AWS WAF

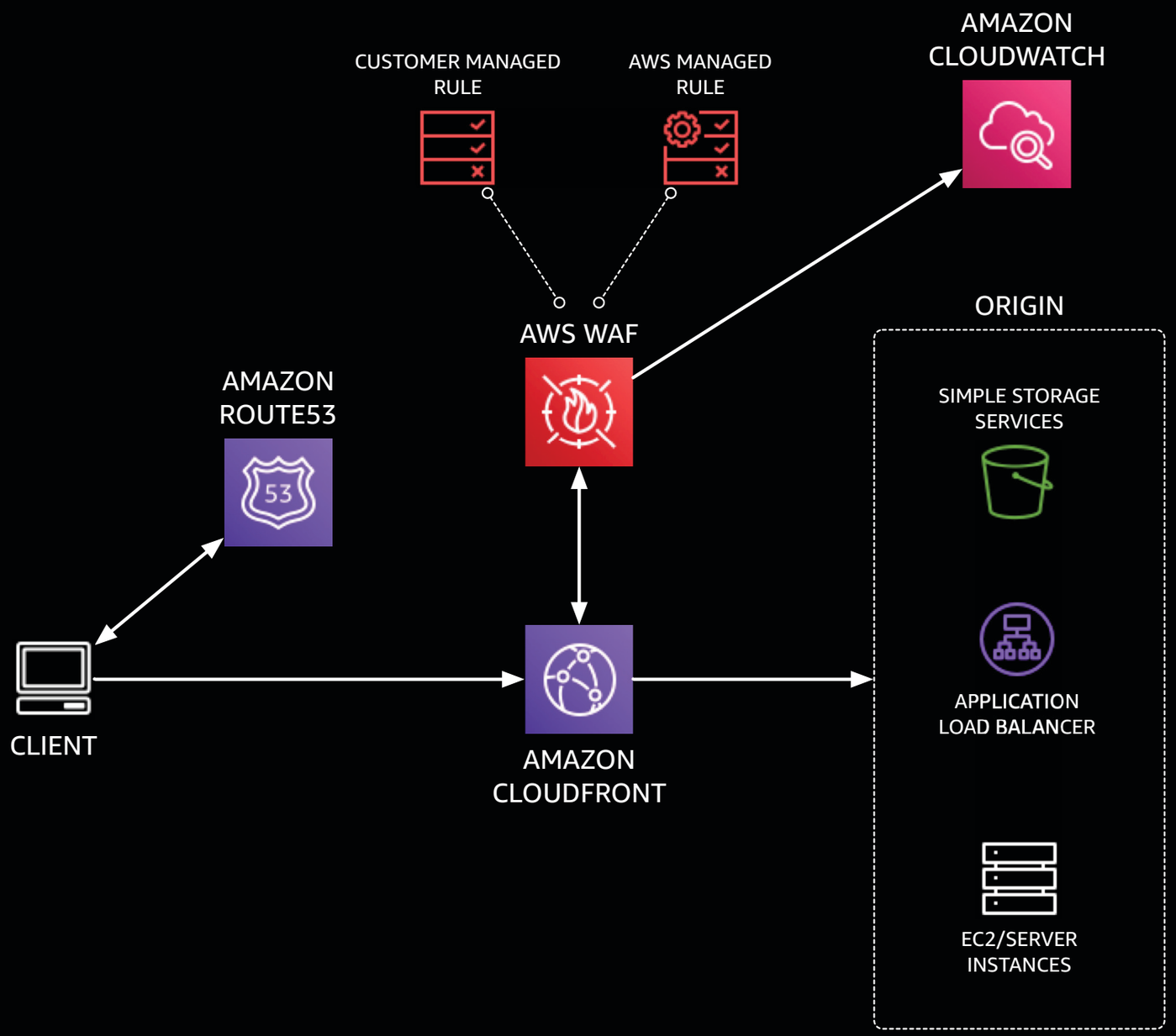
A BEST PRACTICES CHECKLIST

Combine managed and custom rule groups: Managed rule groups offer pre-built rules that defend against widespread threats. For example, the Amazon IP reputation list, a part of the AWS Managed Rules, contains IP addresses associated with malicious activities. Custom rule groups enable you to craft rules specific to your requirements. Subscribe to third-party managed rule sets from AWS Marketplace.

Apply rate limiting: Implement rate limiting rules to shield your web applications from Denial of Service (DoS) attacks or brute force attempts - configure rate limits based on requests per IP address or user agent within a specific time frame.

Turn on logging and monitoring: Enable AWS WAF logging to record request and response data. Integrate logs with monitoring tools like Amazon CloudWatch or AWS Security Hub to assess performance, detect potential threats, and stay updated on WAF activities.

Use count mode for initial deployment: Deploy WAF to production using “count mode” initially, which records the number of web requests your rules would block without blocking them. This approach allows you to gauge the impact of your rules before fully implementing them.



Integrate AWS services for added security: Incorporate AWS WAF with other AWS security services, such as Amazon GuardDuty, AWS Shield, and Amazon Inspector, to establish a comprehensive security ecosystem. Combining these services can strengthen your overall security stance and better protect your applications and infrastructure.

Evaluate your WAF configuration: Test WAF rules in a staging environment before deploying them to production during a low-activity period to ensure their effectiveness. Use tools like AWS WAF Security Automation or third-party testing services to simulate attacks on your web applications and gauge your WAF configuration. Modify your rules based on the vulnerabilities found during testing.

Perform post-deployment assessments: Regularly evaluate WAF even after activating your rules to determine if it blocks legitimate traffic. Then, adjust rules as needed to maintain the effectiveness of your WAF protection.