



Módulo Software Filtrado IP

Identificador
Versión
Fecha
URL de control

SW-FILTROIP-001
v1.0
2025-11-29
<https://docs.fortiseg.eu/SW-FILTROIP-001.pdf>



Versión online

Módulo de Filtrado IP – Descripción Técnica

1. Propósito del módulo

El **Módulo de Filtrado IP** de SolearesMQ permite **restringir el tráfico entrante y saliente** de la RTU para garantizar que únicamente se acepten conexiones desde **IPs explícitamente autorizadas**.

Su objetivo principal es reforzar la ciberseguridad de la instalación, reducir la superficie de ataque y evitar accesos no autorizados desde Internet o redes internas. Este módulo es especialmente importante en: - Proyectos de **Medida Fiscal (MF/TF)** donde REE debe acceder exclusivamente desde sus IPs autorizadas.

- Proyectos **TTR, DD y SRAP**, donde el flujo MQTT debe recibirse únicamente desde servidores/verificadores aprobados.

- Entornos industriales con **redes sensibles o expuestas**.

2. Funcionalidad principal

El módulo implementa un sistema de control de acceso basado en listas blancas:

Funciones clave

- Permitir únicamente tráfico desde **IPs o rangos autorizados**.
- Bloquear tráfico no identificado o potencialmente malicioso.
- Aplicar políticas de filtrado diferentes según:
 - Protocolo (MQTT, 102-TCP, HTTP, Modbus TCP...)
 - Puerto
 - Interfaz (Ethernet / WiFi / 4G)
- Filtro activo tanto para tráfico entrante como saliente.
- Registros opcionales de intentos denegados (modo auditoría).

- Integración total con la RTU SolearesMQ, incluida la arquitectura DUO+.

3. Arquitectura del módulo

3.1 Componentes internos

El módulo consta de: - Motor de filtrado a nivel de firewall interno de la RTU.

- Tabla de reglas persistentes incluso tras reinicio.
- Sistema de validación sintáctica de IPs y rangos CIDR.
- Integración con la capa de servicios para evitar reglas contradictorias.

3.2 Flujo de operación

1. El usuario o técnico define una lista de IPs permitidas.
2. El módulo compila automáticamente las reglas necesarias.
3. El firewall interno aplica dichas reglas.
4. El resto del tráfico queda bloqueado por defecto ("**deny all**").
5. Los accesos denegados pueden registrarse para auditoría si se habilita.

4. Modos de operación

4.1 Modo "Lista Blanca" (predeterminado)

- Solo se permite tráfico explícitamente autorizado.
- Ideal para:
 - Acceso de REE por 102TCP.
 - Comunicaciones MQTT entre RTU y CCO.

4.2 Modo "Restricción parcial"

- Permite tráfico autorizado y ciertos servicios internos esenciales (HCS, DNS, NTP).

4.3 Modo “Auditoría”

- No bloquea tráfico, solo registra intentos para análisis.
- Útil en fase de pruebas antes de activar el filtrado definitivo.

5. Integración con SolearesMQ

5.1 Compatibilidad con módulos

El Filtrado IP se integra con todos los módulos principales: - **MF/TF (102TCP)** – restringe conexiones entrantes a IPs oficiales de REE.

- **TTR** – asegura que el envío MQTT solo se realice a brokers autorizados.
- **DD** – evita conexiones externas no autorizadas.
- **SRAP** – protege el canal crítico de consignas.

5.2 Integración con DUO+

En sistemas DUO+: - El filtrado se aplica **solo al nodo EXTERNO**, evitando accesos desde Internet.

- El nodo INTERNO permanece aislado físicamente y sin puertos de acceso. Esto proporciona doble protección física + lógica.

6. Ventajas operativas

Ciberseguridad

- Reducción casi total de accesos no autorizados.
- Protección frente a escaneos, ataques automatizados y tráfico sospechoso.
- Minimiza la posibilidad de explotación de puertos abiertos.

Estabilidad

- Evita interferencias de tráfico no deseado.
- Reduce carga en la red y mejora el rendimiento de servicios críticos.

Integración limpia

- No requiere VPN ni túneles adicionales.
- Compatible con red 4G, fibra, radioenlaces o accesos mixtos.

7. Especificaciones técnicas

Parámetro	Especificación
Tipos de IP permitidos	IPv4 individual o rangos CIDR
Protocolo soportado	Cualquiera (TCP/UDP)
Interfaz aplicable	Ethernet / WiFi / 4G
Persistencia	Sí, reglas permanentes
Auditoría	Opcional, logs locales
Compatibilidad	Todos los modelos SolearesMQ
Integración DUO+	Total, en nodo EXTERNO

8. Requisitos de instalación

- Definir previamente la lista de IPs autorizadas.
- Conocer los puertos necesarios para cada módulo:
 - **102TCP**: puerto 50134 (REE)
 - **MQTT**: puertos según broker del CCO o HCS
- Comprobar que la tarjeta SIM o proveedor de red permite tráfico IP directo.
- Evitar errores comunes como:
 - Incluir IPs privadas cuando el acceso es público.
 - Olvidar rangos completos necesarios para REE.

9. Casos de uso recomendados

- Aislar completamente las RTU de Internet salvo para IPs explícitas.
- Proteger plantas pequeñas con accesos 4G vulnerables.
- Endurecer comunicaciones TTR/Datos/SRAP.
- Cumplir con normativas de seguridad (ENS, IEC 62443 según caso).
- Fase previa a auditoría interna o integración en CCOs nuevos.

10. Conclusión

El **Módulo de Filtrado IP** es un componente esencial para fortalecer la seguridad de cualquier despliegue con RTUs SolearesMQ, especialmente en comunicaciones críticas con REE o CCOs.

Su filosofía de lista blanca garantiza que solo los sistemas autorizados puedan acceder al dispositivo, eliminando amenazas externas y endureciendo de forma significativa la red de telecontrol.

Es una herramienta ligera, robusta y totalmente integrada con el ecosistema SolearesMQ, ideal para instalaciones industriales que requieren seguridad y disponibilidad 24/7.