IDS/IPS

Hasta ahora se han desplegado redes que implementan mecanismos de control de tráfico entre redes en diferentes puntos. Ahora necesitamos herramientas que ayuden a catalogar amenazas no definidas previamente, definidas por aplicaciones maliciosas o APT (Advanced Persistent Threat).

Los sistemas de detección de intrusiones analizan el tráfico en una red o el comportamiento de un equipo y determinan si están ocurriendo sucesos anómalos que puedan ser asociados a acciones maliciosas o ataques. En la actualidad, para detectar ataques, tenemos 2 enfoques:

- Monitorizar el tráfico de red para localizar ataques conocidos
- Disponer de sistemas de detección de instrucciones que modeliza el comportamiento de una red para detectar si se producen anomalías.

Los despliegues más habituales de sistemas de prevención de intrusiones suelen funcionar por firmas (primer modelo). Para detectar ataques se deben detectar equipos que realizan un abuso de conexiones o reglas de tráfico permitido (Ataque de Escaneo de eventos), en este caso nuestro CPE no reaccionará y las conexiones pasarán al FireWall, donde las conexiones permitidas pasarán. En caso de un ataque de denegación de servicios nuestro servidor va a necesitar memoria para resistir un TCP Sync Flu. Para prevenir ataques DoS la clave es realizar contestaciones lentas desde el servidor. Esto puede ser gestionado por un proxy para evitar ataques DoS, pero si se ve sobresaturado puede caer. Un caso problemático son aquellos ataques que no atraviesan los firewalls y pueden tumbar la red sin necesidad de pasar por estos. Esto puede ocurrir cuando existe una DMZ en la red, se recomienda monitorizar la DMZ para evitar estos tipos de ataques.

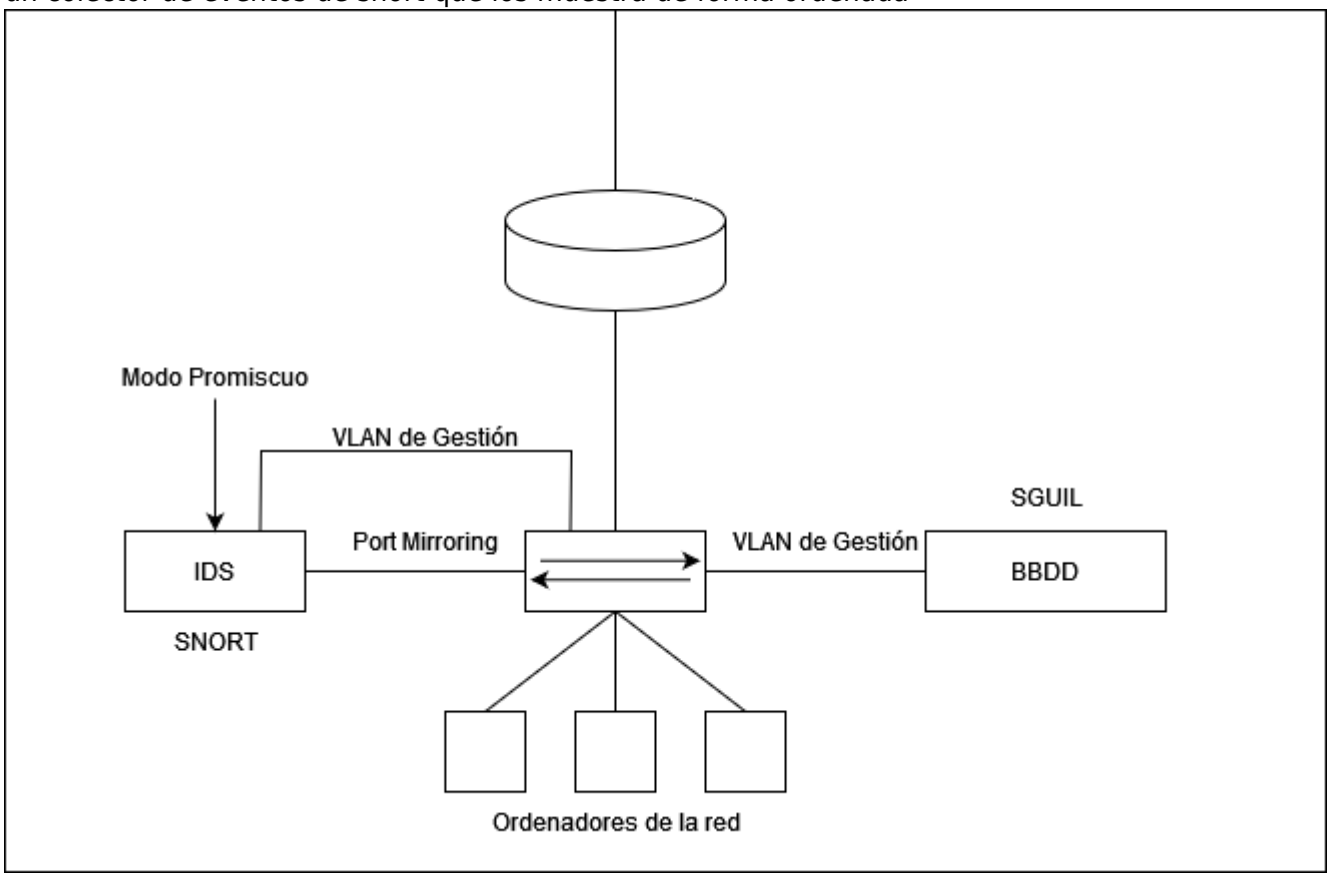
Definiciones

- **Detección de intrusiones**: Servicio de monitorización que requiere obtener información de la red para localizar signos de posibles incidentes de seguridad. Por ejemplo, si se ve una petición HTTP que contenga un “DROP DATABASE” puede identificarse como un posible ataque.
- **Intruson Detection System (IDS)**: Sistema que automatiza el proceso de detección de intrusiones. Detectan ataques y emiten alertas sobre sucesos sospechosos.
- **Intrusion Prevention System (IPS)**: IDS con la capacidad de bloquear las posibles incidencias de seguridad. En vez de emitir una alerta, bloquean directamente el tráfico sospechoso.
- **Intrusion Detection and Prevention System (IDPS)**: La mayor parte de los sistemas son de este tipo ya que pueden implementar características tanto de IDS como IPS, de forma que en función de como se despliegue puede ser un tipo de dispositivo u otro.

IDS: Intrusion Detection System

Los IDS están diseñados para analizar el práctico de forma pasiva y si están basados en firmas comparan en tráfico comparan este con firmas de posibles ataques. El IDS irá conectado a un switch y recibirá una copia de todo el tráfico que pasa por este, el cual analizará en modo promiscuo. El IDS estará conectado a la red de gestión. El IDS más conocido es SNORT que se conecta a SGUIL que es

un colector de eventos de snort que los muestra de forma ordenada



La ventaja que tienen los IDS es que no afectan a la velocidad de la red. Lo malo de los IDS es que no detienen los ataques, solo generan alertas cuando ocurre uno. Antiguamente los IDS solo generaban alertas, pero también pueden utilizar el protocolo SNMP para reconfigurar equipos de red, lo cual tiene la ventaja de que se puede actuar sobre un problema y la desventaja es que se SNMP es un protocolo vulnerable, por lo que se recomienda no hacer esto.

IPS: Intrusion Prevention System

Los IPS