6669 Criptografía y Seguridad Informática

IDPS & Honeypot

Intrusion Detection System (IDS)

- Es una tecnología que monitorea el tráfico de una red y los sistemas de una organización en busca de señales de intrusión, actividades de usuarios no autorizados y la ocurrencia de malas prácticas, como en el caso de los usuarios autorizados que intentan sobrepasar sus límites de restricción de acceso a la información. Al detectarlo informa al administrador de la intrusión.

Intrusion Prevention System (IPS)

- Es una tecnología que monitorea el tráfico de una red y los sistemas de una organización en busca de señales de intrusión, actividades de usuarios no autorizados y la ocurrencia de malas prácticas, como en el caso de los usuarios autorizados que intentan sobrepasar sus límites de restricción de acceso a la información. Al detectarlo bloquea la conexión con el fin de evitar la intrusión.

IPS vs IDS

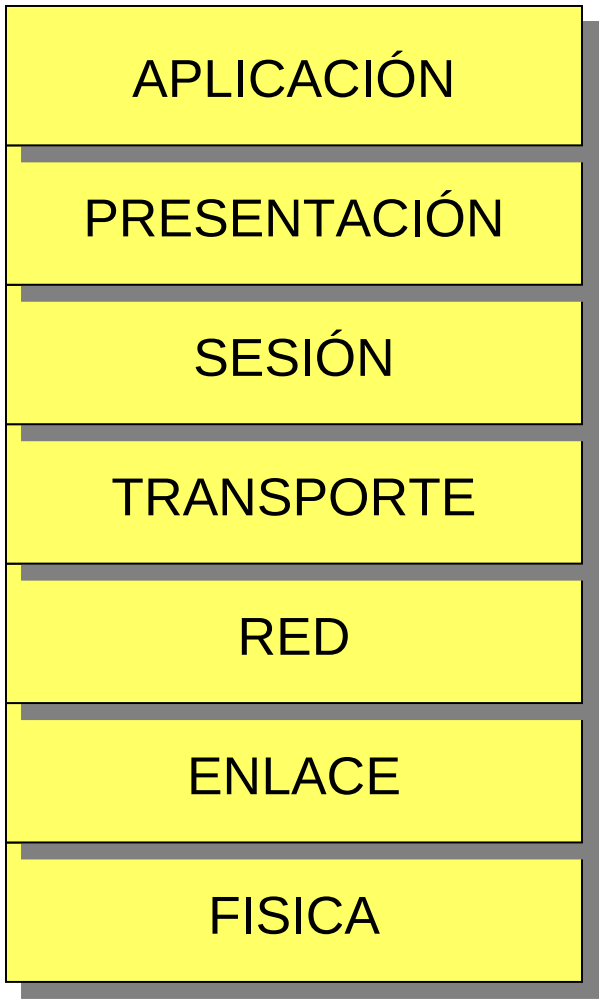
- Según su naturaleza suele diferenciarse en:
  - Pasivos: Detectan una intrusión, la registran y alertan
  - Activos: Detectan una intrusión y cortan la comunicación desde la fuente hostil

IPS vs IDS

- Según su naturaleza suele diferenciarse en:
  - *Pasivos*: Detectan una intrusión, la registran y alertan
  - *Activos*: Detectan una intrusión y cortan la comunicación desde la fuente hostil

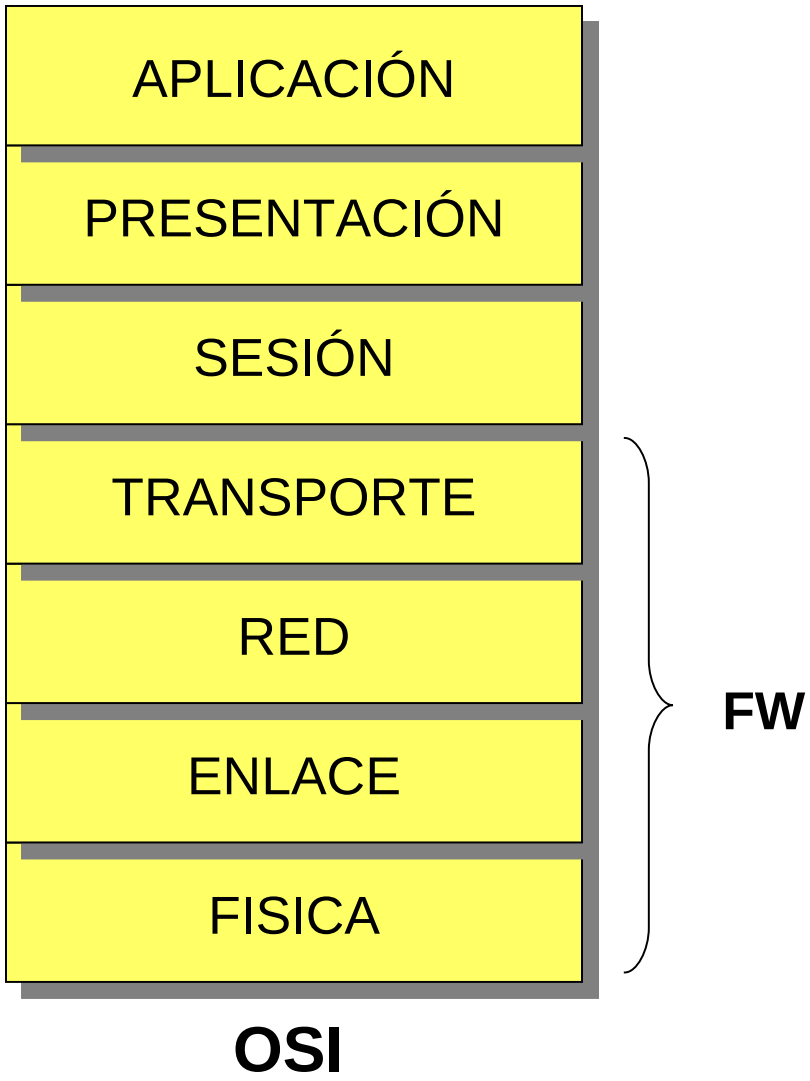
  - Pasivo → IDS
  - Activo → IPS

Firewall vs IDP

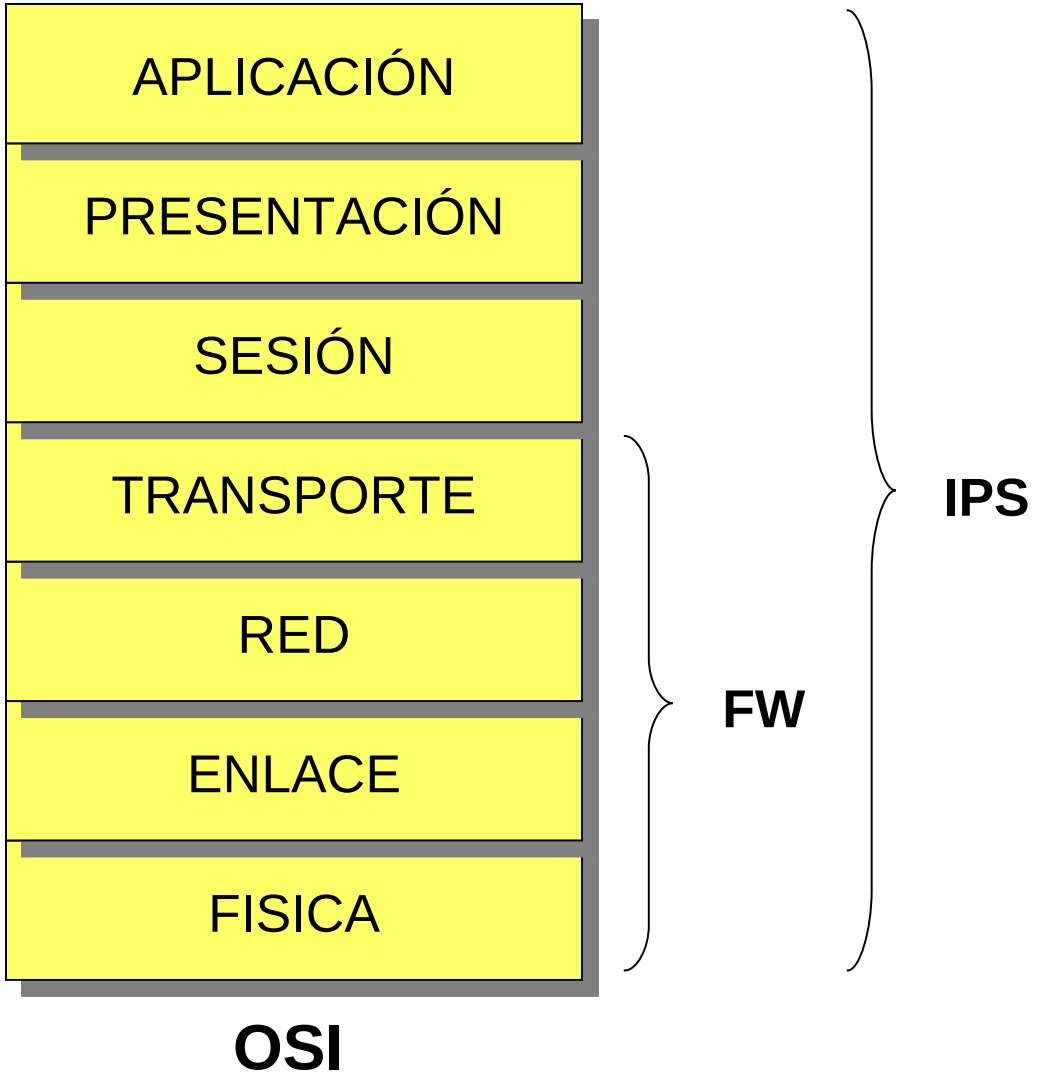


OSI

Firewall vs IDP



Firewall vs IDP



Vulnerabilidad

- Falla en un sistema que permitiría comprometer al menos uno de los pilares de la Seguridad Informática.

Exploit

- Porción de código que permite explotar una vulnerabilidad.

Vulnerabilidad 0-day

- Es una vulnerabilidad que no dispone de parche o mitigación por parte del fabricante.

Vulnerabilidad 0-day

- Es una vulnerabilidad que no dispone de parche o mitigación por parte del fabricante.

El IPS puede prevenir los 0-days

Solo hay que estar atentos a las actualizaciones

IDP según su ubicación

- Al igual que los FW, los IDPs puede ubicarse en:
  - *Red*: NIDS / NIPS
  - *Host*: HIDS / HIPS

IDP

- Disponen de diversas variedades de capacidades, entre ellas:
  - Recolección de Información
  - Generación de trazas
  - Detección
    - Umbral
    - Blacklists y Whitelists
    - Configuración de alertas
    - Visualización de código
  - Prevención

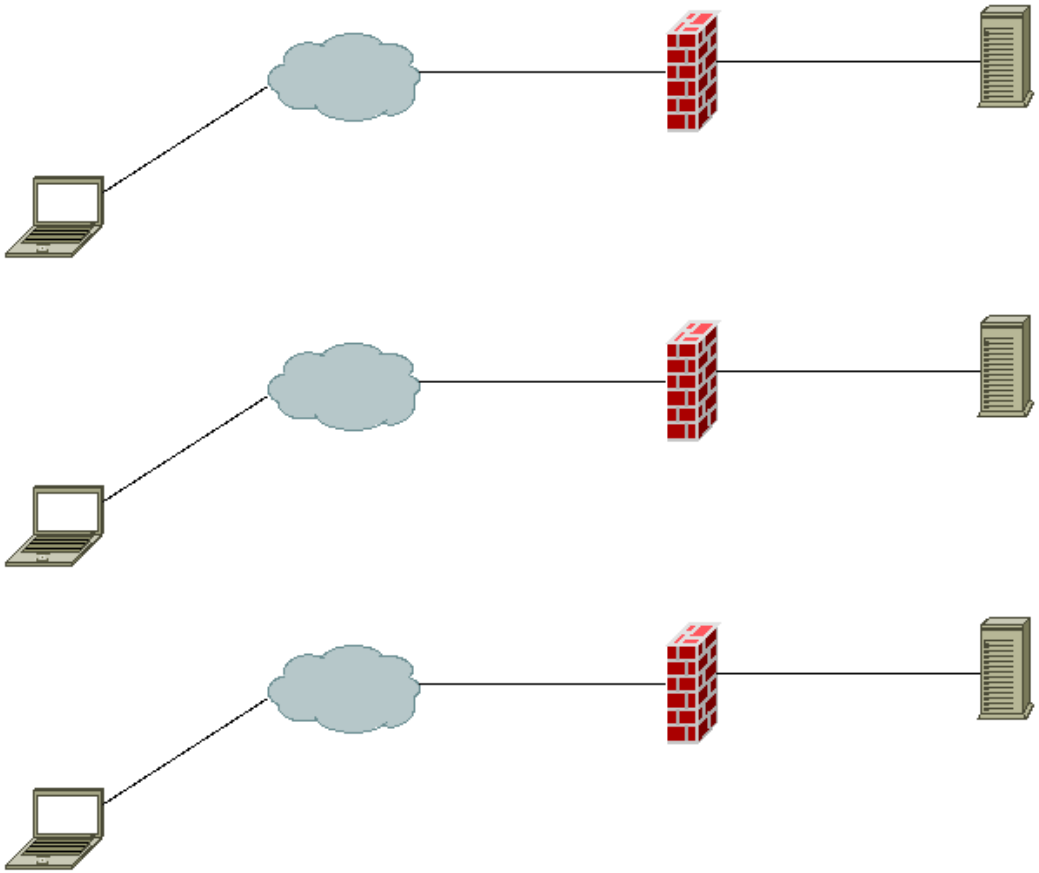
IDP – Componentes

- Componentes típicos en la implementación de un IDP:
  - *Sensor o Agente*: Monitorean la actividad. El término *sensor* suele utilizarse en IDPs de red, mientras que *agente* suele emplearse en los IDPs de host.
  - *Servidor de Gestión*: Dispositivo que centraliza las actividades de los sensores y agentes.
  - *Servidor de Base de Datos*: Repositorio donde se almacena la información de los eventos
  - *Consola*: Software de tipo cliente que permite la interacción entre los administradores y los IDPs.

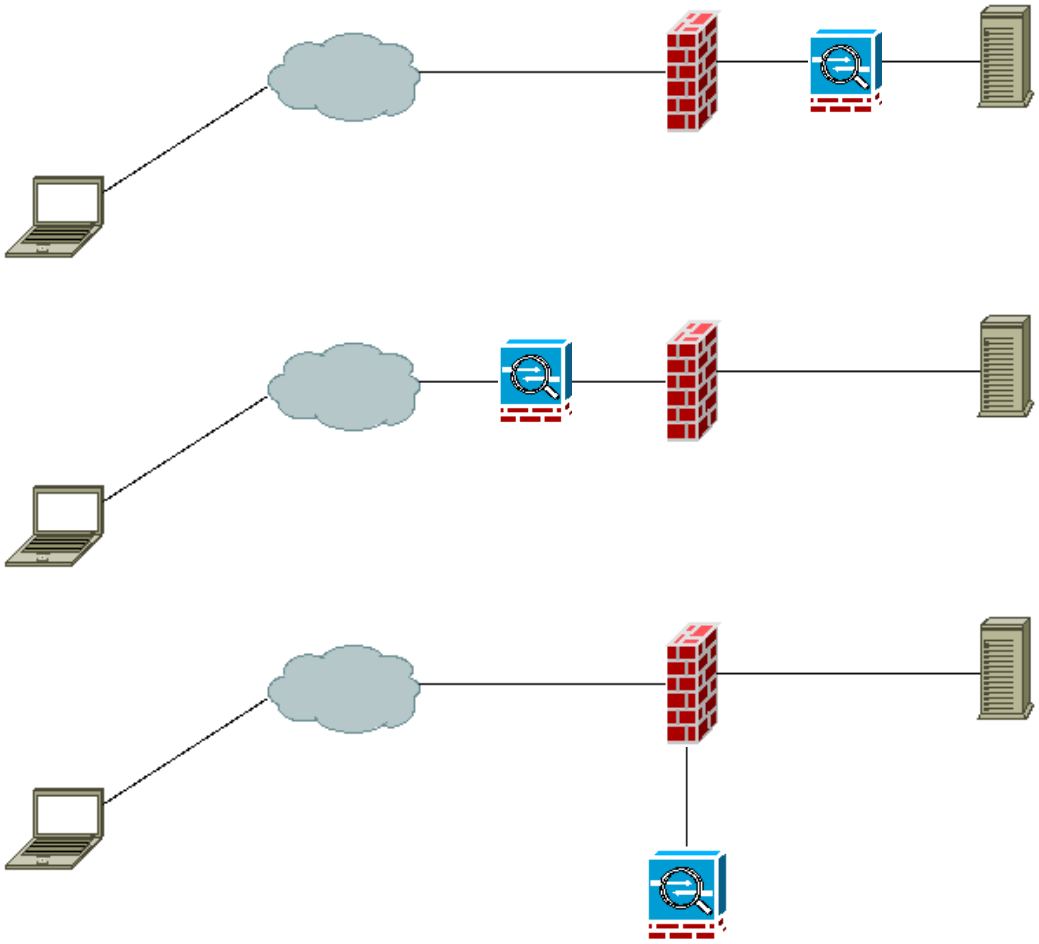
IDP – Comportamientos

- Las metodologías utilizadas para detectar intrusiones son las siguientes:
  - Detección basada en firma
  - Detección basada en una anomalía
  - Análisis de protocolo

IDP – Arquitecturas comunes



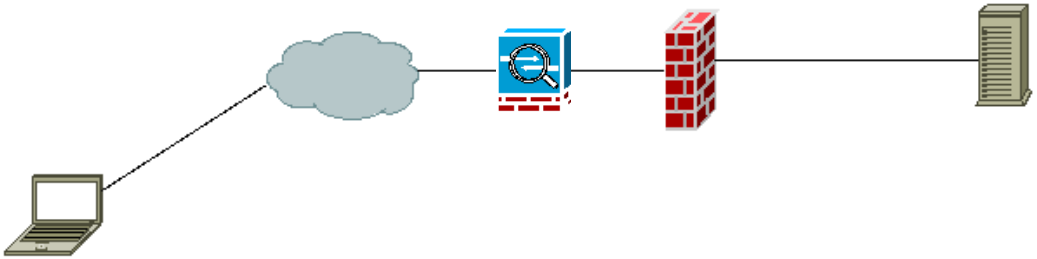
IPS – Arquitecturas comunes



IPS – Arquitectura – Ejemplo 1

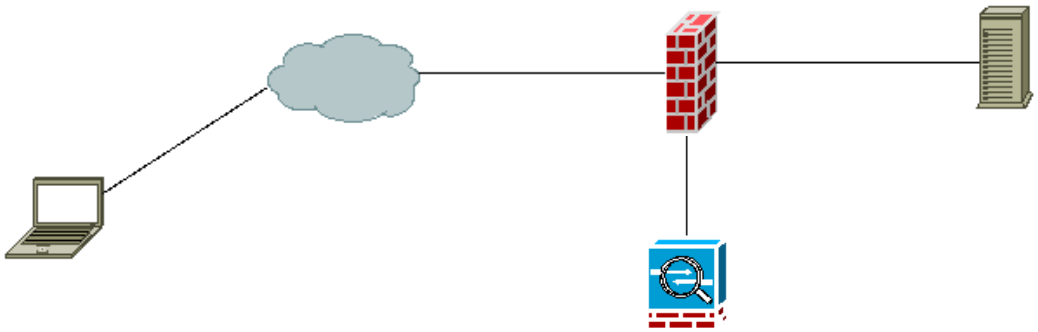
- Pros:
  - Únicamente llegan los paquetes que deja pasar el FW
  - Intercepta todos los paquetes que llegan al servidor
- Contra:
  - Puede ser un cuello de botella

IPS – Arquitectura – Ejemplo 2



- Pros:
  - Intercepta todos los paquetes que llegan al servidor
  - A nuestra red únicamente llegan paquetes limpios
- Contra:
  - Es un gran un cuello de botella

IPS – Arquitectura – Ejemplo 3



- Pros:
  - No genera latencia en la comunicación
- Contra:
  - El primer paquete malicioso pasa al servidor