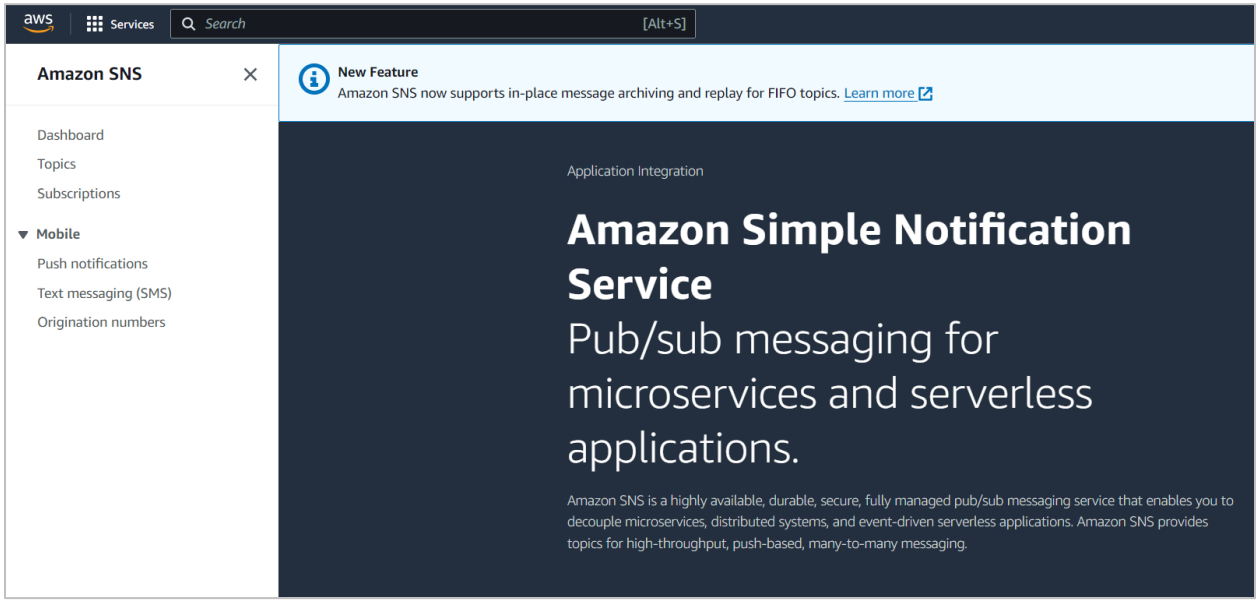
- **Step 4**
  Type in **'delete,'** and click **[Delete]** to complete the process.



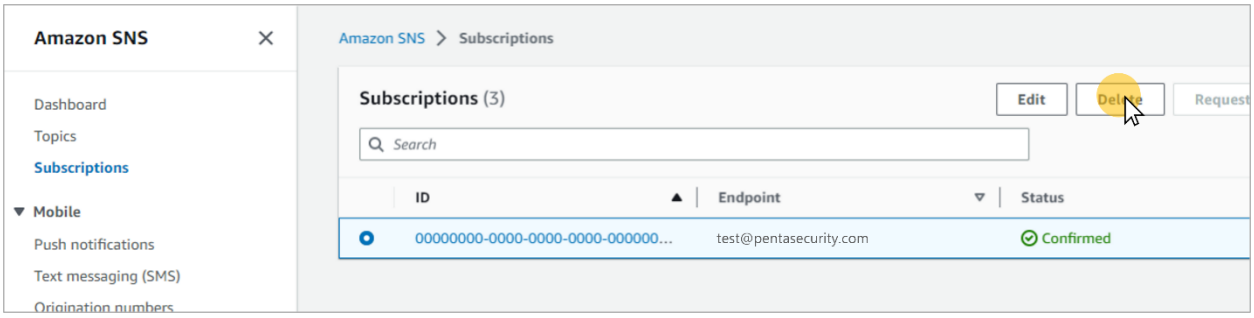
3.3 Canceling Notifications for Cloudbric Managed Rules

- **Step 1**
  Go to Amazon Simple Notification Service (SNS) console.

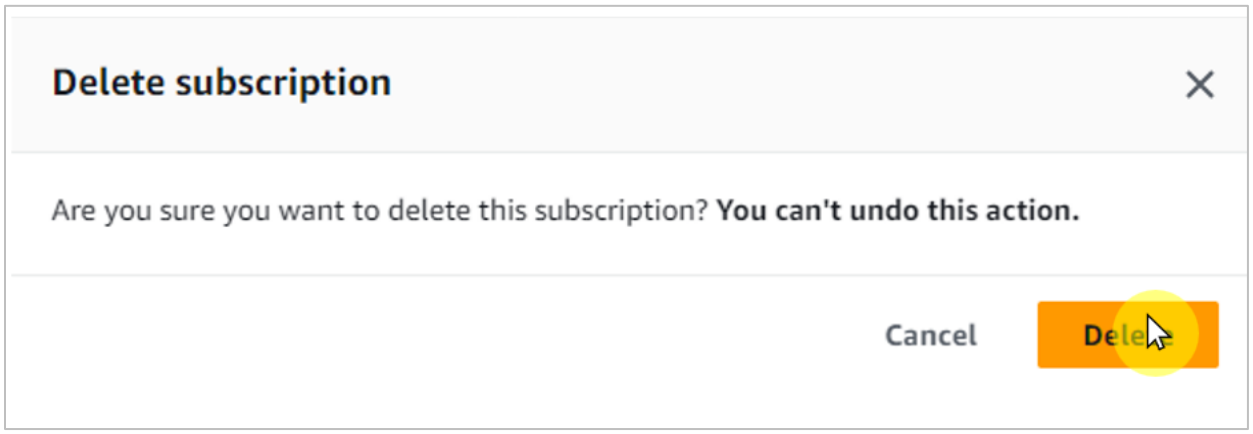
※ *Amazon SNS console:* https://console.aws.amazon.com/sns/home



- **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. This action cannot be undone.



4. Overriding Cloudbric Managed Rules

When a false-positive has occurred, in which a legitimate request has been blocked by Cloudbric managed rule group, the rule action must be changed to **'Count'** to override the rule. However, overriding the rule could also result in permitting malicious requests. To maintain the performance of the rules and apply the override only for a specific pattern that caused the false-positive, the override rule must be defined by adding a label-based, user-defined rule.

※All Rules in Cloudbric OWASP Top 10 Protection are configured with labels.

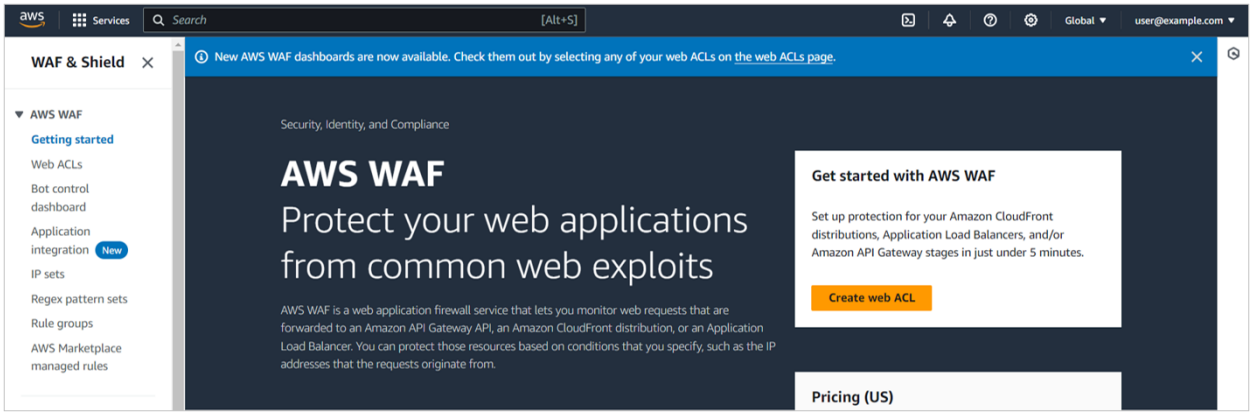
※The IP-based Cloudbric managed rule groups are not configured with any labels due to the dynamic tendency of the IP List.
If you need to override a specific IP, you must create an additional rule, allowing the IP.

4.1 Configuring Rule Action to 'Count'

- **Step 1**

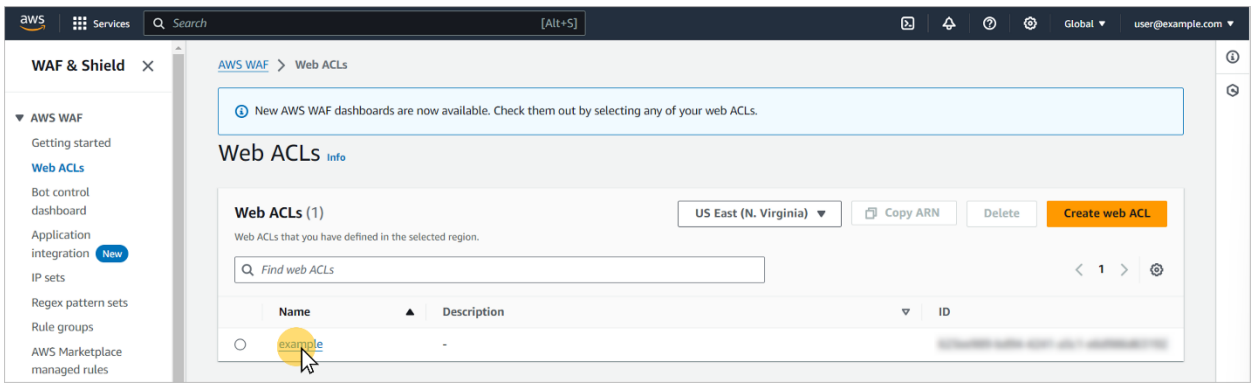
  Go to AWS WAF console.

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



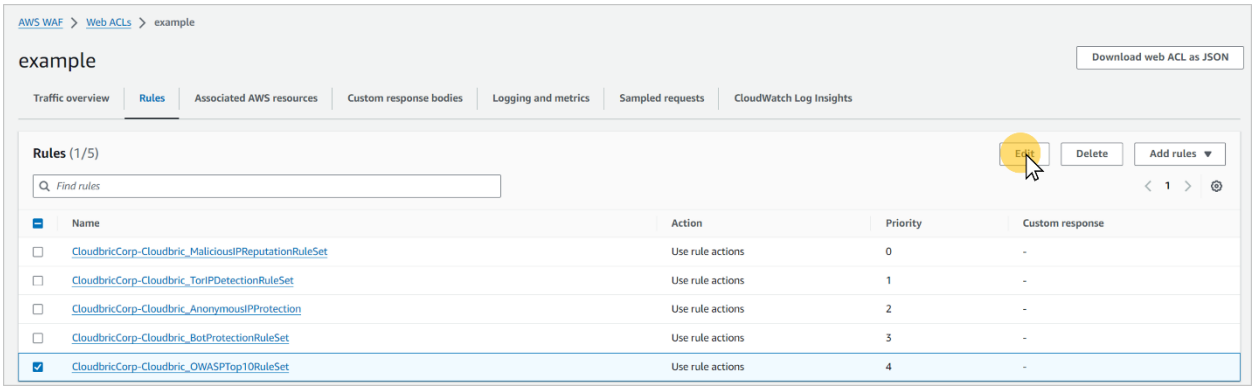
- **Step 2**

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



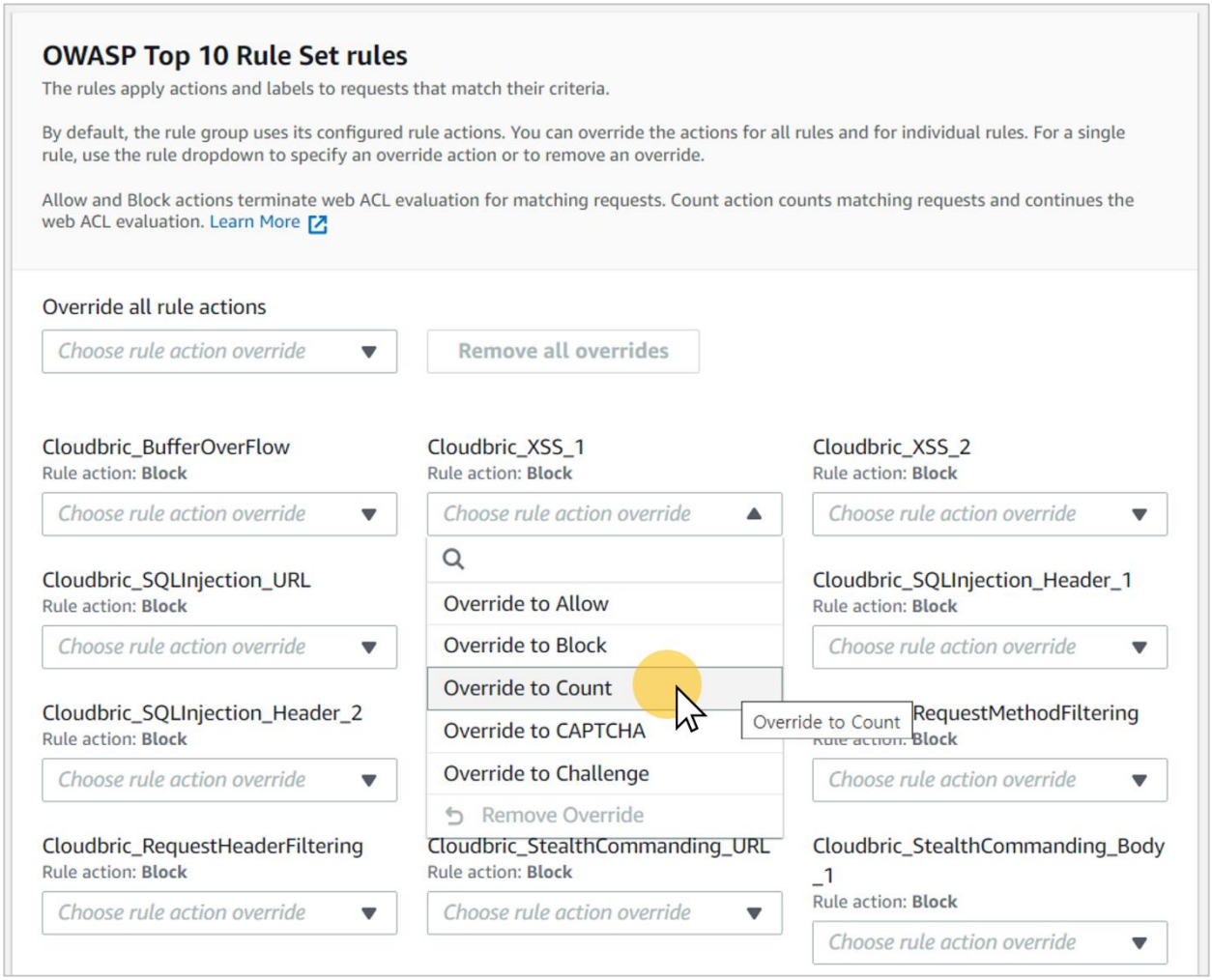
- **Step 3**

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



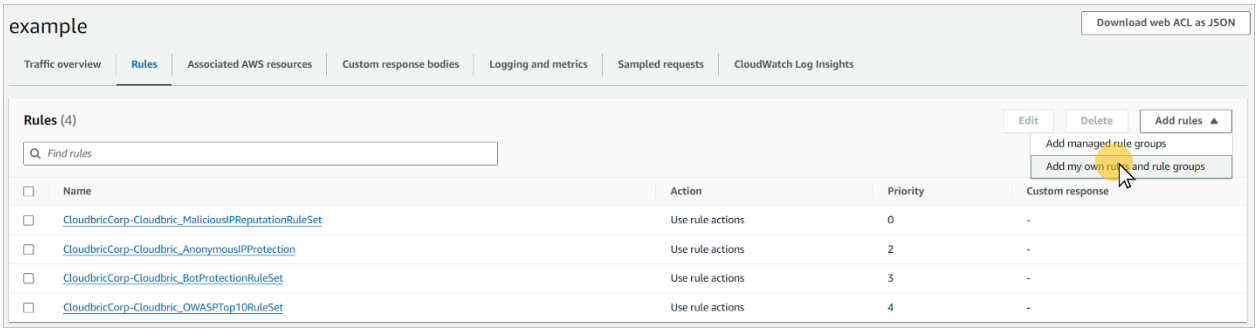
- **Step 4**

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

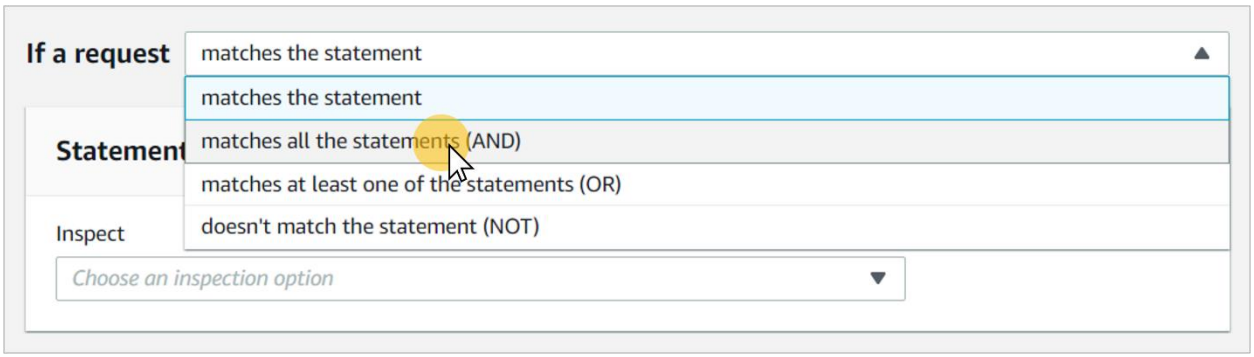


4.2 Adding Override Rules Based on Labels

- **Step 1**
  Go to **[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.



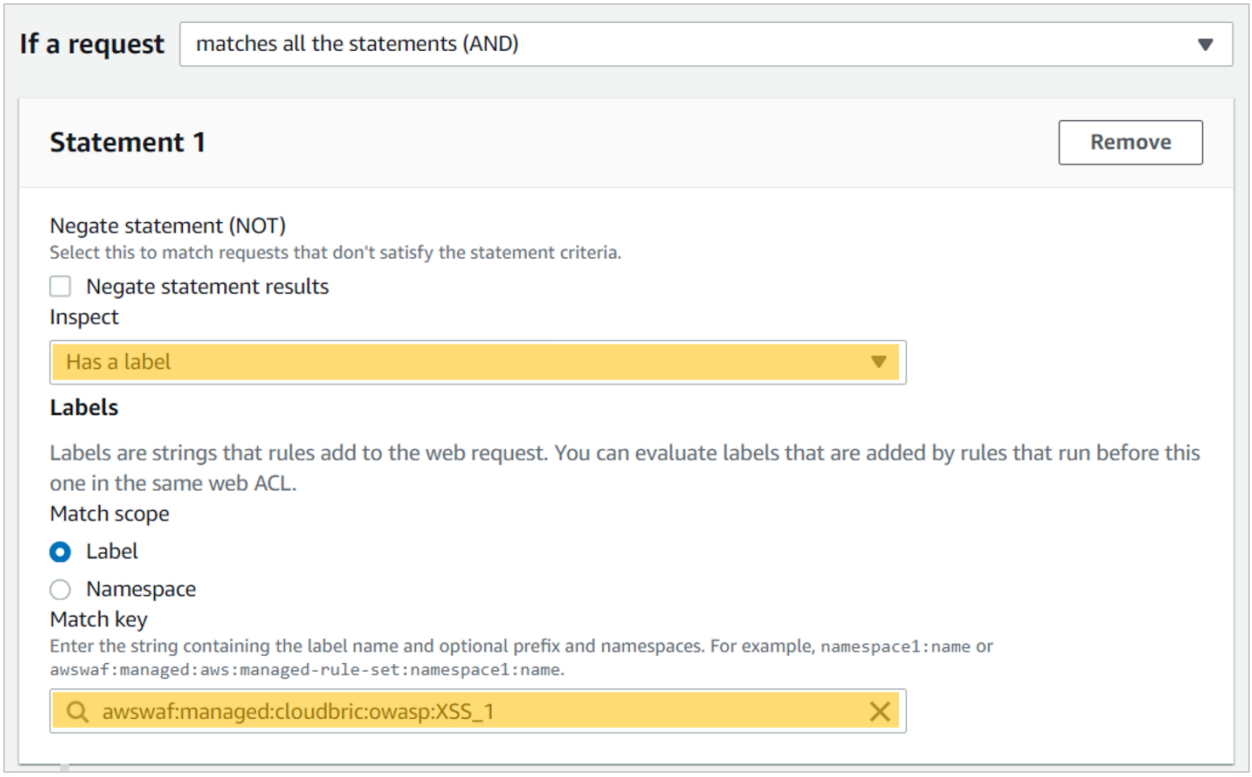
- **Step 2**
  Select the overlapping ‘AND’ option for the request to match the rule if it fulfills 2 statements.
  - If a request: matches all the statements (AND)



- **Step 3**

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

  - Inspect: Has a label
  - Match key: Enter 'Label Name' for the rule configured to override

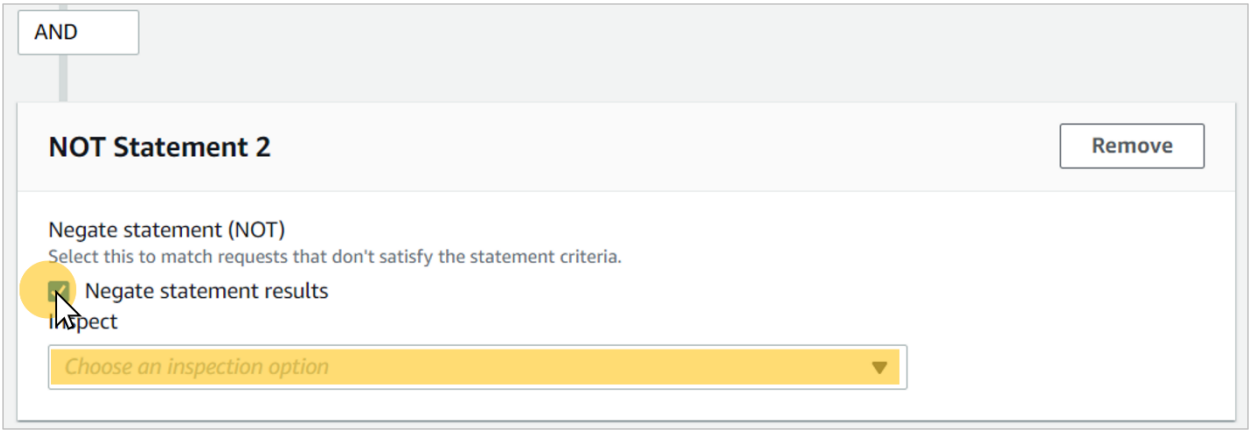


※*The structure of Label Name for Cloudbric OWASP Top 10 Protection:*

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

*- Example: If the Rule Name is 'Cloudbric_XXS_1,' the label is created as: 'awswaf:managed:cloudbric:owasp:**XSS_1**'*

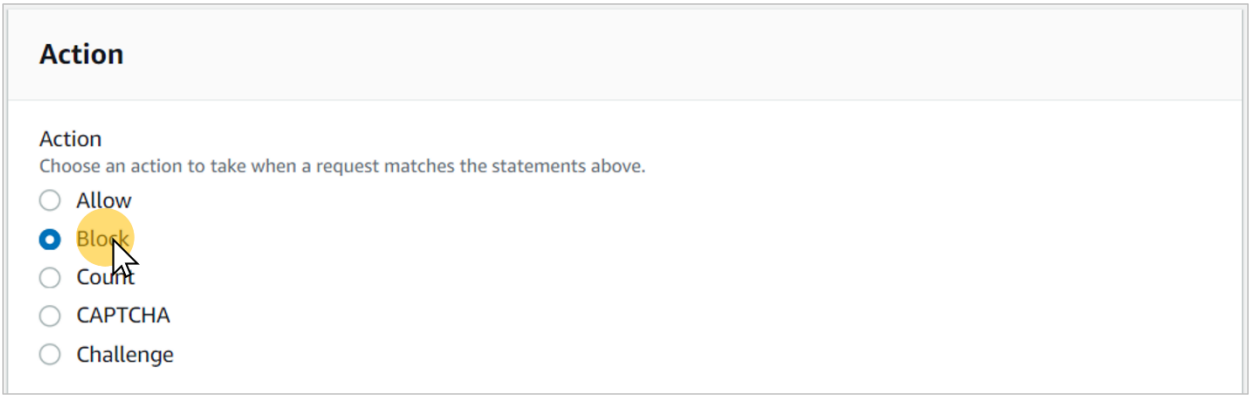
- **Step 4**
  Statement 2 is defined to override the inspection option for the request with the false-positive occurrence from the Rule configured to override in 「4.1」.
  - Negate statement results: Configured to check to override the detection option defined in the statement.
  - Inspect: Configures the inspection option with the false-positive occurrences.



※The inspection option that matched 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.

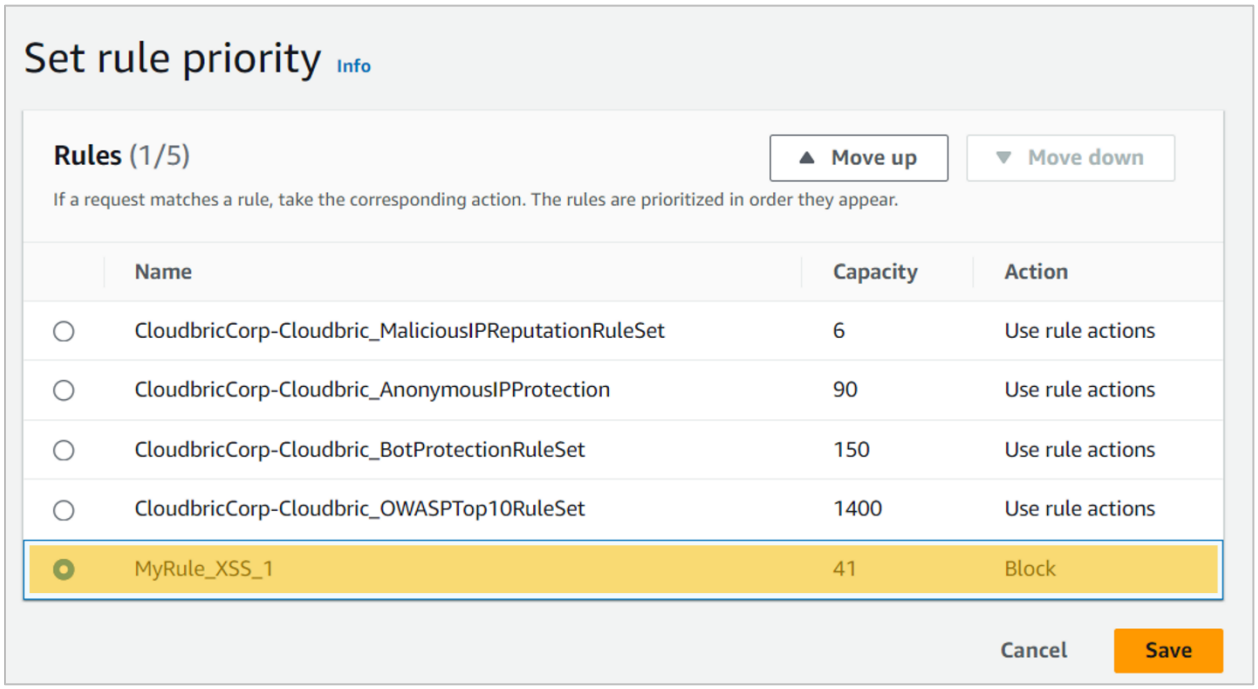
※Please contact awsmkp@pentasecurity.com and provide the log information if any false-positives occurred in the other rules.

- **Step 5**
  Select the Action of the Rule as 'Block' to block the requests when it matches the rule and click **[Add rule]** to add Rule.



- **Step 6**

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



5. Appendix

5.1. FAQ

Q. How do I find the Rule ID that blocked the request?

You can find the Rule ID from **[Sampled requests] > [Rule inside rule group]** from the web ACL, or if the web ACL is configured, it can be found from the **[RuleID]** Log field.

※You can view up to 100 logs of requests from the last 3 hours for Sampled requests.
For details, refer to Viewing a sample of web requests from the AWS Developer Guide.
https://docs.aws.amazon.com/waf/latest/developerguide/web-acl-testing-view-sample.html

The following are Log examples to see the Rule ID.

- **terminatingRuleId**: Rule ID that terminated the request.
  Value is set to Default_Action if there is no rule to terminate the request.
  ex)

```
{
    "timestamp": 1576280412771,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-southeast-2:111122223333:regional/webacl/STMTest/1EXAMPLE-2ARN-3ARN-4ARN-123456EXAMPLE",
    "terminatingRuleId": "STMTest_SQLi_XSS",
    "terminatingRuleType": "REGULAR",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [
        {
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "HIGH",
            "location": "HEADER",
            "matchedData": [
```

- **RuleId**: Rule ID of the nonterminatingMatchingRules that matches the request but has not been terminated.
  ex)

```
{
    "timestamp":1592357192516
    ,"formatVersion":1
    ,"webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-world/5933d6d9-9dde-js82-v8aw-9ck28nv9"
    ,"terminatingRuleId":"Default_Action"
    ,"terminatingRuleType":"REGULAR"
    ,"action":"ALLOW"
    ,"terminatingRuleMatchDetails":[]
    ,"httpSourceName":"-"
    ,"httpSourceId":"-"
    ,"ruleGroupList":[]
    ,"rateBasedRuleList":[]
    ,"nonTerminatingMatchingRules":
    [{
        "ruleId":"TestRule"
        ,"action":"COUNT"
        ,"ruleMatchDetails":
```

※Refer to the example of Log Examples from AWS Developer Guide for more information.

Log examples: https://docs.aws.amazon.com/waf/latest/developerguide/logging-examples.html

Q. Is there a way to check if the Cloudbric managed rule group was properly added?

When the request matches the Rule that was set as Block, AWS WAF returns a 403 Forbidden error as default. You can check if the Cloudbric managed rule group was properly added by entering a simplified XSS attack example on the browser.

- http://your-domain/<script>alert('XSS')</script>

Q. Can I view the inspection criteria of Cloudbric managed rule group?

As a default, the details of the inspection location or pattern of AWS WAF Managed Rules are not disclosed, as they are intellectual properties of the AWS Marketplace vendor, and disclosing the detection criteria may be exploited.

However, the inspection option that matched the request can be reviewed from AWS WAF 'ruleMatchDetails' Log field, limited to the Rules that detect SQL injections and Cross Site Scripting (XSS) attacks.

Log example of inspection option of the Rule matched with SQL injection attacks:

```
"terminatingRuleId": "STMTest_SQLi_XSS",
"terminatingRuleType": "REGULAR",
"action": "BLOCK",
"terminatingRuleMatchDetails": [
    {
        "conditionType": "SQL_INJECTION",
        "sensitivityLevel": "HIGH",
        "location": "HEADER",
        "matchedData": [
            "10",
            "AND",
            "1"
        ]
    }
```

```
,"nonTerminatingMatchingRules":
[{
    "ruleId":"TestRule"
    ,"action":"COUNT"
    ,"ruleMatchDetails":
    [{
        "conditionType":"SQL_INJECTION"
        ,"sensitivityLevel": "HIGH"
        ,"location":"HEADER"
        ,"matchedData":[
            "10"
            ,"and"
            ,"1"]
        }]
```

(Left)When the Rule terminated the request / (Right)When the Rule did not terminate the request

Q. Can the inspection option be changed when a false-positive or over detection occurs?

AWS does not provide any features to change inspection options for managed rules.

However, as AWS WAF Managed Rules are written based on the threats generally observed from majority of clientele, false-positives and over detections may occur according to the environment. Therefore, it is recommended that Cloudbric managed rule groups be implemented after the override rule has been configured as stated in 「4. Overriding Cloudbric Managed Rules」, in accordance with the operating environment, after 2~4 weeks of monitoring before actual implementation of the rule groups.

If you have any difficulties in optimizing the Rule configuration according to the user environment, we recommend using Cloudbric WMS (WAF Managed Service), a security Rule operation and management service for AWS WAF.

- Cloudbric WMS Overview page: https://www.cloudbric.com/cloudbric-wms/
- Cloudbric WMS Service Inquiry: https://cloudbric.zendesk.com/hc/en-us/requests/new

Q. Where can I view the changes made to the Cloudbric Managed Rules?

Since Nov 12th, 2021, any changes or updates to Cloudbric Managed Rules are notified on Cloudbric official homepage.

※Due to the variability of the IP address list, the changes made on the IP address list applied to Malicious IP Reputation Protection are not notified on the Cloudbric official homepage.

Cloudbric Managed Rules for AWS WAF Release note URL

- EN: https://www.cloudbric.com/cloudbric-managed-rules-for-aws-waf-release-notes/
- JP: https://www.cloudbric.jp/managed-rules-for-aws-waf-release-notes/

Q. What is the pricing for Cloudbric Managed Rules each month?

The cost for the AWS WAF Managed Rule is estimated by two cost dimensions based on the Web ACLs with Cloudbric Managed Rules applied as stated as follows.

1 **Region**: Number of Regions with web ACL deployed.

2 **Requests**: Number of Requests received by Web ACL per region by units of 1million requests.

Example of estimating cost for Cloudbric OWASP Top 10 Protection:

- OWASP Top 10 Protection cost information:

Units	Cost
Per Region	$25/Month (Pro-rated by the hour)
Per million requests in each region	$1/Month

- Case A:

2 Web ACL with added Cloudbric Managed Rules created for a single region (ex: us-east-1)
Total number of Web requests the Web ACL received was 10million for a month for 2 Web ACLs
Estimate)
us-east-1 Region
① **Region Cost**: $25.00 * 1 = $25.00
② **Requests Cost**: $1.00(Per million) * 10 Requests (Total of 10million) = $10.00

= Total Cost(①+②): $35.00

- Case B:

2 Web ACL with added Cloudbric Managed Rules created for 2 regions (ex: us-east-1, us-west-2)
Total number of requests for 2 Web ACL in each region received was 10million
Estimate)
us-east-1 Region
① **Region Cost**: $25.00 * 1 = $25.00
② **Requests Cost**: $1.00 (Per million) * 10 Requests(Total of 10million) = $10.00
us-west-2 Region
③ **Region Cost**: $25.00 * 1 = $25.00
④ **Requests Cost**: $1.00 (Per million) * 10 Requests(Total of 10million) = $10.00

= Total Cost(①+②+③+④): $70.00

5.2 Rule Descriptions for OWASP Top 10 Protection

Rule Types	Details
Buffer Overflow	Blocks Request sentence including a volume of data that exceeds the limit which a memory Buffer Overflow attack on the web server.
Cross Site Scripting (XSS)	Blocks malicious script code deployed from the client's side.
SQL Injection	Blocks requests attempting to inject SQL Query.
Directory Traversal	Blocks requests attempting to access directories or files using vulnerabilities of the web server.
Request Method Filtering	Blocks against unsafe HTTP Request Methods.
Request Header Filtering	Detects requests as an abnormal request (for instance sent by an automated attack tool) for requests that lack essential elements in the header or cause an error, unlike normal HTTP Request sentences sent from the web browser.
Stealth Commanding	Blocks requests attempting to execute a particular command within the web server through an HTTP Request.
File Upload	Blocks the upload of the file that can be opened from the web server.
XXE Injection	Blocks attacks that cause the browsing of local files using the External entity of XML documents.