STORMSHIELD

Sistemas DPI y seguridad de red

La tecnología IPS Stateful DPI en entornos de TO

Resumen ejecutivo

Hoy en día, la segmentación de las redes operativas representa un primer nivel en la lucha contra los ciberataques. Sin embargo, para hacer frente a las nuevas amenazas, cada vez más sofisticadas, también es necesario desplegar soluciones de análisis en profundidad (DPI - *Deep Packet Inspection*) de los mensajes intercambiados, a fin de anticipar la protección de esas redes sensibles.

Para superar este desafío en las TO, las soluciones de seguridad desplegadas deben cumplir los estrictos requisitos **de disponibilidad, integridad y confidencialidad,** derivados de los diversos retos de actividad que soportan las redes operativas.

Por tanto, la implantación de un sistema IPS *(Intrusion Prevention System*, sistema de prevención de intrusiones) lo más próximo posible a los dispositivos debe respetar estos aspectos para poder aplicar una política de seguridad proactiva y sostenible, garantizando al mismo tiempo la seguridad de explotación de las redes operativas.

Para ello, hay que tener en cuenta cuatro ejes principales:

- una **solución integrada** que garantice un conocimiento detallado de los protocolos industriales;
- una **capacidad para vigilar el cumplimiento de los mensajes** operativos de cara a identificar mejor las anomalías y preservar los activos de la red de TO;
- una **protección proactiva frente a las diferentes** variantes de amenazas para contrarrestar los ataques dirigidos y evitar las interrupciones de la producción;
- un **enfoque contextual de los intercambios de mensajes** para garantizar el cumplimiento de los procesos comerciales.

Este documento describe los diversos mecanismos que un sistema IPS debe explotar para llevar a cabo su misión de detección y protección. También le facilitará los elementos necesarios que un IPS debe integrar para adaptarse a sus necesidades de seguridad.

El presente estudio está dirigido a los responsables de operaciones y mantenimiento y directores operativos a cargo de infraestructuras críticas, así como a los CISO.

Stormshield

Las empresas, instituciones gubernamentales y organismos de defensa de todo el mundo necesitan a su lado socios de confianza que les guíen en su proyecto de digitalización y que les ayuden a garantizar la ciberseguridad de sus infraestructuras, así como de sus usuarios y datos. Las tecnologías Stormshield, que cuentan con el grado europeo de clasificación más elevado (EU Restricted, OTAN Restricted, Common Criteria EAL3+/EAL4+, cualificaciones y permisos de la Agencia francesa de seguridad de los sistemas de información o ANSSI), permiten hacer frente a los desafíos que plantean la TI y la TO para proteger así sus actividades. Nuestras soluciones de seguridad le brindan la libertad de poder trabajar con total tranquilidad.

Índice

1. Contexto
2. Riesgos cibernéticos asociados a las redes operativas
3. Sistemas de defensa: ¿sonda industrial o IPS?
4. Principios generales del Intrusion Prevention System
   - Firma o búsqueda de protocolo específico: dos enfoques para el control del cumplimiento del protocolo
   - El análisis contextual: los cimientos de la seguridad de los intercambios
   - Búsqueda de amenazas de red
   - Las firmas personalizadas necesarias
5. Criterios para elegir el IPS adecuado
6. El motor *Stateful DPI* Stormshield

Contexto

Los ciberataques contra las infraestructuras operativas son cada vez más sofisticados. Secuenciados en diferentes etapas, se tornan agresivos y difíciles de detectar por los diferentes sistemas de protección. Las *Advanced Persistent Threats* (APT, amenazas persistentes avanzadas) son ciberataques que utilizan un conjunto de técnicas y métodos estratégicamente combinados para alcanzar un objetivo perfectamente definido. Intentan pasar inadvertidos durante el mayor tiempo posible para evitar despertar sospechas, buscando generalmente la exfiltración de datos de elevado valor añadido (patentes, secretos industriales, etc.).

Por tanto, aunque la mayoría de las empresas y organizaciones afirman ser conscientes de los riesgos cibernéticos y de las implicaciones que estos pueden tener (pérdida o robo de datos, interrupciones de la producción, etc.), a menudo corren un riesgo mayor del que sospechan. Con la aparición en los últimos años del Internet industrial de las Cosas (IIoT), los ciberataques se dirigen a empresas de diversos sectores como la aeronáutica, la energía nuclear, la electricidad, la salud, etc. Los actores de vital importancia para la sociedad se están convirtiendo en objetivos primordiales.

Sin embargo, en algunos casos, estos actores saben dónde radican las debilidades de sus sistemas, pero no tienen los medios para reemplazar las aplicaciones y/o el equipo en cuestión. Esto es común en las redes operativas y de misión crítica, como el sector de la salud, que utilizan aplicaciones soportadas únicamente por sistemas operativos obsoletos. En el ámbito industrial, algunos componentes se conservan aunque sean obsoletos, lo que aumenta el riesgo de sufrir un ataque implantado discretamente hace algún tiempo. Como se reveló en un estudio realizado en noviembre de 2019[1], los ciberdelincuentes llevan más de diez años sirviéndose de determinados fallos y vulnerabilidades, que siguen explotando hoy en día.

> El desafío consiste en diseñar una arquitectura capaz de asegurar la transmisión, el tratamiento y **el mantenimiento de la integridad de los datos** entre los sistemas.
>
> Cigref

Pero la ciberseguridad industrial aún es una disciplina relativamente nueva. La experiencia en el ámbito de la TI[2], como el análisis de riesgos, por ejemplo, también resulta útil para dar una respuesta adecuada y eficaz tras realizar algunos ajustes.

Este estudio busca abordar y analizar los métodos de protección de redes de tipo IPS, así como los retos asociados a la seguridad de las redes de TO.

[1] Stormshield, www.stormshield.com/fr/actus/quelles-tendances-cybersecurite-pour-2020/
[2] Stormshield, www.stormshield.com/fr/actus/reseaux-it-ot-raisons-convergence-delicate/

Riesgos cibernéticos asociados a las redes operativas

En los últimos años, la transformación digital marcada por la convergencia TI/TO o el uso del *Edge/Cloud Computing*[3] ha llevado a las redes de empresas industriales de todos los tamaños a una mayor hiperconectividad. Los proyectos de **excelencia** operativa, vinculados a Industria 4.0 (como la optimización avanzada entre la cadena de producción y el ERP de la empresa) hacen que las redes operativas sean más permeables a los riesgos cibernéticos.

Recientemente, con el ataque EKANS (o Snake), **hemos tomado consciencia de nuevo de la peligrosidad** de los riesgos que puede generar una intrusión en la red industrial. Hay factores que favorecen este tipo de riesgos: la falta de homogeneidad entre el equipo instalado y las estaciones de control o incluso componentes industriales con normas y/o requisitos diferentes. Estos elementos que coexisten en el mismo entorno pueden causar fallos que deriven en el colapso de todo el sistema.[4]

Es evidente que, en el universo de la TO, tan pronto como se establecen conexiones entre sistemas y máquinas que antes estaban aislados de la red, aumentan las posibilidades de que se produzcan ataques con graves consecuencias: daños físicos, interrupción de la producción o incluso robo de procesos industriales.

Con la convergencia TI/TO que se está produciendo, muchos fabricantes están empezando a establecer una gestión global de sus emplazamientos para tener más visibilidad sobre sus redes operativas. Por consiguiente, para lograr una adecuada observación de los problemas de ciberseguridad industrial, **los universos de la TI y la TO deben dialogar al tiempo que analizan y evalúan los riesgos para facilitar una aplicación eficiente de los procesos de administración y gestión de la seguridad de red**.

[3] Forbes, www.forbes.com/sites/ronshevlin/2020/08/17/cloud-computing-raises-new-cybersecurity-concerns-for-banking/#5f46307f24ae

[4] Stormshield, www.stormshield.com/fr/actus/industrie-manufacturiere-menace-cyber/

Como señala Vincent Riondet, responsable de los equipos de Proyectos y Servicios de Ciberseguridad de Schneider Electric France, en un estudio anterior, en la mayoría de los emplazamientos industriales *«utilizamos, por tanto, infraestructuras más o menos antiguas, con arquitecturas de red y sistemas operativos más o menos recientes, que no incorporan necesariamente normas de seguridad avanzadas porque* su actualización resulta costosa».

La aplicación de múltiples barreras de protección como la segmentación, el control de flujo, la detección o la prevención de intrusiones, puede ser muy útil para luchar contra las amenazas mediante los flujos de red. Además, ya no basta con controlar el acceso exclusivamente mediante la autorización o no un protocolo de comunicación (a través de su puerto), sino que es necesario analizar los comandos que se envían a través de los protocolos autorizados.

Por tanto, la seguridad de la arquitectura de red debe girar en torno a la protección y la actualización de estas medidas de protección para evitar las fugas de datos o la interrupción del proceso operativo. ¿El objetivo? Luchar mejor contra los ciberataques que pueden producirse en cualquier momento. **Por eso es esencial la implantación de sistemas de defensa proactivos lo más cerca posible de las infraestructuras críticas.**

Sistemas de defensa: ¿sonda industrial o IPS?

Aunque es esencial vigilar la infraestructura industrial, no existe una única matriz de evaluación técnica aplicable a todas las arquitecturas operativas. Una de las preguntas que hay que formularse es: **¿quién procesa las alertas generadas y cómo?** De hecho, más allá de los aspectos técnicos, la instalación de una sonda industrial requiere **un equipo operativo** con la formación adecuada y capaz de gestionar y analizar una **gran cantidad de información** para identificar los sucesos críticos y elevar a instancias superiores los posibles problemas de seguridad, si los hubiere.

Aunque estas soluciones pueden ser complementarias, la elección entre una sonda industrial y una solución IPS debe basarse en un conjunto de parámetros, dependiendo de su uso. Esto requiere una revisión detallada de toda la arquitectura de su red operativa. En función de sus necesidades, cuantifique **la criticidad de la seguridad de cada elemento para determinar la protección adecuada**.

También es importante pensar en cómo encajará la nueva solución en su política general de ciberseguridad, así como en sus procesos y organización actuales y futuros.

¿SABÍA QUE...?

Los sistemas IPS suelen ofrecer las mismas funcionalidades de IDS *(Intrusion Detection System*, sistema de detección de intrusiones) que las sondas industriales. Los sistemas IDS no proporcionan el mismo nivel de detalle en la capacidad de identificación que estas sondas, pero sí reconocen los flujos que pasan a través del equipo.

Se recomienda **llevar a cabo una implantación gradual del IPS a través de una fase de análisis del tráfico de red en IDS**. Este paso preparatorio permite identificar los flujos así como posibles falsos positivos antes de activar la prevención activa de intrusiones para bloquear los flujos ilegítimos.

Una sonda industrial es una herramienta **pasiva** que permite **detectar** posibles flujos maliciosos en la red		**Un sistema IPS** es una herramienta de protección **activa** que permite **identificar** y **bloquear** posibles flujos maliciosos en la red
• No bloquea los paquetes de red	VS	• Actúa bloqueando paquetes sospechosos
• Precisa de la intervención humana para gestionar los incidentes	VS	• Es autónomo para gestionar las alarmas activadas
• Visualiza una copia completa de la red	VS	• Se sitúa en línea
• Proporciona una gran cantidad de información	VS	• Alerta solo en caso de problemas
• Es sensible a las acciones de *flooding*	VS	• Detiene este tipo de ataques
• Es «transparente» en la red en caso de ataque	VS	• Se puede detectar más fácilmente

¿SABÍA QUE...?

Hay soluciones IPS disponibles que integran un **modo de seguridad *(función bypass)* para garantizar, si es necesario, la continuidad de la actividad operativa en caso de avería.**

Principios generales del Sistema de Prevención de Intrusiones

Resumen

La función principal de los IPS es **supervisar los paquetes de red y su contenido en tiempo real para aplicar reglas predefinidas en función del ataque detectado y del objetivo previsto**.

NO CONFUNDIR
Hay dos tipos diferentes de IPS:

- **HIPS (Host-Based Intrusion Prevention System, sistema de prevención de intrusiones de host)**: IPS que supervisa los puestos de trabajo.
- **NIPS (Network Intrusion Prevention System, sistema de prevención de intrusiones de red)**: IPS que supervisa la red.

¿Cómo funciona?

Los sistemas de prevención de intrusión se instalan en línea en la red que protegen. Analizan los paquetes de red, inicialmente para comprobar el cumplimiento del protocolo y monitorizar comandos.

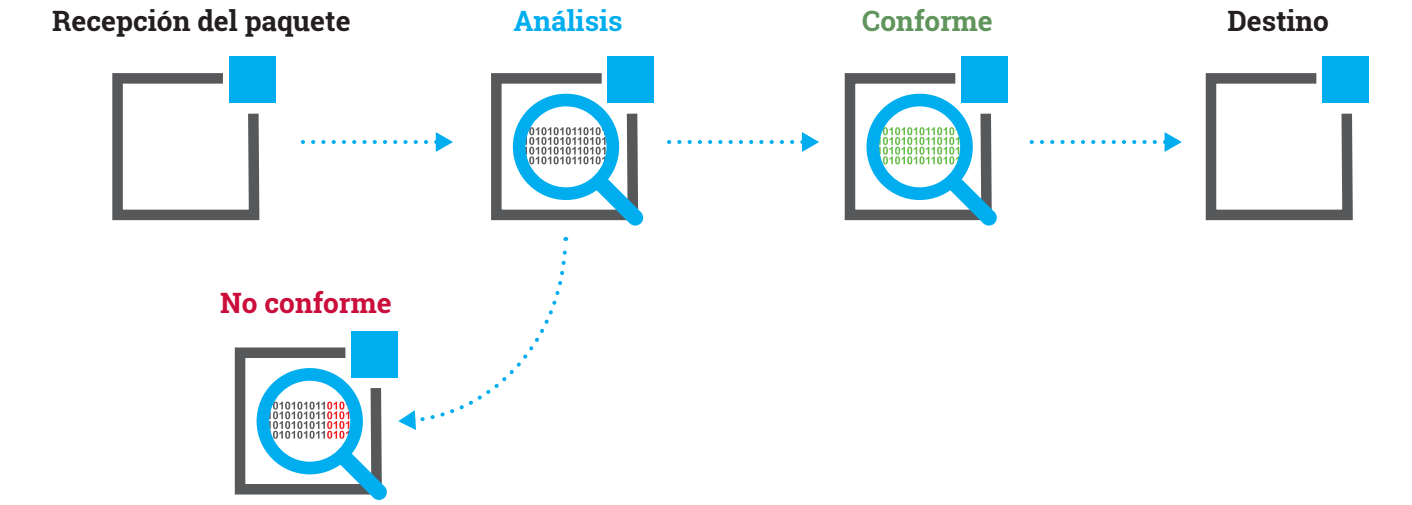
Algunos sistemas IPS son incluso capaces de identificar comportamientos anormales.

A continuación, los sistemas IPS buscan paquetes de red que contengan un conjunto de datos que coincidan con la firma de *malwares* conocidos para bloquear los intentos de ataque.

¿Qué aporta el IPS?

Esta tecnología brinda protección de red para una infraestructura informática y/u operativa.

Por ello, soportar los protocolos utilizados por la organización es un criterio de selección del sistema IPS que no debe descuidarse para garantizar una buena cobertura en la protección de los comandos de control.



Firma o búsqueda de protocolo específico:

dos enfoques para el control del cumplimiento de los protocolos

Los mejores motores IPS garantizan la descodificación de los protocolos utilizados y comprueban la conformidad (longitud del paquete de datos, tipo de protocolo, etc.) de cada uno de los mensajes con respecto al formato previsto, definido en los estándares normalizados de estos protocolos. Son capaces de analizar la información con gran detalle, de ahí el término frecuentemente utilizado de «***Deep Packet Inspection* (DPI)**».

La DPI (Deep Packet Inspection) evalúa el encabezado de un paquete transmitido y los datos asociados, eliminando cualquier incumplimiento del protocolo

Pongamos como ejemplo un paquete de red que traslada un comando:

Encabezado		Comando	Parámetros		
1100	0011	1101	1110	1110	1000

En caso de cumplir con el protocolo, un sistema IPS buscará cadenas de bytes específicas por dos razones principales:

1. **Reconocimiento del protocolo:** primero, reconocer el protocolo en tránsito buscando marcadores característicos.
2. **Cumplimiento del protocolo:** a continuación, asegurarse de que se encuentran en el paquete de red correspondiente al protocolo identificado.

¿SABÍA QUE...?

La aplicación específica de los protocolos en el mundo industrial utiliza sobre todo valores de comando que se personalizan (*custom command*). **El análisis del protocolo basado en la firma no reconoce estos valores, lo que genera errores de detección.**

En este caso, el **análisis «basado en la firma»** busca la secuencia ***111101*** en cualquier parte del paquete.



Aquí, los bytes identificados mediante este enfoque están presentes pero no en el lugar correcto del paquete. La técnica basada en la firma deja pasar igualmente el paquete mal formado (lo que deriva en un falso negativo).

El enfoque específico buscará la información deseada en el lugar correcto, justo donde se supone que debe estar, para evitar el paso de paquetes mal formados (y potencialmente maliciosos).

Por tanto, con el enfoque específico, el paquete mal formado se bloquea.



Así pues, el **análisis de protocolo específico** trae consigo dos ventajas importantes:

1. **Cumplimiento exacto del protocolo**
2. **Limitación de los errores de detección**

El análisis contextual: los cimientos de la seguridad de los intercambios

Este enfoque permite bloquear los ciberataques mediante la contextualización de los mensajes intercambiados entre dos elementos de la red. Para ello, el **análisis contextual** comprueba que la secuencia de los mensajes intercambiados sigue la lógica definida en la norma del protocolo y no muestra ningún comportamiento anormal.

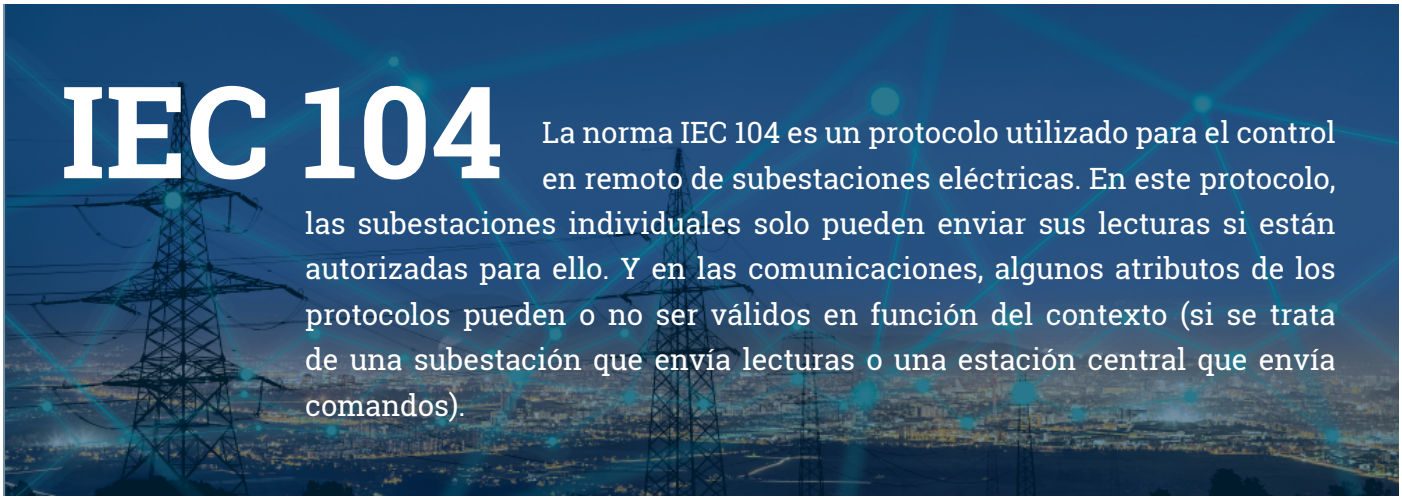
El análisis contextual examina y verifica el mensaje de un intercambio entre dos dispositivos teniendo en cuenta los mensajes anteriores. **Esta tecnología avanzada protege y garantiza la integridad de sus activos y entornos operativos.**

Tomemos el ejemplo de un dispositivo «A» que puede ser controlado por varios controladores. Un controlador «A» solicitará tomar el control enviando una solicitud apropiada. El dispositivo «A» acusará recibo de esta petición enviando la aceptación del comando siempre que no esté ya controlado por otro controlador. En este ejemplo, imaginemos que un atacante toma el control del dispositivo «A». El sistema IPS ve un paquete enviado espontáneamente por el dispositivo «A» que acepta una solicitud de toma de control que no ha sido identificada por el sistema. Con los elementos de contexto, el IPS puede identificar este comportamiento como anormal y bloquearlo.

VENTAJAS

Este tipo de solución IPS, conocida como ***Stateful DPI*** permite **reforzar el nivel de seguridad de la infraestructura operativa para reducir el compromiso de los activos de red.**

Al realizar un **análisis contextual de** las secuencias de paquetes que transitan por la red operativa, este tipo de IPS permite considerar la información relativa a los intercambios entre dos dispositivos. **Tiene en cuenta varios parámetros del mensaje actual en comparación con los ya intercambiados**. Estos parámetros pueden ser: la dirección de la comunicación entre los dos dispositivos, el tipo de comando por ejecutar o los valores de comando por aplicar.



Búsqueda de amenazas de red en los intercambios

El *malware* Triton ilustra bien la debilidad de las redes de TO y demuestra la importancia de un sistema IPS para identificar las amenazas a través de la red, incluso cuando el ataque respeta el cumplimiento del protocolo y sigue la lógica definida en la norma de este último. Para ello, el IPS busca en los datos del paquete de red una secuencia de bytes que corresponda a una firma de ataque conocida.

También hay que señalar que algunos programas maliciosos pueden evolucionar. Las variantes de estos requieren entonces nuevas firmas específicas: si estas no se despliegan en el IPS, este no podrá detectarlas. **Por esta razón, se recomienda utilizar un IPS capaz de explotar firmas proactivas que abarquen las distintas variantes de un ataque permitiendo así su detección.**

VENTAJAS

La protección proactiva tiene otra ventaja considerable: dado que el número de firmas requeridas de base se reduce, **la búsqueda de patrones de ataque conocidos en la red es más rápida y se reduce la latencia de la red generada por el análisis.**

Y lo que es mejor aún, si el motor del IPS es capaz de aprovechar el exhaustivo análisis realizado durante la comprobación del cumplimiento del protocolo para buscar solo las firmas de ataque relevantes en cada parte de los mensajes, **el rendimiento se incrementa aún más y la tasa de falsos positivos se reduce drásticamente.**

Triton: un ciberataque contra los ICS

El malware Triton fue diseñado para atacar los sistemas ICS de una planta petroquímica saudí con el objetivo de provocar una explosión. Afortunadamente, los atacantes cometieron un error, lo que provocó un cierre de emergencia de los sistemas críticos y reveló la intrusión de la red.

Stuxnet: ejemplo de las variantes del gusano

Stuxnet fue diseñado para atacar las centrifugadoras iraníes de enriquecimiento de uranio. La complejidad de este *malware* se basa en un exhaustivo conocimiento de los procesos industriales y las vulnerabilidades del sistema operativo Windows. Los ciberdelincuentes usaron sofisticados e inusuales *exploits* de tipo Día cero.

Las variaciones de Stuxnet también se utilizaron a continuación contra otras infraestructuras industriales.

Algunas organizaciones industriales y expertos en la materia han publicado guías de buenas prácticas para la gestión adecuada de los sistemas de control. Entre otras cosas, mencionan la necesidad de segmentar la red, controlar el acceso, adquirir sistemas reforzados, implantar antivirus y motores de prevención de intrusiones de tipo IPS.

Frente a este tipo de amenazas, un sistema IPS proactivo que tenga en cuenta las posibles variantes del mismo *malware* es una ayuda esencial, incluso vital, para la supervivencia del sistema industrial.

Las firmas personalizadas necesarias

Un sistema IPS debe conocer y gestionar los mensajes intercambiados a través de protocolos industriales para proteger adecuadamente el sistema operacional. Cada valor enviado en los mensajes de control debe analizarse y verificarse correctamente porque cada comunicación de la red actúa directamente en un proceso operacional determinado.

Un sistema de IPS debe poder ofrecer la personalización de firmas con vistas a aplicar el control de los mensajes de comando de conformidad con las limitaciones y los procesos operativos de la actividad

Las soluciones de IPS pueden proporcionar esta verificación a través de firmas personalizadas. El objetivo: controlar los mensajes de comando para que cumplan con los procesos y limitaciones de actividad operativas. Este es el punto más crítico en un entorno operativo para asegurar que los valores no superen ciertos límites que podrían poner en peligro todo el proceso.

Tomemos el ejemplo simplificado de una presa hidráulica, en la que hay que asegurarse de que los comandos de control tengan en cuenta el caudal soportado por una compuerta (en este caso: capacidad total de 50 a 5000 m^3/s). Aunque los nuevos sistemas ICS/SCADA son menos sensibles a esto, es importante para las infraestructuras más antiguas que los valores enviados al controlador respeten estos límites con vistas a evitar caudales más elevados, con graves consecuencias, como inundaciones.

También es fundamental poder comprobar estos valores en tiempo real.

700+
protocolos propios

UMAS, S7, TSAA, SAAT, HNZ, etc.

20+
protocolos estandarizados

Modbus, UMAS, OPC Classic, S7, EtherNet/IP, CIP, BACnet/IP, IEC 60780-5-104, DNP3, PROFINET, IEC 61850 (MMS/GOOSE/SV), OPC UA, etc.

VENTAJAS

Las firmas personalizadas te permiten:

- **adaptarse** al contexto de la actividad;
- **implantar** el análisis en protocolos;
- **controlar** los denominados «valores sensibles» relacionados con la seguridad del sistema operativo;
- **garantizar** el buen funcionamiento del proceso operacional.

Criterios para elegir el IPS adecuado

Elegir un sistema IPS puede parecer una tarea delicada y complicada atendiendo a lo mucho que hay en juego.

El siguiente diagrama le brindará rápidamente una visión general de las funcionalidades más importantes.



¿SABÍA QUE...?

Los sistemas de protección que consisten en varios componentes hacen que su integración sea más compleja. Además de la multiplicidad de herramientas de gestión, licencias y formaciones, estas soluciones generalmente aumentan la latencia en la red.

Maximice la productividad de sus equipos eligiendo una solución IPS todo en uno, fácil de implantar y de usar. Del mismo modo, una interfaz gráfica clara mejorará la integración y la gestión del IPS al proporcionar más visibilidad sobre los sistemas que se deben proteger.

El motor *Stateful DPI* Stormshield

Disponga de un sistema de prevención de intrusiones y de una segmentación de sus redes operativas de alta calidad para garantizar la disponibilidad e integridad de sus sistemas

Potentes análisis de flujos

CONTROL DE CUMPLIMIENTO DE PROTOCOLOS
que combina el control de paquetes y el cumplimiento de los protocolos de las aplicaciones

DPI en más de 10 protocolos soportados
Modbus, OPC Classic, S7, EtherNet/IP, CIP, BACnet/IP, IEC 60780-5-104, DNP3, PROFINET, IEC 61850 (MMS/GOOSE/SV), OPC UA, etc.

Un IPS industrial

basado en múltiples análisis para proporcionar una respuesta proactiva, que incluso previene los ataques tipo Zero-day

Análisis de contexto

Estudio del comportamiento según un contexto de actividad

la **optimización de la integración del IPS** en el sistema operativo integrado

la **búsqueda de firmas de contexto** en una base de datos más refinada y específica

el **análisis de protocolo específico y de contexto** disminuye la latencia y limita los falsos positivos

Un rendimiento superior gracias a...

FIRMA PERSONALIZADA

¿POR QUÉ LO NECESITA?

1. Supervisar el cumplimiento con los procesos operativos
2. Prevenir daños en el equipo industrial y para el medio ambiente
3. Adaptarse a un análisis de protocolo específico

Puesta en marcha sencilla

Solución todo en uno

UI clara y fácil de usar

EXPERIENCIA EN LA PROTECCIÓN DE LAS REDES DE TO:

DISEÑO CONJUNTO

CON LOS FABRICANTES DE EQUIPO, LOS INTEGRADORES INDUSTRIALES Y CLIENTES

www.stormshield.com

STORMSHIELD

La opción europea en ciberseguridad

Las empresas, instituciones gubernamentales y organismos de defensa de todo el mundo necesitan a su lado socios de confianza que les guíen en su proyecto de digitalización y que les ayuden a garantizar la ciberseguridad de sus infraestructuras, así como de sus usuarios y datos. Las tecnologías Stormshield, que cuentan con el grado europeo de clasificación más elevado (EU Restricted, OTAN Restricted, Criterios Comunes EAL3+/EAL4+, cualificaciones y permisos de la Agencia francesa de seguridad de los sistemas de información o ANSSI), permiten hacer frente a los desafíos que plantean la TI y la OT para proteger así sus actividades. **Nuestras soluciones de seguridad le brindan la libertad de poder trabajar con total tranquilidad.** www.stormshield.com

Queda prohibida toda difusión, reproducción o representación, incluso parcial, de este estudio para fines distintos al uso privado en cualquier soporte, lo que podría comprometer la responsabilidad civil y penal de toda persona que no cumpla esta prohibición.