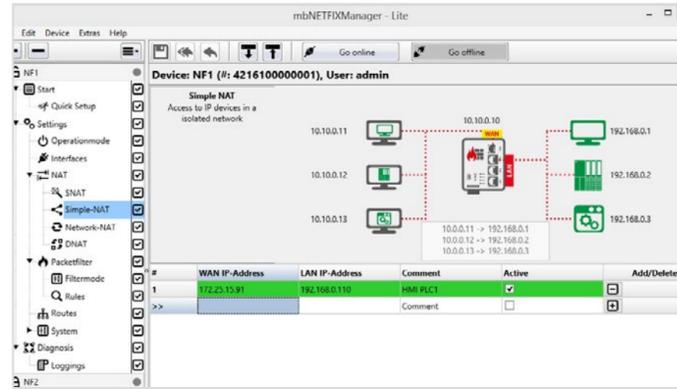## Preserve Automation Users Workflows

Manage the mbNETFIX like you would manage a PLC. Simply prepare a project and upload the configuration. You can go online with the device and make changes and adjustments on the runtime, before saving the project for later reference.

Projects are protected by password and uniquely paired with their run-time version on the device. Projects can be exported and shared with other users, with equal or lesser access capabilities.
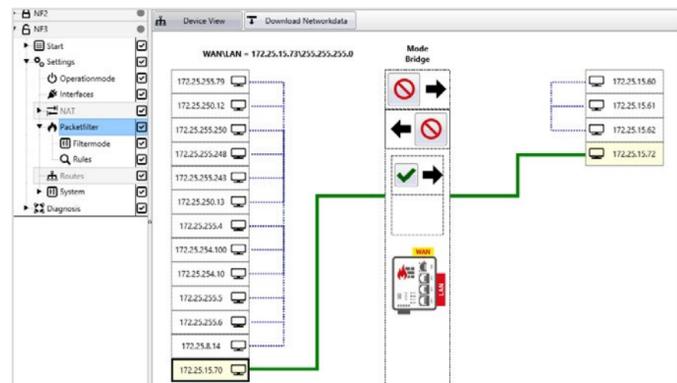
Graphical User Interface
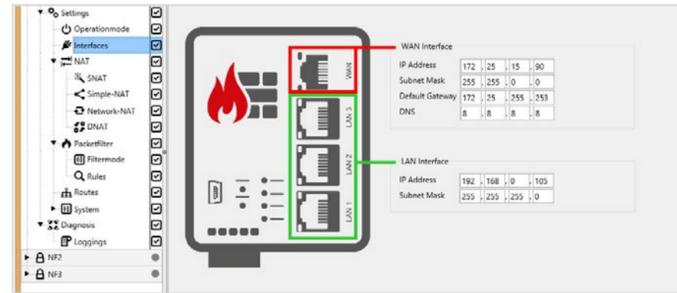
The mbNETFIX manager assists the automation user in creating a project and setting up the device. It is designed to resemble the user interface of a PLC programming software.

The graphical user interface shows dynamically how the device is configured. Changes are displayed immediately. As a result, you can see how the actual NAT- and filtering rules are applied.

Learning Mode

Unplug the machine from the network and connect it to one mbNET-FIX LAN port. Plug the mbNETFIX WAN port back on the network. The firewall will listen to the occurring traffic.

When going online, you can see the traffic in the graphical user interface (GUI), as spotted by the firewall. Now you can select in mbNETFIX manager which connections are to be closed and which should be preserved.

The actual filter rules will be written automatically.

SPECIFICATIONS

✓ IP, port, MAC and protocol filters for monitoring and restricting data traffic

✓ Versatile NAT functionalities, eg 1:1 NAT, SimpleNAT and port forwarding

✓ Static routes

✓ 1x WAN and 3x LAN port switch

✓ Configuration with comfortable software

✓ Security by Design

✓ Power supply 10-30 VDC

✓ DIN rail mounting

✓ Dimensions 69 mm x 38.5 mm x 92.5 mm (W x D x H)

Order Details

Hardware

Name	Item No.	WAN	LAN	Description
NFH100	5.100.200.03.00	1x	3x	3x LAN 10/100 MBit/s

Software

Name	Item No.	Description
mbNETFIX Manager Lite	5.900.000.01.00	USB-Stick mit Manager Lite Software

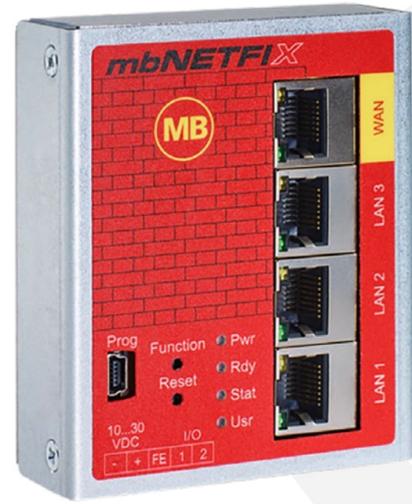mbNETFIX_EN_6S_240325

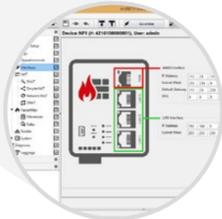REDLION®

MB CONNECTLINE

mbNETFIX

THE AUTOMATION FIREWALL
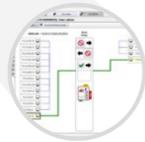
mbNETFIX

SECURE AND CONNECT INDUSTRIAL NETWORKS
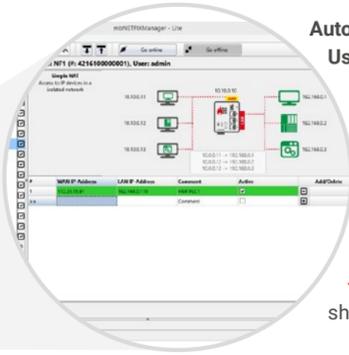
Automation User's Workflow

✓ Prepare projects and upload them to the device

✓ Go online and make changes on the runtime version

✓ Export projects and share with other users

Graphical User Interface

✓ PLC programming-like environment
✓ View configuration and changes
✓ See how setup and rules apply

Learning mode

✓ Visualize actively communicating devices
✓ Choose general traffic policies
✓ Select which connections need to be preserved
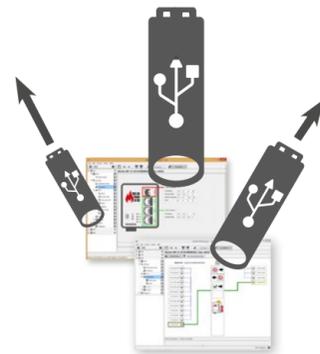

Simple, fast and secure configuration

Step 1
Prepare a project and load the configuration onto the device.

Step 2
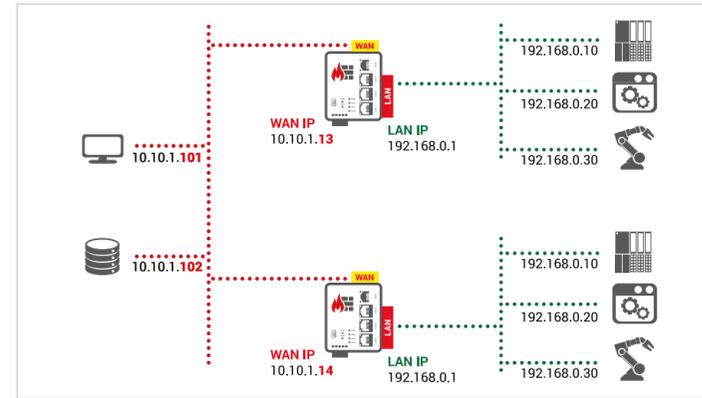Go online and adjust the settings if necessary.

Step 3
Share the project easily and securely in an encrypted container.

Secure Your Production Network

Avoid address conflicts & isolate internal network

Because machine components need to communicate seamlessly with other production devices, it is important to isolate the machine internal network from the factory network and offer a controlled access to its components services.

Hiding the internal network behind a firewall is a way to avoid address conflicts when installing new machines.

10.10.1.101
WAN IP 10.10.1.13 — LAN IP 192.168.0.1 — 192.168.0.10 / 192.168.0.20 / 192.168.0.30

10.10.1.102
WAN IP 10.10.1.14 — LAN IP 192.168.0.1 — 192.168.0.10 / 192.168.0.20 / 192.168.0.30

Secure old equipment

Old machines and production systems are often still very valuable for the factory. Sometimes, plant operators would prefer to postpone changes as long as possible.
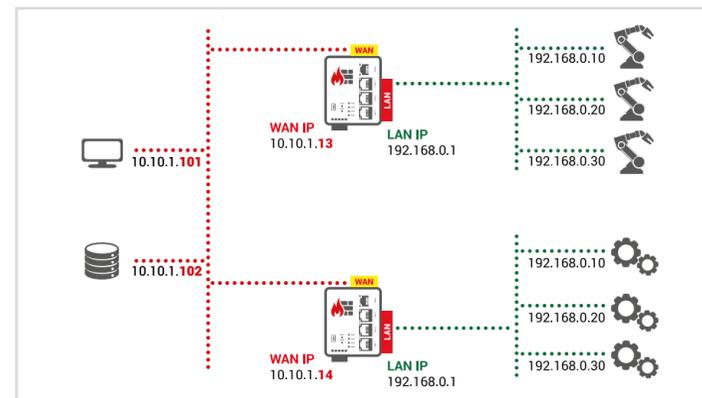
Yet, those systems, running on outdated operating systems are particularly vulnerable to modern cyber-threats. By controlling the access to such equipment, the firewall will contribute to extend its operational lifetime.

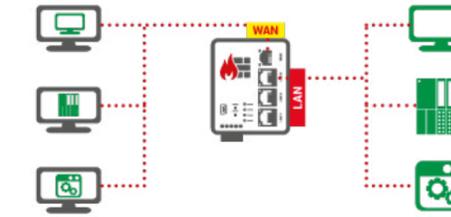192.168.0.x/24
192.168.0.x/24
192.168.0.x/24
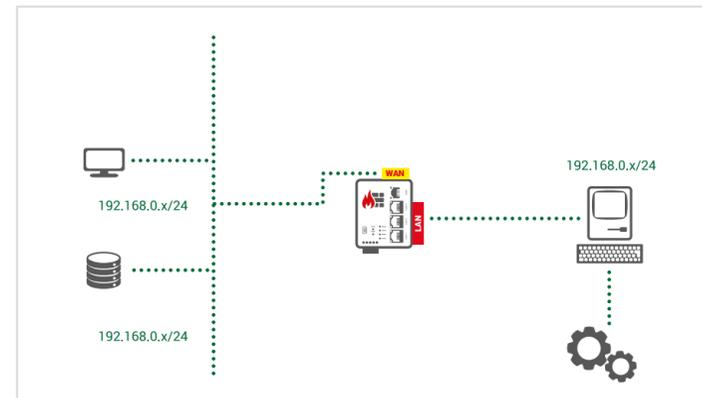
Isolate machines or groups of machines

A factory may use multiple production lines with several independent units. Machines within these units may generate a lot of traffic.

The firewall will keep this traffic locally and preserve the OT-network from it. Also, by segmenting the network and controlling access rules, the firewall will prevent possible cyber-threats to spread from one to another.
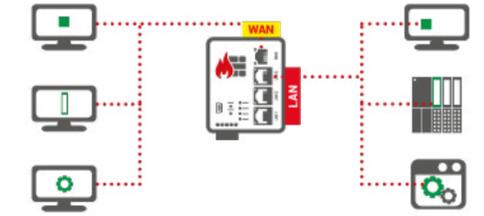
10.10.1.101
WAN IP 10.10.1.13 — LAN IP 192.168.0.1 — 192.168.0.10 / 192.168.0.20 / 192.168.0.30

10.10.1.102
WAN IP 10.10.1.14 — LAN IP 192.168.0.1 — 192.168.0.10 / 192.168.0.20 / 192.168.0.30

Fully functional Router and Firewall

Simple NAT
Selected LAN devices appear with an individual WAN address managed by the router.

Source NAT
LAN devices reply locally to the router, no gateway needed.

Network NAT
LAN network remains hidden, WAN devices access it through a virtual LAN network managed by the router.

Portforwarding
With portforwarding, a single port can be directed to a specific IP-address by specifying the port.

Security by Design

mbNETFIX 1 — public key
mbNETFIX 2
mbNETFIX3

mbNETFIX MANAGER
Project 1 — public key / private key
Project 2
Project 3
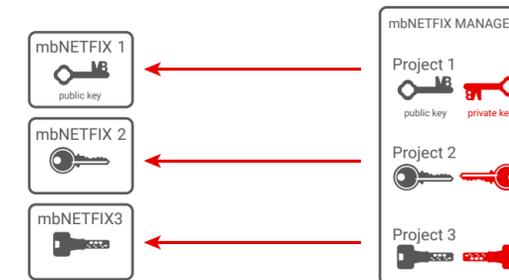
Security by Design is about implementing information security right from the beginning of the design process. In order to keep attack vectors as small as possible the automation firewall features characteristics, such as:

✓ No embedded website: Securing a website is complex and requires considerable resources, hardly available when dealing with embedded programming.

✓ Projects are encrypted and uniquely paired by means of an RSA key. This key is automatically generated and stored on the device. It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communication.

3+1 User Access Levels

Administrator
Full access to the device configuration and can export the projects for users with more restricted accesses.

Operator
Can change routing tables, NAT settings, filtering rules, but not operating mode, system settings, LAN or WAN addresses.

Viewer
Has full viewing access but cannot make any change (diagnostic user).

Factory Reset
Can only reset the unit and requires visual and physical access to the unit to do so.