Monitoring and Troubleshooting Coraza WAF

For users deploying Coraza WAF in production environments, **monitoring and troubleshooting** are essential for ensuring optimal security and performance.

Monitoring WAF Logs

Coraza's WAF rules can be monitored through log files. Logs can be directed to standard output (`/dev/stdout`) to view in real time, or you can configure log files for long-term monitoring.

To monitor logs, ensure you have the following settings in your `dynamic.toml`:

```
[http.middlewares]
  [http.middlewares.coraza-waf-logging.plugin.coraza]
    directives = [
      "SecDebugLog /dev/stdout",
      "SecDebugLogLevel 9"
    ]
```

Use `docker logs` to view the WAF activity logs:

```
docker logs $(docker ps -qf name=traefik)
```

Performance Considerations

Introducing a WAF may add latency to your application due to the extra processing required to inspect HTTP requests. To monitor performance, you can use tools like Prometheus and Grafana to gather metrics on request processing time and WAF performance.

Troubleshooting Issues

When troubleshooting WAF-related issues:

- Check the **debug logs** for detailed information on blocked requests.
- Use **whitelisting** techniques to avoid false positives. For example, you can disable specific rules for known safe traffic by using the `SecRuleRemoveById` directive.

Revision #1
Created 13 October 2024 15:26:52 by aeoneros
Updated 13 October 2024 15:28:44 by aeoneros