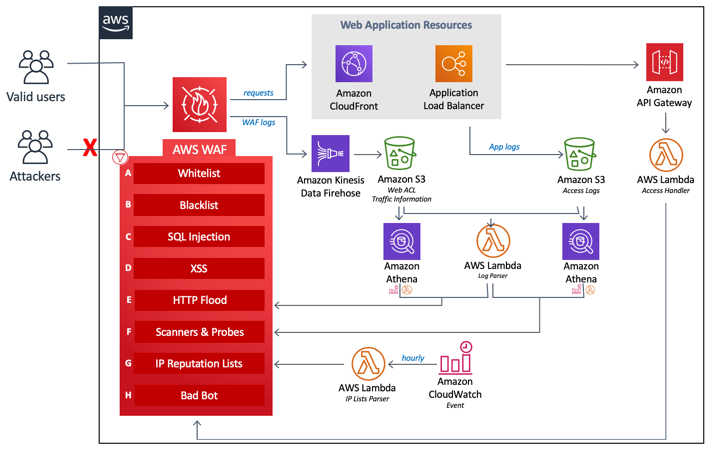
AWS WAF (you can secure your web application using waf)

AWS WAF is amazon web firewall that enables customers to quickly create custom ,application specific rules that block common attack patterns that can affect application availability ,compromise security or consumes excessive resources

AWS WAF can be completely administered by APIs which makes security automation easy , enabling rapid rules propagation and fast incident response .

The AWS WAF Security Automations solution provides fine-grained control over the requests attempting to access your web application.



**AWS WAF Security Automations solution architecture**

**Manual IP lists (A and B):** This component creates two specific AWS WAF rules that allow you to manually insert IP addresses that you want to block (blacklist) or allow (whitelist).

**SQL Injection (C) and XSS (D):** The solution configures two native AWS WAF rules that are designed to protect against common SQL injection or cross-site scripting (XSS) patterns in the URI, query string, or body of a request.

**HTTP flood (E):** This component protects against attacks that consist of a large number of requests from a particular IP address, such as a web-layer DDoS attack or a brute-force login attempt.

**Scanners and Probes (F):** This component parses application access logs searching for suspicious behavior, such as an abnormal amount of errors generated by an origin. It then blocks those suspicious source IP addresses for a customer-defined period of time.

**IP Reputation Lists (G):** This component is the IP Lists Parser AWS Lambda function which checks third-party IP reputation lists hourly for new ranges to block.

**Bad Bots (H):** This component automatically sets up a honeypot, which is a security mechanism intended to lure and deflect an attempted attack.