Mejores prácticas para la segmentación y fortificación de redes industriales

No disponer de dispositivos que permitan el acceso seguro a la red OT, no configurarlos correctamente, desplegarlos con configuraciones por defecto y/o la falta de políticas de segmentación de red, hacen que los equipos, procesos y sistemas ubicados en el entorno de operaciones sean más vulnerables a amenazas tanto externas como internas.

Es por ello que la incorporación de dispositivos que fortifiquen el acceso perimetral y la correcta segmentación de redes, sea unas de las contramedidas básicas que deben considerarse dentro de una estrategia de defensa en profundidad.

En la figura 1 se observa cómo los entornos IT (normalmente niveles 4 y 3 según la normativa ISA95) y OT (niveles 1 y 2) están comunicados por varios switches, pero todos los equipos se encuentran en el mismo rango de direcciones IP (el 192. 168.1.X).

Para reducir o eliminar esta vulnerabilidad se suelen implantar diferentes dispositivos o mecanismos que persiguen justo eso, segmentar y/o fortificar las redes industriales. Entre estos destacan los routers con listas de control de acceso, los switches inteligentes, los firewalls, la creación de DMZs (zona desmilitarizada) o los diodos de datos. A partir de la arquitectura representada en el figura 1, a continuación se presentan varias alternativas para conseguir que las redes IT y OT queden segmentadas y fortificadas mediante el despliegue de algunos de estos dispositivos.

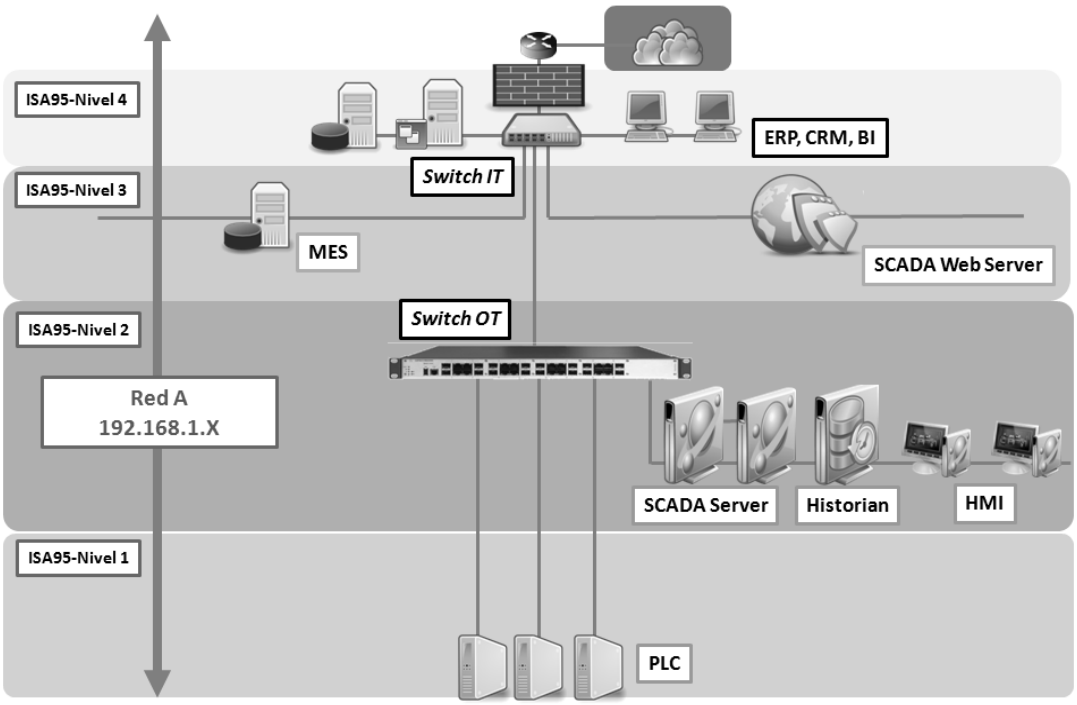

Figura 1. Redes IT y OT no segmentadas

La primera opción que se propone para segmentar ambas redes es la inclusión de un firewall que además permita enrutar tráfico entre las redes IT y OT. Un firewall es un dispositivo que monitoriza y controla el tráfico que fluye entre dos redes. 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.

En la figura 2 puede observarse cómo el dispositivo Firewall/Router separa dos segmentos de redes (la red A, IT con rango de direcciones IP 192.168.1.X y la red B, OT con rango direcciones IP 193.167.1.X). Además de separar, el dispositivo actúa como firewall bloqueando el tráfico no permitido entre ambos segmentos de red. Normalmente este tipo de mecanismo de segmentación puede ser configurado para que realice NAT (Network Address Translation) 1:1, es decir, los equipos ubicados en la red IT sólo ven la dirección IP de la tarjeta de red del router que comunica con los equipos ubicados en la red OT, incrementando así la seguridad en el tránsito de información entre ambas redes.

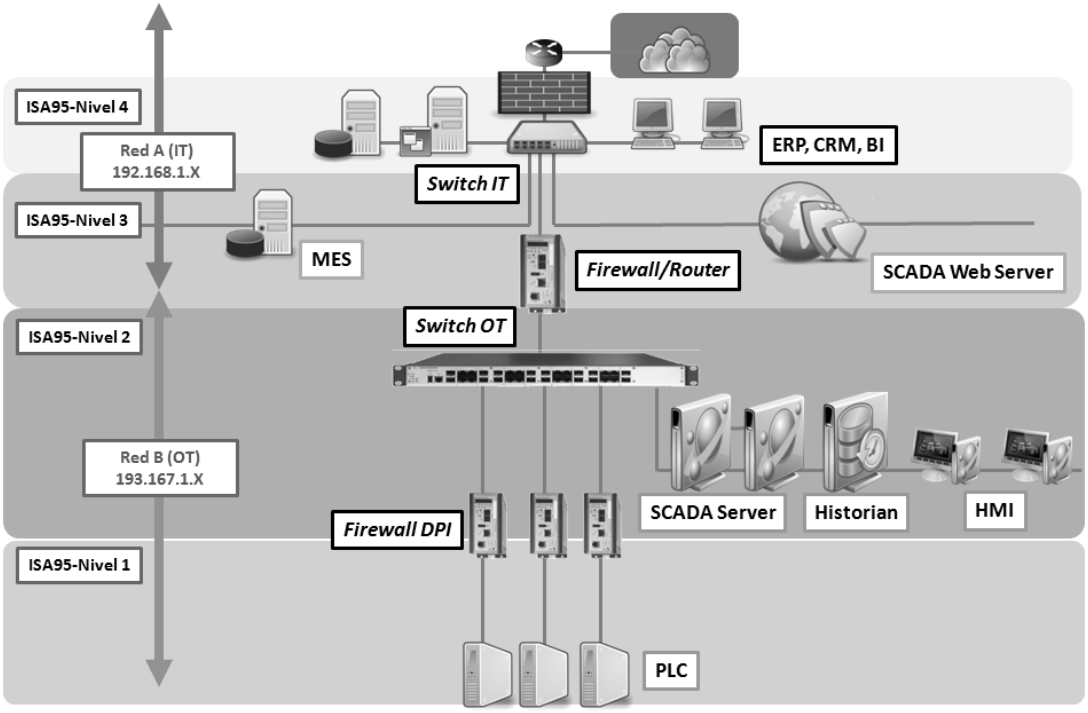

Figura 2. Redes IT y OT segmentadas por un firewall-router

Como complemento a esta primera forma de segmentación, puede crearse una zona desmilitarizada o DMZ. Se trata de una red intermedia que se crea entre dos redes principales a través de dos firewalls. La finalidad de esta red intermedia es que la información/aplicación que quiera ser compartida por los usuarios de las redes principales se ubique en dicha red intermedia, permitiendo por un lado dicho acceso, pero evitando el tráfico y acceso directo entre las dos redes principales.

En la figura 3 se observa cómo entre la red A, IT (192.168.1.X) y la red B OT (193.167.1.X), se ha creado una red intermedia, la DMZ, con su propio rango de direcciones IP (202.168.1.Y). En esta red intermedia se ubican las aplicaciones y/o información que es necesario que sea compartida por los usuarios de las redes IT u OT (las soluciones MES o un Historian-Replicado para que los datos de proceso sean accesible desde IT) o los servidores que deben estar accesibles desde el exterior (SCADA Web Server).

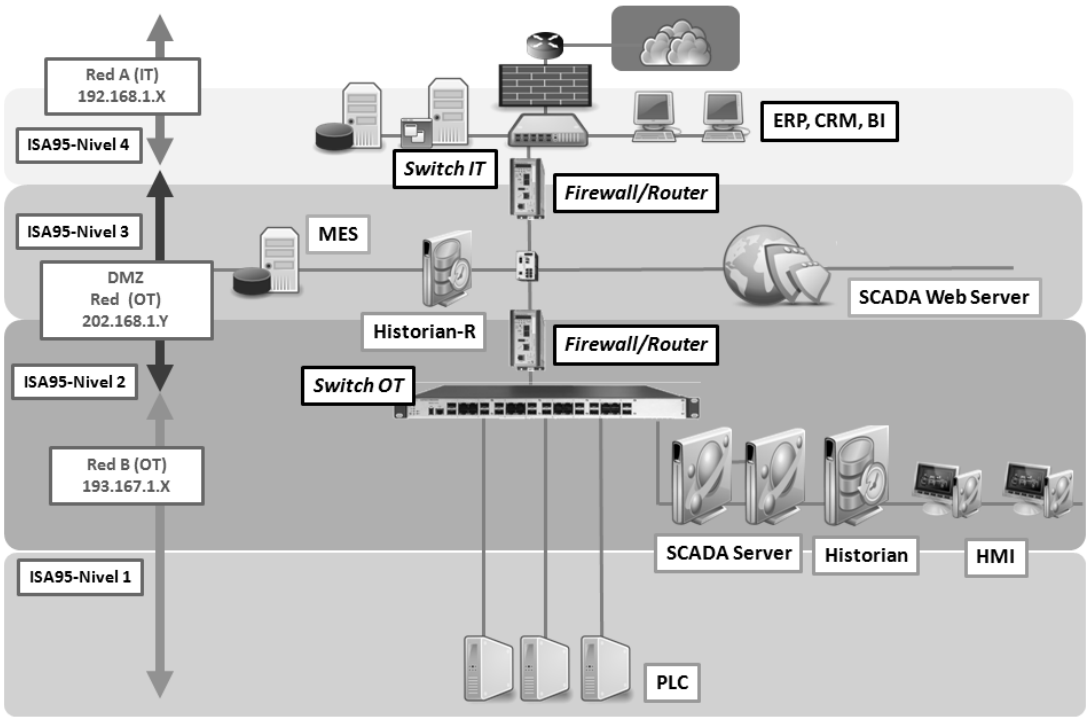

Figura 3. Redes IT, OT y una DMZ creada por dos firewall-router

Para fortificar los niveles 1 y 2, es decir, para proteger el proceso y posibles ataques a los dispositivos de control, se incluyen lo que se denominan Firewalls industriales DPI (Deep Packet Inspection). Como se aprecia en la figura 4, este tipo de firewalls se ubican entre los sistemas SCADA y los PLCs asegurando su disponibilidad y por tanto la del proceso. El hecho de que realicen DPI significa que permiten segmentar tráfico especificando protocolos típicamente industriales (Modbus TCP/IP, Ethernet IP, OPC, etc). Además se pueden configurar reglas de acceso teniendo en cuenta dicho protocolo. Por ejemplo, si el protocolo utilizado es Modbus TCP/IP es posible definir una regla que no permita a un maestro ejecutar las “function codes” 05 “write cole” y 06 “write register” sobre un esclavo. O si se utiliza OPC para comunicar, el firewall es el responsable de asignar un único puerto sobre OPC para realizar comunicaciones seguras entre clientes y servidores.

Por último, hay que mencionar la opción de incorporar un diodo de datos a la arquitectura de red. El diodo de datos es un dispositivo puramente hardware (no existe firmware como el caso de los firewalls) que separa/protege dos redes asegurando la unidireccionalidad en el flujo de información. Es decir, asegura que la información de una red llegue a la otra red (pero no viceversa). De hecho, una de sus principales funciones es sustituir a las ya mencionadas DMZs.

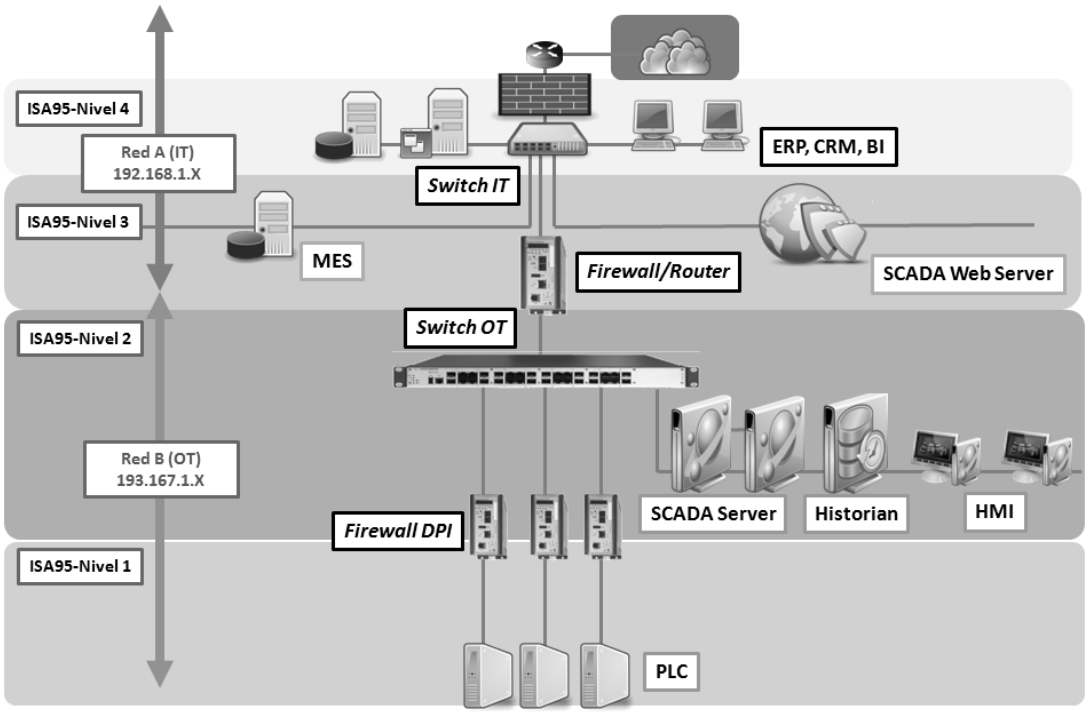

Figura 4. Segmentación entre redes IT, OT y fortificación niveles 1 y 2 a través de firewall DPI

En la figura 5 se representa cómo el diodo de datos segmenta las redes IT y OT. El diodo de datos se compone del hardware que asegura la unidireccionalidad en el tránsito de información (a través de transceptores de fibra óptica) y de dos servidores (denominados proxies). Estos incorporan appliances específicas para transmitir unidireccionalmente información que se maneja en infraestructuras críticas y entornos industriales sobre protocolos como Modbus u OPC, o que se almacena sobre bases de datos industriales como OSIsoft PI o Wonderware Historian.

Cada proxy mantiene comunicaciones bidireccionales entre él y las redes IT y OT respectivamente, sin embargo entre ellos, a través del diodo, la comunicación es unidireccional. La clave del diodo de datos es ésta, es capaz de interpretar protocolos bidireccionales (típico, TCP, que requiere el handshaking de tres vías), “romperlos” y convertirlos en unidireccionales (entre los proxies y el hardware del diodo) y luego presentarlos en la red no comprometida de nuevo como bidireccionales. En la figura se puede ver por un lado, cómo la información que se maneja en la red OT llega a la red IT estando disponible para sus usuarios, sin que estos, en ningún caso, accedan a la

red de operaciones. Por otro, también puede verse cómo los datos de la red OT se transmiten unidireccionalmente a través de Internet a terceros, evitando posibles accesos no autorizados por su parte, ya que el diodo lo impide. Este tipo de solución está muy extendida en las centrales nucleares o en instalaciones militares, por poner sólo dos ejemplos, y podría ser perfectamente extrapolable a otros sectores (aguas, química, oil&gas, telecomunicaciones, etc.).

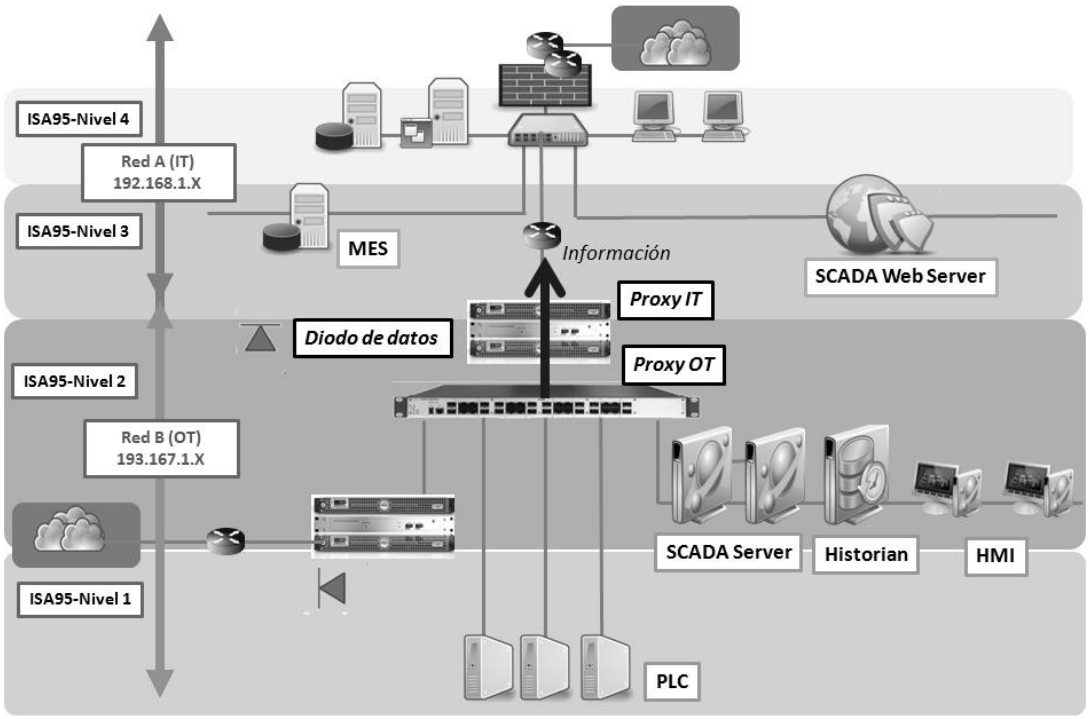

Figura 5. Segmentación entre redes IT, OT a través de diodo de datos

Teniendo en cuenta la arquitectura de red existente en cada planta y la criticidad de los procesos, se deben adoptar las soluciones de segmentación y fortificación más apropiadas. En cualquier caso, considerando la idiosincrasia de los entornos OT y de cara a incrementar la seguridad de sus redes industriales, es imprescindible auditar su estado; inventariando los dispositivos que se conectan a ellas, identificando los medios a través de los cuáles son accesibles y analizando su grado de segmentación.

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