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.

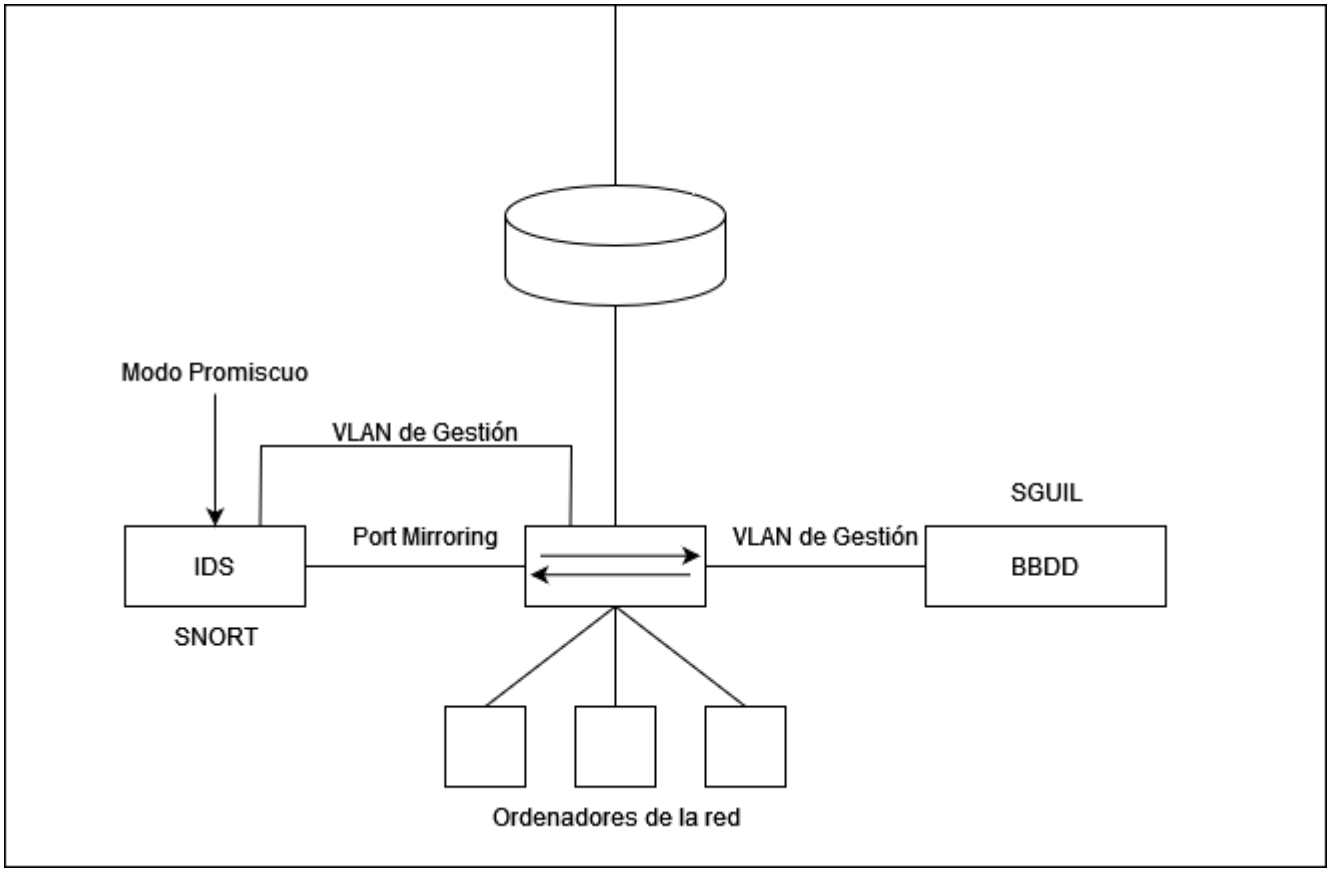
Definiciones

- **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

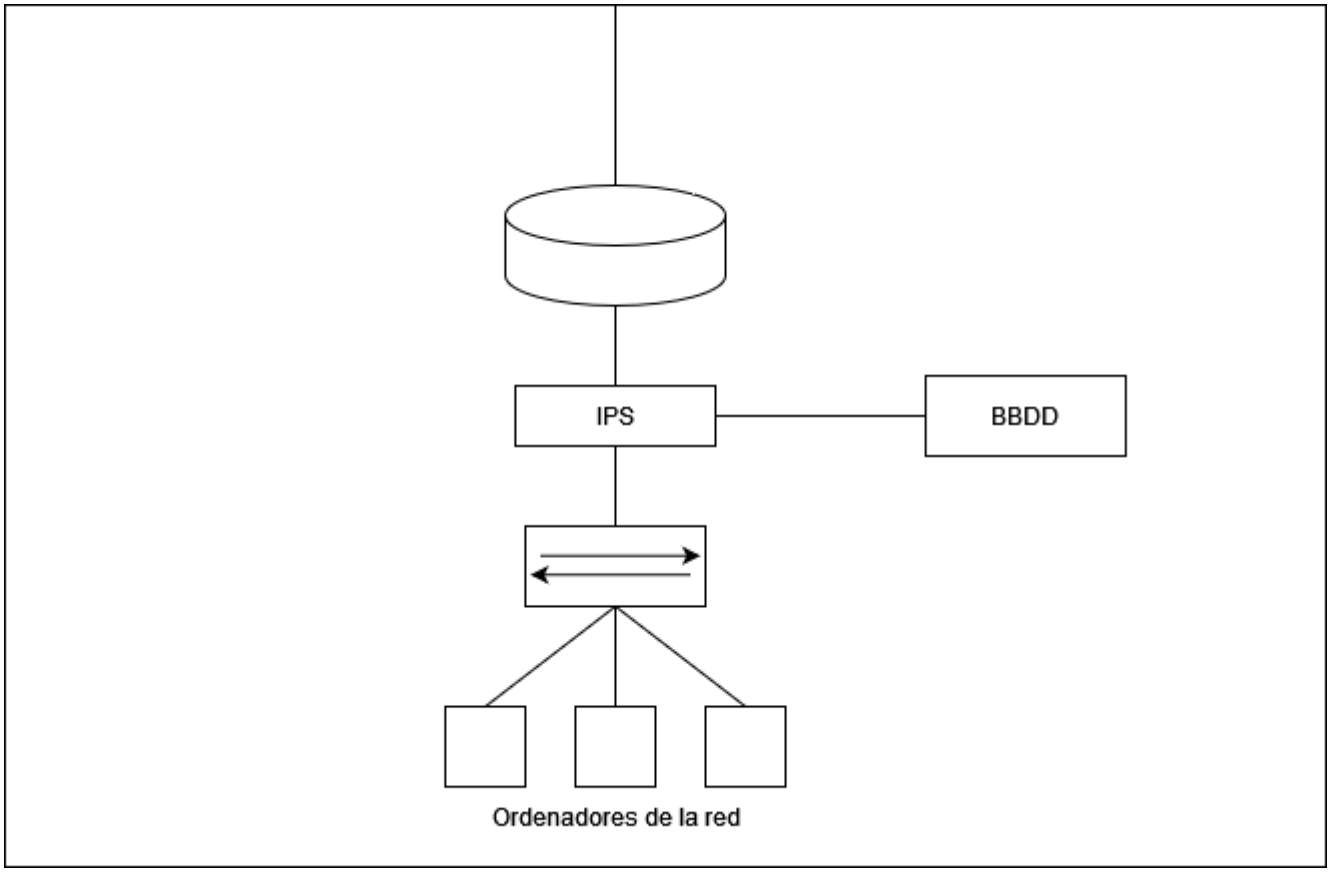
un colector de eventos de snort que los muestra de forma ordenada.



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

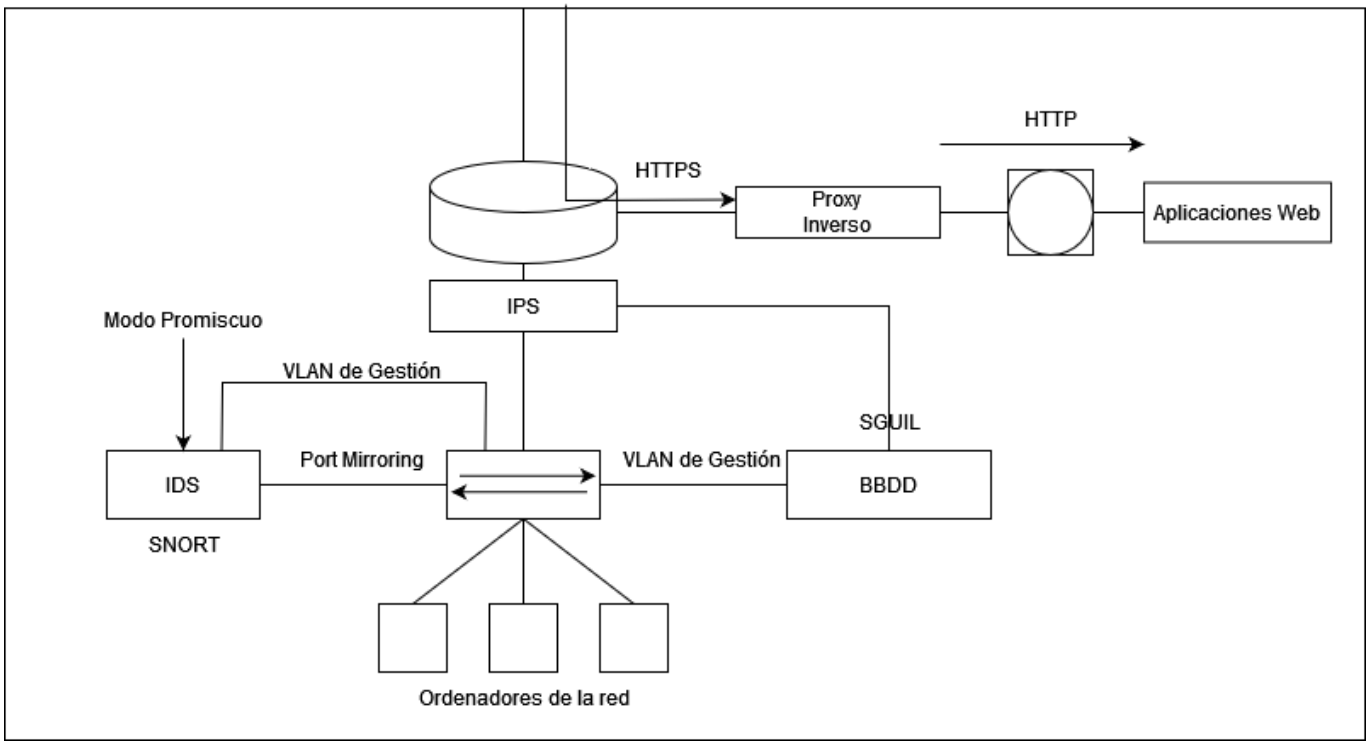
Los IPS, a diferencia de los IDS, se conectan In Line, por lo que van conectados de por medio, haciendo que el tráfico atraviese el equipo:



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.

Métodos de detección de instrucciones

Existen 2 principales aproximaciones: Basada en firmas y Basada en detección de anomalías

Detección basada en firmas

Compara los eventos observados con patrones correspondientes a ataques conocidos. Los IDS incorporan estos patrones en forma de reglas. En la actualidad se despliega un contenedor en el router que puede ser de SNORT para desplegar un IPS en un firewall usando una sintaxis y unas herramientas muy conocidas. Cada IDPS tiene su propio fichero de firmas y sistemas de reglas. Se suelen agrupar en base a servicios como HTTP, DNS, etc... y dentro de cada servicio por tipo de ataques, objetivos, etc... La idea es configurar la configuración. Un proveedor de firmas IDPS puede proveer diferentes tipos de firmas que deben ser usadas para un sistema correcto, no tiene sentido usar firmas de ataques para sistemas windows si nuestros equipos son linux. Los IDPS deben trabajar de forma complementaria con los firewall, se deben concentrar la funcionalidad de IDPS en el tráfico que deja pasar el firewall (No tiene sentido tener firmas activas para proteger de ataques que no deja pasar el firewall).

Ajustar las firmas a los servicios que tenemos es bastante trabajoso. La firma suele contener un mensaje descriptivo del ataque y contenido sobre el flujo de datos que explota la vulnerabilidad. Hay 3 principales tipos de firmas:

- Pattern Matching: Busca determinadas secuencias que coinciden con un ataque conocido.
- Análisis de protocolo: Comprueba que se siguen las reglas y normas del protocolo en cuestión
- Análisis Heurístico o de comportamiento: Relacionado con conjunto de acciones que pueden llegar a tener cierta complejidad como barridos de pings o escaneos de puertos entre otros ataques que no se detectan directamente por coincidencias de patrón o malos usos de protocolos. Se usa para ataques no atómicos (Complejos)

Detección basada en firmas

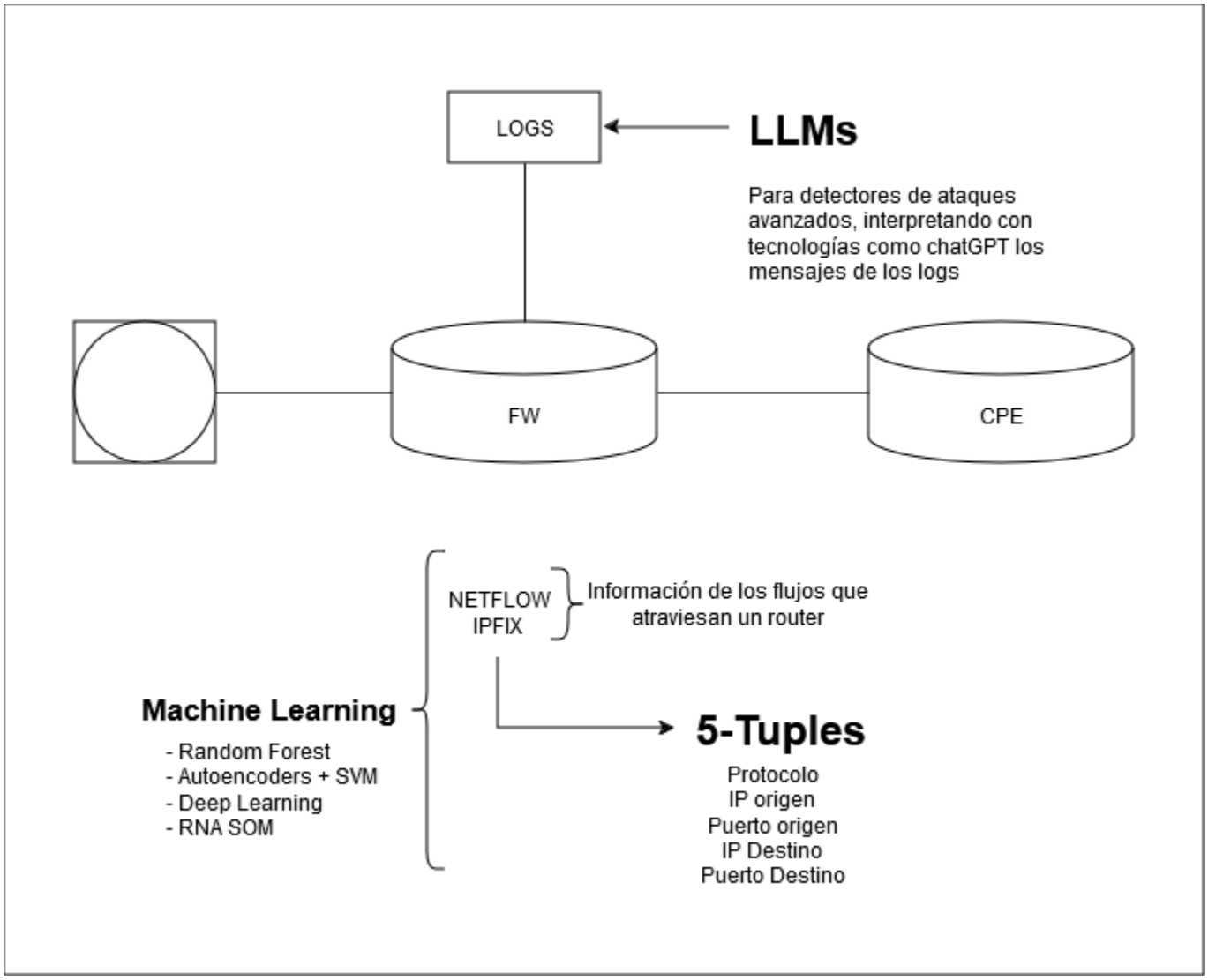
Tiene las siguientes ventajas:

- Es mucho más sencillo que las alternativas
- Efectivo frente a ataques conocidos
- Bajo número de falsos positivos
- La detección puede dar información sobre el tipo de ataque o como bloquearlo, lo que es útil para los adminsitradores.

Y los siguientes problemas

- Ineficaz contra ataques nuevos o variantes de ataques conocidos
- Es necesario actualizar las firmas constantemente
- Problemas ante ataques complejos que usan varios eventos que no son amenazas por sí mismos.

Detección basada en anomalías



Se establecen perfiles de actividad normal. Se usan Netflow e IPFIX para generar lo que se le llama 5-tuples: Protocolo, ip origen, puerto origen, ip destino y puerto destino. Se mira cuanto dura la conexión, paquetes enviados, tamaño de los paquetes enviados, etc… Este tipo de herramientas suelen necesitar un período previo de entrenamiento. Una de las estrategias que más se usan para analizar tanto el tráfico de netflow como otras características son las técnicas de machine learning, además de redes de neuronas de mapas auto organizados (SOM). También se usa la información generada por los Firewalls. Las ventajas de etas tecnologías son:

- Pueden detectar técnicas de ataque no conocidas, un atacante tiene más difícil pasar desapercibido ya que no sabe que puede generar una alerta
- Eficaz contra ataques desde el interior y APTs (Amenazas Avanzadas Permanentes)
- Pueden usarse para aprender firmas de nuevos ataques.

También tienen varios inconvenientes:

- Falsos positivos elevados
- Requieren período de aprendizaje.
- Las alamas son más difíciles de entender

Para entrenar estos sistemas se suelen utilizar las firmas antiguas, los sistemas basados en machine learning necesitan hacer entrenamiento supervisado, usándose las alertas generadas por un sistema basado en firmas, lo que hace que el sistema aprenda que puede ser un ataque. El problema es que las anomalías no son siempre ataques, por ejemplo, si un día en una universidad muchos alumnos

realizan entregas de prácticas a la vez, ocurre una anomalía en la red y el sistema puede idenificar esta erróneamente como un ataque. Las alertas suelen ser más difíciles de entender por se se suelen emitir de forma genérica, la alerta sería algo como un: Se ha detectado X que podría ser un ataque.

Ventajas de los IDPS

- Nos proporcionan sistemas de detección de ataques que no podrían ser detenidos con proxys o firewalls
- Protegen contra ataques complejos como escaneos de puertos
- Permiten identificar de forma clara los ataques recibidos
- Se proporciona información para evitar problemas
- Además puede disuadir a los usuarios de violar las políticas de seguridad

Desventajas de los IDPS

- No son totalmente precisos
- Las respuestas no siempre son inmediatas, hay un proceso de detección y debemos analizar la anomalía y mitigarla (Aunque si estas son muy claras ya las filtra el propio IDPS)
- Existen estrategias para reducir la efectividad de los IDPS como por ejemplo generar ruido, lo que genera un exceso de alertas, dificultando la detección de un ataque.
- Son efectivos solo a corto plazo, a medio y largo plazo necesitan ser reajustados constantemente.

Network Based IDPS

Monitorizan el tráfico de la red. Se colocan sensores (Dispositivos físicos (Appliances) o virtuales (SNORT en un PC)) que reciben una copia del tráfico y lo analizan. Se pueden incorporar de 2 formas:

- IN-LINE (IPS): Desplegado de tal forma que todo el trafico pasa por el, se sitúa entre conexiones de red, puede bloquear el tráfico y generar alertas. Pueden ser colocados dentro de los firewalls o antes/después de un firewall. Security Onion es una distribución Linux con herramientas orientadas a implementación de medidas de seguridad defensiva y no ofensiva que trae un gestor de IDPS para recibir información de múltiples IDPS que puede ser visualizada en una interfaz web.
- ON-LINE o pasivos (IDS): Monitorizan una copia del tráfico. Se colocan varios sensores entre el CPE y el Firewall. Toda la información recopilada se manda a un gestor IDPS que almacena y monitoriza todos los eventos de forma centralizada.

Los IDPS de red puede detectar los siguientes ataques:

- Ataques de capa de aplicación
- Ataques a la capa de transporte
- Ataques a capa de red
- Uso de servicios no esperados
- Violaciones de políticas de seguridad

Capacidades de prevención para INLINE:

- Capacidad de firewalling
- Limitación de ancho de banda para prevenir ataques DDOS
- Modificacion de contenido malicioso

Capacidades de prevención ONLINE:

- Finalización de conexiones

Ambos pueden reconfigurar otros equipos de red y ejecutar programas definidos por el adminsitrador.

Hay las siguientes limitaciones:

- No se puede trabajar con tráfico cifrado como TLS, VPNs o IPSec.
- Capacidades de análisis limitadas
- Pueden generar latencia y degradar el rendimiento de la red
- Los IDS pueden detectar un ataque, pero no se sabe si fue exitoso o no.
- Existen ataques contra los IDPS como Blinding o DDoS

Host Based IPS

Agentes que se ejecutan en dispositivos finales monitorizando eventos que suceden en el host (Como los EndPoint Security). Detectan cambios en archivos críticos y cambios de configuración. Hay casos donde esto solo se aplica al dispositivo y en soluciones enterprise se manda información a un equipo central que gestiona las alertas y demás.También pueden estar en servidores que protegen servicios o aplicaciones específicas. Si una aplicación intenta hacer algo sospechoso se genera una alerta y se bloquea la aplicación. También detecta usos indebidos del sistema.

Pueden bloquear tráfico de red, evitar la ejecución de malware y facilita la detección de procesos que accedan a procesos de sistema. El problema es que consumen muchos recursos, se pueden producir retardos en el envío de alertas, sobre todo si es envío periódico en vez de alertas, si se compromete el dispositivo se puede desactivar el IDPS. En una organización grande interesa que estos sistemas funcionen de forma centralizada, volcando la información en un solo punto. Pueden bloquear también acciones legítimas por error y necesitan actualizaciones periódicas, lo que puede provocar conflictos.