AWS Web ApplicationFirewall (WAF)

Protect Your Web Applications from Common Exploits and Attacks

WHAT IS AWS WAF?

- Managed web application firewall service
- Protects web applications from common threats
- Works with Amazon CloudFront, API Gateway, and ALB

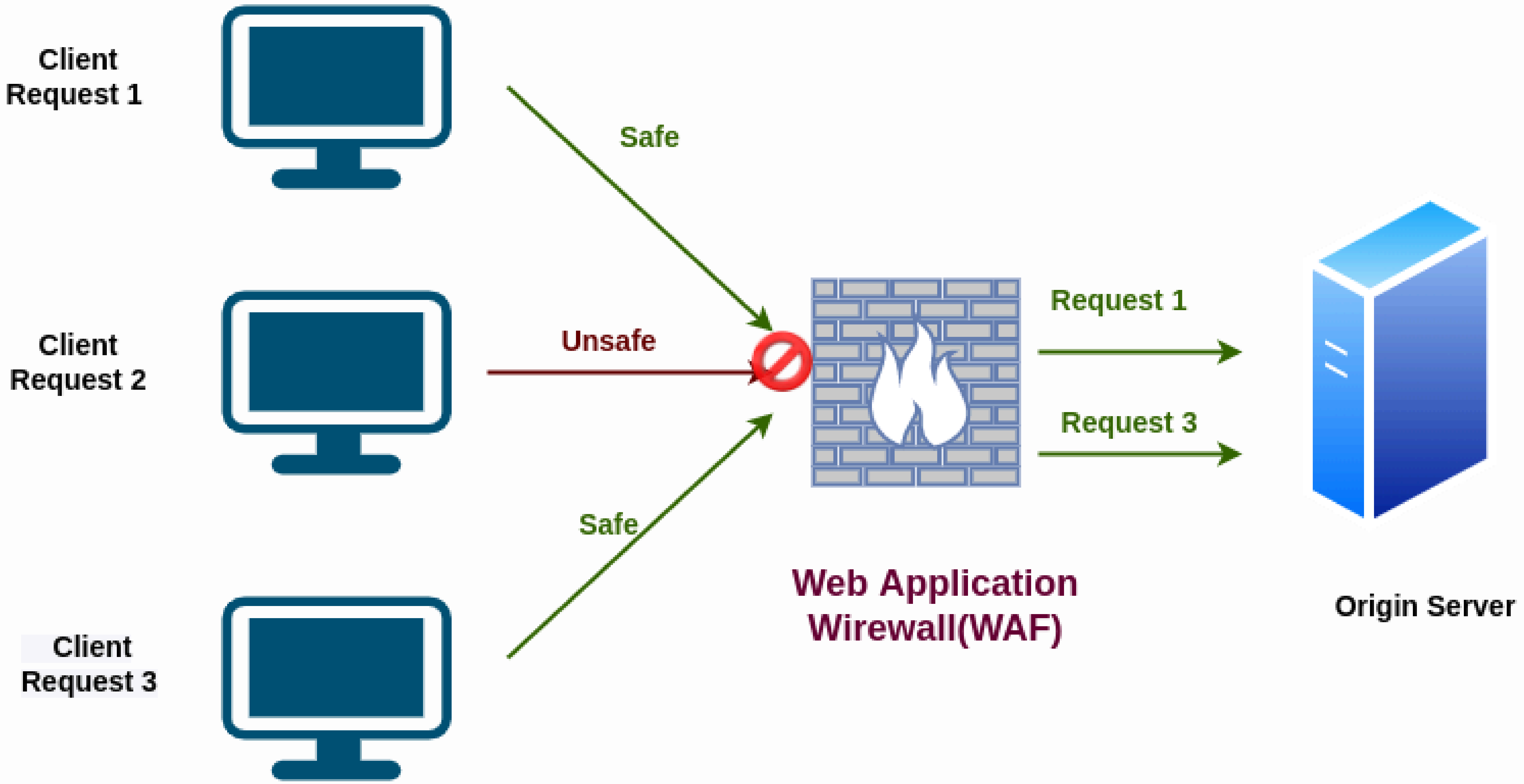
KEY FEATURES

- Web traffic filtering
- Protects against SQL injection, XSS
- Rate-based rules
- Real-time monitoring & logging
- Customizable security rules

BENEFITS

- Easy to deploy and manage
-
- Scalable protection
- Cost-effective (pay-as-you-go)
- Integrates with AWS Shield for DDoS protection

How AWS WAF Works?



Use Cases

- Protect APIs and web applications
-
- Prevent OWASP Top 10 threats
-
- Rate limiting for abusive bots
-
- Real-time attack monitoring

Example Rules in WAF

- SQL injection match rule
- XSS match rule
- IP address whitelist/blacklist
- Rate limit rules

WAF Pricing

NUMBER OF WEB ACLS

NUMBER OF RULES PER ACL

NUMBER OF REQUESTS INSPECTED

Best Practices

- Use managed rule groups.
- Enable logging with Amazon Kinesis.
- Regularly review rule sets.
- Integrate with AWS Shield for layered protection.

Conclusion

- AWS WAF simplifies web application security
- Scalable, customizable, and pay-as-you-go
- Strong protection against modern web threats