

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

25 de julio de 2019



**Universidad
Europea**

LAUREATE INTERNATIONAL UNIVERSITIES

Agenda

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



Reverse Proxy + WAF + aceleración TLS

1 Introducción

- Aplicaciones web y la seguridad
- Mecanismos de protección
- ¿Qué es un WAF?

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.

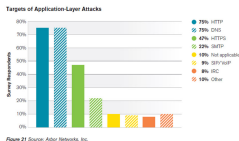


Figure 21 Source: Arbor Networks, Inc.

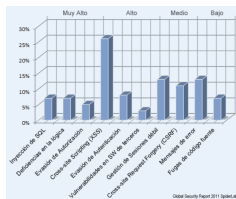


Figura: Ataques en capa de aplicación (fuentes Arbor [2], OWASP [3])

Conclusión

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

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

Solución - Mitigación

Actualizar software y desactivar las versiones o el componente afectados.
El riesgo de afectar la funcionalidad de la plataforma es bajo (dependiendo del entorno).



Soluciones, controles de seguridad

- **Desarrollo de código seguro:** metodologías y herramientas.
Retos: Tiempo y recursos.
- **Aplicar un ciclo de vida de aplicaciones:** Gestión de actualizaciones y configuración segura.
Retos: Una actualización puede afectar al entorno, el objetivo es que la *aplicación funcione*.
chmod 777 o iptables -A INPUT -j ACCEPT funcionan.
- **Protección perimetral de red:** Firewall de red, Sistema de Prevención de Intrusos.
Reto: Visibilidad reducida.
- **Herramientas de firewall de aplicación:** WAF.
Reto: Coste o complejidad.



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 [4]).
- TLS versión 1.3.
- HTTP/2.
- TLS Server Name Indication (SNI [5]).
- 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

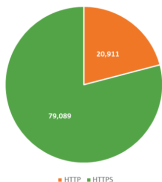


Figura: Tráfico HTTP versus HTTPS [6]

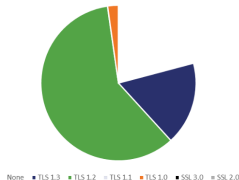


Figura: Máxima versión SSL/TLS soportada [6]

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

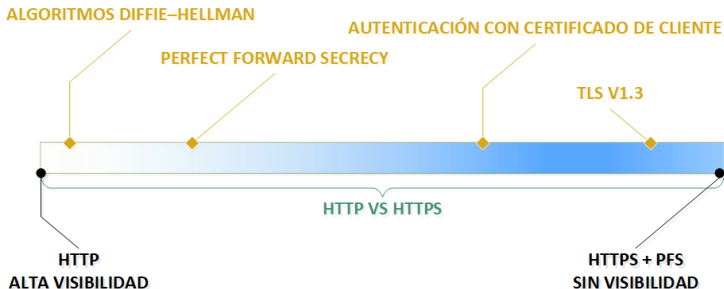


Figura: Evolución y retos: De HTTP a HTTPS

Web Application Firewall (WAF)

¿Qué es un WAF?

Un WAF es una herramienta especializada en filtrar, monitorizar y bloquear las conexiones desde y hacia una aplicación web (Fuente: Instituto Nacional de Ciberseguridad [7]).

Características principales:

- Analiza el tráfico web: Entiende GET, POST, parámetros URL, etc.
- Se aplican políticas y reglas de filtrado. Por ejemplo:

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

- Listas blancas o negras de User Agents, IP, caracteres aceptados en URL o formularios, etc.



Reverse Proxy + WAF + aceleración TLS

- 1 Introducción
 - Aplicaciones web y la seguridad
 - Mecanismos de protección
 - ¿Qué es un WAF?
- 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* [8] de Cloudflare[9].
 - *Kona WAF*[10] de Akamai[11].
 - *Incapsula*[12].
- **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*[13].
 - *Fortiweb*[14] de la empresa *Fortinet*[15].



Ventajas e inconvenientes

Ventajas:

- Sencillas de implementar
- Independencia de la infraestructura de la plataforma web.
- (RBAC del inglés).
- Soporte técnico.
- Funcionalidades adicionales.

Desventajas:

- Elevado coste económico.
- No es posible adaptar la solución a necesidades específicas.



Soluciones WAF de software libre

Existen múltiples soluciones de software libre

- IronBee[16].
- WebCastellum[17].
- RAPTOR[18].
- NAXSI[19].
- OpenWAF[20].
- FreeWAF[21].
- Shadow Daemon[22].
- AQTRONiX WebKnight[23].
- Vulture[24].
- ModSecurity [25].

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 (despliegue y operación)	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	Muy buenas	Buenas	Limitadas	Buenas



Reverse Proxy + WAF + aceleración TLS

- 1 Introducción
 - Aplicaciones web y la seguridad
 - Mecanismos de protección
 - ¿Qué es un WAF?
- 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

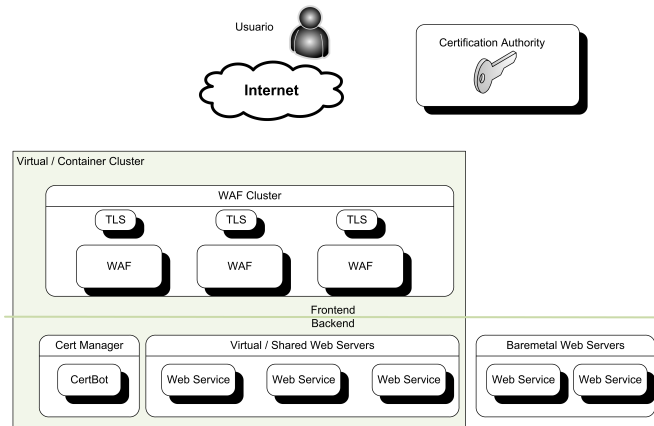


Figura: Diseño a alto nivel de la solución



Componentes

- Web Application Firewall.
- Software criptográfico.
- Virtualización (contenedores).
- Automatización y orquestación.
- Gestión de certificados.
- Políticas y controles de seguridad.



WAF. Funcionalidades

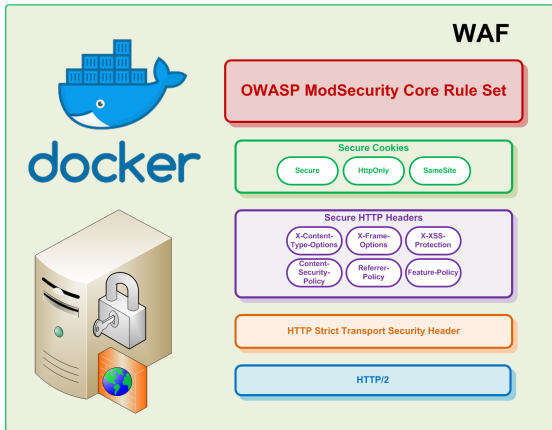


Figura: Controles de seguridad desplegados en el contenedor Docker.

Arquitectura. Gestión de certificados

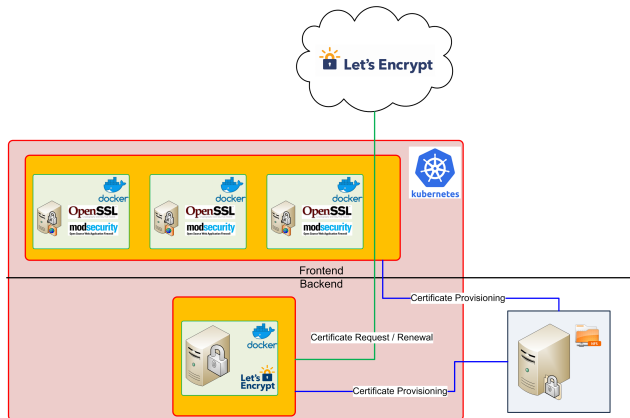


Figura: Diagrama de comunicaciones de Let's Encrypt.

Arquitectura. Peticiones HTTP/HTTPS

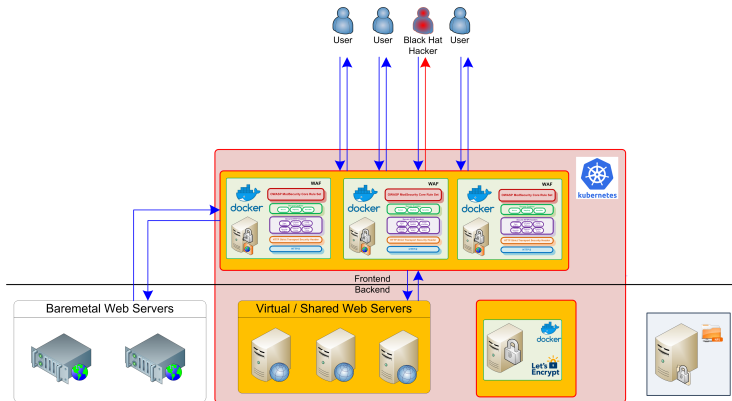


Figura: Peticiones HTTP/HTTPS

Reverse Proxy + WAF + aceleración TLS

1 Introducción

- Aplicaciones web y la seguridad
- Mecanismos de protección
- ¿Qué es un WAF?

2 Estado del arte

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

3 Solucion

- Objetivo
- Diseño
- Arquitectura

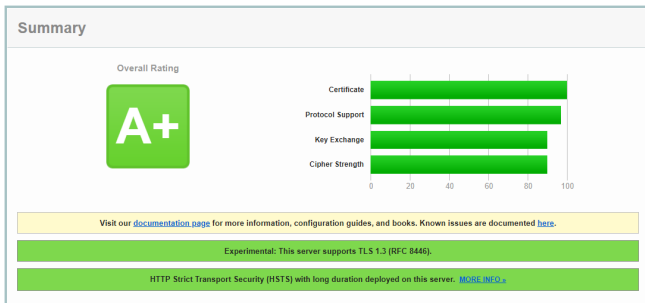
4 Tests y resultados

5 Conclusiones



Resultados TLS

Se ha ejecutado la batería de pruebas proporcionada por Qualys. SSL Labs [26] 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 [27] 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*[28, 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
- ¿Qué es un WAF?

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

Características de la propuesta

- ✓ Independencia de la plataforma web
- ✓ Independencia operacional (RBAC)
- ✓ Complejidad (despliegue y operación)
- ✓ Coste económico
- ✗ Soporte técnico
- ✓ Información accesible por terceros
- ✓ Adaptabilidad / Personalización
- ✓ Acceso al código fuente
- ✓ Funcionalidades adicionales



Conclusiones

- Se ha conseguido crear una solución de **software libre** que permita mejorar la seguridad en las plataformas web en entornos sin los medios o conocimientos necesarios.
- Mejores prácticas de OWASP [29] y Qualys [30].
- Implementa la facilidad de las soluciones privativas.
- Adaptabilidad del software libre.
- Funcionalidades adicionales: Cabeceras de seguridad, cookies, etc.



Trabajo a futuro

- Desplegar en producción.
- Consolidar y estabilizar la solución.
- Añadir funcionalidades:
 - Anti-DDoS (rate limit).
 - Control de bots.
 - Mejorar los ficheros de configuración
 - Botón de modo simulación / modo bloqueo.
 - Botón de modo depuración.



Demo

Demo funcional



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



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.



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/>.



Referencias III



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/>.



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



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



Referencias IV



Akamai

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



Incapsula Web Application Firewall

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



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>.



Referencias V



Fortinet

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



Página oficial de IronBee

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



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>.



Referencias VI



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/>.



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/>.



Referencias VII



Página oficial de Modsecurity

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



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.



Referencias VIII



Open Web Application Security Project (OWASP). *OWASP Best Practices: Use of Web Application Firewalls*

. URL: https://www.owasp.org/index.php/Category:OWASP_Best_Practices:_Use_of_Web_Application_Firewalls.



SSL and TLS Deployment Best Practices

. URL: <https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices>.



Wikipedia. *Systems Development Life Cycle*

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



Glosario I

- DoH** DNS over HTTPS. 4, 34
- HSTS** HTTP Strict Transport Security[28, Wikipedia]. 27
- HTTP** Hypertext Transfer Protocol. 4
- HTTPS** Hypertext Transfer Protocol Secure. 4
- OWASP** Open Web Application Security Project. 5, 34, 41
- RBAC** role-based access control. 14
- SDLC** Systems Development Life Cycle[31, Wikipedia]. 8
- WAF** Web Application Firewall. 7, 11, 21

