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.

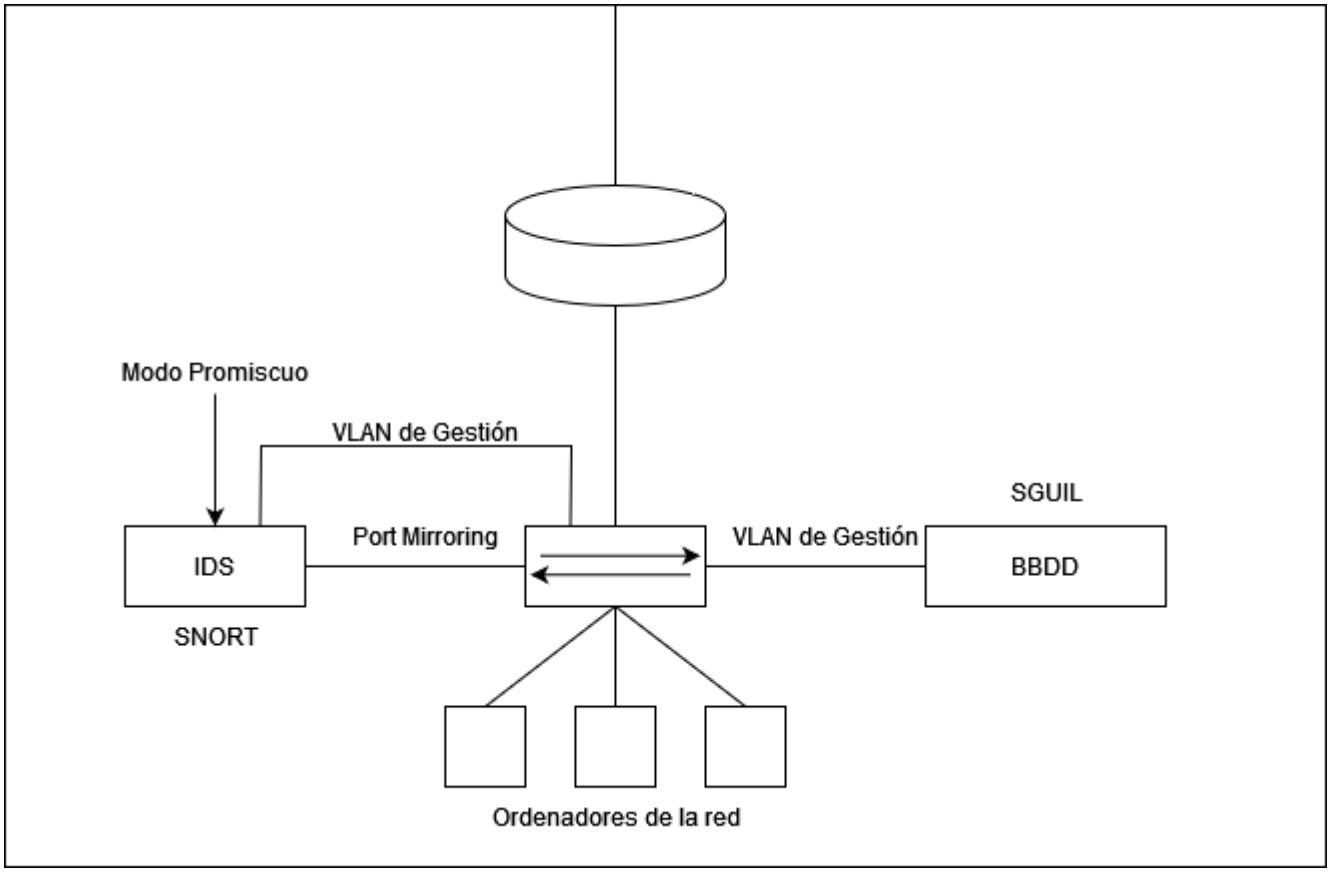
Definiciones

- **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

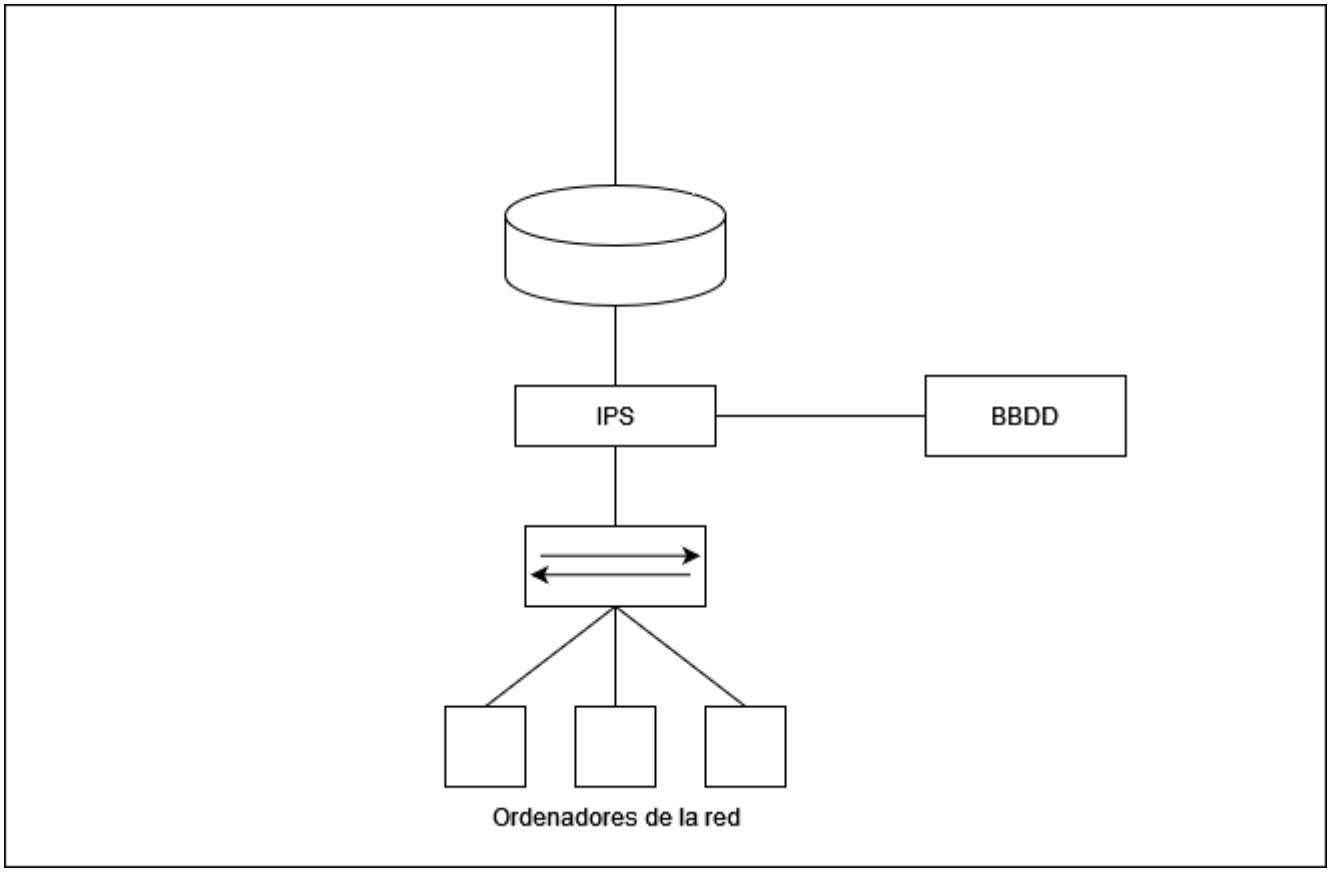
un colector de eventos de snort que los muestra de forma ordenada.



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. Por otro lado, SNMP v3, que es más segura ya que va cifrada, suele ser poco utilizada ya que suelen sobrecargar los procesadores de los equipos de red, aunque en la actualidad los equipos aguantan mejor su uso y sería una opción relativamente viable. En la actualidad a nivel de automatización existen otras herramientas más sencillas para hacer lo mismo que SNMP.

IPS: Intrusion Prevention System

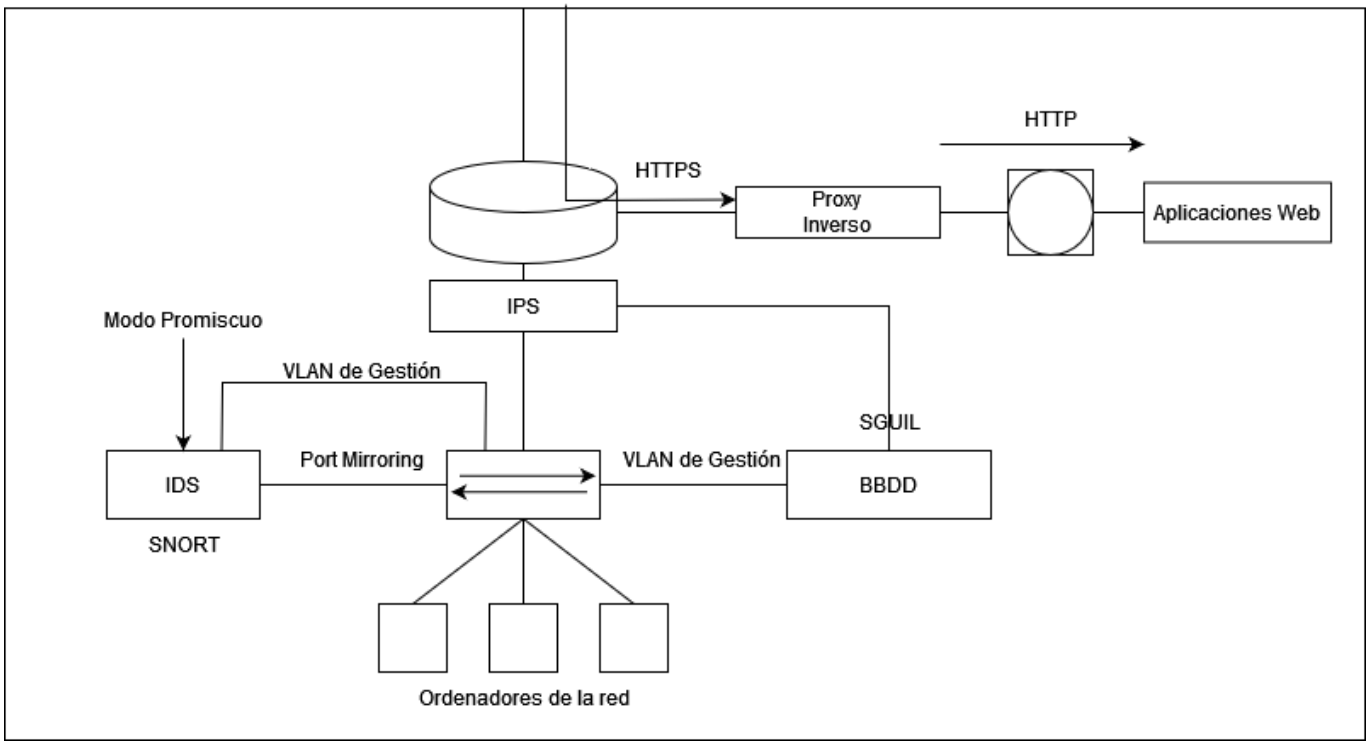
Los IPS, a diferencia de los IDS, se conectan In Line, por lo que van conectados de por medio, haciendo que el tráfico atraviese el equipo:



Los cisco 1941 utilizan un sistema IPS/IDS ya no soportado por cisco. En routers posteriores se usa un IPS/IDS llamado SNORT, que en la actualidad esta mantenido por CISCO En la serie 4621 los equipos usan Cisco IOX o Cisco XE que están basados en IOS y utilizan un contenedor con SNORT que corre dentro del router. Los IDS/IPS se basan en firmas, teniendo cierta similitud con los ACLs. El problema es que existen ataques clásicos basados en saturar el IPS o provocar que suenen alertas en exceso, dificultando la detección del ataque, sobrecargando la CPU, lo que hace que el IPS pase a dejar de filtrar parte del tráfico, pudiendo pasar este sin que se revise. El problema del IPS es que generan problemas de latencia y variabilidad del tráfico. Se recomienda perfilar las firmas que se quiere que se revisen y ajustarlo a las necesidades de la red para reducir la latencia.

IDPS: Intrusion Detection and Prevention System

La mayor parte de sistemas pueden operar tanto en modo IDS como IPS. Algunos IDS son capaces de analizar otros elementos de la red como logs o realizar análisis de flujos de datos, que analizan el conjunto de datos que van de un mismo origen a un destino en cierto período de tiempo acotado. LOS IDPS pueden analizar datos de capa 3, capa 4, aplicación y payload, en general pueden detectar ataques sofisticados.



Cuando se detecta una intrusión, el IDPS puede hacer varias cosas:

- Envía mensajes de log
- Los mensajes de log pueden ser alertas que vayan a consolas con operadores en un SOC.
- Tratar de evitar el éxito del ataque mediante el bloqueo

Existen varios tipos de IDPS:

- Basados en red: Monitoriza tráfico de red y analiza los protocolos IP, TCP, UDP, Aplicación... para identificar actividades sospechosas.
- Basados en Equipos: Analiza un equipo en busca de eventos que puedan representar una actividad ilegarl como conexiones salientes, cambio de permisos en archivos o cambio de privilegios en usuarios.

Los IDPS pueden ser desplegados en casi cualquier lugar, incluso fuera de la red, esto último puede parecer extraño ya que podría crear un exceso de alertas, pero es una práctica que aplican muchas organizaciones para infraestructuras críticas ya que permiten analizar a ataques a posteriori. Otro punto donde se puede colocar un IDPS es en la DMZ ya que es una zona que suele estar expuesta, se hace para detectar si un equipo ha sido infectado y si trata de pivotar el ataque a otros equipos de la red. Se desplegaran sensores IDPS por todas las zonas de la red para monitorizarla y asegurarla y se colocaran clientes IDPS en una zona central para monitorizar la red.

From:
https://www.knoppia.net/ - **Knoppia**

Permanent link:
https://www.knoppia.net/doku.php?id=redes:idsips&rev=1732900998

Last update: **2024/11/29 17:23**