



BLOG CCNA · 13 MINUTOS DE LECTURA

## Los 7 Mejores Sistemas de Prevención de Intrusiones (IPS) 2024

Los 7 mejores sistemas IPS

Inicio > Blog CCNA

2shares



Todo el mundo quiere mantener a los intrusos fuera de su casa. Del mismo modo, y por razones similares, los administradores de red se esfuerzan por mantener a los intrusos fuera de las redes que administran. Uno de los activos más importantes de muchas de las organizaciones de hoy en día es su información. Es tan importante que muchas personas malintencionadas harán todo lo posible para robar esos datos. Lo hacen utilizando una amplia gama de técnicas para obtener acceso no autorizado a redes y sistemas. El número de tales ataques han incrementado exponencialmente y, en reacción, se están implementando sistemas para prevenirlos. Esos sistemas se denominan sistemas de prevención de intrusiones, o IPS. Hoy, echamos un vistazo a los mejores sistemas de prevención de intrusiones que se ha podido encontrar.

### Tabla de Contenido



Prevención de intrusiones – ¿De qué se trata todo esto?

La detección basada en firmas

La detección basada en anomalías

Medidas de prevención de intrusión pasiva

### Los mejores sistemas de prevención de intrusiones

1. Seguridad de red: ManageEngine Firewall Analyzer
  2. SolarWinds Log & Event Manager (PRUEBA GRATUITA)
  3. Splunk
  4. Sagan
  - Comparación de SFP, SFP+ y QSFP para Optimizar la Infraestructura de Red
  5. OSSEC
  6. Abrir WIPS-NG
  7. Fail2Ban
- Extra. Bro Monitor de seguridad de red

## Prevención de intrusiones – ¿De qué se trata todo esto?

Hace años, los virus eran prácticamente las únicas preocupaciones de los administradores de sistemas. Los virus llegaron a un punto en el que eran tan comunes que la industria reaccionó desarrollando herramientas de protección contra virus. Hoy, ningún usuario serio en su sano juicio pensaría en ejecutar una computadora sin protección contra virus. Si bien ya no escuchamos muchos virus, la nueva amenaza es la intrusión o el acceso no autorizado a sus datos por parte de usuarios malintencionados. Dado que los datos son a menudo el activo más importante de una organización, las redes corporativas se han convertido en el blanco de piratas informáticos malintencionados que harán todo lo posible para acceder a los datos. Al igual que el software de protección contra virus fue la respuesta a la proliferación de virus, **Intrusion Prevention Systems** es la respuesta a los ataques de intrusos.

Los sistemas de prevención de intrusiones esencialmente hacen dos cosas. Primero, detectan intentos de intrusión y cuando detectan actividades sospechosas, usan diferentes métodos para detenerlo o bloquearlo. Hay dos formas diferentes de detectar los intentos de intrusión:

### La detección basada en firmas

Funciona analizando el tráfico y los datos de la red, buscando patrones específicos asociados con intentos de intrusión. Esto es similar a los sistemas tradicionales de protección contra virus que se basan en definiciones de virus. La detección de intrusiones basada en firmas se basa en firmas o patrones de intrusiones, el principal inconveniente de este método de detección es que necesita las firmas adecuadas para cargarse en el software. Y cuando hay un nuevo método de ataque, generalmente hay un retraso antes de que se actualicen las firmas de ataque. Algunos proveedores son muy rápidos en proporcionar firmas de ataque actualizadas, mientras que otros son mucho más lentos. La frecuencia y la rapidez con la que se actualizan las firmas es un factor importante a considerar, al elegir un proveedor.

### La detección basada en anomalías

Ofrece una mejor protección contra los ataques de día cero, los que ocurren antes de que las firmas de detección tengan la oportunidad de actualizarse. El proceso busca anomalías en lugar de tratar de

reconocer patrones de intrusión conocidos. Por ejemplo, se activaría si alguien intentara acceder a un sistema con una contraseña incorrecta varias veces seguidas, un signo común de un ataque de fuerza bruta. Esto es solo un ejemplo y normalmente hay cientos de diferentes actividades sospechosas que pueden desencadenar estos sistemas. Ambos métodos de detección tienen sus ventajas y desventajas. Las mejores herramientas son aquellas que utilizan una combinación de firma y análisis de comportamiento para la mejor protección.



Detectar el intento de intrusión es una de las primeras partes en prevenirlos. Una vez detectados, los sistemas de prevención de intrusiones trabajan activamente para detener las actividades detectadas. Estos sistemas pueden emprender varias acciones correctivas diferentes:

- Suspender o desactivar las cuentas de usuario.
- Bloquear la dirección IP de origen del ataque o modificar las reglas del firewall.
- Si la actividad maliciosa proviene de un proceso específico, el sistema de prevención podría detener el proceso.
- Iniciar algún proceso de protección.
- Cierre de sistemas completos para limitar el daño potencial.
- Alertar a los administradores, registrar el evento e informar sobre actividades sospechosas.

## Medidas de prevención de intrusión pasiva

Si bien los sistemas de prevención de intrusiones pueden protegerlo contra numerosos tipos de ataques, nada supera a las medidas pasivas y anticuadas de prevención de intrusiones. Por ejemplo, exigir contraseñas seguras es una excelente manera de protegerse contra muchas intrusiones. Otra medida de protección fácil es cambiar las contraseñas predeterminadas del equipo. Si bien es menos frecuente en las redes corporativas, aunque no es poco frecuente, he visto con demasiada frecuencia las puertas de enlace de Internet que aún tienen su contraseña de administrador predeterminada. Mientras que en el tema de las contraseñas, el envejecimiento de las contraseñas es otro paso concreto que puede implementarse para reducir los intentos de intrusión. Cualquier contraseña, incluso la mejor, se puede descifrar con el tiempo suficiente. La caducidad de la contraseña garantiza que las contraseñas se cambiarán antes de que se hayan descifrado.

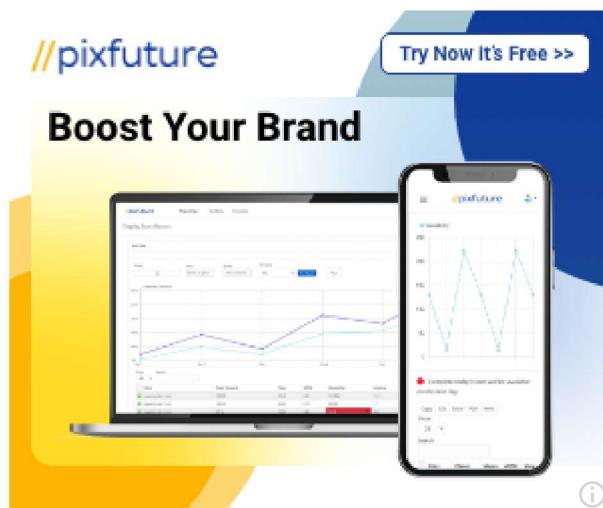
## Los mejores sistemas de prevención de intrusiones

Nuestra lista contiene una combinación de varias herramientas que pueden usarse para protegerse contra intentos de intrusión. La mayoría de las herramientas incluidas son verdaderos sistemas de prevención de intrusiones, pero también incluimos herramientas que, aunque no se comercializan como tales, se pueden usar para prevenir intrusiones. Recuerde que, más que nada, su elección de qué herramienta utilizar debe guiarse por cuáles son sus necesidades específicas.

### 1. Seguridad de red: ManageEngine Firewall Analyzer

Para toda organización es muy importante tener visibilidad y control total sobre la seguridad de la red, y para ello existe un gran producto.

ManageEngine Firewall Analyzer es un software de análisis de registros y gestión de configuración que ayuda a los administradores a recopilar y analizar archivos, sus registros de dispositivos de seguridad y a generar informes forenses a partir de ellos.



Con un sistema de respuesta a eventos en tiempo real y un módulo de gestión de cumplimiento integrado en el Firewall Analyzer, se automatiza el monitoreo de seguridad y se permite el monitoreo del uso del ancho de banda de la red, así como las configuraciones de seguridad y cumplimiento de la auditoría.

Firewall Analyzer facilita la gestión de la configuración de tu dispositivo, proporcionando informes y alertas de los cambios de configuración.

Esta herramienta es un proveedor de diagnósticos y admite casi todos los firewalls de código abierto y código privado como Cisco, Check Point, Juniper, FortiNet, Snort, Squid Project, SonicWALL, Palo Alto y más, IDS/IPS, VPNs, Proxies y otros dispositivos de seguridad relacionados.

[VISITAR FIREWALL ANALYZER](#)

## 2. SolarWinds Log & Event Manager (PRUEBA GRATUITA)

[DESCARGAR SOLARWINDS](#)

Algunas de las funciones avanzadas de este producto lo califican como un sistema de prevención y detección de intrusos, mientras que otras lo colocan en el rango de Información de seguridad y Gestión de eventos (SIEM). La herramienta, por ejemplo, presenta correlación de eventos en tiempo real y remediación en tiempo real.

El Log & Event Manager SolarWinds cuenta con detección instantánea de actividad sospechosa (una funcionalidad de detección de intrusos) y respuestas automatizadas (una funcionalidad de prevención de intrusiones). Esta herramienta también se puede utilizar para llevar a cabo investigación de eventos de seguridad y análisis forense. Debido a todas las características avanzadas del software, lo convierten más en una plataforma de seguridad integrada, que solo en el sistema de administración de eventos y registros.

Las funciones de Prevención de intrusiones del SolarWinds Log & Event Manager funcionan implementando acciones llamadas respuestas activas cada vez que se detectan amenazas. Diferentes respuestas se pueden vincular a alertas específicas. Por ejemplo, el sistema puede escribir en tablas de firewall para bloquear el acceso a la red de una dirección IP de origen que se ha identificado como que realiza actividades sospechosas. La herramienta también puede suspender cuentas de usuario, detener o iniciar procesos y cerrar sistemas.

El precio del SolarWinds Log & Event Manager varía según el número de nodos monitoreados. Los precios comienzan en \$ 4,585 para hasta 30 nodos monitoreados y se pueden comprar licencias para hasta 2500 nodos, lo que hace que el producto sea altamente escalable. Si desea tomar el producto para una prueba y ver por sí mismo si es adecuado para usted, hay disponible una prueba gratuita de 30 días con todas las funciones .

### 3. Splunk

Splunk es probablemente uno de los sistemas de prevención de intrusiones más populares. Está disponible en varias ediciones diferentes con diferentes conjuntos de características. Splunk Enterprise Security (o Splunk ES, como suele llamarse) es lo que necesita para una verdadera prevención de intrusiones. El software supervisa los datos de su sistema en tiempo real, en busca de vulnerabilidades y signos de actividad anormal.

La respuesta de seguridad es uno de los trajes fuertes del producto y lo que lo convierte en un sistema de prevención de intrusiones. Utiliza lo que el proveedor llama el Marco de respuesta adaptable (ARF). Se integra con equipos de más de 55 proveedores de seguridad y puede realizar una respuesta automatizada, acelerando las tareas manuales. La herramienta tiene una interfaz de usuario sencilla y despejada, lo que lo convierte en una solución ganadora. Otras características de protección interesantes incluyen la función "Notables", que muestra alertas personalizables por el usuario y el "Investigador de activos" para marcar actividades maliciosas y prevenir problemas adicionales.

La información de precios de Splunk Enterprise Security no está disponible fácilmente. Deberá contactar a las ventas de Splunk para obtener un presupuesto detallado. Este es un gran producto para el cual está disponible una versión de prueba gratuita.

### 4. Sagan

Sagan es básicamente un sistema de detección de intrusiones gratuito. Sin embargo, la herramienta que tiene capacidades de ejecución de script puede colocarla en la categoría de Sistemas de prevención de intrusiones. Sagan detecta los intentos de intrusión a través de la supervisión de los archivos de registro. También puede combinar Sagan con Snort, que puede enviar su salida a Sagan, lo que le brinda a la herramienta algunas capacidades de detección de intrusos basadas en la red. De hecho, Sagan puede recibir información de muchas otras herramientas como Bro o Suricata, combinando las capacidades de varias herramientas para la mejor protección posible.

Sin embargo, hay una trampa en las capacidades de ejecución de script de Sagan . Tienes que escribir los scripts de remediación. Si bien esta herramienta no se puede utilizar mejor como su única defensa contra la intrusión, podría ser un componente clave de un sistema que incorpora varias herramientas al correlacionar eventos de diferentes fuentes, brindándole lo mejor de muchos productos.

[VER TAMBIÉN](#)

Si bien Sagan solo se puede instalar en Linux, Unix y Mac OS, puede conectarse a sistemas Windows para obtener sus eventos. Otras características interesantes de Sagan incluyen el seguimiento de la ubicación de direcciones IP y el procesamiento distribuido.

## 5. OSSEC

Open Source Security , o OSSEC , es uno de los principales sistemas de detección de intrusos basados en host de código abierto. La herramienta permite especificar acciones que se realizan automáticamente cada vez que se activan alertas específicas, lo que brinda algunas capacidades de prevención de intrusiones. OSSEC es propiedad de Trend Micro, uno de los nombres líderes en seguridad de TI y fabricante de una de las mejores suites de protección contra virus.

Cuando se instala en sistemas operativos similares a Unix, el motor de detección del software se centra principalmente en los archivos de configuración y registro. Crea sumas de comprobación de archivos importantes y los verifica periódicamente, alertándole o activando una acción correctiva cada vez que sucede algo extraño. También supervisará y alertará sobre cualquier intento anormal de obtener acceso de root. En Windows, el sistema también vigila las modificaciones no autorizadas del registro, ya que podrían ser el signo revelador de actividad maliciosa. Cualquier detección activará una alerta que se mostrará en la consola centralizada, mientras que las notificaciones también se enviarán por correo electrónico.

OSSEC es un sistema de protección contra intrusos basado en host. Como tal, debe instalarse en cada computadora que desee proteger. Sin embargo, una consola centralizada consolida la información de cada computadora protegida para facilitar la administración. La consola OSSEC solo se ejecuta en sistemas operativos similares a Unix, pero hay un agente disponible para proteger los hosts de Windows. Alternativamente, otras herramientas como Kibana o Graylog pueden usarse como la parte frontal de la herramienta.

## 6. Abrir WIPS-NG

No estábamos muy seguros de si deberíamos incluir Open WIPS NG en nuestra lista. Es uno de los únicos productos que se dirige específicamente a las redes inalámbricas. Abrir WIPS NG—Donde WIPS significa Wireless Intrusion Prevention System— es una herramienta de código abierto que consta de tres componentes principales. Primero, está el sensor. Este es un proceso sencillo que simplemente captura el tráfico inalámbrico y lo envía al servidor para su análisis. Como probablemente haya adivinado, el siguiente componente es el servidor. Agrega datos de todos los sensores, analiza los datos recopilados y responde a los ataques. Este componente es el corazón del sistema. Por último, pero no menos importante, está el componente de interfaz que es la GUI que utiliza para administrar el servidor y mostrar información sobre las amenazas que se encuentran en su red inalámbrica.

La razón principal por la que dudamos antes de incluir Open WIPS NG en nuestra lista es que, por muy bueno que sea, no a todos les gusta el desarrollador del producto. Es del mismo desarrollador que Aircrack NG, un rastreador inalámbrico de paquetes y un cracker de contraseñas que forma parte del kit de herramientas de todos los piratas informáticos WiFi. Esto abre el debate sobre la ética del desarrollador y hace que algunos usuarios sean cautelosos. Por otro lado, los antecedentes del desarrollador pueden verse como un testimonio de su profundo conocimiento de la seguridad Wi-Fi.

## 7. Fail2Ban

Fail2Ban es un sistema de detección de intrusos de host gratuito relativamente popular con funciones de prevención de intrusos. El software funciona al monitorear los archivos de registro del sistema en busca de eventos sospechosos, como intentos de inicio de sesión fallidos o búsquedas de exploits. Cuando el sistema detecta algo sospechoso, reacciona actualizando automáticamente las reglas del firewall local para bloquear la dirección IP de origen del comportamiento malicioso. Esto, por supuesto, implica que algún proceso de firewall se está ejecutando en la máquina local. Este es el principal inconveniente de la herramienta. Sin embargo, se puede configurar cualquier otra acción arbitraria, como ejecutar un script de reparación o enviar notificaciones por correo electrónico.

Fail2Ban se suministra con varios disparadores de detección preconstruidos llamados filtros, que cubren algunos de los servicios más comunes, como Apache, Courier, SSH, FTP, Postfix y muchos más. Las acciones de remediación se llevan a cabo modificando las tablas de firewall del host. Fail2Ban admite Netfilter, IPtables o la tabla hosts.deny de TCP Wrapper. Cada filtro puede estar asociado a una o varias acciones, los filtros y las acciones se conocen como una cárcel.

## Extra. Bro Monitor de seguridad de red

El Bro Network Security Monitor es otro sistema gratuito de detección de intrusos en la red con una funcionalidad similar a IPS. Funciona en dos fases, primero registra el tráfico y luego lo analiza. Esta herramienta funciona en varias capas hasta la capa de aplicación, lo que explica una mejor detección de intentos de intrusión divididos. El módulo de análisis del producto se compone de dos elementos. El primer elemento se llama el motor de eventos y su propósito es el seguimiento de eventos desencadenantes, como conexiones TCP o solicitudes HTTP. Los eventos son analizados por Policy Scripts, el segundo elemento. El trabajo de Policy Scripts es decidir si activar una alarma, iniciar una acción o ignorar el evento. Es la posibilidad de iniciar una acción que le da al Bro Security Security Monitor su funcionalidad IPS.

El Bro Network Security Monitor tiene algunas limitaciones. Solo rastreará la actividad HTTP, DNS y FTP y también monitoreará el tráfico SNMP. Sin embargo, esto es algo bueno, ya que a menudo se utiliza SNMP para la supervisión de la red a pesar de sus graves fallas de seguridad. SNMP apenas tiene seguridad incorporada y utiliza tráfico no cifrado. Y como el protocolo se puede usar para modificar configuraciones, podría ser fácilmente explotado por usuarios malintencionados. El producto también controlará los cambios de configuración del dispositivo y las capturas SNMP. Se puede instalar en Unix, Linux y OS X, pero no está disponible para Windows, que es quizás su principal inconveniente. De lo contrario, esta es una herramienta muy interesante que vale la pena probar.

¡Listo! Sigue visitando nuestro blog de curso de redes, dale Me Gusta a nuestra fanpage; y encontrarás más herramientas y conceptos que te harán todo un profesional de redes



The image shows the pixfuture logo at the top left, followed by a call-to-action button "Try Now It's Free >>". Below this, the text "Boost Your Brand" is displayed. The central part of the image is a composite of two screenshots: one from a laptop showing a dashboard with multiple line graphs and data tables, and another from a smartphone showing a similar dashboard with a line graph and some text.

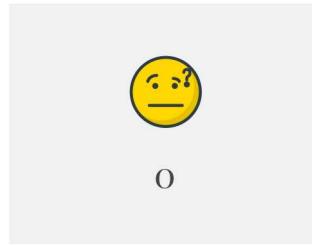
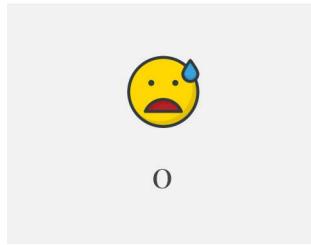
ETIQUETAS

#FIREWALL

#INTRUSIONES

#IPS

#WIPS



## Relacionado

