

TODO SOBRE FIREWALL TIPOS Y USO

Saúl Ruiz Plaza

[@saulruizplaza](#)

¿QUÉ ES UN FIREWALL?



Un firewall es una herramienta clave que **filtra** y **controla** el tráfico de red entre una red segura y redes externas no confiables, evitando accesos no autorizados y ciberataques.

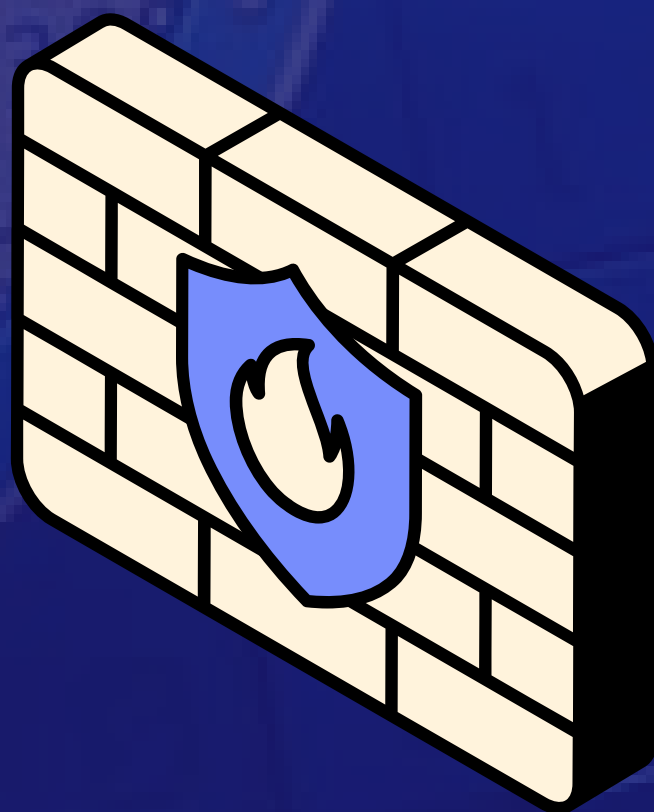
PUNTOS POSITIVOS

Monitorear, analizar y bloquear tráfico no deseado.

@[saulruizplaza](https://twitter.com/saulruizplaza)

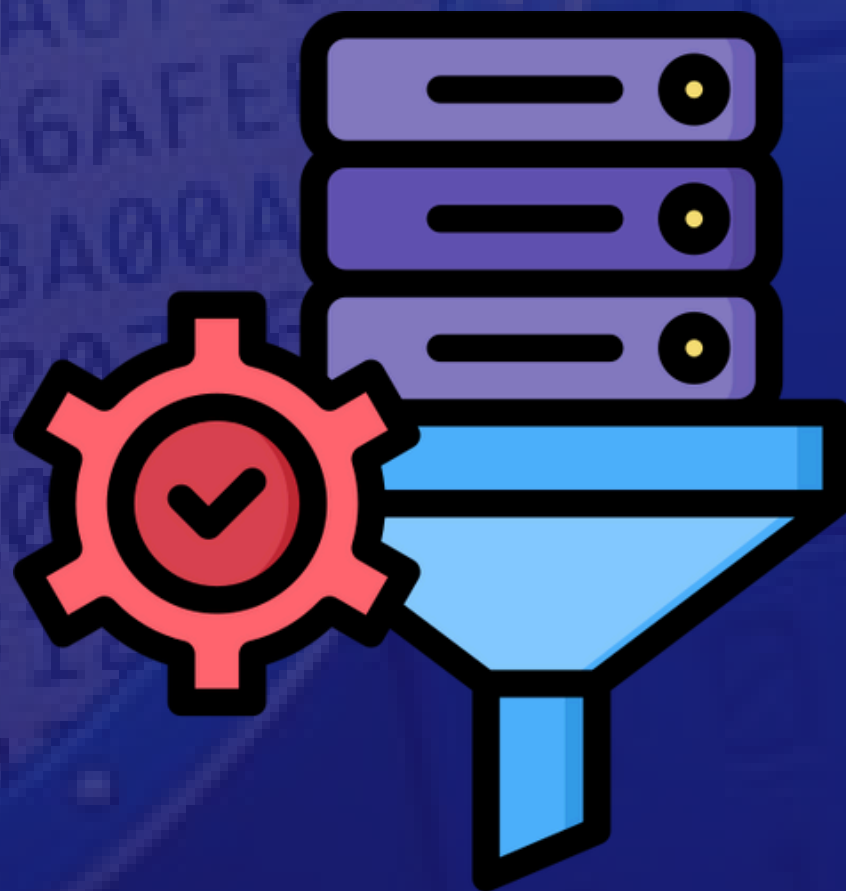
0617463686513200
520616E642074616
E2048657061A0707
C69
A120
61C3A
617
A0174
6697D0
852756B013A00AA
FF661564207
E7D011A001
11BFF12

TIPOS DE FIREWALL



FILTRADO DE PAQUETES

Analiza cada paquete de datos y permite o bloquea el tráfico según reglas predefinidas (como IP, puerto y protocolo), sin tener en cuenta el estado de la conexión.



@saulruizplaza

PUNTOS POSITIVOS

- **Simplicidad** en la configuración.
- **Bajo** consumo de recursos.
- **Eficaz** para redes pequeñas o con tráfico simple.

PUNTOS NEGATIVOS

- No examina el contenido de los paquetes, lo que **limita** su capacidad para detectar amenazas avanzadas.
- No tiene **conciencia** del estado de la conexión, lo que lo hace vulnerable a ciertos ataques.

INSPECCIÓN CON ESTADO

Realiza un **seguimiento** de las conexiones activas, asegurando que los paquetes entrantes pertenezcan a una sesión activa y válida, permitiendo un control más sofisticado.



@saulruizplaza

PUNTOS POSITIVOS

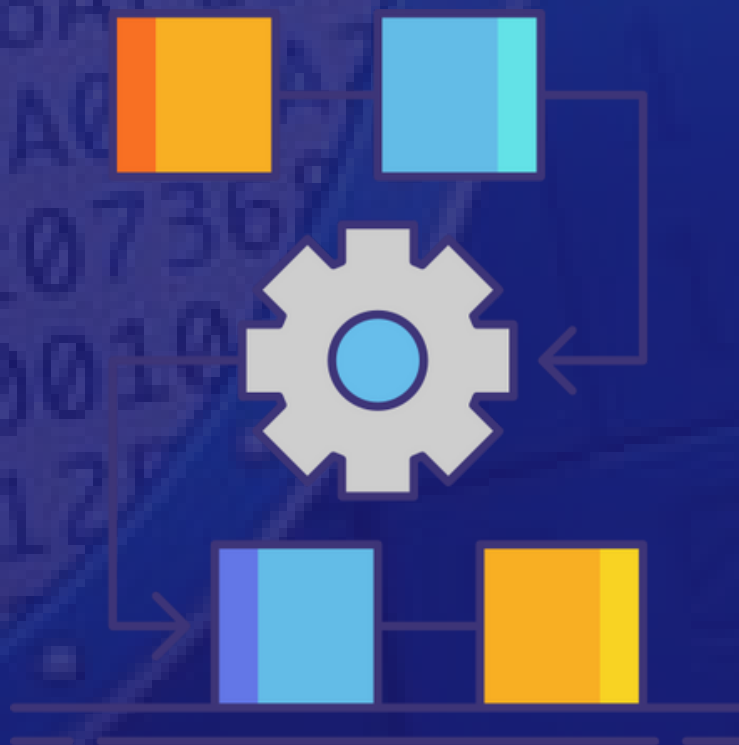
- **Análisis** de contexto y conexión.
- Mejor **protección** frente a ataques como spoofing y falsificación de paquetes.
- Equilibrio entre **seguridad** y **rendimiento**.

PUNTOS NEGATIVOS

- Requiere más recursos de **hardware** y puede impactar en el rendimiento en redes de gran volumen.
- Configuración más **compleja**.

PUERTA DE ENLACE DE NIVEL DE CIRCUITO

Opera en la **capa de transporte** (nivel 4 del modelo OSI) y crea un circuito entre dos dispositivos confiables, asegurando que el tráfico solo pueda pasar si se establece una conexión legítima.



PUNTOS POSITIVOS

- **Eficiente** para filtrar el tráfico de nivel superior y evitar conexiones no deseadas.
- **Bajo** consumo de recursos, ideal para sistemas de alto tráfico.

PUNTOS NEGATIVOS

- No examina el contenido del paquete, lo que deja **vulnerabilidades** ante ataques más sofisticados.
- **Falta de inspección** profunda de los paquetes y sus datos.

FIREWALL PROXY

Actúa como un **intermediario** entre los usuarios y los recursos a los que intentan acceder, analizando cada solicitud y **reescribiendo** el tráfico para asegurarse de que sea seguro antes de permitir su paso.



@saulruizplaza

PUNTOS POSITIVOS

- **Oculto** las direcciones IP internas y proporciona anonimato.
- **Eficaz** para filtrar contenido malicioso y bloquear malware o ataques a nivel de aplicaciones.

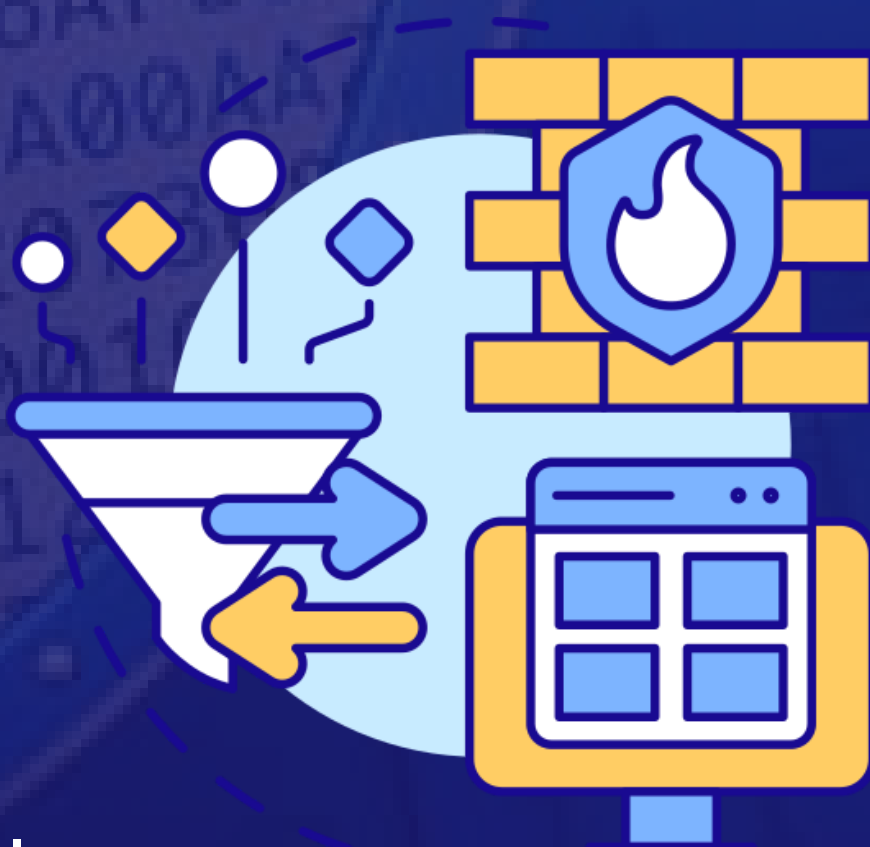
PUNTOS NEGATIVOS

- Incrementa el **tiempo de latencia** debido a la reescritura de los datos.
- Requiere **recursos** de procesamiento adicionales.

@saulruizplaza

WEB APPLICATION FIREWALL (WAF)

Se especializa en **proteger** aplicaciones web contra amenazas como inyección SQL, Cross-Site Scripting (XSS) y ataques de denegación de servicio (DoS), al filtrar el tráfico HTTP y HTTPS.



@saulruizplaza

PUNTOS POSITIVOS

- **Protección** específica para aplicaciones web.
- **Prevención** activa contra ataques comunes en la web.
- Inspección **detallada** de solicitudes HTTP/HTTPS.

PUNTOS NEGATIVOS

- Solo **protege** aplicaciones web, no la red en general.
- Puede ser **costoso y complicado** de implementar en infraestructuras grandes.

@saulruizplaza

NEXT-GENERATION FIREWALL (NGFW)

Firewall de **última generación** que integra funciones adicionales como control de aplicaciones, detección de malware, inspección profunda de paquetes y inteligencia contra amenazas.



@[saulruizplaza](https://twitter.com/saulruizplaza)

PUNTOS POSITIVOS

- **Detección** **avanzada** de amenazas con inteligencia artificial.
- **Control** granular de aplicaciones y protocolos.
- Mejora la **visibilidad** de todo el tráfico de la red

PUNTOS NEGATIVOS

- Mayor **complejidad** y necesidad de personal especializado.
- Puede resultar **costoso** para pequeñas empresas.

APLICACIONES DEL FIREWALL



FIREWALLS EN LA NUBE

Protegen los recursos y servicios desplegados en plataformas de nube pública, como AWS, Microsoft Azure y Google Cloud, monitoreando y controlando el tráfico entre instancias virtuales.



@saulruizplaza

PUNTOS POSITIVOS

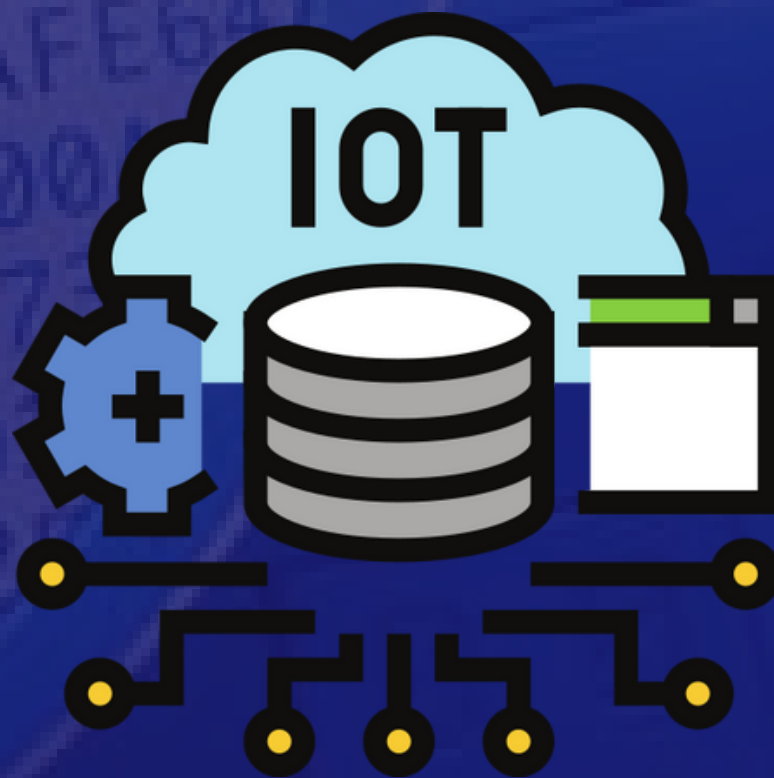
- **Escalabilidad** flexible según las necesidades de la nube.
- **Integración fluida** con otras herramientas de seguridad en la nube.
- **Reducción** de los **costos** de infraestructura.

PUNTOS NEGATIVOS

- **Dependencia** de los proveedores de servicios de la nube para asegurar la red.
- Requiere una **correcta configuración** para evitar brechas de seguridad.

FIREWALLS EN REDES IOT

Los firewalls de Internet de las Cosas (IoT) **protegen** dispositivos IoT de **accesos no autorizados**, filtrando el tráfico hacia y desde los dispositivos, que suelen ser vulnerables.



@saulruizplaza

PUNTOS POSITIVOS

- **Aísla** los dispositivos IoT de redes críticas.
- Mejora la seguridad de entornos con **múltiples dispositivos** conectados.

PUNTOS NEGATIVOS

- Puede ser **difícil** de gestionar a gran escala.
- Los dispositivos IoT suelen **carecer de medidas** de seguridad adecuadas.

INTEGRACIÓN CON OTRAS HERRAMIENTAS DE SEGURIDAD

No deben operar de manera aislada. Su integración con **SIEM, IDS/IPS y antivirus** permite una defensa más completa ante amenazas.



@saulruizplaza

PUNTOS POSITIVOS

- Mejora la **detección** y la respuesta ante incidentes.
- Fomenta la **defensa** en profundidad.

PUNTOS NEGATIVOS

- Puede ser **complejo** gestionar múltiples herramientas de seguridad.
- Requiere recursos de **hardware** y humanos adicionales.

@saulruizplaza

CRITERIOS PARA ELEGIR EL MEJOR FIREWALL PARA TU RED



TAMAÑO Y COMPLEJIDAD DE LA RED

Redes grandes requieren NGFW o firewalls **avanzados**; redes pequeñas pueden usar firewalls básicos de filtrado de paquetes.

TIPO DE TRÁFICO

Para aplicaciones web, usa un **Web Application Firewall (WAF)**. Para IoT o nubes, busca firewalls específicos para esas plataformas.

NIVEL DE PROTECCIÓN

Si manejas datos sensibles, opta por firewalls con inspección profunda de paquetes y **prevención** de intrusiones.

PRESUPUESTO

Los firewalls avanzados son **caros**.
Evalúa si los básicos son suficientes
para tus necesidades.

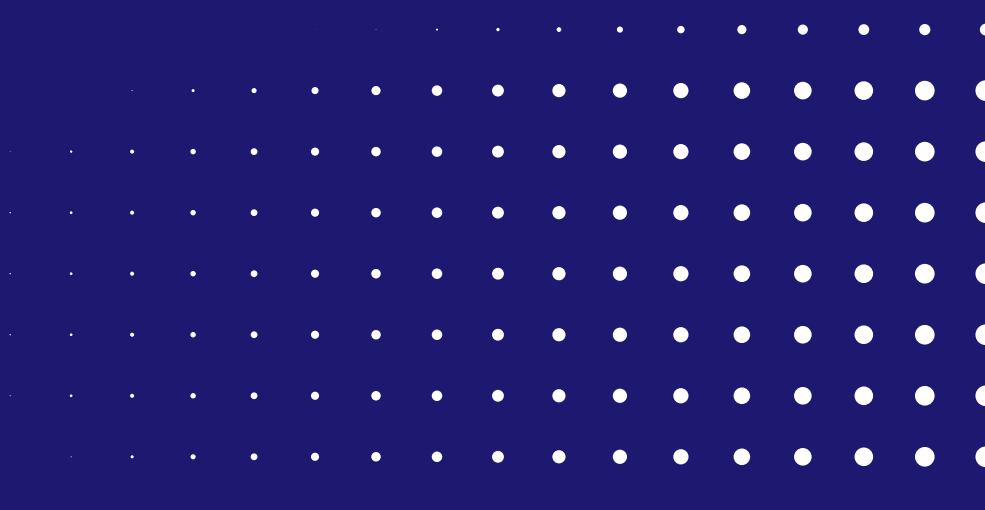
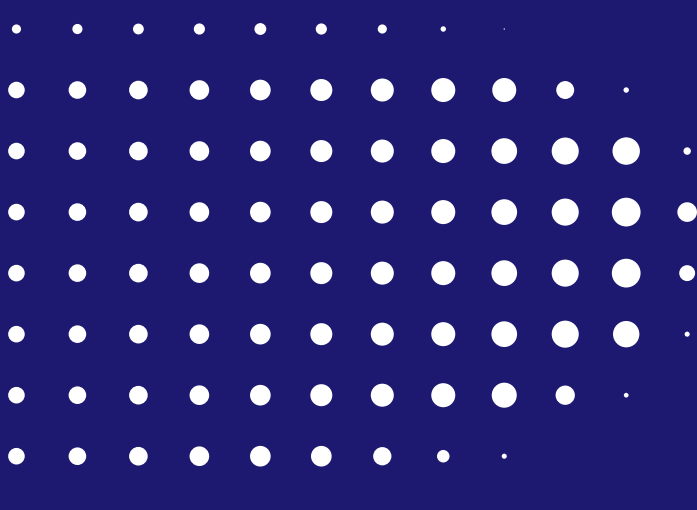
GESTIÓN Y ESCALABILIDAD

Elige un firewall **fácil de gestionar** y
que crezca con tu red. Los **NGFW** son
más escalables.

CUMPLIMIENTO Y REGULACIONES

Asegúrate de que el firewall cumpla
con normativas como **GDPR** o **HIPAA** si
es necesario.

@saulruizplaza



**¿TE HA
SIDO ÚTIL
ESTA
INFORMA
CIÓN?**

[@saulruizplaza](#)



Guardalo