# Big 4 Accounting Firm Improves DDoS Protection with Simulation Testing

RED BUTTON
DDoS Experts

## BACKGROUND

Organizations in the field of accounting face one of the highest percentages of DDoS attack traffic out of total industry traffic. One of the “Big Four” global accounting firms wanted to verify its ability to mitigate a DDoS attack on its online assets.

The company turned to Red Button for help. Together, the firm and Red Button decided to design, plan and carry out attack simulations that would act as realistic stress tests for the kind of DDoS campaigns seen in the industry.

## THE FIRST DDOS SIMULATIONS

The accounting firm uses the Azure DDoS Protection Plan, as well as the Azure WAF integrated into the Application Gateway. The Protection Plan is meant to defend the network layer against attack, while the Azure WAF is designed to protect the application layer.

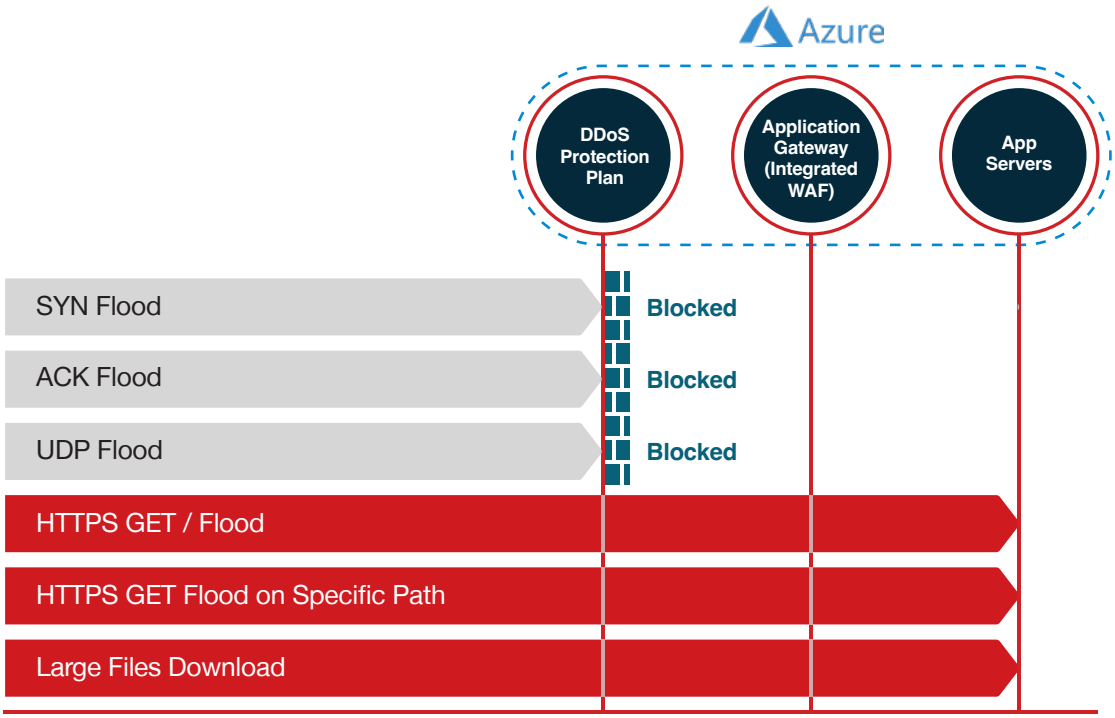
Therefore, Red Button built a series of six DDoS attack simulations - three targeting the network layer and three targeting the application layer.

| Attack Category | DDoS Attack Vector | Maximum Rate |
|---|---|---|
| Network Layer | SYN Flood | 750K RPS |
| | ACK Flood | 750K RPS |
| | UDP Flood | 3.5 Gbps |
| Application Layer | HTTPS GET / Flood | 10K RPS |
| | HTTPS GET Flood on Specific Path | 20K RPS |
| | Large File Download | 6 Gbps |

### The Results: A Failing Grade

All the network layer attacks were detected successfully and mitigated by the Azure DDoS Protection Plan.

However, none of the application layer attacks were even detected, much less mitigated. The result was a denial of service each time. Both the HTTPS GET attacks caused downtime on the servers until the attacks were terminated, while the Large File Download attack consumed server resources without interruption for about 10 minutes.




**DDoS Attack Simulation Results**

The simulation test revealed that the DDoS Resiliency Score (DRS) of the accounting firm, which reflects its ability to withstand DDoS attacks, was a mere 1.5. That is far lower than the 5.5 score Red Button recommends for organizations in the financial industry.

The next obvious question was: What can be done about it?

## Recommendations

Following testing, we provided several recommendations that would make the accounting firm a harder target for attackers by strengthening DDoS protection:

### CDN Deployment

Our top recommendation was to deploy the Azure Front Door CDN service to improve the protection against application layer DDoS attacks. Azure Front Door supports an Azure WAF service with additional DDoS protections, such as rate-limiting and geo-filtering.

### WAF Configuration

Configuring custom rate-limit rules on Azure WAF is an effective means of layer 7 DDoS attack mitigation.

**Follow-Up DDoS Testing**

Once the basic recommended DDoS protection improvements are applied, additional attack simulations should be carried out with a focus on the application layer.

## DDOS SIMULATION TESTING – ROUND 2

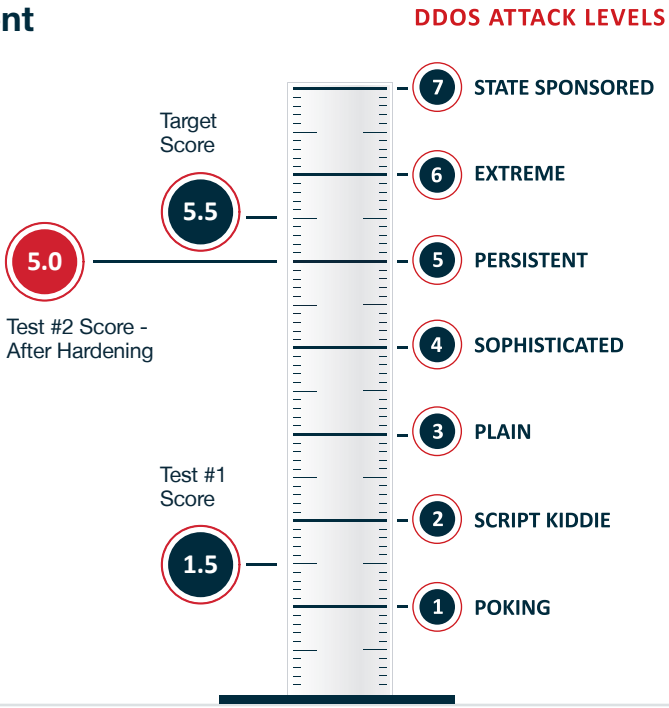
The accounting firm quickly implemented the Red Button recommendations, including requesting a second set of follow-up DDOS simulations.

In order to test the effectiveness of the changes implemented, Red Button set up and ran six application layer attack scenarios. The three attacks that were not stopped in the first round of testing served as a baseline for marking improvement and were repeated. Then, three more advanced attack scenarios were added for additional penetration testing.

### The Results: Massive Improvement

Out of the six attack vectors, five were mitigated thanks to the new rate-limit rules defined in the WAF. One attack, which was supposed to be stopped by the Front Door caching, failed due to a misconfiguration of the caching-related headers in the origin server.

The results were crystal clear – the recommended measures worked. As a result, the accounting firm's DRS score shot up to 5.0, which is very close to the recommended industry-specific score of 5.5.




### Recommendations

Following the second set of attack simulations, Red Button offered the accounting firm several additional recommendations for further hardening its DDoS defenses, including:

**Fine-tuning rate-limit rules in the Azure WAF** in accordance with the organization's baseline traffic; and

**Configuring the caching headers in the origin server** to enable caching static content, ensuring it is delivered from the Front Door CDN.