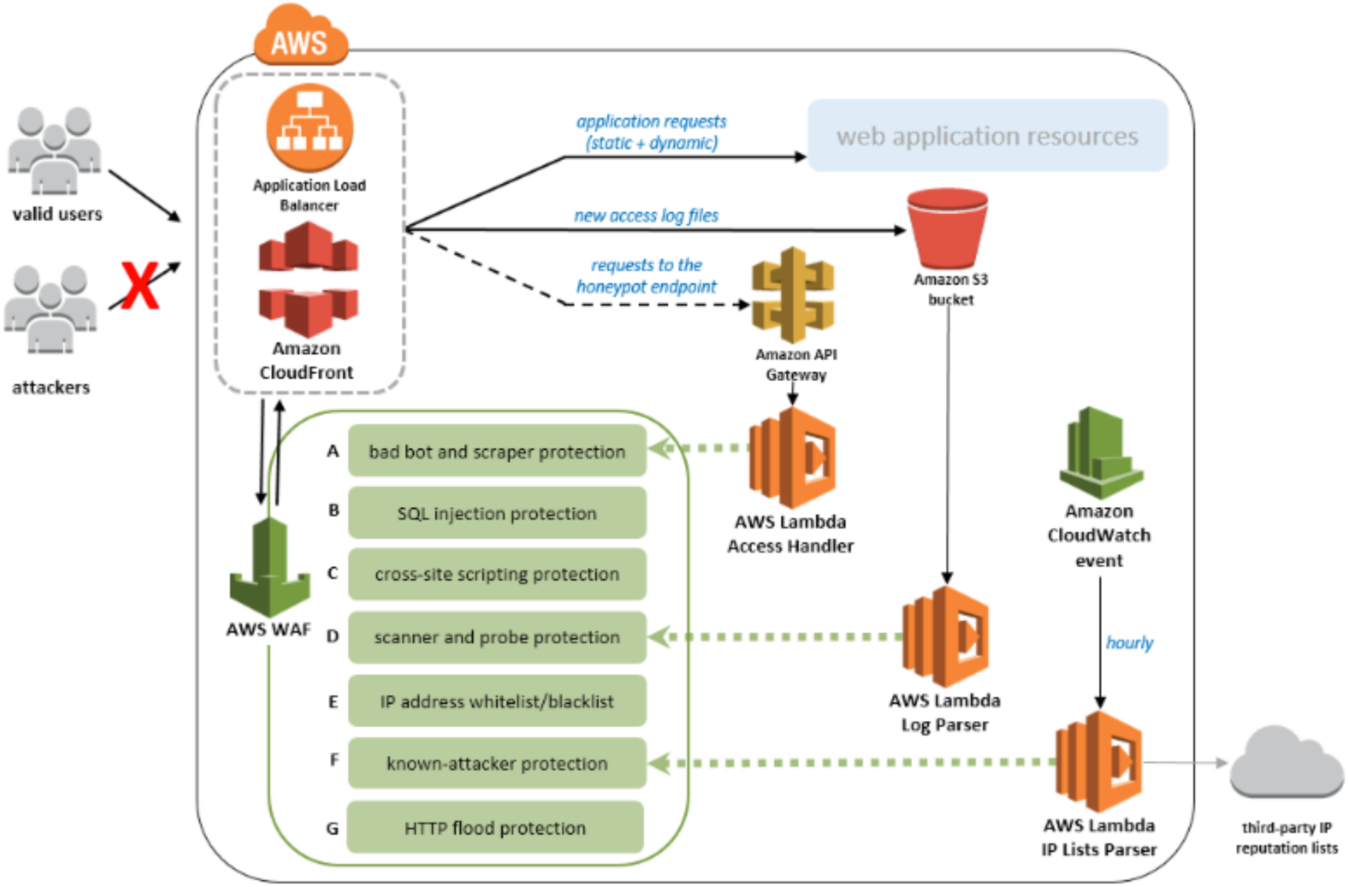
AWS
valid users
attackers
X
Application Load Balancer
Amazon CloudFront
application requests (static + dynamic)
web application resources
new access log files
Amazon S3 bucket
requests to the honeypot endpoint
Amazon API Gateway
AWS WAF
A bad bot and scraper protection
B SQL injection protection
C cross-site scripting protection
D scanner and probe protection
E IP address whitelist/blacklist
F known-attacker protection
G HTTP flood protection
AWS Lambda Access Handler
AWS Lambda Log Parser
Amazon CloudWatch event
hourly
AWS Lambda IP Lists Parser
third-party IP reputation lists

- **Honeypot (A):** This component creates a honeypot to lure and deflect content scrapers and bad bots. A discrete API Gateway endpoint (embedded in the web application) triggers a custom AWS Lambda function, which intercepts the suspicious request and adds the source IP address to the AWS WAF block list.

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

- **Log parsing (D):** A custom AWS Lambda function automatically parses access logs to identify suspicious behavior and add the corresponding source IP addresses to an AWS WAF block list.

- **Manual IP lists (E):** 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).

- **IP-list parsing (F):** A custom AWS Lambda function automatically checks third-party IP reputation lists hourly for malicious IP addresses to add to an AWS WAF block list.

- **HTTP flood protection (G):** This component configures a rate-based rule that automatically blocks web requests from a client once they exceed a configurable threshold.