AWS DDoS Testing – Strengthening a Bank's Protection

RED BUTTON
DDoS Experts

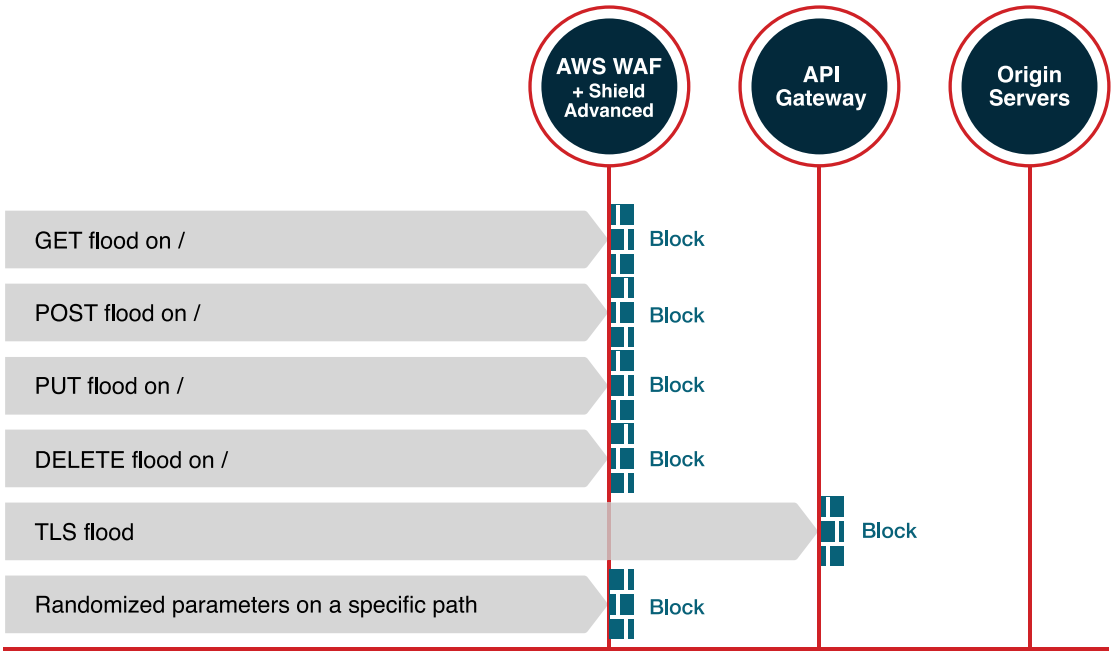
BACKGROUND

The Central American bank, which operates in several countries, wanted to test the DDoS protection status of its IT infrastructure, hosted on Amazon Web Services. While the bank was using the AWS Shield Advanced service, it wanted to validate its configurations and ability to mitigate application-level DDoS attacks. Specifically, the Central American Bank was interested in testing one of its mobile applications that is published to the internet via AWS API Gateway.

AWS Shield Advanced was configured with L7 DDoS auto-mitigation enabled, and was integrated with several application load balancers, Route 53, CloudFront distributions, and Elastic IP addresses.

THE SOLUTION

The Red Button team planned a DDoS attack simulation consisting of six application-level attack vectors. Our objective was to test how different types of HTTPS floods would be detected and mitigated.



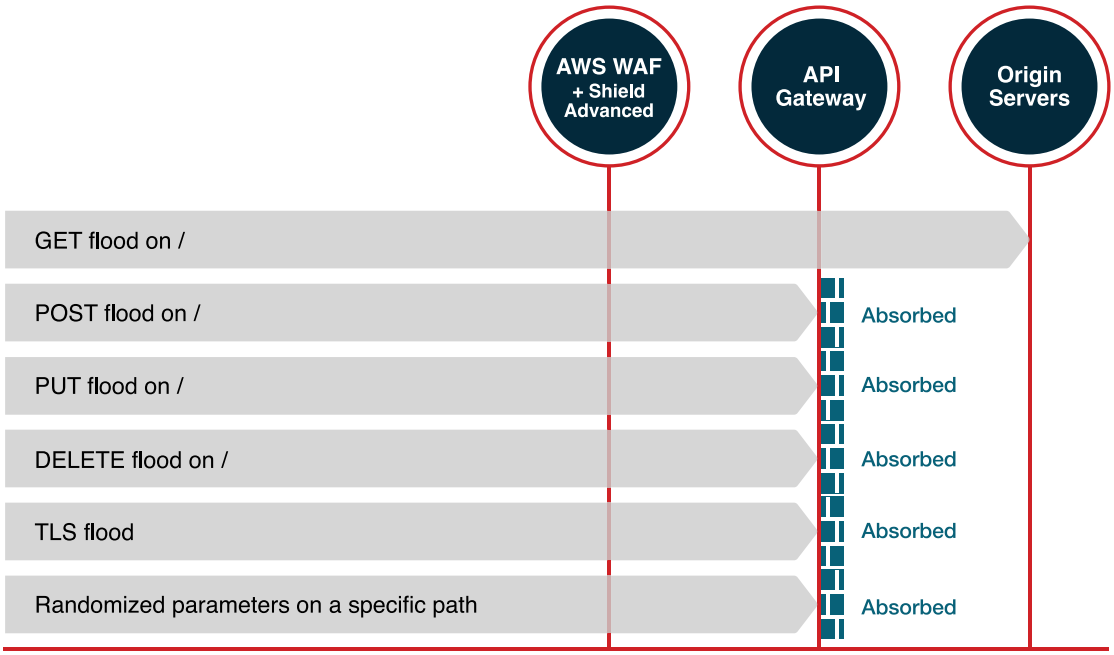
Attack vector analysis plan: Indicating which component should stop each attack vector.

Our expectation was for:

- **AWS Shield Advanced** Layer 7 Automatic Mitigation to detect anomalies and perform auto-mitigation; namely, to create a new rate-limit-based rule in the defined WEB ACL.
- **The API Gateway,** which is responsible for publishing the mobile-application API and for the TLS termination process, to absorb attacks that utilize the TLS flood mechanism.

We did not expect the **Web Application Firewall (WAF)** to block any of the simulated attacks, since it was not configured with any relevant rules.

Test Results



Attack vector analysis: Actual results.

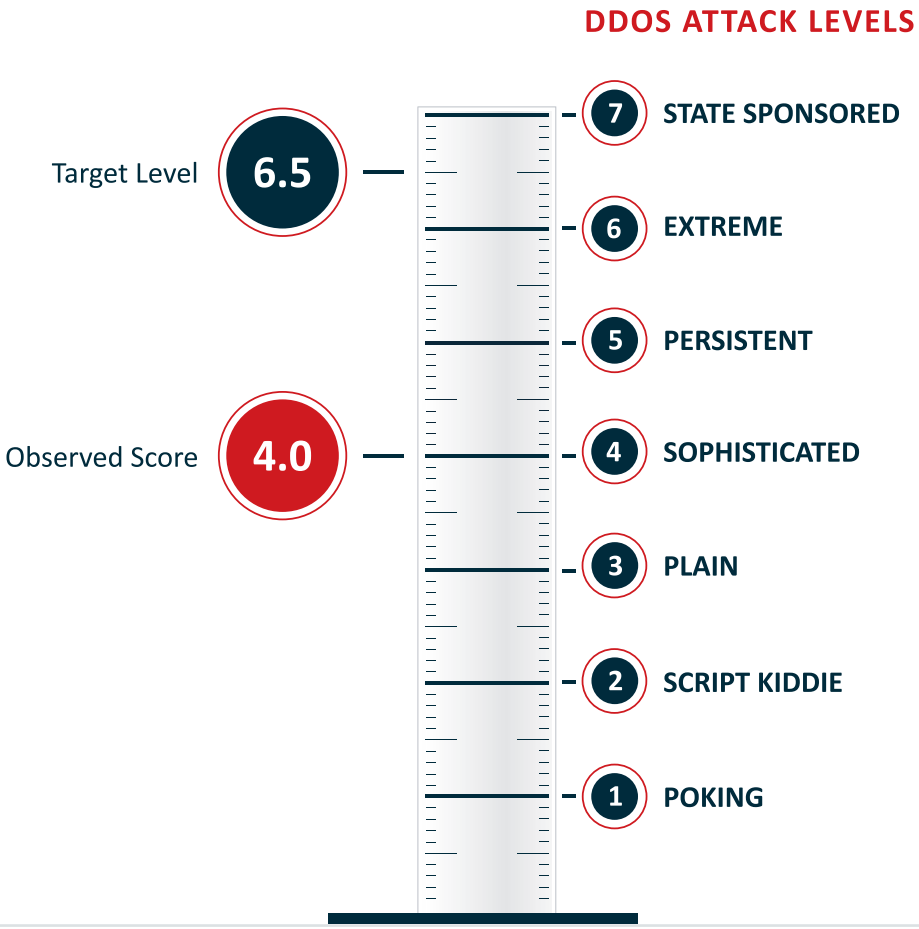
Unexpectedly, all attacks succeeded in bypassing the AWS Shield Advanced protection layer. This was due to an improper configuration of the API Gateway (using Regional API Gateway without CloudFront), which completely disabled the intended protection from AWS Shield Advanced.

Most attacks were absorbed by the API Gateway. This, however, was only due to the low attack rates used. If we were to increase traffic rates, the attacks would have bypassed the Gateway and reached the origin servers. The simulated GET flood attack, a common applicative DDoS attack, bypassed all protection layers and took down the service. This was because it used a valid API request, unlike the other attacks.

DDoS Resiliency Score

Upon completion of DDoS testing, we provide customers a detailed report that includes a DDoS Resiliency Score (DRS) – a numeric value clearly indicating the type of attacks the system can currently withstand and more severe attacks that it cannot.

The DRS score of the Central American Bank was calculated as 4.0, compared to a recommended score (based on the threat level common in the banking industry) of 6.5.



Recommendations

Following testing, we provided several recommendations to strengthen protection:

Architecture

The top recommendation was to deploy CloudFront in front of the API Gateway to protect it with the Shield Advanced automatic mitigation service for application layer DDoS attacks.

WAF Configuration

Create a rate-limit-based rule to help detect and mitigate a large number of DDoS attacks scenarios.

Automation

Implement the Scanners and Probes protection component to automatically detect and block traffic from specific IPs that receive repeated error response codes and are unlikely to be legitimate human users.