Trabajo de Investigación
IDS / IPS

Seguridad en Redes

Docente: Ing. Gonzalo Vilanova

Alumna: Flavia De Rosa

Legajo: 158.739-0

Comisión: K4571

Introducción:

Estas herramientas integran la capacidad de detectar ataques cibernéticos, además de realizar acciones que logran anular sus efectos. Es muy recomendable optar por estos sistemas, en especial si se desea garantizar que las amenazas de ataques informáticos se materialicen o bien, que generen el menor nivel de impacto posible.

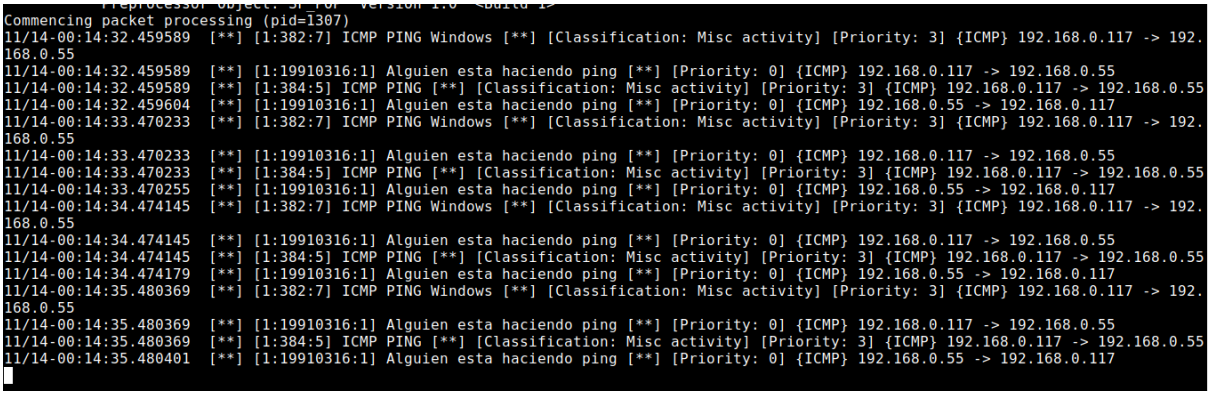
Los IDS/IPS son un complemento que ofrece mayor seguridad a las redes de distintos tamaños, principalmente aquellas redes que requieren un alto nivel de respuesta y servicios. Estos sistemas pueden aplicarse a software o hardware. Tienen la capacidad de detectar ataques cibernéticos y realizar las acciones necesarias para anular los efectos dañinos que se pudieran ocasionar a la red.

Estos sistemas una vez actualizados son capaces de reconocer vulnerabilidades de las aplicaciones más comunes a puertos abiertos en el firewall.

Log

Un log es un registro que deja un sistema informático. Por ejemplo: accesos de usuarios, actividades de borrado y cambios realizados en el sistema.
Un típico archivo de log tiene el siguiente formato, que responde a las preguntas: **cuándo, qué y quién.**
Con esta información podemos ver claramente las actividades que se han realizado en nuestros sistemas y, por lo tanto, con un pequeño análisis podríamos detectar situaciones extrañas y anómalas.
Sin embargo, el análisis de cada log es imposible en entornos grandes, debido a que no se tiene la capacidad para analizar todos estos sistemas.
Es bajo ese escenario donde entran en juego los sistemas IDS, IPS, HIDS, NIPS, SIEM.
Estos sistemas tienen la capacidad de analizar un gran número de fuentes de registros con el objetivo de encontrar anomalías para detectar y luego informar, en el caso de los IDS, o prevenir y responder, en el caso de los IPS y SIEM.

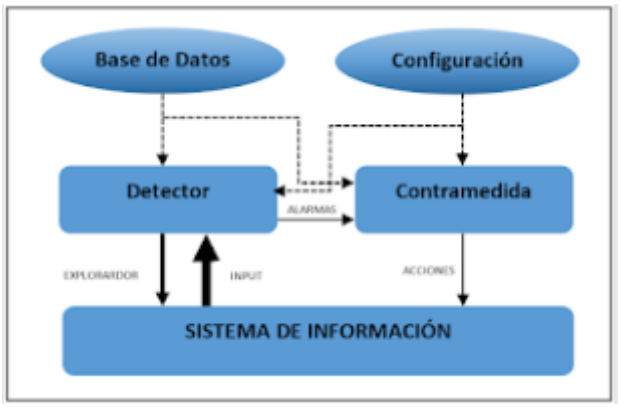
Captura de Logs de snort ante un alerta de una regla icmp



IDS (Intrusion Detection System)

Es una herramienta que tiene como función principal detectar intrusos en nuestros sistemas, un IDS puede conectarse a un gran número de fuentes de log para encontrar anomalías.
Es importante decir que **los IDS no pueden detener los ataques por sí solos**, sino que necesitan herramientas adicionales que ayuden en esta tarea.
Por ejemplo, la conexión a un firewall para el bloqueo.

Los IDS pueden realizar dos tareas fundamentales: la prevención y la reacción. Considerando las tareas que realizan los IDS, podemos distinguir entre **IDS pasivo** (realizan la prevención escuchando el tráfico) e **IDS reactivos** (elaboran respuestas defensivas antes del ataque).

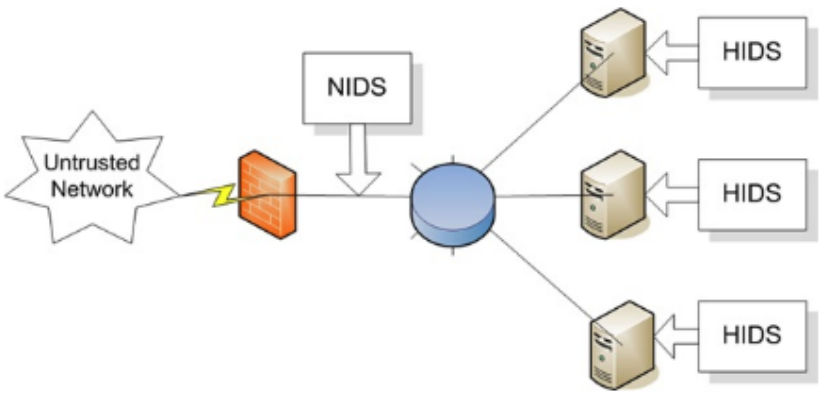


Tipos de IDS

https://infotecs.mx/blog/sistema-de-deteccion-de-intrusos.html

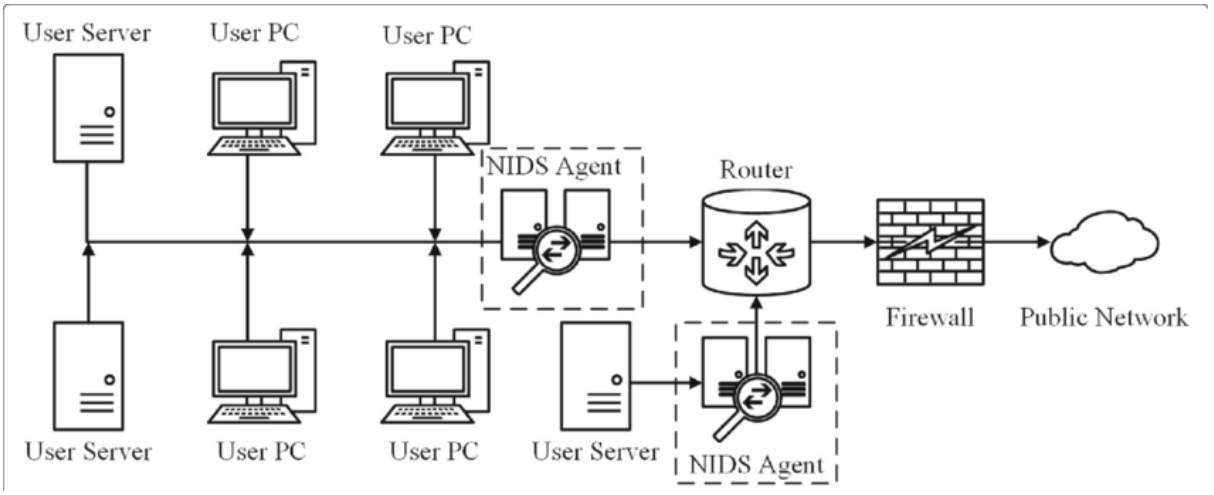
1. **HIDS (Host Intrusion Detections System)**

Se enfoca en la detección basada en host de una única máquina, mirando sus registros de auditoría. Son capaces de detectar situaciones como los intentos fallidos de acceso o modificaciones en archivos considerados críticos.
Algunos ejemplos de HIDS: **Ossec, Wazuh, Samhain**.



2. **NIDS (Network Intrusion Detections System)**

Se enfoca en la detección monitorizando el tráfico de la red a la que están conectados los hosts. Permiten detectar paquetes maliciosamente y diseñados para no ser detectados por los firewall.
Algunos ejemplos de NIDS: **Snort, Suricata, Bro, Kismet**.



3. **DIDS (Distributed Intrusion Detection Systems).**

Es parecido a un NIDS, pero los sensores se distribuyen en distintos puntos de la red y envían las alertas a un sistema centralizado donde serán analizadas por el operador.

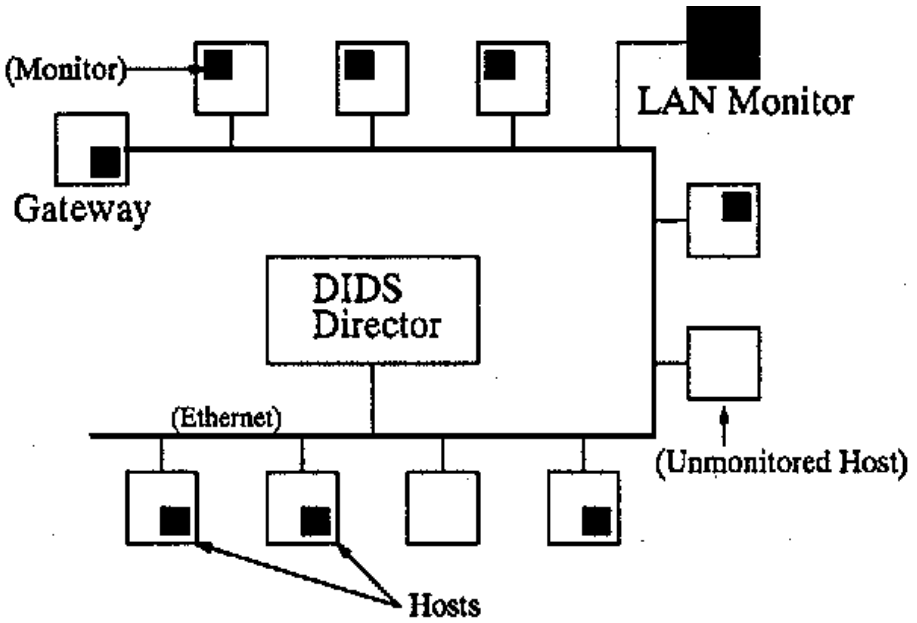


Figure 1: DIDS Target Environment

HIDS más conocidos

Ossec

https://www.ossec.net/
Es un sistema IDS basado en hosts que es desarrollado por un grupo de personas que forman parte de un proyecto de código abierto.
Cuenta con un amplio equipo de desarrolladores dedicados a este sistema, además de una activa comunidad que está orientada a la ayuda a usuarios, creación de traducciones, documentación de soporte y mucho más. OSSEC ya pasa las 500.000 descargas anuales y lo mejor de todo, es que es multiplataforma: está disponible en Windows, macOS.
Este sistema IDS cuenta con su host compatible con Linux

Funcionamiento

OSSEC monitorea los logs de los diversos componentes de tu sistema en tiempo real. Es capaz de detectar todo tipo de cambios a archivos individuales, incluyendo a los registros de Windows más importantes. Esta solución es un sistema IDS, pero así también tiene algunas prestaciones de IPS, estas prestaciones IPS consisten en la respuesta a ataques mediante sus propias capacidades y sus integraciones con herramientas de terceros.

NIDS más conocidos

Snort

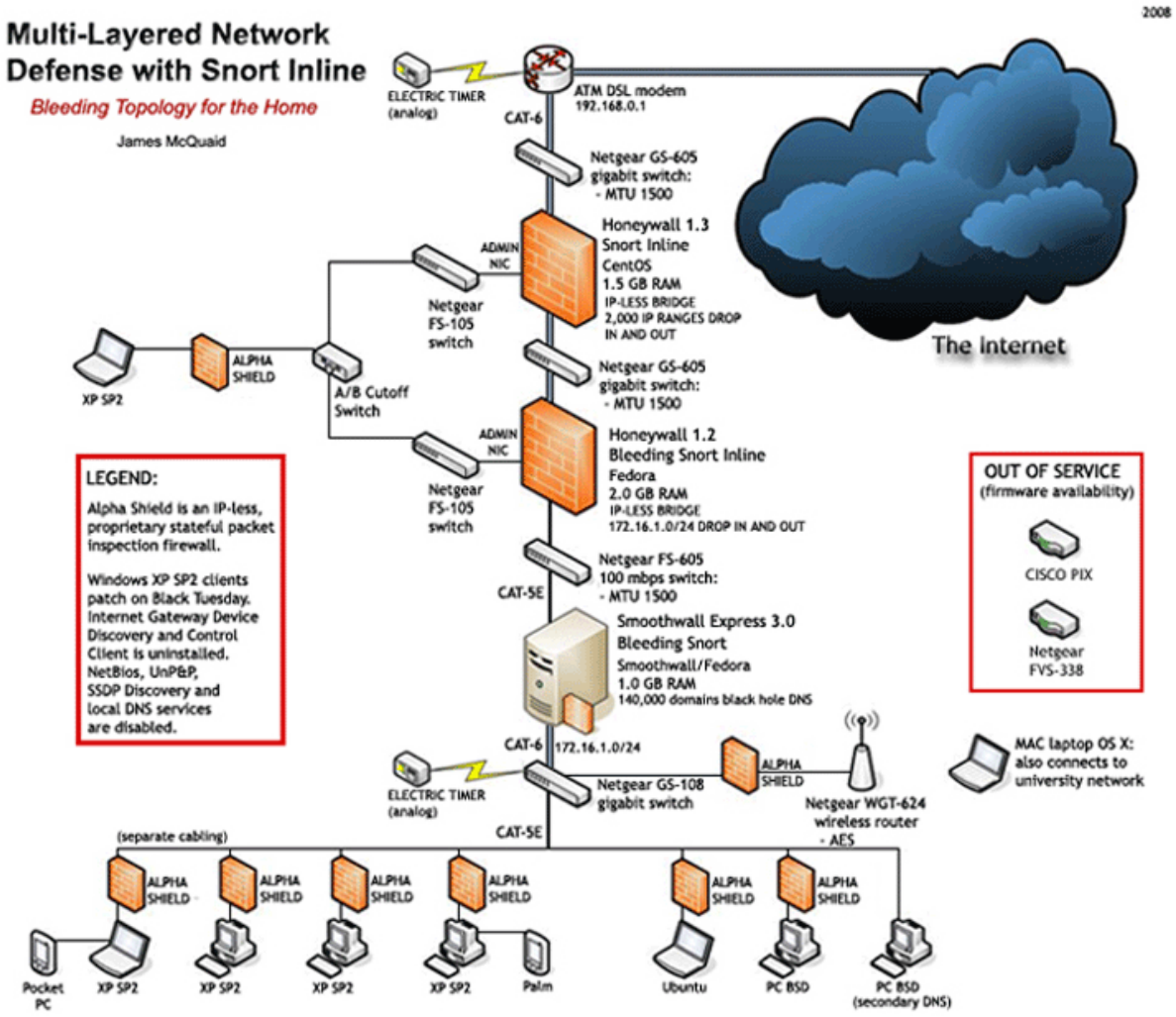
https://www.snort.org/
Es un sistema de detección de Intrusos de Red (NIDS) basado en código abierto, multiplataforma, además es un sniffer de paquetes y un detector de intrusos basado en red (se monitoriza todo un dominio de colisión). Es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas como lo es MySQL.

Implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida. Así mismo existen herramientas de terceros para mostrar informes en tiempo real (ACID) o para convertirlo en un sistema Detector y Preventor de Intrusos.

Las Característica más apreciada de Snort, además de su funcionalidad, es su subsistema flexible de firmas de ataques, **Snort tiene una base de datos de ataques que se está actualizando constantemente** y a la cual se puede añadir o actualizar a través de la Internet

Una de las grandes ventajas de Snort es que cuenta con una comunidad grande y activa. Cualquier persona que lo necesite puede recibir asistencia o dar asistencia, de manera a que todos puedan sacar mayor provecho de esta solución. Además, es completamente gratuita, abierto a modificaciones mediante contribuciones. Las actualizaciones de este sistema IDS

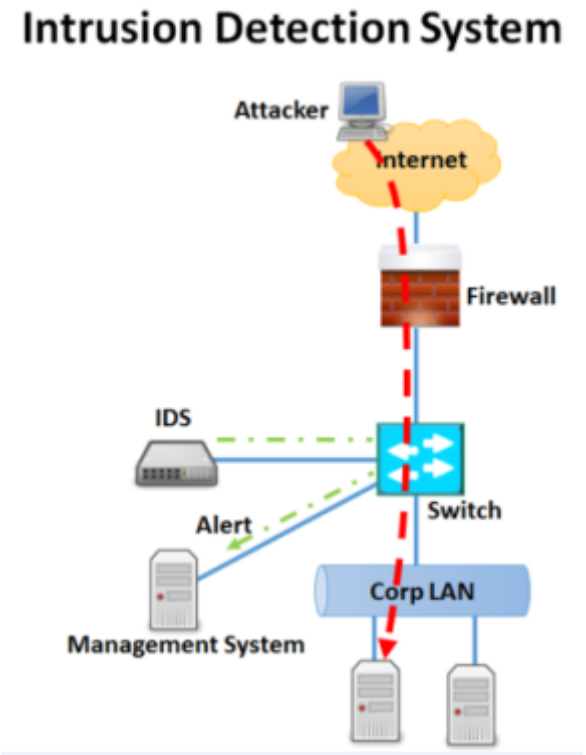
se realizan con frecuencia en base a unas reglas de comunidad y a la licencia GPL, es decir, Licencia Pública General.



También cuentan con soluciones que son de pago, las cuales son algo más accesibles en relación a otras que tienen esta particularidad.
Una curiosidad es que Snort está bajo la gestión del gigante Cisco y varias de las funcionalidades responden considerando las reglas de su sistema propietario NGIPS. Estas siglas responden a Sistema de Prevención de Intrusiones de Siguiente Generación.
https://www.snort.org/#get-started

Componentes

Un IDS puede estar compuesto de varios componentes: **sensores que generan eventos de seguridad, una consola para controlar eventos, alertas de control y los sensores, y un motor central que registra los eventos** registrados por los sensores en una base de datos utilizando un sistema de reglas para generar alertas de eventos de seguridad recibidas.
Hay varias maneras de clasificar un IDS, en función del tipo, la ubicación de los sensores y la metodología utilizada por el motor para generar las alertas. En muchas implementaciones de IDS sencillos los tres componentes se combinan en un único dispositivo o aparato.



Los sistemas de detección de intrusos están compuestos por tres elementos funcionales básicos:

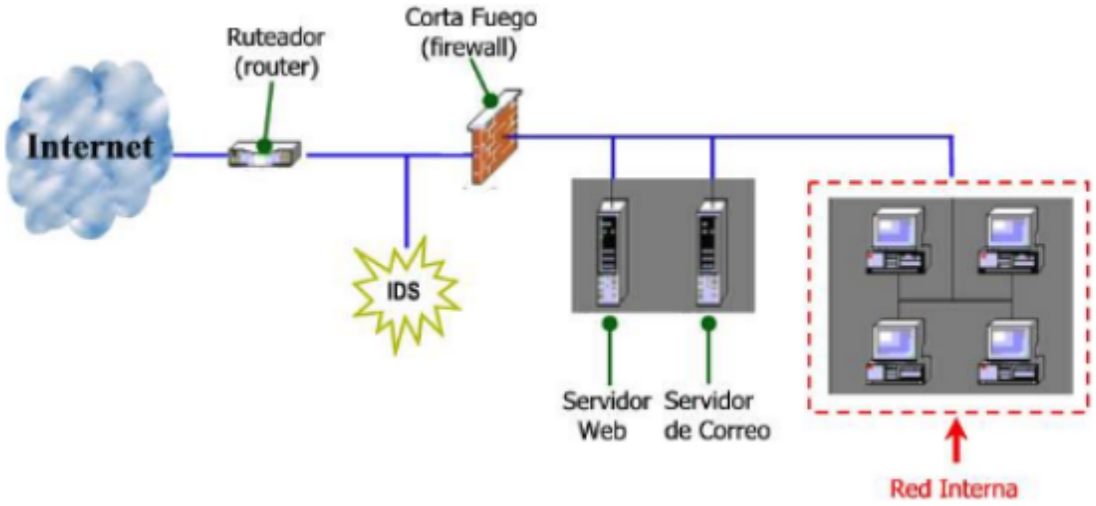
- Una fuente de información que proporciona eventos del sistema.
- Un motor de análisis que busca evidencias de intrusiones.
- Un mecanismo de respuesta que actúa según los resultados del motor de análisis.

Funcionamiento

Un sistema de prevención de intrusos, al igual que un sistema de detección de intrusos, funciona por medio de módulos, pero la diferencia es que la última alerta al administrador ante la detección de un posible intruso.
Se basa en el análisis pormenorizado del tráfico de red. el cual al entrar al analizador es comparado con firmas de ataques conocidas, o comportamientos sospechosos.

El IDS, utiliza tres tipos de información: La recopilada tiempo atrás con datos de ataques previos, la configuración actual del sistema y la descripción del estado actual de términos de comunicación y procesos

El IDS no solo analiza que tipo de tráfico es, sino que también revisa el contenido y su comportamiento.

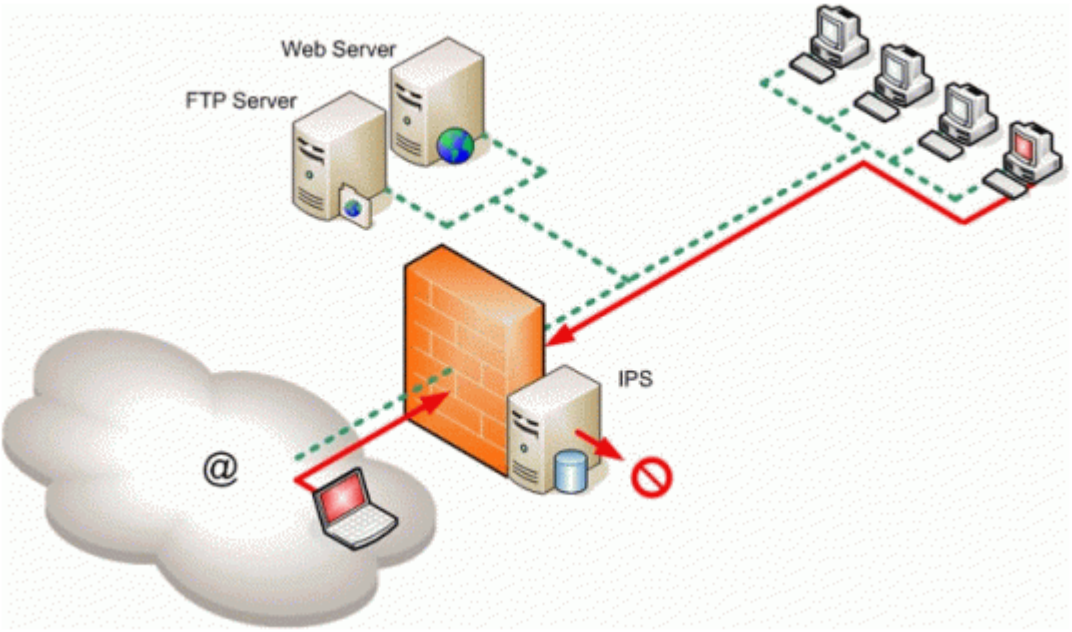


IPS (Intrusion Preventions System)

Es una herramienta que permite la prevención de los ataques, normalmente **ejerce el control de acceso a una red**. Los IPS están muy relacionados con los IDS y se consideran como una extensión de estos.

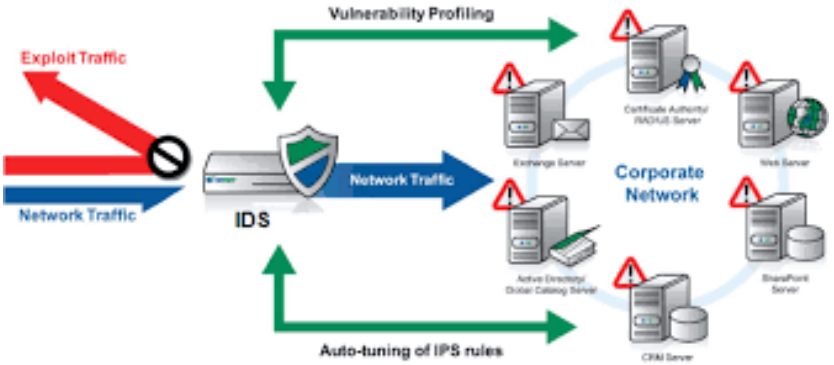
Los sistemas de prevención de intrusos pueden verse como la evolución de dos elementos que han dominado la seguridad en todas las redes informáticas del mundo:

1. **Firewall**: Es el elemento que garantiza o bloquea el acceso a los recursos de nuestra red.
2. **IDS**: Permite mantener el estado de las conexiones y examinar el contenido de los paquetes que circulan por nuestra red.

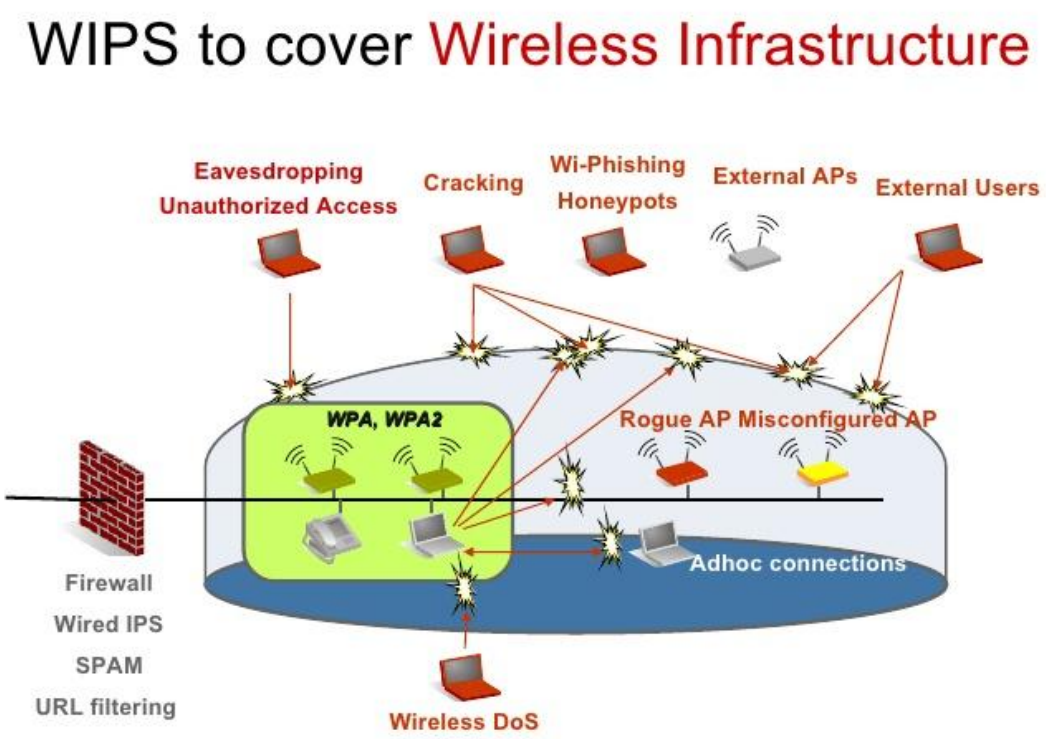


Tipos de IPS

1. **NIPS:** basados en red, buscan tráfico de red sospechoso.

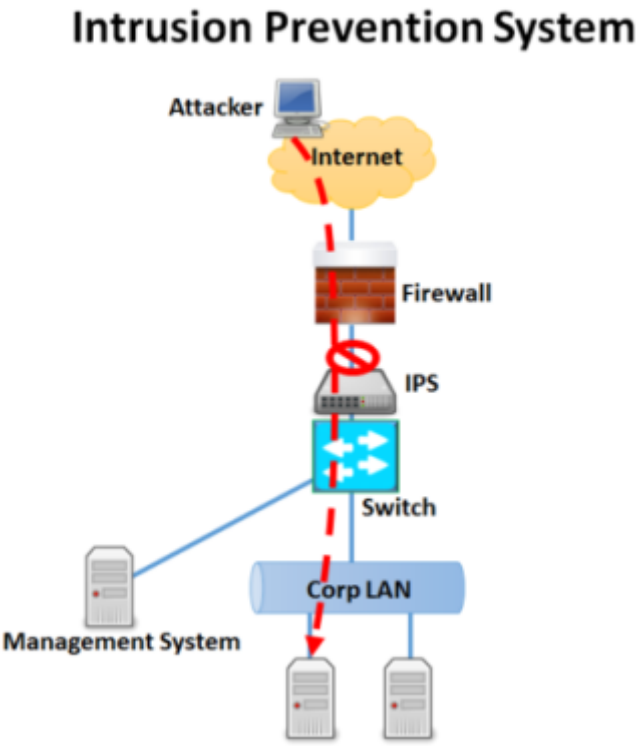


2. **WIPS:** basados en Wireless, buscan en la red inalámbrica tráfico sospechoso.



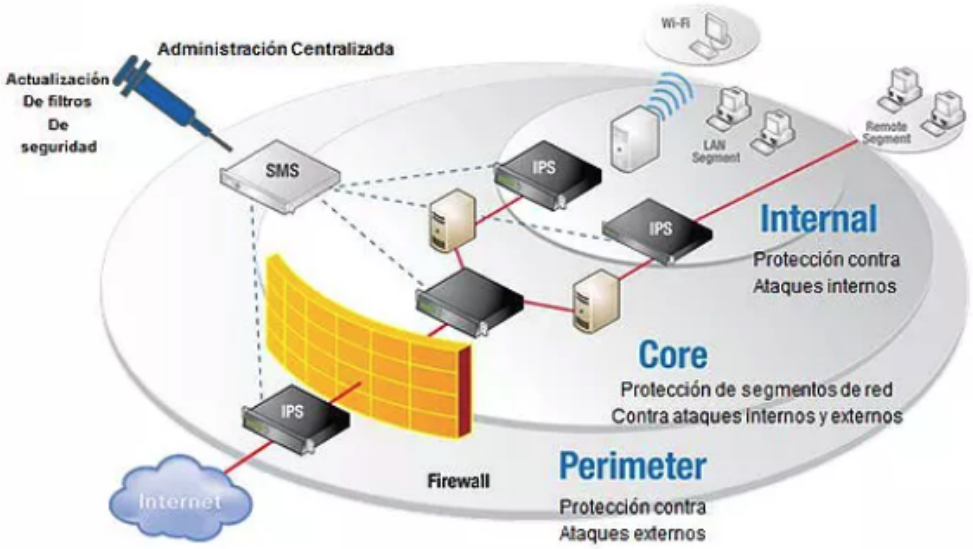
3. **NBA:** basados en el comportamiento de la red, examinan el tráfico inusual como ciertas formas de malware, ataques de denegación de servicios o violaciones de las políticas de seguridad.
4. **HIPS:** buscan actividades sospechosas en host únicos.

Componentes



Funcionamiento

Los IPS presentan una mejora importante sobre las tecnologías de firewall tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o Puertos



Arquitectura IPS

Cuando se protege un sistema basándose en registros estos se analizan mediante una auditoría y para estos se requiere que estos registros sean **almacenados de forma segura de modo que el intruso no pueda eliminar registros** y la alteración de la información contenida y no afectar el rendimiento del sistema proteger.

- Fuente de Datos
- Basados en Máquinas
- Basados en Redes
- Basados en Aplicación
- Basados en Objetivo
- Análisis de respuestas

Tipos de Análisis y Respuestas del IPS

Después del proceso de recopilación de la información, se lleva a cabo **el proceso de análisis**. **Los dos tipos principales son:**

- Detección de usos indebidos
- Detección de anomalía

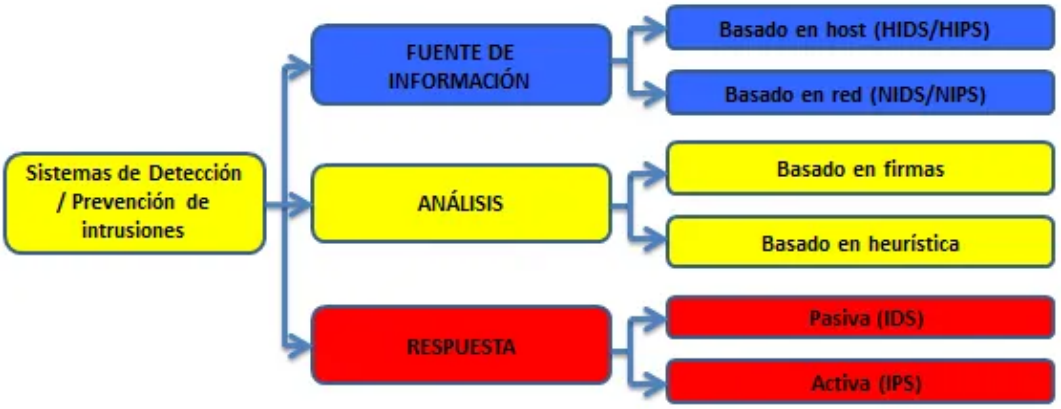
Otro detalle a la hora de distinguir formas de detección de intrusos es teniendo en cuenta el uso de **análisis de tiempo**:

- Por lotes
- Tiempo Real

Respuestas:

- Respuestas Pasivas
- Respuestas Activas

Clasificación general IDS/IPS



Como se puede observar en el diagrama, existen 3 bloques funcionales dentro del proceso de monitorización:

- **Una fuente de información u objeto a monitorizar,** que procesa, transmite o almacena datos
- **Una acción de análisis en donde se recopilarán** datos de comportamiento de la fuente de información y se compararán con los parámetros esperados
- **Una respuesta frente a un comportamiento anómalo,** que puede ser pasiva (alerta) o activa (que puede modificar el entorno para re-alinear el comportamiento)

Bajo este escenario, un sistema que se encargue de obtener datos de una fuente de información, analizarlos, compararlos contra valores predefinidos de comportamiento para detectar comportamientos anómalos y generar acciones de respuesta se denomina «Sistema de detección/prevención de intrusiones«, entendiéndose «intrusión» como una acción no autorizada que puede comprometer la seguridad del objeto monitorizado. Ejemplos de sistemas de detección/prevención de intrusiones se pueden encontrar en sistemas de video-vigilancia física, alarmas, sistemas industriales de control automático, etc.

En el área de seguridad de la información, un sistema de detección de intrusiones («Intrusion Detection System» – IDS) o sistema de prevención de intrusiones («Intrusion Prevention System» – IPS) es un elemento que monitoriza el comportamiento de redes, host y/o aplicaciones en búsqueda de patrones de comportamiento malicioso, compartiendo las mismas características descritas anteriormente, que permiten catalogarlos de acuerdo con su funcionamiento:

- Dependiendo de la fuente de información analizada:
    - **Red (Network IDS/IPS):** que analiza el comportamiento de una red de datos a través de la captura de tráfico empleando técnicas de análisis de paquetes («sniffing»), incluyendo redes inalámbricas (Wireless IDS/IPS)

        - **Host (Host IDS/IPS)**: que analiza el comportamiento de un equipo en particular (por lo general su sistema operativo) y los eventos relacionados con seguridad.
- **Dependiendo del tipo de análisis ejecutado:**
    - Basado en patrones de ataques conocidos (**firmas**)
    - Basado en análisis de comportamiento (**heurística**)
- **Dependiendo del tipo de respuesta activada**:
    - **Pasiva**: No hay una modificación activa del entorno. Se genera una alerta o alarma al responsable. Estos sistemas son catalogados como IDS
    - **Activa**: Adicional a la alerta, se genera una acción correctiva que puede modificar el entorno, como la finalización de una conexión o el bloqueo de un tráfico específico. Estos sistemas son catalogados como IPS

Ventajas/Desventajas de IDS/IPS

IDS

La principal ventaja de un sistema IDS es que permite ver lo que está sucediendo en la red en tiempo real en base a la información recopilada, reconocer modificaciones en los documentos y automatizar los patrones de búsqueda en los paquetes de datos enviados a través de la red. **Su principal desventaja es que estas herramientas, sobre todo en el caso de las de tipo pasivo, no están diseñadas para prevenir o detener los ataques que detecten**, además son vulnerables a los ataques DDoS que pueden provocar la inoperatividad de la herramienta.

IPS

Las ventajas de un IPS son:

- escalabilidad al gestionar multitud de dispositivos conectados a la misma red;
- protección preventiva al comprobarse de forma automatizada comportamientos anómalos mediante el uso de reglas prefijadas;
- fácil instalación, configuración y administración al estar disponibles multitud de configuraciones predefinidas y centralizar en un punto su gestión, aunque puede ser contraproducente para su escalabilidad;/
- defensa frente a múltiples ataques, como intrusiones, ataques de fuerza bruta, infecciones por malware o modificaciones del sistema de archivos, entre otros;
- aumento de la eficiencia y la seguridad de la prevención de intrusiones o ataques a la red.

Entre sus desventajas, destacan **los efectos adversos que pueden producirse en el caso de que se detecte un falso positivo**, si por ejemplo se ejecuta una política de aislamiento de las

máquinas de la red o en el caso de que se reciban ataques de tipo DDoS o DoS que pueden provocar su inutilización.

SIEM (Security Information and Event Management)

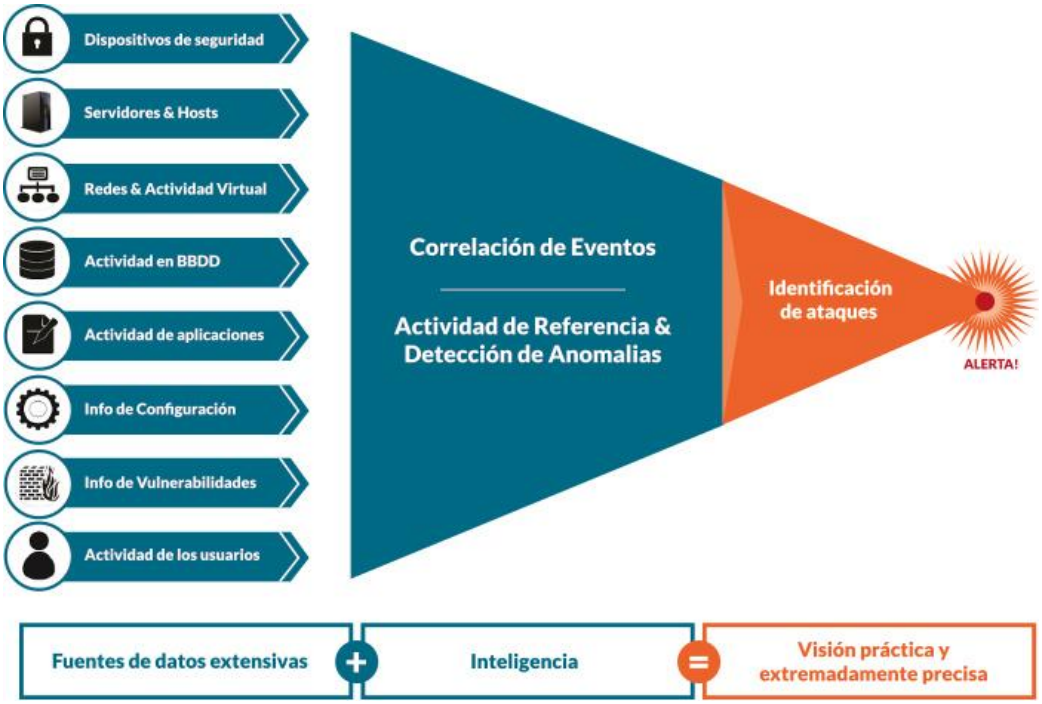
Es una herramienta que nos permite **centralizar la interpretación de los registros** relevantes de seguridad.

Un **SIEM** nos permite recopilar, normalizar y correlacionar eventos de seguridad, proporciona inteligencia de seguridad, descarta falsos positivos, evalúa el impacto de un ataque, unifica la gestión de la seguridad, centraliza la información e integra herramientas de detección de amenazas.

Tipos de SIEM

Las Herramientas de Gestión de la Seguridad de la Información ante eventos (SIEM) incluye Gestión de la Seguridad de la Información (SIM) y la gestión de eventos de seguridad (SEM) juntos proporcionan una solución integral para sus sistemas.

SIEM recopila datos relacionados con la seguridad de varias fuentes y los analiza.
Además, las soluciones SIEM pueden ayudar a su empresa con los problemas relacionados con el cumplimiento.



Uno de los SIEM por excelencia es **OSSIM**.

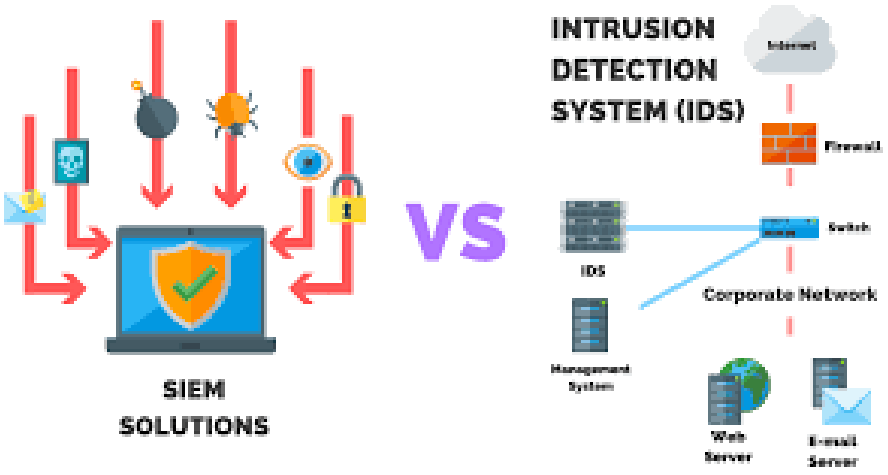
Herramientas que utiliza

- Descubrimientos de activos: **prads, Nmap**
- Detección de amenazas: **OSSEC, snort, Suricata**

- Monitorización: **fprobe, ntop, tcpdump, Nagios**
- Evaluación de vulnerabilidad: **OpenVas, Nikto**

Comparativa con IDS

Las soluciones **IDS y SIEM trabajan juntas**. Las herramientas I**DS detectan todo tipo de actividad sospechosa, violación o evento de seguridad** que ocurre dentro del alcance de sus sistemas y red. Luego, **SIEM es informado sobre tales actividades para notificar a los administradores y tomar las acciones necesarias**.



Herramientas que incluye el paquete de IDS e IPS

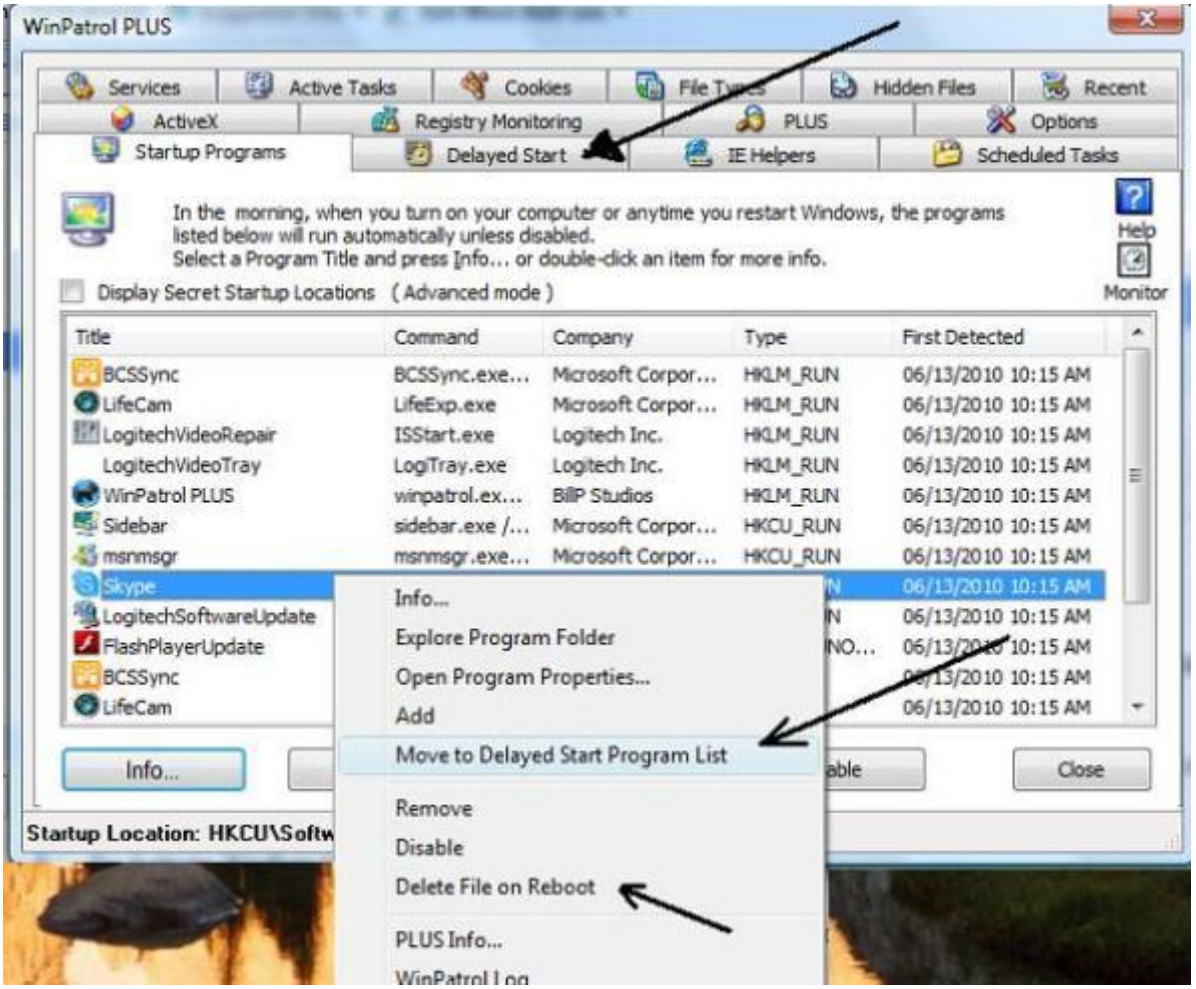
Security Onion

Es una distribución de Linux que funciona como una solución robusta de seguridad. La misma **incluye su propio sistema IDS/IPS y funciona mediante soluciones base como OSSEC y Snort.** Además, también funciona en base al sistema Suricata en relación a las funcionalidades IDS/IPS basados en red.
Un punto super interesante que puede marcar la diferencia a la hora de elegir la solución que necesitas es que **viene integradas con diversas herramientas.** Algunas de ellas son las siguientes:

- **Elasticsearch** (motor de búsqueda distribuido)
- **Logstash** (herramienta de administración de logs)
- **Kibana** (panel de visualización de datos de código abierto)
- Bro (monitor de seguridad de redes)
- Sguil (monitor de seguridad de redes)
- Squert (visualización de datos almacenados de eventos)
- NetworkMiner (herramienta de análisis de redes) y otras herramientas más orientadas a la seguridad

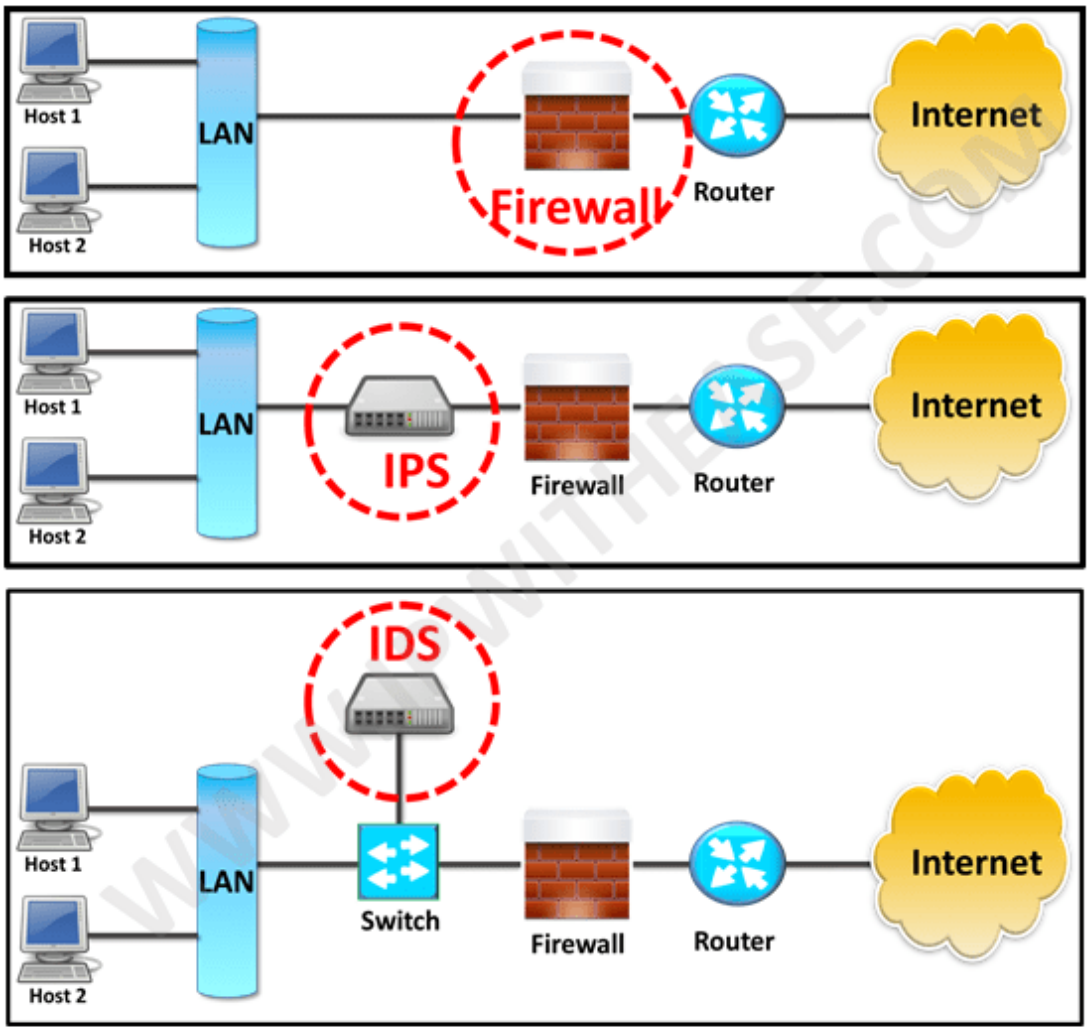
WinPatrol

Muy probablemente, esta **es la solución con funcionalidades IDS/IPS más liviana que podemos encontrar**. No ocupa ni siquiera 2MB, así también la instalación no precisa de más de 4,5 MB. Una vez instalado, ya puedes ejecutarlo muy rápidamente.
Es un programa que te ayuda a gestionar de mejor manera los procesos, programas y otros aspectos de tu sistema operativo. Sin embargo, **cuenta con funcionalidades orientadas a la prevención y detección de intrusiones que puede ser de gran ayuda a usuarios individuales**.
Cuenta con características que **permiten la monitorización ante cambios en asociaciones de tipos de archivos y creación de tareas programadas varias.** Además, podrás tener visibilidad de cambios importantes como los archivos de registro de Windows, archivos ocultos y más.



Sistemas IDS/IPS vs Firewall

Las prestaciones que ofrece cada uno pueden ser similares , pero **no comparten la misma operatoria**.



Un firewall se vale de reglas que previenen la entrada o salida de cierto tráfico de red considerando aspectos como el protocolo, dirección de origen y el destino, los números de puerto y otros aspectos. Es un escudo ante protocolos inseguros y cualquier otra actividad sospechosa que pueda impactar a la red.

Existen ataques que afectan a las redes que igualmente cumplen con las reglas establecidas por el firewall. Un ejemplo que podríamos citar es un ataque de fuerza bruta mediante SSH. Este último es uno de los protocolos seguros más utilizados para la administración remota vía CLI que tenemos actualmente, sin embargo, es posible ejecutar ataques por esta vía.

Ante situaciones como ésta, **resultan de mucha utilidad los sistemas IDS/IPS para detectar que se está realizando un ataque de fuerza bruta.** No debemos olvidar que son capaces de detectar cualquier tipo de actividad maliciosa, aunque «cumpla» con las reglas configuradas en el firewall. Lo que ocurre es que **los firewalls y los IDS/IPS trabajan conjuntamente, el IDS detecta la anomalía, y le «dice» al firewall que bloquee las conexiones**.

Ventajas

- Optimización del acceso al ordenador o Internet de la empresa.
- Administra los accesos de la red privada hacia Internet, centralizando los accesos y controlando la seguridad.
- Protección de la información privada de la empresa y sus clientes.
- Protección ante intrusos externos.
- Control de acceso

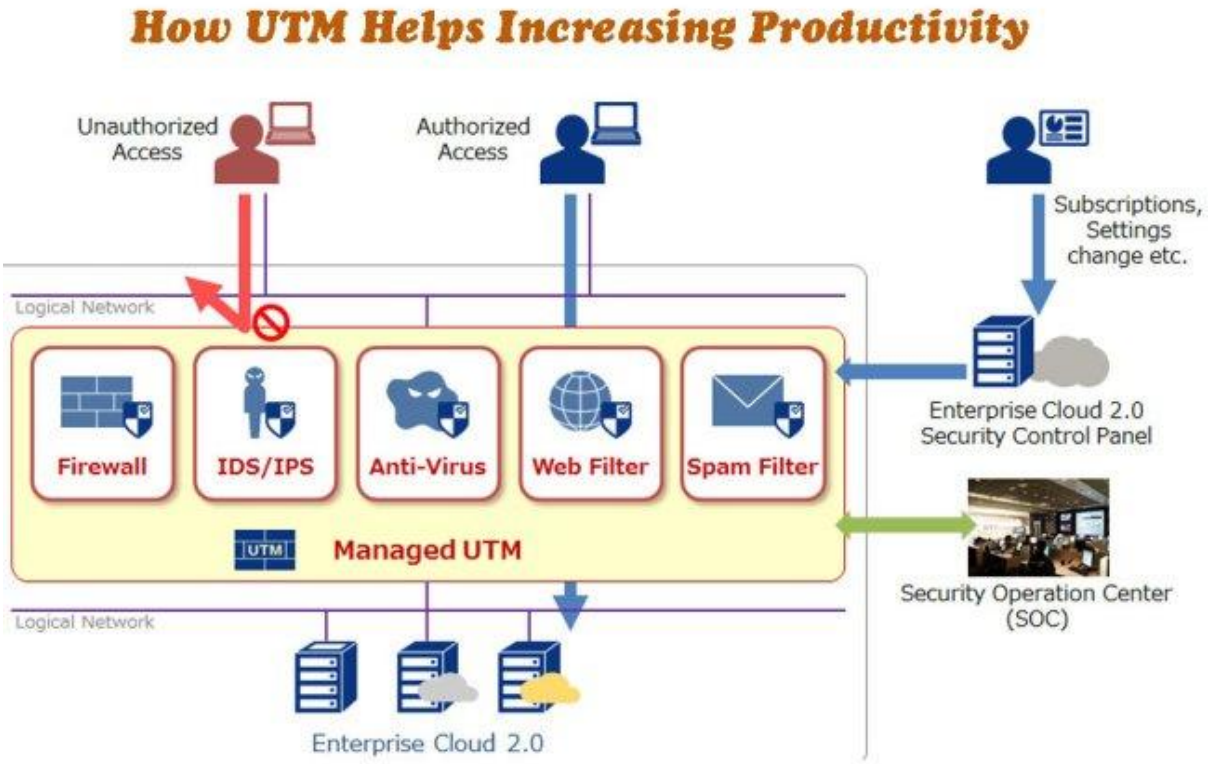
Desventajas

- Reducción del Desempeño: Los firewalls basados en software, en particular, pueden limitar el rendimiento general de su computadora y ralentizarlo.
- Alto Costo
- Indefenso contra ataques de malware
- Alta Complejidad - sobre todo los que son utilizados en grandes organizaciones.
-

Sistemas IDS/IPS vs UTM(Unified Threat Management)

Los sistemas UTM son una concepción de gestión de ciberseguridad que **permite a un administrador monitorizar y administrar una gran variedad de aplicaciones relativas a la seguridad y componentes de infraestructura, desde una consola centralizada**.

Los IPS y UTM, por su naturaleza, deben estar en línea (en paralelo) y por tanto tienen la limitación de poder controlar únicamente el tráfico que entra y sale de la zona. Siempre está presente la preocupación de que estén mal configurados, ya que si es así pueden afectar al tráfico legítimo entre un negocio y sus clientes, ocasionando pérdidas.



Los UTM, que **son normalmente adquiridos como servicios cloud o aplicativos de red, proporcionan un firewall, Intrusion Detection (IDS), antimalware, antispam o filtrado de contenido en un mismo paquete,** que puede administrarse o actualizarse fácilmente. También suelen incorporar capacidades de VPN o Red Privada Virtual.

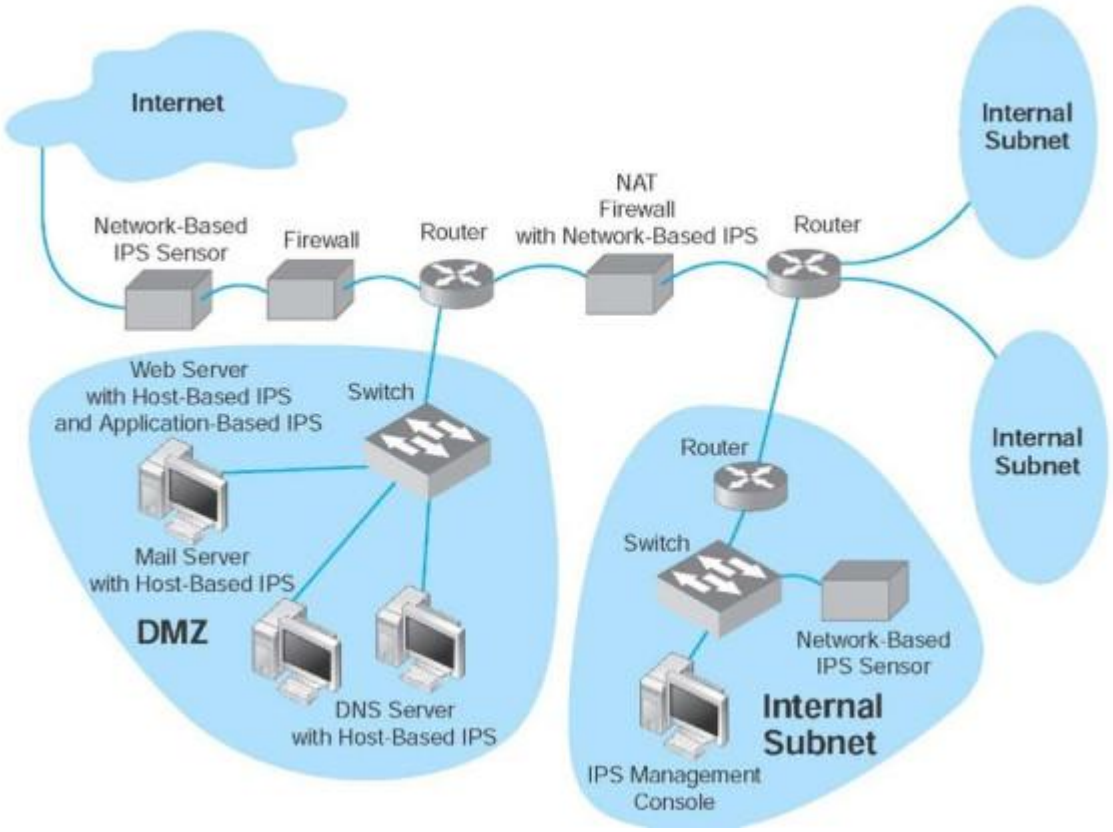
Ventajas

La principal ventaja de un sistema de este tipo es la de reducir la complejidad.

Desventajas

La principal desventaja, por otro lado, es que puede convertirse en un punto de fallo simple.

Normalmente, los UTM se sitúan entre nuestra LAN o DMZ, quizá en nuestra pasarela de Internet.



Fuentes

https://www.a2secure.com/blog/ids-ips-hids-nips-siem-que-es-esto/
https://www.redeszone.net/tutoriales/seguridad/sistemas-deteccion-prevencion-intrusiones-ids-ips/amp/
https://netddv.wordpress.com/2018/02/28/sistema-prevencion-de-intrusos-e-sistema-de-deteccion-de-intrusos-ips-e-ids/
https://pupilo.wordpress.com/2018/08/07/funcionamiento-de-ids-ips-y-utm-que-es-cada-cosa/
https://www.pcihispano.com/controles-tecnicos-de-pci-dss-parte-v-sistemas-de-deteccionprevencion-de-intrusiones-idsips/
https://www.istartips.com/advantages-of-firewall.html
https://www.pcihispano.com/controles-tecnicos-de-pci-dss-parte-v-sistemas-de-deteccionprevencion-de-intrusiones-idsips/
https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips