¿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.

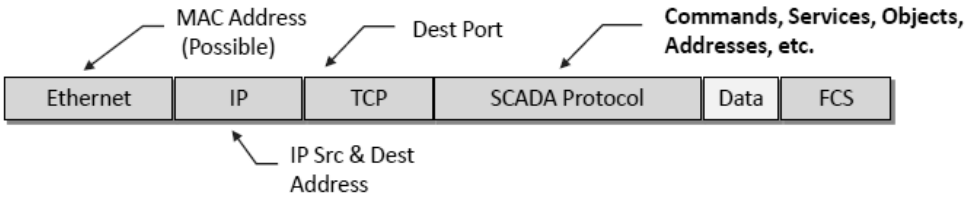
Y para terminar, **¿qué se entiende por DPI (Deep Packet Inspection)?**

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?

- Entiende el tráfico que es transmitido entre dos equipos industriales. Es decir, es capaz de inspeccionar las tramas del protocolo que hablan entre ellos.



- 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 **protocolos industriales**	NO	Dep.	NO	SI
5. Definir reglas a nivel protocolo (function codes) si el protocolo es **Modbus, Ethernet/IP** o asingar un único puerto **sobre OPC**	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 Tofino Xenon de Hirschmann?

El dispositivo **TOFINO Xenon 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 0º a 60º (opcional -40°C a +70°C o ATEX/Class I Div 2), 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 o Ethernet/IP 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 **Tofino Xenon** se compone de tres elementos:

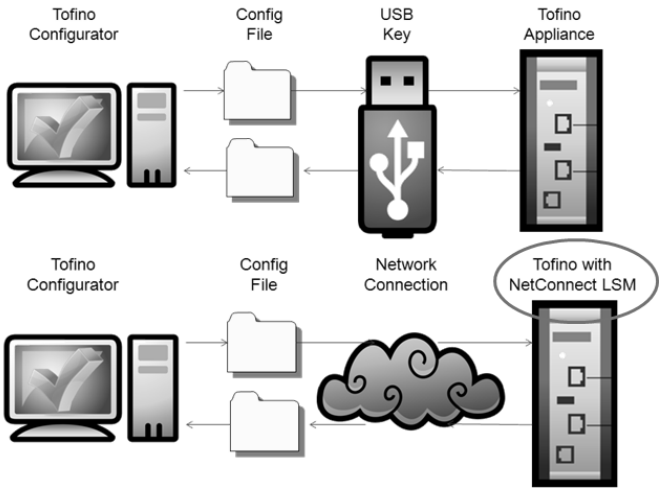
1. **El SA (Security Appliance)** es el dispositivo hardware (firewall) que se instala físicamente entre el HMI y el PLC. Cada dispositivo lleva su propio firmware al que se asocian diferentes LSM (Loadable Security Modules).

2. **Los LSM (Loadable Security Modules)** son los diferentes módulos software (firmware) que se instalan en cada uno de los SA en el momento de ser solicitados, dependiendo de las necesidades funcionales. Se dividen en básicos, el utilizado para parametrizar los SA a través de la red y los denominados Enforcers.

Básicos	Parametrización vía red	Enforcers
• Firewall • Event Logger	• NetConnect	• Modbus TCP Enforcer • OPC Classic Enforcer • Ethernet/IP Enforcer

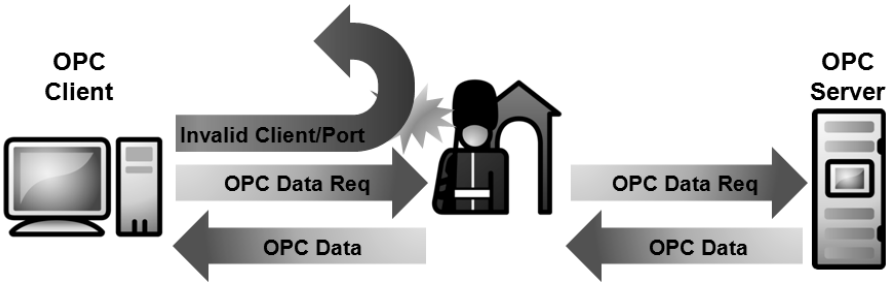
- **Básicos**
  - El módulo de **Firewall** es imprescindible para realizar las reglas de segmentación a nivel MAC e IP. Compara el tráfico que fluye entre dispositivos teniendo en cuenta las reglas definidas.
    - Por defecto se bloquea todo el tráfico que no esté específicamente autorizado.
  - El módulo **Event Logger** permite a los SA (Security Appliance) almacenar hasta 4MB de eventos en formato CEF (Common Event Format).
    - Son accesibles a través del puerto USB o bien exportables a cualquier servidor Syslog.

- **Parametrización vía red**
  - El módulo **NetConnect** permite realizar los procesos de carga, validación y verificación de ficheros de configuración de reglas a través de la red. Habitualmente, la configuración se realiza off-line a través de llaves USB.



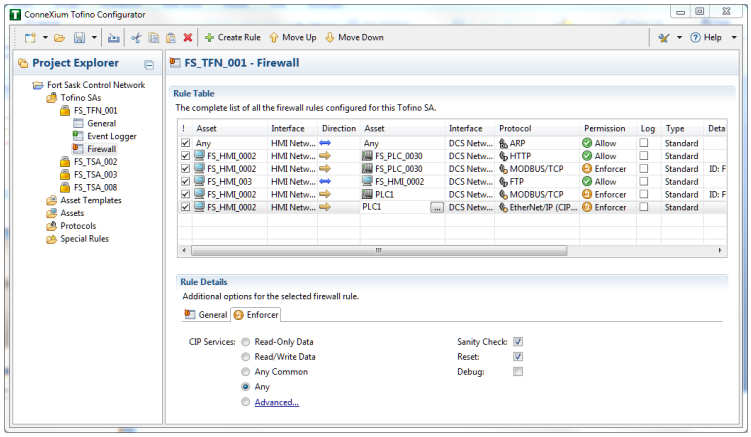
- **Enforcers**
  - El módulo **Modbus TCP Enforcer** segmenta tráfico que no sea conforme al "estandar" Modbus (segmentando sobre todos los componentes Modbus TCP/IP: MBAP header contents, packet size, payload size, register/coil address range), permite definir reglas teniendo en cuenta un rango de direcciones de "register" y "coils" y permite definir reglas de segmentación por Function Codes. Por ejemplo: Una regla que no permita a un maestro ejecutar las "function codes" 05 "write cole" y 06 "write register" sobre un esclavo.

  - El módulo **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. Además, permite acotar el tiempo que debe utilizarse para realizar la transmisión de datos.



- El módulo **Ethernet/IP Enforcer** segmenta tráfico que no sea conforme con el protocolo EtherNet/IP CIP Class 3 asociado a los dispositivos ControlLogix y basado en los ODVA Standards. Permite como en el caso del enforcer de Modbus, realizar reglas de lectura y escritura.

3. El **Tofino Configurator** es la consola que permite configurar la topología de red y llevar a cabo la gestión integral de la seguridad del proyecto. Entre sus principales funciones destacan:
   - Facilitar la gestión del proyecto a través de un entorno gráfico sencillo y amigable.
   - Permitir la autenticación múltiple de acceso a los proyectos (autenticando mediante la license key, user/administrator o usuario Windows).
   - Realizar la creación de plantillas (activos, SA, redes…), incluyendo la funcionalidad “copy-paste” de proyectos.
   - Crear las reglas de segmentación (estándares, especiales, rating y enforcers).
   - Ejecutar las reglas en diferentes modos: pasivo, test y operación.
   - Llevar a cabo la configuración logs de eventos.



   - Cargar las configuraciones vía USB o a través de la red (utilizando en este último caso el NetConnect).
   - Validar y verificar las configuraciones realizadas.
   - Gestionar las versiones de las configuraciones a través de un audit log.

Dr. Fernando Sevillano | fernando.sevillano@logitek.es | Industrial Cybersecurity Manager