Protecting a Gaming Company Against DDoS Attacks on AWS

RED BUTTON
DDoS Experts

BACKGROUND

As one of the world's most popular online gaming companies, the company is a prime target for DDoS attacks.

Previously, the gaming company operated its own data centre, where it implemented extensive DDoS protection mechanisms with the help of Red Button. For various reasons, the company moved its data centre to Amazon Web Services (AWS).

THE CHALLENGE

The move to the cloud required a complete restructuring of the DDoS defence. The company's security team wanted to ensure its DDoS protection on AWS was at the same top level as the previous, on-premises data centre.

AWS provides two DDoS protection services: **AWS Shield** Standard (a free service) and AWS Shield Advanced, a paid service with additional detection and mitigation capabilities. While the company clearly needed the advanced protection service, it was still not enough.

Achieving first-rate protection with full visibility, alerts, and an extensive defence against all types of attacks requires customer-specific setup, configuration, and fine-tuning.

THE SOLUTION

Our DDoS expert team started with a thorough analysis of the company's serverless system architecture to assess the full scope of DDoS vulnerabilities. Next, the following activities were implemented.

Network-Level Attack Mitigation

Preliminary analysis, which was later backed up in testing, indicated that AWS can block network attacks in both the AWS CloudFront (its CDN service) and the AWS ALB (its load-balancing service).

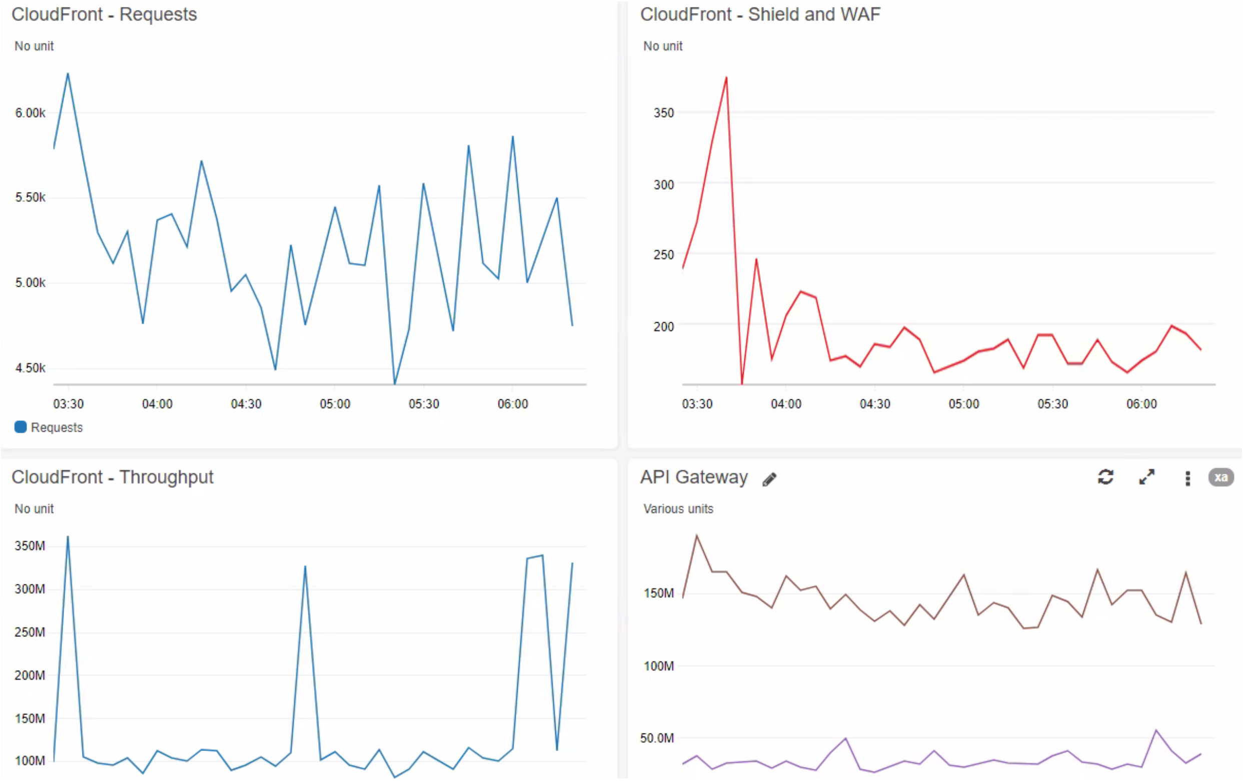
Application-Level Attack Mitigation

The first defence line against application-level attacks was created by defining rate limit rules in AWS WAF (Web Application Firewall). Additional setup and configuration steps were implemented to handle 'under-the-radar' types of attacks, with small attack rates by each bot. To protect against web application attacks, additional AWS Managed rules were added, such as Core rule set (CRS), Admin protection rules, Known bad inputs rules, SQLi rules, and Amazon IP reputation list.

Real-Time Attack Visibility

An essential objective was to provide security and NOC personnel with real-time visibility to inbound traffic volume and its effect so that they could assess whether a DDoS attack was taking place. This was achieved by building a dedicated dashboard in CloudWatch (AWS monitoring solution), with multiple widgets, each presenting different metrics.

For example, the CloudFront Distribution widgets related to *Inbound Requests per Second* and *Error Response Rate* enable assessing whether an applicative DDoS attack is taking place, while the *Cache Hit Rate* widget enables evaluating the degree to which the Caching mechanism blocks the attack.



Any spike in these dashboards can indicate a DDoS attack. The security officer can understand the layers in which the attack takes place, the nature of the attack (network or application), and whether or not it is mitigated.

Automatic DDoS Detection

Using specific CloudWatch alarms, we implemented DDoS detection capabilities, providing notifications about issues such as a high number of requests per second, a high byte upload rate, or a large number of errors.

DDoS Attack Analysis

Next, we developed tools to provide insight into a potential attack. Using the external Kibana software, we created visualization dashboards that identify the attacked hostname or URL, query and payload parameters in HTTP requests, IP addresses of attacking bots, attack rates, and originating countries.

DDoS Testing

We executed DDoS tests to evaluate all the DDoS detection and mitigation capabilities, including the rules and threshold levels defined. We launched multiple application-level attacks.

Procedures and Training

Beyond technology, DDoS mitigation depends on the human factor. As our last step, we created a DDoS playbook containing written procedures for the NOC and Security teams and an eLearning kit for new NOC members.