



Sistemas de detección de intrusos

Carlos Ariza, Fernando Talavera y Leandra Vega,



Índice

1. ¿Qué es un Sistema de Detección de Intrusos?
2. Tipos de intrusiones
3. Características de un IDS
4. Tipos de IDS
5. Network-Based IDS
6. Host-Based IDS
7. Tipos de análisis
8. Implementación de un IDS en una organización
9. Implementación de un IDS en un ISP
10. Intrusion Prevention System
11. IDS vs IPS
12. Tipos de IPS
13. IDS Open Source

¿Qué es un Sistema de Detección de Intrusos?

Es un mecanismo que monitoriza el tráfico en la red con el fin de detectar actividades sospechosas o accesos de usuarios no autorizados a un computador o a una red.



Tipos de intrusiones




- Intrusivas pero no anómalas
- No intrusivas pero anómalas
- No intrusiva ni anómala
- Intrusiva y anómala



Características de un IDS

Todo IDS, independientemente del mecanismo en el que esté basado, debe cumplir estos puntos para ser considerado un IDS fiable y de calidad:

- Independencia
 - Tolerancia a fallos
 - Resistencia a perturbaciones
 - Sobrecarga mínima
 - Detección de intrusos
 - Adaptabilidad
- 




Según su naturaleza


Pasivos

Detectan las intrusiones y
recopilan información

Reactivos

Detectan las intrusiones y
ejecutan medidas.






Según su software

Host-Based IDS

Se ejecutan en todos los dispositivos en la red con acceso directo tanto a internet cómo a la red interna de la empresa.

Network-Based IDS

La mayoría de los IDS son de este tipo. Detectan ataques a todo el segmento de la red en el que se encuentren, o en un backbone de la red.






Network-Based IDS (NIDS)

Ventajas

- Puede monitorizar una red grande
- Tienen un impacto pequeño en la red
- Se pueden configurar para que sean muy seguros ante ataques haciéndolos invisibles al resto de la red.

Desventajas

- Tienen dificultades procesando todos los paquetes en una red grande o con mucho tráfico. Pueden fallar en reconocer ataques lanzados con tráfico alto.
 - No analizan la información cifrada.
 - No saben si el ataque tuvo o no éxito
 - Algunos tienen problemas al tratar con ataques basados en red que viajan en paquetes fragmentados.
- 




Host-Based IDS (HIDS)

Ventajas

- Pueden detectar ataques que un NIDS no detectaría
- Pueden operar en un entorno donde el tráfico de red está cifrado

Desventajas

- Son más costosos de administrar.
 - Puede ser deshabilitado si un ataque tiene éxito.
 - No son adecuados para detectar ataques a toda una red
 - Pueden ser deshabilitados por ataques de DoS.
 - Usan recursos del host que están monitorizando
- 




Tipos de análisis

Basado en firmas

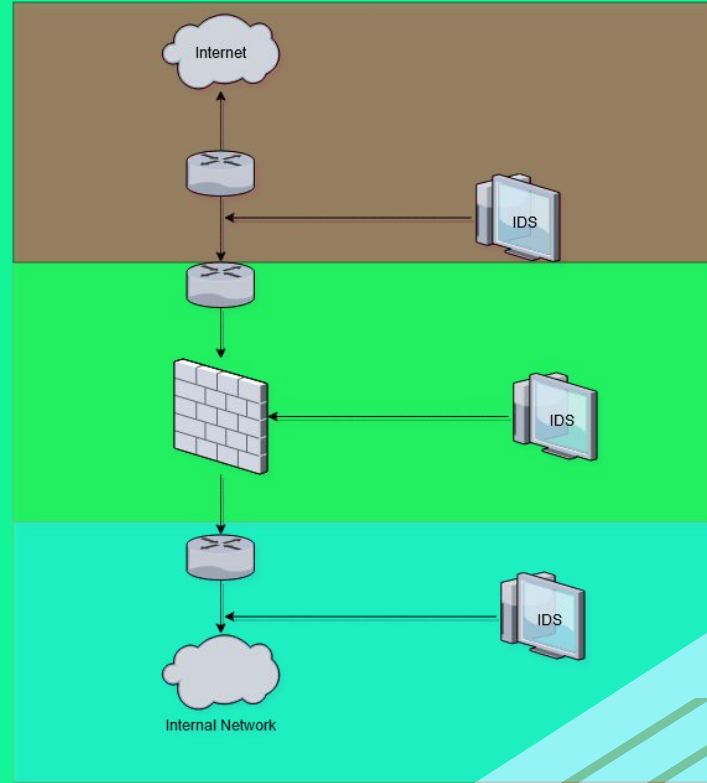
Existen patrones o reglas que contemplan tráfico malicioso conocido y que serán cotejadas por la herramienta. Cuando se encuentre una coincidencia con un patrón, recibiremos una alerta.

Basado en anomalías

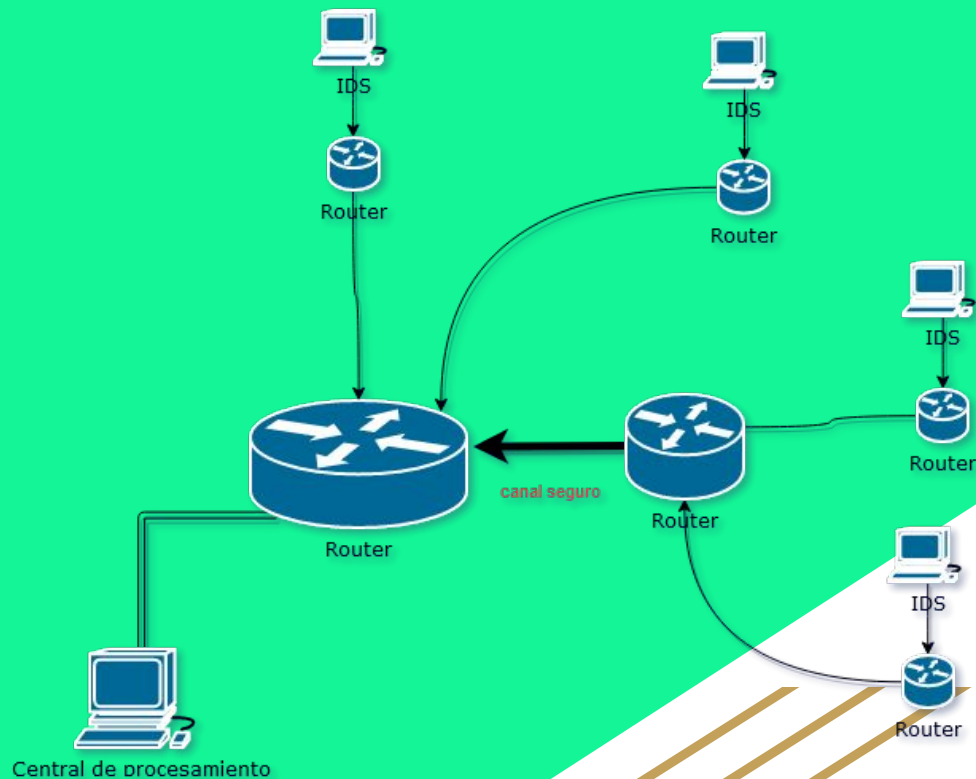
Se basa en una “línea base” de funcionamiento, a partir de la cual se buscará actividad inusual que se desvíe de los promedios , así como actividad no contemplada anteriormente.



Implementar el IDS en una organización



Implementar el IDS en un ISP



Intrusion Prevention System

Software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

Considerada por algunos como una extensión de los sistemas de detección de intrusos, en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos.



IDS vs IPS



Entre las principales funciones de un IPS, se encuentran no sólo la de identificar la actividad maliciosa, sino la de intentar detener esta actividad. Siendo esta última una característica que distingue a este tipo de dispositivos de los IDS.

Tipos de IPS

- Basados en Red Lan (NIPS)
- Basados en Red Wireless (WIPS)
- Análisis de comportamiento de red (NBA)
- Basados en Host (HIPS)



INTRUSION
PREVENTION SYSTEMS

IDS Open Source

Security
nion
Solutions



OSSEC



SURICATA



Demo