ALEF

F5 Distributed Cloud Bot Defense

OVERVIEW

Our customer publishes its business-critical applications in two ways:

- it has a web GUI that external customers can access
- additionally, it provides public APIs to their B2B partners.

They faced some issues caused by automated traffic, so they were searching for a solution that was able to identify and eliminate bot-generated requests in a reliable way.

CHALLENGE

Our customer identified the following issues caused by automated traffic:

1. Because they have several public-facing entry points their attack surface is really wide.
2. Although they use WAF they experienced it cannot protect their application against sophisticated, automated, fraudulent attacks.
3. They have a Business Analyst Department that is gathering access statistics and based on that tuning their GUI, Business Logic and portfolio. They need to go deep in data trying to filter automated traffic making a mess in statistics and generating unreliable data.
4. Their existing WAF solution has already reached the limit of its filtering capacity although they would only use half of the performance if they did not need to analyze the automated traffic.

SOLUTION

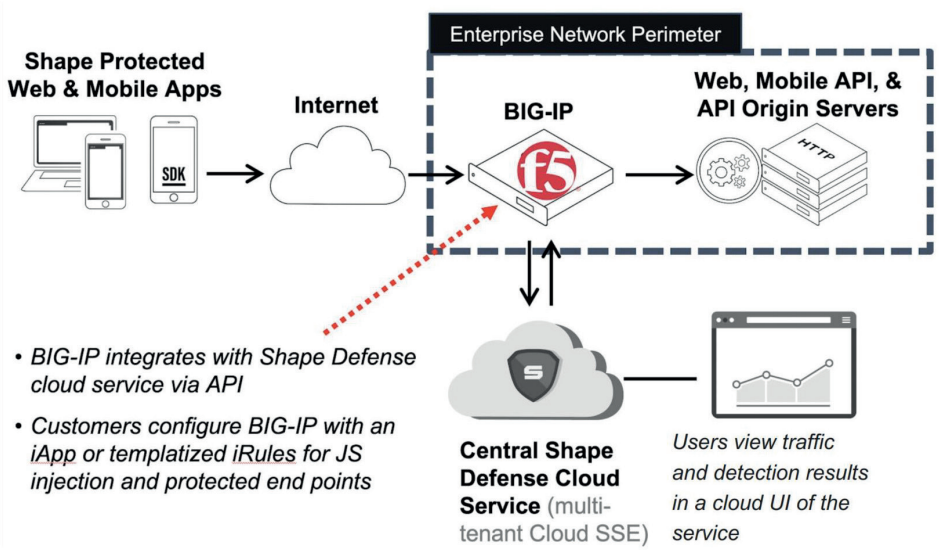
Our customer decided to use F5 Advanced WAF together with F5 Distributed Cloud Bot Defense to solve all the challenges.

Thanks to the professionalism of our Value-Added Partner our customer totally learned the wide range of features that they can reach using F5 portfolio. Considering the investment protection and broad future expandability they purchased an HA pair of rSeries, the new generation of the standalone F5 platforms. Having F5 Advanced WAF on the new device they can protect their applications on advanced level with the possibility of detailed configuration, fully automated deployments, great visibility and reporting, good understanding of attacks and application-level DoS protection.

To utilize F5 Distributed Cloud Bot Defense our customer needed to have a proxy between their users and application servers. F5 Advanced WAF works exactly in the required mode, additionally, it provides native integration within BIG-IP software. Thanks to this integrated solution it was just a matter of minutes to deploy their new managed cloud-based Bot Defense solution.

Trust the Strong

ALEF Distribution SK, s. r. o. | Galvaniho 17/C, 821 04 Bratislava
Slovenská republika | Phone: +421 (2) 4920 3888
sk-sales@alef.com | www.alef.com



F5 Distributed Cloud Bot Defense

F5 Distributed Cloud Bot Defense or formerly known Shape Integrated Bot Defense (IBD) protects your web properties from automated attacks by identifying and mitigating malicious bots. IBD uses JavaScript and API calls to collect telemetry and mitigate malicious users without re-routing traffic through a proxy server.

IBD is a standalone solution that integrates with existing components in your infrastructure. The integration process is simplified with an integration module that F5 provides, and you deploy and configure. Once IBD is integrated with your environment, you can view and filter traffic and transactions to see which users are malicious and how they're being mitigated.

RESULT

Our customer has successfully deployed F5 Advanced WAF combined with F5 Distributed Cloud Bot Defense. With this they now have a full-scale protection in front of their business critical, public-facing applications. They can mitigate all the unwanted automated traffic, so now they can trust and use the access statistics. Additionally, they experienced a dramatic decrease in loads throughout the whole app infrastructure (including app servers, WAF and others).

On top of their original needs our customer learned about the free offering from F5 called Device ID+ that is a real-time device identifier that utilizes advanced signal collection and proven machine-learning algorithms to assign a unique identifier to each device visiting your site. It is using exactly the same mechanism that F5 Distributed Cloud Bot Defense but with the unique identifier it provides our customer is now able to specialize offerings and messages to its users and to decrease the need of authenticating users again and again, thus providing a frictionless user experience to them.

ADDITIONAL RESOURCES

- Advanced Web Application Firewall (WAF) | F5
- Distributed Cloud Bot Defense | F5
- Building a Fraud Profile with Device ID+ (Part 1: Set Up & Demo) - YouTube
- Building a Fraud Profile with Device ID+ (Part 2: Analytics & Reporting) - YouTube
- F5 Device ID+ - NGINX

Trust the Strong

ALEF Distribution SK, s. r. o. | Galvaniho 17/C, 821 04 Bratislava
Slovenská republika | Phone: +421 (2) 4920 3888
sk-sales@alef.com | www.alef.com