Fortiseg

Configuración y Pruebas de Filtrado IP para Modbus

Identificador	SRV-CYB-002
Versión	v1.0
Fecha	2026-02-23
Generado	202602241121
URL de control	https://docs.fortiseg.eu/SRV-CYB-002.pdf

Versión online

Servicio: Configuración y Pruebas de Filtrado IP para Modbus

1. Descripción del servicio

Servicio de **configuración, verificación y puesta en marcha** del Módulo de Filtrado IP de SolearesMQ para entornos que utilizan el protocolo **Modbus TCP**. El objetivo es garantizar que las RTUs solo acepten conexiones Modbus TCP desde las **IPs autorizadas del SCADA, centro de control o sistemas de supervisión**, bloqueando cualquier otro tráfico entrante al puerto del servicio.

Modbus TCP, al ser un protocolo **sin autenticación nativa**, es especialmente vulnerable a accesos no autorizados. El filtrado IP proporciona una capa de protección fundamental para evitar lecturas o escrituras no autorizadas en registros de la RTU.

2. Alcance

Incluido

- Revisión de la arquitectura de red y conectividad de la RTU.
- Identificación de las IPs autorizadas (SCADA, CCO, sistemas de supervisión, integradores).
- Configuración del Módulo de Filtrado IP en modo **lista blanca** para el puerto Modbus TCP (502 o el configurado).
- Verificación de conectividad con las IPs autorizadas tras activar el filtrado.
- Pruebas de bloqueo de conexiones no autorizadas.
- Activación del modo auditoría para registro de intentos denegados.
- Documentación de la configuración aplicada.

No incluido

- Configuración del propio protocolo Modbus (mapas de registros, polling, etc.).
- Modificaciones en la red del cliente o proveedor de comunicaciones.
- Suministro de hardware o tarjetas SIM.

3. Metodología

Fase 1 — Análisis previo

1. Recopilación de datos de red: IPs del SCADA/CCO, puertos Modbus configurados, interfaz de comunicación.
2. Identificación de todos los masters Modbus que deben acceder a la RTU.
3. Verificación del estado actual del módulo de filtrado.
4. Revisión de servicios activos que deben permanecer accesibles.

Fase 2 — Configuración

1. Definición de reglas de filtrado:
   - **Entrada:** permitir IPs autorizadas al puerto Modbus TCP.
   - **Salida:** permitir respuestas Modbus y servicios esenciales (NTP, DNS si aplica).
   - **Por defecto:** deny all.
2. Aplicación de reglas en el Módulo de Filtrado IP.
3. Verificación de persistencia tras reinicio.

Fase 3 — Pruebas

1. **Test de conectividad positiva:** confirmar que el SCADA/CCO conecta correctamente vía Modbus TCP y realiza lecturas/escrituras con normalidad.
2. **Test de bloqueo:** verificar que conexiones Modbus desde IPs no autorizadas son rechazadas.
3. **Test de auditoría:** comprobar que los intentos denegados quedan registrados.
4. **Test de integridad:** verificar que las respuestas Modbus no se ven afectadas por el filtrado (tiempos de respuesta, timeouts).
5. **Test de estabilidad:** mantener el filtrado activo durante un periodo de observación (mínimo 24h recomendado).

Fase 4 — Documentación y entrega

1. Informe de configuración con las reglas aplicadas.
2. Registro de pruebas realizadas y resultados.
3. Recomendaciones de mantenimiento y revisión periódica.

4. Requisitos previos del cliente

- RTU SolearesMQ con Módulo de Filtrado IP instalado y licenciado.

- Listado de **IPs autorizadas** para el servicio Modbus TCP (SCADA, CCO, supervisión, integradores con acceso permanente).
- **Puerto configurado** para el servicio Modbus TCP (por defecto 502).
- Acceso remoto o presencial a la RTU para configuración.
- Contacto técnico del cliente o integrador para coordinación de pruebas.

5. Entregables

Entregable	Formato
Informe de configuración	PDF
Registro de pruebas	PDF
Tabla de reglas aplicadas	Incluida en informe
Recomendaciones de mantenimiento	Incluidas en informe

6. Duración estimada

Fase	Duración
Análisis previo	1-2 horas
Configuración	1-2 horas
Pruebas	2-4 horas (+ periodo de observación)
Documentación	1-2 horas
Total	**1 jornada** (+ observación remota)

7. Protocolos y puertos afectados

Protocolo	Puerto típico	Dirección	Acción
Modbus TCP	502	Entrada	Permitir solo IPs autorizadas
NTP	123	Salida	Permitir (sincronización horaria)
DNS	53	Salida	Permitir si necesario
Resto	*	*	Bloquear (deny all)

8. Consideraciones de seguridad específicas de Modbus

Modbus TCP presenta vulnerabilidades inherentes al protocolo que hacen especialmente relevante el filtrado IP:

- **Sin autenticación:** cualquier cliente que conecte al puerto puede leer y escribir registros.
- **Sin cifrado:** el tráfico viaja en claro, susceptible de interceptación.

- **Function codes críticos:** escrituras en registros (FC 05, 06, 15, 16) pueden alterar el comportamiento de la instalación.
- **Escaneo trivial:** herramientas como Nmap detectan puertos Modbus abiertos en segundos.

El filtrado IP mitiga estos riesgos al restringir el acceso exclusivamente a los sistemas autorizados.

9. Compatibilidad

- Todos los modelos de RTU SolearesMQ.
- Arquitectura DUO+ (filtrado en nodo EXTERNO).
- Interfaces: Ethernet, 4G, WiFi, radioenlace.
- Compatible con cualquier master Modbus TCP estándar.
- Soporta múltiples masters simultáneos (cada uno con su IP autorizada).