The Integration of Cloudflare WAF

FERMILAB-POSTER-24-0156-SQMS

Ethan Blum, University of South Alabama, Under the Mentorship of Yesenia Gonzalez and Jeny Teheran
Security and Emergency Management Division, Cybersecurity Team, Fermi National Accelerator Laboratory, Batavia, Illinois 60510

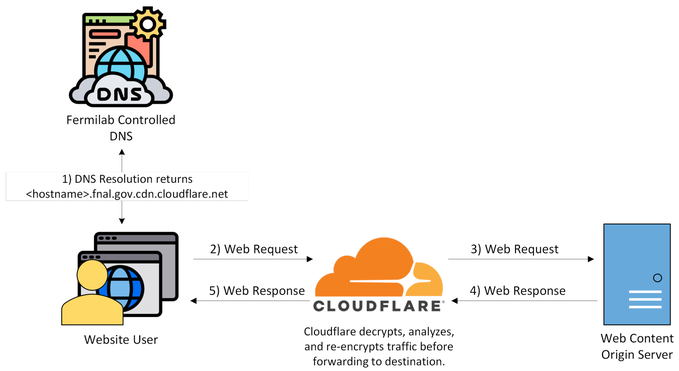
Background

HTTP Strict Transport Security (HSTS) is a standard that ensures website visitor's traffic is always sent using HTTPS ensuring that all traffic is protected during transit. This initiative was adopted in 2012 by the IETF and has grown in popularity all around the world. Because the traffic is encrypted with TLS/SSL, it can be used by attackers to bypass various cybersecurity capabilities such as a site firewall. To address this lack of visibility into encrypted traffic in motion, the CST at Fermilab acquired the Cloudflare Web Application Firewall (WAF). To help in the implementation and integration of the Cloudflare WAF, I was directed to learn about and aid in this process. This has been a profound learning experience into the on-goings of project management, web application firewalls, collaboration, and networking.

Cloudflare WAF

A WAF (Web Application Firewall) is a reverse proxy firewall that inspects network packets using a rule base or ruleset to analyze layer 7 web application traffic, analyzing HTTP and HTTPS traffic, and filters out malicious traffic by decrypting, analyzing, and alerting on or blocking the traffic.

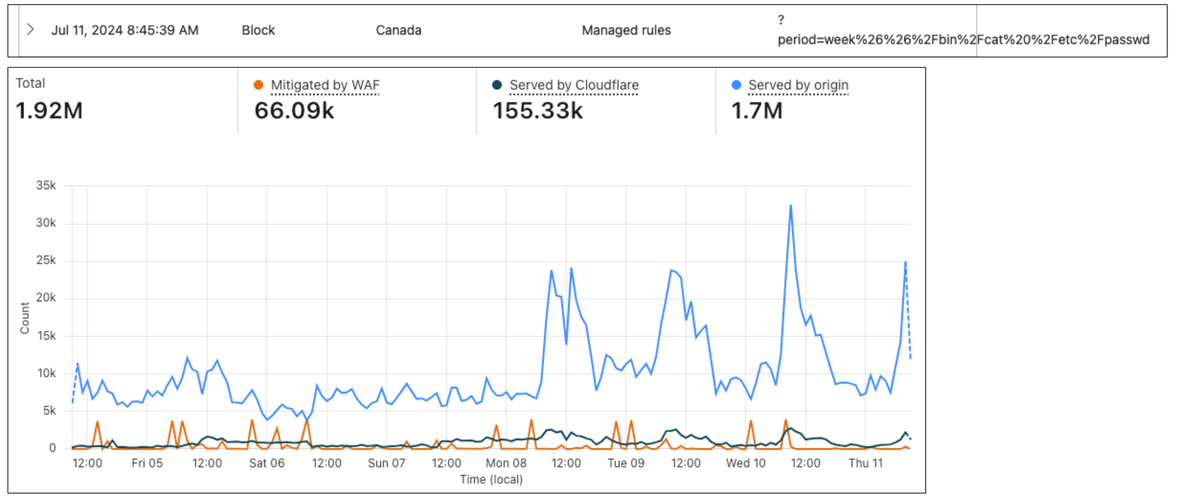
Cloudflare Flow



Onboarding Process

The onboarding process for new websites at Fermilab follows a predictable pattern that allows for transparency and efficiency. So far, we have onboarded two websites into Cloudflare, with plans to add many more in the future. This part of the project was the most impactful because it allowed me to work closely with website owners, other technology teams across Fermilab, and directly with the Cloudflare technical team. It gave me insight into IT and cybersecurity project management.

Current Website Analytics



These stats show all the web traffic we now have visibility into for the 2 onboarded sites. Benign traffic is shown in light and dark blow, and malicious traffic blocked by Cloudflare is noted in orange. This graph shows that, in the period of 1 week, over 1 million requests were made in total. That is over 1 million requests that Cloudflare inspected and took an action on, with malicious traffic never reaching the website server.

Lessons Learned

This project has taught me a lot about managing major projects, spanning many months. I have also learned a lot about networking and the inner workings of a reverse proxy. I can better understand web traffic and the adversarial misuse websites face, and what can be done to help mitigate those attempts/attacks.

This research was supported in part by the U.S. Department of Energy Omni Technology Alliance Program, administered by the Oak Ridge Institute for Science and Education.

This work was produced by Fermi Research Alliance, LLC under Contract No. DE-AC02-07CH11359 with the U.S. Department of Energy. Publisher acknowledges the U.S. Government license to provide public access under the DOE Public Access Plan.