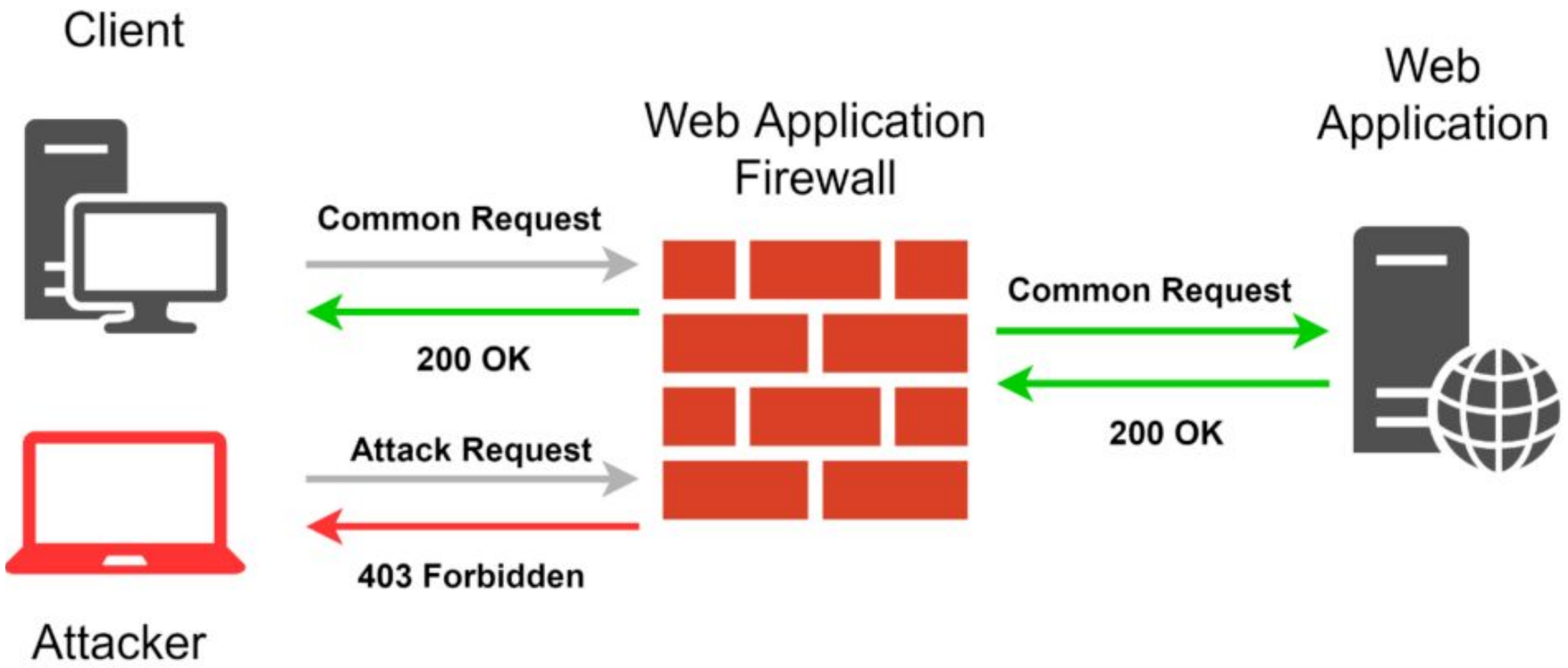
THE BRIDGE

CYBER SECURITY

Web Application Firewall (WAF)

WAF - Web Application Firewall

- Un **Web Application Firewall (WAF)** protege de múltiples ataques al servidor de aplicaciones web en el **backend**.
- La función del **WAF** es garantizar la seguridad del servidor web mediante el análisis de paquetes de petición **HTTP** / **HTTPS** y modelos de tráfico.
- El **WAF** examina cada petición enviada al servidor, antes de que llegue a la aplicación, para asegurarse de que cumple con las reglas del firewall.



https://www.section.io/engineering-education/web-application-firewall-bot-mitigation-comparison/

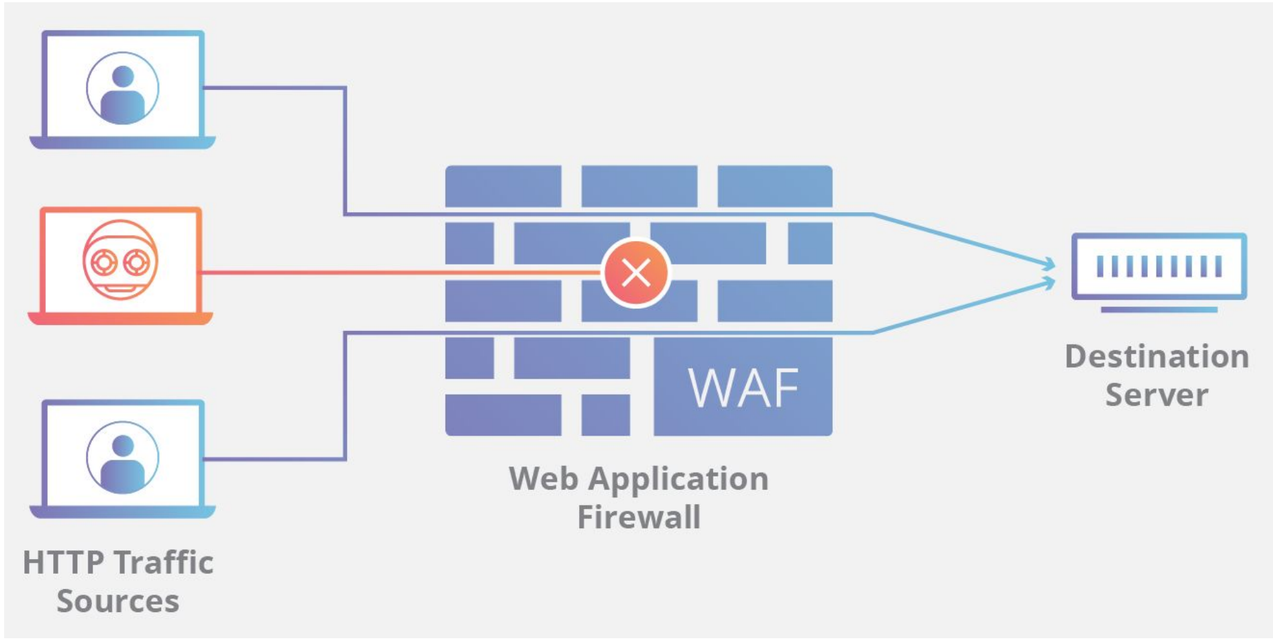
WAF - Web Application Firewall

- **Funcionamiento**
  - Los pasos para procesar el tráfico entrante son los mismos en la mayoría de los Firewalls y hay cinco etapas:
    - Analizando el paquete HTTP que vino del cliente.
    - La elección de las reglas depende del tipo de parámetro de entrada.
    - Normalización de datos a una forma adecuada para el análisis.
    - Aplicación de la regla de detección.
    - Tomar una decisión sobre la nocividad del paquete. En este punto, WAF finaliza la conexión o pasa al nivel de aplicación.
  - Para el tráfico HTTPS es necesario instalar en el WAF el certificado del servidor web con la clave privada correspondiente.

- **WAF de lista negra vs lista blanca**
  - Un firewall de aplicaciones web que opera basado en una **lista negra** (modelo de seguridad negativo) protege contra ataques conocidos.

  - Basado en una **lista blanca** (modelo de seguridad positivo) solo admite tráfico que ha sido aprobado previamente.

  - Tanto las **listas negras** como las **listas blancas** tienen sus ventajas e inconvenientes, por lo que muchos Firewalls ofrecen un modelo de seguridad híbrido, que implementa ambos.



https://www.cloudflare.com/es-es/learning/ddos/glossary/web-application-firewall-waf/

Tipos de implementaciones

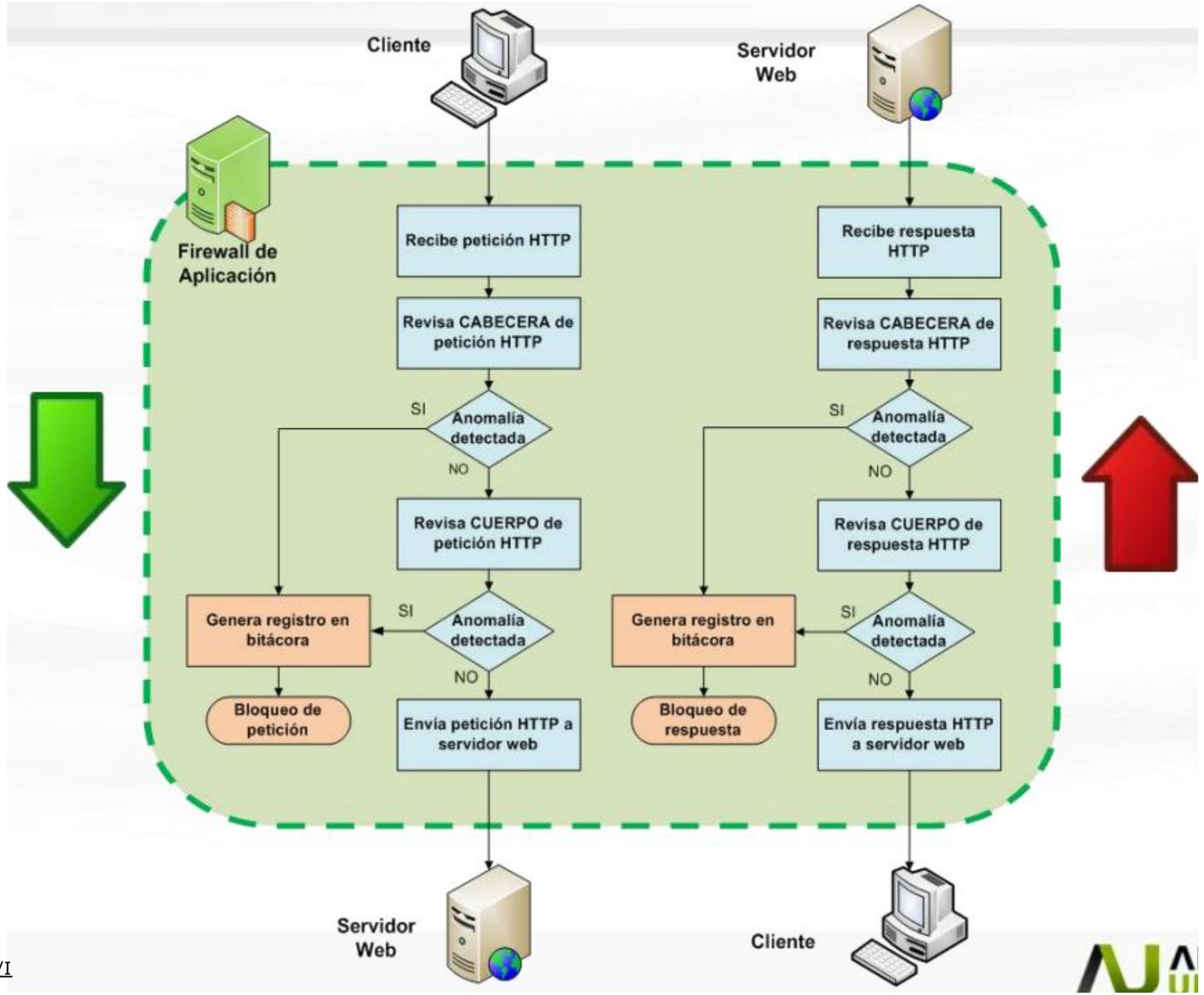
- **Un Web Application Firewall se puede implementar de tres maneras diferentes, cada una con sus propios beneficios y defectos:**

  - **Basado en red**
    - Generalmente está soportado en hardware.
    - Como se instalan localmente, minimizan la latencia, pero al estar basados en red son la opción más costosa y también requieren el almacenamiento y mantenimiento de equipos físicos.

  - **Basado en host**
    - Puede integrarse completamente en el software de una aplicación.
    - Esta solución es menos costosa que una solución basada en redes y ofrece más personalización.
    - La desventaja de un WAF basado en host es el consumo de recursos del servidor local, la complejidad de la implementación y los costos de mantenimiento. Estos componentes generalmente requieren tiempo de ingeniería y pueden ser costosos.

  - **Basados en la nube**
    - Ofrecen una opción asequible que es muy fácil de implementar.
    - Por lo general, ofrecen una instalación llave en mano que es tan simple como un cambio en el DNS para redirigir el tráfico.
    - Tienen un costo inicial mínimo, ya que los usuarios pagan mensualmente o anualmente por la seguridad como servicio.
    - Se actualiza constantemente para proteger contra las amenazas más recientes sin ningún trabajo o costo adicional para el usuario.

Funcionamiento de un WAF



https://adminunam.seguridad.unam.mx/2014/sites/adminunam.seguridad.unam.mx/files/Implementaci%C3%B3n%20de%20ModSecurity%20-%20AdminUNAM%202012.pdf

Herramientas

1. ModSecurity
2. IronBee
3. NAXSI
4. WebKnight
5. Shadow Daemon
6. Lua-resty-waf
7. Vulture

Herramientas opensource

https://serverguy.com/security/open-source-web-application-firewall/

Source: Gartner (August 2022)

Herramientas comerciales

https://ww.cloudflare.com/es-es/lp/ppc/gartner-magic-quadrant-waap-2022/


THE
BRIDGE