

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

8 de julio de 2019



**Universidad
Europea**

LAUREATE INTERNATIONAL UNIVERSITIES

Agenda

- Introducción:
 - Aplicaciones web y la seguridad.
 - Qué es un Web Application Firewall (WAF).
 - Comunicaciones cifradas. Transport Layer Security (TLS).
- Situación actual. Estado del arte:
 - Soluciones WAF privativas.
 - Soluciones WAF de software libre.
 - Uso de HTTP / HTTPS.
- Solución.
 - Objetivo.
 - Diseño.
 - Arquitectura.
- Conclusiones.
- Test y resultados.



Reverse Proxy + WAF + aceleración TLS

- 1 Introducción
 - Aplicaciones web y la seguridad
- 2 Estado del arte
 - Soluciones WAF privativas
 - Soluciones WAF de software libre
 - Uso de HTTP y HTTPS
- 3 Solucion
 - Objetivo
 - Diseño
 - Arquitectura
- 4 Conclusiones
- 5 Tests y resultados



Aplicaciones web y la seguridad

Premisa

La seguridad 100 % no existe.

Las aplicaciones web están siendo atacadas continuamente.

Targets of Application-Layer Attacks

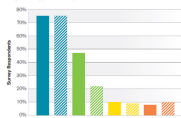


Figure 21 Source: Arbor Networks, Inc.

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 y evolución de los canales cifrados

En los últimos años se ha descubierto múltiples vulnerabilidades críticas en los canales TLS.

Ejemplo de vulnerabilidades con impacto alto:

Vulnerabilidad	Componente afectado
POODLE	SSL v3.0
BEAST	TLS v1.0
CRIME	TLS compression
BREACH	HTTP compression
Heartbleed	OpenSSL

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).



Uso de canales cifrados

El uso de



Reverse Proxy + WAF + aceleración TLS

- 1 Introducción
 - Aplicaciones web y la seguridad
- 2 Estado del arte
 - Soluciones WAF privativas
 - Soluciones WAF de software libre
 - Uso de HTTP y HTTPS
- 3 Solucion
 - Objetivo
 - Diseño
 - Arquitectura
- 4 Conclusiones
- 5 Tests y resultados



Soluciones WAF privativas

TODO



Soluciones WAF de software libre

TODO



Uso de HTTP y HTTPS

TODO



Reverse Proxy + WAF + aceleración TLS

- 1 Introducción
 - Aplicaciones web y la seguridad
- 2 Estado del arte
 - Soluciones WAF privativas
 - Soluciones WAF de software libre
 - Uso de HTTP y HTTPS
- 3 **Solucion**
 - Objetivo
 - Diseño
 - Arquitectura
- 4 Conclusiones
- 5 Tests y resultados



Objetivo

TODO



Diseño

TODO



Componentes

TODO



Arquitectura

TODO



Reverse Proxy + WAF + aceleración TLS

- 1 Introducción
 - Aplicaciones web y la seguridad
- 2 Estado del arte
 - Soluciones WAF privativas
 - Soluciones WAF de software libre
 - Uso de HTTP y HTTPS
- 3 Solucion
 - Objetivo
 - Diseño
 - Arquitectura
- 4 Conclusiones**
- 5 Tests y resultados



Conclusiones

TODO



Reverse Proxy + WAF + aceleración TLS

- 1 Introducción
 - Aplicaciones web y la seguridad
- 2 Estado del arte
 - Soluciones WAF privativas
 - Soluciones WAF de software libre
 - Uso de HTTP y HTTPS
- 3 Solucion
 - Objetivo
 - Diseño
 - Arquitectura
- 4 Conclusiones
- 5 Tests y resultados



Tests y resultados

TODO



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.



Glosario I

