

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

10 de julio de 2019



**Universidad
Europea**

LAUREATE INTERNATIONAL UNIVERSITIES

Agenda

- Introducción:
 - Aplicaciones web y la seguridad.
 - Estándares y protocolos.
- 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
 - Estándares y protocolos
 - 2 Estado del arte
 - Soluciones WAF privativas
 - Soluciones WAF de software libre
 - Comparativa soluciones actuales
 - 3 Solucion
 - Objetivo
 - Diseño
 - Arquitectura
 - 4 Conclusiones
 - 5 Tests y resultados
- Siglas



Aplicaciones web y la seguridad

Premisa

La seguridad 100 % no existe.

Las aplicaciones web están siendo atacadas continuamente.

Targets of Application-Layer Attacks

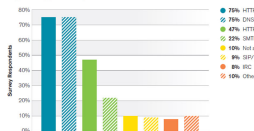


Figure 21 Source: Arbor Networks, Inc.

Application-Layer Attack Tools

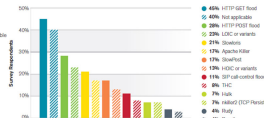


Figure 22 Source: Arbor Networks, Inc.

Figura: Ataques en capa de aplicación (fuente Arbor [1])

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 [2]).

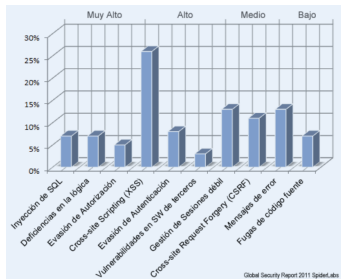


Figura: Tipo de Vulnerabilidades por Impacto [3]

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. I

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.



Soluciones. II

- Una actualización puede afectar al entorno.
- *chmod 777* o *iptables -A INPUT -j ACCEPT* funcionan.
- **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.



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 Herramientas están disponibles y ofrecen mecanismos válidos para mejorar la seguridad de las plataformas web pero su implementación puede ser compleja o tener un elevado coste.



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

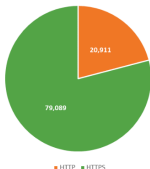


Figura: Tráfico HTTP versus HTTPS [6]

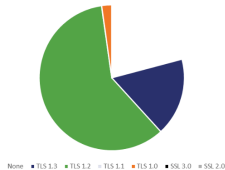


Figura: Máxima versión SSL/TLS soportada [6]

Uso e implementación

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



Reverse Proxy + WAF + aceleración TLS

- 1 Introducción
 - Aplicaciones web y la seguridad
 - Estándares y protocolos
 - 2 Estado del arte
 - Soluciones WAF privativas
 - Soluciones WAF de software libre
 - Comparativa soluciones actuales
 - 3 Solucion
 - Objetivo
 - Diseño
 - Arquitectura
 - 4 Conclusiones
 - 5 Tests y resultados
- Siglas



Soluciones WAF privativas

- Tecnología 1.
- Tecnología 1.
- Tecnología 1.



Ventajas e inconvenientes

PRO: Facilidad de despliegue y gestión. PRO: Funcionalidades adicionales (p.e. CDN). CONS: Coste. CONS: Falta de flexibilidad.



Soluciones WAF de software libre

- Tecnología 1.
- Tecnología 1.
- Tecnología 1.



Ventajas e inconvenientes

PRO: Coste. CONS: Complejidad.



Comparativa soluciones actuales

TODO



Reverse Proxy + WAF + aceleración TLS

- 1 Introducción
 - Aplicaciones web y la seguridad
 - Estándares y protocolos
 - 2 Estado del arte
 - Soluciones WAF privativas
 - Soluciones WAF de software libre
 - Comparativa soluciones actuales
 - 3 **Solucion**
 - **Objetivo**
 - **Diseño**
 - **Arquitectura**
 - 4 Conclusiones
 - 5 Tests y resultados
- Siglas



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

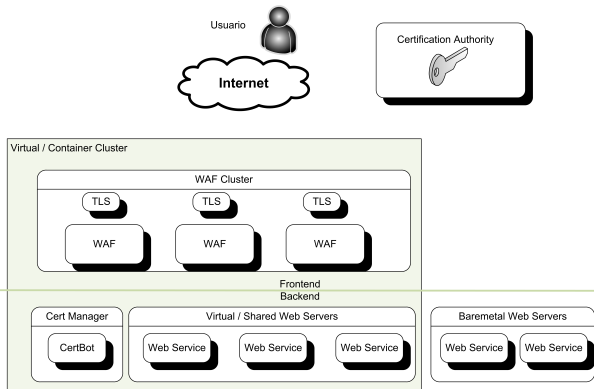


Figura: Diseño a alto nivel de la solución

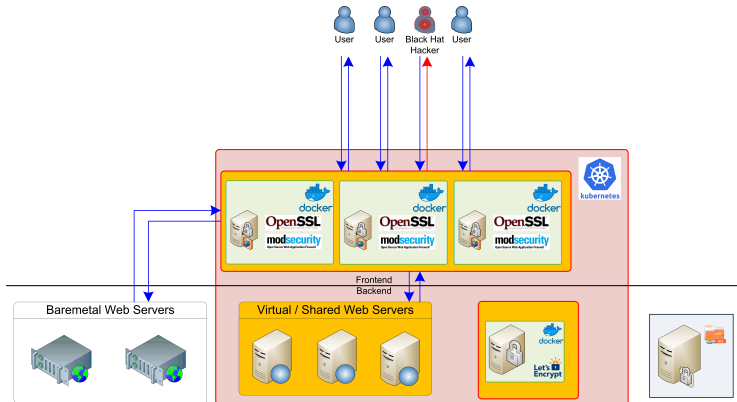


Componentes

- WAF.
- Software criptográfico.
- Software de virtualización.
- Software de orquestación.
- Software de aprovisionamiento y gestión de certificados.
- Servicio de almacenamiento.
- Políticas de auditoría y controles de seguridad.



Arquitectura



Reverse Proxy + WAF + aceleración TLS

- 1 Introducción
 - Aplicaciones web y la seguridad
 - Estándares y protocolos
 - 2 Estado del arte
 - Soluciones WAF privativas
 - Soluciones WAF de software libre
 - Comparativa soluciones actuales
 - 3 Solucion
 - Objetivo
 - Diseño
 - Arquitectura
 - 4 Conclusiones
 - 5 Tests y resultados
- Siglas



Conclusiones

TODO



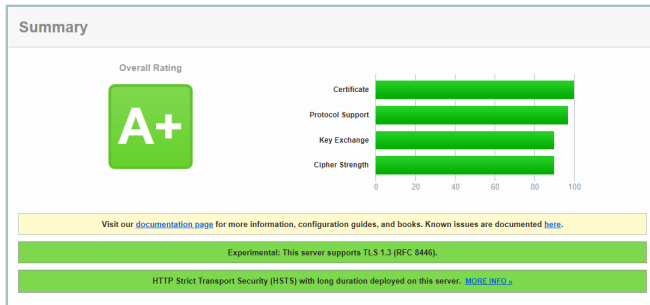
Reverse Proxy + WAF + aceleración TLS

- 1 Introducción
 - Aplicaciones web y la seguridad
 - Estándares y protocolos
 - 2 Estado del arte
 - Soluciones WAF privativas
 - Soluciones WAF de software libre
 - Comparativa soluciones actuales
 - 3 Solucion
 - Objetivo
 - Diseño
 - Arquitectura
 - 4 Conclusiones
 - 5 **Tests y resultados**
- Siglas



Resultados TLS

Se ha ejecutado la batería de pruebas proporcionada por Qualys. SSL Labs [7] 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 [8] con el siguiente resultado:

Security Report Summary



Site:	https://finkalinux.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* (HSTS), *X-XSS-Protection*, *Content-Security-Policy* o la reciente *Feature-Policy*.

Ruegos y preguntas

¿Preguntas?



Referencias I



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>.



Vicente Aguilera Díaz. *Controles técnicos de seguridad para la protección de aplicaciones web*. URL: http://www.vicenteaguileradiaz.com/pdf/SIC94_Seguridad_Aplicaciones_OWASP.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



Qualys. *SSL Labs. SSL Server Test*

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



Netsparker. *Security Headers Test*

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



Wikipedia. *Systems Development Life Cycle*

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



Glosario I

HSTS HTTP Strict Transport Security. 26

OWASP Open Web Application Security Project. 5, 28

SDLC Systems Development Life Cycle[9, Wikipedia]. 9

