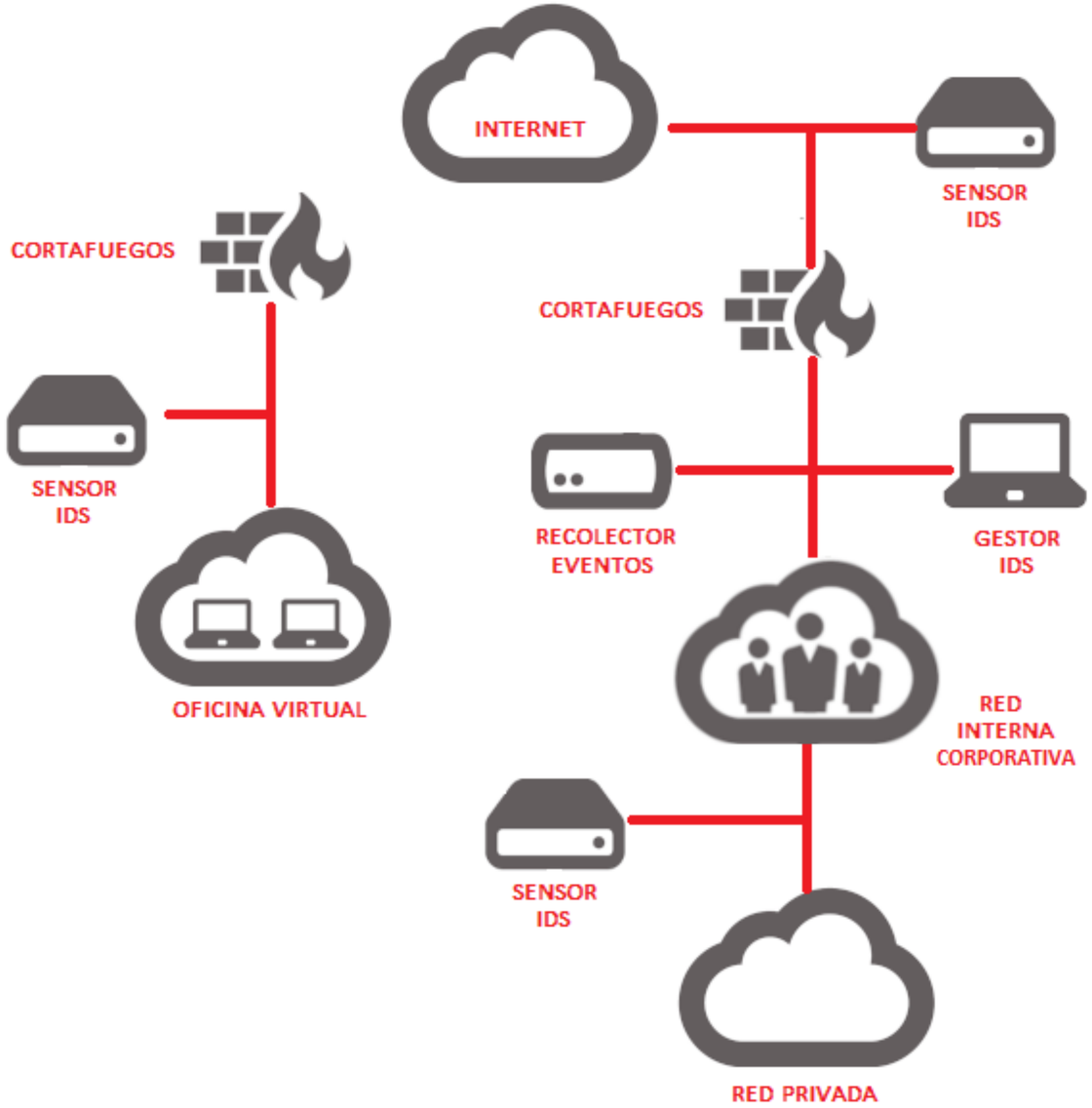
Sistemas de Detección y Prevención de Intrusiones (IPS/IDS)

Fundamentos

Sistemas IDS/IPS

Qué son

- Sistemas de protección de las comunicaciones que **monitorizan** el tráfico que entra o sale de la red
- **Detectan** patrones sospechosos de tráfico
- **Previenen** de amenazas, bloqueando tráfico considerado perjudicial



IDS — Sistema de Detección de Intrusiones

Intrusion Detection System

- Aplicación que **detecta accesos no autorizados** a un ordenador o a una red
- **Monitoriza el tráfico entrante**, cotejándolo con una base de datos de firmas de ataque conocidas
- **Emite alertas** cuando detectan actividad sospechosa
- **No tratan de mitigar** la intrusión

Ventajas e Inconvenientes de los IDS

Ventajas

- Permite ver lo que sucede en tiempo real
- Reconoce modificaciones en datos y documentos
- Automatiza patrones de búsqueda

Inconvenientes

- No previenen ni detienen ataques
- Son sensibles a ataques DDoS

IPS — Sistema de Prevención de Intrusiones

Intrusion Prevention System

- **Protege** a los sistemas de ataques e intrusiones, actuando preventivamente
- **Analiza** en tiempo real conexiones y protocolos
- **Identifica ataques** según patrones, anomalías o comportamientos sospechosos
- Permite o inhibe el **acceso a la red**, pudiendo **descartar paquetes** o **desconectar conexiones**

Ventajas e Inconvenientes de los IPS

Ventajas

- Escalabilidad en la gestión de múltiples dispositivos
- Protección preventiva
- Defensa frente a múltiples ataques
- Eficaces y seguros

Inconvenientes

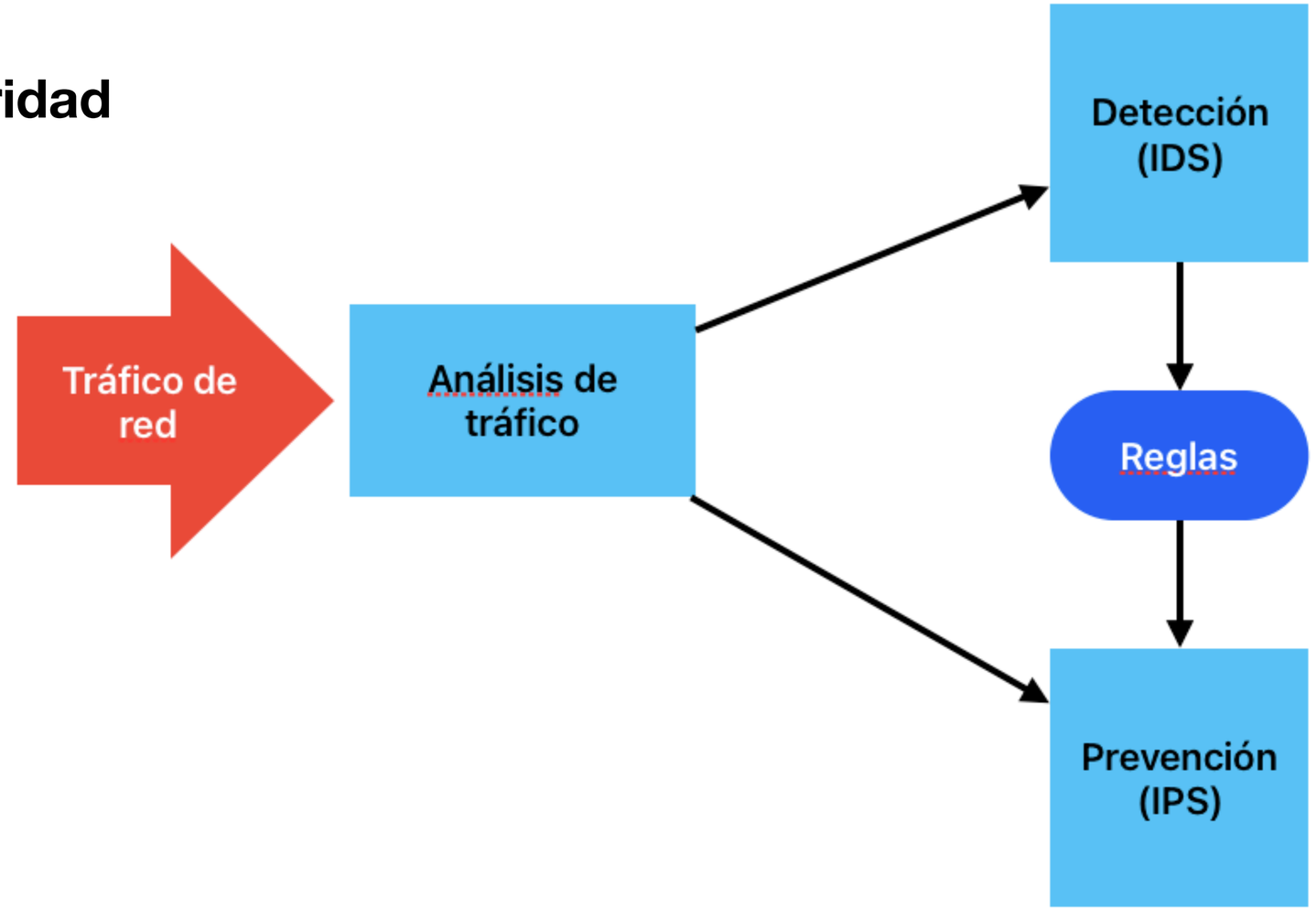
- Falsos positivos
- Inutilización de recursos en caso de recibir ataques DoS o DDoS

Esquema de funcionamiento

SIEM — Sistema de Gestión de Eventos e Información de Seguridad

Solución híbrida centralizada que engloba la gestión de la información de seguridad y la gestión de eventos.

1. Monitorización
2. Detección
3. Protección



Técnicas de detección

- Técnicas basadas en firmas de ataque
- Técnicas basadas en anomalías

Tipos de IDS

IDS basados en la red (NIDS)

Hacen la detección sobre el tráfico de toda la red. Dicho tráfico se redirige al IDS para que lo analice.

Ejemplos:

- Snort
- Suricata
- Zeek (anteriormente Bro)

IDS basados en el host (HIDS)

Hacen la detección sobre el tráfico del propio host.

Ejemplos:

- OSSEC
- Samhain

Monitorización de Integridad de Ficheros (FIM)

Ejemplos:

- AFICK
- Tripwire