ModSecurity WAF for Kong API server running on top of Nginx

Overview:

Kong is one of the most popular open source Microservice API Gateway which manages the communication between clients and microservices via API. It’s a Lua application running in Nginx and made possible by the lua-nginx-module.

A great tool for securing Nginx-based applications is ModSecurity, used by over a million sites around the world. It protects against a broad range of Layer 7 attacks, such as SQL injection (SQLi), local file inclusion (LFI), and cross‑site scripting (XSS), which together accounted for 95% of known Layer 7 attacks in Q1 2017, according to Akamai. Best of all, ModSecurity is open source.

This documentation illustrates the implementation of ModSecurity WAF system on our Kong API Gateway server which runs on the top of Nginx server, so the installation is done basically on Nginx itself with some modifications on the Kong-Nginx configuration files.

Implementation steps:

1. Compiling and Installing ModSecurity for NGINX by Building the Docker Image.
2. Save the docker image file and push the image into Gitlab repo.
3. Update the task definition and start a new Amazon ECS service.
4. Load ModSecurity commercial rules into Kong server.
5. Test the rules functionality.
6. **Compiling and Installing ModSecurity for NGINX by Building the Docker Image:**

As long as our Kong API system is running on version 0.14.1, so we will build our image based on the below options so it can be compatible with the Cassandra database:

* Ubuntu Bionic 18.04
* Kong 0.14.1
* OpenResty (Nginx + LuaJIT) 1.13.6.2
* ModSecurity 3.0

Below are the installation steps which are done in the Dockerfile in order:

1. Install Kong version 0.14.1 on Ubuntu 18.04:

The Docker image is based on Ubuntu 18.04 and Kong 0.14.1 as shown below:



1. Install Prerequisite Packages:

The next step is to install the packages required to complete the remaining steps. Run the following command, which is appropriate for a freshly installed Ubuntu system:



1. Download and Compile the ModSecurity 3.0 Source Code:

With the required prerequisite packages installed, the next step is to compile ModSecurity as an NGINX dynamic module. In ModSecurity 3.0’s new modular architecture, libmodsecurity is the core component which includes all rules and functionality. The second main component in the architecture is a connector that links libmodsecurity to the web server it is running with. There are separate connectors for NGINX, Apache HTTP Server, and IIS. We cover the NGINX connector in the next section.