FAQs

General

1. What is AWS WAF?

AWS WAF is a web application firewall that helps protect web applications from attacks by allowing you to configure rules that allow, block, or monitor (count) web requests based on conditions that you define. These conditions include IP addresses, HTTP headers, HTTP body, URI strings, SQL injection and cross-site scripting.

2. How does AWS WAF block or allow traffic?

As the underlying service receives requests for your web sites, it forwards those requests to AWS WAF for inspection against your rules. Once a request meets a condition defined in your rules, AWS WAF instructs the underlying service to either block or allow the request based on the action you define.

3. How does AWS WAF protect my web site or application?

AWS WAF is tightly integrated with Amazon CloudFront and the Application Load Balancer (ALB), services that AWS customers commonly use to deliver content for their websites and applications. When you use AWS WAF on Amazon CloudFront, your rules run in all AWS Edge Locations, located around the world close to your end users. This means security doesn't come at the expense of performance. Blocked requests are stopped before they reach your web servers. When you use AWS WAF on Application Load Balancer, your rules run in region and can be used to protect internet-facing as well as internal load balancers.

4. Can I use AWS WAF to protect web sites not hosted in AWS?

Get Started with AWS for Free

Create a Free Account

Receive twelve months of access to the AWS Free Tier and enjoy AWS Basic Support features including, 24x7x365 customer service, support forums, and more.

of AWS.

5. What types of attacks can AWS WAF help me to stop?
AWS WAF helps protects your website from common attack techniques like SQL injection and Cross-Site Scripting (XSS). In addition, you can create rules that can block attacks from specific user-agents, bad bots, or content scrapers. See the AWS WAF Developer Guide for examples.

6. Can I get a history of all AWS WAF API calls made on my account for security, operational or compliance auditing?
Yes. To receive a history of all AWS WAF API calls made on your account, you simply turn on AWS CloudTrail in the CloudTrail's AWS Management Console. For more information, visit AWS CloudTrail home page or visit the AWS WAF Developer Guide.

7. Does AWS WAF support IPv6?
Yes, support for IPv6 allows the AWS WAF to inspect HTTP/S requests coming from both IPv6 and IPv4 addresses.

8. Does IPSet match condition for an AWS WAF Rule support IPv6?
Yes, you can setup new IPv6 match condition(s) for new and existing WebACLs, as per the documentation.

9. Can I expect to see IPv6 address appear in the AWS WAF sampled requests where applicable?
Yes. The sampled requests will show the IPv6 address where applicable.

10. Can I use IPv6 with all AWS WAF features?
Yes. You will be able to use all the existing features for traffic both over IPv6 and IPv4 without any discernable changes to performance, scalability or availability of the service.

11. What services does AWS WAF support?
AWS WAF can be deployed on Amazon CloudFront and the Application Load Balancer (ALB). As part of

resources and content at the Edge locations and as part of the Application Load Balancer it can protect your origin web servers running behind the ALBs.

12. In what Regions is AWS WAF on ALB available in?

AWS WAF on ALB is available in the following AWS Regions.

13. Is AWS WAF HIPAA eligible?

Yes, AWS has expanded its HIPAA compliance program to include AWS WAF as a HIPAA eligible service. If you have an executed Business Associate Agreement (BAA) with AWS, you can use AWS WAF to protect your web applications from common web exploits. For more information, see HIPAA Compliance.

14. How does AWS WAF pricing work? Are there any upfront costs?

AWS WAF charges based on the number of web access control lists (web ACLs) that you create, the number of rules that you add per web ACL, and the number of web requests that you receive. There are no upfront commitments. AWS WAF charges are in addition to Amazon CloudFront Pricing and/or the Application Load Balancer (ALB) pricing.

15. What is Rate-based Rule in AWS WAF?

Rate-based Rules are a new type of Rule that can be configured in AWS WAF. This feature allows you to specify the number of web requests that are allowed by a client IP in a trailing, continuously updated, 5 minute period. If an IP address breaches the configured limit, new requests will be blocked until the request rate falls below the configured threshold.

16. How does a Rate-based rule compare to a regular AWS WAF Rule?

Rate-based Rules are similar to regular Rules, with one addition: the ability to configure a rate-based block all IPs that have more than 2,000 requests in the last 5 minute interval. A Rate-based Rule can also contain any other AWS WAF Condition that is available for a regular rule.

17. What does the Rate-based Rule cost?

A Rate-based Rule costs the same as a regular AWS WAF Rule which is $1 per rule per WebACL per month

18. What are the use cases for the Rate-based Rule?

Here are some popular use cases customers can address with Rate-based rules:

- I want to blacklist or count an IP address when that IP address exceeds the configured threshold rate (configurable in web requests per trailing 5 minute period)
- I want to know which IP address are currently being blacklisted because they exceeded the configured threshold rate
- I want IP addresses that have been added to the blacklist to be automatically removed when they are no longer violating the configured threshold rate
- I want to exempt certain high-traffic source IP ranges from being blacklisted by my Rate-based rules

19. Are the existing matching conditions compatible with the Rate-base Rule?

Yes. Rate-based rules are compatible with existing AWS WAF match conditions. This allows you to further refine your match criteria and limit rate-based mitigations to specific URLs of your website or traffic coming from specific referrers (or user agents) or add other custom match criteria.

20. Can I use Rate-based rule to mitigate Web layer DDoS attacks?

force login attempts and bad bots.

21. What visibility features does Rate-based Rules offer?

Rate-based Rules support all the visibility features currently available on the regular AWS WAF Rules. Additionally, they will get visibility into the IP addresses blocked as a result of the Rate-based Rule.

22. Can I use Rate-based rule to limit access to a certain parts of my Webpage?

Yes. Here is an example. Suppose that you want to limit requests to the login page on your website. To do this, you could add the following string match condition to a rate-based rule:

- The Part of the request to filter on is “URI”.
- The Match Type is “Starts with”.
- A Value to match is “/login” (this need to be whatever identifies the login page in the URI portion of the web request)

Additionally, you would specify a Rate Limit of, say, 15,000 requests per 5 minutes. Adding this rate-based rule to a web ACL will limit requests to your login page per IP address without affecting the rest of your site.

23. Can I exempt certain high-traffic source IP ranges from being blacklisted by my Rate-based Rule(s)?

Yes. You can do this by having an IP Whitelist condition within the Rate-base Rule.

24. How accurate is your GeoIP database?

The accuracy of the IP Address to country lookup database varies by region. Based on recent tests, our overall accuracy for the IP address to country mapping is 99.8%.

WAF

1. What are AWS WAF Managed Rules?

AWS WAF Managed Rules are an easy way to deploy pre-configured rules to protect your applications common threats like application vulnerabilities like OWASP, bots, or Common Vulnerabilities and Exposures (CVE). All Managed Rules are automatically updated by AWS Marketplace security Sellers.

2. How can I subscribe to Managed Rules?

You can subscribe to a Managed Rule provided by a Marketplace security Seller from the AWS WAF console or from the AWS Marketplace. All subscribed Managed Rules will be available for you to add to an AWS WAF web ACL.

3. Can I use Managed Rules along with my existing AWS WAF rules?

Yes, you can use Managed Rules along with your custom AWS WAF rules. You can add Managed Rules to your existing AWS WAF web ACL to which you might have already added your own rules.

4. Does a Managed Rule have multiple AWS WAF rules?

Yes, each Managed Rule could have multiple AWS WAF rules. The number of rules depends on each security seller and their Marketplace product.

5. Will Managed Rules add to my existing AWS WAF limit on number of rules?

The number of rules inside a Managed Rule does not impact your AWS WAF limits. But each Managed Rule added to your web ACL will count as 1 rule.

6. How can I disable a Managed Rule?

You can add a Managed Rule to a web ACL or remove it from the web ACL anytime. The Managed Rules are disabled once you disassociate a Managed Rule from any web ACLs.

for a Managed Rule, which counts the number of web requests that are matched by the rules inside the Managed Rule. You can look at the number of counted web requests to estimate how many of your web requests would be blocked if you enable the Managed Rule.

AWS WAF Configuration

1. Can I configure custom error pages?
Yes, you can configure CloudFront to present a custom error page when requests are blocked. Please see the CloudFront Developer Guide for more information

2. How long does it take AWS WAF to propagate my rules?
After an initial setup, adding or changing to rules typically takes around a minute to propagate worldwide.

3. How can I see if my rules are working?
AWS WAF includes two different ways to see how your website is being protected: one-minute metrics are available in CloudWatch and Sampled Web Requests are available in the AWS WAF API or management console. These allow you to see which requests were blocked, allowed, or counted and what rule was matched on a given request (i.e., this web request was blocked due to an IP address condition, etc.). For more information see the AWS WAF Developer Guide.

4. How can I test my rules?
AWS WAF allows you to configure a “count” action for rules, which counts the number of web requests that meet your rule conditions. You can look at the number of counted web requests to estimate how many of your web requests would be blocked or allowed if you enable the rule.

5. How long are Real-Time Metrics and Sampled Web Requests stored?
Real-Time Metrics are stored in Amazon CloudWatch. Using Amazon CloudWatch you can configure the time period in which you want to expire events. Sampled Web Requests are stored for up to 2 hours.

6. Can AWS WAF inspect HTTPS traffic?
Yes. AWS WAF helps protect applications and can inspect web requests transmitted over HTTP or HTTPS.

Twitter Facebook Podcast Twitch AWS Blog RSS News Feed
Email Updates

AWS & Cloud Computing

What is Cloud Computing?
What is Caching?
What is NoSQL?
What is DevOps?
What is Docker?
Products & Services
Customer Success
Economics Center
Architecture Center
Security Center
What's New
Whitepapers
AWS Blog
Events
Sustainable Energy
Press Releases
AWS in the News
Analyst Reports
Legal

Solutions

Websites & Website Hosting
Business Applications
Backup & Recovery
Disaster Recovery
Data Archive
DevOps
Serverless Computing
Big Data
High Performance Computing
Mobile Services
Digital Marketing
Game Development
Digital Media
Government & Education
Health
Financial Services
Windows on AWS

Oil & Gas

Automotive

Blockchain

Manufacturing

Resources & Training

Developers

Java on AWS

JavaScript on AWS

Mobile on AWS

PHP on AWS

Python on AWS

Ruby on AWS

.NET on AWS

SDKs & Tools

AWS Marketplace

User Groups

Support Plans

Service Health Dashboard

Discussion Forums

FAQs

Documentation

Articles & Tutorials

Quick Starts

Manage Your Account

Management Console

Billing & Cost Management

Subscribe to Updates

Personal Information

Payment Method

AWS Identity & Access Management

Security Credentials

Request Service Limit Increases

Contact Us

Amazon Web Services is Hiring.

Amazon Web Services (AWS) is a dynamic, growing business unit within Amazon.com. We are currently hiring Software Development Engineers, Product Managers, Account Managers, Solutions Architects, Support Engineers, System Engineers, Designers and more. Visit our careers page to learn more.

Language Bahasa Indonesia | Deutsch | English | Español | Français | Italiano | Português | Tiếng Việt | Türkçe | Русский | ไทย | 日本語 | 한국어 | 中文 (简体) | 中文 (繁體)

Site Terms | Privacy

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.