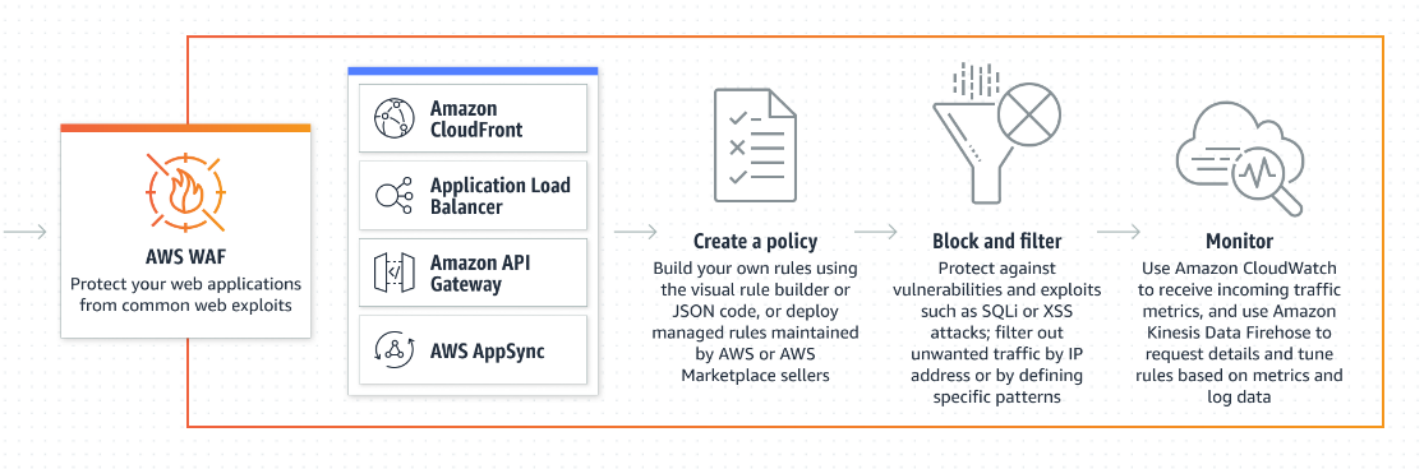
Web Application Firewall (WAF) Overview:

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.

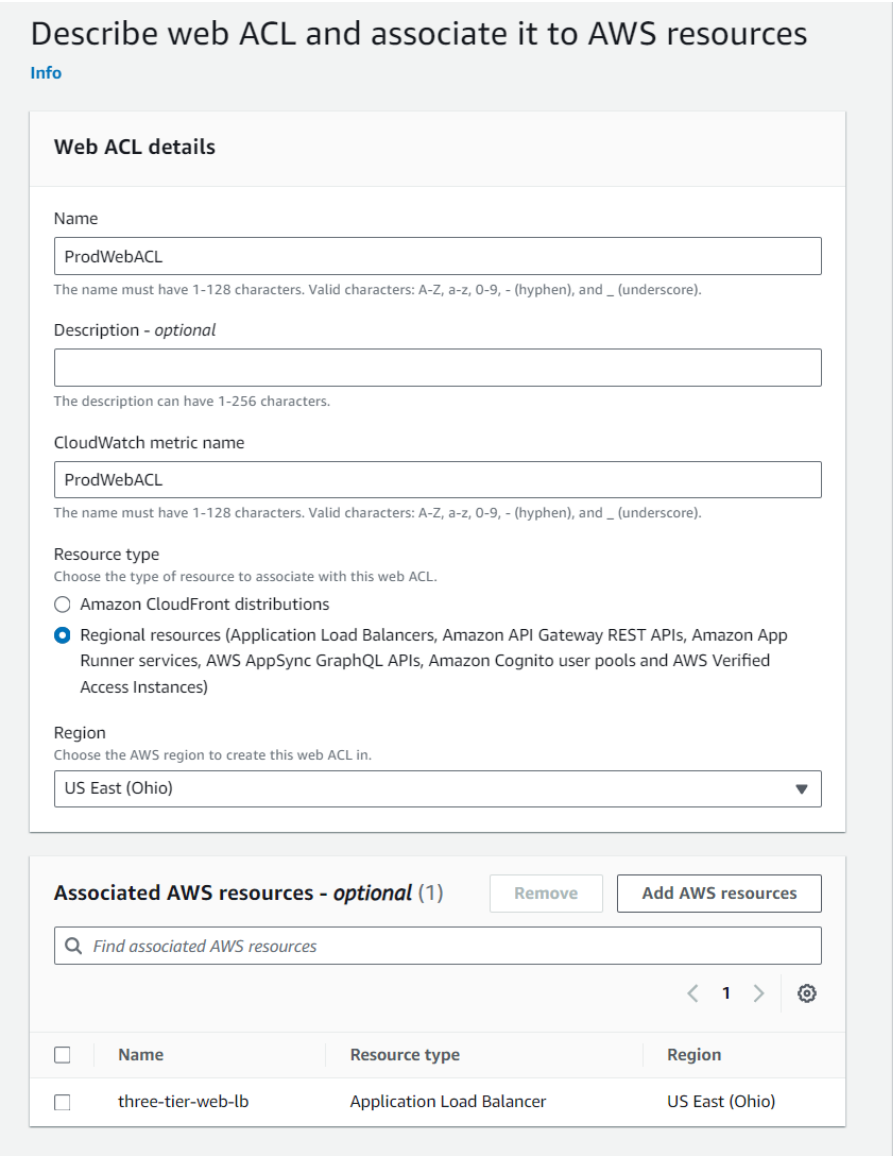
Benefits of WAF:

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.



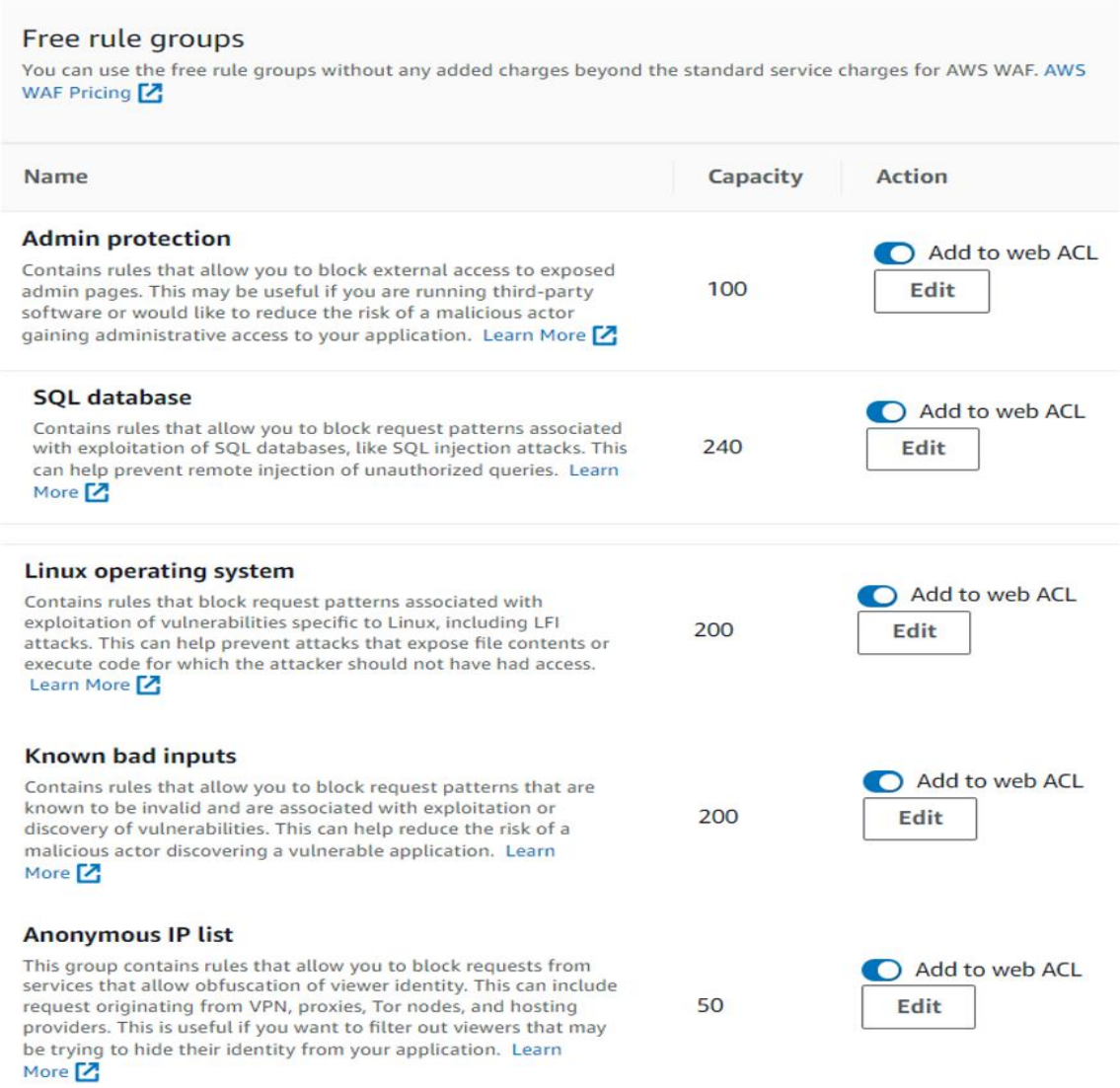
WAF Configuration for Three-Tier Infrastructure:

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



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.



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

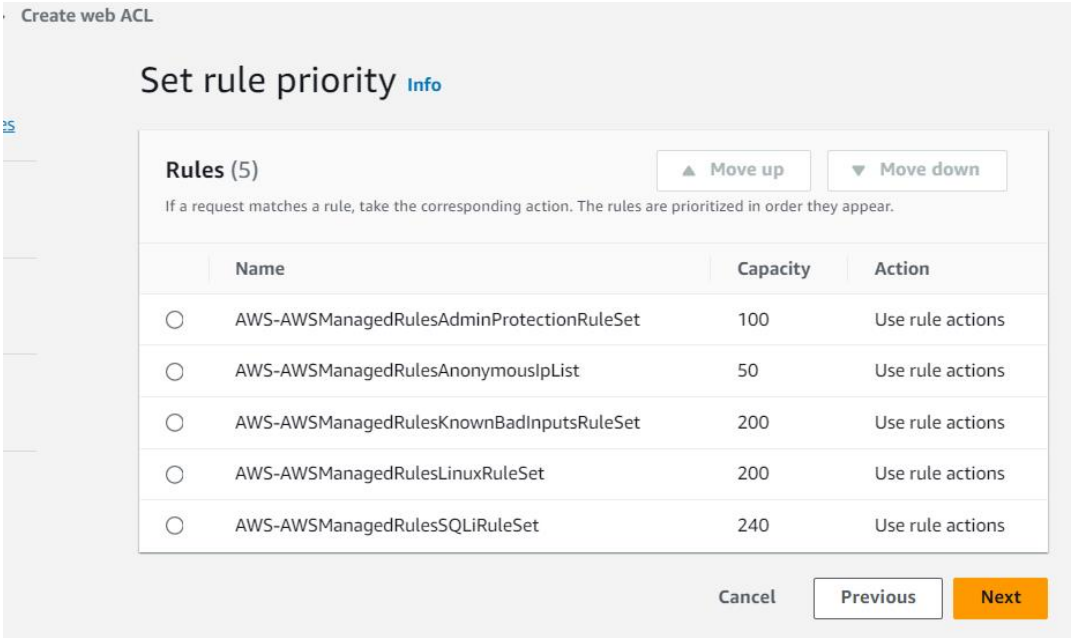
Blocks requests with suspicious patterns commonly used in malicious inputs.

4. **Linux OS Rule:**
    - **Rule Name:** AWS-AWSManagedRulesLinuxRuleSet

Protects against threats specific to Linux operating systems.

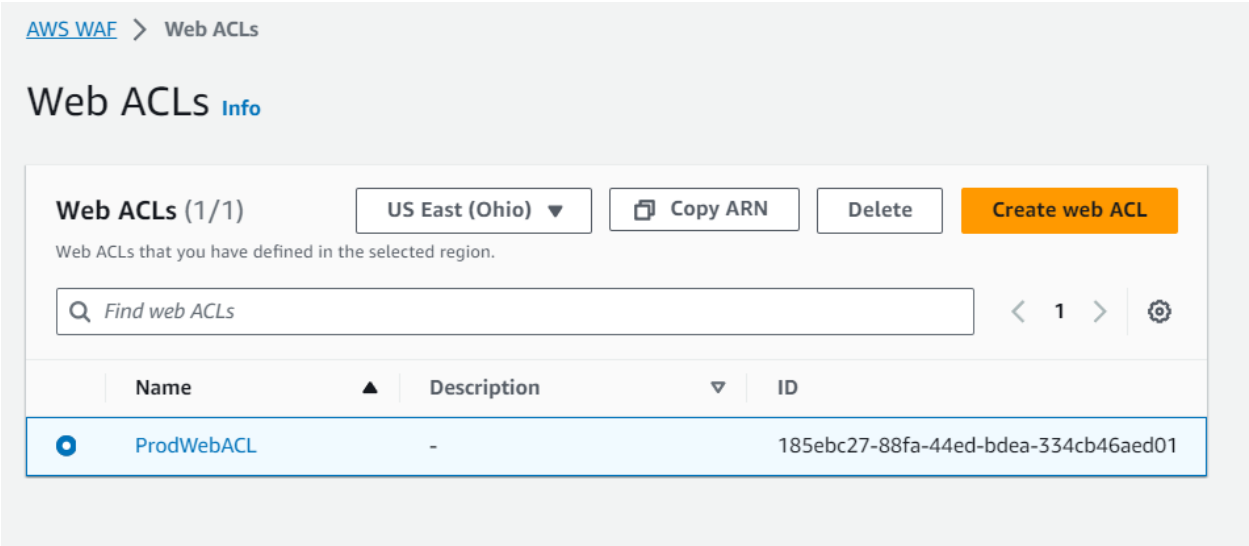
5. **SQL Rule:**
    - **Rule Name:** AWS-AWSManagedRulesSQLiRuleSet

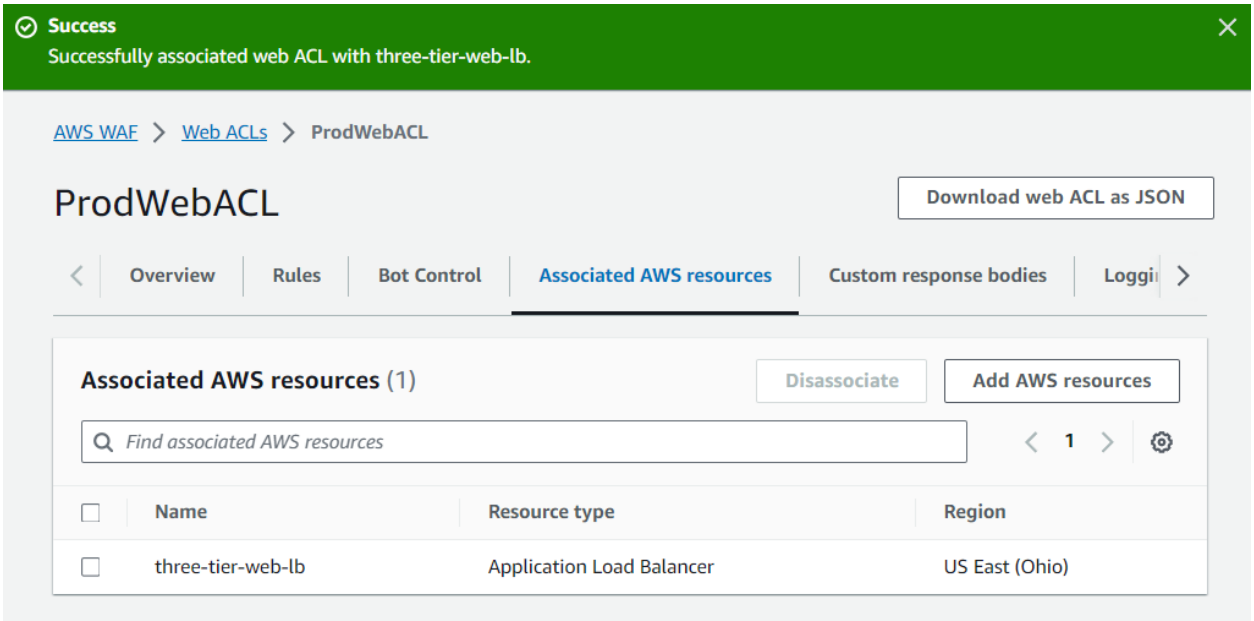
Protects the SQL-based database by identifying and blocking common SQL injection patterns.



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".





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.