Deploying Fortinet AWS WAF Partner Rule Groups

Setup, configuration and FAQ for Fortinet's WAF Rule Groups on Amazon Web Services.

(Updated December 27, 2018)

Overview

AWS WAF Partner Rule Groups are subscription-based web application firewall signatures offered by third-party vendors to augment the basic WAF protections offered by Amazon's WAF product. These new rule groups allow AWS WAF customers to choose pre-packaged WAF rules from leading IT security providers. Until now AWS was offering only SQL Injection and Cross Site Scripting protection. With Partner Rule Groups vendors now offer protection from a wide variety of application layer attacks packaged in a variety of security rulesets.
Fortinet is offering 4 rule groups to AWS customers based on the FortiWeb WAF Service offered by FortiGuard:

RuleGroup	**Description**
SQLi/XSS Rule Group	The SQLi/XSS RuleGroup provides protection from the two primary web application attack types identified in the OWASP Top 10, SQL Injection and Cross-Site Scripting.
General Attacks and Known Exploits Rule Group	The General and Known Exploits rule group detects common and advanced OWASP Top 10 threats including numerous Injection attacks, Remote file inclusion (RFI), Local File Inclusion (LFI), HTTP Response Splitting, Database Disclosure vulnerabilities and other Common Vulnerabilities and Exposures (CVEs).
Malicious Bots Rule Group	The Malicious Bots Rule Group analyzes requests and blocks known content scrapers, spiders looking for vulnerabilities, and other unwanted automated clients that OWASP has identified as risks to web applications.
Complete OWASP Top 10 Rule Group	The Complete OWASP Top 10 Rule Group combines Fortinet's other AWS WAF rule groups into one comprehensive package for the best web application protection offered by Fortinet to cover the entire list of OWASP Top 10 web application threats. Included are the SQLi/XSS, General and Known Exploits, and Malicious Bots rule groups.

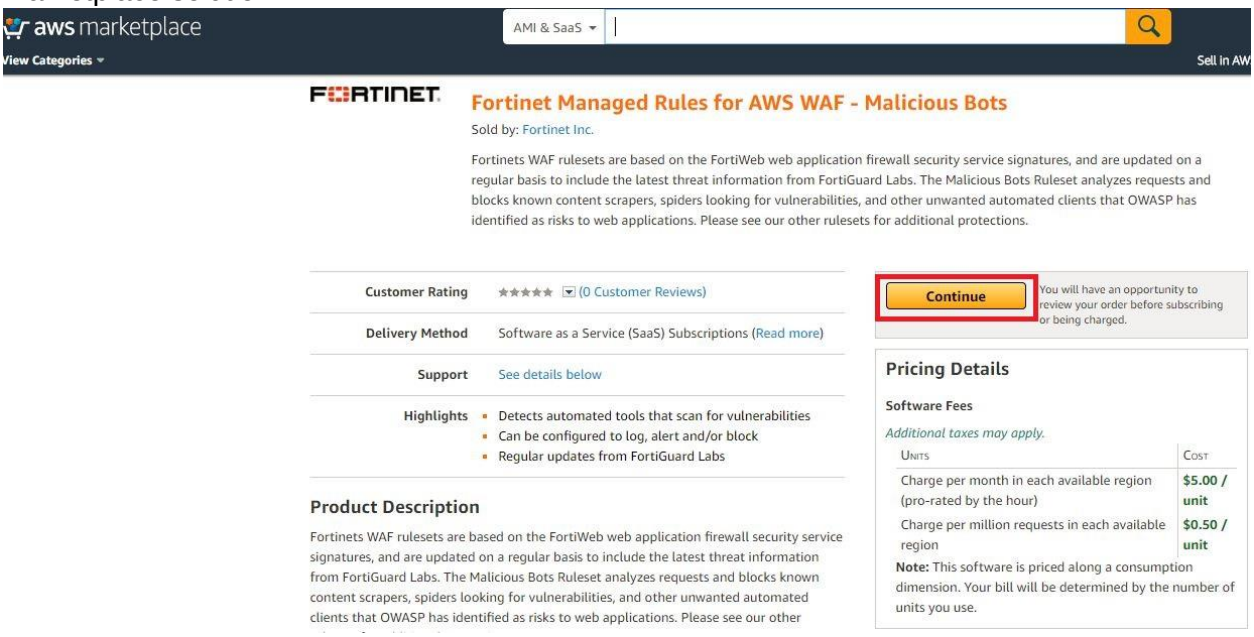
Setup

Similar to the existing AWS WAF solution Partner Rule Groups are implemented in either AWS' ALB (Application Load Balancer) or AWS CloudFront. Since these are a set of signatures and not an actual platform you are not deploying a new VM but rather installing these on an existing instance - either ALB or CloudFront

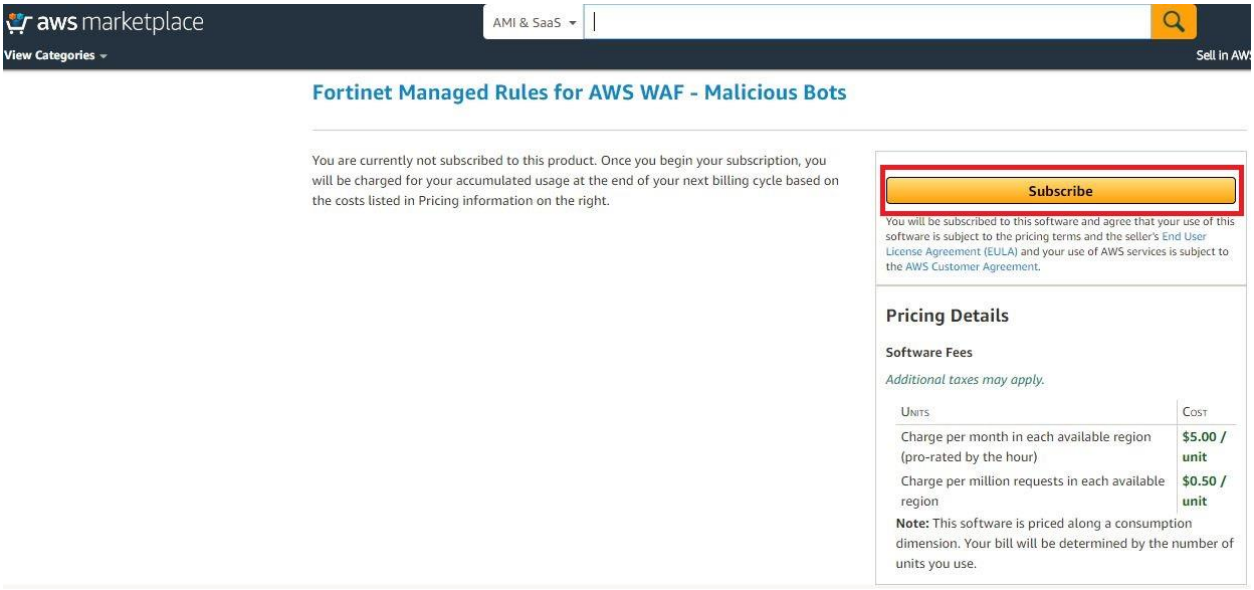
Example

In the following example we deploy Fortinet Malicious Bots Rule Group

- Enable the 'Fortinet Malicious Bots Rule Group subscription'. Click 'Continue' in the marketplace solution.

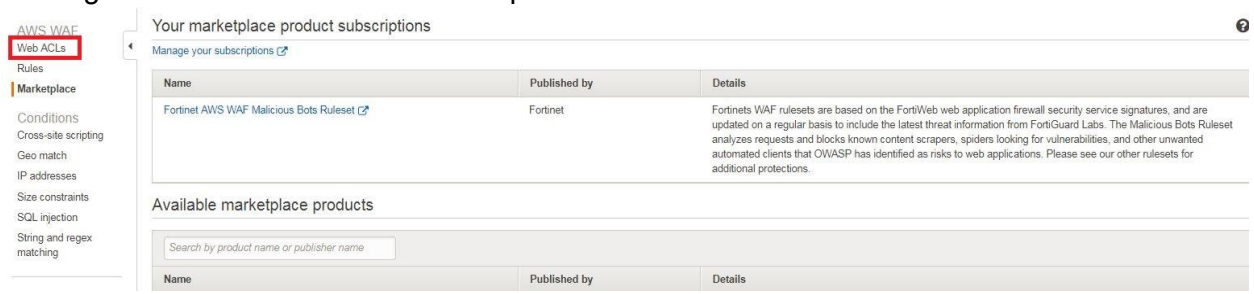


- Click 'Subscribe'

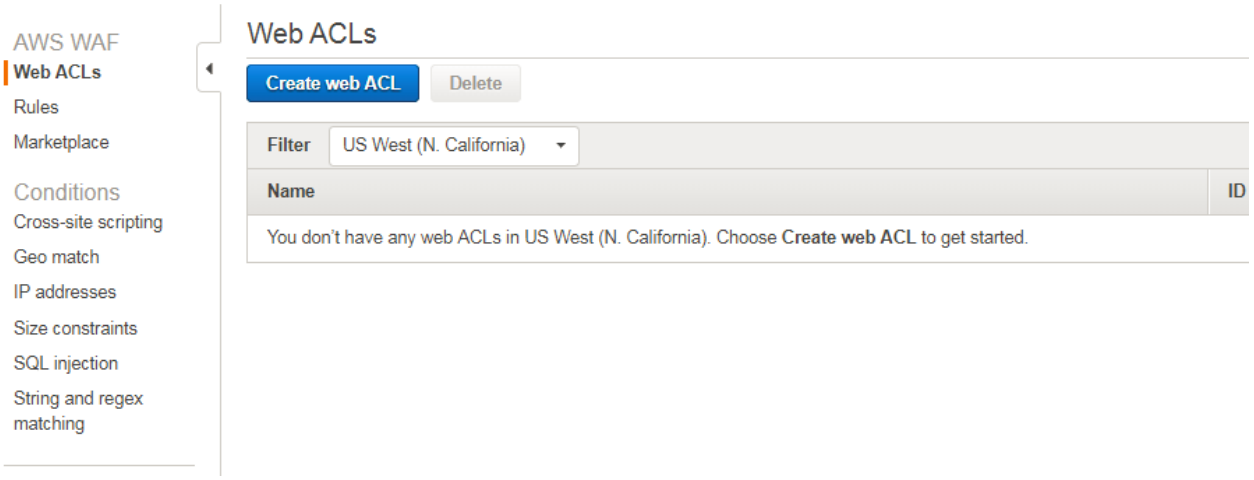


- This will now take you to your existing subscriptions. Now it's time to use this in an

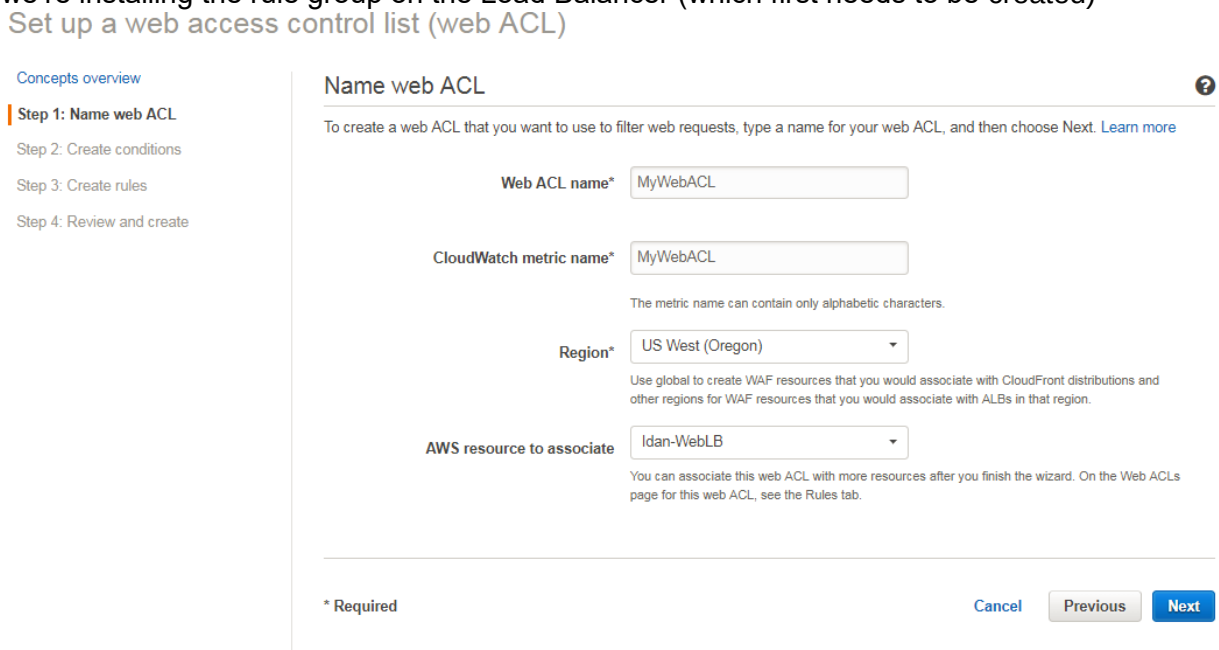
existing VPC. Click ‘WebACL’ on the top left corner



- Choose the region and click on Create web ACL

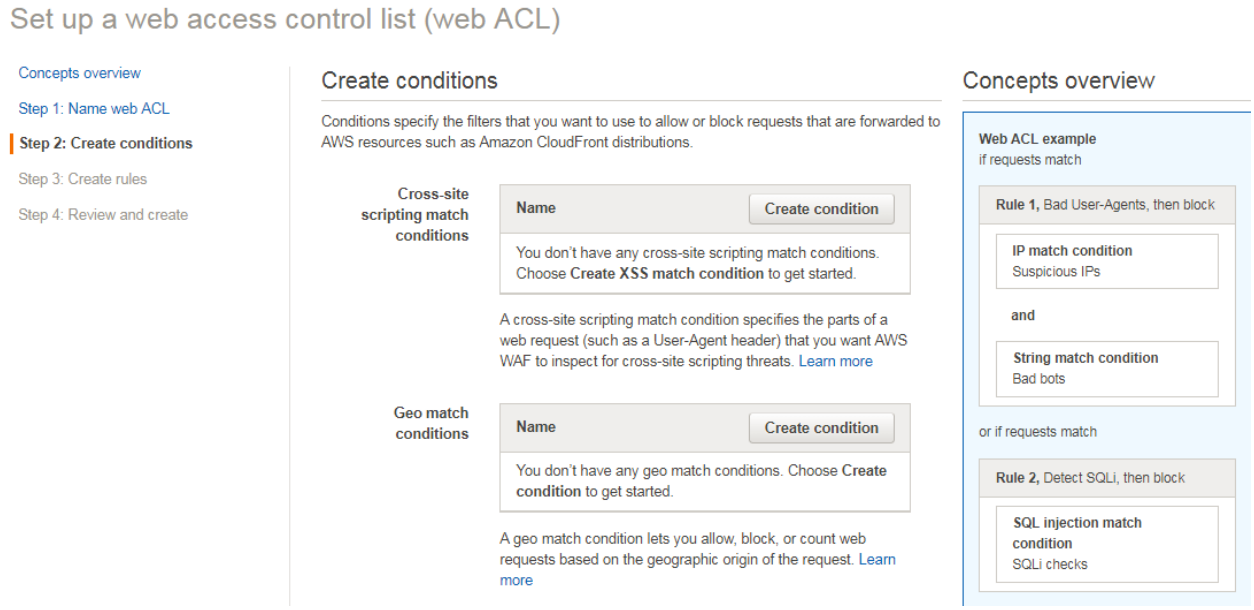


- Name the Web ACL, choose the region and the AWS resource to deploy on. In this case we’re installing the rule group on the Load Balancer (which first needs to be created)

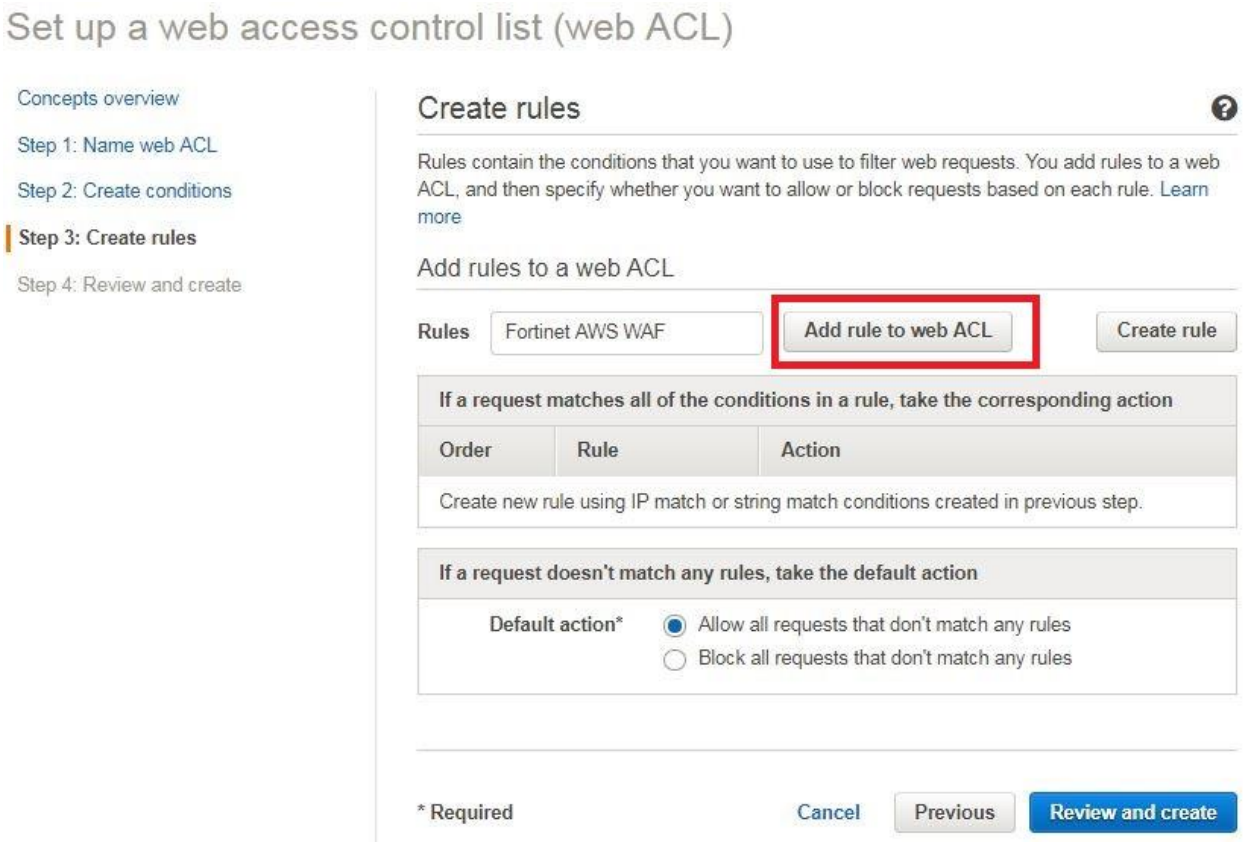


- In this section you can choose predefined AWS WAF conditions. Scroll to the bottom

and click ‘Next’



- Now click on ‘Add rule to web ACL’



- The subscription we chose in phase 2 will be shown. Use the default ‘no override’ unless you don’t want any blocking. Also use the default ‘Allow all requests that don't match any rules’ so AWS WAF blocks only the rule matches

Set up a web access control list (web ACL)

- Concepts overview
- Step 1: Name web ACL
- Step 2: Create conditions
- **Step 3: Create rules**
- Step 4: Review and create

Create rules

Rules contain the conditions that you want to use to filter web requests. You add rules to a web ACL, and then specify whether you want to allow or block requests based on each rule. Learn more

Add rules to a web ACL

Rules Fortinet AWS WAF | Add another rule | Create rule

If a request matches all of the conditions in a rule, take the corresponding action

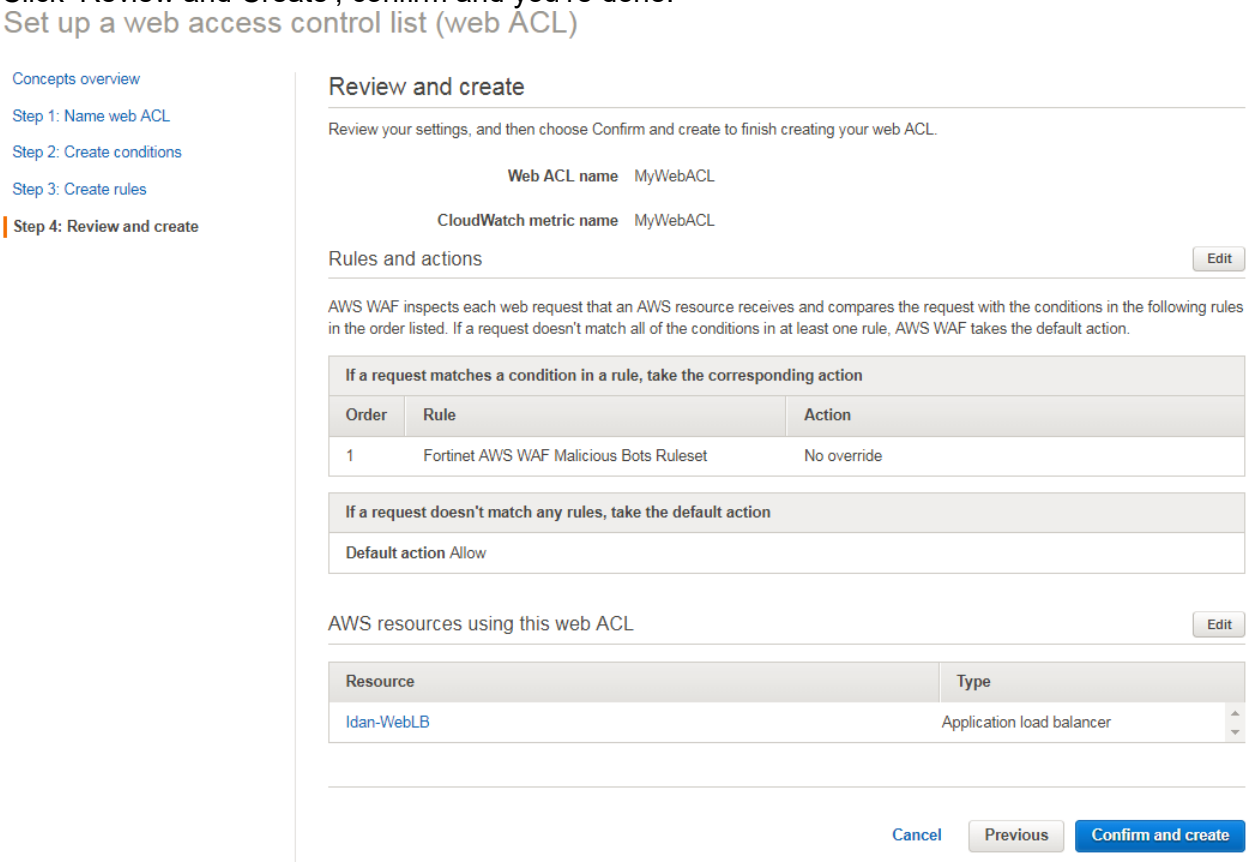
Order	Rule	Action
1	Fortinet AWS WAF Malicious Bots Ruleset	(•) No override ( ) Override to count

If a request doesn't match any rules, take the default action

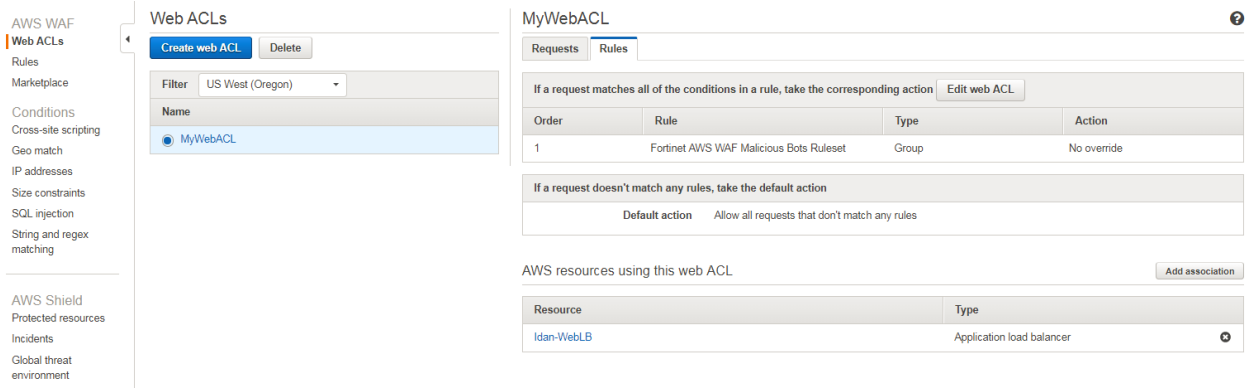
Default action* (•) Allow all requests that don't match any rules ( ) Block all requests that don't match any rules

* Required | Cancel | Previous | Review and create

- Click ‘Review and Create’, confirm and you’re done!



- You should now see your Web ACL and the subscription associated with it



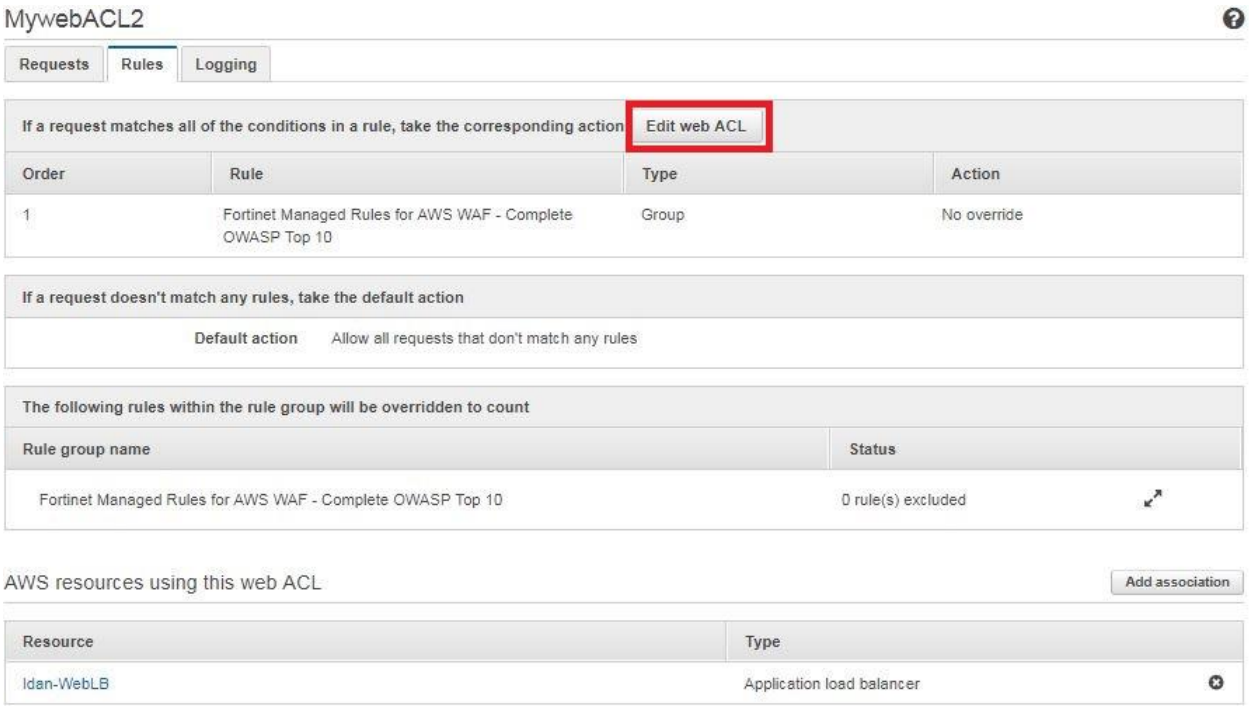
Creating Exceptions/Whitelisting

Sometimes a certain application URL/Page will be blocked by the Rule Group and after further analysis it will be deemed as a false positive. As of December 21, 2018 AWS WAF supports Exceptions for Managed Rules. You can now exclude a specific rule from the Rule Group. The rule is not removed from the Rule Group but the action is changed from BLOCK to COUNT. You will still receive logs for that rule however the page will not be blocked anymore.

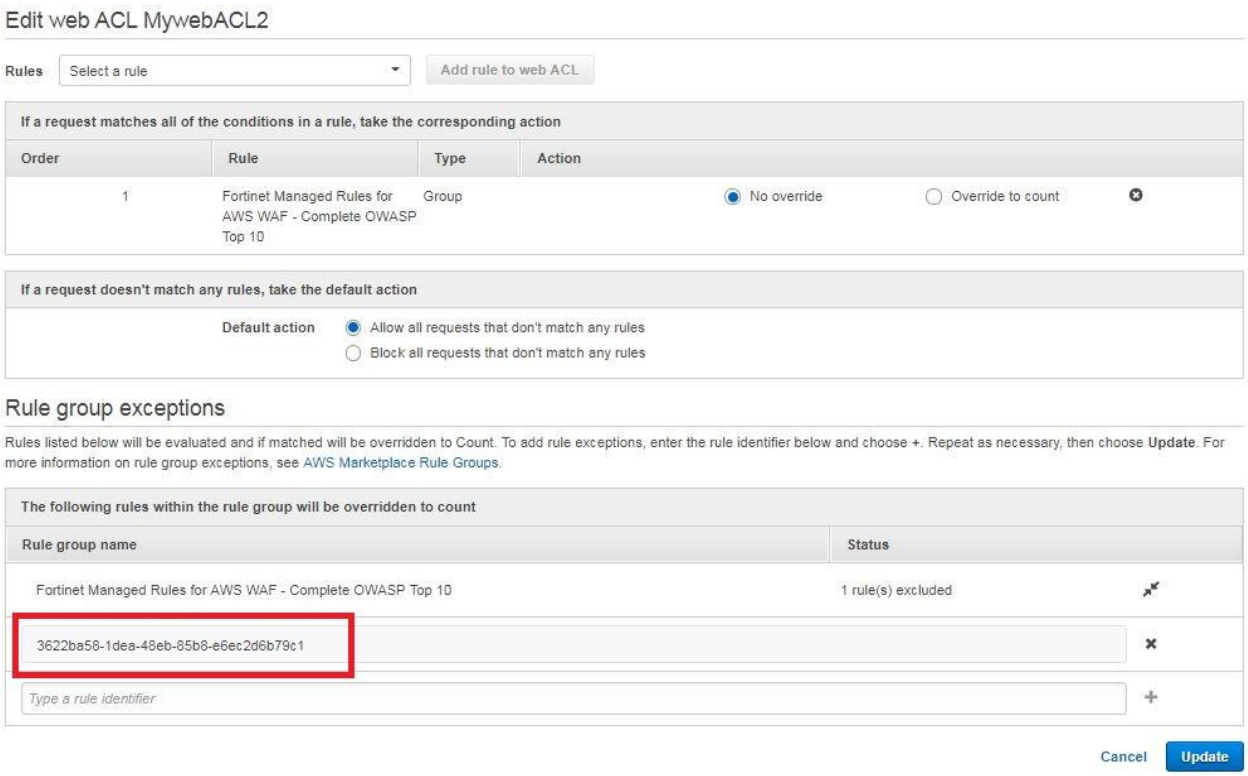
Example

In the following example we will create an Exception for the OWASP Top 10 Rule Group

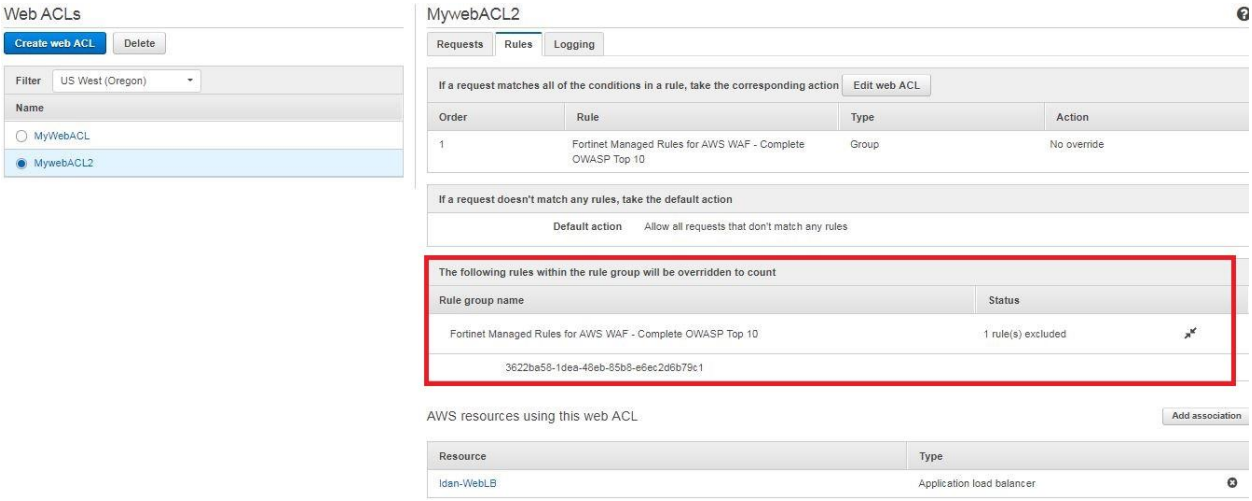
- First, identify the rule that blocked the page. This can be done from either the attack logs or the Full Web Logs. For example - 3622ba58-1dea-48eb-85b8-e6ec2d6b79c1
- Go to the Web ACL and click on 'Rules' and then "Edit web ACL'



- In the Edit page, under Rule group exceptions enlarge the Rule group name. Click the '+' sign and add the rule ID. Click 'Update'



- Upon clicking “Update’ you’ll be taken back to the Web ACL page. You can now see the new rule ID as an exception, which is already in effect. To remove a rule from the exception list simply edit the Web ACL again, click the ‘X’ sign next to the rule ID and click ‘Update’ again.

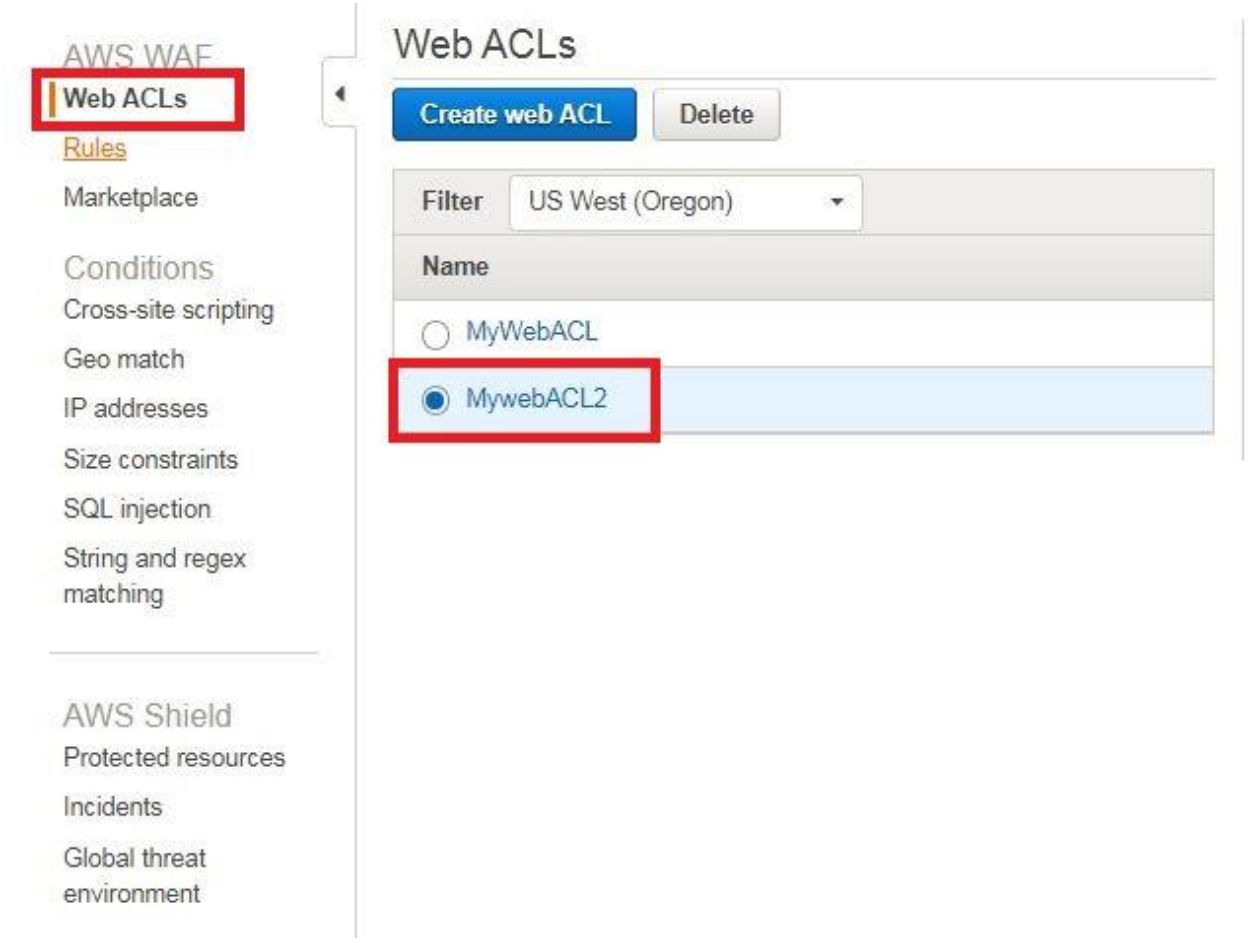


Viewing Attack Logs

There are two ways to view logs. One is through ‘Sample logs’ which generates just a sample of logs. The other is through full web logs, which logs all requests. This is done by using Amazon

Kinesis Data Firehose.

Here is how to view via Sample Logs - You can view logs by choosing the specific WebACL the Rule Group is attached to. Choose the relevant WebACL and then go to the bottom right corner and click “Get new samples”. AWS WAF then produces up to 100 request samples that triggered a rule within the rule group in the previous 15 minutes. Notice this is a sample of logs, AWS does not provide all logs



Sampled requests

To view new samples, choose **Get new samples.**

Fortinet Managed Rules for AWS

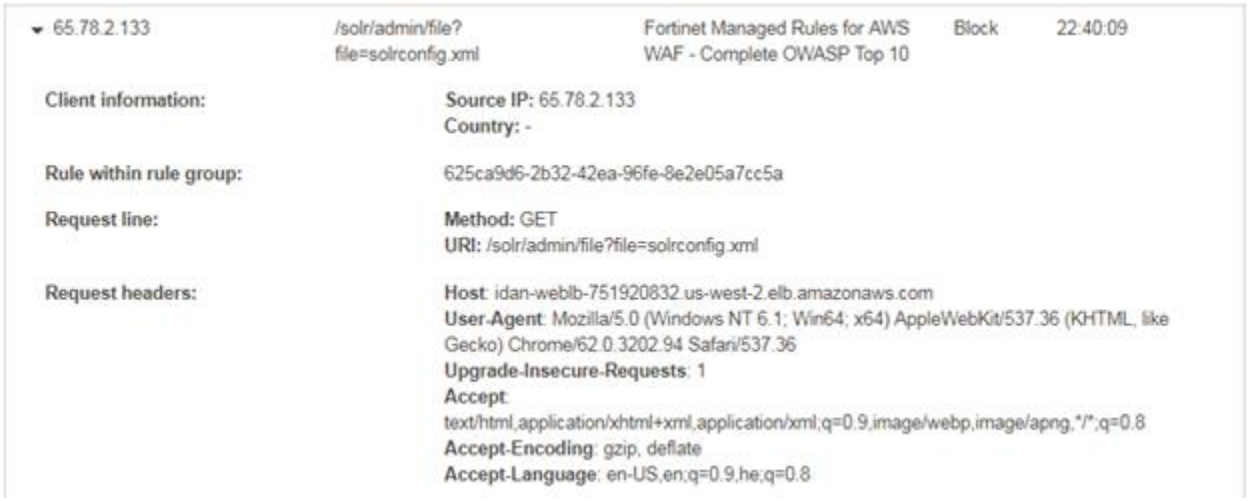
WAF - Complete OWASP Top 10

Get new samples

Sample data from 2017-12-08 22:27:19 to 22:42:19

Source IP	URI	Matches rule	Action	Time (UTC)
65.78.2.133	/login.php?login=http://rfi.nessus.org/rfi.txt	Fortinet Managed Rules for AWS WAF - Complete OWASP Top 10	Block	22:39:16
65.78.2.133	/login.php?login=http://rfi.nessus.org/rfi.txt	Fortinet Managed Rules for AWS WAF - Complete OWASP Top 10	Block	22:39:27
65.78.2.133	/login.php?login=http://rfi.nessus.org/rfi.txt	Fortinet Managed Rules for AWS WAF - Complete OWASP Top 10	Block	22:39:27
65.78.2.133	/login.php?login=http://rfi.nessus.org/rfi.txt	Fortinet Managed Rules for AWS WAF - Complete OWASP Top 10	Block	22:39:28
65.78.2.133	/solr/admin/file?file=solrconfig.xml	Fortinet Managed Rules for AWS WAF - Complete OWASP Top 10	Block	22:40:09
65.78.2.133	/login.php?login=-dauto_prepend_file%3d/etc/passwd	Fortinet Managed Rules for AWS WAF - Complete OWASP Top 10	Block	22:40:30
65.78.2.133	/login.php?login=php://filter/read=convert.base64-encode/resource=config.php	Fortinet Managed Rules for AWS WAF - Complete OWASP Top 10	Block	22:41:00

Notice that the HTTP body is not recorded so HTTP POST parameter information will not be visible. As can be seen from the screenshot the rule ID that triggered the violation is provided but not the rule name (this is the rule within the rule group).



FAQ

Q: Where can customers deploy AWS WAF Partner Rule Groups?

A: AWS WAF Partner Rule Groups can be deployed on AWS CloudFront and AWS ALB

Q: Are Partner Rule Groups deployed globally or per region?

A: Per region. Unless you deploy Partner Rule Groups on CloudFront, which is global, you will need to deploy Partner Rule Groups in each AWS region you have a applications deployed.

Q: Is there a way to view the signatures/rules within the rule group itself?

A: No. The signatures/rules are proprietary vendor information and is not exposed to customers

Q: Can I view the rule name that blocked a request?

A: No. AWS WAF log only reveals the rule ID but not the rule name. Fortinet support can look up the code for more information if needed

Q: Does an AWS log provide HTTP POST information as well?

A: No. AWS logs do not provide visibility into the HTTP body so HTTP POST arguments are not visible

Q: Can I whitelist a rule that triggers a false positive similar to how this is done in FortiWeb?

A: Yes. As of January 21, 2018 AWS support Exceptions. Please see Creating Exceptions/Whitelisting bullet above

Q: Do the Fortinet Rule Group include support?

A: Yes. By purchasing a Fortinet Rule Group customers are entitled for support from Fortinet

Q: What is the process for opening a support ticket with Fortinet?

A: Customers should reach out to awswaf@fortinet.com. Support should direct customers to using this email alias.

Appendix A

AWS WAF Partner Rule Group vendors
https://aws.amazon.com/mp/security/WAFManagedRules/

AWS WAF Rule Group step by step explanation
http://docs.aws.amazon.com/waf/latest/developerguide/waf-managed-rule-groups.html

Viewing a Sample of the Web Requests
http://docs.aws.amazon.com/waf/latest/developerguide/web-acl-testing.html#web-acl-testing-view-sample

Viewing full web logs
https://aws.amazon.com/about-aws/whats-new/2018/08/aws-waf-launches-new-comprehensive-logging-functionality/

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

Creating a rule exception
https://docs.aws.amazon.com/waf/latest/developerguide/waf-managed-rule-groups.html#waf-managed-rule-group-exclude-rule-procedure