

Reverse Proxy con capacidades de Firewall de aplicación web y aceleración TLS

Alumno: Pedro Pozuelo Rodríguez
Directora: Ana del Valle Corrales Paredes

Universidad Europea
Proyecto de Fin de Grado

18 de julio de 2019



**Universidad
Europea**

LAUREATE INTERNATIONAL UNIVERSITIES

Agenda

- Introducción:
 - Aplicaciones web y la seguridad.
 - Mecanismos de protección.
- Situación actual. Estado del arte:
 - Soluciones WAF privativas.
 - Soluciones WAF de software libre.
 - Comparativa soluciones actuales.
- Solución.
 - Objetivo.
 - Diseño.
 - Arquitectura.
- Conclusiones.
- Test y resultados.



Reverse Proxy + WAF + aceleración TLS

1 Introducción

- Aplicaciones web y la seguridad
- Mecanismos de protección
- Aplicaciones web y la seguridad

2 Estado del arte

- Soluciones WAF privativas
- Soluciones WAF de software libre
- Comparativa soluciones WAF

3 Solucion

- Objetivo
- Diseño
- Arquitectura

4 Tests y resultados

5 Conclusiones



Aplicaciones web y la seguridad

Algunos ejemplos de uso de protocolos HTTP y HTTPS:

- Aplicaciones web.
- Aplicaciones móviles.
- *Internet of things* (IoT): edificios inteligentes, *wearables*, etc.
- Arquitectura de microservicios.
- DNS over HTTPS (DoH [1]).

HTTP + TLS

HTTPS es cada vez más utilizado en todo tipo de aplicaciones y no se limita a las aplicaciones web como venía siendo tradicionalmente.



Aplicaciones web y la seguridad

Premisa

La seguridad 100 % no existe.

Las aplicaciones web están siendo atacadas continuamente.

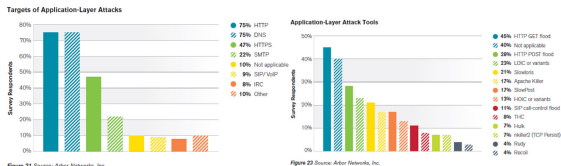


Figura: Ataques en capa de aplicación (fuente Arbor [2])

Conclusión

Se debe realizar un esfuerzo continuo para mejorar la seguridad de las plataformas web.

Vulnerabilidades en plataformas web

Existen múltiples vulnerabilidades en las plataformas web (referencia *Open Web Application Security Project*, OWASP [3]).

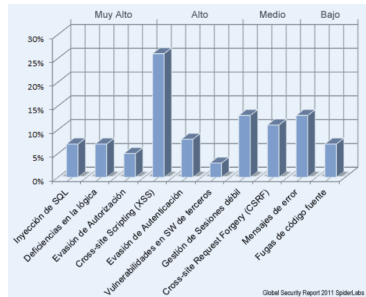


Figura: Tipo de Vulnerabilidades por Impacto [4]

Histórico del riesgo

Muchas de estas vulnerabilidades están presentes en el Top 10 de vulnerabilidades OWASP desde 2007 y existen controles que permiten mitigar el riesgo.



Vulnerabilidades recientes en canales cifrados

Otro componente en el que se han descubierto múltiples vulnerabilidades críticas son los canales SSL/TLS.

| Vulnerabilidad | Componente afectado |
|----------------|---------------------|
| POODLE | SSL ver. 3.0 |
| BEAST | TLS ver. 1.0 |
| CRIME | TLS compression |
| BREACH | HTTP compression |
| Heartbleed | OpenSSL ver. 1.0.1 |

Conclusión

La solución, en la mayoría de de los casos, consiste en desactivar las versiones o el componente afectados y el riesgo de afectar la funcionalidad de la plataforma es bajo (dependiendo del entorno).



Soluciones en el ciclo de desarrollo

Como respuesta a éstas y otras vulnerabilidades existen múltiples soluciones:

- **Desarrollo de código seguro:** metodologías de desarrollo seguro de aplicaciones, herramientas de análisis de código.
Retos:

- Costes en tiempo y recursos
- Conocimiento y herramientas.
- Nuevas vulnerabilidades no están consideradas.

- **Aplicar un ciclo de vida de aplicaciones:** Aplicar actualizaciones y configuración segura de aplicaciones.
Retos:

- El objetivo es que la aplicación dé servicio. Los demás aspectos son secundarios.
- Una actualización puede afectar al entorno.
- *chmod 777* o *iptables -A INPUT -j ACCEPT* funcionan.



Soluciones en la infraestructura

Como respuesta a éstas y otras vulnerabilidades existen múltiples soluciones:

- **Herramientas de protección perimetral de red:** Firewall de red, Sistema de Prevención de Intrusos.

Reto:

- Desconoce la lógica de aplicación. Lógica limitada a las capas 3 y 4 de red o firmas (cadenas de texto).
- Mínima visibilidad con el tráfico cifrado.

- **Herramientas de protección perimetral de aplicación.**

Reto: Elevado coste o complejo de mantener.



Soluciones. Estándares y protocolos

Existen múltiples iniciativas cuyo objetivo es mejorar la seguridad de las aplicaciones web:

- Metodología del Ciclo de Vida de Desarrollo de Software (SDLC del inglés).
- Estándares como el *Payment Card Industry Data Security Standard* (PCI DSS [5]).
- TLS versión 1.3.
- HTTP/2.
- TLS Server Name Indication (SNI [6]).
- Security Headers.

Uso e implementación

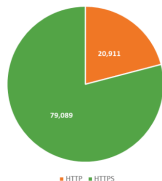
Estas soluciones están disponibles y ofrecen mecanismos válidos para mejorar la seguridad de las plataformas web pero su implementación puede ser compleja.



Uso e implementación

Las alternativas implican un coste elevado, implementar soluciones complejas o aceptar el riesgo de seguridad. Y el resultado es el siguiente:

HTTPS Usage in the Alexa Top 100,000



None TLS 1.3 TLS 1.2 TLS 1.1 TLS 1.0 SSL 3.0 SSL 2.0

| None | TLS 1.3 | TLS 1.2 | TLS 1.1 | TLS 1.0 | SSL 3.0 | SSL 2.0 |
|--------|---------|---------|---------|---------|---------|---------|
| 20,911 | 17,345 | 59,830 | 53 | 2,221 | 5 | 0 |

Figura: Tráfico HTTP versus HTTPS [7]

Figura: Máxima versión SSL/TLS soportada [7]

Uso e implementación

Se ha elegido la versión SSL/TLS como ejemplo de un vector de ataque conocido popularmente cuya mitigación es sencilla.



Visibilidad reducida

Causas: TLS 1.3.

Causas: Diffie–Hellman.

Causas: Autenticación con certificado de cliente.

Consecuencia: Visibilidad muy reducida



Web Application Firewall (WAF)

¿Qué es un WAF?

Definición

Un WAF es una herramienta especializada en filtrar, monitorizar y bloquear las conexiones desde y hacia una aplicación web (Fuente: Instituto Nacional de Ciberseguridad [8]).

Características principales:

- Analiza el tráfico web.
- Listas blancas o negras de User Agents, IP, caracteres aceptados en URL o formularios, etc.
- Se aplican políticas y reglas de filtrado. Por ejemplo:

```
admin'--  
' or 1=1#  
' or 1=1-- --
```

- Modelo de seguridad negativa.
 - Busca patrones de ataques conocidos y bloquea las peticiones o respuestas.
- Modelo de seguridad positiva.
 - Proceso de aprendizaje.
 - Deniega las peticiones por defecto y sólo acepta aquellas que considera válidas.



Reverse Proxy + WAF + aceleración TLS

1 Introducción

- Aplicaciones web y la seguridad
- Mecanismos de protección
- Aplicaciones web y la seguridad

2 Estado del arte

- Soluciones WAF privativas
- Soluciones WAF de software libre
- Comparativa soluciones WAF

3 Solucion

- Objetivo
- Diseño
- Arquitectura

4 Tests y resultados

5 Conclusiones



Soluciones WAF privativas

Destacan las siguientes soluciones:

- **Soluciones WAF SaaS.** Desplegados en las instalaciones del fabricante - o el Cloud - y gestionados por el mismo.
 - *Cloud Web Application Firewall* [9] de Cloudflare[10].
 - *Kona WAF*[11] de Akamai[12].
 - *Incapsula*[13].
- **Soluciones WAF tipo appliance o máquina virtual.**
Máquinas o instancias dedicadas en las que se tiene un acceso exclusivamente a la configuración de la aplicación.
 - *Imperva WAF Gateway*[14].
 - *Fortiweb*[15] de la empresa *Fortinet*[16].



Soluciones WAF privativas SaaS

Las soluciones WAF SaaS ofrecen una serie de funcionalidades adicionales:

- Red de distribución de contenidos (Content Delivery Network del inglés).
- Protección contra ataques de denegación de servicio (DoS del inglés) en capa de aplicación.
- Caché de contenido estático.
- Suscripción a listas de reputación de IP, dominios o Localizador de recursos uniforme (URL del inglés).
- Bloqueo de bots maliciosos.
- Sistema de creación de informes.



Soluciones WAF privativas tipo appliance

Las soluciones WAF de tipo appliance ofrecen a su vez las siguientes funcionalidades adicionales:

- Crear perfiles de las aplicaciones web y filtrar parámetros no permitidos.
- Parcheo virtual de vulnerabilidades mediante la integración con escaneadores de vulnerabilidades.
- Suscripción a listas de reputación de IP, dominios o URL.
- Aceleración TLS.
- Bloqueo de bots maliciosos.
- Sistema de creación de informes.
- Antivirus.



Ventajas e inconvenientes

Ventajas:

- Sencillas de implementar (especialmente en las soluciones SaaS).
- Relativa independencia de la infraestructura de la plataforma web.
- Permite implementar seguridad basada en roles (RBAC del inglés).
- Buen soporte técnico.
- Funcionalidades adicionales.

Desventajas:

- Elevado coste económico.
- No es posible adaptar la solución a necesidades específicas.
- Capacidad muy limitada de crear o modificar reglas (especialmente en las soluciones SaaS).



Soluciones WAF de software libre

Existen múltiples soluciones de software libre

- IronBee[17].
- WebCastellum[18].
- RAPTOR[19].
- NAXSI[20].
- OpenWAF[21].
- FreeWAF[22].
- Shadow Daemon[23].
- AQTRONiX WebKnight[24].
- Vulture[25].
- ModSecurity [26].

ModSecurity

Entre ellas destaca ModSecurity por ser la solución de software libre más extendida y activa de la comunidad e implementa un número significativo de los controles de seguridad deseables en un WAF.



Ventajas e inconvenientes

Ventajas:

- Más económicos.
- Acceso al código fuente y la capacidad de modificarlo.
- (en la mayoría de las soluciones) elimina la dependencia del proveedor.
- Más adaptables a las necesidades de cada entorno.

Desventajas:

- Dependencia de la plataforma web (tradicionalmente un módulo de ésta).
- Más difíciles de implementar y de mantener.
- Proceso de depuración de errores es más complejo.
- Actualización o migración de la plataforma web y el WAF deben realizarse conjuntamente.



Comparativa soluciones

A continuación se muestra un resumen de las características de las distintas soluciones y la solución del presente proyecto:

| Características | WAF SaaS | WAF Appliance | WAF Software libre | Propuesta |
|--|--------------|---------------|--------------------|------------|
| Independencia de la plataforma web | ↑ Muy buena | ↑ Buena | ↓ Mala | ↑ Buena |
| Independencia operacional (RBAC) | ↑ Muy buena | ↑ Buena | ↓ Mala | ↑ Buena |
| Complejidad de despliegue y administración | ↑ Muy baja | ↑ Baja | ↓ Alta | ⇒ Media |
| Coste económico | ↓ Alto | ↓ Alto | ↑ Bajo | ↑ Bajo |
| Soporte técnico | ↑ Bueno | ↑ Bueno | ↓ Limitado | ↓ Limitado |
| Información accesible por terceros | ↓ Sí | ↑ No | ↑ No | ↑ No |
| Adaptabilidad / Personalización | ↓ Muy baja | ↓ Baja | ↑ Alta | ↑ Alta |
| Acceso al código fuente | ↓ No | ↓ No | ↑ Sí | ↑ Sí |
| Funcionalidades adicionales (por defecto) | ↑ Muy buenas | ↑ Buenas | ↓ Limitadas | ↑ Buenas |

Reverse Proxy + WAF + aceleración TLS

1 Introducción

- Aplicaciones web y la seguridad
- Mecanismos de protección
- Aplicaciones web y la seguridad

2 Estado del arte

- Soluciones WAF privativas
- Soluciones WAF de software libre
- Comparativa soluciones WAF

3 Solucion

- Objetivo
- Diseño
- Arquitectura

4 Tests y resultados

5 Conclusiones



Objetivo

Como respuesta a la situación actual, se define el siguiente objetivo:

Objetivo

Construir una solución de software libre con capacidades de WAF y aceleración SSL/TLS, que sea fácilmente desplegable y que minimice el esfuerzo y el impacto que dicha solución tiene sobre la plataforma web actual o futura.

También debe ser fácilmente adaptable a diferentes necesidades y entornos.



Diseño

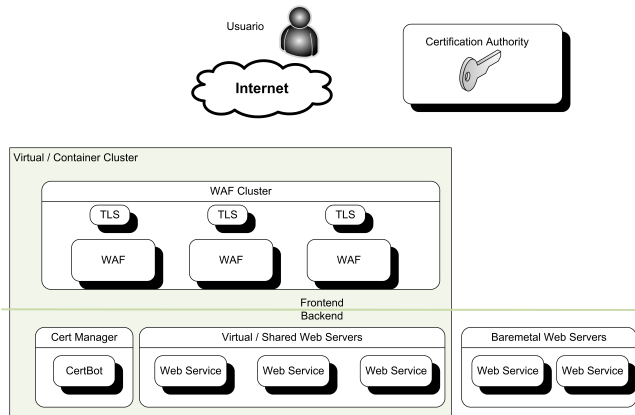


Figura: Diseño a alto nivel de la solución



Componentes

Componentes de la solución:

Web Application Firewall

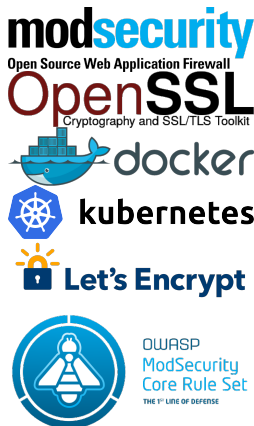
Software criptográfico

virtualización (contenedores)

Automatización y orquestación.

Gestión de certificados.

Políticas y controles de seguridad.



Componentes

Componentes de la solución:

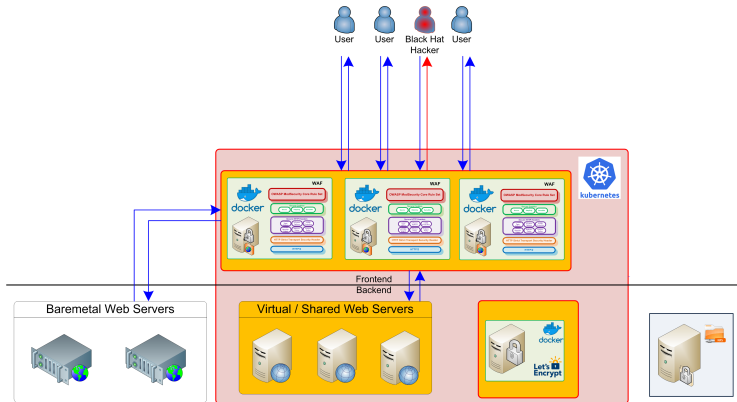
- Web Application Firewall
- Software criptográfico.
- Software de virtualización.
- Software de orquestación.
- Software de aprovisionamiento y gestión de certificados.
- Políticas de auditoría y controles de seguridad.

Componentes externos:

- Servicio DNS.
- Servicio de almacenamiento NFS [27].



Arquitectura



Reverse Proxy + WAF + aceleración TLS

1 Introducción

- Aplicaciones web y la seguridad
- Mecanismos de protección
- Aplicaciones web y la seguridad

2 Estado del arte

- Soluciones WAF privativas
- Soluciones WAF de software libre
- Comparativa soluciones WAF

3 Solucion

- Objetivo
- Diseño
- Arquitectura

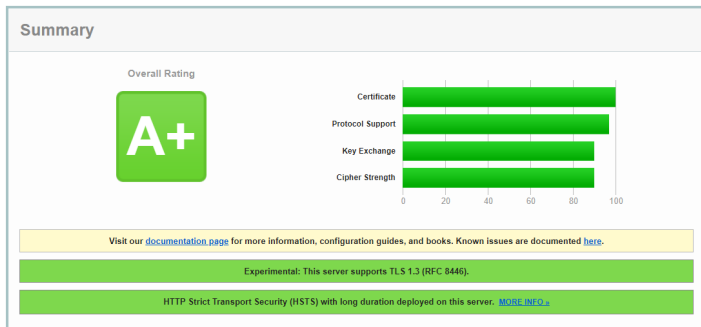
4 Tests y resultados

5 Conclusiones



Resultados TLS

Se ha ejecutado la batería de pruebas proporcionada por Qualys. SSL Labs [28] con el siguiente resultado:




Entre otros, los test ejecutados incluyen: Configuración TLS, vulnerabilidades TLS y configuración de certificados.



Resultados cabeceras HTTP de seguridad

Se ha ejecutado la batería de pruebas proporcionada por Netsparker [29] con el siguiente resultado:

Security Report Summary



| | |
|--------------|--|
| Site: | https://finklinux.ddns.net/ |
| IP Address: | 37.11.104.227 |
| Report Time: | 07 Jul 2019 11:36:06 UTC |
| Headers: | <div><div>✔ Strict-Transport-Security</div><div>✔ X-Content-Type-Options</div><div>✔ X-Frame-Options</div><div>✔ X-XSS-Protection</div><div>✔ Content-Security-Policy</div><div>✔ Referrer-Policy</div><div>✔ Feature-Policy</div></div> |

Entre otros, los test ejecutados incluyen: *HTTP Strict Transport Security*[30, Wikipedia] (HSTS), *X-XSS-Protection*, *Content-Security-Policy* o la reciente *Feature-Policy*.

Reverse Proxy + WAF + aceleración TLS

1 Introducción

- Aplicaciones web y la seguridad
- Mecanismos de protección
- Aplicaciones web y la seguridad

2 Estado del arte

- Soluciones WAF privativas
- Soluciones WAF de software libre
- Comparativa soluciones WAF

3 Solucion

- Objetivo
- Diseño
- Arquitectura

4 Tests y resultados

5 Conclusiones



Conclusiones

TODO



Ruegos y preguntas

¿Preguntas?



Referencias I



Internet Engineering Task Force (IETF). *Estándar RFC8484. DNS Queries over HTTPS (DoH)*

. URL: <https://tools.ietf.org/html/rfc8484>.



Dr. Gulshan Kumar Ahuja. «Denial of service attacks - an updated perspective». En: *Systems Science and Control Engineering* 4 (ene. de 2016), págs. 285-294. DOI: 10.1080/21642583.2016.1241193.



Open Web Application Security Project. *OWASP Top 10*. URL: <https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf>.



Referencias II



Vicente Aguilera Díaz. *Controles técnicos de seguridad para la protección de aplicaciones web*

. URL: http://www.vicenteaguileradiaz.com/pdf/SIC94_Seguridad_Aplicaciones_OWASP.pdf.



TLS compatibility with PCI DSS (Payment Card Industry Data Security Standard)

. URL: <https://blog.wao.io/tls-compatibility-with-pci-dss/>.



Wikipedia. *Server Name Indication*

. URL: https://es.wikipedia.org/wiki/Server_Name_Indication.



Referencias III



Hashed Out Blog. *Nearly 21 % of the world's top 100,000 websites still aren't using HTTPS*

. URL: <https://www.thesslstore.com/blog/nearly-21-of-the-worlds-top-100000-websites-still-arent-using-https/>.



INCIBE. *WAF: cortafuegos que evitan incendios en tu web*

. URL: <https://www.incibe.es/protege-tu-empresa/blog/waf-cortafuegos-evitan-incendios-tu-web>.



Cloudflare WAF

. URL: <https://www.cloudflare.com/waf/>.



Referencias IV



Cloudflare

. URL: <https://www.cloudflare.com/>.



Kona WAF

. URL:
<https://www.akamai.com/uk/en/resources/waf.jsp>.



Akamai

. URL: <https://www.akamai.com/es/es/>.



Incapsula Web Application Firewall

. URL: <https://www.incapsula.com/website-security/web-application-firewall.html>.



Referencias V



Imperva WAF Gateway

. URL: <https://www.imperva.com/products/on-premises-waf/>.



FortiWeb: Web Application Firewall

. URL: <https://www.fortinet.com/products/web-application-firewall/fortiweb.html>.



Fortinet

. URL: <https://www.fortinet.com/>.



Página oficial de IronBee

. URL: <https://github.com/ironbee/ironbee>.



Referencias VI



Repositorio de código oficial de WebCastellum

. URL: <https://sourceforge.net/p/webcastellum/code/HEAD/tree/>.



Repositorio de código oficial de Raptor WAF

. URL: https://github.com/CoolerVoid/raptor_waf.



Página oficial de NAXSI

. URL: <https://github.com/nbs-system/naxsi>.



Página oficial de OpenWAF

. URL: <https://github.com/titansec/OpenWAF>.



Blog oficial de FreeWAF / lua-resty-waf

. URL: <https://www.cryptobells.com/reintroducing-lua-resty-waf/>.



Referencias VII



Página oficial de Shadow Daemon

. URL: <https://shadowd.zecure.org/overview/introduction/>.



Página oficial de AQTRONiX WebKnight

. URL: <https://www.aqtronix.com/?PageID=99>.



Página oficial de Vulture WAF

. URL: <https://www.vultureproject.org/>.



Página oficial de Modsecurity

. URL: <https://www.modsecurity.org/>.



*Internet Engineering Task Force (IETF). Estándar RCF7530.
Network File System (NFS) Version 4 Protocol*

. URL: <https://tools.ietf.org/html/rfc7530>.



Referencias VIII



Qualys. *SSL Labs. SSL Server Test*

. URL: <https://www.ssllabs.com/ssltest/index.html>.



Netsparker. *Security Headers Test*

. URL: <https://securityheaders.com/>.



Wikipedia. *HTTP Strict Transport Security*

. URL: https://es.wikipedia.org/wiki/HTTP_Strict_Transport_Security.



Wikipedia. *Systems Development Life Cycle*

. URL: https://es.wikipedia.org/wiki/Systems_Development_Life_Cycle.



Glosario I

CDN Content Delivery Network. 16

DoH DNS over HTTPS. 4, 34

DoS Denial-of-service. 16

HSTS HTTP Strict Transport Security[30, Wikipedia]. 30

HTTP Hypertext Transfer Protocol. 4

HTTPS Hypertext Transfer Protocol Secure. 4

OWASP Open Web Application Security Project. 6, 34

RBAC role-based access control. 18



Glosario II

SaaS Software as a Service. 16

SDLC Systems Development Life Cycle[31, Wikipedia]. 10

URL Uniform Resource Locator. 16

WAF Web Application Firewall. 13, 25, 26

