



@saulruizplaza

PROTECCIÓN DE REDES EN CIBERSEGURIDAD



FIREWALL

LA PRIMERA LÍNEA



1

¿QUÉ ES UN FIREWALL?



Los firewalls son dispositivos o software que **filtran el tráfico de red entrante y saliente** según reglas predefinidas. Funcionan como una barrera que permite o bloquea conexiones basándose en criterios como la dirección IP, puertos y protocolos.

1.2

TIPOS DE FIREWALL



- **Firewalls de hardware:** Son dispositivos físicos que protegen redes enteras. Suelen ser rápidos y robustos, ideales para grandes organizaciones.
- **Firewalls de software:** Programas instalados en sistemas operativos o servidores, útiles para redes más pequeñas o dispositivos individuales.
- **Next-Generation Firewalls (NGFW):** Incorporan tecnologías avanzadas como inspección profunda de paquetes, control de aplicaciones y detección de malware.

DETECCIÓN DE INTRUSOS IDS



2

¿QUÉ ES UN IDS?



Un IDS (Intrusion Detection System) es una herramienta diseñada para **monitorear el tráfico** de red y detectar actividades sospechosas que puedan indicar intentos de intrusión o ataques en curso.

El IDS **no bloquea ni mitiga amenazas**, solo detecta y alerta. Por ello, se utiliza en conjunto con otras herramientas de seguridad.

2.2

CARACTERÍSTICAS

- **Alertas:** Notifica a los administradores de seguridad cuando detecta un patrón anómalo o comportamiento sospechoso.
- **Detección basada en firmas:** Compara el tráfico con una base de datos de ataques conocidos.
- **Detección basada en anomalías:** Identifica actividades que se desvían del comportamiento normal de la red.



PREVENCIÓN DE INTRUSOS IPS



3

¿QUÉ ES UN IPS

El IPS (Intrusion Prevention System) es similar al IDS, pero con una diferencia crucial: además de detectar amenazas, **puede actuar automáticamente para detenerlas.**



3.2

TIPOS DE IPS

- **Basados en red (NIPS):** Protegen la infraestructura completa al analizar el tráfico en todos los puntos de acceso.
- **Basados en host (HIPS):** Se instalan en dispositivos específicos, protegiéndolos contra ataques dirigidos.



3.3

CARACTERÍSTICAS

- **Bloqueo de amenazas:** Interviene activamente al bloquear o redirigir el tráfico malicioso.
- **Prevención en tiempo real:** Analiza los paquetes de datos mientras pasan por la red y los descarta si detecta comportamientos sospechosos.
- **Integración con firewalls y otros sistemas:** Trabaja en conjunto para ofrecer una seguridad más robusta.



VIRTUAL PRIVATE NETWORK VPN



4

¿QUÉ ES UNA VPN

Las VPNs cifran la comunicación entre el usuario y la red, **creando un túnel seguro** que protege los datos de miradas indiscretas. Son esenciales para conexiones a través de redes públicas como el Wi-Fi de cafeterías o aeropuertos.



4.2

CASOS DE USO

- **Teletrabajo:** Garantiza que los empleados accedan de forma segura a los recursos corporativos desde casa.
- **Sucursales:** Permiten interconectar diferentes oficinas de una empresa de manera segura.



SEGMENTACIÓN DE REDES



5

¿QUÉ ES LA SEGMENTACIÓN DE REDES?

La segmentación **divide la red en subredes más pequeñas**, limitando el acceso entre ellas. Esto significa que, si un atacante compromete una parte de la red, no podrá moverse libremente hacia otras áreas.



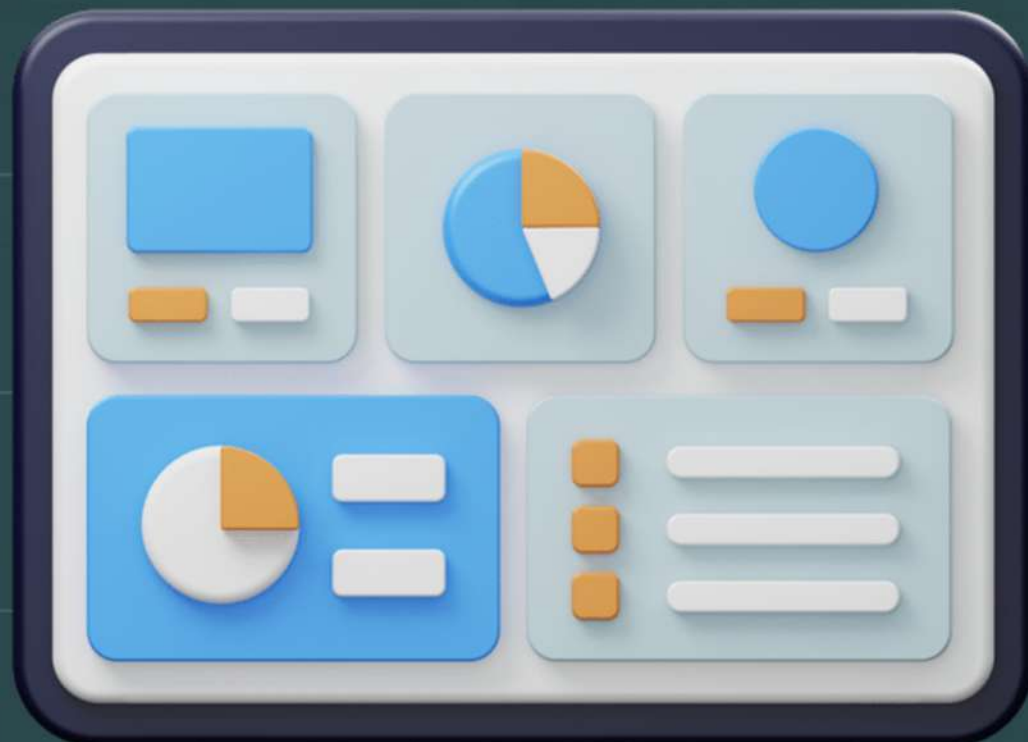
MONITOREO EN TIEMPO REAL



6

¿EN QUÉ CONSISTE MONITORIZAR?

Herramientas como los sistemas **SIEM (Security Information and Event Management)** recopilan y analizan datos de múltiples fuentes en la red para detectar amenazas avanzadas.



HERRAMIENTAS

6.2 IBM QRADAR

IBM QRadar destaca por su enfoque en la automatización de la detección de amenazas utilizando inteligencia artificial, y se integra fácilmente con otras soluciones de IBM y herramientas de terceros, mejorando la visibilidad y la gestión de redes.



HERRAMIENTAS

6.3 SPLUNK

Splunk es una de las soluciones más conocidas, con potentes capacidades de análisis de datos en tiempo real y una gran escalabilidad para manejar grandes volúmenes de información, además de ofrecer paneles e informes personalizables.

splunk®

ACTUALIZACIONES

PARCHES



7

¿PARA QUÉ ACTUALIZAR?



Mantener el software y hardware actualizado es esencial para **proteger la red frente a vulnerabilidades conocidas**. Los atacantes suelen aprovecharse de sistemas obsoletos para lanzar ataques.

7.2 MEJORES PRÁCTICAS



Establecer un calendario para aplicar actualizaciones de software y hardware de manera programada. Así se minimiza el riesgo de ataques aprovechando vulnerabilidades no parcheadas

7.3

MEJORES PRÁCTICAS



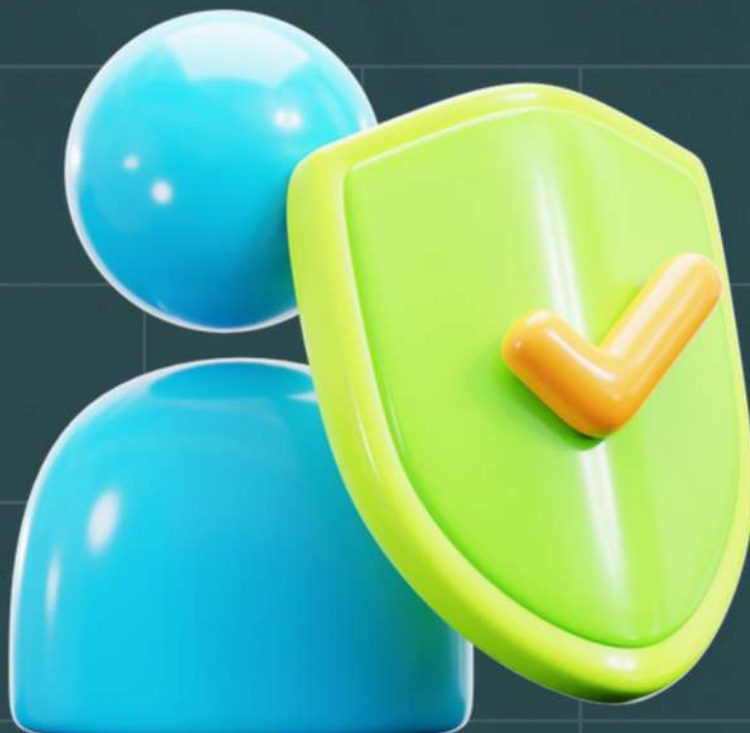
Configurar actualizaciones automáticas para asegurar que los parches críticos se apliquen sin intervención manual. Así se minimizará errores humanos

POLÍTICAS DE SEGURIDAD



¿POR QUÉ LAS POLÍTICAS DE SEGURIDAD?

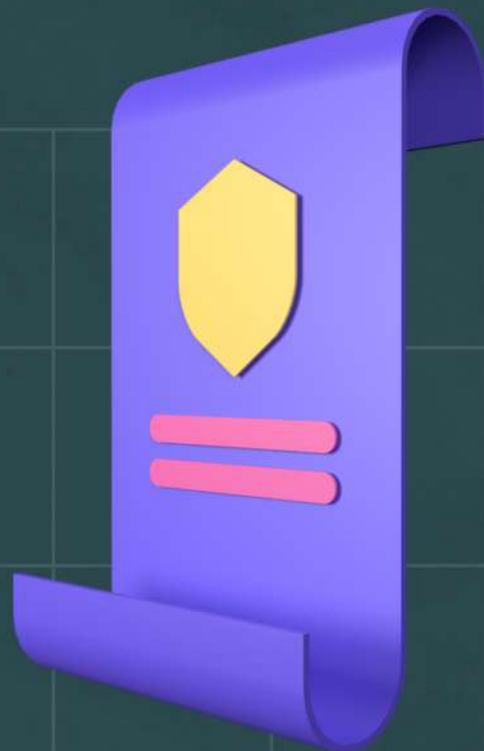
El factor humano es una de las principales causas de los incidentes de seguridad. A menudo, los **atacantes explotan el desconocimiento o la falta de precaución de los usuarios** para realizar ataques como el phishing o el uso indebido de contraseñas.



8.2

MEJORES PRÁCTICAS

- **Definir reglas claras** sobre contraseñas, acceso a sistemas y manejo de datos sensibles. Revisar periódicamente para adaptarse a nuevas amenazas.
- **Capacitar regularmente** a los empleados frecuentemente sobre amenazas comunes (phishing, uso de contraseñas, etc.).



9

CONCLUSIÓN

La seguridad de redes requiere una **combinación** de herramientas tecnológicas, políticas claras y capacitación continua. Al mantener sistemas actualizados, usar herramientas adecuadas y formar a los empleados, se minimizan los riesgos y se **fortalece la protección frente a ciberamenazas**.

MUCHAS
GRACIAS



@saulruizplaza