Universidad Europea
Proyecto de Fin de Grado

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

Alumno: Pedro Pozuelo Rodríguez
Directora: Ana del Valle Corrales Paredes
Titulación: Grado en Ingeniería Informática
Fecha: 27 de mayo de 2019

Índice general

Estado del arte

En los últimos años, la mayoría de los ataques en Internet se realizan contra aplicaciones web, con lo que es cada vez más importante contar con una solución que sea capaz de analizar el tráfico web y proteger las aplicaciones.

Las soluciones de firewall tradicional son capaces de analizar el tráfico de red en capa 3 del modelo TCP/IP (equivalentas a las capas 3 y 4 del *modelo OSI[1]*). Sin embargo, carecen de la funcionalidad necesaria para analizar el tráfico en capa 7. Esto implica que, una vez se publica un servicio web, dichos firewalls permitirán todo el tráfico dirigido a estos servicios, con independencia de que se trate de una petición legítima, una petición malformada o un ataque.

Para proteger estos servicios y poder diferencias entre estas peticiones es necesario disponer de tecnologías que entiendan analicen el tráfico en la capa de aplicación siguiendo la lógica propia del servicio a proteger.

Actualmente existen diversas soluciones de firewall de aplicación web (en adelante WAF, de sus siglas en inglés, Web Application Firewall).

Se ha utilizado el documento de buenas prácticas de OWASP[2] como referencia para elegir las soluciones a analizar. El criterio seguido es que la solución debe ser capaz de proteger la plataforma web implementando una mayoría de los controles de seguridad (referenciados como *Countermeasure* en la página de OWASP[2, apartado A3.2]).

Dentro de las soluciones disponibles, podemos distinguir principalmente entre soluciones privativas y soluciones de software libre. Este criterio no se circunscribe exclusivamente al modelo de licencias si no que está íntimamente ligado al coste asociado tal como veremos.

1.1 Soluciones WAF privativas

Las soluciones de WAF privativas se caracterizan por emplear un modelo de *licenciamiento privativo[3]*. Se trata de soluciones con un elevado coste y con la imposibilidad de acceder al código o modificarlo. Así mismo, ofrecen una serie de funcionalidades adicionales y una mayor capacidad de procesamiento.

Existen dos arquitecturas principales en este tipo de WAF:

Por un lado tenemos modelos WAF desplegados en las instalaciones del fabricante y gestionados por él. Este tipo de soluciones suelen estás alojadas en el Cloud (en el modelo de distribución de software conocido como *software como servicio* (en adelante SaaS, de sus siglas en inglés, Software as a Service).

En segundo lugar, tenemos WAF de tipo appliance o máquina virtual. Se trata de máquinas dedicadas en las que el software requiere de una máquina específica proporcionada por el fabricante. Si bien hardware y software se adquieren conjuntamente, es posible acceder a nuevas funcionalidades

adquiriendo nuevas licencias.

1.1.1 Soluciones WAF SaaS

Dentro de las soluciones WAF SaaS, destacan y se han analizado *Cloud Web Application Firewall* [4] de Cloudflare[5] (*Cloudflare* en adelante), *Kona WAF[6]* de *Akamai[7]* e *Incapsula[8]*.

Habitualmente, estos proveedores no se limitan a ofrecer servicios WAF, pues por su infraestructura permite añadir funcionalidades adicionales como son las siguientes.

- Red de distribución de contenidos (en adelante CDN, de sus siglas en inglés, Content Delivery Network).
- Protección contra ataques de denegación de servicio (en adelante DoS, de sus siglas en inglés, Denial-of-service) en capa de aplicación.
- Habilitar el caché de contenido estático.
- Suscripción a listas de reputación de IP, dominios o URL.
- Bloqueo de bots maliciosos.
- Sistema de creación de informes.

De hecho, la funcionalidad CDN es el servicio mínimo que se puede contratar a Akamai y Cloudflare; pues es su nicho mercado y su producto principal, siendo el servicio WAF una funcionalidad que ofrecen a sus cliente para dar un valor añadido. Incapsula, por el contrario, proviene de soluciones WAF tipo appliance y su modelo de negocio está más enfocado a estos servicios.

Uno de las principales características que comparten estos proveedores es el modelo de negocio. En todos los casos el coste está asociado al volumen de tráfico que se genere, ya sea en caudal de datos (en adelante Throughput), como es el caso de Incapsula, o por volumen mensual de datos en el caso de Akamai y Cloudflare.

Modo de licenciamiento y coste

En la mayoría de las soluciones no existe un precio oficial de mercado proporcionado por los proveedores. En estos casos se ha optado por incluir referencias externas con el fin de disponer información del coste aproximado de estas soluciones.

A modo de referencia, se puede consultar los precios de Akamai y Cloudflare en la tabla de precios CDN. Estos precios se corresponden con sus servicios de CDN y podrá ser superior si se añaden funcionalidades como WAF. Adicionalmente, se debe tener en cuenta que se trata de precios estimativos proporcionados por terceros, pues en el caso de Akamai la lista de precios no es pública y ofrecen un coste ajustado a cada cliente.

	Akamai CDN	**CloudFlare CDN**
6 TB plan	900 USD al mes aprox.	750 USD al mes aprox.
25 TB plan	2800 USD al mes aprox.	2800 USD al mes aprox.
50 TB plan	5500 USD al mes aprox.	5000+ USD al mes aprox.
100 TB plan	8000 USD al mes aprox.	5000+ USD al mes aprox.

Cuadro 1.1: Precios de CDN[9] (consultado en abril de 2019)

En el caso de Incapsula, su solución más económica - el plan *PRO* - tiene un coste de 59 USD por web al mes[10]. Dicha solución soporta SSL de manera limitada y es necesario contratar un plan superior en caso de que se requiera dar servicio a clientes que no soporten la extensión TLS SNI o se requieran certificados con validación extendida (en adelante EV, de sus siglas en inglés, Extended Validation). En esta situación habría que contratar el plan *business* que tiene un coste de 299 USD por web al mes[10].

Implementación y operación

Independientemente de la solución, grosso modo estos son los pasos a realizar para implantar este tipo de soluciones:

1. Cambio en la gestión de certificados SSL.

   Dado que la mayoría de las aplicaciones web deben soportar SSL, es necesario generar nuevos certificados para que el proveedor pueda publicar los servicios web de manera confiable. En la mayoría de los casos el fabricante será responsable del mantenimiento y la operación de dichos certificados.

2. Preparación de un entorno de pruebas - *staging* - en el que se puedan probar las aplicaciones web de manera interna sin impactar a los clientes. Para ello, habitualmente, se redireccionan los dominios a probar en el fichero *hosts* de la máquina cliente.

3. Cambio del direccionamiento DNS.

   Una ya se ha validado que la solución web y el WAF funcionan adecuadamente, se procede a cambiar el direccionamiento ofrecido a nivel DNS para que los clientes se conecten a la plataforma WAF en lugar de a la aplicación web.

La operación de estas plataformas es realizada por el proveedor, por lo que como clientes no necesitamos disponer del conocimiento o el tiempo necesario para mantener o actualizar la plataforma WAF.

Ventajas

Una de las principales ventajas que tiene este tipo de soluciones consiste en su independencia respecto a la infraestructura de la aplicación web.

Esta independencia nos permite realizar cambios en cualquier de las soluciones - WAF o plataforma Web - sin que afecte a la otra. Ya sean cambios en la operación diaria, migraciones de software o rediseño de la arquitectura.

La mencionada independencia no se limita a independencia tecnológica; el hecho de que el WAF y la plataforma web sean completamente independientes también permite asignar roles independientes a cada entorno, lo cual permite implementar seguridad basada en roles (en adelante RBAC, de sus siglas en inglés, role-based access control). Esto no sólo nos permite mejorar la seguridad del entorno, si no que además evita que el desarrollador web o el administrador de la plataforma web tenga que conocer en detalle la configuración del WAF y viceversa.

Por otro lado, este tipo de soluciones son las muy sencillas de implementar, tal como se ha visto en la sección anterior.

Otra ventaja radica en la aplicación de nuevas reglas de seguridad de forma transparente para el cliente. No necesitaremos dar seguimiento a las últimas vulnerabilidades web que se publican o idear qué reglas o firmas son necesarias, pues el proveedor se hará cargo de su implementación y mantenimiento.

Las soluciones WAF SaaS también nos permiten contratar diversas modalidades de soporte que garanticen respuesta 24/7 en caso de que se produzca un incidente con el servicio.

Por último, nos podemos beneficiar de las funcionalidades adicionales ya mencionadas para mejorar el estado de la seguridad de nuestra plataforma o mejorar la experiencia del usuario.

Desventajas

Una de las principales desventajas radica en el coste económico. Este tipo de soluciones tienen un elevado coste. Esto implica que este tipo de WAF sólo son viables económicamente en portales que generen un beneficio económico importante o aquellos en los que la empresa/entidad responsable de la aplicación pueda asumir su inversión.

Aunque este tipo de soluciones disponen de modalidades relativamente económicas (ver Modo de licenciamiento y coste), lo cierto es que estas soluciones están muy limitadas y es necesario contratar funcionalidades adicionales en la mayoría de los casos. Es un modelo económico muy dirigido a las ofertas personalizadas y suele ser habitual requerir el modelo de licenciamiento *Enterprise* junto con ciertas licencias adicionales, lo cual encarece todavía más el servicio.

En cualquier caso, este tipo de soluciones no están al alcance de pequeñas o medianas empresas o de particulares.

Otra desventaja que tienen este tipo de soluciones consiste en la pocas posibilidades que tenemos de personalizar las reglas o las firmas a nuestras necesidades. La arquitectura de este tipo de plataformas SaaS consiste en que múltiples clientes comparten la misma plataforma, para lo cual el proveedor requiere mantener un sistema homogéneo para todos los clientes y esto evita que se pueda personalizar el WAF según nuestras necesidades. A modo de ejemplo, en los servicios estándar de este tipo de soluciones no podremos configurar reglas para filtrar las cabeceras HTTP o los parámetros de tipo query en las URL si nuestra aplicación utilizada *Path Parameters* o *URL Routing*, lo que dejaría expuesta la aplicación web a ataques de inyección de código.

1.1.2 Soluciones WAF tipo Appliance

Otra modalidad de soluciones WAF son los de tipo appliance. Dentro de las opciones disponibles en el mercado se han analizado *Imperva WAF Gateway[11]* (*Imperva* en adelante) y *Fortiweb[12]* de la empresa *Fortinet[13]*.

El modelo de negocio tradicional consiste en adquirir máquina física junto con un paquete de licencias, aunque en los últimos años se han incorporado soluciones virtuales en los catálogos de los principales proveedores de Cloud.

Al igual que sucede con las soluciones SaaS, los proveedores de este tipo de WAF también incluyen mecanismos de seguridad adicionales que no son propiamente funcionalidades WAF. Si bien estas funcionalidades dependen en gran medida del proveedor, a continuación se enumeran algunas de las más interesantes:

- Crear perfiles de las aplicaciones web y filtrar las peticiones web en función de los parámetros permitidos.
- Parcheo virtual de vulnerabilidades mediante la integración del WAF con programas de escaneo de vulnerabilidades.
- Suscripción a listas de reputación de IP, dominios o URL.
- Aceleración TLS.

Dado que el dispositivo suele estar en la misma red que la aplicación web, es posible que el WAF realice el descifrado del tráfico SSL/TLS y envíe el tráfico sin cifrar a la aplicación web, lo que permite liberar los recursos asignados al cifrado y descifrado en la aplicación web.

- Bloqueo de bots maliciosos.
- Sistema de creación de informes.
- Antivirus.

Modo de licenciamiento y coste

Al igual que sucede con las soluciones SaaS, en las soluciones appliance los proveedores no publican abiertamente el coste que tienen sus productos y optan por realizar presupuestos personalizados dependiendo de las necesidades de cada cliente. Al igual que en el análisis del modelo SaaS se ha optado por incluir referencias externas con el fin de mostrar el coste que tienen este tipo de soluciones.

En el caso de Imperva, su oferta está enfocada a soluciones WAF y firewall de base de datos (en adelante DBF, de sus siglas en inglés, Database Firewall). Se trata de la misma compañía que ha desarrollado y comercializa Incapsula, siendo ésta la alternativa SaaS a Imperva.

Imperva ofrece diversos modelos de appliances según el throughput que son capaces de gestionar, desde 500 Mbps en el modelo más básico - X2010 o X2020 - hasta los 10 Gbps en el modelo X10K.

El coste del appliance de 500 Mbps es de 4200 USD (según [14] y [15]), a lo que hay que sumar el coste anual de licencias y mantenimiento. La licencia necesaria para este modelo tiene un coste que puede ir desde 4800 USD[16] hasta 9600 USD[17]. Por lo tanto, la opción más económica requiere una inversión inicial de 9000 USD y un coste anual mínimo de 4800 USD.

En el caso de que la plataforma web esté alojada en el Cloud (por ejemplo AWS), la opción más económica ofrecida por Imperva tiene un coste mínimo de 8927 USD anuales para una instancia con capacidad de hasta 100 Mbps[18] o 21567 USD por año para el equivalente de la opción appliance de 500 Mbps[19].

Otra solución appliance que se ha analizado es Fortiweb. Si bien sigue un modelo de negocio similar a Imperva, dispone de modelos más económicos. En la tabla de precios Fortiweb se recogen los modelos appliance más económicos ofrecidos por Fortinet.

Modelo	Throughput	Coste de appliance	Coste licencia básica	Coste total
FortiWeb-100D	25 Mbps	5034 USD[20]	755 USD[20]	5789 USD
FortiWeb-400D	100 Mbps	9194 USD[21]	1572 USD[21]	10766 USD
FortiWeb-600D	250 Mbps	14000 USD[22]	2100 USD[22]	16100 USD

Cuadro 1.2: Precios de Fortiweb

La solución AWS de Fortiweb tiene un coste de 5374 USD[23] al año.

Implementación y operación

La implementación de las soluciones tipo appliance es más compleja que en el modelo SaaS debido a que el WAF será parte de nuestra arquitectura y es necesario analizarla y adaptarla con el fin de incluir este nuevo elemento.

Los pasos que se deben realizar para implantar un WAF de tipo appliance en una arquitectura son los siguientes:

1. Evaluar la arquitectura actual e identificar los potenciales puntos en los que se podría desplegar el WAF.

   Algunos de los punto de conexión donde se suelen desplegar WAF de este tipo son inmediatamente después del firewall red o inmediatamente antes de los balanceadores de carga de aplicación, pero puede variar significativamente según la arquitectura. Especialmente se debe tener en cuenta los siguientes elementos:

   - Tolerancia frente a fallos (en adelante *failover*).
   - Tipo de enrutamiento: estático o dinámico, unicast o multicast, etc.
   - Sistemas distribuidos o redundantes.
   - Balanceadores de red o de aplicación.
   - Volumen de tráfico en los distintos puntos de red a evaluar.

     Por ejemplo, si se instala el WAF en el punto de entrada de una DMZ, el appliance debe ser capaz de gestionar el throughput agregado de todos los servicios publicados en dicha DMZ. Sin embargo, si se instala inmediatamente antes de una aplicación web, el WAF sólo debe analizar el tráfico de dicha aplicación. Por contra, si se despliega una nueva aplicación web es posible que ésta no esté protegida por el WAF.
   - Lógica de la aplicación web.

     A modo de ejemplo, en una arquitectura en la que se disponga de un servidor web para servir contenido estático, es posible configurar el WAF para que no acepte el paso de parámetros o que sólo proteja el servidor web de contenido dinámico si se decide aceptar el riesgo asociado.
   - Aplicación alojada en un único centro de datos (en adelante CPD) o en varios.

2. Analizar dichos puntos y evaluar el modo de despliegue en el que se desplegará el WAF. Los modos más comunes son modo transparente, en el que el WAF no participa en las capas 3 a 7 del modelo OSI, o como proxy web explícito, en cuyo caso el WAF participa en las capas 3 y 4 y opcionalmente en la capa de aplicación.

3. Evaluar el impacto que este cambio tendrá en el desempeño de la aplicación web, entre otros se debe evaluar la latencia que añade a la red y a la aplicación o cómo afecta al throughput que deben soportar los distintos componentes.

4. Adaptar el diseño de red incluyendo los nuevos elementos.

5. Elegir el o los modelos de appliance que mejor cumple las necesidades del nuevo diseño.

6. Desplegar los nuevos elementos. Típicamente este punto comprende las siguientes actividades:

   (a) Instalación de la solución en el bastidor del CPD (en adelante rack).

   (b) Conexión y configuración de las interfaces de gestión y de los elementos de red necesarios.

   (c) Instalación de los certificados SSL y configuración inicial de las funcionalidades WAF.

   (d) Preparación de un entorno de pruebas de forma similar a la indicada para WAF de tipo SaaS.

   (e) Cambio del direccionamiento de DNS o de IP según proceda.

   Una ya se ha validado que la solución web y el WAF funcionan adecuadamente, se procede a cambiar el direccionamiento ofrecido a nivel de red para que el tráfico de la aplicación web se enrute a través del WAF.

Si se comparan estas actividades con las equivalente de la solución WAF SaaS, esta solución es más compleja de desplegar y se deben tener en cuenta más factores. Esto es así debido a que al elegir esta solución se debe modificar la arquitectura de red y debemos tener en cuenta cómo WAF va a impactar a la plataforma web.

Por otro lado, dado que la administración y mantenimiento no están delegados en una empresa externa, debemos disponer de las personas adecuadas - con conocimiento, experiencia y tiempo - para administrar y operar el WAF.

Ventajas

Las soluciones WAF de tipo appliance son más personalizables que las soluciones WAF SaaS. Esto es así debido a que disponemos de unos dispositivos dedicados para nuestra plataforma web, y por lo tanto podemos crear reglas específicas que se adapten a nuestras necesidades.

Estas soluciones también cuenta como ventaja que toda la información está en nuestras instalaciones, lo cual nos permite tener mayor control de la información y puede simplificar el cumplimiento de ciertas regulaciones, como son el reglamento europeo RGDP o el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (en adelante PCI DSS, de sus siglas en inglés, Payment Card Industry Data Security Standard).

Una ventaja que comparten con las soluciones SaaS es su independencia del software utilizado en la plataforma web. Esto es así debido a que se despliegan como un elemento perimetral y no está conectado con la plataforma web a nivel de aplicación.

Igualmente, comparten las ventajas de independencia operacional; aunque en el caso de los WAF de appliance esta independencia es prácticamente obligatoria debido a que requiere un mayor conocimiento especializado tal como se verá en la siguiente sección.

Al igual que los WAF SaaS, en este tipo de soluciones requiere un servicio de mantenimiento o de suscripción; esto permite que no sea necesario mantenerse al día de las últimas vulnerabilidades y podamos abstraernos parcialmente de cómo proteger la plataforma, pues lo proveedores mantienen las reglas actualizadas como parte del servicio contratado.

Por último, las soluciones WAF de tipo appliance también nos permiten añadir algunos de los mecanismos de seguridad que no son propiamente de WAF que se han comentado anteriormente.

Desventajas

Tal como se ha anticipado, implementar y administrar este tipo de soluciones requiere de ciertos conocimientos en materia de seguridad, tanto acerca de las técnicas ofensivas más frecuentes, como los mecanismos necesarios para proteger la infraestructura.

Por otro lado, la capacidad de crear nuevas reglas en este tipo de entornos es limitada. Si bien se menciona como ventaja que estos WAF permiten mayor versatilidad que las soluciones SaaS, hay que tener en cuenta que todas las soluciones de este tipo hacen uso de licencias de software privativas, con las restricciones que este tipo de licencias implica: No es posible acceder al código fuente o modificarlo para implantar nuevas funcionalidades o solucionar fallos y el ciclo de vida del appliance es el que el fabricante impone.

Este problema se agrava en las soluciones de tipo appliance debido a que no es infrecuente que el fabricante imponga la renovación de hardware o software de forma agresiva y nos veamos obligados a realizar inversiones adicionales no planificadas.

Otra desventaja de este tipo de soluciones es su elevado coste económico. Si bien el coste recurrente suele ser inferior a las soluciones SaaS equivalentes, sigue siendo un coste elevado; por otro lado, las

soluciones WAF de tipo appliance requieren la compra de los dispositivos, lo que supone un mayor coste de inversión inicial que en las soluciones SaaS.

Al igual que sucede con las soluciones SaaS, este tipo de soluciones no están al alcance de pequeñas o medianas empresas o de particulares.

1.2 Soluciones WAF de software libre

Dentro de las soluciones WAF de software libre, se han evaluado las siguientes:

- IronBee[24].
- WebCastellum[25].
- RAPTOR[26].
- NAXSI[27].
- OpenWAF[28].
- FreeWAF[29].
- Shadow Daemon[30].
- AQTRONiX WebKnight[31].
- Vulture[32].
- ModSecurity [33].

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.

También destacan OpenWAF y FreeWAF (también conocido como *lua-resty-waf*) debido a que tienen un planteamiento y unas funcionalidades muy interesantes.

Éstas y las demás soluciones se evaluarán en la posterior fase de análisis.

Modo de licenciamiento y coste

En la tabla resumen de WAF de software libre podemos comparar las diferentes soluciones:

Solución	Licencia	Coste	Soporte
IronBee	Apache License 2.0	Gratuito	No
WebCastellum	Eclipse Public License	Gratuito	No
RAPTOR	GNU GPL 2.0	Gratuito	No
NAXSI	GNU GPL 3.0	Gratuito	Comunidad
OpenWAF	BSD license	Gratuito	Comunidad
FreeWAF	GNU GPL 3.0	Gratuito	Comunidad
Shadow Daemon	GNU GPL 2.0	Gratuito	Comunidad
WebKnight	GNU GPL	145 USD / año	Proveedor
Vulture	No se especifica	Gratuito	Proveedor(de pago)
ModSecurity	Apache License 2.0	Gratuito y de pago*	Comunidad o Proveedor

Cuadro 1.3: Modos de licenciamiento y costes de WAF de software libre

* Modsecurity ofrece la solución WAF de forma gratuita, que cuenta con soporte por parte de la comunidad, y una versión de pago por 495 USD al año que ofrece soporte por parte de Trustware[34] y un conjunto mayor de reglas [35].

Implementación y operación

Las soluciones WAF de software libre se implementan, en la mayoría de los casos, como módulos adicionales al servidor de aplicación web, ya sea Apache HTTP Server[36] (en adelante, Apache), Nginx[37], Internet Information Services[38], etc.

Esto implica que el WAF debe ejecutarse como parte del servicio web y su configuración y operación depende del administrador de la plataforma web.

Si en los WAF de tipo appliance se ha visto que las tareas de implantación tienen cierta complejidad en lo relativo a analizar la plataforma web desde un punto de vista de red, en el caso de los WAF que se ejecutan como parte del servicio web la complejidad radica en que el WAF debe integrarse dentro de la plataforma web.

Este tipo de WAF requiere que se revise el dimensionamiento de la plataforma web debido a que consumen recursos del servidor y puede afectar a su rendimiento.

Estas son las tareas que se deben abordar de forma genérica a la hora de implantar un WAF de software libre:

1. Evaluar la plataforma web actual e identificar qué soluciones WAF son compatibles con el servicio web.
2. Desplegar un un entorno de pruebas equivalente a la plataforma web actual o prueba de concepto (en adelante PoC, de sus siglas en inglés, Proof of concept).
3. Desplegar el WAF en el entorno de pruebas.
4. Realizar pruebas exhaustivas sobre el nuevo entorno, especialmente pruebas funcionales y de rendimiento.
5. Evaluar el impacto del WAF, entre otros se debe evaluar errores en la lógica de aplicación, latencia que añade, aumento en el consumo de recursos o cómo afecta al throughput soportado por la plataforma.

   Tradicionalmente este punto y el anterior se deberán ejecutar de forma reiterativa hasta que los resultados sean concluyentes y la nueva configuración se considere suficientemente robusta como para desplegarla en producción.
6. Desplegar el WAF en el entorno de producción (si la plataforma lo permite, se recomienda realizar el despliegue de forma escalonada) y realizar un conjunto de pruebas similar a las realizadas en el entorno de pruebas.

Aunque en este tipo de soluciones se han enumerado menos pasos que en las soluciones anteriores, esto es debido a que las tareas dependen en gran medida del software y la plataforma elegidos, por lo que las actividades se han identificado de forma más general.

Ventajas

Los WAF de software libre son más económicos que las alternativas privativas. Si bien es cierto que esto no quiere decir que sean gratis, pues requieren personas que los administren y consumen una serie de recursos de la plataforma web.

Pero, aun eligiendo alguna de las opciones de pago y con soporte como por ejemplo ModSecurity, el coste en licencias es muy inferior a las otros modelos privativos.

Debido al tipo de licenciamiento, estas soluciones se distribuyen como software libre, con todas las ventajas inherentes a este tipo de software entre las que destaca desde un punto de vista funcional el acceso al código fuente y la capacidad de modificarlo de acuerdo a nuestras necesidades entre otras. Está fuera del alcance del documento evaluar las ventajas generales del software libre frente a otro tipo de licencias.

No en todos los casos, pero en la mayoría de las soluciones analizadas el equipo de desarrollo es un conjunto de individuos pertenecientes a distintos ámbitos o empresas, por lo que se elimina la estricta dependencia del proveedor. Si bien este modelo tiene sus ventajas e inconvenientes, lo cierto es que se elimina la dependencia de realizar una migración del software si se considera conveniente (por ejemplo, para alinear dicha migración según una planificación propia en lugar de una planificación impuesta).

Se puede pues decir que estas soluciones son más adaptables a las necesidades específicas de cada entorno.

Desventajas

Este tipo de soluciones son más difíciles de implementar y de mantener. El hecho de que estén integradas como parte de la plataforma web hace que sea complejo diferenciar los roles del administrador de la plataforma web del administrador del WAF. Por lo tanto, la misma persona debe tener conocimiento de ambas plataformas y ambos campos del conocimiento, lo cual no es común y puede provocar en errores de configuración de alguna de las plataformas.

Precisamente debido a la gran dependencia existente entre el software WAF y de la plataforma web, es necesario analizar en detalle las configuraciones y las reglas que se habilitarán, pues el proceso de depuración de errores es más complejo y los fallos son más difíciles de identificar y solucionar.

Las actividades de actualización de componentes y migraciones de software son así mismo más complejas, pues se deben actualizar o migrar ambas plataformas conjuntamente.

Por otro lado, el soporte en este tipo de soluciones puede ser de menor calidad que en las alternativas privativas. Al fin y al cabo en muchos casos el soporte depende de la comunidad y si se elige un WAF que tenga una comunidad reducida, es probable que no se obtenga una respuesta inmediata. Por supuesto, si se elige una solución con soporte o se contrata un servicio de consultoría, se puede paliar esta desventaja. Si se trata de un entorno de producción en el que el tiempo de caída del servicio es crítico, se recomienda contratar algún servicio de soporte o consultoría.

Requisitos y casos de uso

2.1 Requisitos candidatos

En primer lugar se identifican los requisitos que se intentarán cumplir con la solución propuesta.

Se agrupan los requisitos según estén más orientados al componente WAF o al componente de TLS.

Requisitos orientados principalmente al componente WAF:

R1. La solución debe poder ejecutarse en un sistema operativo o máquina independiente de la plataforma de la aplicación web con el objetivo de garantizar independencia en las tareas de administración y permitir aplicar un modelo RBAC.

R2. La solución debe disponer de un conjunto básico de políticas de auditoría o bloqueo que permitan proteger la aplicación web frente a los ataques más comunes.

R3. La plataforma debe permitir implementar parches virtuales frente a ataques conocidos.

R4. La solución debe permitir la elaboración de reglas personalizadas según las necesidades específicas de la plataforma del cliente.

R5. La plataforma debe ser compatible con el modelo de licencias de *software libre[39]* tipo Licencia Pública General de GNU (en adelánte GPL, de sus siglas en inglés GNU General Public License[40, Licencia GPL]) o Licencia Pública General Reducida de GNU (en adelánte LGPL, de sus siglas en inglés GNU Lesser General Public License[41, Licencia LGPL]).

R6. La plataforma debe generar logs de seguridad exportables a soluciones externas de gestión de información y eventos de seguridad (en adelante SIEM de sus siglas en inglés, Security information and event management).

A continuación se recogen los requisitos asociados al componente de TLS:

R1. La solución debe poder participar en la negociación TLS, presentando certificados confiables a los clientes.

R2. La solución deber poder gestionar los certificados presentados a los clientes incluyendo soporte a la extensión SNI de TLS.

R3. La plataforma debe soportar TLS versión 1.3, HTTP/2 y otros elementos incluidos en las *buenas prácticas de TLS[42]*.

R4. Debe permitir aplicar soluciones de SSL offloading, entre el WAF y los frontales de la plataforma web, o permitir cifrado punto a punto.

En caso de utilizar la funcionalidad de SSL offloading:

a) Esta opción es recomendable en entornos controlados en los que prima el rendimiento.

b) Las comunicación entre el WAF y la plataforma web debe permitir tráfico HTTP.

En caso de cifrado punto a punto:

a) Esta opción es recomendable en las soluciones en las que prime la seguridad o en aquellos escenarios en los que no se tenga el control de elementos intermedios, como por ejemplo en entornos cloud o multi-datacenter.

b) Las comunicación entre el WAF y la plataforma web debe permitir tráfico HTTPS.

c) El WAF debe confiar en la CA que firma los certificados de la plataforma web o, alternativamente, en los certificados hoja.

2.2 Identificación de actores

Se han identificado los siguientes actores.

- **Cliente**. Se utiliza este término para referirse al cliente web que consume los servicios HTTP o HTTPS.
- **Atacante**. Se trata de un tipo de cliente malintencionado.
- **Plataforma web**. Se considera toda la infraestructura necesaria para servir los contenidos web. En esta infraestructura no se incluyen los elementos desarrollados en el presente proyecto.
- **Autoridad de certificación** (en adelante CA). Es el elemento encargado de firmar los certificados TLS. El cliente debe confiar en la CA o en los certificados hoja alternativamente. En caso de cifrado punto a punto el WAF deberá confiar en los certificados presentados por la plataforma web.
- **Sistema de virtualización o gestión de contenedores**. Es la infrastructura sobre la que se desplegará la solución WAF. Inicialmente se considera una solución de gestión de contenedores como [43].

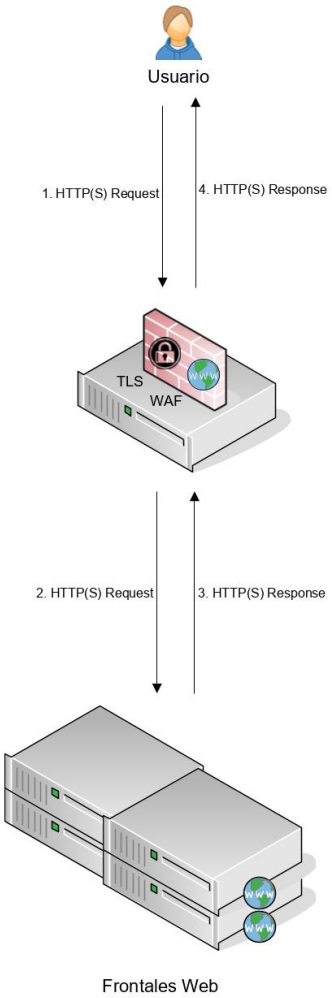
2.3 Casos de uso

Estos son los casos identificados.

1. Caso de uso: Petición identificada como legítima de recurso web.

   - Actores: Cliente, plataforma web.
   - Descripción: Se trata del caso de uso que sucede con mayor frecuencia, pues representa las peticiones legítimas de clientes a la plataforma web. Podemos desglosar las comunicaciones en los siguientes pasos:
     (a) El cliente realiza una petición web a nuestra solución.
     (b) Nuestra solución evalúa la petición, la considera legítima y la envía a la plataforma web.
     (c) La plataforma web recibe la petición y envía una respuesta a la plataforma WAF.
     (d) La plataforma WAF recibe la respuesta y se la envía al cliente.

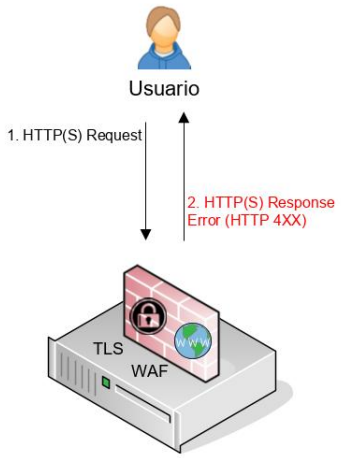
     Se debe tener en cuenta que en este caso de uso se incluyen peticiones legítimas y falsos negativos cuando el WAF falla al detectar un ataque.
   - Diagrama:



2. Caso de uso: Petición identificada como no legítima de recurso web.

   - Actores: Atacante.
   - Descripción: Este caso de uso se dará siempre que nuestra plataforma reciba una petición y la considere un ataque. En este caso podemos identificar los siguientes pasos:
     (a) El atacante realiza una petición web a nuestra solución.
     (b) Nuestra solución recibe la petición, la evalúa y, considerándola como ataque, envía un mensaje de error al atacante.

     A tener en cuenta que nuestra plataforma ha considerado que el cliente es un atacante y este caso de uso se dará tanto en ataque reales como con falsos positivos (cuando se diagnostica como ataque a una petición legítima).
   - Diagrama:

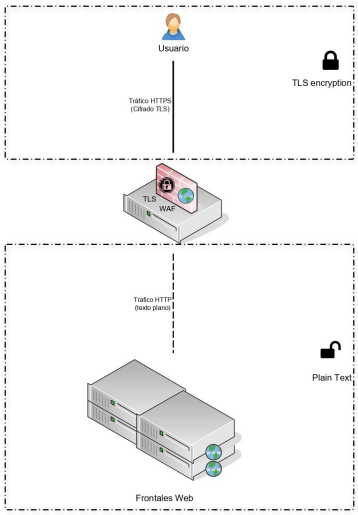


3. Caso de uso: Petición HTTPS en un entorno con TLS offloading.

    - Actores: Cliente, plataforma web.
    - Descripción: Se trata de una derivada del Caso de primer caso de uso. En este escenario las peticiones HTTPS realizadas por el cliente se envían sin cifrar (o en texto plano) a la plataforma web.

      Con ello se consigue reducir la carga que debe soportar la plataforma web y optimizar sus recursos.

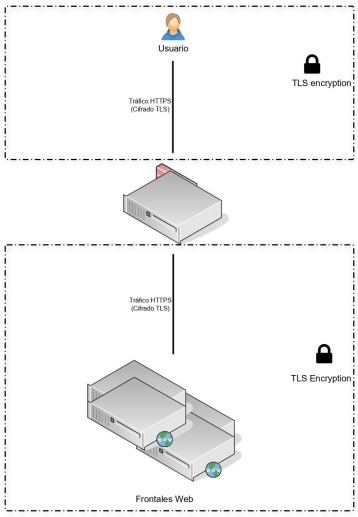
      Sin embargo, también se aumenta el riesgo a un ataque en caso de que un potencial atacante tuviese acceso a la infraestructura situada entre la solución WAF y la plataforma web. Es por ello que esta solución sólo se recomienda en escenarios en los que los elementos situados entre ambos estén protegidos y monitorizados adecuadamente.
    - Diagrama:



4. Caso de uso: Petición HTTPS con cifrado punto a punto.

    - Actores: Cliente, plataforma web.
    - Descripción: Se trata de un caso de uso alternativo al anterior. En este escenario se mantienen las comunicaciones cifradas también entre el WAF y la plataforma web, con lo que se consigue el cifrado punto a punto.

      Para ello se establecen dos túneles TLS: El primero entre el cliente y la plataforma WAF y un segundo túnel entre el WAF y la plataforma web.
    - Diagrama:



5. Caso de uso: Petición de validación y firma de certificado TLS a una CA de confianza.

   - Actores: Certification Authority.
   - Descripción: Este caso de uso tiene como objetivo obtener un certificado digitalmente por una CA que sea de confianza para el cliente. Se puede dividir en dos flujos similares.

     El primer flujo se da entre el WAF y la CA siguiendo los siguientes pasos:

     (a) El WAF - o un administrador del WAF - genera un certificado CSR [44, Wikipedia] asociado a su clave privada que siga el *estándar X.509 v3 [45, IETF 5280]*.
     (b) Se envía el certificado a la CA solicitando que ésta lo firme.
     (c) La CA valida que la petición es legítima y firma el certificado con su clave raíz o, alternativamente, una clave intermedia.
     (d) La CA envía el certificado firmado digitalmente el WAF.
     (e) Una vez el WAF disponga de dicho certificado, este puede presentar sus servicios web a los clientes y estos podrán validar al WAF durante la negociación TLS si cuentan confían en el certificado raíz de la CA o en la jerarquía de certificados.

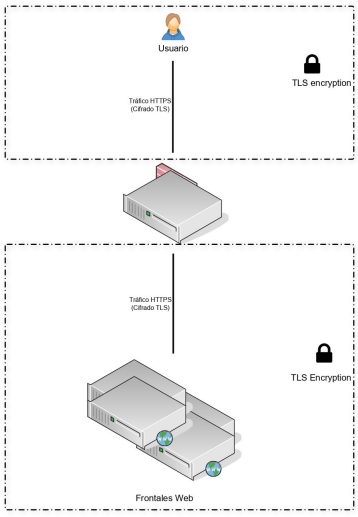
     El segundo flujo es opcional. Se trataría de un flujo similar al descrito para el WAF pero el solicitante de certificado sería la plataforma web en este caso.

     Se considera que es opcional debido a que la plataforma web sólo estará expuesta al WAF y se podría crear una relación de confianza sin necesidad de hacer uso de una CA externa.

     No obstante, dado que actualmente obtener este tipo de certificados no tiene un coste económico, y que tampoco debería tener un impacto operacional significado, se recomienda seguir el mismo proceso que para el WAF.

     En nuestro caso, se intentará hacer uso del protocolo ACME (Automatic Certificate Management Environment[46, Estándar ACME]) mediante *Let's Encrypt [47]* con el objetivo de automatizar las actividades de creación y renovado de certificados.

   - Diagrama:



Acrónimos

ACME Automatic Certificate Management Environment[46, Estándar ACME]. 18

CA Certification Authority. 18

CDN Content Delivery Network. 3

DBF Database Firewall. 6

DoS Denial-of-service. 3

EV Extended Validation. 4

GPL GNU General Public License[40, Licencia GPL]. 12

LGPL GNU Lesser General Public License[41, Licencia LGPL]. 12

PCI DSS Payment Card Industry Data Security Standard. 8

PoC Proof of concept. 10

RBAC role-based access control. 4

RGDP Reglamento General de Protección de Datos. 8

SaaS Software as a Service. 2

SIEM Security information and event management. 12

SNI Server Name Indication[48, Wikipedia]. 4, 12

WAF Web Application Firewall. 2

Glosario

Atacante El atacante es un individuo u organización que intenta obtener el control de un sistema informático para utilizarlo con fines maliciosos, robo de información o de hacer daño a su objetivo. [49, Wikipedia]. 13, 15

CA En criptografía, las expresiones autoridad de certificación, o certificadora, o certificante, o las siglas AC o CA (por la denominación en idioma inglés Certification Authority), señalan a una entidad de confianza, responsable de emitir y revocar los certificados, utilizando en ellos la firma electrónica, para lo cual se emplea la criptografía de clave pública. [50, Wikipedia]. 13

Throughput La tasa de transferencia efectiva (en inglés throughput) es el volumen de trabajo o de información neto que fluye a través de un sistema, como puede ser una red de computadoras. [51, Wikipedia]. 3

Bibliografía

[1] *Estándar del modelo OSI, del inglés* Open Systems Interconnection model. *ISO/IEC standard 7498-1:1994*
. URL: http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip.

[2] *OWASP Best Practices: Use of Web Application Firewalls*
. URL: https://www.owasp.org/index.php/Category:OWASP_Best_Practices:_Use_of_Web_Application_Firewalls.

[3] *Software propietario o privativo*
. URL: https://www.definicionabc.com/tecnologia/software-propietario.php.

[4] *Cloudflare WAF*
. URL: https://www.cloudflare.com/waf/.

[5] *Cloudflare*
. URL: https://www.cloudflare.com/.

[6] *Kona WAF*
. URL: https://www.akamai.com/uk/en/resources/waf.jsp.

[7] *Akamai*
. URL: https://www.akamai.com/es/es/.

[8] *Incapsula Web Application Firewall*
. URL: https://www.incapsula.com/website-security/web-application-firewall.html.

[9] *CDN Cost Comparison - Global Traffic Monthly Plans*
. URL: https://www.cdn77.com/compare-cdn-providers.

[10] *Imperva Incapsula. Pricing and plans*
. URL: https://www.incapsula.com/pricing-and-plans.html.

[11] *Imperva WAF Gateway*
. URL: https://www.imperva.com/products/on-premises-waf/.

[12] *FortiWeb: Web Application Firewall*
. URL: https://www.fortinet.com/products/web-application-firewall/fortiweb.html.

[13] *Fortinet*
. URL: https://www.fortinet.com/.

[14] *Precio de appliance Imperva, modelo X2020*
. URL: https://www.comparitech.com/net-admin/best-web-application-firewall/.

[15] *Precio de appliance Imperva, modelo X2010*
. URL: https://searchsecurity.techtarget.com/feature/Comparing-the-best-Web-application-firewalls-in-the-industry.

[16] *Precio de licencias anuales de Imperva, modelo X2010*
. URL: https://www.globenetstore.com/shop/search.aspx?search=SS-WAF-X21-SL.

[17] *Precio de licencias anuales de Imperva, modelos X2500 y X4500 (fichero de Microsoft Excel)*
. URL: https://cdn2.hubspot.net/hubfs/2539908/Imperva%20Price%20List.xlsx.

[18] *SecureSphere WAF AV1000 Gateway for AWS*
. URL: https://aws.amazon.com/marketplace/pp/B00UAWMZ1U?qid=1555322432672.

[19] *SecureSphere WAF AV2500 Gateway for AWS*
. URL: https://aws.amazon.com/marketplace/pp/B00UAWN0FU?qid=1555323193972.

[20] *AVFirewalls.com. Fortinet FortiWeb 100D*
. URL: http://www.avfirewalls.com/FortiWeb-100D.asp.

[21] *AVFirewalls.com. Fortinet FortiWeb 400D*
. URL: http://www.avfirewalls.com/FortiWeb-400D.asp.

[22] *Real Data Solutions. Fortinet FortiWeb 600D*
. URL: http://realdatasolutions.net/index.php?id_product=220&controller=product.

[23] *AWS Marketplace. Fortinet FortiWeb Web Application Firewall WAF VM*
. URL: https://aws.amazon.com/marketplace/pp/B00L9JODAE?ref=_ptnr_ftnt_web_fortiweb.

[24] *Página oficial de IronBee*
. URL: https://github.com/ironbee/ironbee.

[25] *Repositorio de código oficial de WebCastellum*
. URL: https://sourceforge.net/p/webcastellum/code/HEAD/tree/.

[26] *Repositorio de código oficial de Raptor WAF*
. URL: https://github.com/CoolerVoid/raptor_waf.

[27] *Página oficial de NAXSI*
. URL: https://github.com/nbs-system/naxsi.

[28] *Página oficial de OpenWAF*
. URL: https://github.com/titansec/OpenWAF.

[29] *Blog oficial de FreeWAF / lua-resty-waf*
. URL: https://www.cryptobells.com/reintroducing-lua-resty-waf/.

[30] *Página oficial de Shadow Daemon*
. URL: https://shadowd.zecure.org/overview/introduction/.

[31] *Página oficial de AQTRONiX WebKnight*
. URL: https://www.aqtronix.com/?PageID=99.

[32] *Página oficial de Vulture WAF*
. URL: https://www.vultureproject.org/.

[33] *Página oficial de Modsecurity*
. URL: https://www.modsecurity.org/.

[34] *Página oficial de Trustware*
. URL: https://www.trustwave.com/en-us/.

[35] *Modalidades de soporte de Modsecurity*
. URL: https://www.modsecurity.org/help.html.

[36] *Página oficial del servidor web Apache HTTP Server*
. URL: https://httpd.apache.org/.

[37] *Página oficial del servidor web Nginx*
. URL: http://nginx.org/.

[38] *Página oficial del servidor web Microsoft Internet Information Services*
. URL: https://www.iis.net/.

[39] *¿Qué es el software libre?*
. URL: https://www.gnu.org/philosophy/free-sw.es.html.

[40] *GNU General Public License*
. URL: https://www.gnu.org/licenses/gpl-3.0.html.

[41] *GNU Lesser General Public License*
. URL: https://www.gnu.org/licenses/lgpl-3.0.html.

[42] *SSL and TLS Deployment Best Practices*
. URL: https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices.

[43] *Página oficial de Docker*
. URL: https://www.docker.com/.

[44] Wikipedia. *Certificate signing request*
. URL: https://en.wikipedia.org/wiki/Certificate_signing_request.

[45] Internet Engineering Task Force (IETF). *Estándar RFC5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*
. URL: https://tools.ietf.org/rfc/rfc5280.txt.

[46] Internet Engineering Task Force (IETF). *Estándar RFC8555. Automatic Certificate Management Environment (ACME)*
. URL: https://tools.ietf.org/html/rfc8555.

[47] *Página oficial de Let's Encrypt*
. URL: https://letsencrypt.org/.

[48] Wikipedia. *Server Name Indication*
. URL: https://es.wikipedia.org/wiki/Server_Name_Indication.

[49] Wikipedia. *Ciberataque*
. URL: https://es.wikipedia.org/wiki/Ciberataque.

[50] Wikipedia. *Autoridad de certificación*
. URL: https://es.wikipedia.org/wiki/Autoridad_de_certificaci%C3%B3n.

[51] Wikipedia. *Throughput*
. URL: https://es.wikipedia.org/wiki/Throughput.