Service Name

AWS WAF

Service Overview

AWS WAF is a web application firewall service that helps protect web applications from attacks by monitoring HTTP(S) requests to protected resources and allowing, blocking, or counting requests based on defined conditions. The service provides protection against common web exploits like SQL injection, cross-site scripting, and DDoS attacks at the application layer. AWS WAF can be deployed on Amazon CloudFront, Application Load Balancer, API Gateway, AWS AppSync, Amazon Cognito user pools, AWS App Runner, AWS Verified Access, and AWS Amplify applications. The service uses web access control lists (ACLs) containing rules that evaluate requests based on criteria like IP addresses, HTTP headers, HTTP body content, URI strings, query strings, and geographic locations.

Key Use Cases

- Web Application Protection: Shield applications from common attacks like SQL injection, cross-site scripting (XSS), file inclusion, and cross-site request forgery
- Bot Control and Mitigation: Block malicious bots while allowing legitimate ones like search engines and monitoring tools using machine learning and advanced detection
- DDoS Protection: Provide application-layer DDoS protection with rate-based rules and automatic baseline detection to mitigate volumetric attacks
- API Security: Protect REST APIs and GraphQL APIs from abuse, rate limiting, and malicious requests across multiple AWS services
- Fraud Prevention: Prevent account takeover attempts and fraudulent account creation using behavioral analysis and credential intelligence
- Geographic Access Control: Block or allow traffic based on geographic location to comply with regional regulations or business requirements

Features

- **Web Traffic Filtering**: Create rules based on IP addresses, HTTP headers, HTTP body, URI strings, and query parameters
- **AWS Managed Rules**: Pre-configured rule groups maintained by AWS for common threats like OWASP Top 10
- **Bot Control**: Advanced bot detection and mitigation using machine learning to distinguish legitimate from malicious bots
- **Rate-based Rules**: Limit the number of requests from specific IP addresses within defined time windows

- **Fraud Control**: Account takeover prevention and account creation fraud detection with behavioral analysis
- **Real-time Visibility**: Real-time metrics, sampled web requests, and comprehensive logging with CloudWatch integration
- **Custom Response**: Configure custom response codes, headers, and error pages when blocking requests
- **Geographic Blocking**: Allow or block requests based on country of origin using GeoIP database

Value Proposition

AWS WAF offers comprehensive application-layer security with native integration across AWS services, eliminating the need for separate security appliances or complex configurations. The service provides expert-level protection through continuously updated managed rules, reducing the security expertise burden on customers:

- With simplified configuration workflows and pre-configured protection packs, setup time is reduced by up to 80%
- AWS WAF scales automatically without capacity planning, offers pay-as-you-use pricing with no upfront costs, and provides unified management through AWS Firewall Manager
- The service integrates seamlessly with AWS Shield for DDoS protection and provides real-time visibility and monitoring capabilities through CloudWatch

Service Integration

AWS WAF integrates natively with multiple AWS services as the first line of defense. Core integrations include Amazon CloudFront for global edge protection, Application Load Balancer for regional application protection, Amazon API Gateway for REST API security, and AWS AppSync for GraphQL API protection:

- Additional integrations cover Amazon Cognito user pools for authentication security, AWS App Runner for container applications, AWS Verified Access for zero-trust access, and AWS Amplify for hosted web applications
- The service works closely with AWS Shield Advanced for enhanced DDoS protection, AWS Firewall Manager for centralized management, Amazon CloudWatch for monitoring and alerting, and supports logging to Amazon S3, CloudWatch Logs, and Amazon Data Firehose

Onboarding and Offboarding

Customers can get started with AWS WAF through the simplified new console experience by creating a protection pack (web ACL) tailored to their application type. The setup process involves selecting AWS resources to protect, choosing initial protection rules from managed rule groups or custom rules, and configuring default actions and logging:

- The new console provides guided workflows with pre-configured protection packs for different application types like e-commerce and transaction processing
- Customers can also use Infrastructure as Code tools like AWS CloudFormation or AWS CDK for programmatic deployment
- The service offers one-click integration with supported AWS services, and customers can start with count mode to test rules before enabling blocking actions

Getting Started Guide: https://docs.aws.amazon.com/waf/latest/developerguide/setup-iap-console.html

Data Removal

To offboard from AWS WAF, customers must first disassociate web ACLs from all protected resources, then delete the web ACLs, rules, rule groups, IP sets, and regex pattern sets. Configuration data is removed immediately upon deletion. Log data stored in CloudWatch Logs, S3, or Data Firehose must be deleted separately according to the respective service's data retention policies. Customers should ensure all AWS resources are disassociated before deletion to prevent service disruptions.

Backup/Restore and Disaster Recovery

AWS WAF configurations are automatically replicated within the region for high availability but do not provide built-in cross-region backup capabilities. Customers must implement their own backup strategies using Infrastructure as Code tools like CloudFormation or by exporting configurations via APIs. Rule configurations, IP sets, and web ACL settings can be recreated programmatically. Log data stored in associated services follows those services' backup and disaster recovery capabilities.

Backup Capabilities

AWS WAF does not provide native backup capabilities for configuration data. Customers must use Infrastructure as Code practices with AWS CloudFormation, AWS CDK, or direct API calls to maintain configuration backups:

- The service automatically maintains rule evaluation state but does not backup historical configurations
- Rule sets and web ACL configurations should be version controlled externally for backup purposes

Disaster Recovery

AWS WAF supports disaster recovery through multi-region deployment strategies where customers deploy identical configurations across regions. The service integrates with Application Recovery Controller for coordinated failover:

- Configuration replication must be managed manually or through automation

- AWS WAF does not integrate directly with AWS Elastic Disaster Recovery but can be part of broader disaster recovery architectures

Recovery Objectives

AWS WAF helps achieve aggressive RTO and RPO objectives through its real-time processing capabilities and regional availability. Rule changes propagate within minutes, and the service maintains sub-second latency for request processing. For disaster recovery scenarios, customers can achieve RTOs of minutes to hours depending on automation sophistication. RPO is near-zero for active configurations since rules are evaluated in real-time without data persistence requirements.

Service Constraints

Service Quotas: https://docs.aws.amazon.com/waf/latest/developerguide/limits.html

FAQ: https://aws.amazon.com/waf/faqs/

Technical Requirements

Service Documentation: https://docs.aws.amazon.com/waf/latest/developerguide/waf-chapter.html

User Guide: https://docs.aws.amazon.com/waf/latest/developerguide/waf-chapter.html

API Reference: https://docs.aws.amazon.com/waf/latest/APIReference/Welcome.html

Pricing Overview

Please see the AWS UK G Cloud 15 Pricing Document accompanying this service in the Digital Marketplace.

Public Pricing: https://aws.amazon.com/waf/pricing/

Cost Optimization

AWS WAF offers several unique cost optimization strategies including scope-down statements to limit advanced rule evaluation to specific pages, reducing Bot Control costs. Using AWS Shield Advanced eliminates additional WAF charges for high-volume workloads:

- Customers can optimize by applying lower-cost rules before expensive managed rules, separating static content to different distributions, and using protection packs to avoid individual rule charges
- Rate-based rules provide cost-effective DDoS protection compared to always-on blocking rules
- The service offers request-based pricing with no upfront costs, allowing precise cost control based on actual usage

Savings Considerations

Primary cost savings come from preventing application downtime and data breaches through proactive threat blocking. Automated managed rules reduce operational overhead compared to manual security management:

- The pay-per-use model eliminates capital expenses for security appliances
- Integration with AWS Shield Advanced provides additional WAF features at no extra cost for qualifying workloads
- Bot Control helps reduce infrastructure costs by blocking malicious traffic before it reaches applications
- Customers save on operational costs through centralized management with AWS Firewall Manager and reduced need for specialized security expertise through pre-configured protection packs