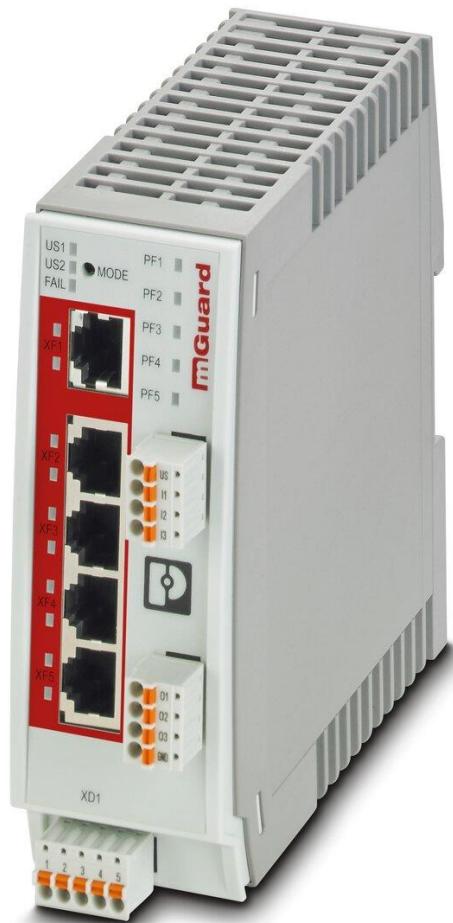


Configuración básica FL MGUARD 1102

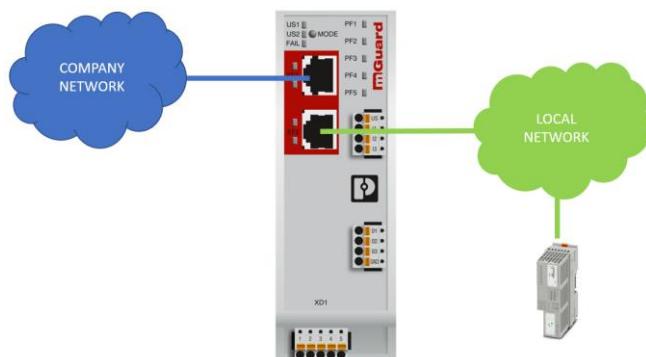


Contenido

1	Introducción	3
2	Descripción de la configuración de ejemplo.....	3
3	Configuración del mGuard	4
4	Cambio del password por defecto	8
5	Habilitar acceso desde XF1 (WAN)	8
6	Devolver el equipo a estado de fábrica (factory reset).....	9

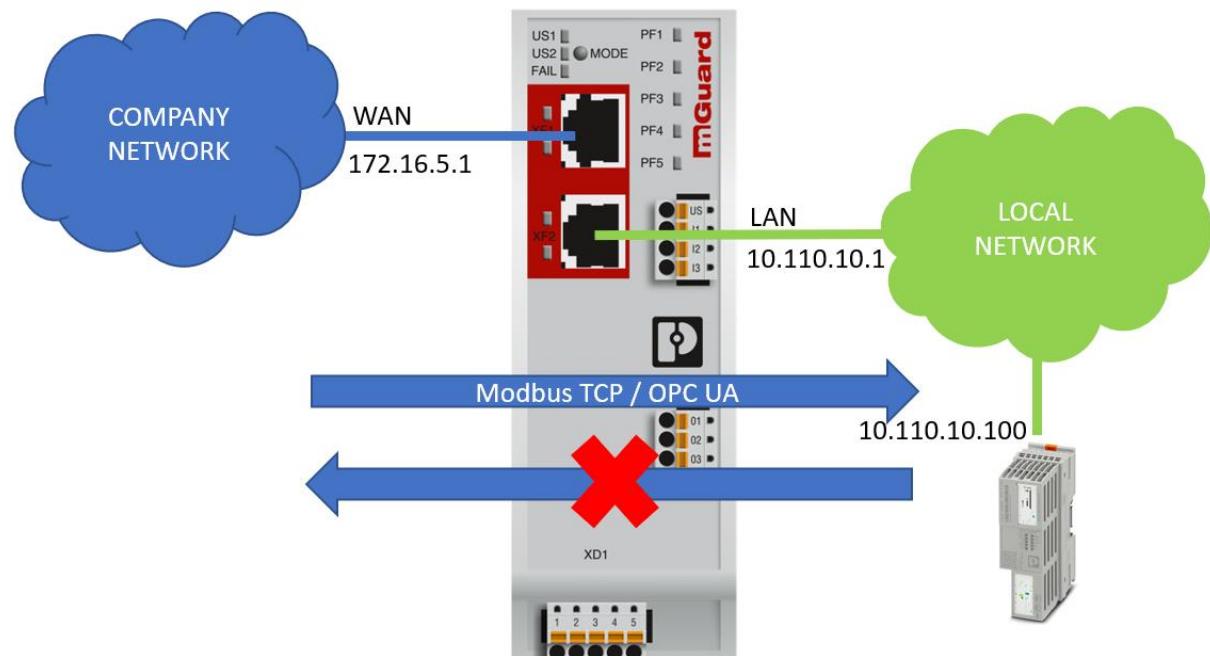
1 Introducción

En la siguiente guía se describen los pasos para hacer una configuración básica del FL MGUARD 1102 para hacer una segmentación entre 2 redes.

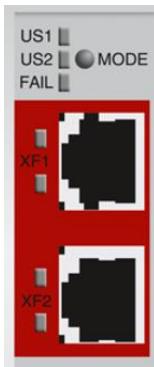


2 Descripción de la configuración de ejemplo

Nuestro objetivo en esta guía es la configuración del FL MGUARD 1102 permitiendo tráfico Modbus TCP y OPC UA desde la red externa (red de empresa) hacia un PLC conectado en nuestra red local. El resto del tráfico está bloqueado desde la red externa hacia la red local.



La red externa tendrá un rango 172.16.5.x y la interna 10.110.10.x .



El puerto marcado como XF1 es WAN (red externa) y XF2 es LAN (red local).

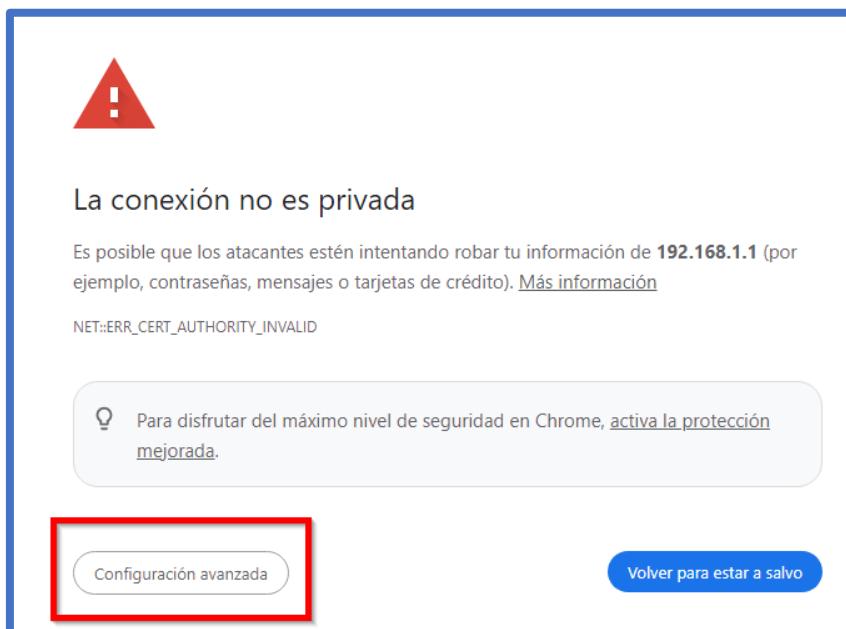
Asumimos que el mGuard se encuentra en estado de fábrica. Si no es así, vaya al punto **XXXX** de esta guía para hacer un reset a etado incial.

3 Configuración del mGuard

Ajustamos la dirección IP de nuestro PC a la 192.168.1.100 y lo conectamos al puerto XF2 del mGuard.

Escribimos <https://192.168.1.1> en cualquier navegador web.

Aparecerá este mensaje:



Presionamos "Configuración avanzada":



La conexión no es privada

Es posible que los atacantes estén intentando robar tu información de **192.168.1.1** (por ejemplo, contraseñas, mensajes o tarjetas de crédito). [Más información](#)

NET::ERR_CERT_AUTHORITY_INVALID

💡 Para disfrutar del máximo nivel de seguridad en Chrome, [activa la protección mejorada.](#)

Ocultar configuración avanzada

Volver para estar a salvo

Este servidor no ha podido probar que su dominio es **192.168.1.1**, el sistema operativo de tu ordenador no confía en su certificado de seguridad. Este problema puede deberse a una configuración incorrecta o a que un atacante haya interceptado la conexión.

[Acceder a 192.168.1.1 \(sitio no seguro\)](#)

Presionamos “Acceder a 192.168.1.1 (sitio no seguro)”.

Nos aparecerá la página de introducción de usuario y contraseña.

The page is titled "Login". It features a logo for "PHOENIX CONTACT" with a stylized "P" icon. Below the logo is a horizontal bar composed of colored dots (blue, green, yellow, orange, red). The main form has two input fields: one for "username" containing "admin" and another for "password" containing "*****". To the right of the password field is a small "eye" icon for password visibility. Below the form is a note: "mGuard Security Appliance" followed by "The usage of this mGuard security appliance is reserved to authorized staff only. Any intrusion and its attempt without permission is illegal a...". A "Show more" link is present. At the bottom is a teal "Log in" button.

Introducimos admin/private como usuario/password.

Ahora vamos a asignar las direcciones IP para XF1 (WAN) y XF2 (LAN).

The screenshot shows the mGuard configuration interface. The left sidebar has 'Network' (1) selected under 'Interfaces' (2). The top navigation bar has 'Interfaces' (3) selected. The main area shows 'Net zone 1' and 'Net zone 2'. For 'Net zone 1', 'Router mode' is 'Static' (4), 'IP address' is 172.16.5.1 (5), and 'Netmask' is 24. For 'Net zone 2', 'IP address' is 10.110.10.1 (6) and 'Netmask' is 24.

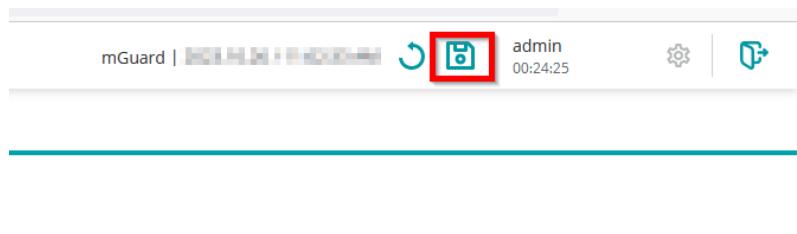
Debemos ir al menu Network (1) → Interfaces (2), pestaña Interfaces (3).

Cambiar el modo (Mode) a Router (4).

Para Net zone 1 (WAN) seleccionar Static e introducir los datos de la dirección IP (5).

Para Net zone 2 (LAN), ajustar la dirección IP (6).

Pulsar el icono del diskette en la parte superior derecha de la página web para guardar los cambios.



Nos aparecerá el siguiente mensaje advirtiendo de que hemos hecho cambios en las IPs y esto afectará a la conectividad. El equipo ya no será accessible mediante 192.168.1.1 como hasta ahora.



The changes have been saved successfully. The device will soon be reachable via the new IP address. If required, use the new IP address to log in to the device.

El mGuard será configurable ahora usando <https://10.110.10.1> cuando estemos conectados al puerto XF2 (LAN).

Crearemos ahora unas reglas de port forwarding para permitir tráfico (Modbus TCP y OPC UA) desde XF1 (WAN) hacia XF2 (LAN).

Para ello iremos al menú Network (1) → Interfaces (2) → NAT (3).

The screenshot shows the mGuard configuration interface. The left sidebar has a tree structure: Management, Authentication, Network (1), Interfaces (2), DHCP server, DNS, Network security, Logging, and Support. The 'Network' node has a red circle with the number 1. The 'Interfaces' node has a red circle with the number 2. The 'NAT' tab in the main content area is selected and has a red circle with the number 3. In the 'IP masquerading (NAT)' section, there are two toggle switches: 'Masquerade to net zone 1' is set to 'On' (highlighted with a red circle 4) and 'Masquerade to net zone 2' is set to 'Off'. Below this is a 'Port forwarding' section with a 'Add row' button (highlighted with a red circle 5). A table header for 'Port forwarding' includes columns: ID, Protocol, From, Incoming port, To IP, To port, Comment, and Select All. Below is a '1:1 NAT' section with its own 'Add row' button and a table header: ID, Real IP/network, Translated IP/network, Comment, and Select All.

Nos aseguraremos de que la opción Masquerade to net zone 1 es ACTIVA (4).

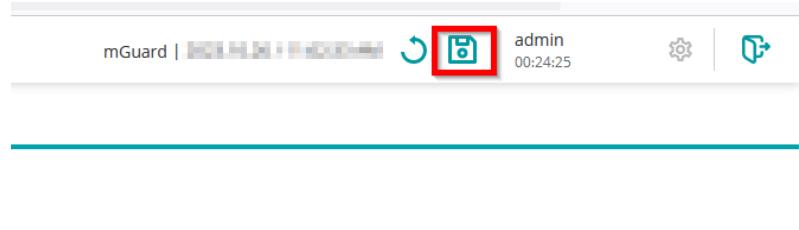
Hacemos click en el botón Add row (5). Deberemos introducir las siguientes líneas.

Port forwarding

ID	Protocol	From	Incoming port	To IP	To port	Comment	Select All
1	TCP	Net zone 1	502	10.110.10.100	502	Modbus TCP	<input type="checkbox"/>
2	TCP	Net zone 1	4840	10.110.10.100	4840	OPCUA	<input type="checkbox"/>

Estas dos entradas redireccionarán el tráfico deseado hacia el PLC con dirección IP 10.110.10.100

Salvamos los cambios realizados con el mismo icono del diskette que hemos usado antes.





Nos aseguraremos de que el PLC tiene asignada la IP 10.110.10.1 como puerta de enlace. De otra manera habrá problemas de funcionamiento

4 Cambio del password por defecto

Probablemente necesitemos/deseemos cambiar el password por defecto del equipo.

Esto se puede hacer usando el icono que se encuentra en la esquina superior derecha del servidor web del mGuard.

Change own password x

Current password

New password

Confirm new password

Cancel Change password

El nuevo password puede ser introducido desde este menú.

5 Habilitar acceso desde XF1 (WAN)

Por defecto el acceso al servidor web del mGuard se realiza desde la red XF2 (LAN).

En caso de que necesitemos habilitar el acceso desde XF1 (WAN), lo podremos hacer en la forma que se describe a continuación.

En el menú de la izquierda vamos a Management (1) → Device access (2) → enable HTTPS access from net zone 1 (3).



WARNING: THE DEFAULT PASSWORD HAS NOT YET BEEN CHANGED.

- Management 1
- Device access 2

Device access

Time and date

Firmware update

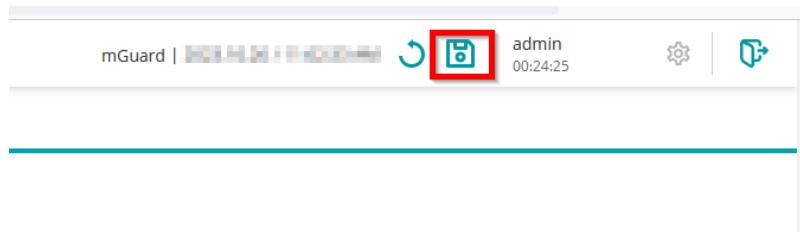
SNMP

System

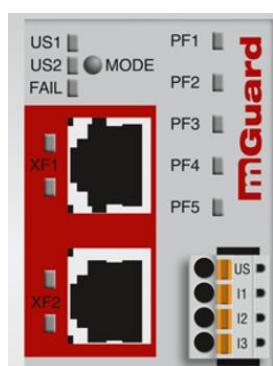
HTTPS access from net zone 1 On 3

HTTPS access from net zone 2 On

De nuevo debemos recordar guardar los cambios realizados.



6 Devolver el equipo a estado de fábrica (factory reset).



- Apagar el equipo.
- Encenderlo.
- En menos de 2 segundos, presionar el botón MODE.
- Esperar hasta que los sleds PF1...PF5 parpadeen en verde.
- Soltar botón MODE.
- Presionar y soltar MODE hasta que PF3 esté ON.
- Presionar MODE hasta que PF1..PF5 parpadeen verde.
- Soltar botón MODE.
- Reiniciar el equipo.