

¿Qué es un firewall industrial DPI?

En el whitepaper [“Mejores prácticas para la segmentación y fortificación de redes industriales”](#) se introducía el **concepto de firewall**. Se definía como un dispositivo hardware o aplicación software que monitoriza y controla el tráfico que fluye entre dos redes e intercepta el tráfico no autorizado comparando cada unidad de información (paquete, segmento, datagrama o trama, dependiendo del nivel al que trabaje) con una serie de reglas predefinidas.

¿Por qué un firewall puede ser calificado como industrial? Porque:

- Se han diseñado de forma específica pensando en los entornos ambientales y operación de las redes industriales.
- Su instalación y despliegue no es intrusiva ni invasiva.
- Su configuración y módulos de gestión de reglas son fáciles de utilizar.
- Incorporan funcionalidades específicas que permiten incrementar la seguridad de las redes OT.

Y para terminar, ¿qué se entiende por DPI (Deep Packet Inspection)?

Según el tipo de funcionamiento, existen diferentes tipos de firewalls.

- Los más sencillos son los firewalls que funcionan a nivel red (capa 3 del modelo OSI). Entre estos están los **Packet Filter Firewalls**, es decir aquellos que definen reglas básicas sin considerar relaciones entre paquetes y los **Stateful Firewalls**, que permiten parametrizar y aplicar reglas de segmentación considerando relaciones entre paquetes de información.
- Los que funcionan sobre la capa 7 del modelo OIS, reciben el nombre de **Application Firewalls o Proxy Firewalls**. En este caso se basan en un análisis a un nivel más alto que tiene en cuenta los parámetros específicos de cada aplicación. Algunos ejemplos de protocolos típicos sobre los que se realizan reglas de segmentación son HTTP, SMTP, Telnet, FTP...
- Por último, un **firewall DPI** (el más sofisticado) es aquel que puede filtrar por protocolos/tipos de archivos específicos, como SOAP o XML (por ejemplo en entornos transaccionales).

¿Y qué significa que un firewall realiza DPI en entornos industriales o de infraestructuras?

- Es un firewall que se despliega físicamente entre los sistemas SCADA, HMI (nivel II de la ISA95) y los dispositivos de campo como los PLCs, DCSs, RTUs (nivel I de la ISA95).
- Bloquea malware construido sobre protocolos típicamente IT. Es decir, la mayoría del malware no está construido sobre protocolos industriales. Al poder definir reglas de segmentación específicas por protocolo industrial (Modbus, Profinet, OPC, Ethernet/IP, DNP3) este tráfico no estaría permitido.
- Segmenta tráfico que no es conforme al “estandar” del protocolo industrial seleccionado.
- Permite definir reglas de segmentación por Function Codes específicas de protocolos como Modbus o Ethernet IP.

En la siguiente tabla, se resumen las principales diferencias entre los firewalls tradicionales y los industriales.

Funcionalidad	Packet Filter Firewalls	Stateful Firewalls	Aplicación	Deep Packet Inspection Firewall industrial
1. Definir reglas básicas sin considerar relaciones entre paquetes	SI	SI	SI	SI
2. Definir reglas básicas considerando relaciones entre paquetes	NO	SI	SI	SI
3. Definir reglas básicas a nivel aplicación (DPI).	NO	NO	Dep	SI
4. Bloquear tráfico con malware al poder segmentar por <u>protocolos industriales</u>	NO	Dep.	NO	SI
5. Definir reglas a nivel protocolo (function codes) si el protocolo es <u>Modbus, Ethernet/IP</u> o <u>asignar un único puerto sobre OPC</u>	NO	NO	NO	SI
6. Eventos y logs	SI	SI	SI	SI
7. Preparados para entornos industriales	NO	NO	NO	SI

¿Qué es el dispositivo Eagle Tofino de Hirschmann?

El dispositivo **EAGLE TOFINO de Hirschmann** es un **firewall industrial DPI** que se ubica entre el SCADA/HMI y el PLC/RTU protegiendo y asegurando la disponibilidad y la integridad de los equipos de control y por tanto del proceso.

Entre sus características técnicas destacan:

- Es fácilmente desplegable y no requiere de configuración del SCADA, del PLC ni de la red (no lleva asociado dirección IP).
- Diseñado específicamente para entornos OT. Dispone de un rango de temperaturas de operación entre -40° a 60° , IP20 y con posibilidad de instalarse sobre carril DIN.
- Permite definir reglas a nivel físico, red, transporte y aplicación (protocolo). Entre los protocolos, se incluyen hasta 50 protocolos industriales para segmentar tráfico atendiendo a este criterio.
- Además, si se trata de Modbus TCP/IP, Ethernet/IP, IEC-104 es capaz de realizar reglas filtrando por function codes.
- En el caso de OPC, autentica cliente y servidor OPC, comprueba que el protocolo utilizado es OPC y permite que el tráfico fluya sólo entre el puerto asignado por el servidor OPC para realizar comunicaciones seguras entre clientes y servidores.
- Ayuda a crear zonas, conductos y canales seguros siguiendo la ISA99.



¿Cuáles son sus principales componentes?

La solución Eagle Tofino se despliega basándose en tres componentes:

1. El TSA (Tofino Security Appliance)

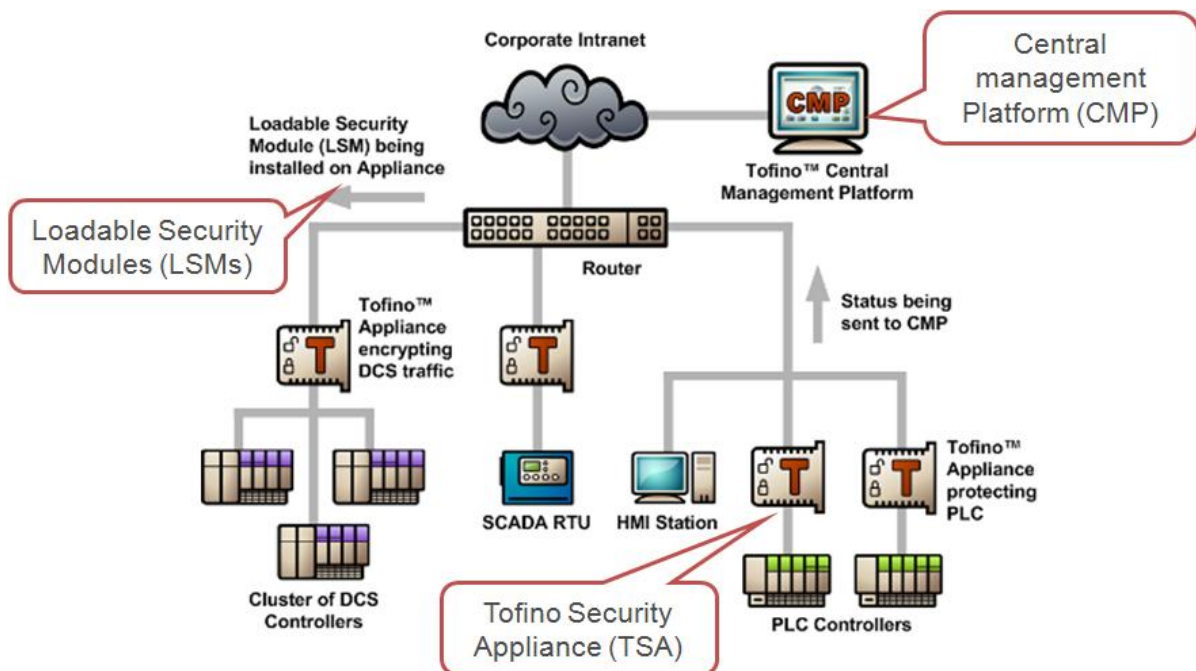
- Es el dispositivo hardware (firewall) que se instala físicamente entre el HMI y el PLC.

2. El CMP (Central Management Console)

- Consola de gestión desde donde se crea la arquitectura lógica de red, las reglas de segmentación, se cargan los LSM (Loadable Security Modules) y se gestionan los logs.

3. Los LSM (Loadable Security Modules)

- Son los diferentes módulos software (firmware) que se instalan en el TSA (a través del CMP) dependiendo de las necesidades funcionales.



Los módulos LSM, permiten que Tofino realice DPI. Estos módulos son:

1. **Firewall:** imprescindible para realizar las reglas de segmentación a nivel IP. Compara el tráfico que fluye entre dispositivos teniendo en cuenta las reglas definidas.
2. **Event Logger:** este módulo permite a los SA (Security Appliance) almacenar eventos, syslog heartbeats y alarmas simultáneamente en un servidor IT (utilizando el protocolo syslog), el datalogger que incorpora la propia SA y la máquina donde esté instalada el CMP (en ficheros .txt).

Eagle Tofino LSM

Firewall

Event Logger

Security Asset Management

Modbus TCP Enforcer

OPC Enforcer

3. **Security Asset Management:** localiza automáticamente todos los dispositivos de red que estén en el mismo rango de direcciones IP que el CMP. En caso de actualizaciones o nuevas incorporaciones de equipos genera avisos de alarmas.
4. **Modbus TCP Enforcer:** segmenta tráfico que no sea conforme al “estandar” Modbus, permite definir reglas teniendo en cuenta un rango de direcciones de “register” y “coils” y permite definir reglas de segmentación por Function Codes. Ejemplo: Una regla que no permita a un maestro ejecutar las “function codes” 05 “write coil” y 06 “write register” sobre un esclavo.
5. **OPC Enforcer:** autentica cliente y servidor OPC, comprueba que el protocolo utilizado es OPC y permite que el tráfico fluya sólo entre el puerto asignado por el servidor OPC para realizar comunicaciones seguras entre clientes y servidores.