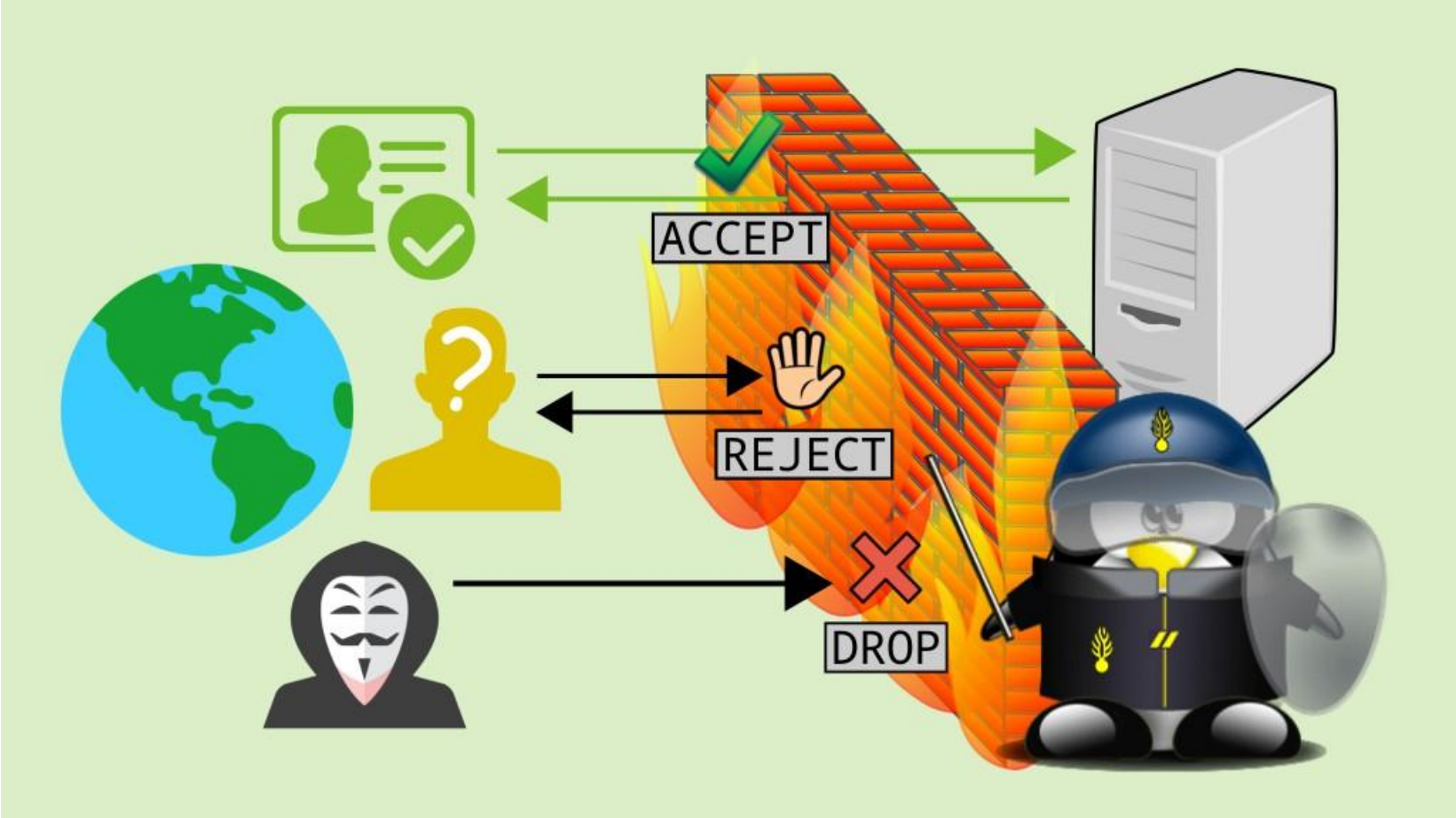
Herramientas de seguridad de la información dentro de una arquitectura de soluciones

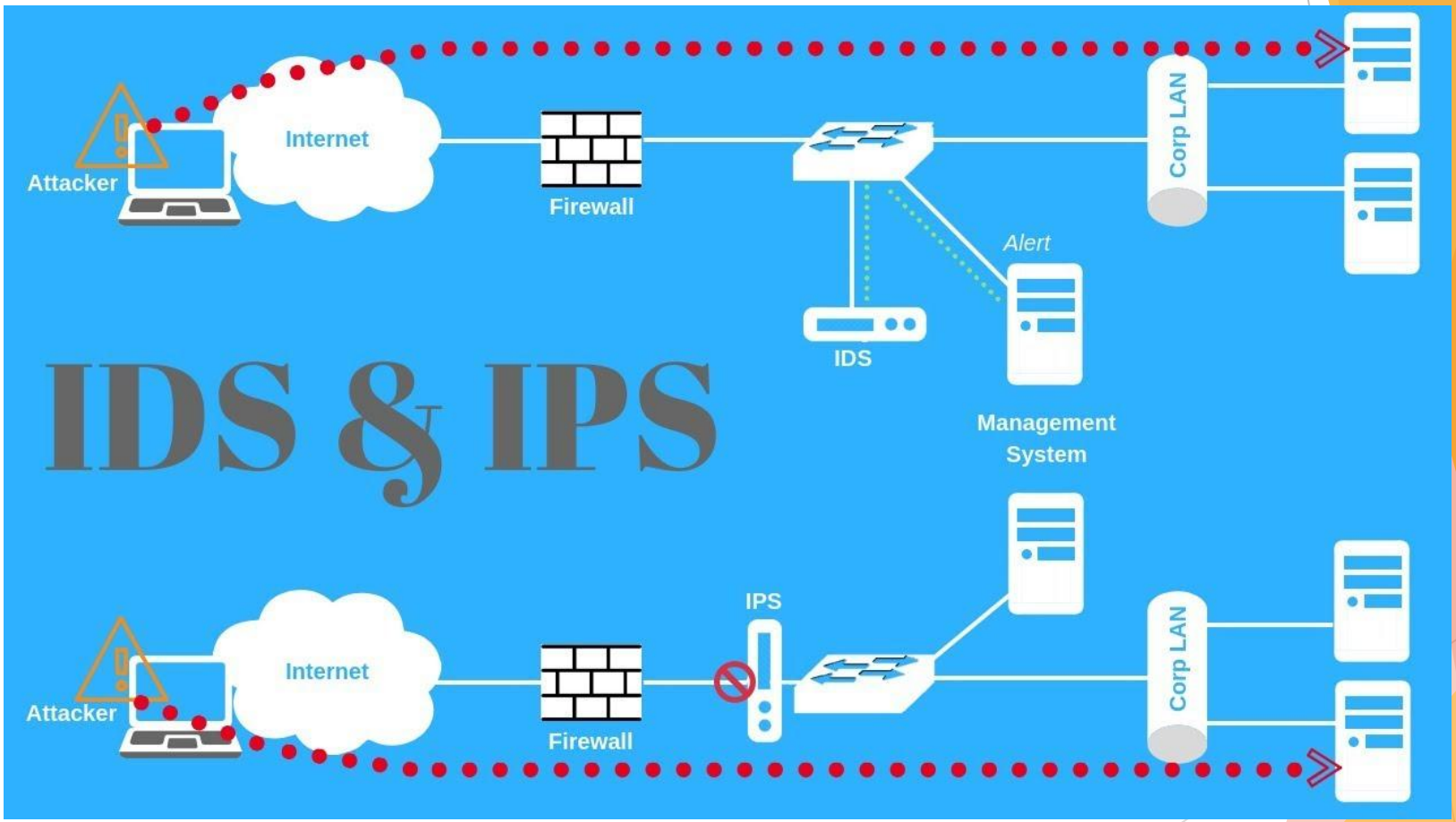
ADR – UTN – FRBA -2023

Firewall



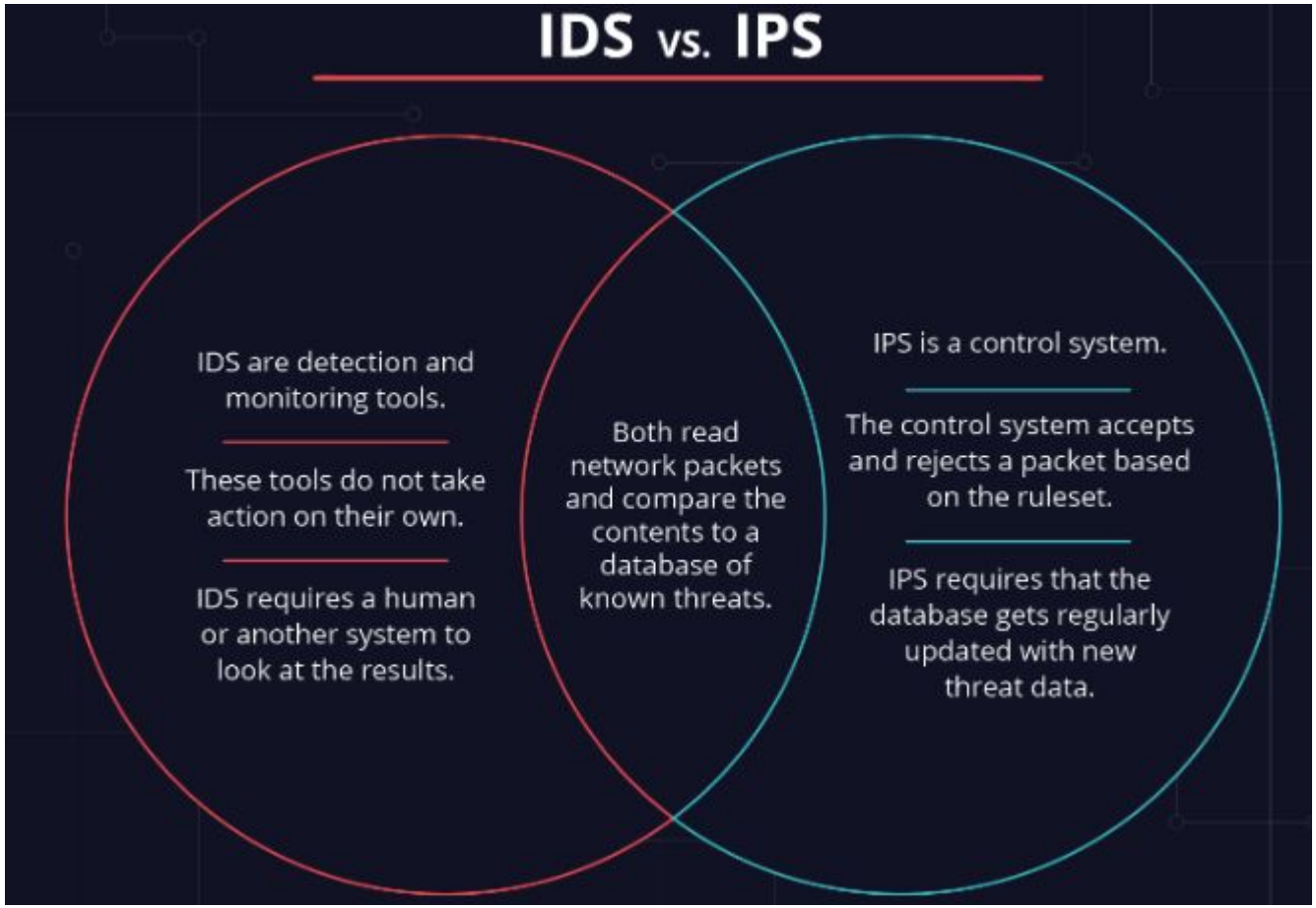
Más información relacionada:
https://www.tecnologia-informatica.com/que-es-firewall-como-funciona-tipos-firewall/

IDS - Intrusion detection system IPS - Intrusion protection system



Más información relacionada:
https://www.juniper.net/uk/en/products-services/what-is/ids-ips/

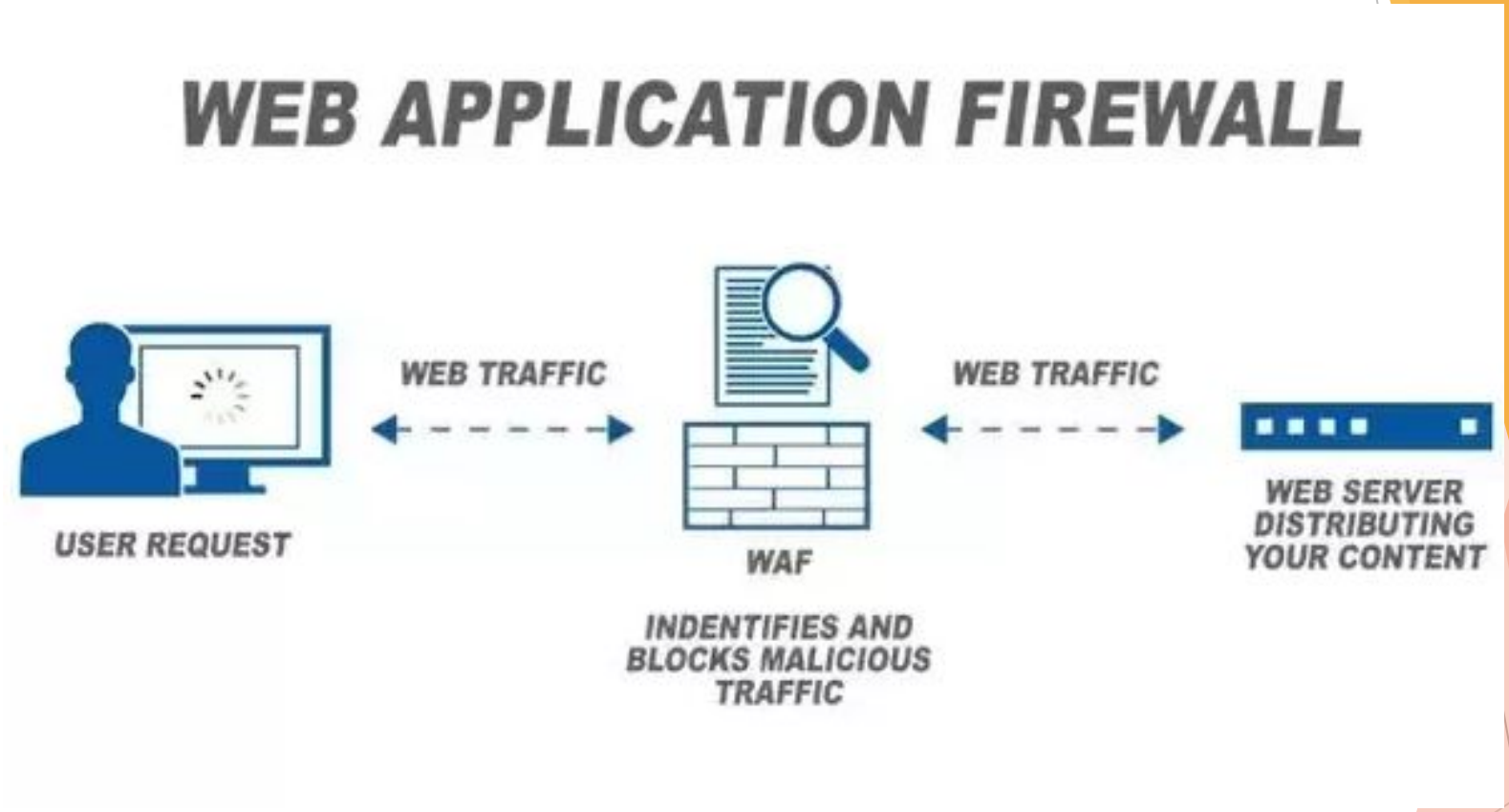
IDS & IPS



Más información relacionada:

https://www.quora.com/What-are-IDS-and-IPS-What-is-the-difference-between-them

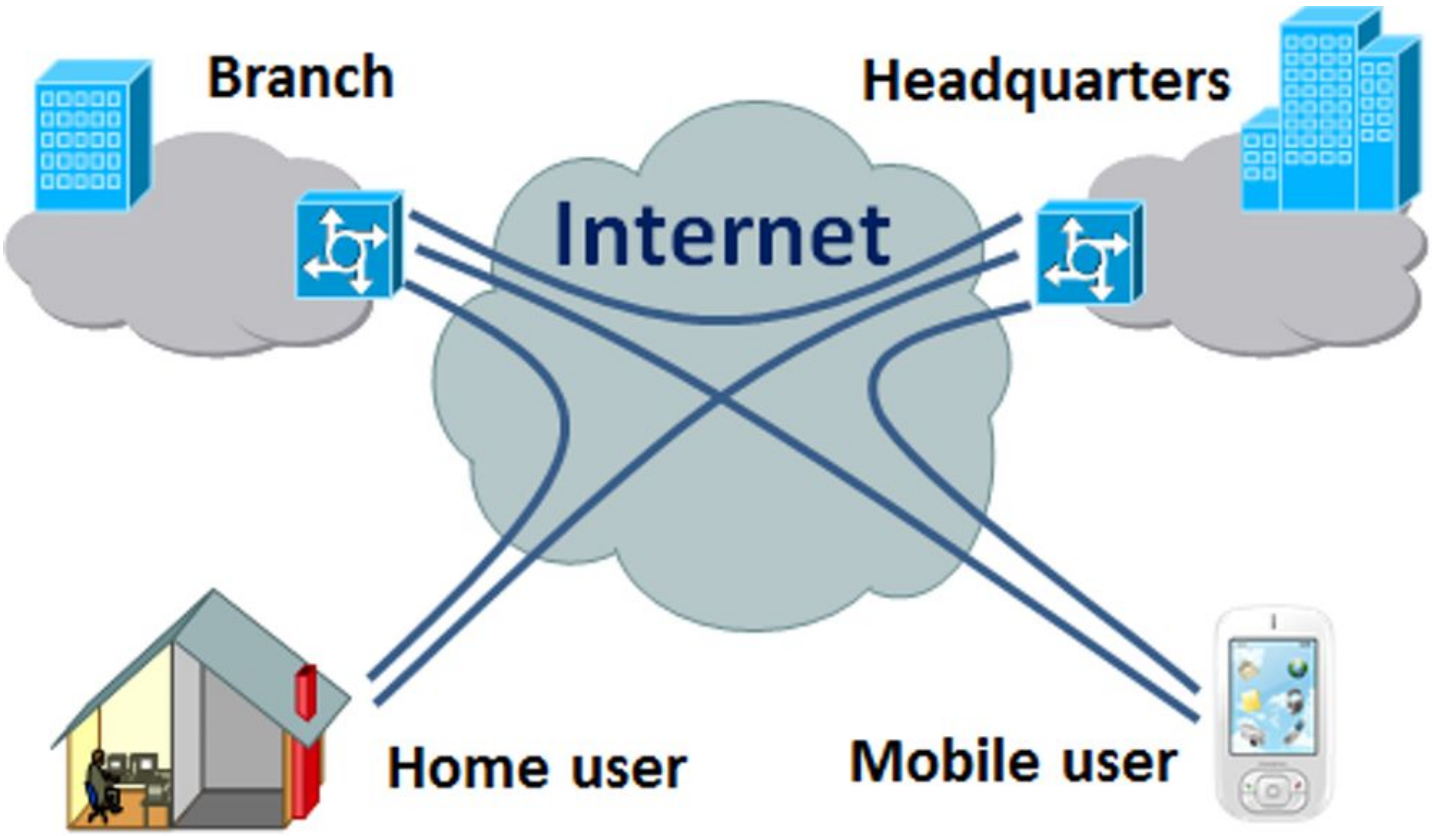
WAF - Web Application Firewall



Más información relacionada:

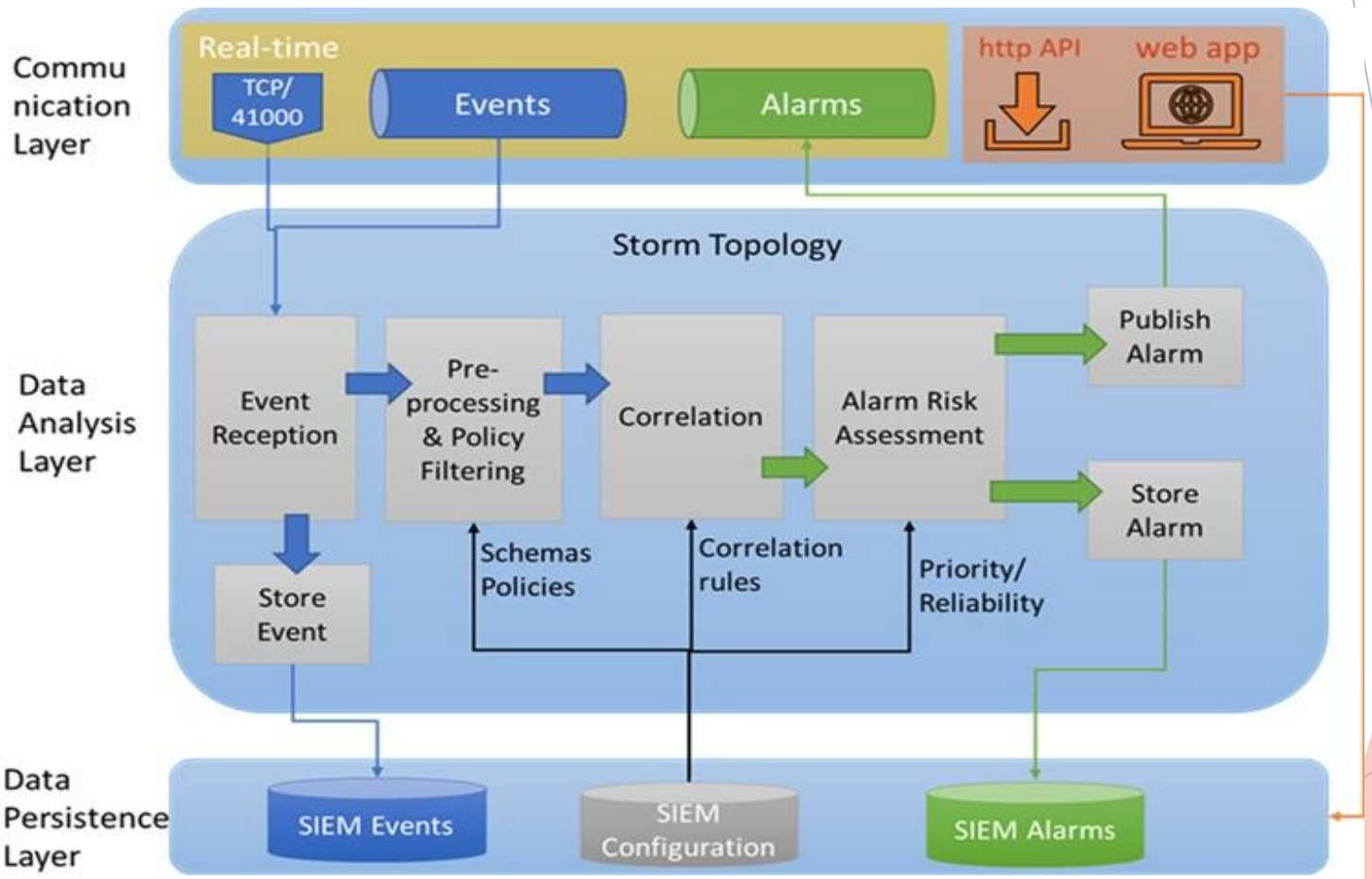
https://www.cybercureme.com/what-is-a-web-application-firewall-waf-different-types-of-waf/

VPN - Virtual private network



Más información relacionada:

SIEM - Security information and event management



Más información relacionada:

https://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM

Actualizaciones de seguridad

En toda solución informática intervienen elementos de hardware, software y comunicaciones. Todos ellos son en última instancia, controlados por algún componente de software.

Por ejemplo:

- Firmware
- Sistemas operativos
- Bases de datos
- Aplicaciones

Cualquiera de estos sistemas son susceptibles de presentar fallos de seguridad por tanto resulta clave en cualquier solución controlar el estado de TODOS los sistemas involucrados en la misma de manera que se encuentren actualizados es sus versiones de manera que impida a cualquier atacante “explotar” posibles vulnerabilidades conocidas dentro de versiones de software que no hayan sido actualizadas.

Buscamos entonces:

- Reducir la exposición a ciberataques.
- Eliminar la pérdida de productividad por salidas de servicio.
- Proteger los datos.
- Proteger a otros sistemas de la posible explotación propia para daño a terceros.

Más información relacionada:

https://www.blackstratus.com/what-is-a-security-patch/

¿Por qué todo ésto es importante?

Porque toda solución deberá contener, en al menos alguno de sus elementos, las características de:

- Disponibilidad
- Confidencialidad
- Integridad

La disponibilidad, ¿no la resguarda la escalabilidad y la redundancia?
Si, pero solo en los casos de tráfico bien intencionado. Cuando hablamos de tráfico NO genuino, la escalabilidad y la redundancia NO alcanza.

La confidencialidad, ¿no deja de ser importante cuando el contenido es público?
Si, pero ese contenido es servido probablemente por algún código dinámico, alguna base de datos o incluso administrado por otra aplicación que podría estar expuesta, y a partir de allí ser explotada de manera malintencionada.

¿Qué pasa con la integridad?
En general el menor de los problemas de integridad es detectar alguna alteración accidental o intencional de los datos y recuperarlo desde algún sistema de resguardo. La mayor gravedad de los problemas de integridad sobrevienen cuando a partir de fallas de integridad sobrevienen consecuencias con terceros a la organización, las cuales NO solo pueden sobrellevar problemas de imagen de marca, o desvalorización de la empresa sino que pueden involucrar cuestiones legales.

GRACIAS