AWS WAF or AWS Shield: What's the Difference?

AWS WAF (Web Application Firewall) and AWS Shield can help you protect your web applications against various types of cyberattacks, such as Distributed Denial of Service (DDoS) attacks and other web application vulnerabilities.

AWS WAF focuses on protecting your web applications from common web exploits. Use AWS WAF to create customizable web security rules to filter malicious traffic, protect against attacks such as SQL injection and cross-site scripting (XSS), and integrate with other AWS services.

AWS Shield is a managed DDoS protection service. Use AWS Shield to turn on always-on detection and automatic mitigations and protect against common DDoS attacks at the network and transport layers.

While AWS Shield defends against large-scale, network-level attacks, with AWS Shield Advanced, you can associate an AWS WAF web ACL with a resource to provide protection at the application layer. AWS WAF provides more granular protection against application-specific vulnerabilities. Use both services in tandem for a multi-layered defense strategy, safeguarding your applications from a broader range of potential threats across different network layers.

Here's a high-level view of the key differences between these services.

Category	AWS WAF	AWS Shield
Primary Purpose	Protects against exploits on web applications (such as SQL injection or XSS)	Protects against DDoS attacks (such as SYN or UDP floods)
Layer of protection	Application layer (L7)	Network, transport, and application layers (L3/L4/L7)
Deployment	Must be explicitly set up	AWS Shield Standard protection included for all customer accounts

Category	AWS WAF	AWS Shield
Customization	Highly customizable with custom rules	Turn on or disable AWS Shield Advanced, with options to turn on automatic mitigation of application layer DDoS protections
Managed Rules	Includes AWS Managed Rules and third-party rules	Not applicable
Pricing model	Pay-as-you-go pricing based on number of rules and requests	AWS Shield Standard included; AWS Shield Advanced incurs additional cost
Attack Response Team	Not applicable	Available with AWS Shield Advanced (24/7 DDoS Response Team)
Real-time monitoring	Yes	Yes
Traffic Inspection	Request-level	Packet-level

Differences between AWS WAF and AWS Shield

Explore eight key areas of difference between AWS Shield and AWS WAF, covering layer of protection, deployment, customization, managed rules, pricing model, attack response team, real-time monitoring, and traffic inspection.

Layer of Protection

AWS WAF

Operates the application layer (Layer 7). It protects web applications by filtering and monitoring HTTP/S traffic. AWS WAF defends against common web exploits such as SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). You can create custom rules to block malicious requests based on various criteria like IP addresses, query strings, and headers.

AWS Shield

Operates primarily on the network (Layer 3) and transport (Layer 4) layers. It is designed to mitigate Distributed Denial of Service (DDoS) attacks that aim to overwhelm network resources, such as SYN/ACK floods, UDP reflection attacks, and volumetric attacks. AWS Shield ensures that network traffic reaching your AWS resources remains available even under attack. AWS Shield's protection works by analyzing network traffic patterns and automatically mitigating identified threats at the AWS network edge.

The services described best practices outlined in the design principles of the AWS Well-Architected Framework Security Pillar to secure the edge devices and applications themselves. Together, implementation of these services provides a strong defense in depth strategy to secure edge devices and applications.

Deployment

AWS WAF

Requires explicit setup and configuration. It can be deployed on multiple AWS services, including Amazon CloudFront, Application Load Balancer (ALB), Amazon API Gateway, and AWS AppSync. You must create and associate web ACLs (Access Control Lists) with your resources, defining rules to allow, block, or monitor specific web requests. AWS WAF offers customizable deployment options, allowing you to tailor security policies to your specific application needs.

AWS Shield

Automatically integrated with AWS services and is always on, requiring no additional setup for basic protection. AWS Shield Standard is automatically included with all AWS accounts, protecting resources like Amazon EC2, Elastic Load Balancing (ELB), Amazon CloudFront, and Route 53. For enhanced protection with AWS Shield Advanced, you must explicitly turn it on for specific resources. Deployment is seamless, and no additional configuration is necessary once AWS Shield is turned on.

Customization

AWS WAF

Provides extensive customization capabilities. You can create custom web ACLs (Access Control Lists) with rules that define specific conditions for allowing, blocking, or counting web requests based on IP addresses, HTTP headers, query string parameters, and more. AWS WAF supports

managed rule groups from AWS or third parties, which can be customized further to suit your specific application needs. You can also set up rate-based rules to limit the number of requests from a single IP address and integrate AWS WAF with AWS Lambda for advanced request inspection and response.

AWS Shield

Offers limited customization options. With AWS Shield Standard, protection is automatic and non-configurable. AWS Shield Advanced allows for customization, such as enabling advanced metrics and alerts, setting up Health Checks, and accessing the AWS DDoS Response Team (DRT) for tailored mitigation support. However, its focus remains on automated DDoS protection rather than user-defined settings. You can associate an AWS WAF web ACL with resources to turn on application layer protection.

Managed Rules

AWS WAF

Offers a range of managed rules that can be applied to web applications to protect against common web threats. These managed rules are pre-configured by AWS or third-party security vendors and cover various security scenarios such as SQL injection, cross-site scripting (XSS), and known bad IP addresses. You can subscribe to and apply these managed rule groups to your web ACLs, providing out-of-the-box protection that is regularly updated to address new vulnerabilities and threats. Managed rules can be customized and combined with custom rules to tailor security policies to specific application needs. AWS WAF also provides managed intelligent threat mitigation features. These are advanced, specialized protections that you can implement to protect against threats such as malicious bots and account takeover attempts.

AWS Shield

Primarily focused on DDoS protection and doesn't offer traditional managed rules. AWS Shield Standard automatically applies a set of predefined protections against common network and transport layer DDoS attacks. AWS Shield Advanced enhances these protections but doesn't provide customizable managed rules. Instead, it offers more advanced mitigation techniques and access to the DDoS Response Team for tailored assistance.

Pricing Model

AWS WAF

Uses a pay-as-you-go pricing model. You are charged based on the number of web ACLs you create the number of rules you deploy within each ACL, and the number of web requests processed by the rules. This model allows for scalable costs based on actual usage, meaning you only pay for the resources you need. Additional charges apply for managed rule groups provided by AWS or third-party vendors. AWS WAF also provides managed rules for Bot control and fraud control with a similar per request pricing model. AWS WAF also offers a captcha/challenge feature which is charged by the number of captchas attempts and challenge responses served.

AWS Shield

Has a tiered pricing model. AWS Shield Standard is included at no additional cost with all AWS accounts, providing basic DDoS protection. AWS Shield Advanced incurs a fee based on a monthly subscription and additional charges for data transfer and mitigation beyond a certain threshold. This subscription includes 24/7 access to the AWS DDoS Response Team (DRT), advanced attack diagnostics, and cost protection during attacks.

Attack Response Team

AWS WAF

Does not include a dedicated attack response team as part of its service. Instead, it provides tools and features that allow you to create, manage, and adjust security rules themselves. You can monitor traffic and make real-time changes to your web ACLs based on the threat landscape, but you don't have direct access to a specialized support team for attack mitigation.

AWS Shield

Offers access to the AWS DDoS Response Team (DRT) as part of its AWS Shield Advanced service. The DRT is a 24/7 team of experts that assists with real-time attack mitigation and response. When under a DDoS attack, you can contact the DRT for customized advice and support to manage and mitigate the threat effectively. This includes guidance on best practices, incident analysis, and coordinated responses to minimize the impact on your AWS resources.

Real-time Monitoring

AWS WAF

It offers real-time monitoring by integrating with AWS CloudWatch, allowing you to track metrics such as blocked or allowed requests, request rates, and the effectiveness of specific rules. AWS WAF provides near real-time visibility into web traffic and security events through the AWS Management Console or APIs. You can set up custom CloudWatch alarms based on your AWS WAF metrics to respond quickly to potential threats or unusual traffic patterns.

AWS Shield

Provides real-time monitoring primarily through AWS Shield Advanced. It integrates with AWS CloudWatch to deliver near real-time metrics and alerts related to DDoS attacks. You can monitor attack diagnostics, traffic patterns, and the effectiveness of mitigation. AWS Shield Advanced also offers detailed reports and visibility into attack vectors and scales automatically in response to threats, providing insights through the AWS Management Console

Both services provide dashboards for visualizing attack patterns and traffic trends. AWS Shield's monitoring focuses on network-level anomalies and volumetric attacks, while AWS WAF provides deeper insights into application-layer requests and rule effectiveness.

Traffic Inspection

AWS WAF

Inspects traffic at the application layer (Layer 7), analyzing the contents of HTTP/S requests. It evaluates web traffic against user-defined rules, checking for specific attack patterns such as SQL injection, cross-site scripting (XSS), or other malicious payloads within the request body, headers, or URL parameters.

AWS Shield

Focuses on protecting against DDoS attacks, primarily inspecting traffic at the network (Layer 3) and transport (Layer 4) layers. It does not inspect the contents of application layer traffic (HTTP/S), but rather looks for patterns typical of DDoS attacks, such as unusually high traffic volumes or protocol misuse. AWS Shield automatically mitigates these threats without user defined rules or content-based inspection, ensuring the availability of AWS services under attack.

Source: AWS Documentation