What are WAFs and WAAPs?

Overview

A traditional firewall typically serves as the first line of defense in a network's fight against malicious visitors. These firewalls focus on the Network and Transport layers, layers 3 and 4 in the OSI model, meaning they are unable to interpret and process HTTP and HTTPS traffic, which is the type of traffic making requests to your web applications.

In order to protect your websites, web applications and APIs, you would want to use a web application firewall (WAF), as these exist to help filter out the "good" and "bad" HTTP and HTTPS traffic at the Application layer, layer 7, in the OSI model.

A WAF sits in between the client and origin server, meaning that any request a client makes would pass through the WAF for an "inspection" first, before arriving at its destination, the website's origin server.

What is a WAAP

A WAAP (Web Application and API Protection) is a security tool that offers the basic protection of a WAF in addition to more advanced measures aimed to protect your web applications and APIs from modern-day cyberattack methods.

StackPath's security platform offers the following core features of a WAAP:

- Next-gen WAF
- Bot protection
- API protection
- API Discovery
- DDoS mitigation

As these malicious attacks continue to evolve and become more sophisticated, our WAF will continue to undergo upgrades and maintenance needed to keep our platform up-to-date and effective against these attacks.

How StackPath's WAF Works

A WAF works by taking incoming requests and performing checks on them, to determine whether or not they are safe. These checks are performed using rule sets, and with the StackPath WAF, we provide both pre-defined rule sets and the ability to create custom ones.

The StackPath WAF is a cloud-based next-gen WAF that uses a two part system to perform these checks. These two parts are the WAF edge nodes that perform actions against requests

and a cloud intelligence component that runs heuristics and ML models and performs behavioral analytics.

WAF edge nodes and behavioral components work together to provide protection against common vulnerabilities such as L7 DDoS attacks, OWASP Top 10 threats, bots and more.

WAF Edge Nodes

WAF edge nodes are responsible for running rule sets against requests. They will also perform actions against the requests(block, allow or monitor) based on the recommendation provided by the second part, the behavioral component. The existence of nodes that run rule sets against traffic is what essentially defines a typical first-gen WAF.

The WAF Policies Explained section in our Help Center explains the various default rule sets (policies) our WAF provides. Our WAF Rules article explains the ways you can create custom rule sets to filter traffic as you desire.

Behavioral Component

The behavioral component is centralized and is responsible for analyzing the traffic coming from the WAF edge nodes asynchronously. This component then takes its analysis and instructs the edge nodes to either block, allow or monitor a request. This analytical part of the system in combination with the fact that these two parts are independent of each other are what helps take our WAF to the next-gen level.

Bot Protection

When someone mentions the term "bot" in regards to website security, both "good" and "bad" bots should be considered.

Good bots can exist for various reasons, such as to crawl websites for search engines, provide automated customer support via chatbots or engage in social media activity. Bad bots usually exist to perform malicous business logic attacks to gain access to your system and accomplish tasks such as scraping, inventory attacks or even DDoS attacks.

The StackPath WAF offers sets of pre-defined policies that filter bot traffic which allow the "good" ones and block the "bad" ones.

For more information, please see our Enabling and Troubleshooting Bot Protection article.

L7 DDoS Protection

The StackPath WAF offers protection for your web applications, websites and APIs from DDoS attacks at the application layer, layer 7, in the OSI model. Protection is offered using multiple

techniques and is always active regardless of the status of your WAF (Monitor vs Protect). Once a DDoS attack is identified, a multilayer approach is taken to mitigate it for the minimum duration of 10 minutes or until the attack has ended.

For more information, please see our L7 DDoS Protection article.

API Discovery

API Discovery is a WAF feature that provides automatic detection of potential APIs and is an overall simpler way to manage your API protection.

This feature has the ability to "do the work for you" by scanning your site for potential API endpoints, where you can then determine whether or not they need additional protection.

For more information, please see our API Discovery article.

Related Documentation

If you would like to add WAF protection to a website that's already integrated with StackPath's CDN, please see Setting up a WAF Instance on an Existing Site.

Otherwise, please see Setting up a WAF Instance on a New Site.