Helmholz
COMPATIBLE WITH YOU

WALL IE / WALL IE PLUS / WALL IE Compact
Industrial NAT Gateway and Firewall

Manual

Version 14 | 8.04.2026

Order numbers:

WALL IE	700-860-WAL01 as of firmware V 1.10.232
WALL IE PLUS	700-862-WAL01 as of firmware V 1.00.032
WALL IE Compact	700-862-WAL01 as of firmware V 1.00.032

Link to the latest version of the manual

Helmholz GmbH & Co. KG | Hannberger Weg 2 | 91091 Großenseebach | Germany
Phone +49 9135 7380-0 | Fax +49 9135 7380-110 | info@helmholz.de | www.helmholz.com

Quick start guide & structure of the manual

This manual contains all the information necessary to install, commission, and safely operate WALL IE products.

Section 1 contains **general information and safety instructions**.

To start up the WALL IE, you must connect it correctly to the power supply and the network. For more information, see Section 2, "**Installation**" and Section 3.5 "**Connecting**".

Section 3 explains the applications of the WALL IE, the structure of the devices, and the status indicators of the LEDs.

Once WALL IE is ready for operation, the device must be configured for its intended use via the **web interface**. Section 4 explains how to access the web interface for the first time using the default IP address and describes the structure of the menus.

Sections 5-11 explain how to configure the WALL IE according to different use cases and additional functions.

Section 12 explains how to update the firmware.

Section 13 describes how to reset a WALL IE to its factory settings.

The technical data for the Cabinet Guard is documented in Section 16.

ACHTUNG

Before planning your network or deploying or configuring WALL IE products, please read the **security guidelines** in Section 14!

NOTE

If you have any questions about the possible applications and configuration of the Cabinet Guard, please do not hesitate to contact us.

You can reach our support team at support@helmholz.de.

By phone at **+49 (9135) 7380-110**.

Further information on Helmholz Support can be found at Helmholz Service & Support.

The latest product information can be found at the product website of WALL IE.

Legal Notes

This manual and all content contained therein (texts, illustrations, graphics, photos, tables, and layout) are protected by copyright. The copyright holder is Helmholz GmbH & Co. KG. All rights reserved.

This manual may only be used for the purpose of installing, commissioning, operating, and maintaining the associated product. Reproduction or distribution - even in parts - is permitted for internal use by the installer or operator and only to the extent necessary for this purpose. The documentation may be passed on in case of the resale of the product or for system documentation purposes.

Any other use, in particular publication, making it publicly available (e.g. on the Internet/Intranet), distribution to third parties, editing, translation or commercial exploitation, requires the prior written consent of Helmholz GmbH & Co. KG.

Electronic versions of this manual may be stored and printed for internal purposes. Posting on freely accessible systems, passing on to third parties, or making available for download is not permitted without express written permission.

All rights reserved in the event of patent registration.

All trademarks shown or mentioned in this document are the property of their respective owners or manufacturers. They are shown and mentioned solely for the purpose of explaining the possible uses and settings of the products documented here. No further rights arise from their mention.

STEP, TIA, and Simatic are registered trademarks of Siemens AG.

The information in this manual has been compiled with the utmost care. Nevertheless, errors cannot be completely ruled out. Technical changes, errors, and misprints are reserved. The current version of the manual is authoritative and can be found on the Internet at www.helmholz.de.

We welcome suggestions for improvement and comments.

Further legal information can be found in Chapter 1.

Revision record:

Version	Date	Change
1	5/12/17	First version / Firmware V1.04
2	1/16/19	Conversion to application cases NAT and Bridge; Addenda for firmware V1.08 (DHCP server/client, port ranges) and corrections
3	7/8/19	FW V1.08.100: SNAT added
4	9/27/19	Mistyping in Chap. 1.2 Updated QR-Codes and Hyperlinks
5	1/16/20	Firmware V1.08.200: update screenshots Update of dimensions
6	4/8/20	Added note for Recycling / WEEE Added pictures with higher resolution Firmware V1.08.400: IP ranges for NAT rules
7	1/13/21	New: DNS server (Chap. 11.2) New: ICMP in filter rules (Chap. 6.5, 7.4) New: FTP-Helper in Bridge mode (Chap. 0)
8	18.2.2022	Update of security recommendations Firmware V1.10.100: FTP Helper now also works in NAT mode
9	18.7.2022	Various text corrections
10	26.08.2022	Added WALL IE PLUS
11	27.4.2023	Added WALL IE Compact added “NTP on LAN” and DHCP “static leases”
11b	5.5.23	Typos
12	28.3.24	Port assignment better explained; minor text corrections
13	20.12.24	Text and picture corrections; Supplement "Conduit" use case; Update of Security recommendations
14	8.4.2026	Quick start added, legal notices updated, chapters rearranged, Security Guide rewritten (Chapter 14) Chapter für 802.1X added

Contents

1 General

This operating manual applies only to devices, assemblies, software, and services of Helmholz GmbH & Co. KG.

1.1 Target audience for this manual

This description is only intended for trained personnel qualified in control and automation engineering who are familiar with the applicable national standards. For installation, commissioning, and operation of the components, compliance with the instructions and explanations in this operating manual is essential.

WARNING

Configuration, execution, and operating errors can interfere with the proper operation of the WALL IE and result in personal injury, as well as material or environmental damage. Only suitably qualified personnel may operate the devices!

The specialist personnel is to ensure that the application or the use of the products described fulfills all safety requirements, including all applicable laws, regulations, provisions, and standards.

1.2 Safety instructions

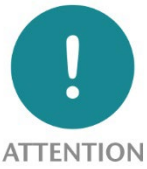
The safety instructions must be observed in order to prevent harm to living creatures, material goods, and the environment. The safety notes indicate possible hazards and provide information about how hazardous situations can be prevented.

1.3 Note symbols and signal words

If the hazard warning is ignored, there is an imminent danger to life and health of people from electrical voltage.

If the hazard warning is ignored, there is a probable danger to life and health of people from electrical voltage.

If the hazard warning is ignored, people can be injured or harmed.



Draws attention to sources of error that can damage equipment or the environment.

Gives an indication for better understanding or preventing errors.

1.4 Intended use

The WALL IE "Industrial Bridge and Firewall" series products (hereinafter referred to as "the device" or "the devices") connects two Ethernet networks.

All components are supplied with a factory hardware and software configuration. The user must carry out the hardware and software configuration for the conditions of use. Modifications to hardware or software configurations that extend beyond the documented options are not permitted and nullify the liability of Helmholz GmbH & Co. KG.

The device must not be used as the sole means of preventing dangerous conditions on machinery and equipment.

The WALL IE Industrial Bridge and Firewall cannot be used for a direct connection to the Internet. Always use a dedicated router with a sufficiently dimensioned Internet firewall for an Internet connection. Observe the security recommendations for project planning, use and maintenance (see chap. 14).

Successful and safe operation of the devices requires proper transport, storage, setup, assembly, installation, commissioning, operation, and maintenance.

The ambient conditions provided in the technical specifications must be adhered to.

The devices have a protection rating of IP 20 and must be installed in an electrical operating room or a control box/cabinet in order to protect it against environmental influences. To prevent unauthorized access, the doors of control boxes/cabinets must be closed and possibly locked during operation.

1.5 Improper use

The consequences of improper use may include personal injury to the user or third parties, data protection breaches, as well as property damage to the control system, the product, or the environment. Use the devices only as intended!

1.6 Liability

The contents of this manual are subject to technical changes resulting from the continuous development of products of Helmholz GmbH & Co. K. In the event that this manual contains technical or clerical errors, we reserve the right to make changes at any time without notice.

No claims for modification of delivered products can be asserted based on the information, illustrations, and descriptions in this documentation. Beyond the instructions contained in the operating manual, the applicable national and international standards and regulations must also be observed in any case.

1.6.1 Disclaimer of liability

Helmholz GmbH & Co. KG is not liable for damages if these were caused by use or application of products that was improper or not as intended.

Helmholz GmbH & Co. KG assumes no liability for any printing errors or other inaccuracies that may appear in the operating manual unless there are serious errors of which Helmholz GmbH & Co. KG was already demonstrably aware.

Beyond the instructions contained in the operating manual, the applicable national and international standards and regulations must also be observed in any case.

Helmholz GmbH & Co. KG is not liable for damage caused by software that is running on the user's equipment that compromises, damages, or infects additional equipment or processes through the remote maintenance connection, and which triggers or permits unwanted data transfer.

1.6.2 Warranty

Report any defects to the manufacturer immediately upon discovery of the defect.

The warranty is not valid in case of:

- Failure to observe these operating instructions
- Use of the device that is not as intended
- Improper work on and with the device
- Operating errors
- Unauthorized modifications to the device

The agreements met upon contract conclusion under "General Terms and Conditions of Helmholz GmbH & Co. KG" apply.

1.7 Open Source

Among other things, our products contain open-source software. This software is subject to the relevant license terms. The relevant license terms, including a copy of the full license text, are downloadable from the product website. They are also provided in our download area of the respective products at www.helmholz.de.

Furthermore, we offer to send the complete corresponding source code of the respective open-source software to you and to any third party as a DVD upon your request for a contribution towards expenses of Euro 10.00. This offer is valid for a period of three years, calculated from the delivery of the product.

2 Installation

2.1 Access restriction

The devices are open operating equipment and must only be installed in electrical equipment rooms, cabinets, or housings.

Access to the electrical equipment rooms, cabinets, or housings must only be possible using a tool or key, and access should only be granted to trained or authorized personnel.

2.2 Mounting and minimum distances

The devices can be mounted on a DIN rail and installed in any position. It is recommended to keep minimum distances when mounting. By keeping the minimum distances

- the modules can be mounted or dismantled without having to dismantle other parts of the system.
- there is enough space to connect all existing connections and contacting possibilities with commercially available accessories.
- There is space for any necessary cable route.

ATTENTION

Installation must be carried out in accordance with VDE 0100/IEC 364 and applicable national standards. The device has protection level IP20. If a higher degree of protection is required, it must be installed in an enclosure or a control cabinet.

2.3 Electrical installation

Observe the regional safety regulations.

2.4 Protection against electrostatic discharges

To prevent damage through electrostatic discharges, the following safety measures are to be followed during assembly and service work:

- Never place components and modules directly on plastic items (such as polystyrene, PE film) or in their vicinity.
- Before starting work, touch the grounded housing to discharge static electricity.
- Only work with discharged tools.
- Do not touch components and assemblies on contacts.

2.5 Overcurrent protection

Overcurrent protection isn't necessary as the device transports no load current. The power supply of the device electronics is to be secured externally with a fuse of maximum 1 A (slow-blowing).

2.6 EMC protection

To ensure electromagnetic compatibility (EMC) in your control cabinets in electrically harsh environments, the known rules of EMC-compliant configuration are to be observed in the design and construction.

ATTENTION

When setting up the system and laying the necessary cables, observe all standards, regulations, and rules regarding shielding. Errors in shielding can lead to malfunctions or even system failure.

2.7 Operation

Operate the device only in flawless condition. The permissible operating conditions and performance limits must be adhered to.

Retrofits, changes, or modifications to the device are strictly forbidden.

The device is a piece of operating equipment intended for use in industrial plants. During operation, all covers on the unit and the installation must be closed in order to ensure protection against contact.

ATTENTION

When the WALL IE is switched off, connections are interrupted! Before starting any work on the device, make sure that no impermissible interference occurs in connected systems when the connections are interrupted.

2.8 Removal / Recycling / WEEE

Perform a factory reset of the device to delete all security-related data (user data, logging protocols, passwords, certificates) from the device. Before recycling, remove all cables from the connectors.

You can send the device to us for recycling at your own expense or take it to a certified disposal company yourself.

According to Directive 2012/19/EU on waste electrical and electronic equipment (WEEE), they must not be disposed of by municipal waste disposal companies.

The company Helmholz GmbH & Co. KG is registered as a manufacturer with the HELMHOLZ brand and the device type "Small devices of information and telecommunications technology for exclusive use in households other than private households" as well as the following registration data:

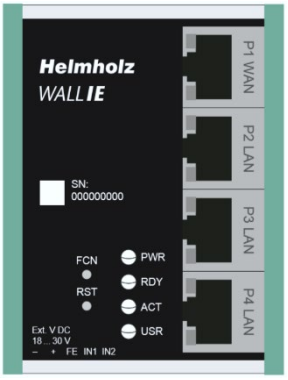
Helmholz GmbH & Co. KG,
Location / Headquarters: 91091 Großenseebach,
Address: Hannberger Weg 2,
Name of authorized representative: Carsten Bokholt,

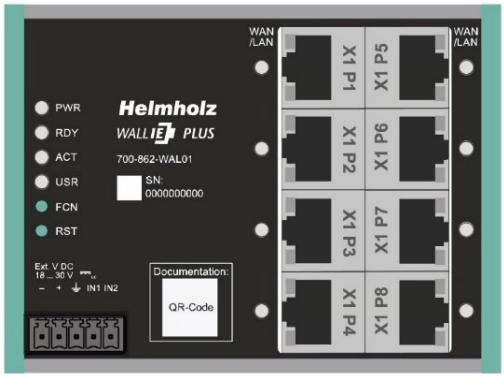
Registration number: **DE 44315750**

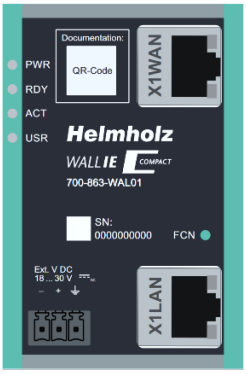
3 Overview

The products of the WALL IE "Industrial NAT Gateway and Firewall" series easily integrate machine networks into the higher-level company or production network by means of network segmentation, packet and MAC address filtering.

Currently, the product series consists of the following variants: **WALL IE (700-860-WAL01)**, **WALL IE PLUS (700-862-WAL01)** and **WALL IE Compact (700-863-WAL01)**.
Unless otherwise noted, this manual describes features that are supported equally by all devices.







The **NAT operating mode** serves the forwarding of the data traffic between 2 subnets. It enables the address-translation via NAT and uses packet filters for the limitation of access to the automation network located behind.

In the **Bridge operating mode**, the WALL IE acts as a network bridge in an IPv4 subnetwork. In contrast to normal switches, packet filtering is possible in this operating mode. This means that the restriction of access to individual areas of your network can be achieved without having to use different networks for this purpose.

Features of WALL IE:

- NAT (Basic NAT, SNAT, NAPT and port forwarding) for network segmentation
- Bridge functionality for securing network areas within the same subnet
- Access restriction through packet filters: IPv4 addresses, protocol (TCP/UDP), ports
- MAC address filtering with black and whitelisting
- DHCP server (LAN), DHCP client (WAN)
- Quick and easy configuration thanks to responsive web interface
- Static routes to other networks
- Reporting of events to a Syslog server
- Export/import of configuration
- Industry-compatible design for installation on DIN rails
- 4x RJ45 interfaces 100 Mbps, 1x WAN + 3 x LAN *(WALL IE, 700-860-WAL01)*
- 8x RJ45 interfaces 100/1000Mbps, WAN/LAN freely adjustable *(WALL IE PLUS, 700-862-WAL01)*
- 2x RJ45 interfaces 100/1000Mbps, 1x WAN + 1x LAN *(WALL IE Compact, 700-863-WAL01)*

3.1 Use cases

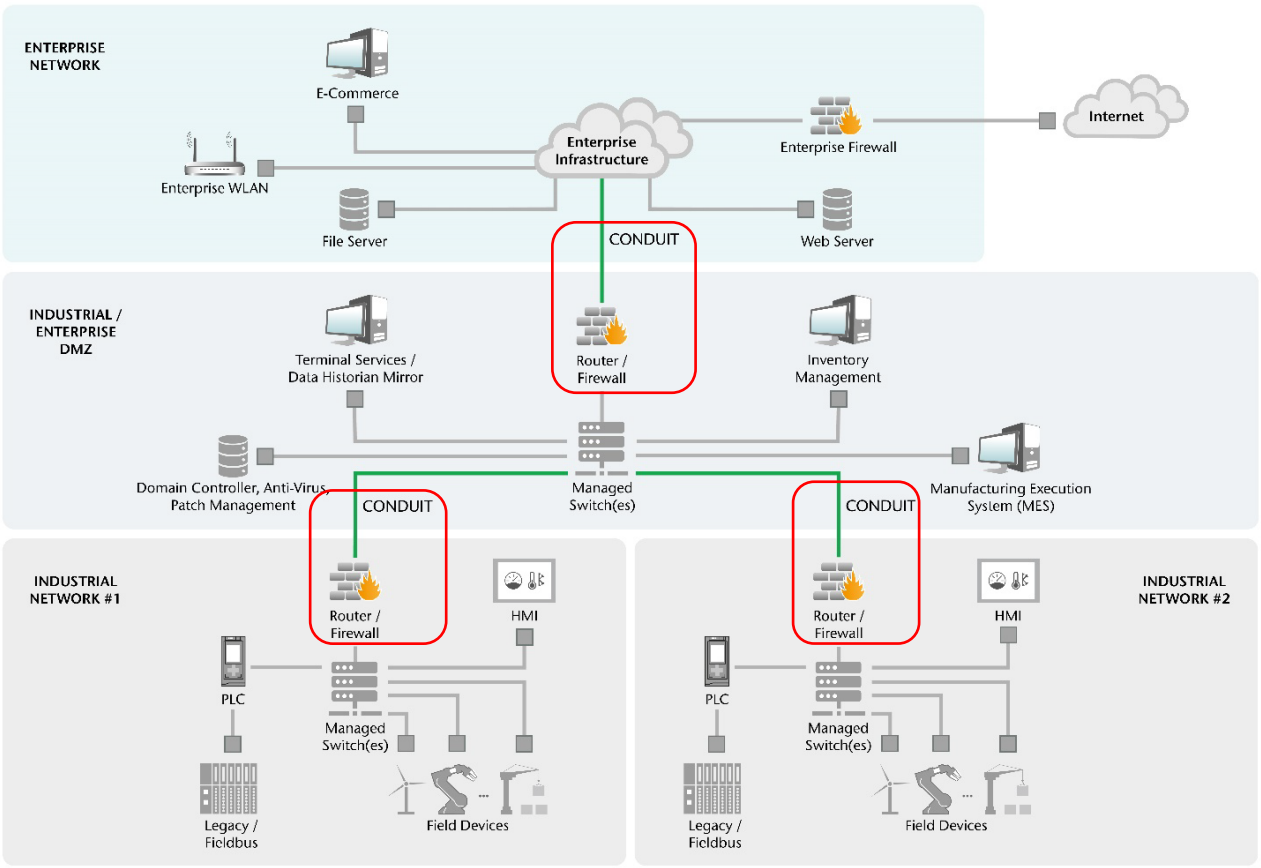
The products in the WALL IE series can be used as a firewall in the context of cyber security or, more practically, as a NAT gateway for managing the machine's IP addresses.

Cybersecurity is a critical issue - not only for corporate IT, but also increasingly for operational technology (OT). OT was originally a rather isolated environment in which PLCs, networks and control components were interconnected for a specific task. The term "security" primarily referred to safe operation, rather than cyber threats. Today, however, OT networks are often connected to IT systems or the cloud via Ethernet or WiFi.

With the convergence of IT and OT, factory automation and industrial applications must be prepared for current and future cybersecurity threats. Although IT incidents occur more frequently, OT incidents are usually much more destructive and can endanger life and limb as well as entire companies. The technical gap between IT and OT systems makes it difficult to simply adopt established IT security mechanisms.

In the context of cybersecurity, the structure of the network plays a decisive role in a production plant. Just as the lord of a castle wants his castle to be secured by walls and gates, the plant operator should divide his network into different areas that are self-contained and have secure passages.

What IT may have previously established through measures such as VLANs in managed switches in the factory network should now be implemented via protection components at the boundaries of the various network areas. Such network transitions - also known as "conduits" - ensure the connection of zones of trust. The conduit only allows the necessary communication between the networks.



Standard series such as IEC 62443 for industrial communication or the new Machinery Directive regulation 2023/1230 describe precisely these applications and suggest the structure of the network with conduits accordingly.

Dividing a network into zones and inserting conduits (zone transitions) is usually also possible with existing systems or machines and does not change the functionality of the system. This means that a decisive factor for system security can be incorporated without having to plan the machine or system from scratch.

The products in the WALL IE series can be used and configured as conduits in these applications.

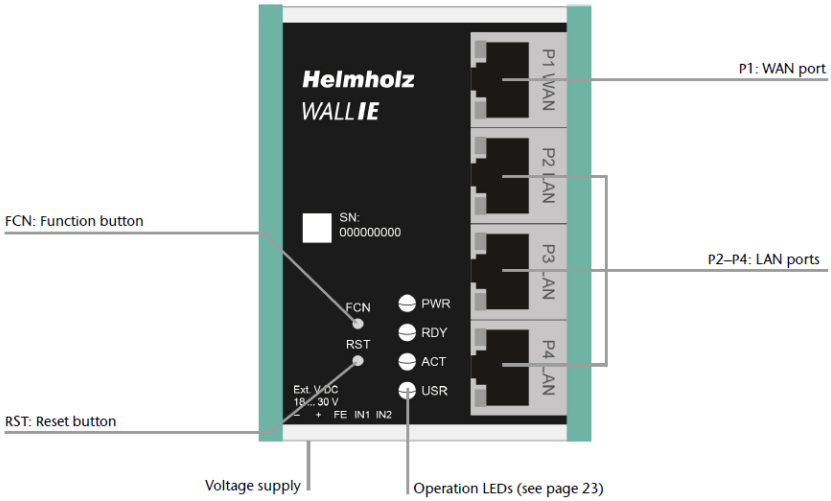
The use of a WALL IE therefore enables you to increase the security of your system, as required by current and future regulations and directives.

ATTENTION

Before planning your network or deploying or configuring WALL IE products, please read the **security guideline** in section 14.

3.2 WALL IE (700-860-WAL01)

The WALL IE has a 100 Mbps WAN port (P1) and three 100 Mbps LAN ports (P2-P4, switched).

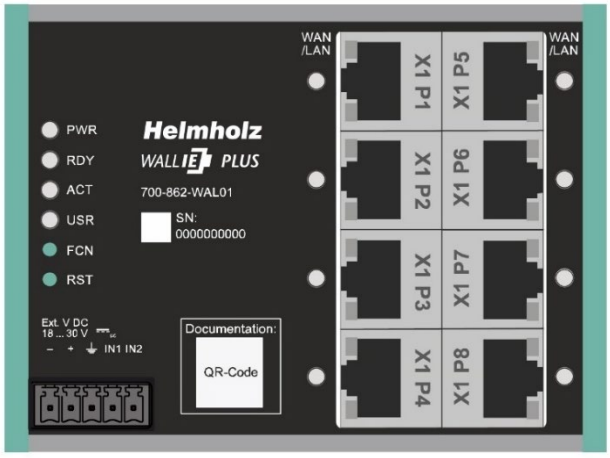


A reset to factory settings can be initiated with the function button (FCN) (see ch. 12). The reset button (RST) initiates a restart of the WALL IE.

3.3 WALL IE PLUS (700-862-WAL01)

The WALL IE PLUS has 8 switched ports with 100/1000Mbit (X1 P1- X1 P8). The ports can be assigned as desired in the configuration of the WALL IE PLUS for WAN or LAN (see ch. 4.3). A LED on each port indicates the assignment. On delivery, port P1 is set for the WAN network and ports P2 to P8 for the LAN network.

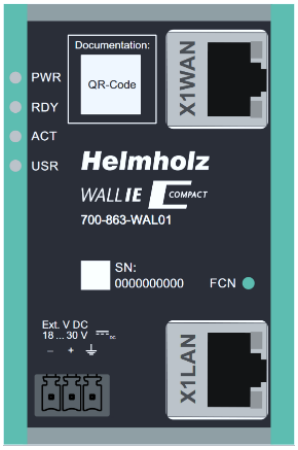
A reset to factory settings can be initiated with the function button (FCN) (see ch. 12). The reset button (RST) initiates a restart of the WALL IE PLUS.



3.4 WALL IE Compact (700-863-WAL01)

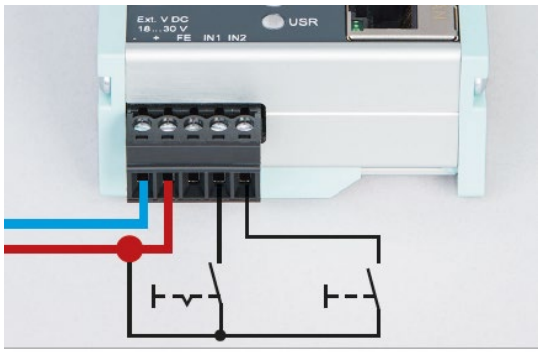
The WALL IE compact has the smallest design of the WALL IE series and provides 2 ports with 100/1000Mbit (X1 WAN - X1 LAN).

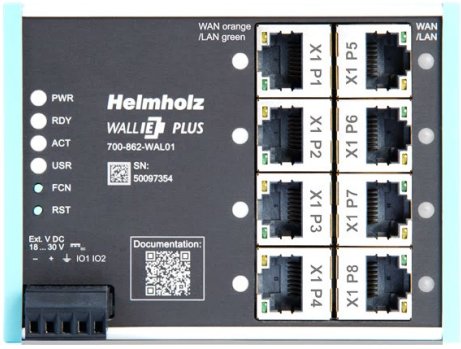
A reset to factory settings can be initiated with the function button (FCN) (see ch. 12).

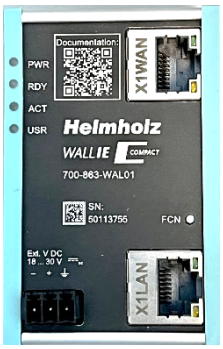


3.5 Connecting the WALL IE

The WALL IE must be supplied with 24 V DC at the wide range input 18-30 V DC via the provided connector. Connection FE is for the functional ground. The WALL IE is designed exclusively for operation with safety extra-low voltage (SELV/PELV).







The RJ45 socket "P1 WAN" of the WALL IE (700-860-WAL01) is used to connect the external network. The RJ45 sockets "P2 LAN-P4 LAN" are switched and are used to connect the internal network.

The RJ45 sockets "X1 P1" to "X1 P8" of the WALL IE PLUS (700-862-WAL01) can be assigned to the network WAN or LAN as desired. In the factory setting, port P1 is set for WAN and ports P2-P8 for LAN. The LEDs next to the port indicate the assignment, orange for WAN and green for LAN. Chapter 4.3 explains how to configure the ports for LAN or WAN.

The WALL IE Compact (700-863-WAL01) has a socket "X1 WAN" at the top for the external network and a socket "X1 LAN" at the bottom for the internal network.

The inputs IN1 and IN2 of the WALL IE and WALL IE PLUS have no function in the current firmware version. The WALL IE Compact has no inputs.

NOTE

The housing of the WALL IE is not grounded. Please connect the functional earth connection (FE) of the WALL IE properly to the reference potential.

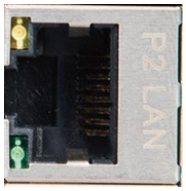
NOTE

The device may only be operated with power supplies that meet the specifications of EN 62368-1 for power sources of limited capacity. Otherwise, the device must be operated in an enclosure that meets the requirements of a fire protection enclosure according to EN 62368-1.

3.6 LEDs status information

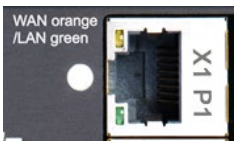
3.6.1 WALL IE (700-860-WAL01)

PWR	Off	No power supply or device defective
	On	Device is correctly supplied with voltage
RDY	On	Device is ready to operate
ACT	Flashing light or on	Permitted data transfer between WAN and LAN
USR	Flashing light	Reset to factory setting activated
RJ45 LEDs	Green (Link)	Connected
	Orange (Act)	Data transfer at the port



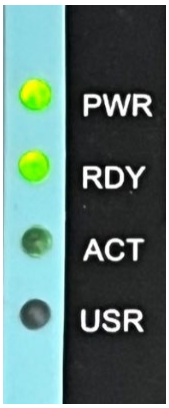
3.6.2 WALL IE PLUS (700-862-WAL01)

PWR	Off	No power supply or device defective
	On	Device is correctly supplied with voltage
RDY	On	Device is ready to operate
ACT	Flashing or on	Permitted data transfer between WAN and LAN
USR	Flashing	Reset to factory setting activated
LEDs at RJ45 Ports	Orange	Port is assigned to the WAN network
	Green	Port is assigned to the LAN network
RJ45 LEDs	Green (Link) flashing	Connected with 100 Mbps
	Green (Link) on	Connected with 1000 Mbps
	Orange (Act)	Data transfer at the port



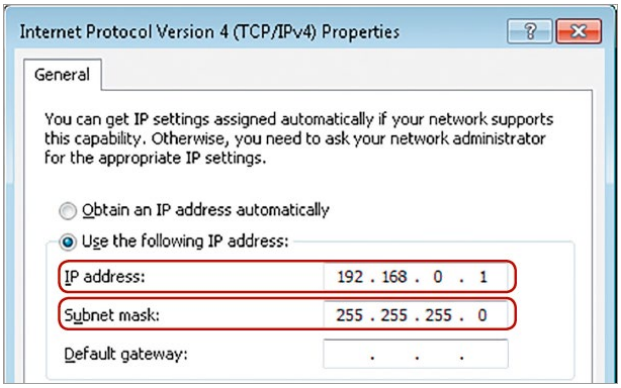
3.6.3 WALL IE Compact (700-863-WAL01)

PWR	Off	No power supply or device defective
	On	Device is correctly supplied with voltage
RDY	On	Device is ready to operate
ACT	Flashing or on	Permitted data transfer between WAN and LAN
USR	Flashing	Reset to factory setting activated
RJ45 LEDs	Green (Link) flashing	Connected with 100 Mbps
	Green (Link) on	Connected with 1000 Mbps
	Orange (Act)	Data transfer at the port



4 Initial access to the web interface

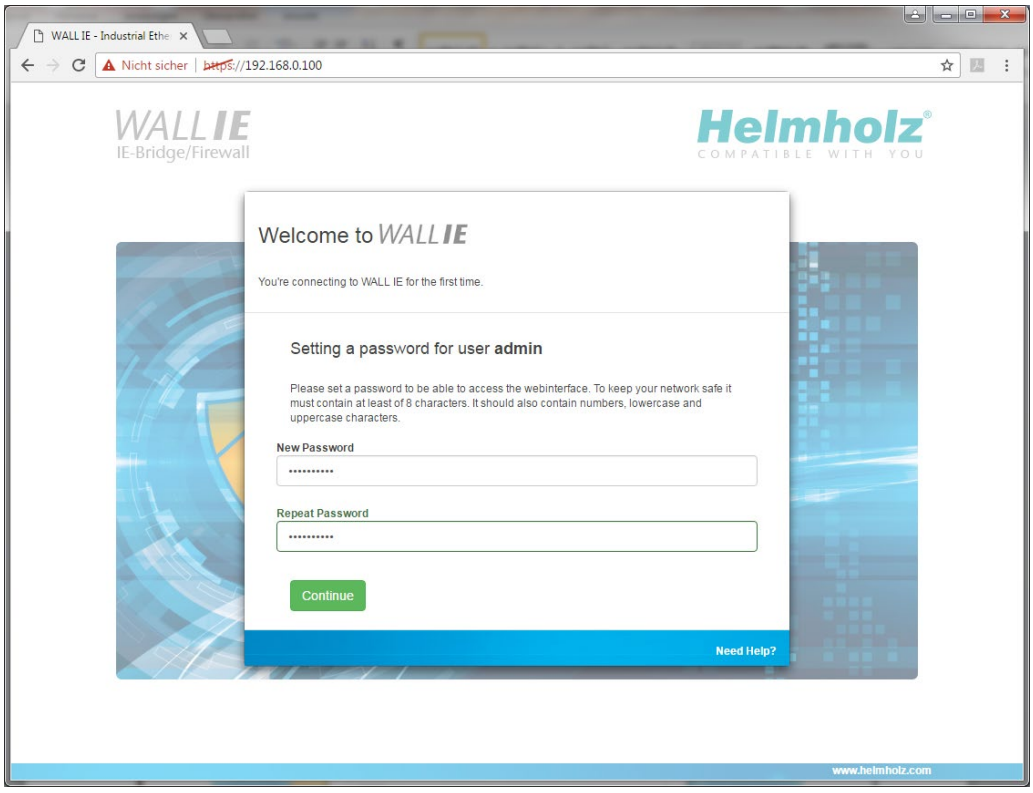
The WALL IE is delivered ex works with the IP address 192.168.0.100 and the subnet mask 255.255.255.0 on the LAN side. The web interface of the WALL IE (700-860-WAL01) can be accessed via the LAN ports P2 - P4. With the WALL IE PLUS (700-862-WAL01), access is possible via the ports P2 - P8 or via all ports whose LED lights up green in the delivery state. With WALL IE Compact (700-863-WAL01) use the LAN-Port.



First, the IP address of your network card must be in the same subnet as the WALL IE interface. In the network settings of the network adapter, assign the PC an IP address within the WALL IE's default subnet , e.g. 192.168.0.1 with subnet mask 255.255.255.0.

Now connect a patch cable with the LAN connection of your PC and one of the LAN ports of WALL IE.

The web interface can be reached in the delivery condition by entering URL "**https://192.168.0.100**" in the browser page.



NOTE

For security reasons, the web interface can only be reached through a secured HTTPS connection. An exception rule must be confirmed in the browser once to reach the website. A certificate for the connection backup can be stored in the "Device/HTTPS" menu.

4.1 Initial registration

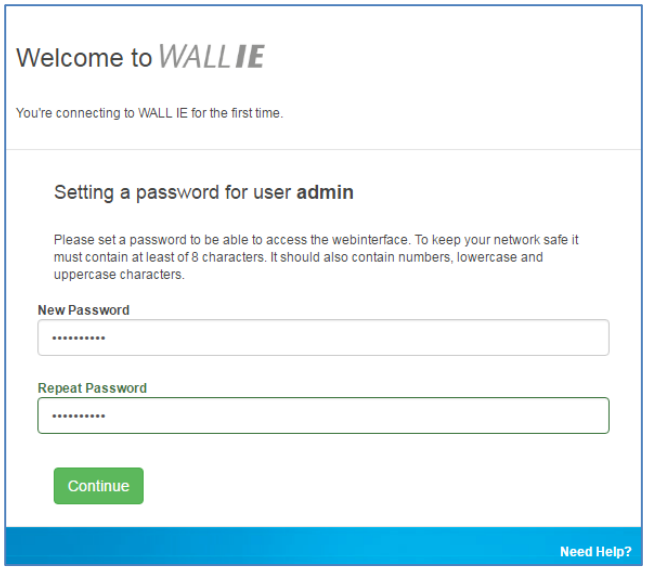
You will be prompted to set a password with the initial registration.

The password must have at least 8 characters and may have a maximum of 128 characters. It may contain special characters and numbers. With the “Continue” button, the password is stored in the device, and you will be forwarded to the “Overview” page of the WALL IE.

The main user is always “admin”.

In addition to the main user “admin”, the “it-user” and “machine-user” can also be used with limited rights.

The users can be activated, and the affiliated passwords set in the “Device/Password” menu.

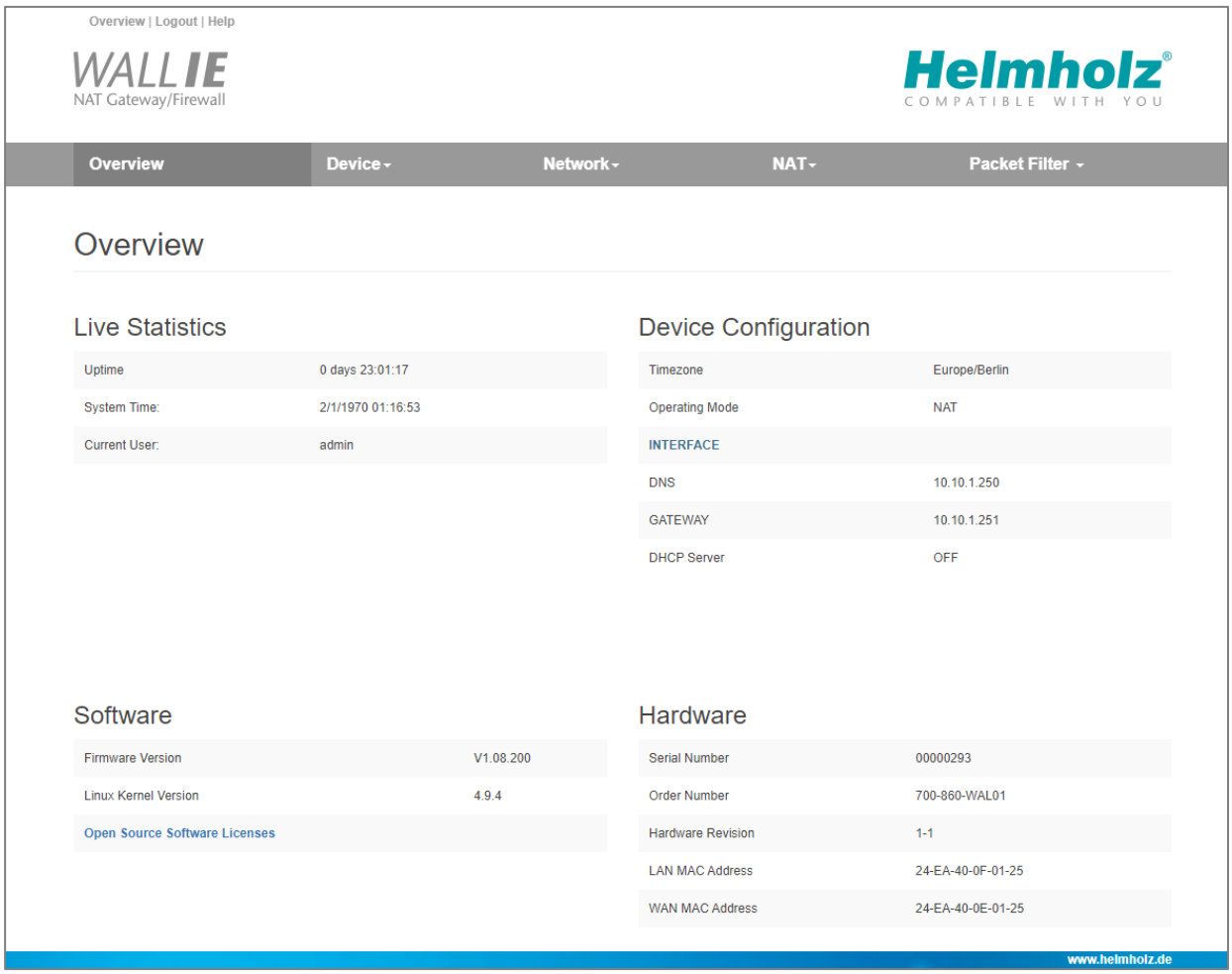


ATTENTION

Please note the password carefully! For security reasons it is not possible to reset the password without setting the device to the factory settings.

4.2 Main view

The “Overview” website of the WALL IE always opens after the login. The “Overview” main view contains an overview of the most important settings and information of the WALL IE.
The topmost line contains the menu with the functions for configuration.

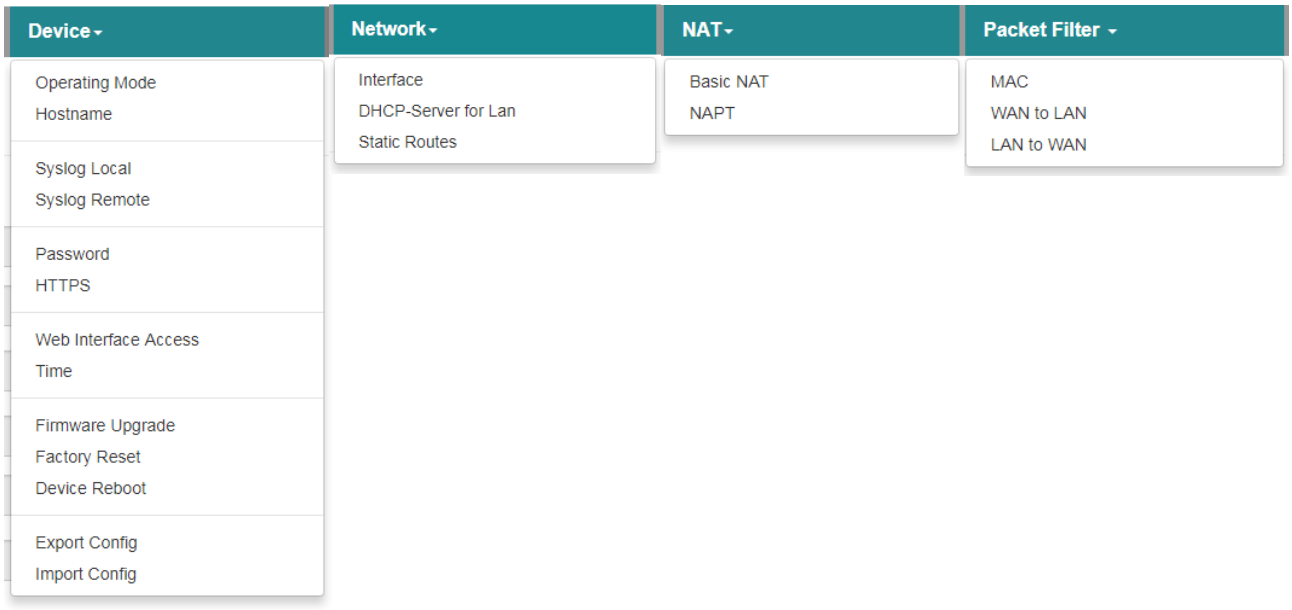


NOTE

Please check at the website of the WALL IE for a newer firmware version.
The firmware update is described in chapter 12.

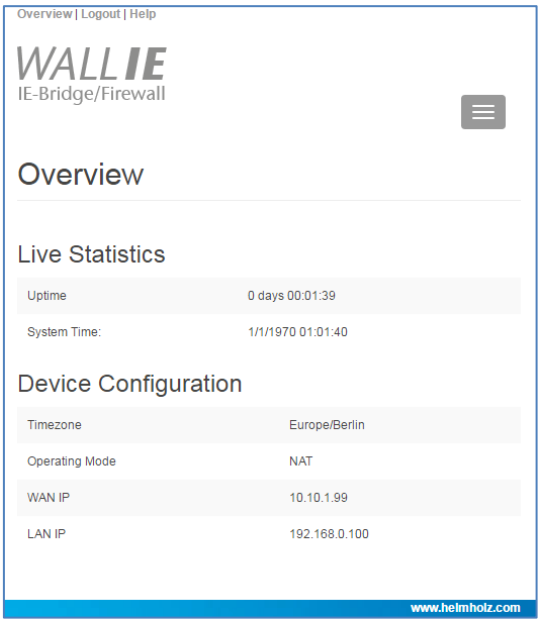
Link to firmware:
https://www.helmholz.de/goto/700-860-WAL01
https://www.helmholz.de/goto/700-862-WAL01
https://www.helmholz.de/goto/700-863-WAL01

4.2.1 Menu overview



4.2.2 Responsive design

The web interface is also suitable for use on tablets and smartphones (“Responsive design”).



NOTE

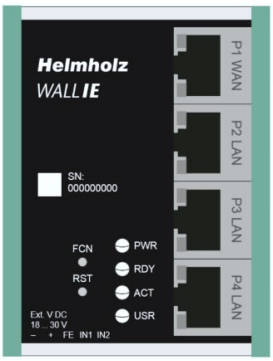
Please note that web access to the WALL IE is equipped with inactivity monitoring for security reasons. When the website isn’t used for several minutes, an automatic “log out” takes place.

4.3 Port assignment WAN/LAN

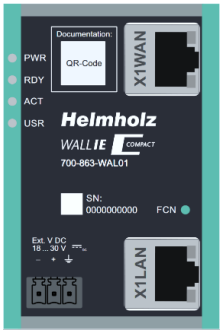
4.3.1 Port assignment for WALL IE and WALL IE Compact

The assignment of the ports for WAN (company network) and LAN (machine network) are fixed for the WALL IE (700-860-WAL01).

The top port "P1 WAN" connects the WALL IE with the company network, the 3 other ports ("P2-P4 LAN") connect the WALL IE with the machine network. The ports P2 to P4 are switched internally.

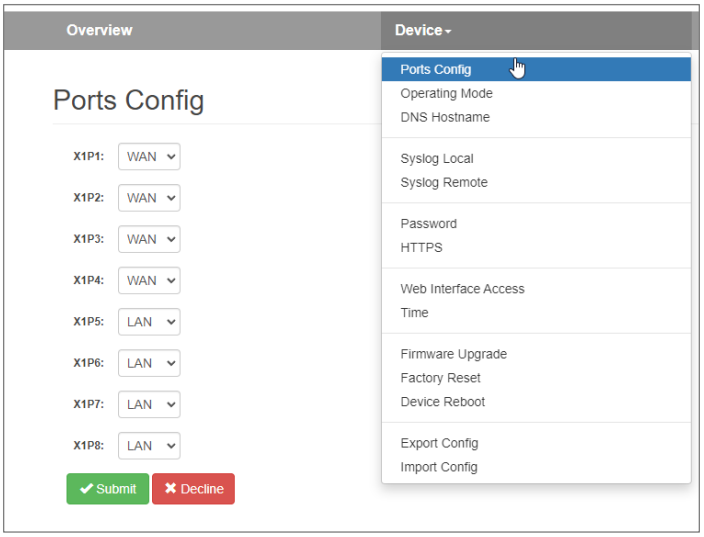


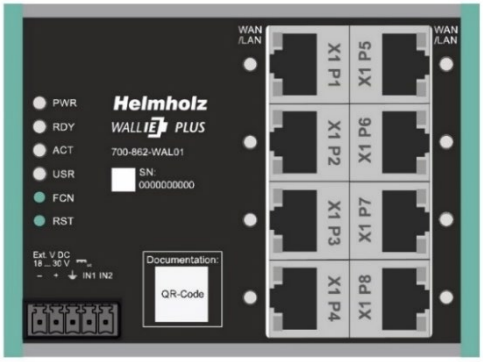
The WALL IE Compact (700-863-WAL01) has a WAN port ("X1WAN") for the company network and a LAN port the company network and a LAN port ("X1LAN") for the machine network.



4.3.2 Port assignment for WALL IE PLUS

The WALL IE PLUS (700-862-WAL01) has 8 ports (X1 P1 - X1 P8) which can be freely set for WAN (company network) or LAN (machine network).





The configuration of the ports can be set in the "Device/ Ports Config" menu. All ports for LAN and all ports for WAN are switched to each other internally.

ACHTUNG

At least one port of the WALL IE PLUS must be assigned to LAN and at least one port to WAN

5 Choosing the operating mode

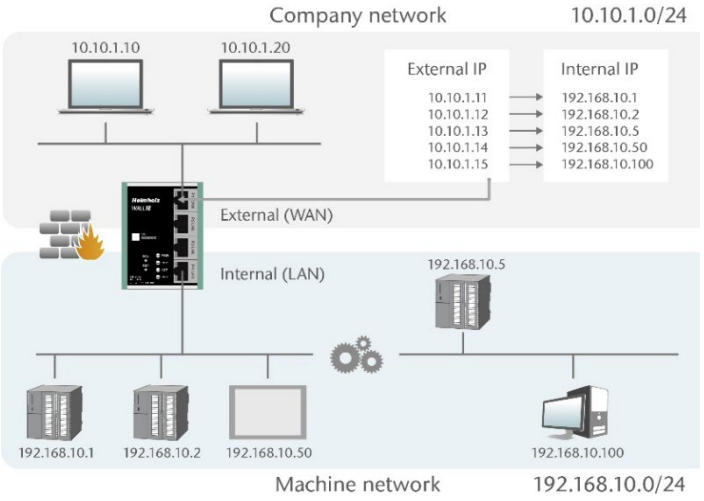
The following explanations apply equally to WALL IE (700-860-WAL01) and WALL IE PLUS (700-862-WAL01). For better readability, only "WALL IE" will be referred to in the following.

Depending upon the application case for the WALL IE, the operating mode must first be defined. WALL IE supports two principal operating modes: NAT and Bridge

5.1 The NAT operating mode

When an automation cell with preset IP addresses is to be incorporated into a company network in different IP subnet, the IP addresses of the machine must normally all be set again.

When using Network Address Translation (NAT), WALL IE offers the possibility to leave the IP addresses of the machine as they are, but to enable communication with the machine network with own IP addresses from the company network.



In the NAT operating mode, WALL IE forwards the data transfer between various IPv4 networks (Layer 3) and exchanges the IP addresses with the help of NAT.

Packet filters and MAC address filters can also be configured to control the data transfer.

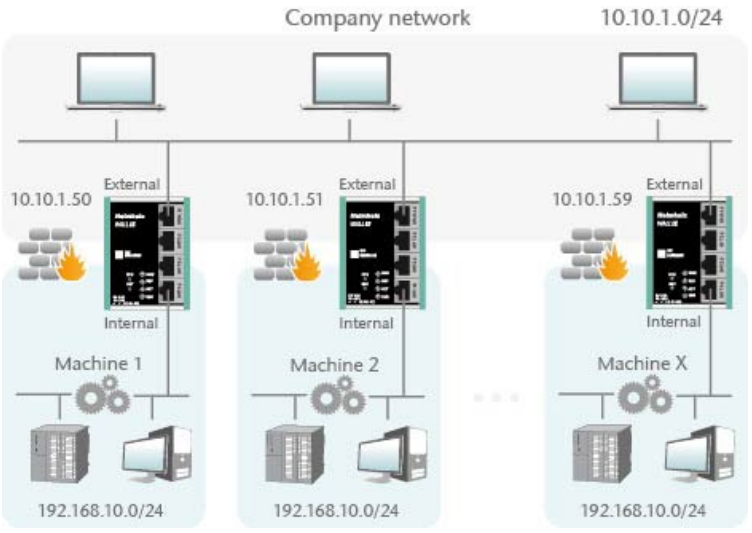
Broadcast traffic is generally filtered at the WALL IE, which means that the time behavior of the machine network is not impaired by the company network.

Basic NAT, also known as “1:1 NAT” or “Static NAT”, is the translation of individual IP addresses or of complete IP address ranges.

With the help of **port forwarding**, it is possible as an alternative to configure those packets to be forwarded to a particular TCP/UDP port of the WALL IE to a certain participant in the machine network (LAN).

The NAT operating mode thus also allows the integration of several automation cells that use an identical IP address range into the same Company network.

Each automation cell can be assigned different free IP addresses from the company network.



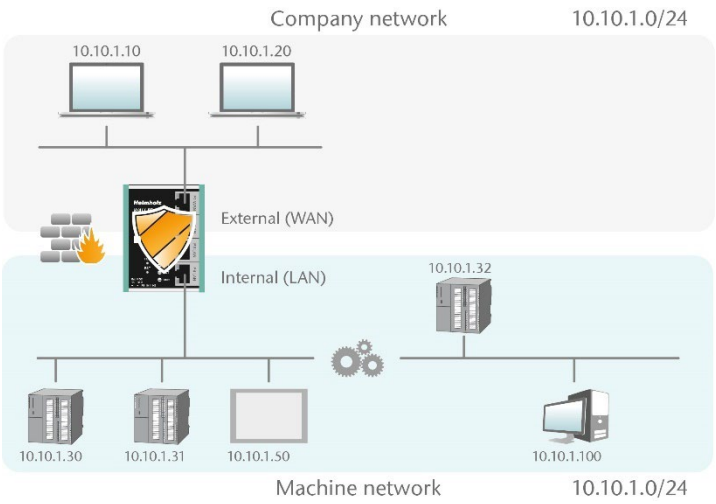
If “NAT” is your planned application case, please continue reading in chapter 6.

5.2 The Bridge operating mode

In the Bridge operating mode, WALL IE behaves like a layer 2 switch between the machine network (automation cell) and the company network. The IP addresses in the company network are in this case in the same IP address space (subnet) as the addresses in the machine network.

Access between the two network areas can be limited or secured with packet filters and MAC address filters.

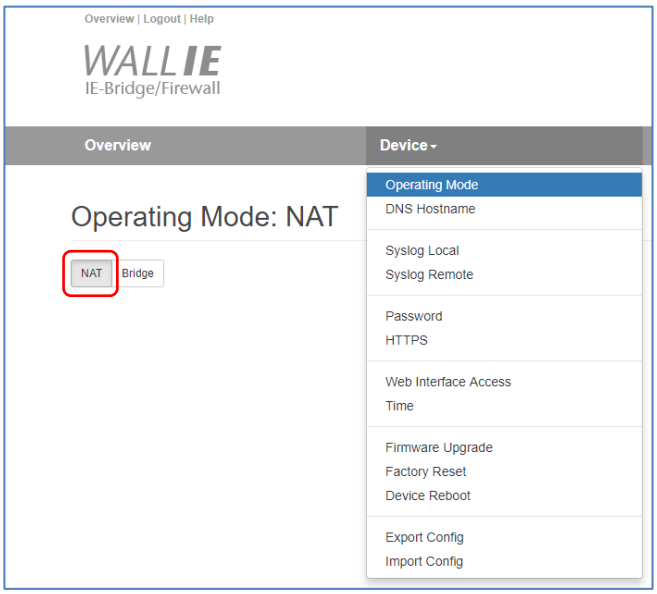
This allows the separation of part of the company network without using different network addresses.



If “bridge” is your planned application case, please continue reading in chapter 7.

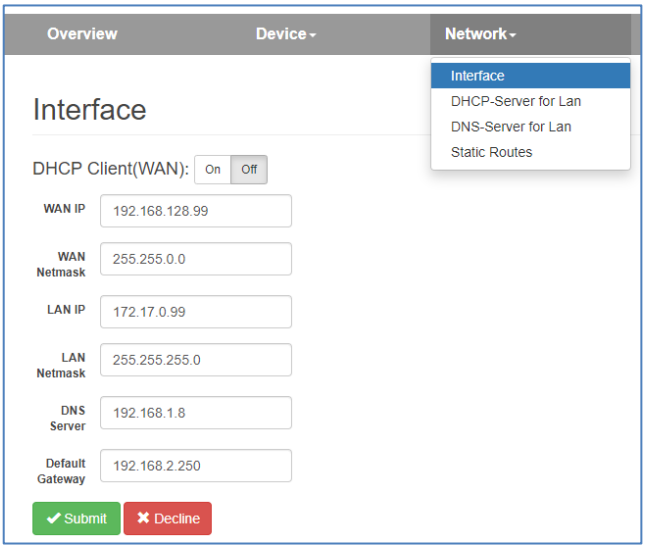
6 Application “NAT”

To activate the NAT operating mode, select the “Operating Mode” menu point in the “Device” menu and set this to “NAT”.



6.1 Adjustment of the IP addresses in the NAT operating mode

Click on the “Network” menu and select the sub-menu “Interface”. The IP addresses of the WALL IE in the WAN and in the LAN (“WAN IP”/”LAN IP”), as well as the affiliated subnet masks (“WAN netmask”/”LAN netmask”) can be defined here.



A DNS server and a default gateway can also be defined. This is necessary when devices from the LAN should reach the Internet via the WALL IE. If these are not indicated (“0.0.0.0”), then communication of devices in the LAN with the Internet is prevented.

Optionally, the WAN-IP settings, the DNS server, and the default gateway can also be obtained using DHCP.

The entry is saved with the “Submit” button and the IP settings are then activated immediately. The current entry is rejected without acceptance with “Decline”.

It is necessary to indicate a DNS server for the SNTP service (see ch. 11.9).

ATTENTION

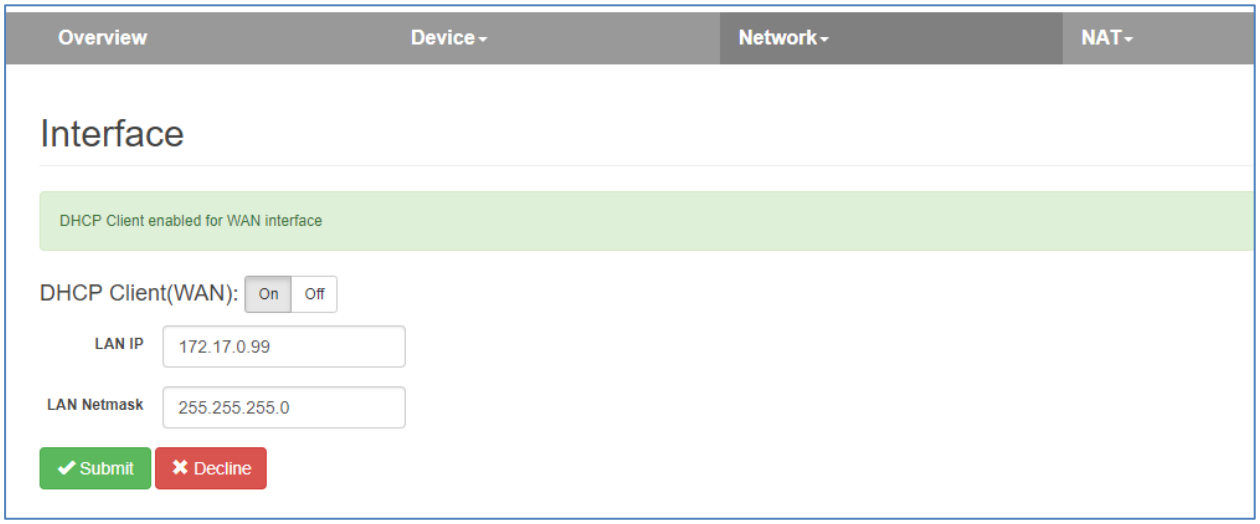
When you change the LAN IP address, you may need to reopen the website of the WALL IE in the browser using the new IP address and log in again.

NOTE

The WALL IE has only one active configuration. Changes to the configuration are always immediately activated. A restart of the WALL IE is not required when changing the configuration.

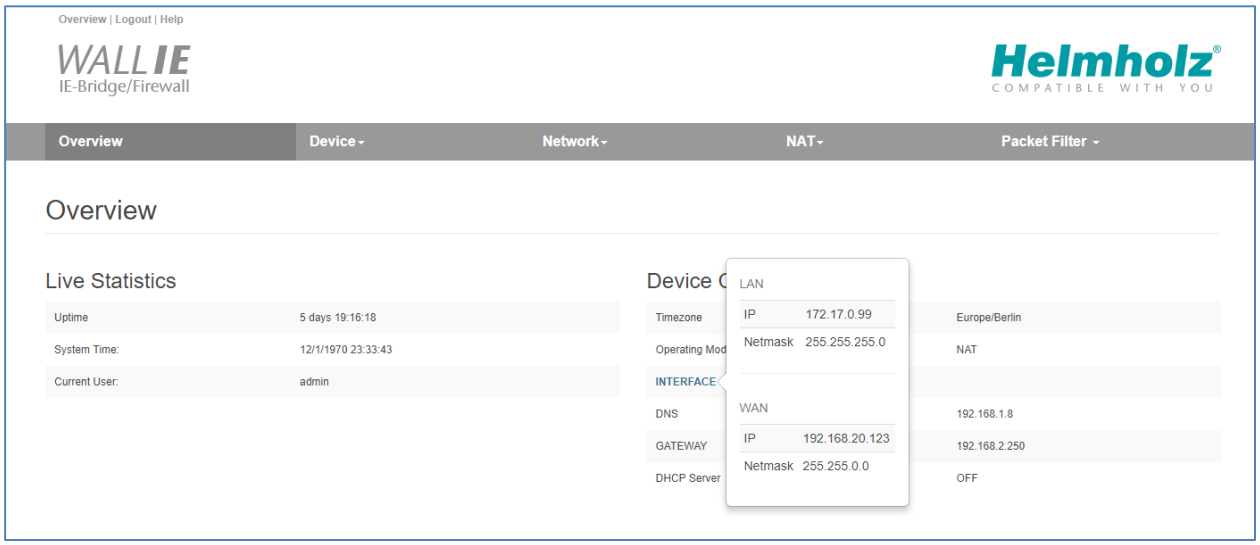
6.2 Activate DHCP client at the WAN interface

As an alternative to entering the IP address, a DHCP client can also be activated for the WAN interface.



The use of the DHCP client presumes that a DHCP server is active in the WAN network.

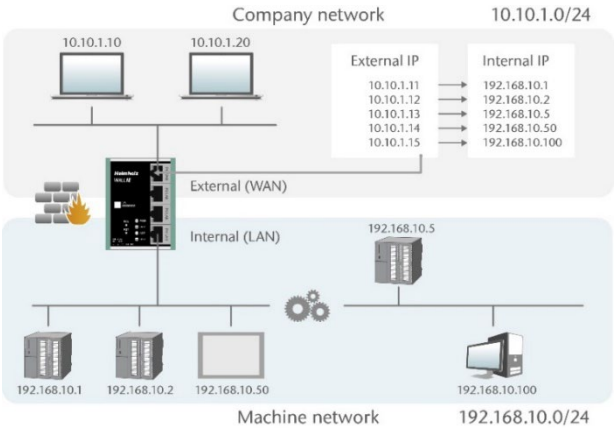
The IP settings acquired from the DHCP client are made visible on the overview page by clicking on “INTERFACE”.

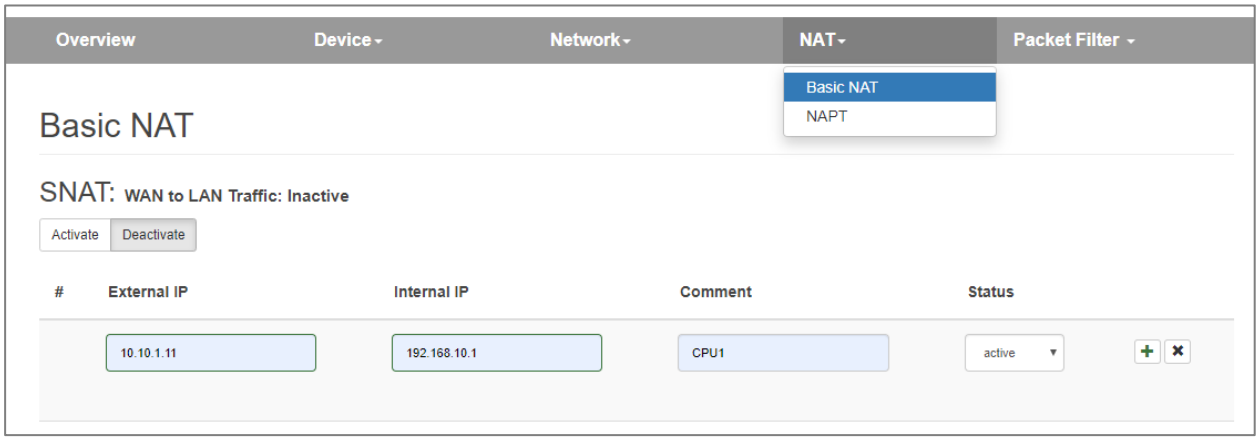


6.3 Setting up “Basic NAT” rules

In order to use Basic NAT functionalities, WALL IE operating mode must be set to "NAT"

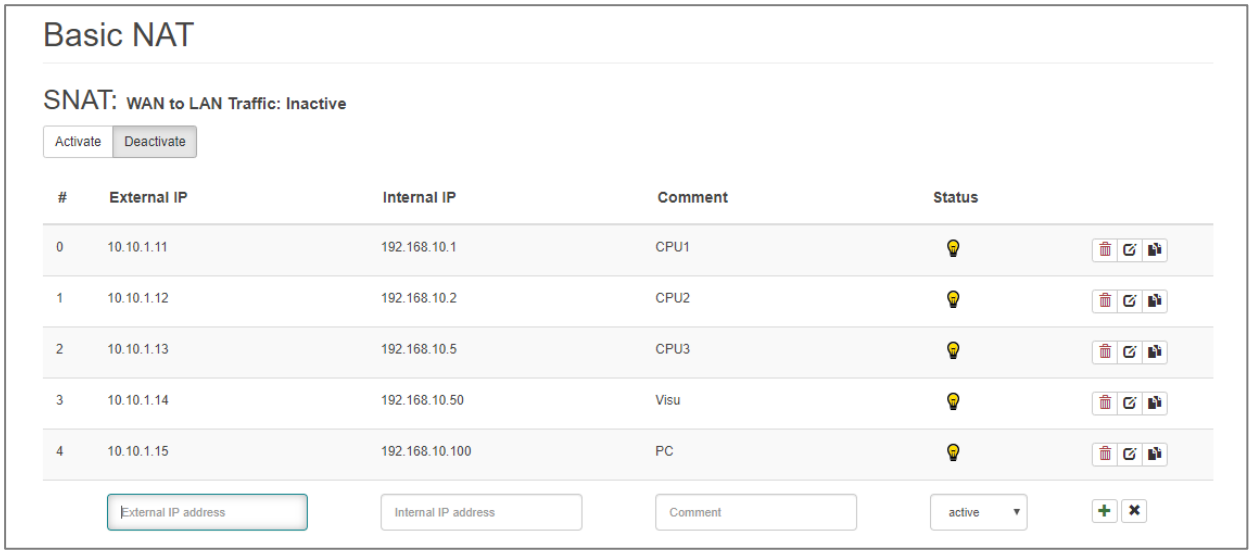
Then select the “NAT” menu and the sub-menu “Basic NAT”. Enter the first rule and save it with the ⊕ button.





"External IP" is a free IP address from the WAN IP address range; it is also referred to as a virtual address. This must not have been assigned to any other Ethernet device (in the WAN)!
The "Internal IP" is the address of the physical device in the LAN network (the target device). WALL IE assigns the IP address according to the NAT rule and routes the packets from the WAN to the LAN and vice versa.

Each entry is confirmed with the message “Rule added successfully”.

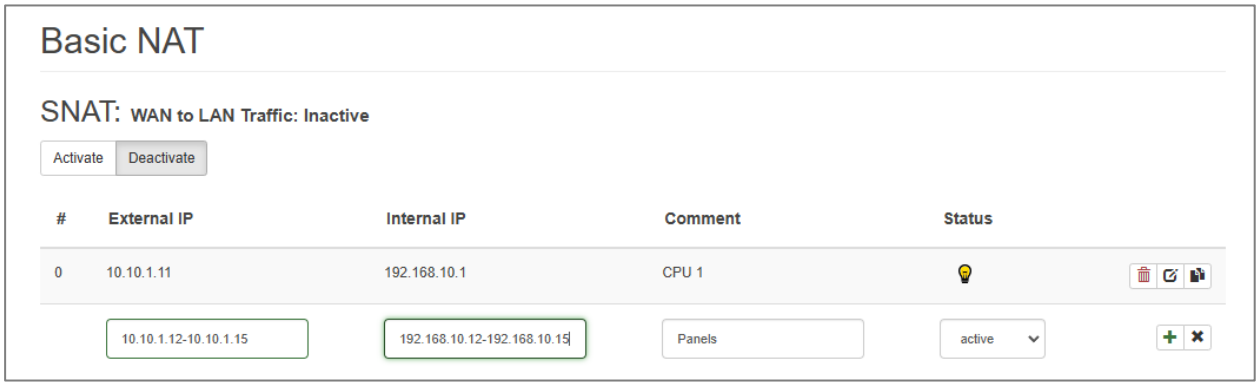


Status: 💡 = Rule is active, a click on the lamp symbol changes the rule status to inactive

💡 = Rule is inactive, a click on the lamp symbol changes the rule status to active

Possible actions: 🗑 delete a rule ✎ edit a rule 📋 copy a rule

You can also define ranges of IP addresses in a NAT rule if the devices have consecutive IP addresses.



Using a subnet mask suffix to describe an entire IP range is also possible here: "10.10.2.1/24" defines a NAT rule for all IP addresses from 10.10.2.0 to 10.10.2.255.

ATTENTION

In the case of a “Basic NAT” rule, all ports for “WAN to LAN” data transfer are initially blocked for this rule for security reasons!

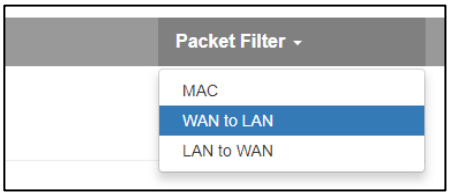
In order to enable access, packet filter rules must be created or the default action for the packet filters be set to “Accept”. See the following chapter.

The “LAN to WAN” data transfer is initially always enabled but can also be limited by packet filters rules or the default action.

NOTE

A maximum of 128 basic NAT entries can be defined.

6.4 Packet filter “WAN to LAN”



The packet filters enable the limitation of access between the company network (WAN) and the machine network (LAN).

For example, it can be configured that only certain participants from the company network may exchange data with defined participants from the automation cell (machine network).

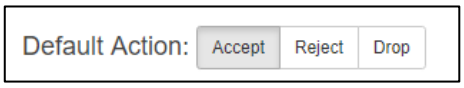
The following filter criteria on layers 3 and 4 are available: IPv4 addresses, protocol (TCP/UDP/ICMP), and ports.

The packet filters are always also available in the direction “LAN to WAN”, see chapter 6.6.

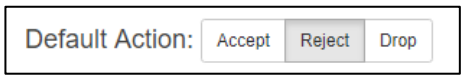
Click on the “Packet Filter” menu and select the sub-menu “WAN to LAN”.

With the “Default Option” you can set whether all frames are generally allowed (“Accept”) and only special packets are filtered (“Blacklisting”), or whether all frames are generally prohibited (“Reject” / “Drop”) and only those frames are allowed to pass through that correspond with the filter rules (“Whitelisting”).

If you initially do not wish to filter, set the default action to “Accept”.

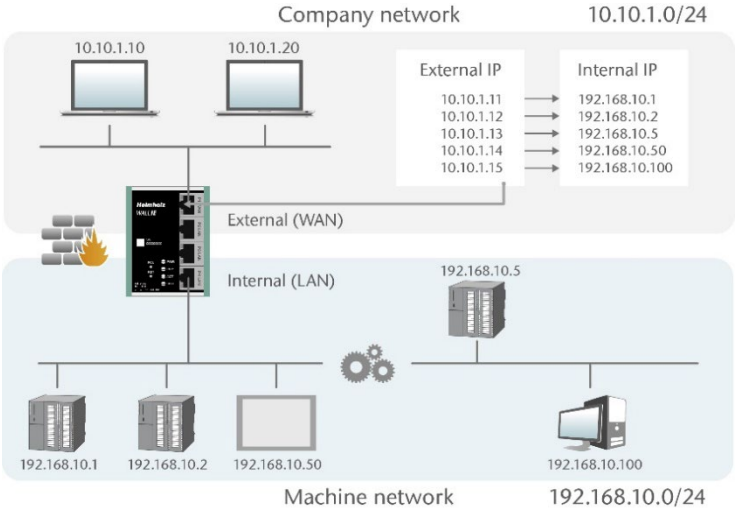


In order to limit access to the machine network to certain participants in the WAN, set the default action to “Reject” or “Drop”. In the case of prohibited frames from the WAN, “Reject” sends an error message in response, while “Drop” rejects the frame without sending an error message.

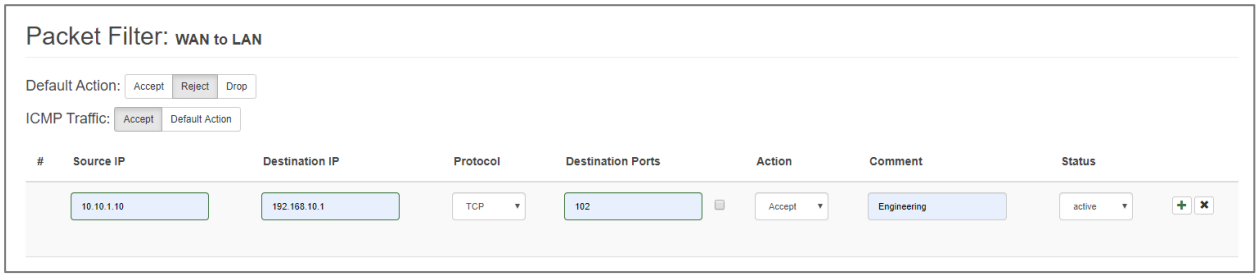


Example: A PC in the company network (WAN) has the IP address 10.10.1.10 (e.g. a visualization).

This PC should be able to access the CPU with the IP address 192.168.10.1 within the LAN over the TCP port 102.



Now enter the following rule and save it with the + button.



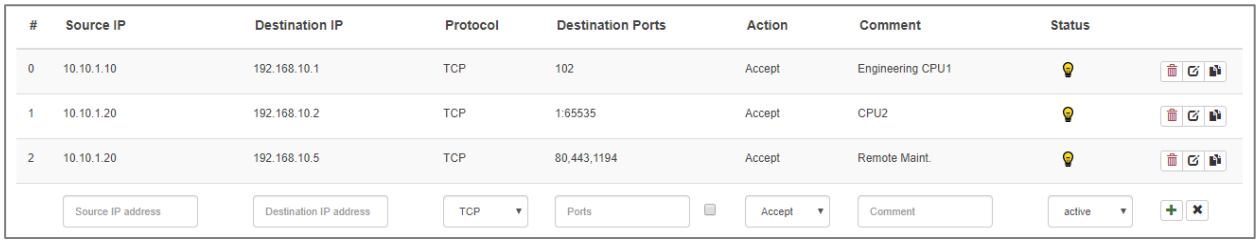
Source IP indicates the IP address of the active device in the company network (WAN).

Destination IP specifies the addressed device in the machine network (LAN).

The filter rules can be defined for one protocol type with **protocol** “TCP”, “UPD” or “ICMP”.

Destination Ports indicates the ports to which the filter rules apply.

If a filter rule applies to several or even all ports, this can be simply defined in the “Destination Ports” field. A list of ports is indicated separated by commas: “80,443,1194”. A port range can be indicated with a colon: “4000:5000” or “1:65535” for all ports. Combinations of this are also possible: “80,443,4000:5000”.



#	Source IP	Destination IP	Protocol	Destination Ports	Action	Comment	Status
0	10.10.1.10	192.168.10.1	TCP	102	Accept	Engineering CPU1	
1	10.10.1.20	192.168.10.2	TCP	1:65535	Accept	CPU2	
2	10.10.1.20	192.168.10.5	TCP	80,443,1194	Accept	Remote Maint.	
	Source IP address	Destination IP address	TCP	Ports	Accept	Comment	active

It is also possible to configure the access of several participants with one another. An IP range can be defined with a dash: “10.10.1.10-10.10.1.20“. A list of IP addresses is indicated with commas: “10.10.1.10,10.10.1.15,10.10.1.20”. IP subnet can be also declared using CIDR notation: "10.10.1.10/24".

3	10.10.1.1-10.10.1.9	192.168.10.1	TCP	1:65535	Accept	Many	
4	10.10.1.200	192.168.10.1-192.168.10.200	TCP	1:65535	Accept	All LAN access	

In the event that the source IP address is not known at commissioning, e.g. if WALL IE obtains its WAN IP via DHCP, then the entire WAN IP range can also be enabled. For this you have to enter "0.0.0.0-255.255.255.255" at **Source IP**.

Action defines whether this rule allows communication (“Accept”), rejects with error message (“Reject”), or simply drops packets (“Drop”). The appropriate method here should always be chosen in interaction with the “Default Action”. If the Default Action is, for example, “Reject” or “Drop”, the filter rules should all be set to “Accept” (Whitelisting). If the Default Action is “Accept”, a block can be defined in the filter rules with “Reject” or “Drop” for certain devices (Blacklisting).

Status: = Rule is active; a click on the lamp symbol changes the rule status to inactive

= Rule is inactive: A click on the lamp symbol changes the rule status to active

Possible actions: delete a rule edit a rule copy a rule

NOTE

A maximum of 128 packet filter rules per direction (“WAN to LAN” and “LAN to WAN”) can be defined.

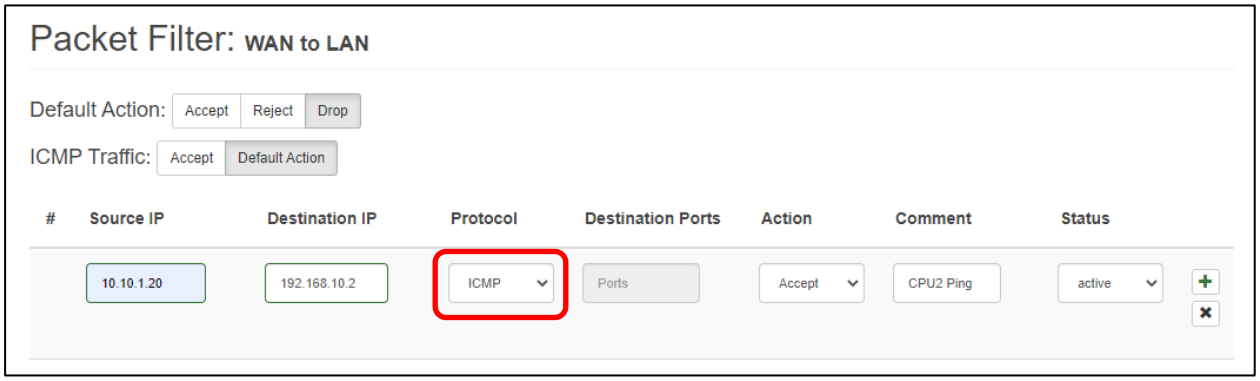
6.5 ICMP Traffic “WAN to LAN”

The Internet Control Message Protocol (ICMP) serves the purpose of exchanging information and error messages via the Internet protocol IPv4. Typical ICMP frames include “ping” or “traceroute”.

With "ICMP Traffic" option, you can generally "Accept" ICMP packets or apply "Default Action".

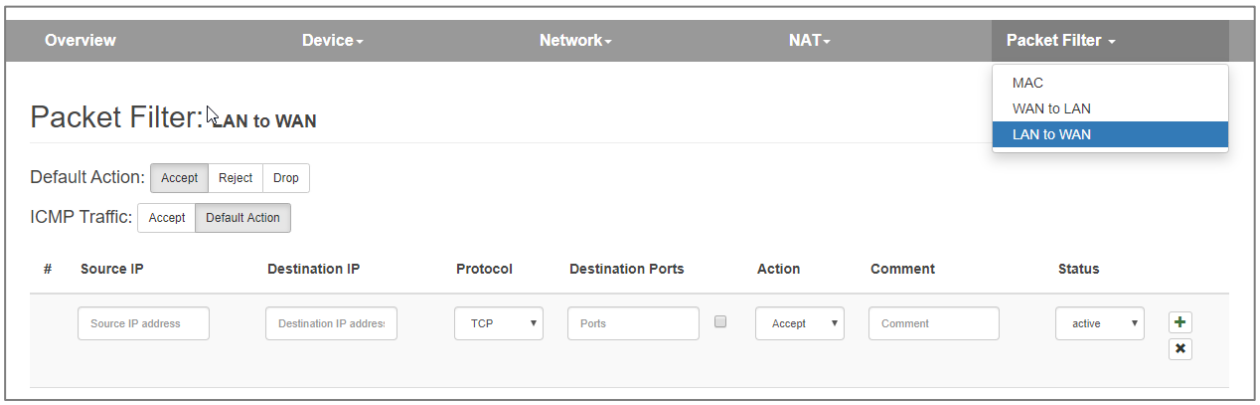
If, for example, the packet filters “Default Action” are set to “Reject” or “Drop”, and ICMP Traffic to “Default Action”, then no ICMP frames are rejected or dropped.

In addition to general ICMP rule, you can further customize your firewall by adding specific packet filter rules for ICMP protocol.



6.6 Packet filter “LAN to WAN”

By default data traffic is permitted for devices from the machine network (LAN) to the company network (WAN) without limitations (“Default Action”: “Accept”).



General rule can be changed by setting the "Default Action" to "Reject" or "Drop". In addition to general rule, filtering can be further customized using specific packet filter rules."

The entry of the filter rules corresponds to the "WAN to LAN" packet filter rules, the source IP now indicates the IP address of the active device in machine network (LAN), and destination address represents the device in company network (WAN).

NOTE

A maximum of 128 packet filter rules per direction (“WAN to LAN” and “LAN to WAN”) can be defined.

6.7 ICMP Traffic “LAN to WAN”

With "ICMP Traffic" option, you can generally "Accept" ICMP packets or apply "Default Action".

If, for example, the packet filters “Default Action” are set to “Reject” or “Drop”, and ICMP Traffic to “Default Action”, then ICMP frames are rejected or dropped.

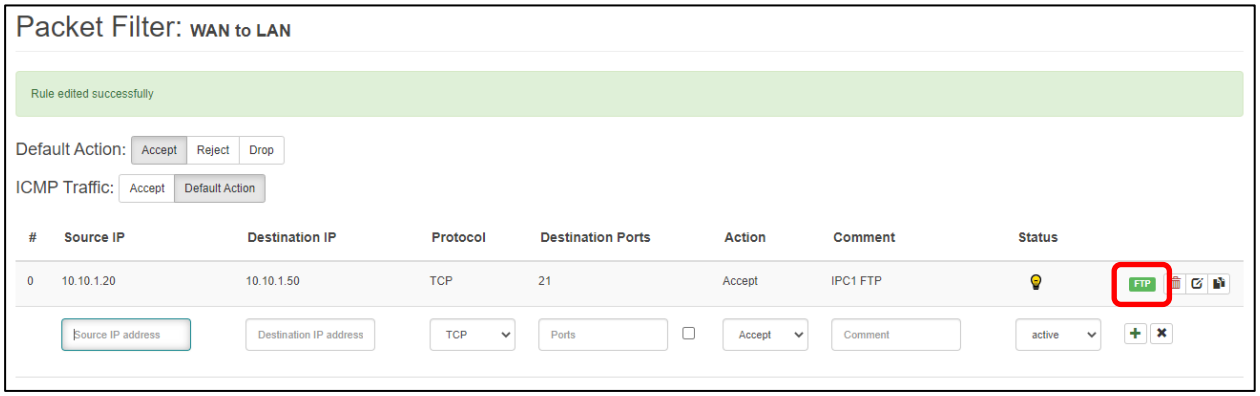
In addition to general ICMP rule, you can further customize your firewall by adding specific packet filter rules for ICMP protocol.

6.8 FTP helper for active FTP

A special application in connection with filter rules at port level is the active FTP protocol. In contrast to the passive FTP protocol, where port 20 is fixed for data exchange, with active FTP the port used for data exchange is randomly determined after the connection is established via port 21. Since it is not possible to know the port when setting up WALL IE, it is not possible to set a fixed port rule. In order not to have to always open all ports for this use case WALL IE supports the function "FTP-Helper".

The FTP helper reads the FTP protocol during FTP connection establishment and releases only the port negotiated there for the time of the FTP connection after connection establishment.

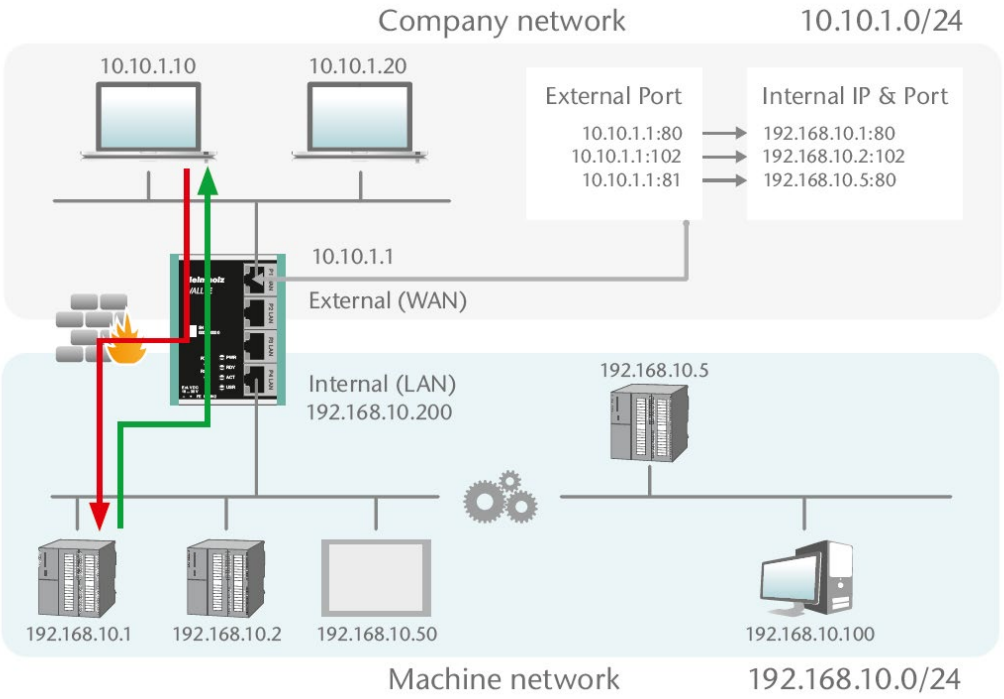
Create a "WAN to LAN" rule for FTP connection establishment and then enable the "FTP Helper" option on the rule for active FTP.



6.9 SNAT

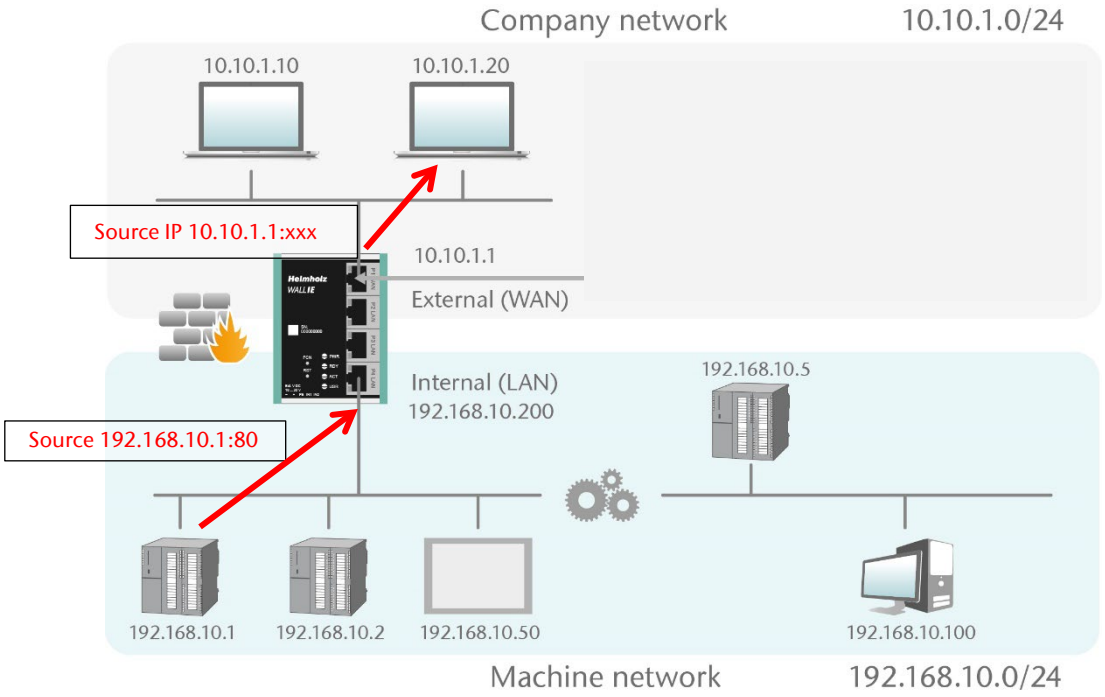
The function “SNAT (Source NAT)” transparently forwards incoming traffic from the WAN side to the LAN network. To all packets, forwarded on LAN side by WALL IE, source IP address is replaced with WALL IE LAN IP address.

Therefore, none of the LAN participants needs the WALL IE LAN-IP as „gateway“. This is a considerable advantage when integrating into existing network structures since the parameters no longer have to be changed here.

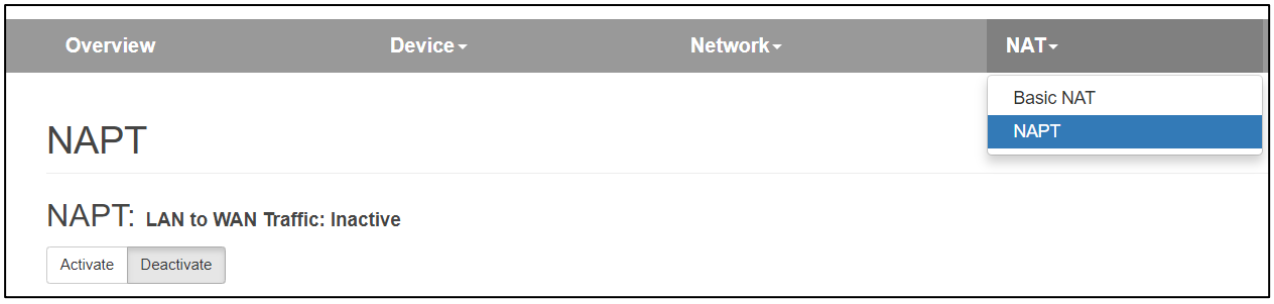


6.10 NAPT

“NAPT for LAN to WAN traffic” replaces the sender addresses of queries from the LAN with the WALL IE WAN IP address.



Enabling the “**NAPT: Active**” option allows devices in the LAN to communicate with devices in the WAN. In this mode, the WALL IE functions as a gateway that manages address translation for outgoing connections and automatically handles the mapping of return traffic.



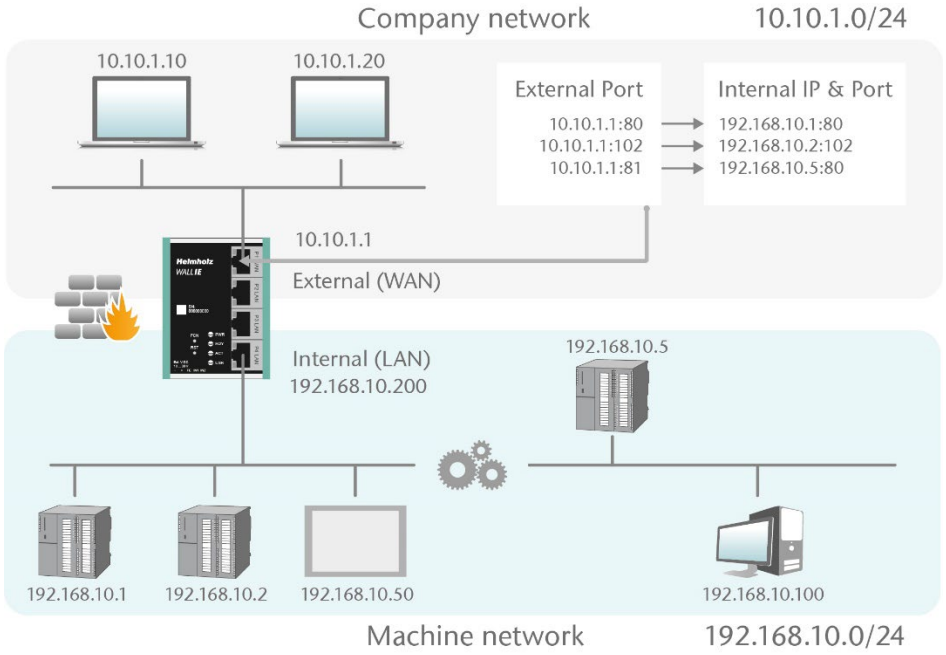
ATTENTION

In order for the communication from LAN to WAN to work when NAPT is activated, the WALL IE LAN IP address must be entered as gateway in all devices on the LAN!

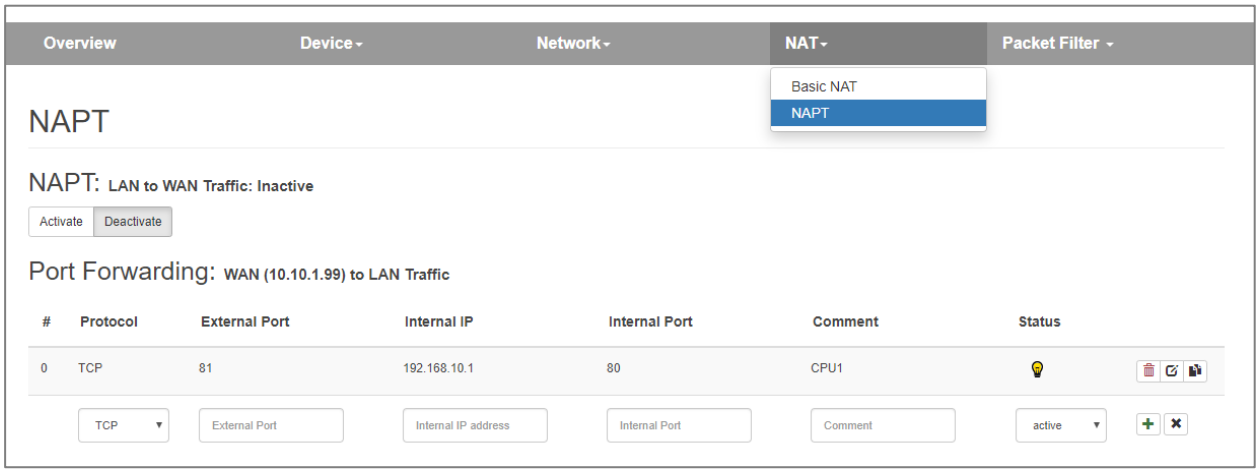
If the **NAPT** option is deactivated, the query packets from the LAN are forwarded from the LAN to the WAN with their original sender IP and sender port.

6.11 Port forwarding

With the help of port forwarding (“Port forwarding for WAN to LAN traffic”), it can be configured that packets at a certain TCP/UDP port of the WALL IE (WAN) can be forwarded to a participant in the LAN (e.g. 10.10.1.1:81 to 192.168.10.5:80).



In the following example, the website (Port 80) of the CPU with the IP 192.168.10.1 via WAN can be reached through access to the WALL IE-own IP address 10.10.1.1 with Port 81.



Protocol: “TCP” or “UDP”

External port: Port number through which the device on LAN side is accessed. On LAN side, device is accessed using internal IP address and internal port number.

Internal IP: IP address of device connected to LAN.

Internal Port: Port used to access device connected to LAN.

Comment: Freely definable comment.

Status: = Rule is active; a click on the lamp symbol changes the rule status to inactive

= Rule is inactive: A click on the lamp symbol changes the rule status to active

Possible actions: delete a rule edit a rule copy a rule

NOTE

"Port forwarding" and "Basic NAT" can be used simultaneously in the NAT operating mode.

ATTENTION

If with the packet filters "WAN to LAN" default action is set to "Reject" or "Drop", the corresponding packet filter rules for access must also be created for each port forwarding entry.

NOTE

It is not possible to use the reserved ports 443 and 80 when WALL IE has activated its own websites on the WAN (Web Interface Access = "WAN and LAN", see chapter 11.8).

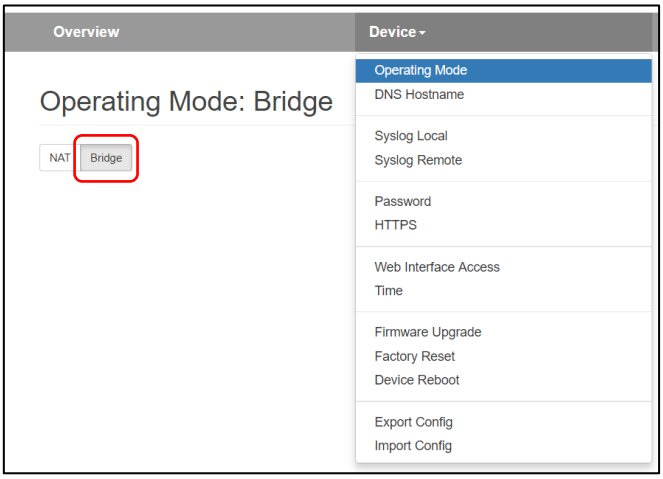
ATTENTION

A maximum of 128 port forwarding entries can be created.

7 Application “Bridge”

7.1 Activate Bridge mode

To activate the Bridge operating mode, select the “Operating Mode” menu point in the “Device” menu and set this to “Bridge”.

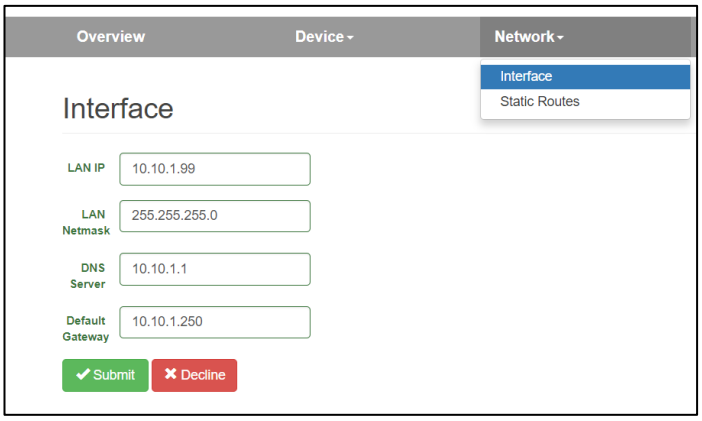


7.2 Adjustment of the IP addresses in the bridge operating mode

Click on the “Network” menu and select the sub-menu “Interface”. The IP addresses of the WALL IE (“LAN IP”) and affiliated subnet mask (“LAN netmask”) can be defined here.

A DNS server and a default gateway can also be defined.

The entry is saved with the “Submit” button and the IP settings are thus activated immediately. The current entry is rejected without acceptance with “Decline”.



ATTENTION

When you change the LAN IP address, you may need to reopen the website of the WALL IE in the browser using the new IP address and log in again.

A DHCP client or a DHCP server are not available in the bridge operating mode.

NOTE

In the bridge operating mode, the defined interface settings are equally valid at the WAN port of the WALL IE.

ATTENTION

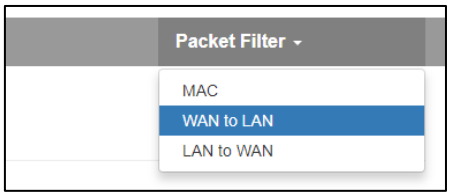
In the bridge mode, all ports are initially blocked for “WAN-to-LAN” data transfer for security reasons!

In order to enable access, packet filter rules must be created or the default action for the packet filters be set to “Accept”. See the following chapter.

The “LAN to WAN” data transfer is initially always released but can also be limited by packet filters or the default action.

7.3 Packet filter “WAN to LAN”

The packet filters enable the limitation of access between the company network (WAN) and the machine network (LAN).



For example, it can be configured that only certain participants from the company network may exchange data with defined participants in the automation cell.

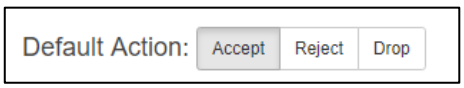
The following filter criteria on layers 3 and 4 are available: IPv4 addresses, protocol (TCP/UDP/ICMP), and ports.

Note: The packet filters are always also available in the direction “LAN to WAN”, see chapter 7.5.

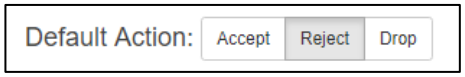
Select the “WAN to LAN” menu point in the “Packet Filter” menu.

With the “Default Option” you can set whether all frames are generally allowed (“Accept”) and only special packets are filtered (“Blacklisting”), or whether all frames are generally prohibited (“Reject” / “Drop”) and only those frames are allowed to pass through that correspond with the filter rules (“Whitelisting”).

If you initially don’t wish to filter, set the default action to “Accept”.

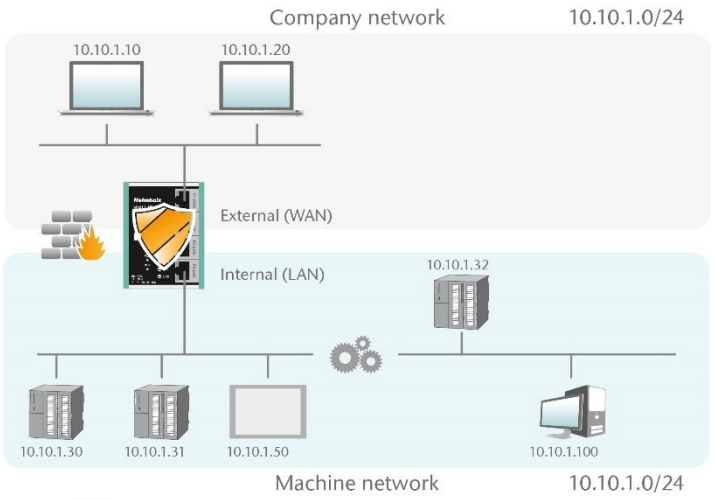


In order to limit access to the machine network to certain participants in the WAN, set the default action to “Reject” or “Drop”. In the case of prohibited frames from the WAN, “Reject” sends an error message in response, while “Drop” rejects the frame without sending an error message.

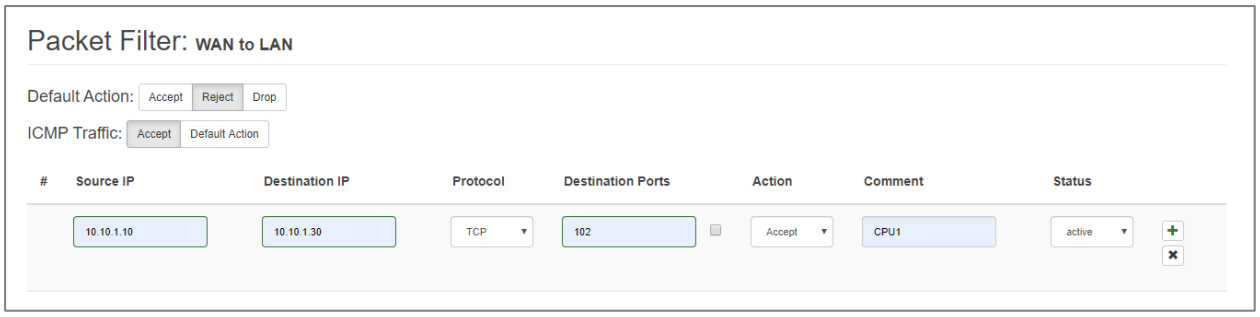


Example: A PC in the company network (WAN) has the IP address 10.10.1.11 (e.g. a visualization).

This PC should be able to access the CPU with the IP address 10.10.1.30 within the LAN over the TCP port 102.



Now enter the following rule and save it with the + button.



Source IP indicates the IP address of the active device in the company network (WAN).

Destination IP the addressed device in the machine network (LAN).

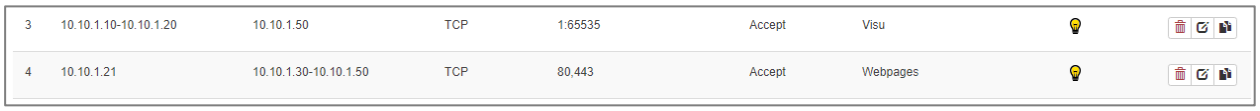
The filter rules can be defined for one protocol type with **protocol** “TCP”, “UPD” or “ICMP”.

Destination Ports indicates the ports to which the filter rules apply.

If a filter rule applies to several or even all ports, this can be simply defined in the “Destination Ports” field. A list of ports is indicated separated by commas: “80,443,1194”. A port range can be indicated with a colon: “4000:5000” or “1:65535” for all ports. Combinations are also possible: “80,443,4000:5000.”

#	Source IP	Destination IP	Protocol	Destination Ports	Action	Comment	Status
0	10.10.1.10	10.10.1.30	TCP	102	Accept	CPU1	
1	10.10.1.20	10.10.1.30	TCP	1:65535	Accept	Engineering	
2	10.10.1.20	10.10.1.31	TCP	80,443,1194	Accept	Remote Maint.	

It is also possible to configure the access of several participants with one another. An IP range can be defined with a dash: “10.10.1.10-10.10.1.20“. A list of IP addresses is indicated with commas: “10.10.1.10,10.10.1.15,10.10.1.20”. IP subnet can be also declared using CIDR notation: "10.10.1.10/24".



3	10.10.1.10-10.10.1.20	10.10.1.50	TCP	1:65535	Accept	Visu	
4	10.10.1.21	10.10.1.30-10.10.1.50	TCP	80,443	Accept	Webpages	

Action defines whether this rule allows communication (“Accept”), rejects with error message (“Reject”), or simply drops packets (“Drop”). The appropriate method here should always be chosen in interaction with the “Default Action”.

If the Default Action is, for example, “Reject” or “Drop”, the filter rules should all be set to “Accept” (Whitelisting). If the Default Action is “Accept”, a block can be defined in the filter rules with “Reject” or “Drop” for certain devices (Blacklisting).

NOTE

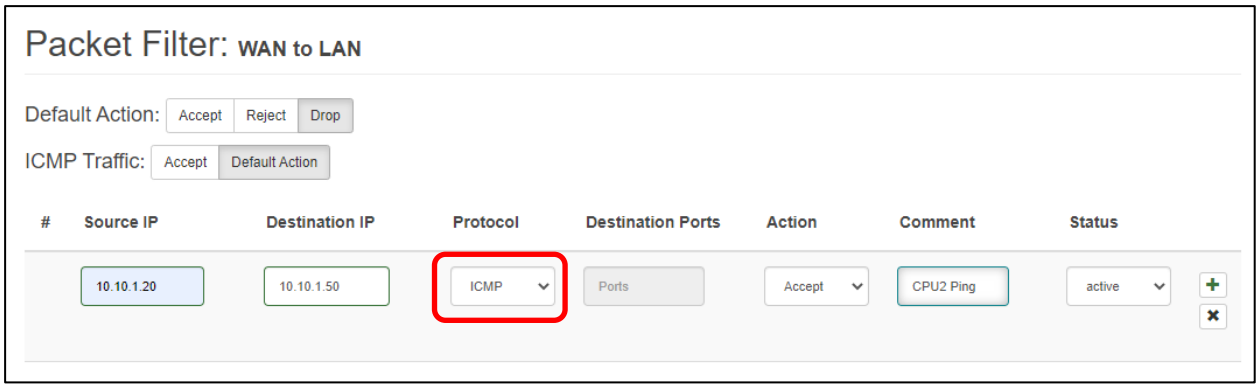
A maximum of 128 packet filter rules per direction (“WAN to LAN” and “LAN to WAN”) can be defined.

7.4 ICMP Traffic “WAN to LAN”

With "ICMP Traffic" option, you can generally "Accept" ICMP packets or apply "Default Action".

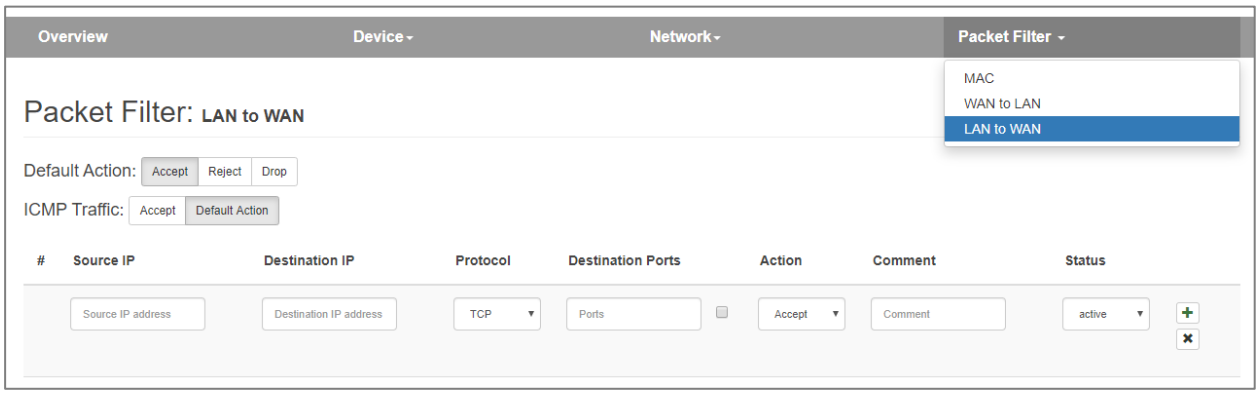
If, for example, the packet filters “Default Action” are set to “Reject” or “Drop”, and ICMP Traffic to “Default Action”, ICMP frames are rejected or dropped.

In addition to general ICMP rule, you can further customize your firewall by adding specific packet filter rules for ICMP protocol.



7.5 Packet filter “LAN to WAN”

By default data traffic is permitted for devices from the machine network (LAN) to the company network (WAN) without limitations (“Default Action”: “Accept”).



General rule can be changed by setting the "Default Action" to "Reject" or "Drop". In addition to general rule, filtering can be further customized using specific packet filter rules.

7.6 ICMP Traffic “LAN to WAN”

With "ICMP Traffic" option, you can generally "Accept" ICMP packets or apply "Default Action".

If, for example, the packet filters “Default Action” are set to “Reject” or “Drop”, and ICMP Traffic to “Default Action”, ICMP frames are rejected or dropped.

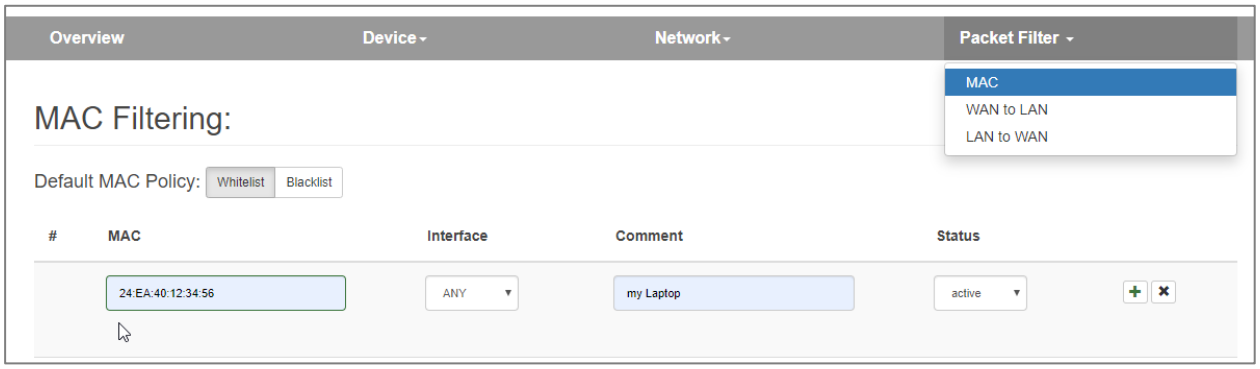
In addition to general ICMP rule, you can further customize your firewall by adding specific packet filter rules for ICMP protocol.

8 MAC address filtering

With the function “MAC Filtering;” communication via the WALL IE can be limited to devices with certain MAC addresses (“Whitelisting”) or devices with certain MAC addresses can be denied access (“Blacklisting”).

MAC Filtering can be used both in the NAT and in the bridge operating mode.

Filtering for each MAC address can be activated on the WAN, on the LAN, or on both interfaces.



MAC addresses must always be entered in the format “AA:BB:CC:DD:EE:FF;” whereby numbers are to be indicated with hexadecimals.

ATTENTION

MAC Filtering has the highest priority of all filters in the WALL IE.

As soon as the first MAC address is entered in the MAC filter mode “Whitelist”, only frames from this MAC address are allowed through, irrespective of all other packet filter rules.

When MAC Filtering is used in the “Whitelist” mode, the MAC addresses of **all** allowed devices must be indicated.

If no MAC filter rule has been entered, the “MAC Filtering” is deactivated, irrespective of the “Default MAC Policy”.

NOTE

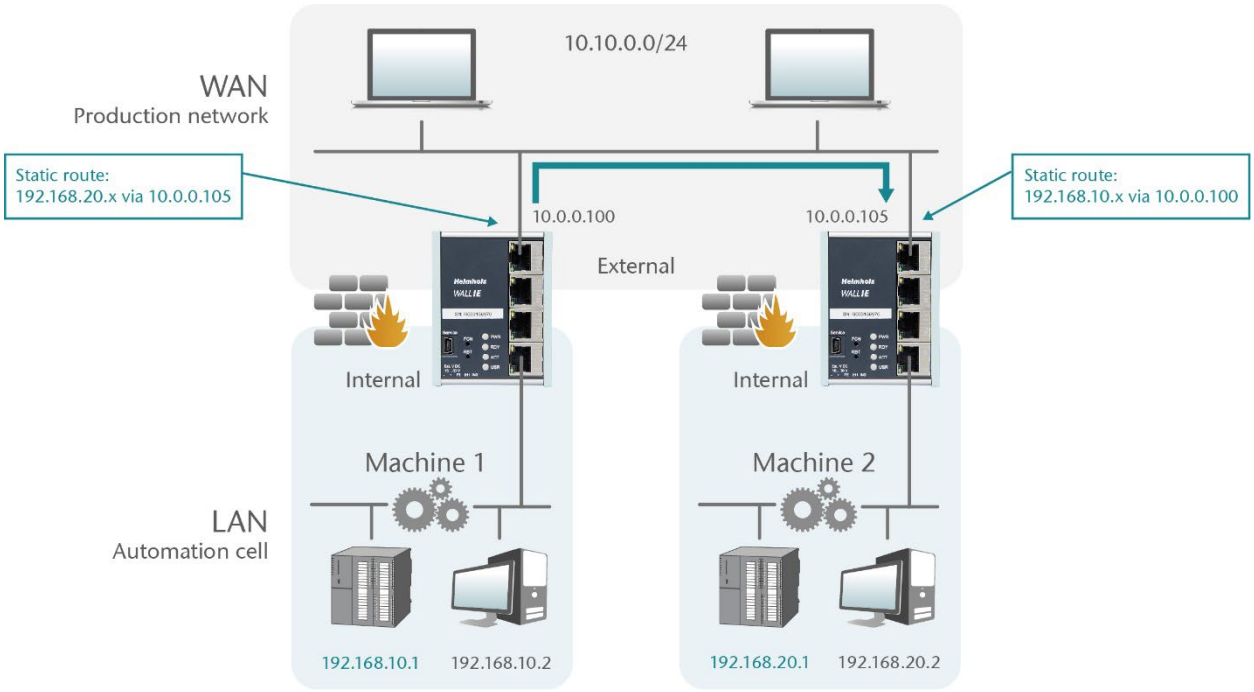
In the NAT mode, the MAC filtering is only carried out WHEN the MAC address is also indicated in the IP header of the packet. Layer 2 frames are not forwarded in the NAT mode.

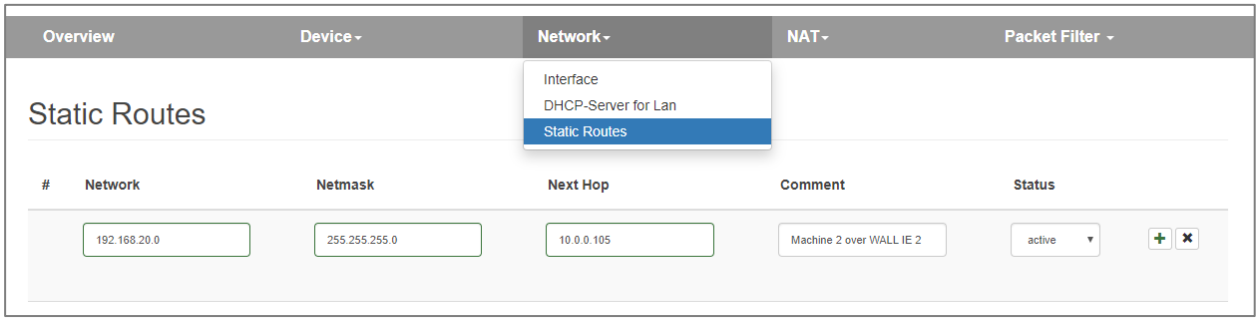
The MAC filtering takes place on layer 2 in the bridge mode.

A maximum of 128 MAC filter rules can be defined.

9 Static routes

Static routes are used for communication with other automation cells. To this purpose, the network and the address of the router or WALL IE responsible for this (“Next Hop” or “Gateway”) must be configured.





ATTENTION

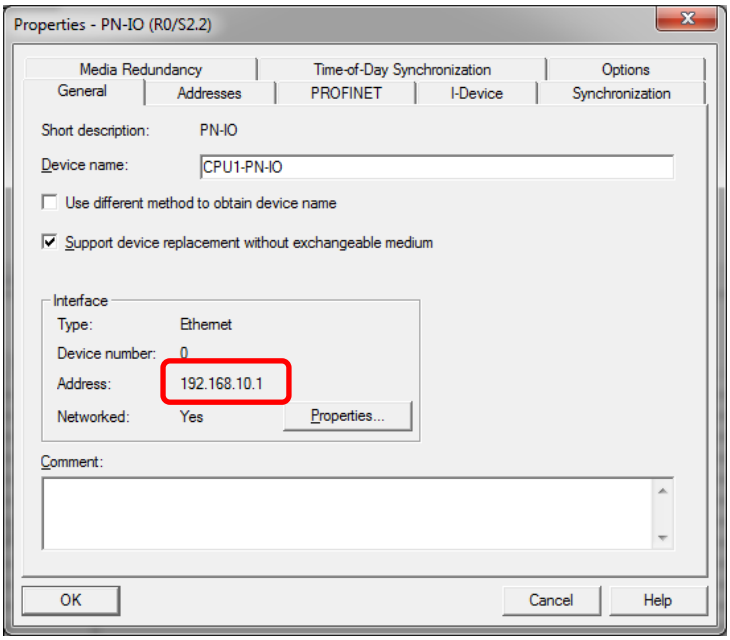
In order to enable the return route of the answer, a route for the IP address of the WALL IE of machine 1 must also be set up in the remote gateway (Machine 2)!

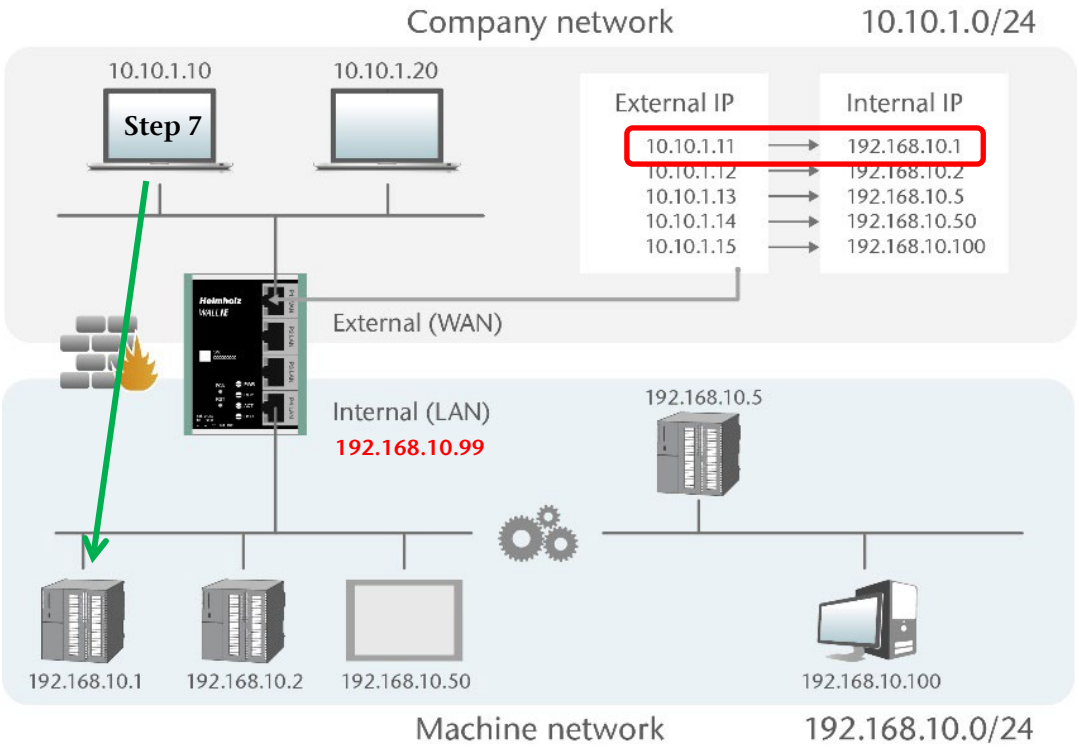
10 Use with Simatic Step 7 / TIA portal

Problem: If Simatic CPUs in the LAN behind a WALL IE are to be addressed or planned with an engineering station in the WAN, the problem is that the Step 7 or TIA portal uses the IP address from the project for access to the CPU.

In the case of access via a WALL IE, which is configured in the operating mode Basic NAT, another IP address must be used for access to the CPU in the Step 7 or TIA portal.

The solutions described in the following can also function in adapted form for other applications.

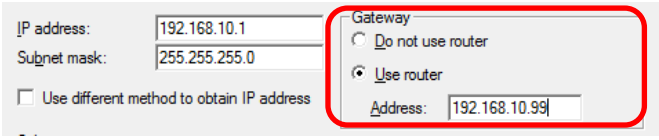




10.1 Application with step 7

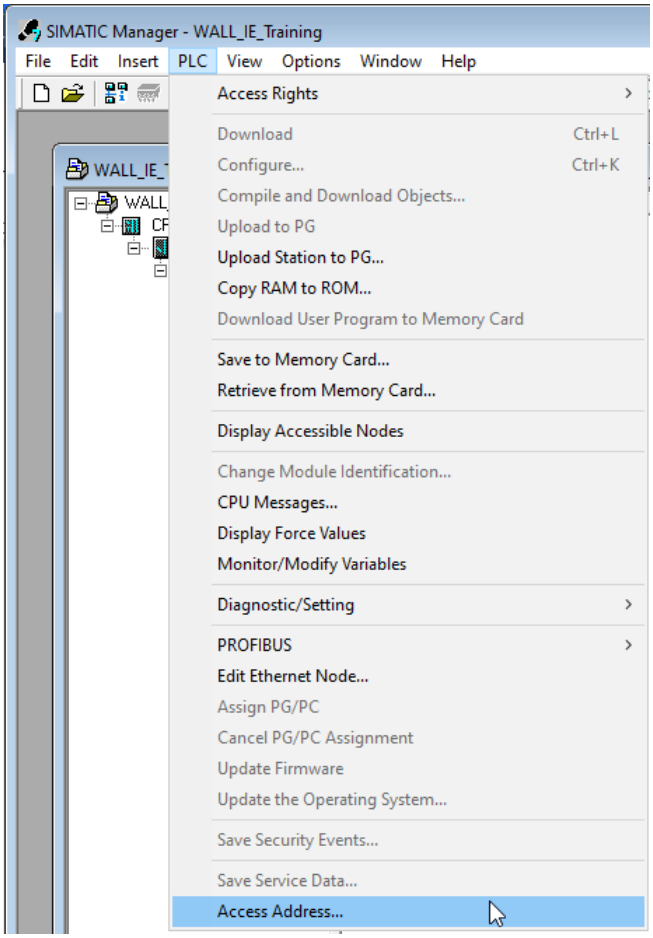
Step 7 offers the possibility to access a CPU and to use an IP address other than that set in the project in the process.

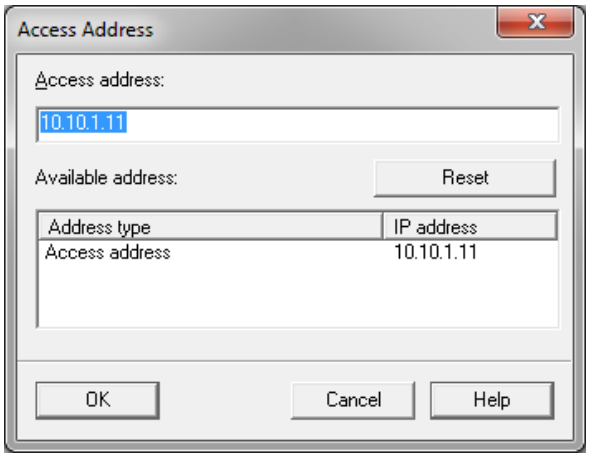
In order to be able to redirect the responses from the CPU back to the engineering station in the WAN via the WALL IE, either the SNAT function must be activated in WALL IE under "Basic NAT" or the WALL IE must be entered as the router for the CPU in the project.



In order to be able to reach a CPU via an alternative IP address, this can be entered in the menu “Destination system” in the dialog “Access address”.

This address remains active until it is deleted in the same dialog through “Reset”.





ATTENTION

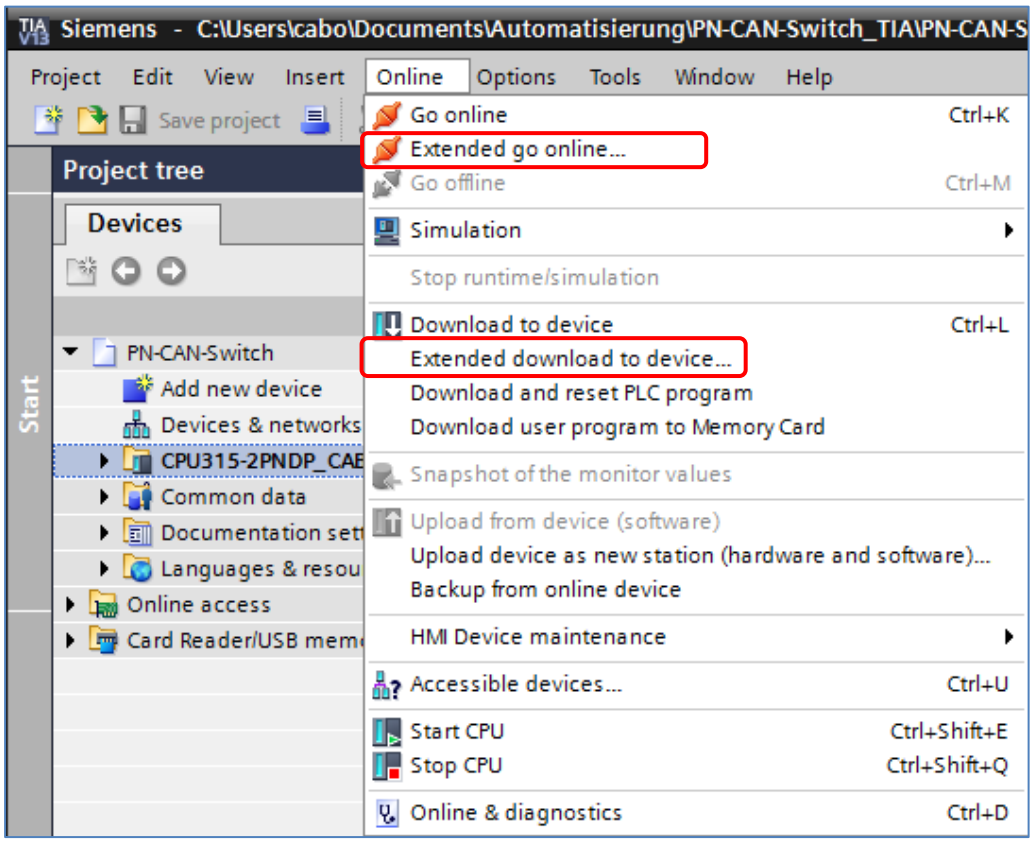
This solution can only be sensibly used in the Basic NAT operating mode. In the case of NAPT with port forwarding, only one CPU can be reached, as the Simatic Manager always accesses the CPU with the non-adjustable port 102.

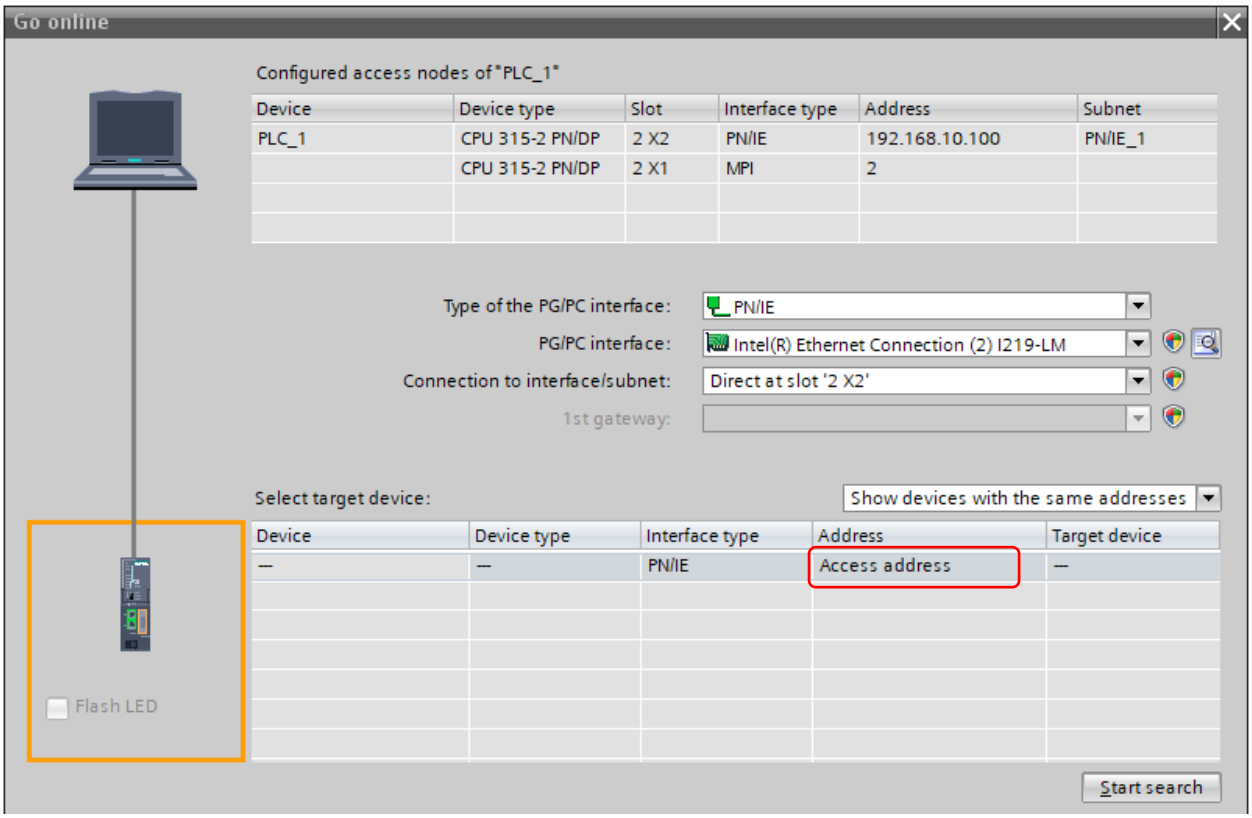
The search via the Siemens function “reachable participants” doesn’t function through the WALL IE firewall.

PROFINET RT frames are not routed through by WALL IE!

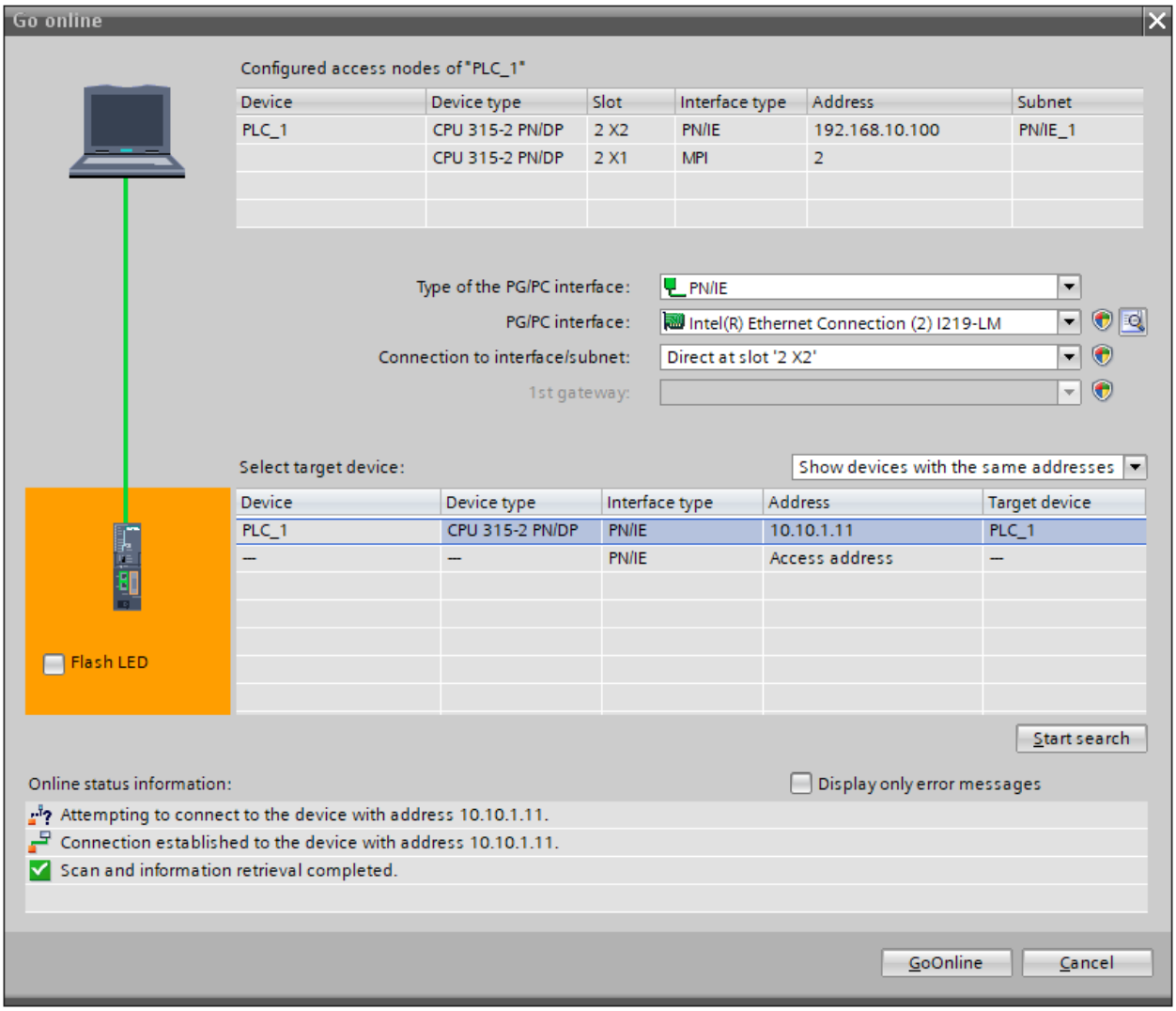
10.2 Use in the TIA portal

Here you use the function “Expanded loading in the device” in the menu under “Online” or, where necessary, “Connect expanded online”.





Click on "Access Address" and enter the WAN IP address specified for the device (CPU) in the WALL IE in Basic NAT. Confirm the entry by clicking on the window. An attempt is now made to establish a connection using the entered IP address.



ATTENTION

This solution can only be used in Basic NAT operating mode. In the case of using WALL IE with NAPT and port forwarding, only one CPU can be reached, as the Simatic Manager/TIA portal always accesses the CPU with the non-adjustable port 102.

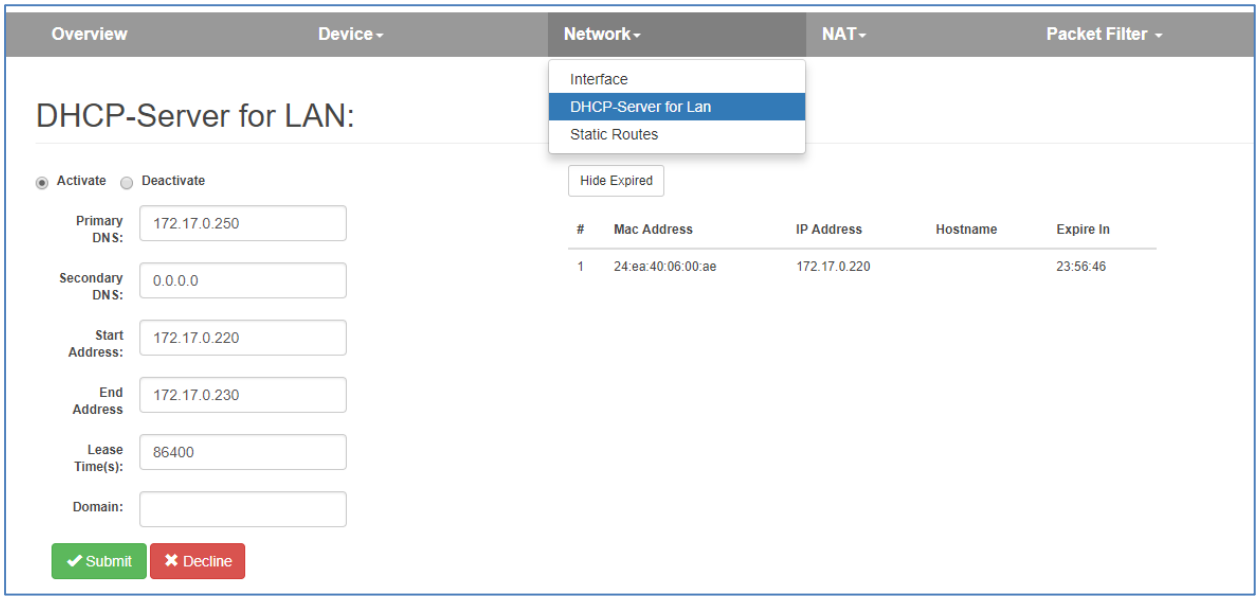
The search via the Siemens function “reachable participants” function does not work through the WALL IE firewall.

PROFINET RT frames are not routed through by WALL IE!

11 Other functions

11.1 DHCP server for LAN

A DHCP server can be activated for the LAN network of the WALL IE in order to enable dynamic IP address assignment in the LAN.



Primary/Secondary DNS: Specifies the IP address of a DNS server that is available to a DHCP client.

Start Address: First IP address in the LAN subnet that can be assigned by the DHCP server.

End Address: Last IP address in the LAN subnet that can be assigned by the DHCP server.

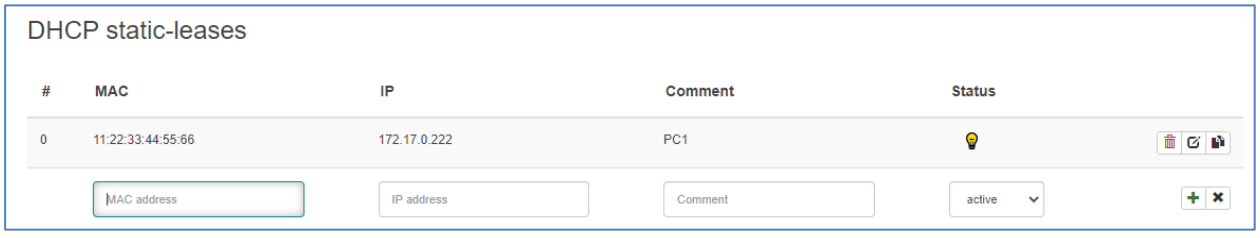
Lease Time (s): Amount of time a network device can use an IP Address in network. Once the lease time expires device needs to renew the lease or IP address will be reclaimed by DHCP server and can be offered to other devices. The Standard Lease Time is 86,400 seconds (1 day). The Lease Time can be set from 60 seconds to 31,536,000 seconds (365 days).

Domain: Domain name assigned to DHCP clients. A domain name is an identification string that defines a realm of administrative autonomy, authority, or control within the network. To use Domain name, at least one DNS server must be assigned.

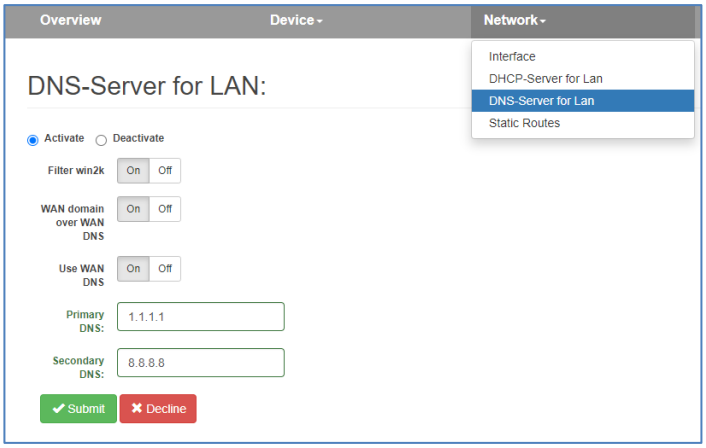
On the right side of the website there is a table of the IP addresses assigned by the DHCP server with the affiliated device MAC addresses.

With "**Hide Expired**", the list of assigned IP addresses can be shortened by the entries that are no longer active.

For fixed assignment of an IP address using DHCP, WALL IE also supports "Static Leases":



11.2 DNS-Server for LAN



A DNS server can be activated for the LAN network of the WALL IE.

The DNS server in the WALL IE answers DNS queries directly on the LAN. For this, WALL IE requires access to authoritative DNS server on WAN interface.

If the DNS server is used in WALL IE, the devices in the LAN do not have to access DNS servers through WALL IE and no separate filter rules have to be created.

The DNS servers used by the WALL IE (Primary, Secondary) can be specified on the "**DNS-Server for Lan**" configuration page.

With the option "**Use WAN DNS**", an existing DNS server in the WAN can also be used. This will then be queried first.

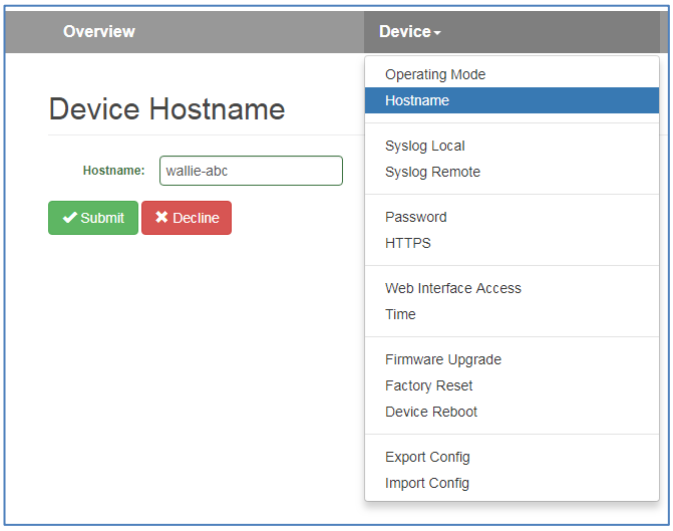
"**WAN domain over WAN DNS**": Any DNS query will usually be sent to all DNS servers from the list (Primary, secondary, etc.) regardless of domain. In case there is query within domain for which WAN DNS is responsible, this will force sending the query to WAN DNS.

"**Filter win2k**" filters periodic DNS queries that do not receive meaningful responses from the public DNS. These queries can cause problems by triggering dial-on-demand connections.

11.3 Host name (WAN)

The DNS host name of the WALL IE can be defined for the WAN interface.

The entered device host name is transmitted to the DHCP / DNS server when the DHCP lease has been assigned and the DHCP server used supports the “DHCP Option 12”. Whenever a new device name is defined with this function, the DHCP lease is approved and a new one requested.



11.4 Syslog server

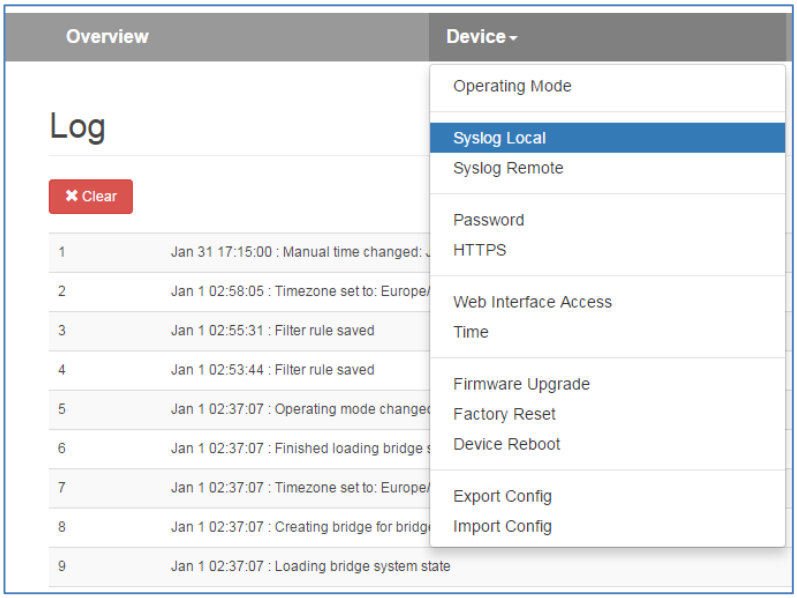
The Syslog server installed in the WALL IE logs all user and system events with time of day and date. User events are changes to the configuration or the user login. The system events originate from the operating system or the running application. In order that the Syslog server displays the correct time, this must be set in the “Time” menu (see Ch. 11.9).

In addition, Syslog logs network access attempts blocked by the WALL IE filters.

11.4.1 Syslog local

The local Syslog display lists the recorded events.

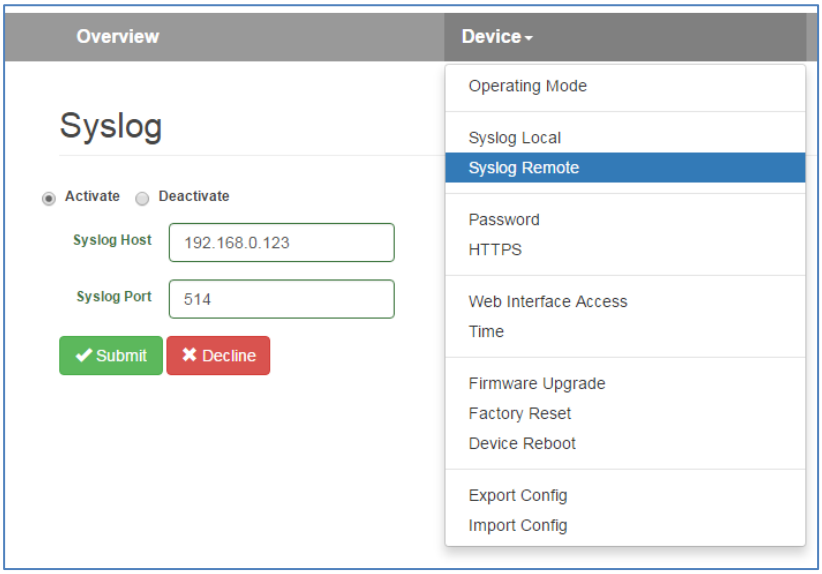
The Syslog memory can be deleted with “Clear”.



11.4.2 Syslog remote

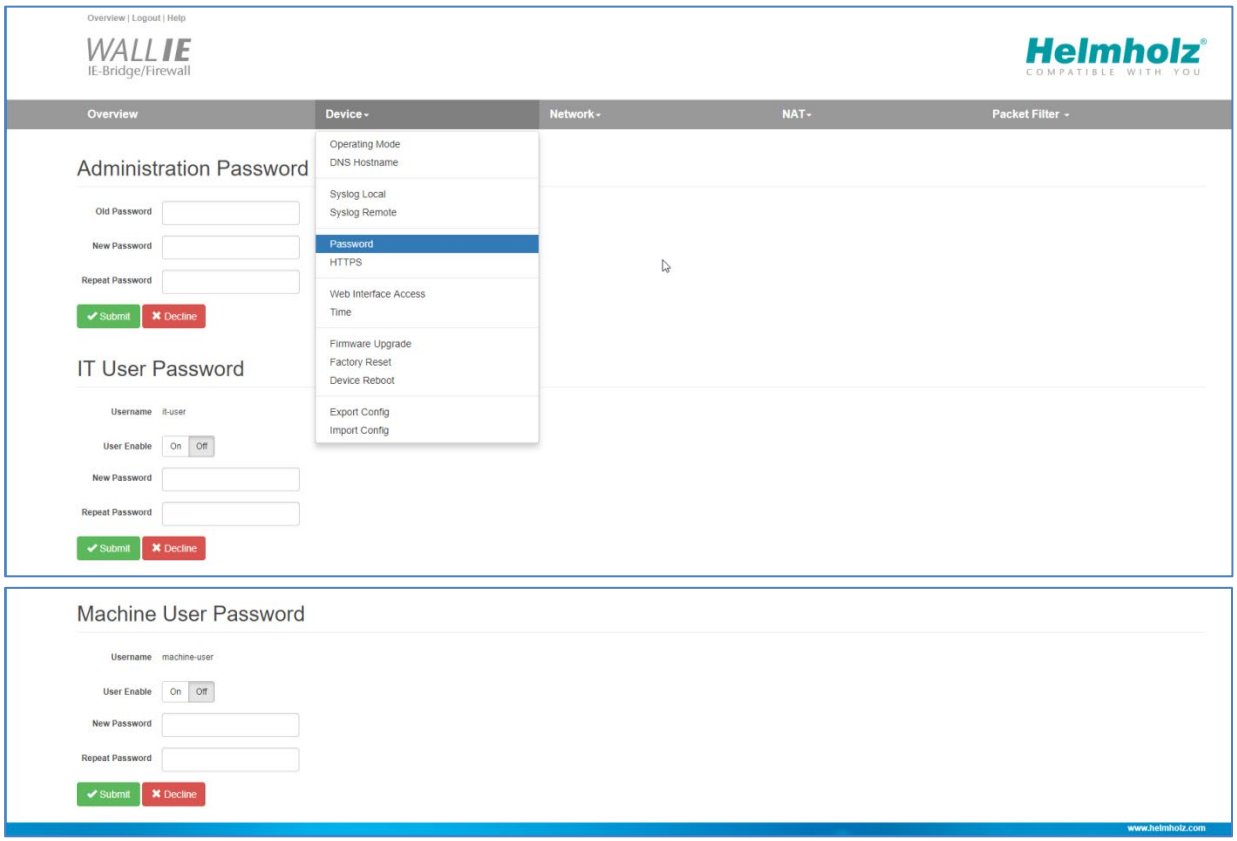
The Syslog messages can also be sent by the WALL IE to a PC through the network on which a program for Syslog recording is running.

The IP address of the host and the port can be indicated here.



11.5 Change password and User management

In the “Password” menu, the password of the administrator, “admin”, can be changed, the additional users activated, and passwords defined or changed.



In addition to the “admin” user, which has unlimited access rights, WALL IE supports two more users with limited access rights: “it-user” and “machine-user”.

Access rights of the “it-user”.

- Access to the WALL IE exclusively via the WAN interface
- Change host name
- Update TLS certificate
- Setting of remote Syslog server
- Change DHCP client for WAN
- Restart device
- Export WALL IE configuration
- Change password of the “it-user”
- Edit date and time settings
- All other settings are “ReadOnly”

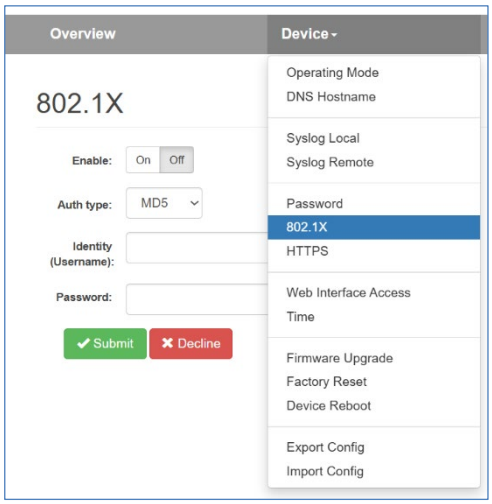
“machine-user” access rights:

- Access to the WALL IE exclusively via the LAN interface
- Change to the settings of the DHCP server
- Changing of the Basic NAT/NAPT rules and settings
- Changing all packet filter rules

- Changing the MAC filter rules
- Changing the Static Routing rules
- Change password of the “machine-user”
- Restart device
- Export WALL IE configuration
- All other settings are “ReadOnly”

11.6 Port-based network access control (802.1X)

IEEE 802.1X is a network authentication protocol that provides port-based access control for network connections. It ensures that only authorized devices can connect to the network by requiring authentication before granting access.



The protocol operates with three key components:

- **Supplicant**: The client device requesting network access
- **Authenticator**: The network device (switch or access point) controlling access to the network
- **Authentication Server**: A trusted server that validates credentials and makes the access decision

When a device connects to an 802.1X-enabled port, the authenticator blocks all traffic except authentication messages until the supplicant successfully authenticates with the authentication server. This prevents unauthorized devices from accessing network resources.

Use Cases:

- Secure network access control
- Authentication of devices before granting network access
- Integration with existing enterprise network security infrastructure (e.g. RADIUS servers)
- Compliance with network security policies requiring port-based authentication

WALL IE acts as an 802.1X supplicant on the WAN-network side, requesting network access through port-based network access control. WALL IE authenticates itself to the network using the Extensible Authentication Protocol (EAP) over LAN (EAPOL) before gaining access to network resources. 802.1X is not supported on the LAN side.

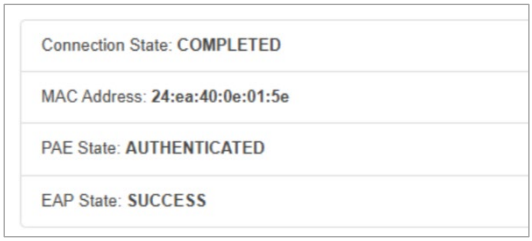
802.1X Authentication Process:

- Supplicant initiates authentication when connected to an 802.1X-enabled network port
- Supplicant sends authentication credentials to the Authenticator (network switch/access point)
- Authenticator forwards credentials to the Authentication Server
- Upon successful authentication, network access is granted
- Failed authentication keeps the port in unauthorized state, blocking network traffic
- Re-authentication can be triggered periodically or manually

Supported EAP Methods:

- „MD5“: EAP-MD5 (Message Digest 5)
- “PWD”: EAP-PWD (Password)
- “TLS”: EAP-TLS (Transport Layer Security) with certificate-based authentication
- “TLS”: EAP-TTLS (Tunneled Transport Layer Security)
  - Inner Authentication types: MSCHAP, MSCHAPv2, MSCHAPv2 (No EAP), CHAP, MD5, and GTC
- “PEAP”: EAP-PEAP (Protected Extensible Authentication Protocol)
  - PEAP version 0 and 1 supported
  - Inner Authentication types: MSCHAPv2, MD5, and GTC

802.1X Status display:



Connection State:

ASSOCIATED – Connection established

COMPLETED - Authentication completed

MAC Address: Device MAC address

PAE State:

CONNECTING - Initial EAPOL exchange

AUTHENTICATING - Authentication procedure is in progress

AUTHENTICATED - Device is successfully authenticated by the Authenticator

HELD - Device failed to authenticate

EAP State:

IDLE - In process of authenticating

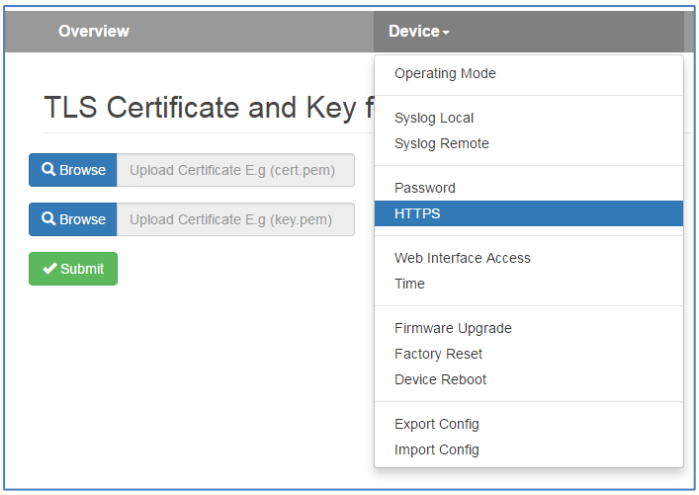
SUCCESS - Successfully authenticated

FAILURE - Failed to authenticate

11.7 Web access certificate for HTTPS

A customized company certificate can be filed for the website of the WALL IE.

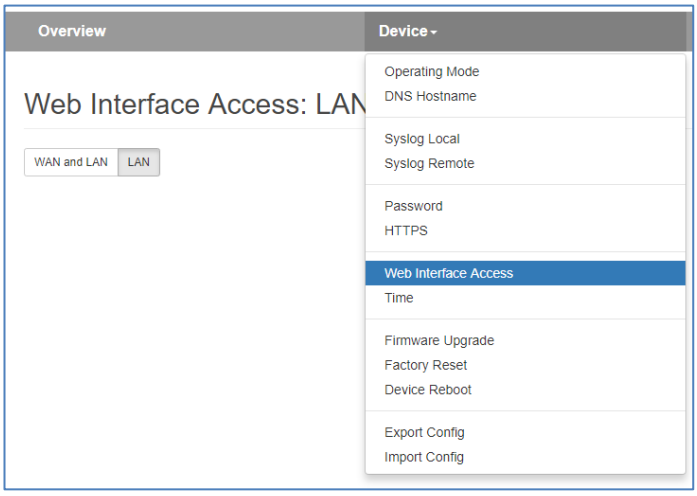
This ensures that the calling up of the WALL IE configuration website, in addition to the HTTPS encoding, is also trustworthy.



11.8 Allow web interface access over WAN network (Web Interface Access)

For security reasons, the web interface can only be reached via the LAN network as a default.

If the web interface should also be accessible via WAN network, this can be set in the "Web Interface Access" menu → "WAN and LAN".

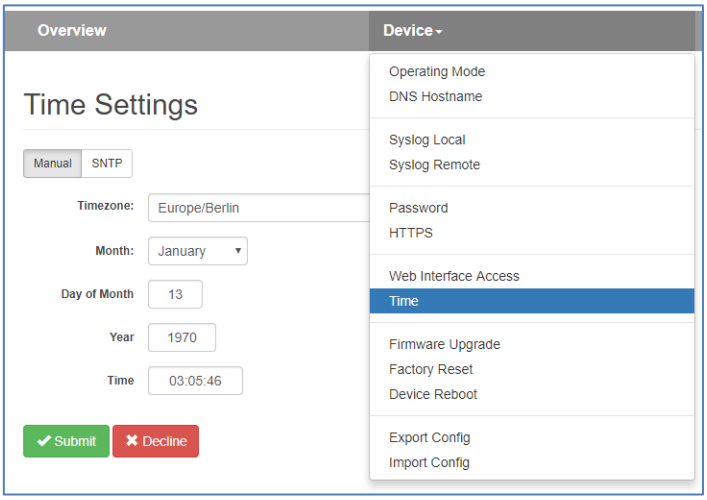


11.9 Time settings (Time)

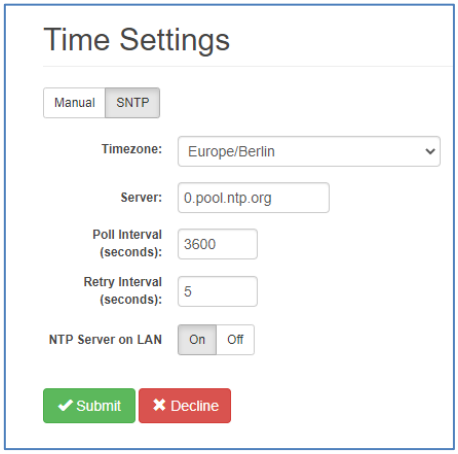
The time of day of the WALL IE can be set in the “Time” menu.

The time of day is mainly required for the Syslog records.

The time of day can be set either manually or be derived automatically from a SNTP server (“Simple Network Time Protocol”).



With the option "NTP server on LAN" WALL IE can provide the current time in the LAN network via NTP to the devices connected there.



ATTENTION

The manually set time of day is not saved in the event of a power failure. “SNTP” should be used for a constantly available time indication.

ATTENTION

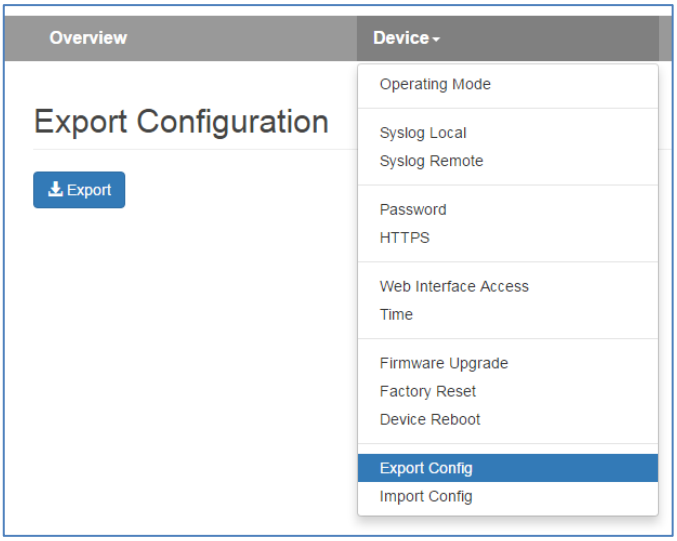
For “SNTP”, the default gateway and the DNS server must be configured in the interface settings in order that the SNTP service can reach the NTP server in the Internet

11.10 Export/import of configuration

The configuration of the WALL IE can be exported into a readable configuration file and imported again.

It is thus possible to secure both a backup of a WALL IE configuration and to copy an existing configuration for a new WALL IE with a similar application.

The configuration files have the file ending “CFG”.



Example of a WALL IE configuration file:

```
general :
{
      router-mode = true;
      web-wan-access = false;
      intip = "192.168.0.100";
      intip-netmask = "255.255.255.0";
      extip = "10.10.1.99";
      extip-netmask = "255.255.255.0";
      dnsip = "0.0.0.0";
      gatewayip = "0.0.0.0";
      rsyslog :
      {
            active = false;
            host = "0.0.0.0";
            port = 514;
      };
      time :
      {
            sntp = false;
            zone = "Europe/Berlin";
            sntp-host = "0.pool.ntp.org";
            poll-interval = 3600;
            retry-interval = 5;
      ;
};
…
```

12 Firmware update

The firmware of the WALL IE can be very simply updated via the website. Please download the firmware update file in advance.

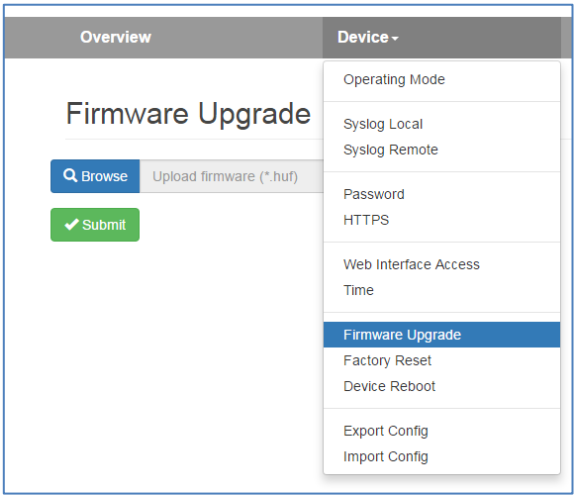
Link to firmware:
https://www.helmholz.de/goto/700-860-WAL01 (WALL IE)
https://www.helmholz.de/goto/700-862-WAL01 (WALL IE PLUS)
https://www.helmholz.de/goto/700-863-WAL01 (WALL IE Compact)

The firmware file can be recognized by ".HUF" extension (Helmholz Update File) and is also encoded to protect it from being changed.

Save the firmware file on your PC and select the location with "Browse" in the "Device" menu under "Firmware Upgrade".

The firmware file is then transferred to the WALL IE. This can take up to 1 minute, depending upon the network connection.

The firmware file is decrypted and checked in WALL IE. If the content is correct, the firmware is transferred retentively to the program memory and then an automatic restart is performed.



ATTENTION

Operation of the WALL IE is interrupted during the update procedure. Do not turn off the device during the update procedure!

NOTE

The configuration of the WALL IE is retained at a higher version following an update, to the extent that this is technically possible. However, a "downgrade" to an older firmware version can result in configuration errors. Carrying out a factory reset is recommended following a downgrade.

NOTE

Following a firmware update, it may be necessary to delete the browser cache once in order to update obsolete JavaScript elements of the WALL IE website.

13 Resetting to factory settings

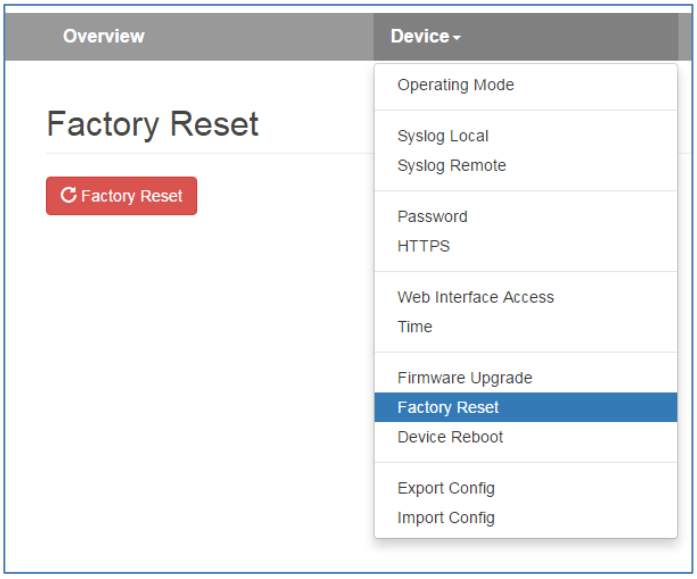
The resetting of the WALL IE to factory settings can be initiated both via the website and without access to the device with the “FCN” button.

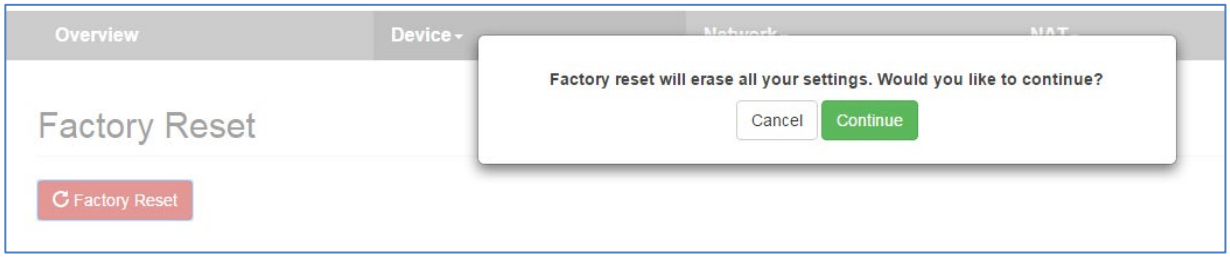
When resetting the WALL IE, the configuration is irretrievably deleted and the IP settings are set to the delivery status. The firmware remains at the current status in the process.

13.1 Resetting to factory settings via the website

Select the menu point “Factory Reset” in the “Device” menu.

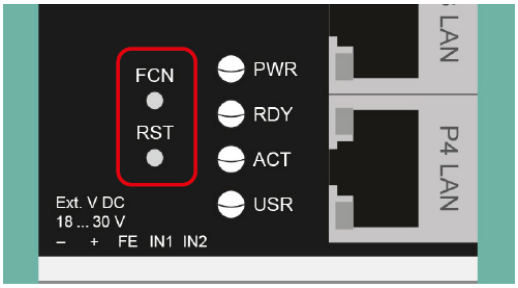
Press the “Factory Reset” button and confirm with the confirmation prompt.





13.2 Resetting to factory settings with button

In order to reset WALL IE to the delivery status, the “**FCN**” button must be held pressed while the device is restarted. The successful resetting of the parameters and settings is acknowledged by the lit “USR” LED. The “FCN” button can then be released.



The "**RST**" button triggers an immediate restart of the WALL IE in which all stored settings are retained.

The WALL IE Compact does not have a reset button.

You can check whether the WALL IE has been reset to factory settings by accessing it via the default IP address 192.168.0.100; if you are prompted to enter a new admin password, the device has been reset.

14 Security Guideline

WALL IE is a network infrastructure component and therefore an important element in the security considerations for a system or network. When using WALL IE, therefore, observe the following guidelines and recommendations to prevent unauthorized access to systems and equipment.

14.1 What is the IEC 62443 series of standards?

As the central standard in the field of industrial communication, the international IEC 62443 series of standards deal with the cybersecurity of industrial automation and control systems (IACS) and pursues a holistic approach for operators, integrators, and manufacturers.

It therefore affects everyone involved in the design and operation of machinery. The corresponding responsibilities for machine manufacturers, suppliers, and end customers are defined there.

The standard is currently divided into four parts. While Part 1 clarifies terminology and explains general concepts, Parts 2 to 4 deal with the perspectives of the **product manufacturer** (Part 4), the **integrator/machine builder** (Part 3), and the **operator** (Part 2).

Further information on the legal framework (Cyber Resilience Act, Machinery Directive) and the relevant standards can be found on our website in our Security Whitepaper.

14.2 IEC 62443-4 standard for product manufacturers

The substandard 62443-4 consists of two parts:

62443-4-1 specifies the secure development process for secure products and how manufacturers should deal with vulnerabilities. Helmholz bases the development and maintenance of WALL IE and its vulnerability management on IEC 62443-4-1.

62443-4-2 contains a list of security requirements for products that must be implemented depending on the product type and the desired security level. The implemented security requirements of the WALL IE are explained in the following sub-chapters.

14.3 Defense in Depth concept

An essential concept in the safety design of a machine or system is the concept of "defense in depth."

At the core is the component that must be developed securely and maintained at a secure level.

Above that is the system, the network, the machine, right up to the entire factory. These levels must be set up with appropriate security concepts, such as zones of trust and firewalls.

Above that are the "policies and procedures," i.e., the rules and processes governing how the system and equipment must be handled (perimeter protection, access authorizations, passwords, update cycles, etc.).

Responsibility for training and security awareness is anchored at the highest level of management.

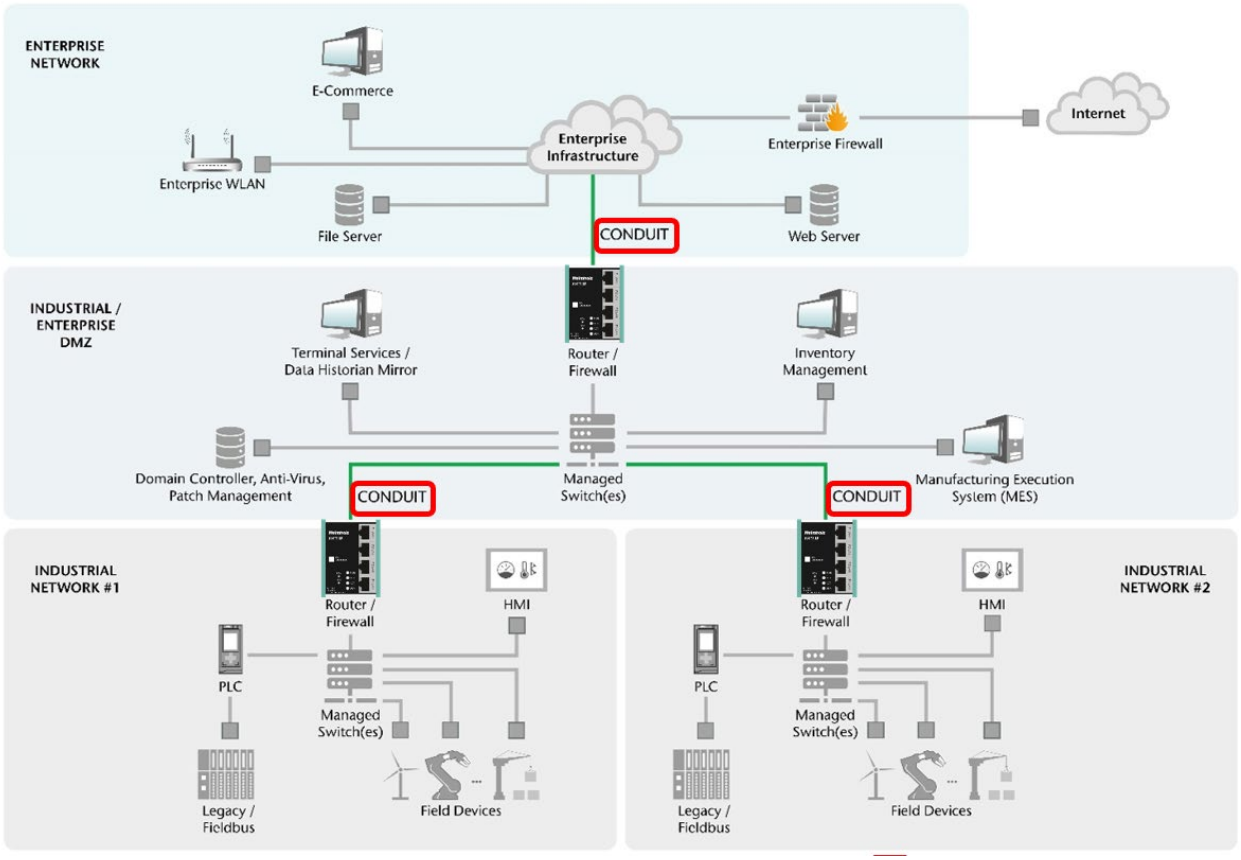
WALL IE is a component in the machine (system) and supports the machine's network security.

14.4 Security context of the WALL IE (intended use)

In order to meet the requirements defined in the IEC 62443 series of standards, WALL IE must be used in the intended applications ("intended use") resulting from the defined security context.

The following figure shows the general security context. WALL IE is used here as a secure conduit for transitioning between different zones of trust to establish zone protection in production facilities. It can be used to separate production or automation cells from the production network in the system integrity layer.

The core function of WALL IE is to block unwanted network traffic and allow desired network traffic to pass through.



To meet the requirements, organizational measures and settings on the WALL IE as well as settings on external systems are necessary. The following measures are mandatory to meet the requirements specified in the IEC 62443-4-2 standard.

It is important to note that components of an automation system can also be combined so that the overall system meets the desired security requirements. It is therefore not necessary for each individual component to achieve the desired security level; instead, security can or should be ensured through a combination of devices and measures.

14.5 Hardening the security of the WALL IE / Secure operation

To ensure the secure operation of WALL IE and to minimize the risks for its use in the security context, the following assets must be protected in the device:

- Firewall configuration
- Firmware
- Certificates
- Session keys
- User data
- Log files

When used in accordance with the security guideline, the device offers protection against the following threats:

- Data manipulation (breach of integrity)
- Denial of service (DoS) (breach of availability)
- Espionage (breach of confidentiality)

ATTENTION

Failure to comply with this security guideline may result in the core function of the WALL IE not being maintained, i.e., unwanted network traffic between zones may be enabled.

This could allow other devices in the network to be attacked and compromise the function of the entire application.

14.5.1 Organizational measures during planning

The use and configuration of the WALL IE is intended exclusively for users who are familiar with the relevant safety concepts of automation technology and the applicable standards and other regulations, in particular the IEC 62443 series of standards ("skilled or instructed personnel").

Only authorized persons should be granted access rights to the configuration or logging information of the WALL IE.

WALL IE should be installed in a restricted access control cabinet in the production facility to which only authorized personnel have access (perimeter protection). Only grant access to components, networks, and systems to persons for whom this is absolutely necessary.

The higher-level networks must be planned in accordance with the defense-in-depth principle and the requirements of the IEC 62443(-3/-2) series of standards.

WALL IE should not be used for a direct Internet connection. The connection to the Internet should always be established via a suitable secure router.

WALL IE does not include deep packet inspection. The content of the communication permitted by the filter rules through WALL IE is in the responsibility of the network and communication planning for the machine or system.

14.5.2 Security measures provided by WALL IE

WALL IE provides the following measures to protect against security-attacks:

- Secure web access via HTTPS with user certificates
- Verification of input values in the web frontend
- User authentication with User and role management
- Port authentication according to 802.1X on the WAN port
- Event-Logging (SysLog): Detailed internal logging and transmission to a syslog server
- Logging blocked network access in the syslog
- Web interface on WAN side can be disabled
- Only necessary services are implemented (see chapter 14.5.6)
- Time synchronization for logging data using SNTP
- Secure default configuration
- Verification of configuration integrity
- Device configurations can be exported and imported
- Exported configurations can be compared
- Minimum footprint Linux, which only contains the necessary function modules
- Secure firmware update with integrity check
- Integrity check of base configuration (MAC addresses, serial numbers, etc.)
- “Factory reset” deletes all data in the WALL IE

NOTE

If the integrity of the configuration data (device or user configuration) or the firmware integrity is compromised, the device will not allow any network traffic between the WAN and LAN.
WALL IE also stops network traffic transmission in the event of denial-of-service attacks.

The WALL IE is then in "fail-close" state.

14.5.3 Internal measures to strengthen the WALL IE security

Perform the following steps when configuring the WALL IE to enhance the security of the device:

- Secure web access with your own web certificate (see section 11.7).
- Turn off unused interfaces and services, e.g., access to the configuration website in the WAN, if it is not necessary.
- Enable time synchronization to obtain correct timestamps for the log files (see section 11.9).
- Use the users and roles according to the responsibilities and capabilities of the WALL IE users and limit access rights to the minimum necessary ("least privilege")

14.5.4 Secure user and role management

- Set secure passwords
- Disable unused users
- Only use administrator access when necessary
- The following user roles are provided by WALL IE: “admin”, “it-user”, “machine-user”. See chapter 11.5

14.5.5 Services/ports used in the WALL IE

The following table lists the services implemented by WALL IE. Take this into account when considering your network security as a whole.

Dienst / Service	Port	LAN / WAN ?	Remark
HTTPS	443	LAN + WAN	Access can be restricted to LAN. Default access only via LAN
HTTP	80	LAN + WAN	Port 80 is forwarded to port 443 and only HTTPS traffic is permitted. Access can be restricted to LAN. Default access only via LAN.
DHCP-Client	68	WAN, no open Port	DHCP on WAN can be configured (static IP)
DHCP-Server	67	LAN	DHCP on LAN is disabled by default.
DNS-Server	53	LAN	DNS server on LAN is disabled by default
NTP	123	WAN	Disabled by default
SNTP-Server	123	LAN, only sending	Disabled by default
Syslog	514	WAN, only sending	Can be activated, port is adjustable, syslog data is only sent

14.6 External measures - Use, maintenance and monitoring

- Only use up-to-date browsers with the latest encryption technologies when accessing WALL IE via the web.
- Regularly check for new advisories regarding the WALL IE products. These can be found on the CERT@VDE website.
- Check regularly for new firmware. Update the firmware if necessary to keep your system at the desired security level (see section 12). The firmware that can be downloaded from the Helmholz website is encrypted, and only official Helmholz firmware files are accepted for updating in the WALL IE.
- Log changes to the WALL IE configuration.
- After each configuration change, create a backup of the WALL IE configuration (see section 11.10).
- Check the logging data regularly or send the logging data to a remote log server (syslog server) with downstream evaluation, e.g., SIEM applications (see section 11.4).
- Conduct periodic reviews of all above-mentioned measures

14.7 Removal – safe disposal

Perform a factory reset of the device to delete all security-related data (user data, logging protocols, passwords, certificates) from the device before removing it.

Instructions for performing a factory reset can be found in section 13.

You can check whether the WALL IE has been reset to factory settings by accessing it via the default IP address 192.168.0.100; if you are prompted to enter a new admin password, the device has been reset.

14.8 Vulnerability monitoring / The PSIRT team

The Helmholz **Product Security Incident Response Team (PSIRT)** provides proactive support to help you protect your machines as effectively as possible in the context of industrial communication. Whenever new potential threats arise or are reported to us, we evaluate and process them immediately and provide you with recommendations for action, patches, and updates as quickly as possible to minimize the risk.

You can find more information about Helmholz PSIRT hear.

14.9 Reporting vulnerabilities

You can help too: **Report any abnormalities** relating to the product to the Helmholtz PSIRT team at psirt@helmholz.de or support@helmholz.de or to CERT@VDE.

14.10 Information on the security of Helmholz products

Helmholz is a member of **CERT@VDE**. Here you can find specific information on security in industrial environments.

In addition to our technical newsletter, we communicate security-related updates, patches, and advisories to you as a user of Helmholz products via CERT@VDE. The latest advisories for Helmholz products can be found here: https://certvde.com/de/advisories/vendor/helmholz/

14.11 Further information on industrial security

Further information on the topic of security can be found here, for example.:

- TeleTrust
- Sichere-industrie.de
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Allianz für Cyber-Sicherheit

14.12 General security recommendations

General:

- Ensure at regular intervals that all relevant components fulfill these recommendations and possibly any other internal security guidelines.
- Evaluate your system holistically with a view to security. Use a cell protection concepts ("defense-in-depth") with corresponding products, such as the WALL IE.
- Regularly inform yourself about security threats for all your components
- Train your employees regularly on the subject of security and the safe use of components

Physical access:

- Restrict physical access to components to qualified, trained, and authorized personnel.

Security of the software:

- Always keep the firmware of all communications components up to date.
- Use up-to-date web browsers and communication software
- Inform yourself regularly of firmware updates for the product. Information on this can be found in chapter 12.
- Only activate protocols and functions you really need
- If possible, always use those variants of protocols that provide more security

Passwords:

- Define rules and roles for usage of the devices and the awarding of passwords
- Change standard passwords
- Only use strong passwords. Avoid weak passwords like, for example, "password1", "123456789", or similar.
- Ensure that all passwords are inaccessible to unauthorized personnel.
- Don't use one password for various users and systems.

Data protection:

- To avoid disclosure of sensitive data, always reset the device to factory settings before decommissioning it.
- Resetting to factory settings will delete all configurations, users, passwords, logging data, and certificates.

15 FAQ

Are broadcasts or multicasts allowed through the WALL IE?

In NAT mode broadcast and multicast messages cannot be forwarded between interfaces (WAN to LAN or LAN to WAN). In Bridge mode it is possible to enable forwarding of ARP and DCP messages. The blocking of broadcasts reduces the bus load in both networks and increases the real time capability of the machine network.

Can I send frames via the WALL IE PROFINET RT?

No, PROFINET RT frames are not forwarded between LAN and WAN interface.

What must I take into consideration when I wish to work with a CPU in the LAN via the WALL IE with the Simatic Manager or the TIA Portal (WAN)?

In the NAT operating mode, the LAN address of the WALL IE must be entered in the CPU as a router in order that the answers of the CPU find their way back to the PC in the WAN. You can find more information on this application case in chapter 10.

Can the WALL IE save multiple configurations?

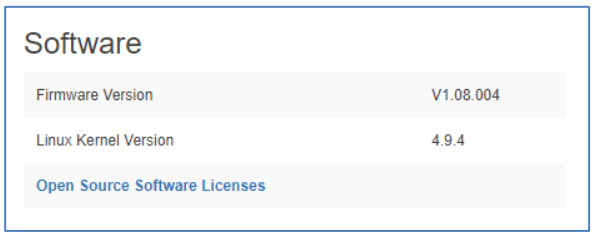
No, the WALL IE always only has one current configuration. However, it is possible to deactivate or activate individual packet filter rules or NAT entries via the lamp symbol. It is also possible to export, edit and import a WALL IE configuration again.

How can I determine whether I have the latest firmware and where do I find the most recent firmware?

The active firmware of the WALL IE is shown in the "Overview" website of the WALL IE.

The most recent firmware can be downloaded at the website www.helmholz.de.

The installation of the firmware is described in chapter 12.



16 Technical data

16.1 WALL IE (700-860-WAL01)

Order no.	**700-860-WAL01**
Name	WALL IE, Industrial NAT Gateway/Firewall
Dimensions (D x W x H)	32,5 x 58,5 x 76,5 mm
Weight	Approx. 130 g
WAN interface	
Number	1
Type	10Base-T/100Base-Tx
Connection	RJ45 socket
Transmission rate	10/100 Mbps
LAN interface	
Number	3, switched
Type	10 Base-T/100 Base-Tx
Connection	RJ45 socket
Transmission rate	10/100 Mbps
Operating modes	Bridge, NAT (Basic NAT, NAPT)
Packet filter	IPV4 addresses, protocol (TCP/UDP), ports (“WAN to LAN” and “LAN to WAN” separate), MAC addresses (black & whitelisting)
Status indicator	4 LEDs function status, 8 LEDs Ethernet status
Voltage supply	24 V DC, 18–30 V DC
Current draw	Max. 250 mA at 24 V DC
Power dissipation	Max. 2,4 W
Ambient conditions	
Installation position	Any
Ambient temperature	-40 °C ... +75°C
Transport and storage temperature	-40 °C ... +85°C
Relative air humidity	95 % r H without condensation
Pollution degree	2
Protection rating	IP20
Certifications	CE, UL
UL	UL 61010-1/UL61010-2-201
Voltage supply	DC 24 V (18 ... 30 V DC, SELV and limited energy circuit)
Pollution degree	2
Altitude	Up to 2000m
Temperature cable rating	87°C
RoHS	Yes
REACH	Yes

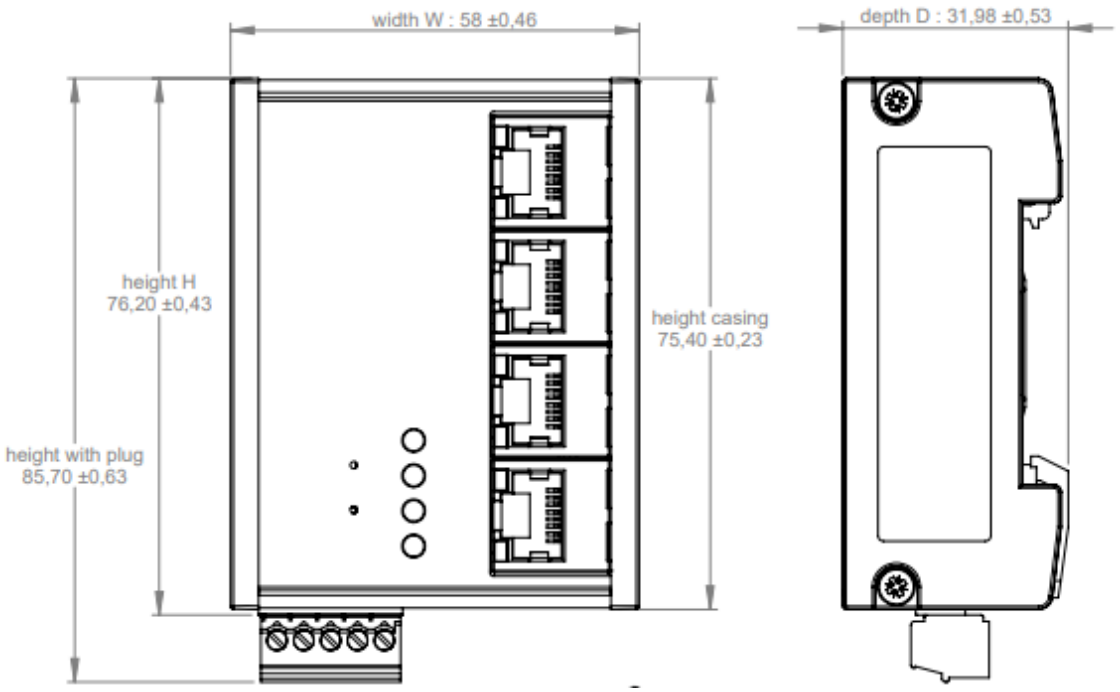
16.2 WALL IE PLUS (700-862-WAL01)

Order no.	**700-862-WAL01**
Name	WALL IE PLUS, Industrial NAT Gateway/Firewall
Dimensions (D x W x H)	32,5 x 101,5 x 76,5 mm
Weight	Approx. 230 g
WAN/LAN interface	
Number	8, switched
Type	100Base-Tx/1000Base-T
Connection	RJ45 socket
Transmission rate	100/1000 Mbps
Operating modes	Bridge, NAT (Basic NAT, NAPT)
Packet filter	IPV4 addresses, protocol (TCP/UDP), ports (“WAN to LAN” and “LAN to WAN” separate), MAC addresses (black & whitelisting)
Status indicator	4 LEDs function status, 8 LEDs Ethernet status
Voltage supply	24 V DC, 18–30 V DC
Current draw	Max. 275 mA at 24 V DC
Power dissipation	Max. 6,7 W
Ambient conditions	
Installation position	Any
Ambient temperature	0 °C ... +60°C
Transport and storage temperature	-40 °C ... +85°C
Relative air humidity	95 % r H without condensation
Pollution degree	2
Protection rating	IP20
Certifications	CE
RoHS	Yes
REACH	Yes

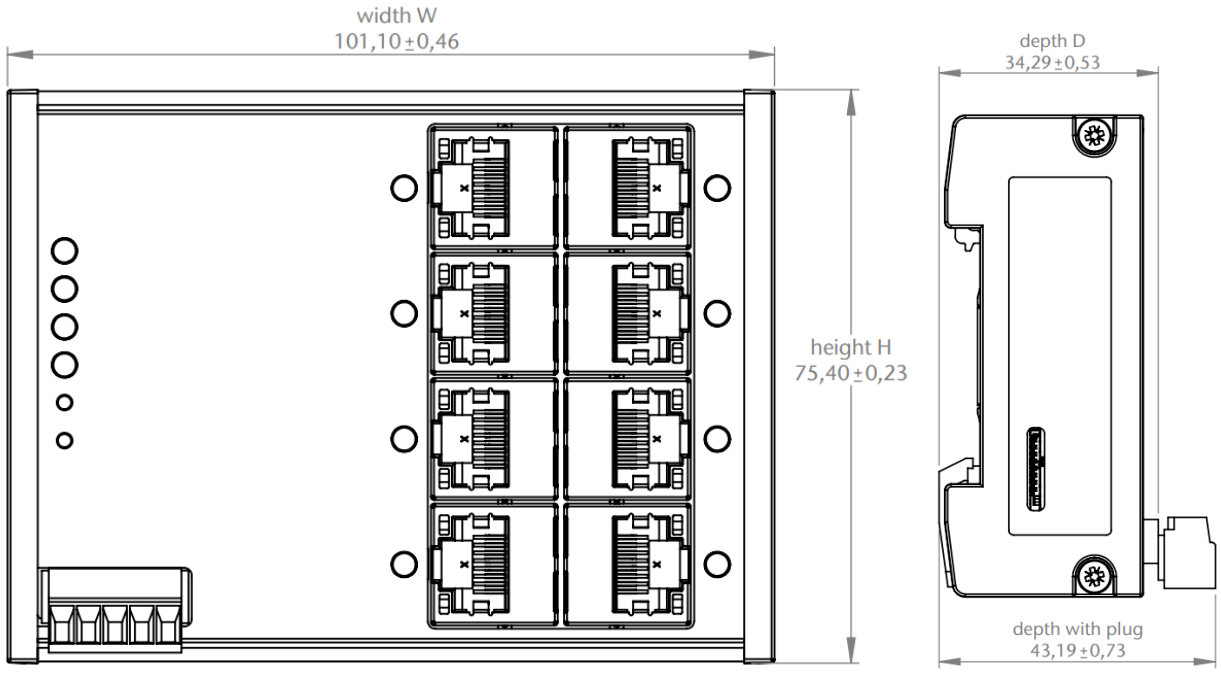
16.3 WALL IE Compact (700-863-WAL01)

Order no.	**700-863-WAL01**
Name	WALL IE Compact, Industrial NAT Gateway/Firewall
Dimensions (D x W x H)	35 x 48.5 x 76 mm
Weight	approx. 105 g
WAN/LAN interface	
Number	2
Type	100Base-Tx/1000Base-T
Connection	RJ45 socket
Transmission rate	100/1000 Mbps
Operating modes	Bridge, NAT (Basic NAT, NAPT)
Packet filter	IPV4 addresses, protocol (TCP/UDP), ports (“WAN to LAN” and “LAN to WAN” separate), MAC addresses (black & whitelisting)
Status indicator	4 LEDs function status, 4 LEDs Ethernet status
Voltage supply	24 V DC, 18–30 V DC
Current draw	max. 140 mA at 24 V DC
Power dissipation	max. 3,3 W
Ambient conditions	
Installation position	Any
Ambient temperature	0 °C ... +60°C
Transport and storage temperature	-40 °C ... +85°C
Relative air humidity	95 % r H without condensation
Pollution degree	2
Protection rating	IP20
Certification	CE
RoHS	Yes
REACH	Yes

16.4 Dimension drawing WALL IE (700-860-WAL01)



16.5 Dimension drawing WALL IE PLUS (700-862-WAL01)



16.6 Dimension drawing WALL IE Compact (700-863-WAL01)