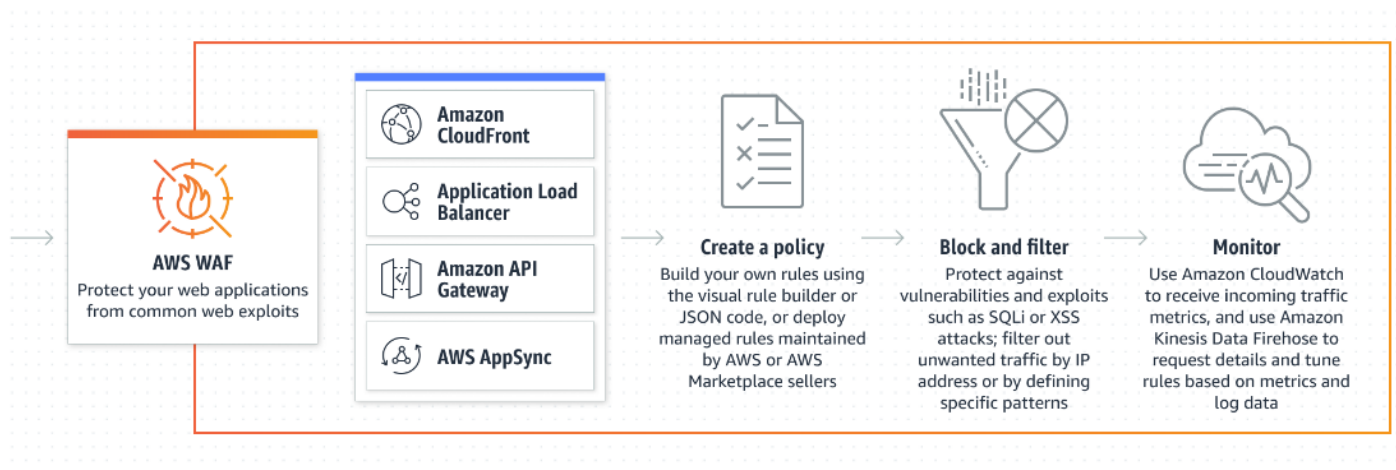


Web Application Firewall (WAF) Overview:

A Web Application Firewall (WAF) is a specific form of a firewall that monitors, filters, and blocks data packets as they travel to and from a website or web application. Unlike traditional firewalls that filter traffic based on port and protocol, WAFs dive deeper to inspect the content of the data and are designed to protect web apps from various types of malicious traffic.

Benefits of WAF:

1. **Protection Against Web Attacks:** WAFs safeguard web applications by filtering and monitoring HTTP traffic between a web application and the Internet.
2. **Mitigation of OWASP Top 10 Risks:** WAFs can help mitigate vulnerabilities from the OWASP Top 10, including SQL injection, cross-site scripting, and more.
3. **Customizable Rules:** WAFs allow for custom rules that fit specific use cases of web applications, providing tailored security.
4. **Defends Against DDoS:** WAFs offer protection against certain types of DDoS attacks targeting application layers.
5. **Access Control:** Restrict who can access your web application, preventing unauthorized access.



WAF Configuration for Three-Tier Infrastructure:

1. Web ACL Details:

- **Name:** ProdWebACL
- **Associated AWS Resources:** Load Balancer named "three-tier-web-lb".

Describe web ACL and associate it to AWS resources

Info

Web ACL details

Name

ProdWebACL

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Description - optional

The description can have 1-256 characters.

CloudWatch metric name

ProdWebACL

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Resource type

Choose the type of resource to associate with this web ACL.

☐ Amazon CloudFront distributions

☒ Regional resources (Application Load Balancers, Amazon API Gateway REST APIs, Amazon App Runner services, AWS AppSync GraphQL APIs, Amazon Cognito user pools and AWS Verified Access Instances)

Region

Choose the AWS region to create this web ACL in.

US East (Ohio)

Associated AWS resources - optional (1)

Remove

Add AWS resources

Find associated AWS resources

< 1 > ⚙






<input type="checkbox"/>	Name	Resource type	Region
<input type="checkbox"/>	three-tier-web-lb	Application Load Balancer	US East (Ohio)

Rule Groups Configuration:

- **Selection Reasoning:** Free rules were chosen due to this being an independent study.
- **Rule Groups:**
 - **Admin Protection:** Helps prevent unauthorized administrative access.
 - **SQL Database:** Since the database employed is SQL-based, this rule ensures protection against SQL-related vulnerabilities.
 - **Linux Operating System:** As the EC2 instances are Linux-based, this rule group offers relevant protection measures.
 - **Known Bad Inputs:** Protects against known malicious input patterns.
 - **Anonymous IP List:** Blocks access from IP addresses that prefer to remain anonymous, adding an extra layer of security.

Free rule groups

You can use the free rule groups without any added charges beyond the standard service charges for AWS WAF. [AWS WAF Pricing](#) 

Name	Capacity	Action
Admin protection Contains rules that allow you to block external access to exposed admin pages. This may be useful if you are running third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application. Learn More 	100	<input checked="" type="radio"/> Add to web ACL Edit
SQL database Contains rules that allow you to block request patterns associated with exploitation of SQL databases, like SQL injection attacks. This can help prevent remote injection of unauthorized queries. Learn More 	240	<input checked="" type="radio"/> Add to web ACL Edit
Linux operating system Contains rules that block request patterns associated with exploitation of vulnerabilities specific to Linux, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which the attacker should not have had access. Learn More 	200	<input checked="" type="radio"/> Add to web ACL Edit
Known bad inputs Contains rules that allow you to block request patterns that are known to be invalid and are associated with exploitation or discovery of vulnerabilities. This can help reduce the risk of a malicious actor discovering a vulnerable application. Learn More 	200	<input checked="" type="radio"/> Add to web ACL Edit
Anonymous IP list This group contains rules that allow you to block requests from services that allow obfuscation of viewer identity. This can include request originating from VPN, proxies, Tor nodes, and hosting providers. This is useful if you want to filter out viewers that may be trying to hide their identity from your application. Learn More 	50	<input checked="" type="radio"/> Add to web ACL Edit

Rule Priority Setup in Web ACL:

The Web ACL's rule priority determines the order in which rules are evaluated. A request is evaluated against the rule with the highest priority (lowest number) first. From the provided screenshot, the rule priorities are as follows:

1. Admin Protection Rule:

- **Rule Name:** AWS-AWSManagedRulesAdminProtectionRuleSet

Aimed at safeguarding administrative interfaces and endpoints.

2. Anonymous IP List Rule:

- **Rule Name:** AWS-AWSManagedRulesAnonymousIpList

Designed to block requests from anonymous IP sources such as VPNs and Tor browsers.

3. Known Bad Inputs Rule:

- **Rule Name:** AWS-AWSManagedRulesKnownBadInputsRuleSet

Blocks requests with suspicious patterns commonly used in malicious inputs.

4. Linux OS Rule:

- **Rule Name:** AWS-AWSManagedRulesLinuxRuleSet

Protects against threats specific to Linux operating systems.

5. SQL Rule:

- **Rule Name:** AWS-AWSManagedRulesSQLiRuleSet

Protects the SQL-based database by identifying and blocking common SQL injection patterns.

Create web ACL

Set rule priority [Info](#)

Rules (5) ▲ Move up ▼ Move down

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

	Name	Capacity	Action
<input type="radio"/>	AWS-AWSManagedRulesAdminProtectionRuleSet	100	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesAnonymousIpList	50	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesKnownBadInputsRuleSet	200	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesLinuxRuleSet	200	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesSQLiRuleSet	240	Use rule actions

Cancel Previous Next

Web ACL Creation & Association:

- **Created Web ACL:** The Web ACL named "ProdWebACL" was successfully created.
- **Association:** The aforementioned Web ACL was successfully associated with the Load Balancer "three-tier-web-lb".

[AWS WAF](#) > Web ACLs

Web ACLs [Info](#)

Web ACLs (1/1) US East (Ohio) ▼ Copy ARN Delete Create web ACL

Web ACLs that you have defined in the selected region.

< 1 > ⚙️

	Name ▲	Description ▼	ID
<input checked="" type="radio"/>	ProdWebACL	-	185ebc27-88fa-44ed-bdea-334cb46aed01

✓ **Success**
Successfully associated web ACL with three-tier-web-lb. ✕

[AWS WAF](#) > [Web ACLs](#) > ProdWebACL

ProdWebACL Download web ACL as JSON

< Overview Rules Bot Control **Associated AWS resources** Custom response bodies Logging >

Associated AWS resources (1) Disassociate Add AWS resources

< 1 > ⚙️

<input type="checkbox"/>	Name	Resource type	Region
<input type="checkbox"/>	three-tier-web-lb	Application Load Balancer	US East (Ohio)

Analysis of ProdWebACL Traffic Inspection:

- **Traffic Spike:** Around "02:40 UTC," there's a noticeable increase in traffic. This spike was intentionally generated by me for testing purposes.
- **Blocked Requests:** Concurrently with this traffic surge, the WAF blocked 4 requests based on the *Anonymous IP List Rule*. These blocked requests suggest potential access attempts from anonymous sources like VPNs or Tor browsers.
- **Conclusion:** This test confirms the WAF's effectiveness in identifying and mitigating potentially suspicious activity. Regular monitoring and periodic testing are vital for maintaining a secure infrastructure.

