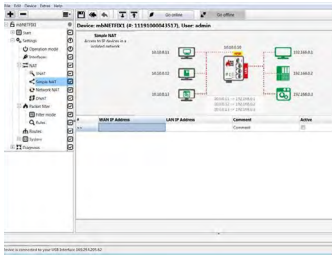
COMPACT INDUSTRIAL FIREWALL

RED LION™
a spectris company

EXCELLENCE. REDEFINED.

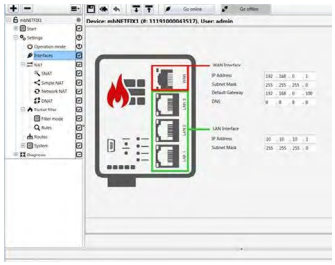
COMPACT INDUSTRIAL
FIREWALL RA10C

AUTOMATION USER'S WORKFLOW



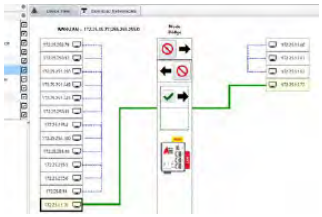
- Prepare projects and upload them to the device
- Go online and make changes on the runtime version
- Export projects and share with other users

GRAPHICAL USER INTERFACE



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

LEARNING MODE



- Visualize actively communicating devices
- Chose general traffic policies
- Select which connections need to be preserved

PROVIDERS OF OT-CYBERSECURITY

Industrial network convergence brings many benefits to the automation applications in-regards to data flow, process integration, and device accessibility, but this connectivity also brings an increased need for cybersecurity within OT-networks.

Electronic equipment, which used to be isolated on a proprietary serial network, is now connected via Ethernet to an ever more interconnected network. The control network is connected to the factory, the factory network is connected to the office and the office network is connected to the internet.

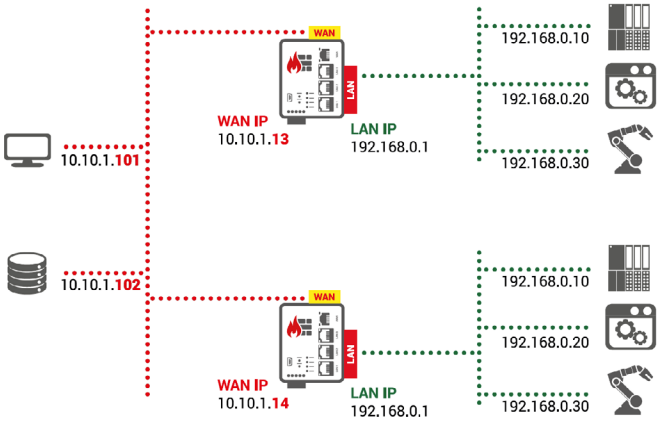
While IT strives to protect an organizations network from external threats, OT networks are left unprotected with an increased threats coming from inside the premises. Threats can include an unfortunate click on an email attachment, an infected USB drive plugged on an operator panel, or even a service technician servicing the machine from an infected PC. These incidents happen, and segmenting the network is the best way to prevent malware from spreading across the whole production floor.

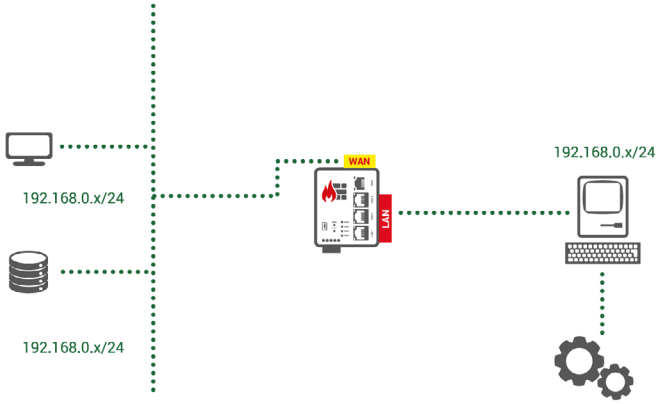
SECURE YOUR INDUSTRIAL NETWORK

AVOID ADDRESS CONFLICTS & ISOLATE INTERNAL NETWORK

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

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





SECURING OLD EQUIPMENT

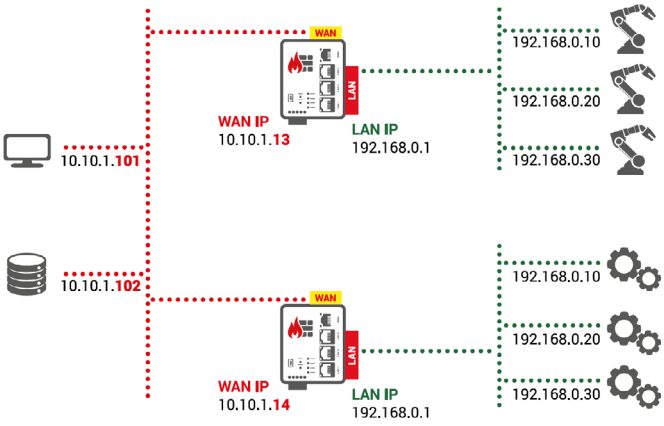
Old machines and production systems are often still very valuable in factory environments. Most of the time, plant operators would prefer to postpone replacement of equipment for as long as possible.

Yet, those systems, running on older or outdated operating systems, are particularly vulnerable to modern cyber-threats. By controlling access to equipment, firewalls can extend the operational lifetime of this legacy equipment.

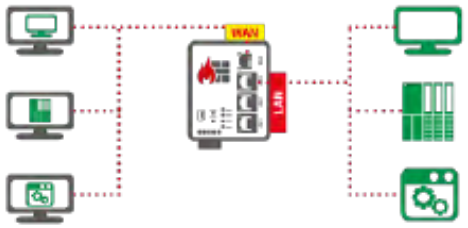
ISOLATE MACHINES OR GROUPS OF MACHINES

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

The firewall can keep this traffic local preserving the OT network for critical communications. Also, by segmenting the network and controlling access rules, the firewall can prevent possible cyber-threats from spreading between production lines.



FULLY FUNCTIONAL
ROUTER AND FIREWALL



SIMPLE NAT

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

SOURCE NAT

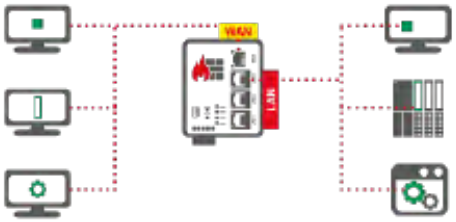
LAN devices reply locally to the router, no gateway needed

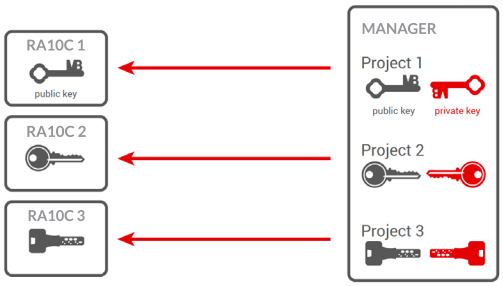
NETWORK NAT

LAN networks remain hidden, WAN devices access it through a virtual LAN network managed by the router

PORT FORWARDING

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





SECURITY BY DESIGN

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

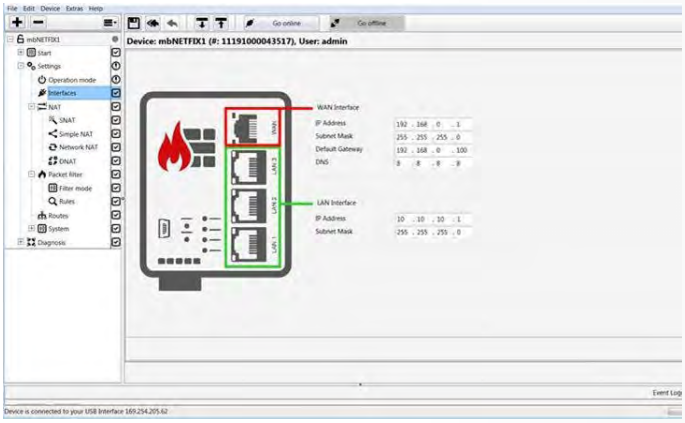
Can only reset the unit and requires visual and physical access to the unit to do so

PRESERVE AUTOMATION USERS' WORKFLOWS

Manage the RA10C, using mbNETFIX Manager, like 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 runtime 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.

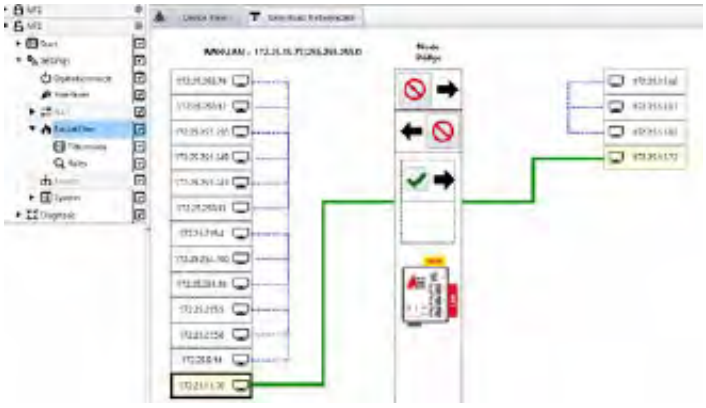
The graphical user interface shows dynamically how the device is configured. Changes are displayed immediately. As a result, you can see how the actual NAT and filtering rules are applied.

LEARNING MODE

Unplug the machine from the network and connect it to one RA10C LAN port. Plug the RA10C 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.



RED LION™
a spectris company

EXCELLENCE. REDEFINED.

www.redlion.net

Red Lion has delivered innovative solutions to global markets since 1972 through communication, monitoring, and control for industrial automation and networking. Its technology enables companies worldwide to gain real-time data visibility that drives productivity.

Red Lion is part of Spectris plc, the productivity-enhancing instrumentation and controls company.

For more information, please visit www.redlion.net.

ADLD0503 093020