Helmholz
COMPATIBLE WITH YOU

WALL IE, Industrial Ethernet Bridge and Firewall

Manual

Version 1 | 5/15/2017 | as of firmware V 1.04

Manual order number: 900-860-WAL01

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

Notes

To download the latest version of this manual, please visit our website at www.helmholz.de.
We welcome all ideas and suggestions.

Our products contain open source software, among others. This software is subject to the respectively relevant license conditions. We can send you the corresponding license conditions, including a copy of the complete license text together with the product. They are also provided in our download area of the respective products under www.helmholz.de.

We also offer to send you or any third party the complete corresponding source text of the respective open source software for an at-cost fee of 10.00 Euro as a DVD upon request. This offer is valid for a period of three years, starting from the date of product delivery.

Helmholz GmbH & Co. KG

Hannberger Weg 2 | 91091 Großenseebach

Revision Record:

Version	Date	Change
1	12.5.2017	First version / Firmware V1.04

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.

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

Qualified personnel must ensure that the application and use of the products described meet all the safety requirements, including all relevant 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 Ethernet Bridge and Firewall ("the device" in the following) 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 which extend beyond the documented options are not permitted and nullify the liability of Helmholz GmbH & Co. KG.

The device may not be used as the only means for preventing hazardous situations on machinery and systems.

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

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

The device has 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, as well as property damage to the control system, the product, or the environment. Use the device only as intended!

1.6 Installation

1.6.1 Access restriction

The modules 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.

1.6.2 Electrical installation

Observe the regional safety regulations.

1.6.3 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.

1.6.4 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).

1.6.5 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.

1.6.6 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.

1.6.7 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.

1.6.8 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 which compromises, damages, or infects additional equipment or processes through the remote maintenance connection, and which triggers or permits unwanted data transfer.

1.6.9 Warranty

Report any defects to the manufacturer immediately after 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.

2 Overview

WALL IE, the new Industrial Ethernet Bridge and Firewall, simply integrates your machinery network into the higher-level production network. A packet filter protects the networks from unauthorized access. If identical IP address ranges are to be realized, WALL IE functions as a bridge.

The **NAT operating mode** serves the forwarding of the data traffic between various IPv4 networks. It enables the address translation via NAT and uses packet filters for the limitation of access to the automation network located behind.

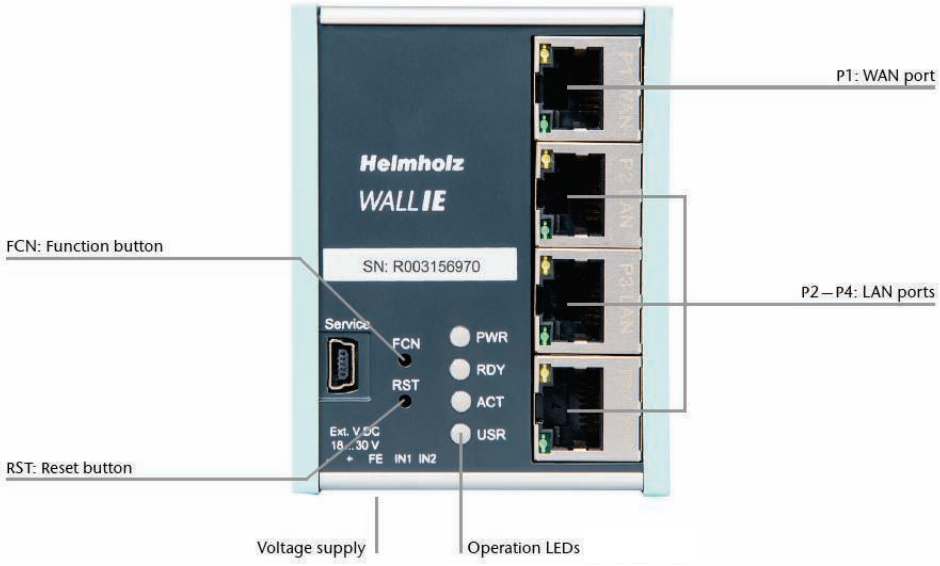
In the **bridge operating mode**, WALL IE acts as a layer 2 switch. In contrast with normal switches, however, packet filtering is also possible in this operating mode. This means that the restriction of access to individual areas of your network can be achieved without having to use different networks for this purpose.

WALL IE features:

- Bridge functionality for identical IP address ranges
- NAT (Basic NAT, NAPT and port forwarding)
- Access restriction through packet filters: IPv4 addresses, protocol (TCP/UDP), ports
- MAC addresses, black and whitelisting
- 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

2.1 Setup

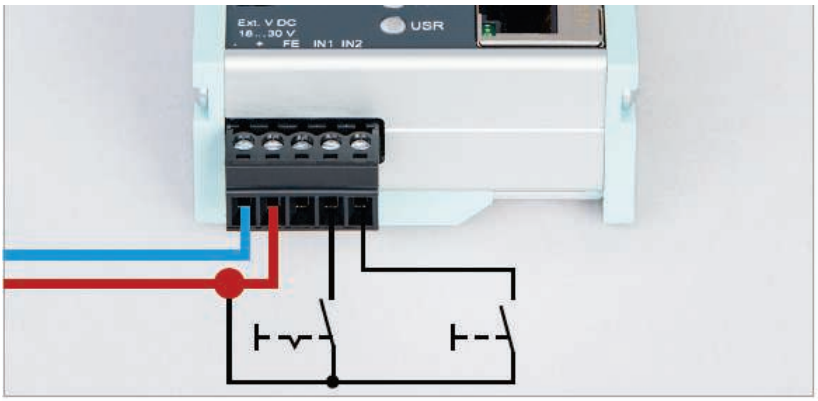
The WALL IE has a 100 Mbps WAN port (P1) and three 100 Mbps LAN ports (P2-P4) that have been switched.



A reset to factory settings can be initiated with the function button (FCN) (see ch. 11). The reset button (RST) initiates a restart of the WALL IE.

2.2 Connection of the power supply

The WALL IE is connected with 24 V DC voltage via the 5-pin power supply socket. There is also a connection for the functional ground (FG). The connection of a functional ground is recommended.



The inputs IN1 and IN2 do not yet have a function in the current firmware version, but will be available in a later firmware version for the external switching of firewall rules.

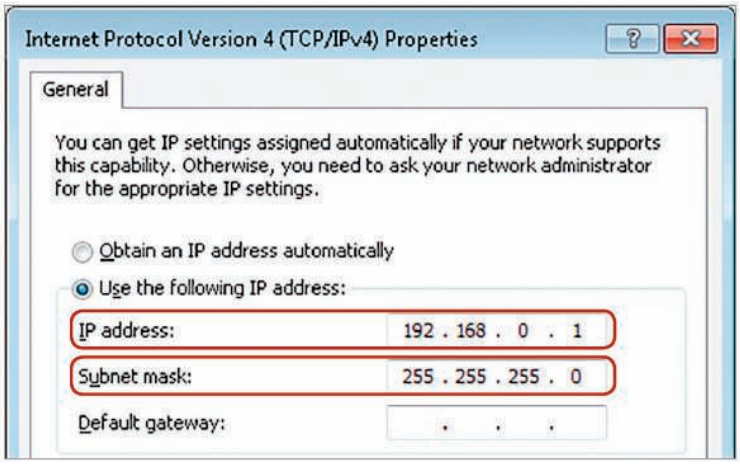
2.3 LEDs status information

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	Data transfer permitted between WAN and LAN.
USR	On	Factory settings reset active.
RJ45 LEDs	Green (Link)	Connected
	Orange (Act)	Data transfer at the port

3 Initial access to the web interface

The WALL IE is set on the LAN-side at the factory with the IP address 192.168.0.100 and the subnet mask 255.255.255.0. Access to the web interface is only possible via the LAN connections P2—P4.

The IP address of your network adapter must first be set in accordance with the IP subnet of the WALL IE:
Start → control panel →
Network and sharing settings →
Adapter settings →
LAN connection properties →
Internet Protocol Version 4



Now connect a patch cable with the LAN connection of your PC and one of the LAN ports P2- P4 of the WALL IE.

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

NOTE

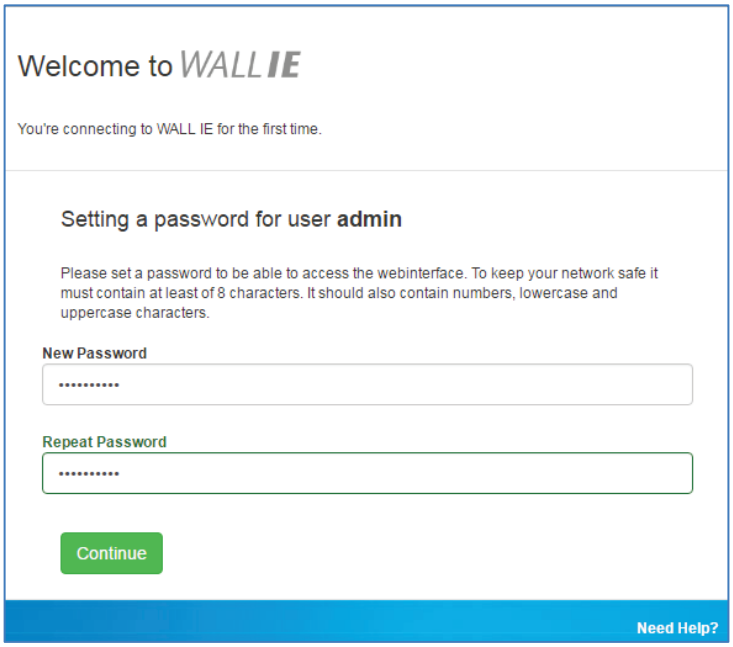
For security reasons, the web interface can only be reached through a secured HTTPS connection. An exception rule needs to be confirmed once in order to reach the website. A certificate for the connection authentication can be stored in the "Device/HTTPS" menu.

3.1 Initial Login

You will be prompted to set a password at the initial Login.

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". Additional user management hasn't been implemented yet.

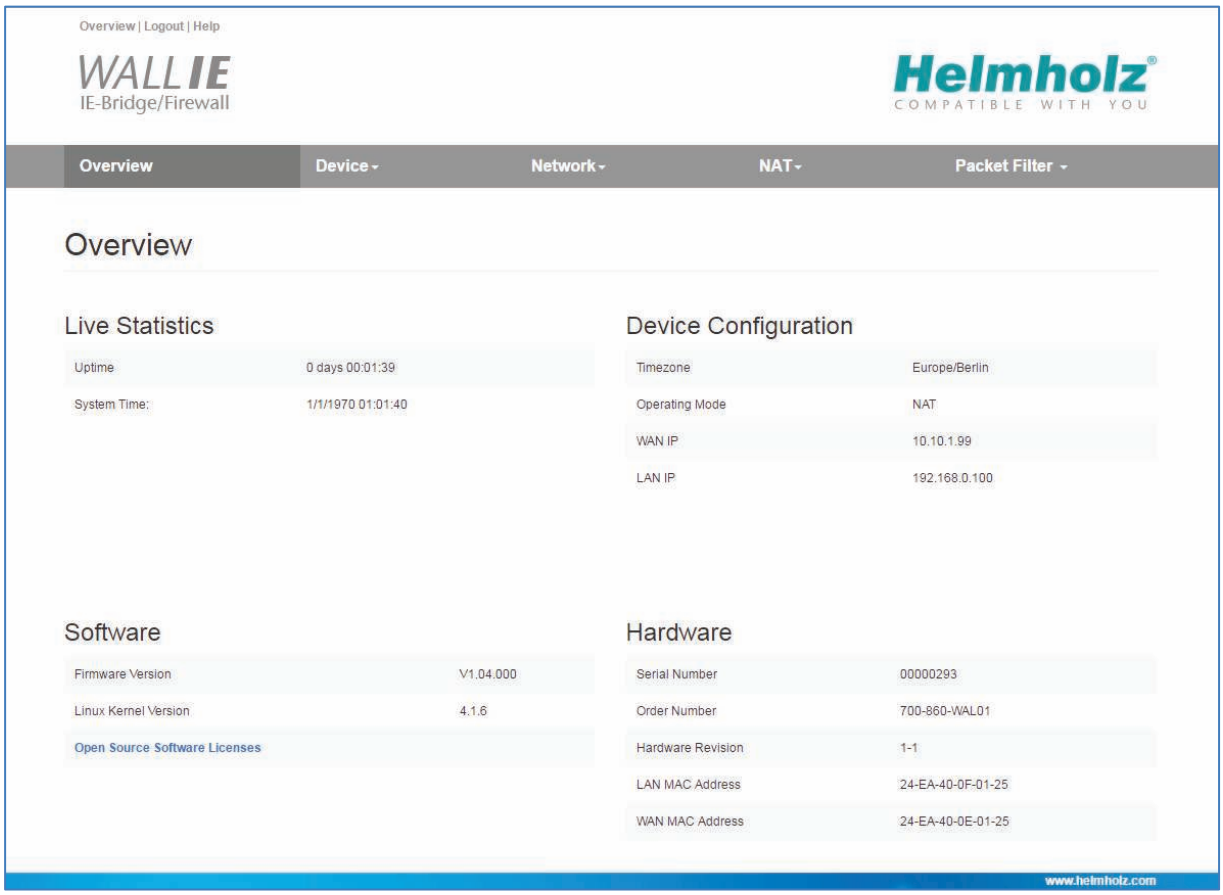


ATTENTION

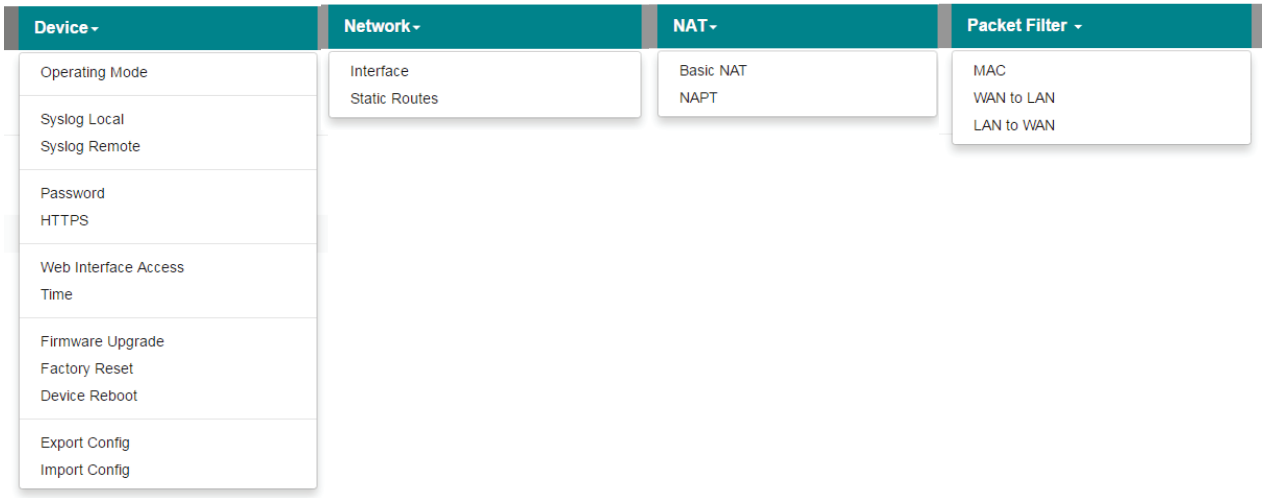
Please note the password well! For security reasons there is no possibility to reset the password without resetting the device to the factory settings.

3.2 Main view

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.



3.2.1 Menu overview



3.2.2 Responsive design

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

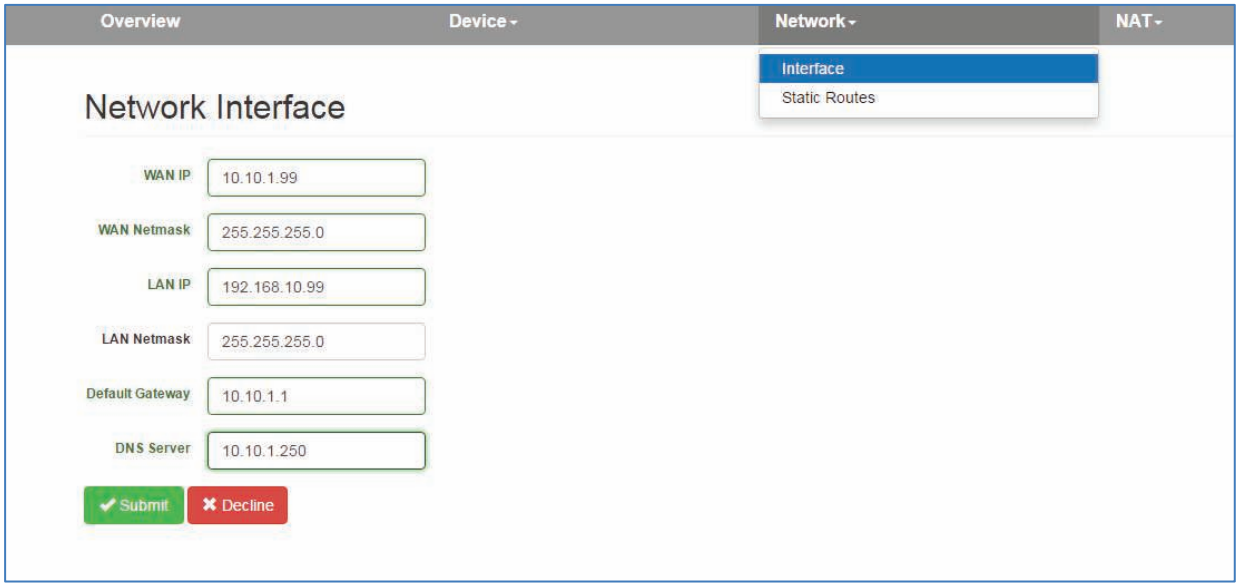
NOTE

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.

3.3 Adjustment of the IP addresses (Network interface)

Click on the "Network" menu and select the sub-menu "Interface".

The desired IP addresses for LAN and WAN and the related subnet masks (LAN/WAN net mask) can be defined here.



The default gateway is necessary when devices from the LAN wish to establish a connection with the Internet or when devices from the LAN should communicate with other networks via WAN. If this is not permitted or is not desired, "0.0.0.0" is to be entered.

A DNS server can also be indicated where necessary. It is necessary to indicate a DNS server for the SNTP service (see ch. 10.6).

The entry is saved with the "Save" button and the IP addresses are activated immediately. The current entry is rejected without acceptance with "Decline."

ATTENTION

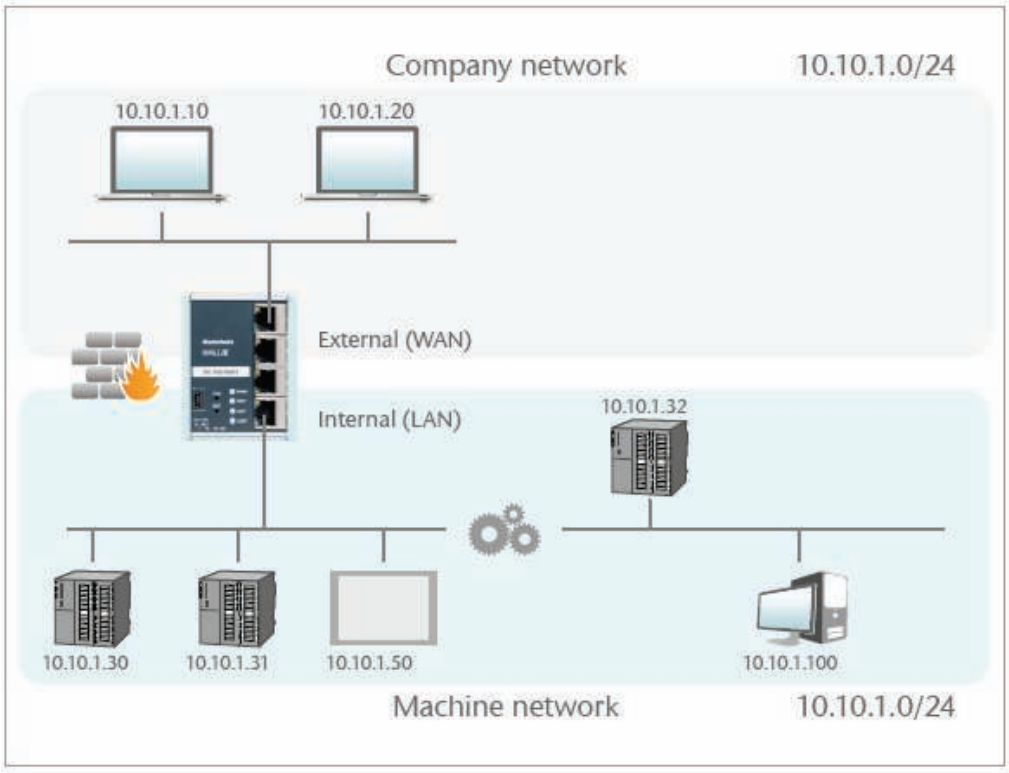
When you change the LAN IP address, you may need to reopen the website of the WALL IE in the browser under the new IP address and log in again.

NOTE

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

4 The bridge mode

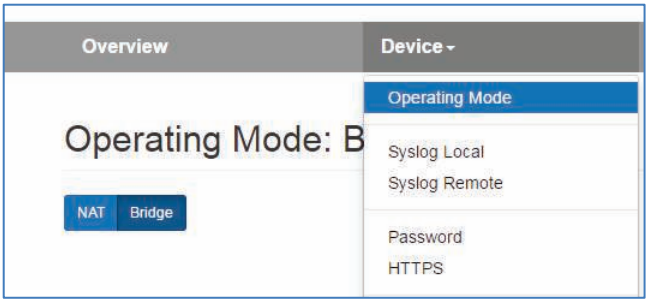
In the bridge operating mode, WALL IE behaves like a layer 2 switch between the automation cell (LAN) and the production network (WAN). The packet filter can be used to limit access between the two areas. This enables the separation of a part of the production network without using different network addresses.



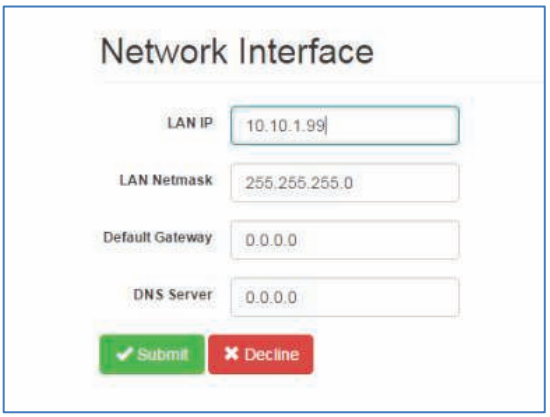
4.1 Activate bridge mode

Switch the WALL IE to the bridge mode via "Device → Operating Mode → Bridge."

In the bridge mode, the IP address of the WAN interface is identical to the IP address of the LAN interface. It is thus transparent.



When setting the IP addresses of the WALL IE under "Network → Interface," only one IP address can be set in the bridge mode as a result:



ATTENTION

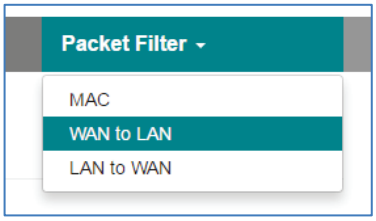
In the bridge mode, all ports are blocked for "WAN-to-LAN" data transfer as a default!

In order to enable access, packet filter rules must be created or the default action for the packet filters be set to "Accept".

The "LAN to WAN" data transfer is initially always allowed, but can also be limited by packet filters or the default action.

5 Packet filter functionality

The packet filters define the of access between the production network (WAN) and the automation cell (LAN) in both directions. For example, it can be configured that only certain participants from the production network may exchange data with defined participants from the automation cell.



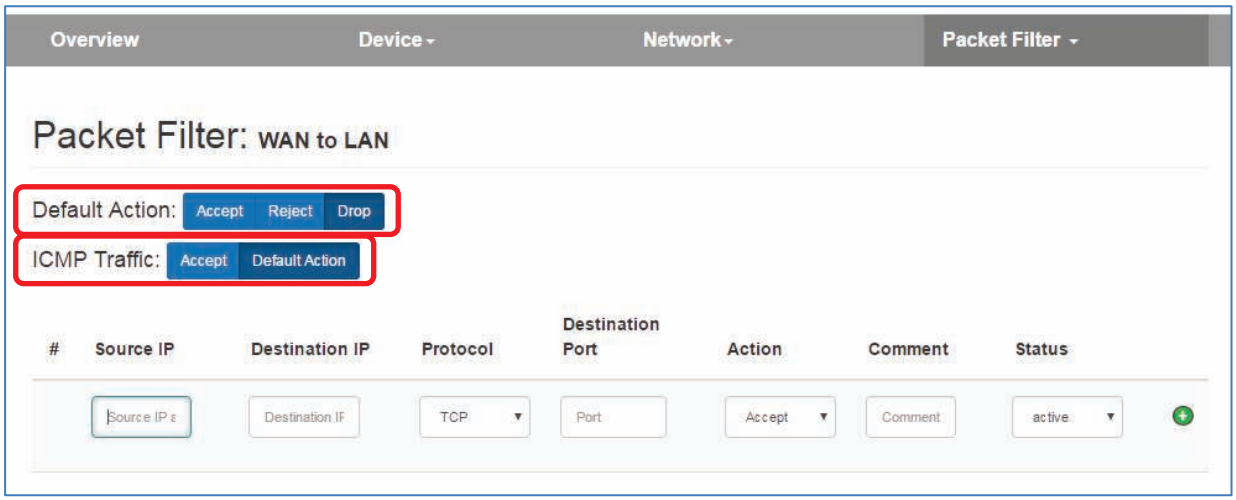
The following filter criteria on layers 3 and 4 are available:

- IPv4 addresses
- Protocol (TCP/UDP)
- Ports

The packet filters are available in both the "WAN to LAN" direction and in the direction "LAN to WAN".

5.1 Creation of rules in the packet filter

In the "Packet Filter" menu, select "WAN to LAN" or "LAN to WAN", depending upon which communication direction you wish to restrict.



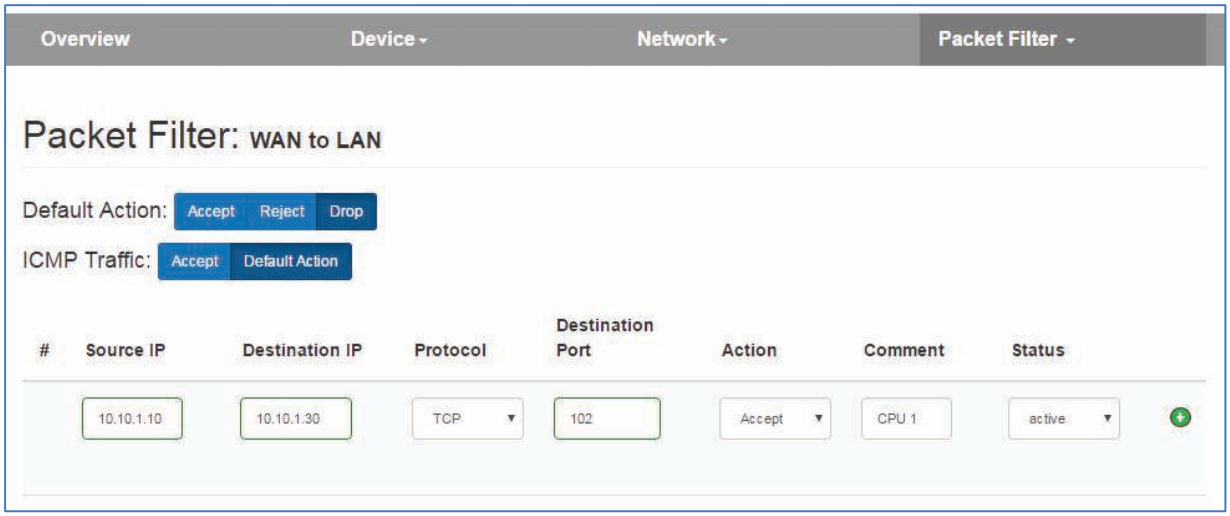
With the "**Default Action**" option you can set how the standard action of the packet filter should work.

In the "Accept" setting, all frames are generally permitted and only special packets are filtered.

In the "Reject" or "Drop" settings, all frames are generally prohibited and only the frames indicated in the filter rules are accepted. "Reject" hereby rejects frames with an error message. "Drop" rejects frames without error messages.

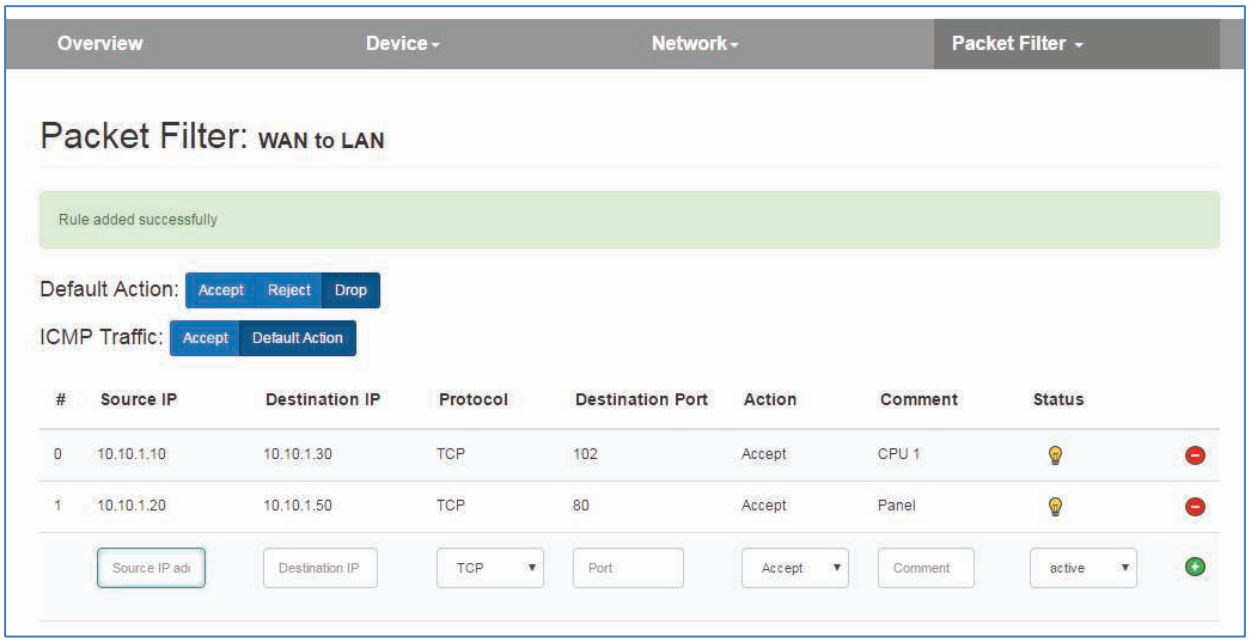
Whitelisting can be realized with "Accept," blacklisting with "Reject" or "Drop."

With the option "**ICMP Traffic**", you can allow the passage of ICMP packets - e.g. a "Ping".



A new rule is entered with the  symbol.

In the example above, a PC in the WAN network with the IP address 10.10.1.10 (e.g. visualization) is now allowed access to the CPU 10.10.1.30 in the LAN network via port 102 with the TCP protocol.

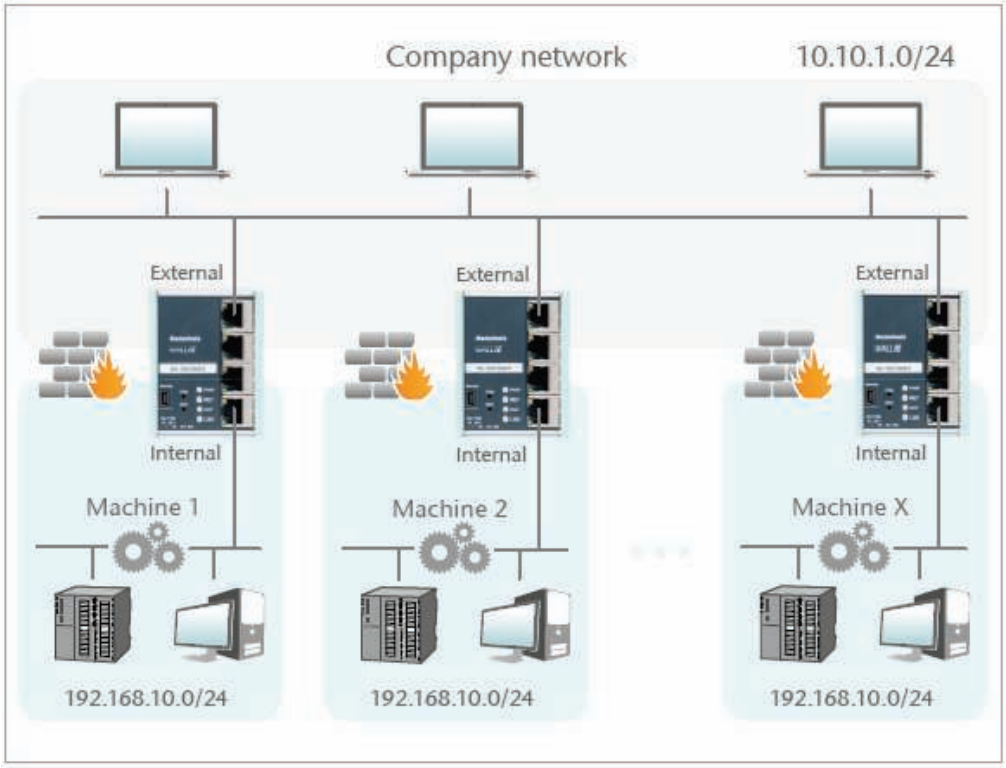


Source IP	IP address of the device in the external network (WAN) from which the query originates.
Destination IP	IP address of the device in the internal network (LAN) on which access is allowed by this rule.
Protocol	Selection of the permitted protocol, TCP or UDP.
Destination port	The device port to be reached in the internal network.
Action	Packages from the external network (WAN) can be accepted ("Accept") or rejected ("Reject" / "Drop"). "Drop" rejects a packet mutely and "Reject" provides an ICMP error message.
Comment	A comment on the rule can be entered here.
Status	Rule active (A click on the lamp changes the status)
	Rule active (A click on the lamp changes the status)
	Deletes a rule
	Adds a rule

6 NAT operating mode

When several automation cells with the same address range are to be incorporated into a production network, this can result in collisions, as the addresses in the entire network are not unambiguous.

Using Network Address Translation (NAT), WALL IE makes it possible to incorporate several automation cells into the production network.

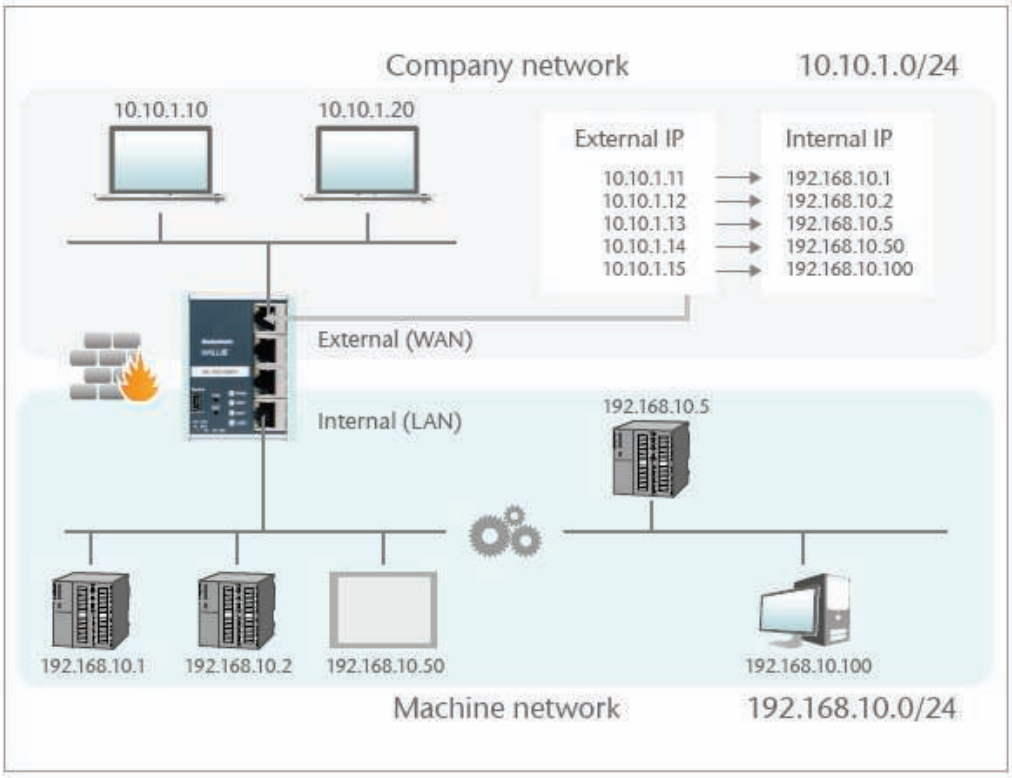


In the NAT operating mode, WALL IE forwards the data transfer between various IPv4 networks (Layer 3) and exchanges the IP addresses with the help of NAT. The packet filters and MAC addresses white/blacklisting can also be used to check the data traffic.

6.1 Basic NAT

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

The "External IP" must be a free or unused IP address in the WAN network. The "Internal IP" is the IP address of the device in the LAN that is assigned to the "External IP" in the WAN. Translation takes place at the IP level and all ports can be addressed. Access can be limited to certain ports by entering packet filter rules.



ATTENTION

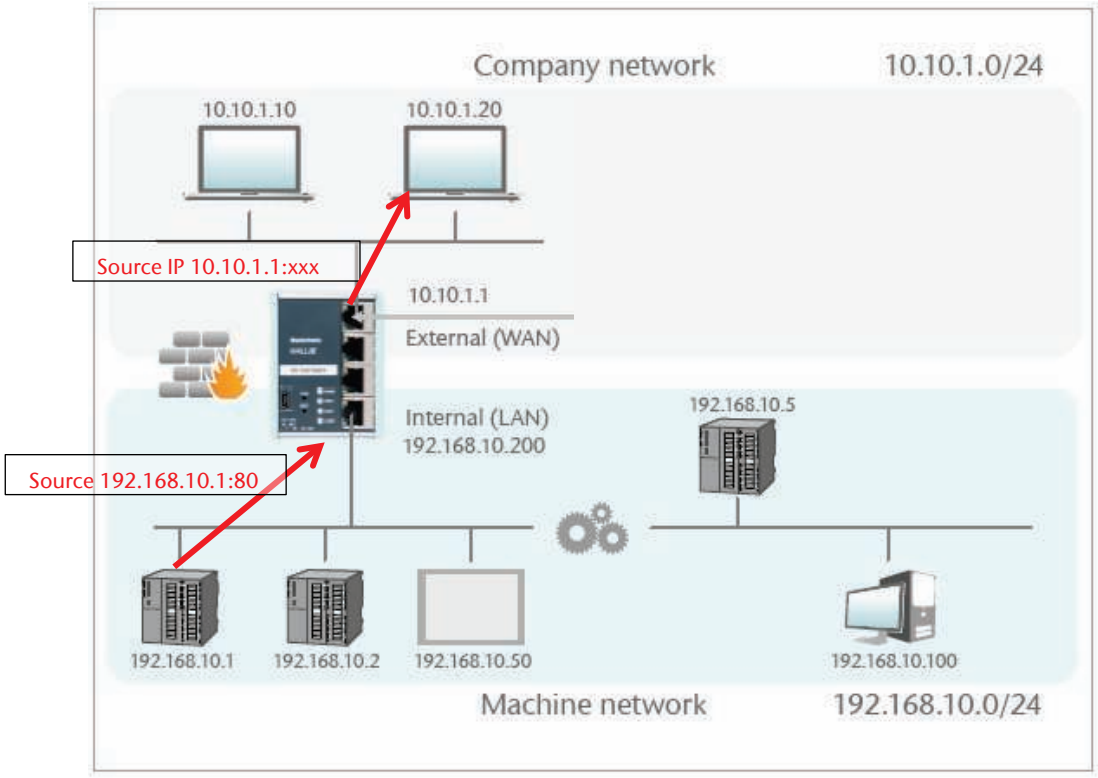
When defining a "Basic NAT" rule, all ports for "WAN to LAN" data transfer are initially blocked for data transfer!

In order to enable access, packet filter rules must be created or the default action for the packet filters be set to "Accept".

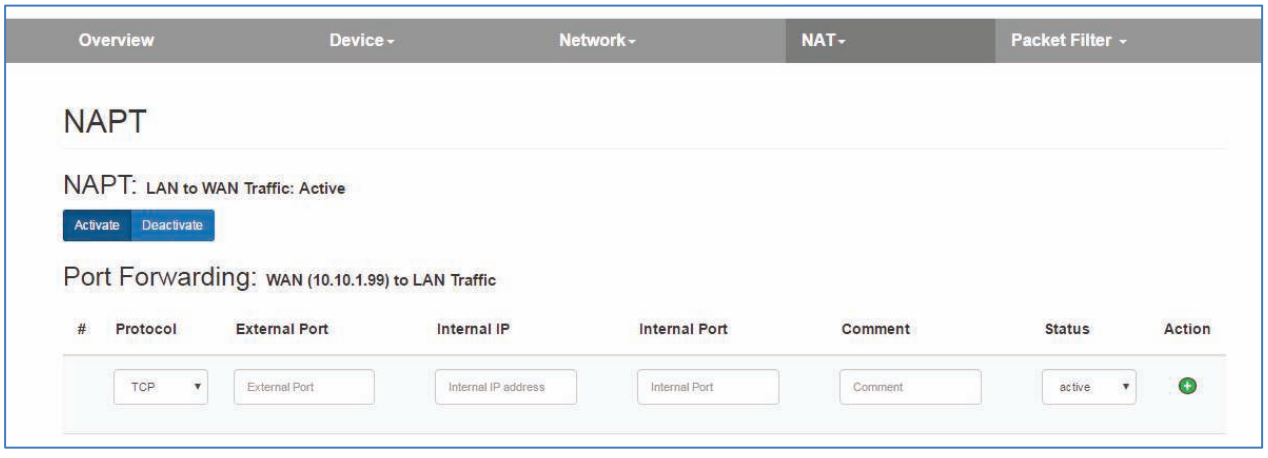
The "LAN to WAN" data transfer is initially always allowed, but can also be limited by packet filters or the default action.

6.2 NAPT

"NAPT for LAN to WAN traffic" replaces the sender addresses of queries from the LAN through the address of the WALL IE in the WAN. NAPT is also referred to as "Port Address Translation" (PAT).



The option "**NAPT: Active**" thus enables communication of devices from the LAN with devices in the WAN. WALL IE thereby acts as a gateway to manage the exchange of the IP addresses of the WAN network and also looks after the assignment of the response.



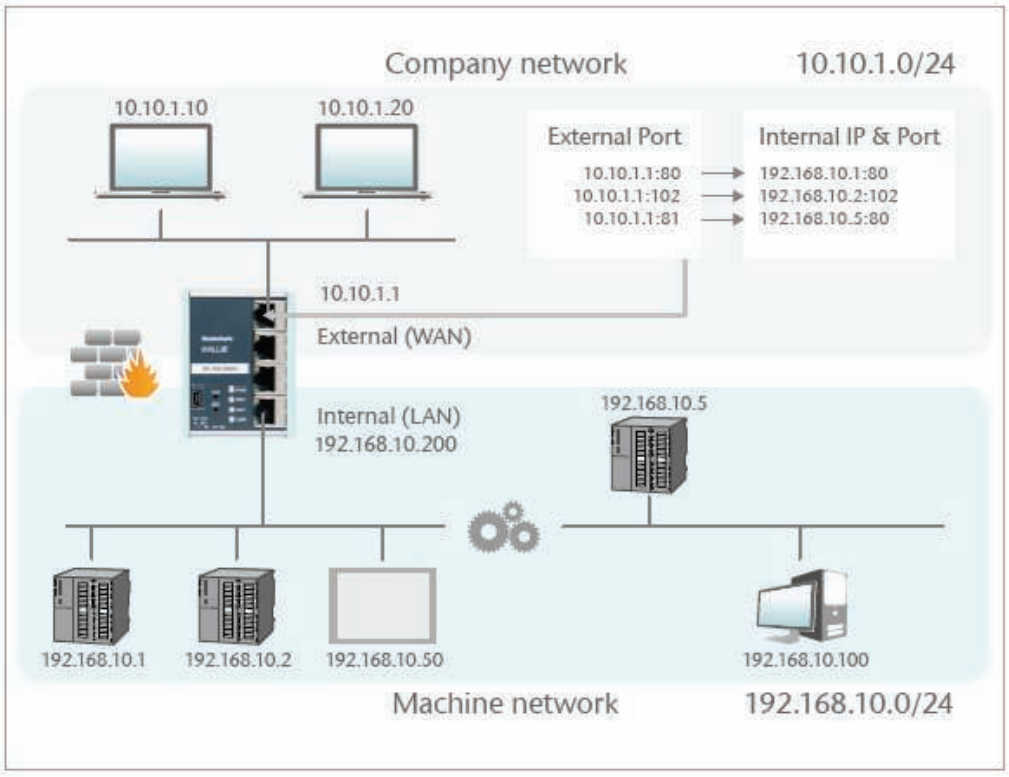
ATTENTION

In order that the communication with activated NAPT from the LAN to WAN functions, the LAN address of the WALL IE must be entered into the devices in the LAN as a gateway!

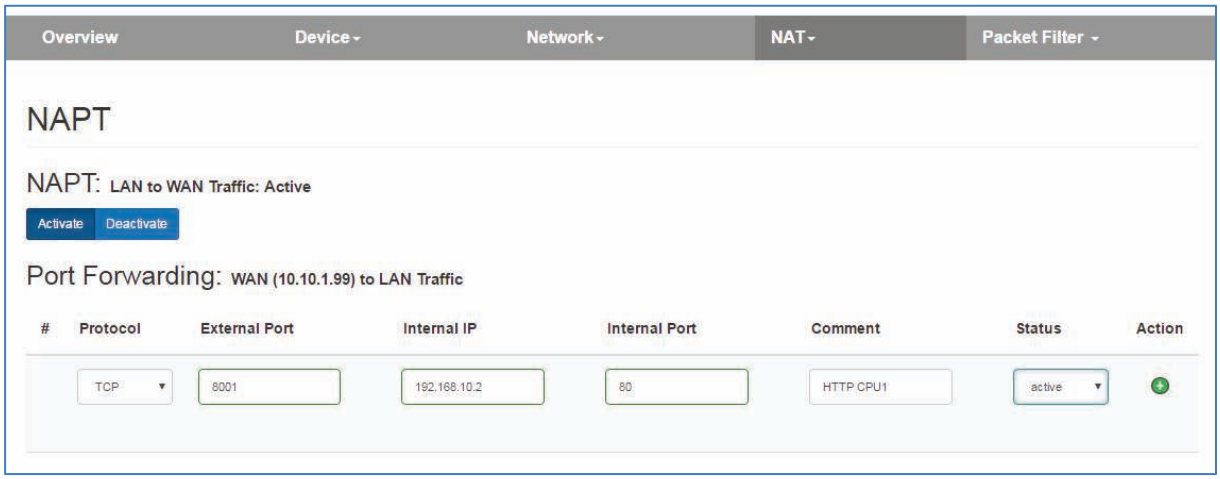
If the **NAPT** option is deactivated, the query packets from the LAN are forwarded from the LAN to the WAN with their original sender IP and sender port. In this configuration, however, no answer frame can be sent back from the WAN to the LAN.

6.3 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.



In the following example, the website (Port 80) of the CPU can be reached with the IP 192.168.10.2 via WAN through access to IP 10.10.1.99 with Port 8001.



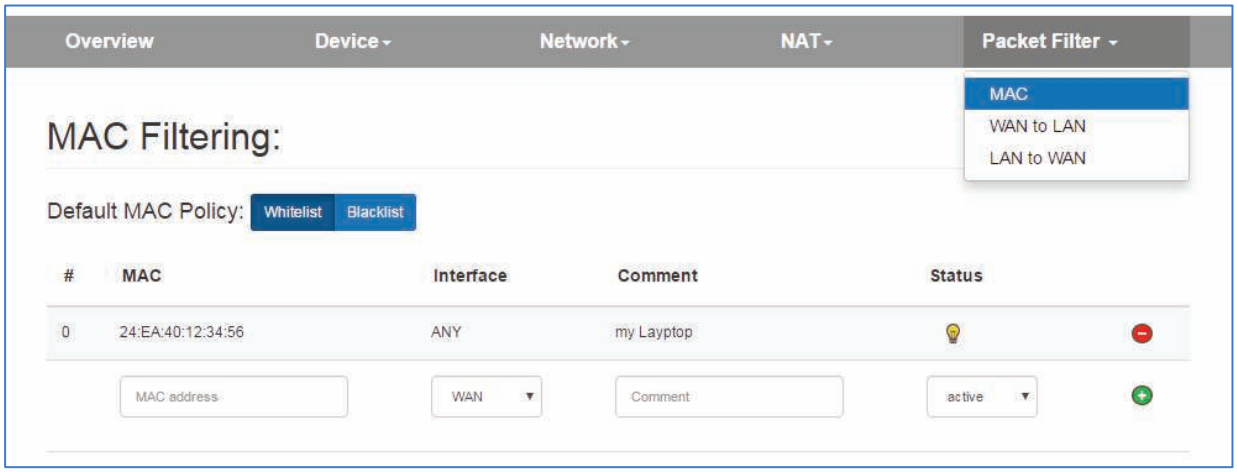
If with the packet filters "WAN to LAN" the default action is set to "Reject" or "Drop", the corresponding filter rules for access must also be created for each port forwarding entry.

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 10.4).

7 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").

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



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

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

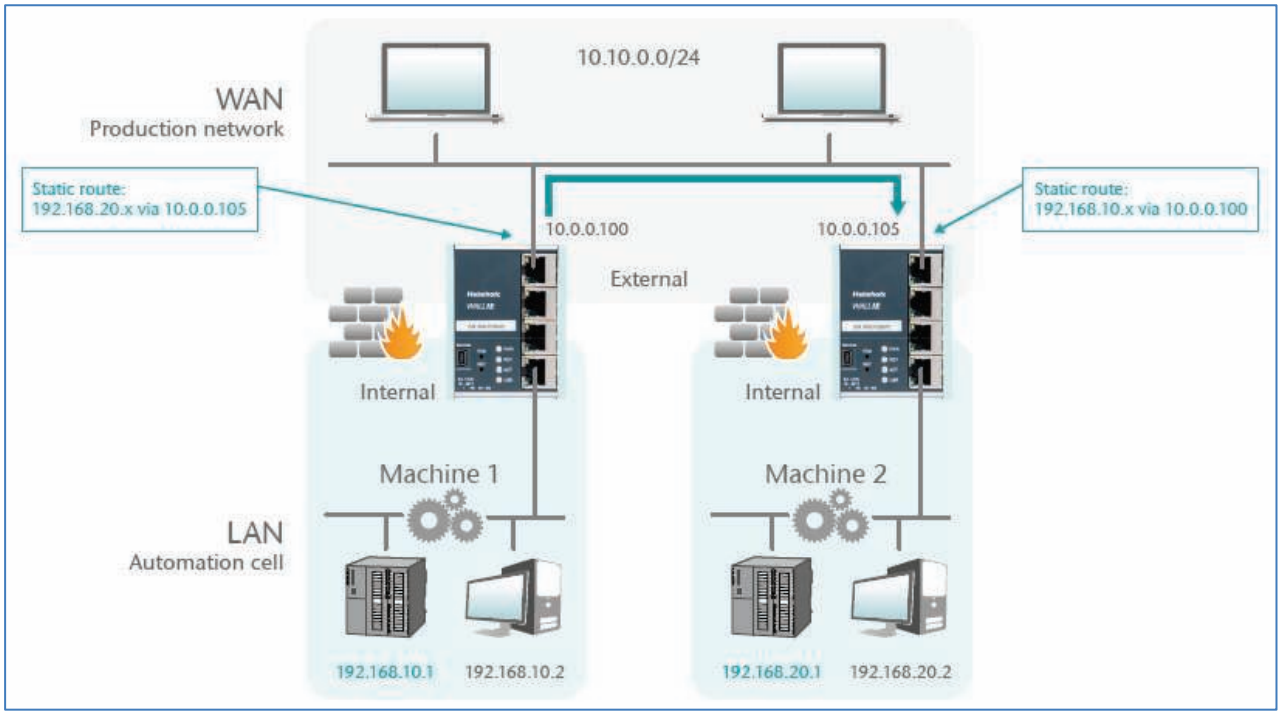
NOTE

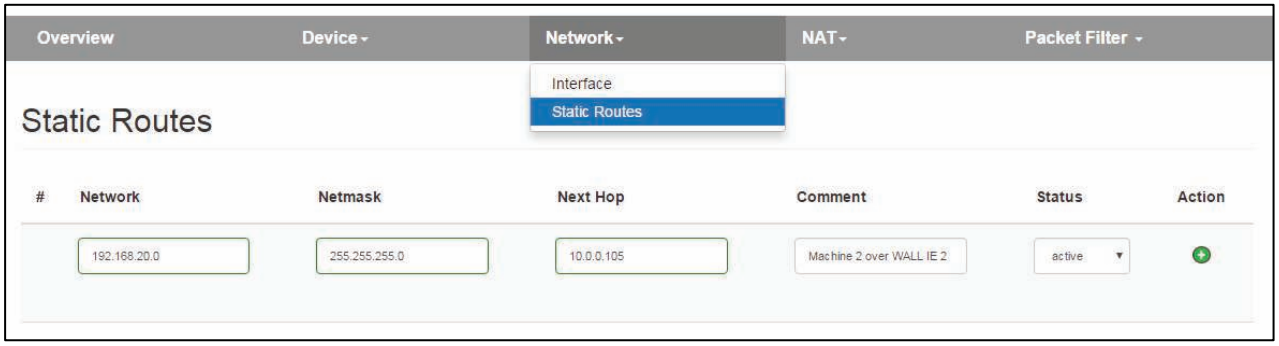
In the NAT mode, the MAC filtering is only carried out if the MAC address is also indicated in the IP header of the packet. Layer 2 frames are not forwarded in the NAT mode.

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

8 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

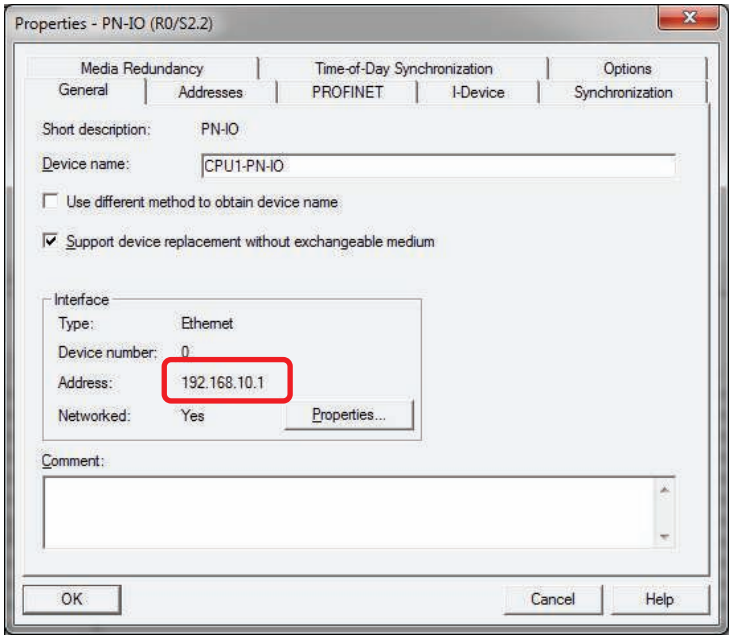
In order to enable the return route of the answer, a route for the IP address of the WALL IE of machine 1 must be set up in the second gateway!

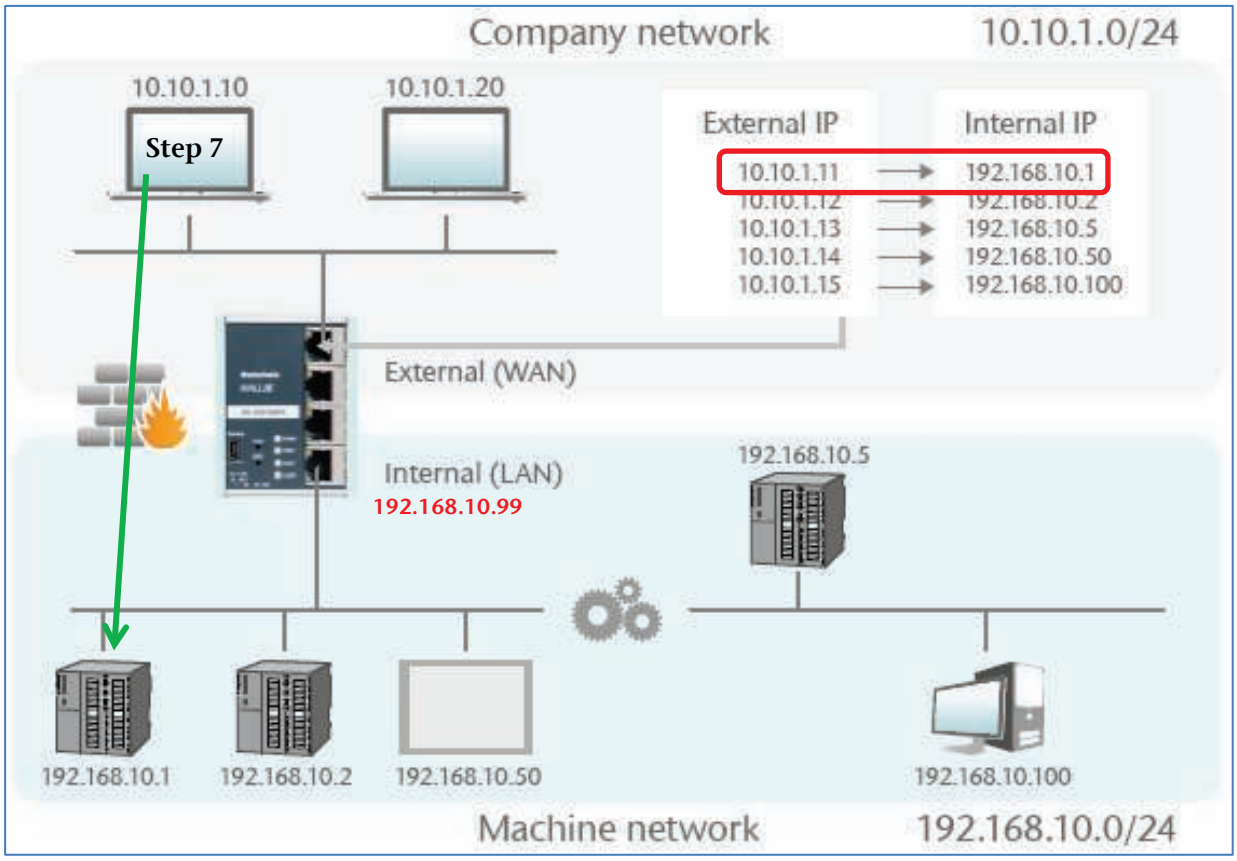
9 Use with Simatic Step 7 / TIA portal

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 an adapted form for other applications.

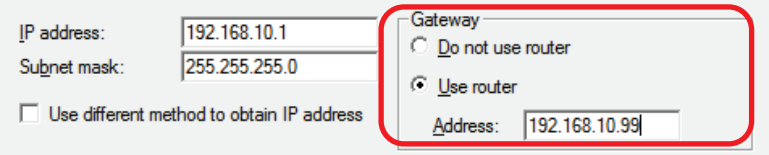




9.1 Solution in Step 7

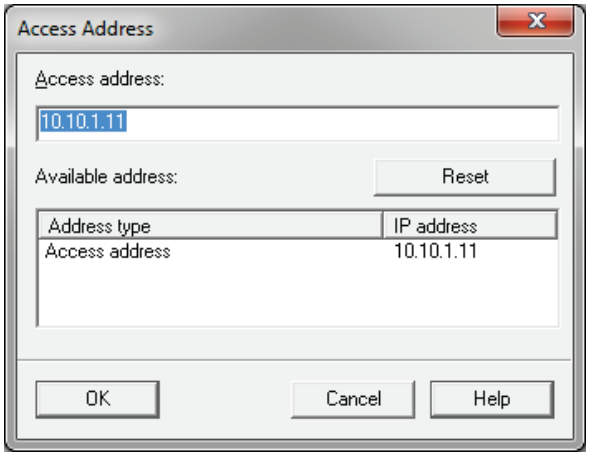
Step 7 offers the possibility to access a CPU and to use an IP address other than that set in the project.

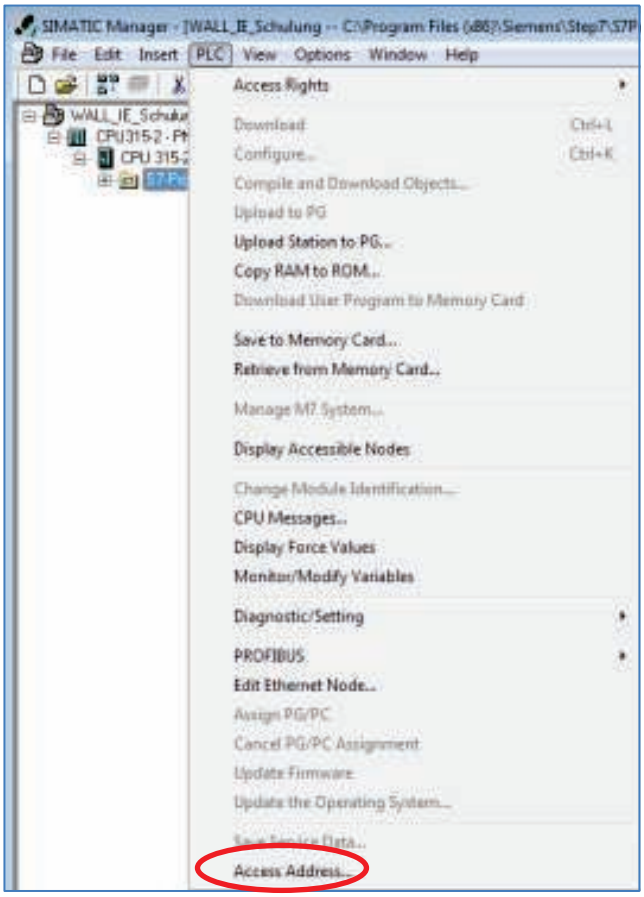
However, in order that the responses from the CPU can also be redirected back to the engineering station in the WAN via the WALL IE, the WALL IE must be entered as the router for the CPU in the project.



In order to be able to reach a CPU via an alternative IP address, this can be entered in the menu "PLC" in the dialog "Access address."

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





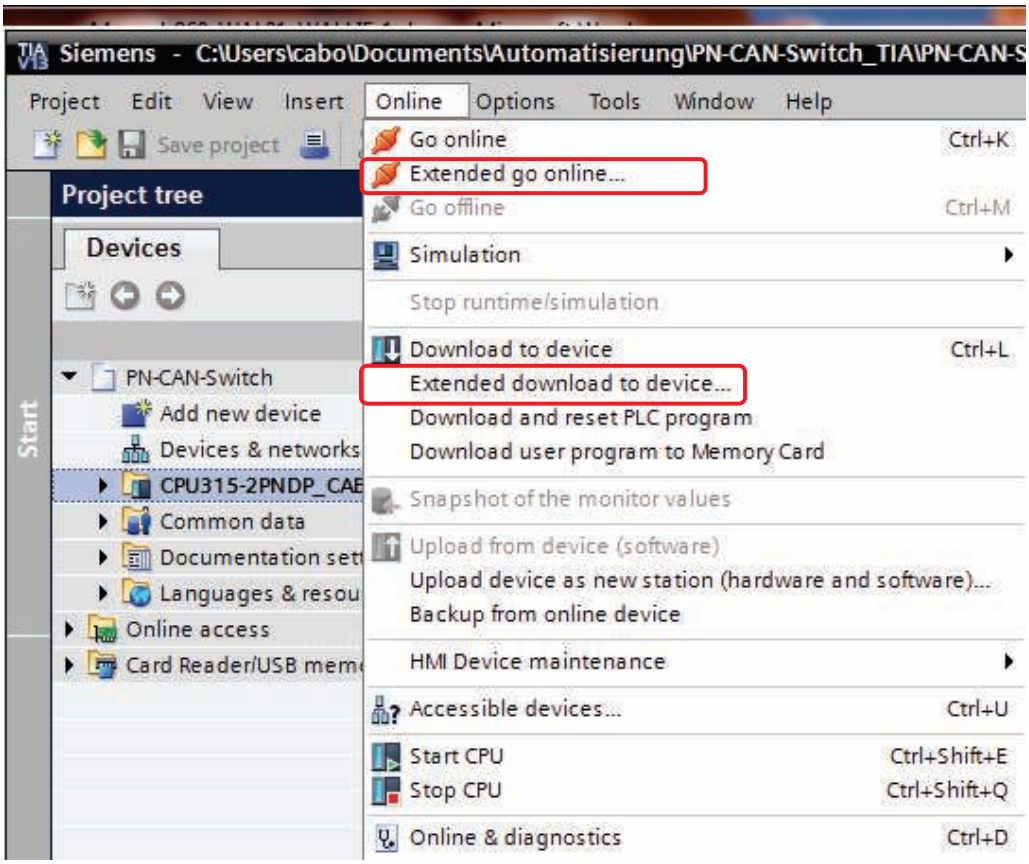
ATTENTION

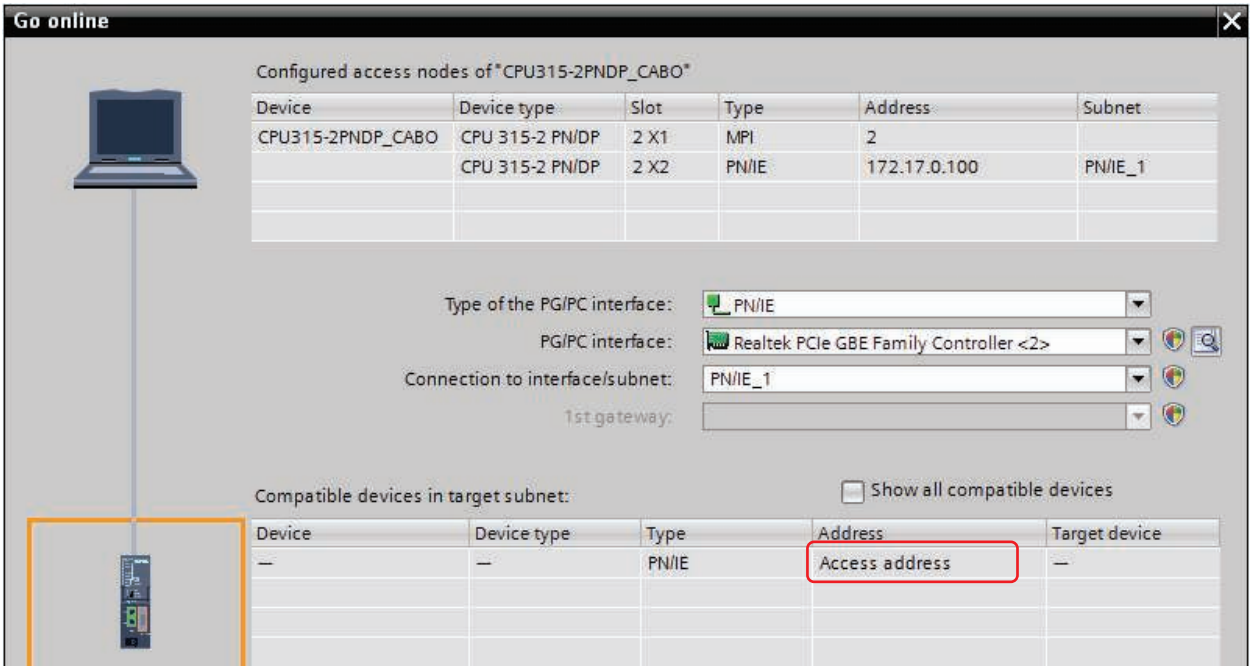
This solution can only be used in the Basic NAT operating mode. In the case of NAPT with port forwarding, only one CPU can be reached, as the Simatic Manager always accesses the CPU with the non-adjustable port 102.

The search via the Siemens function "Accessible nodes" doesn't function through the WALL IE firewall.

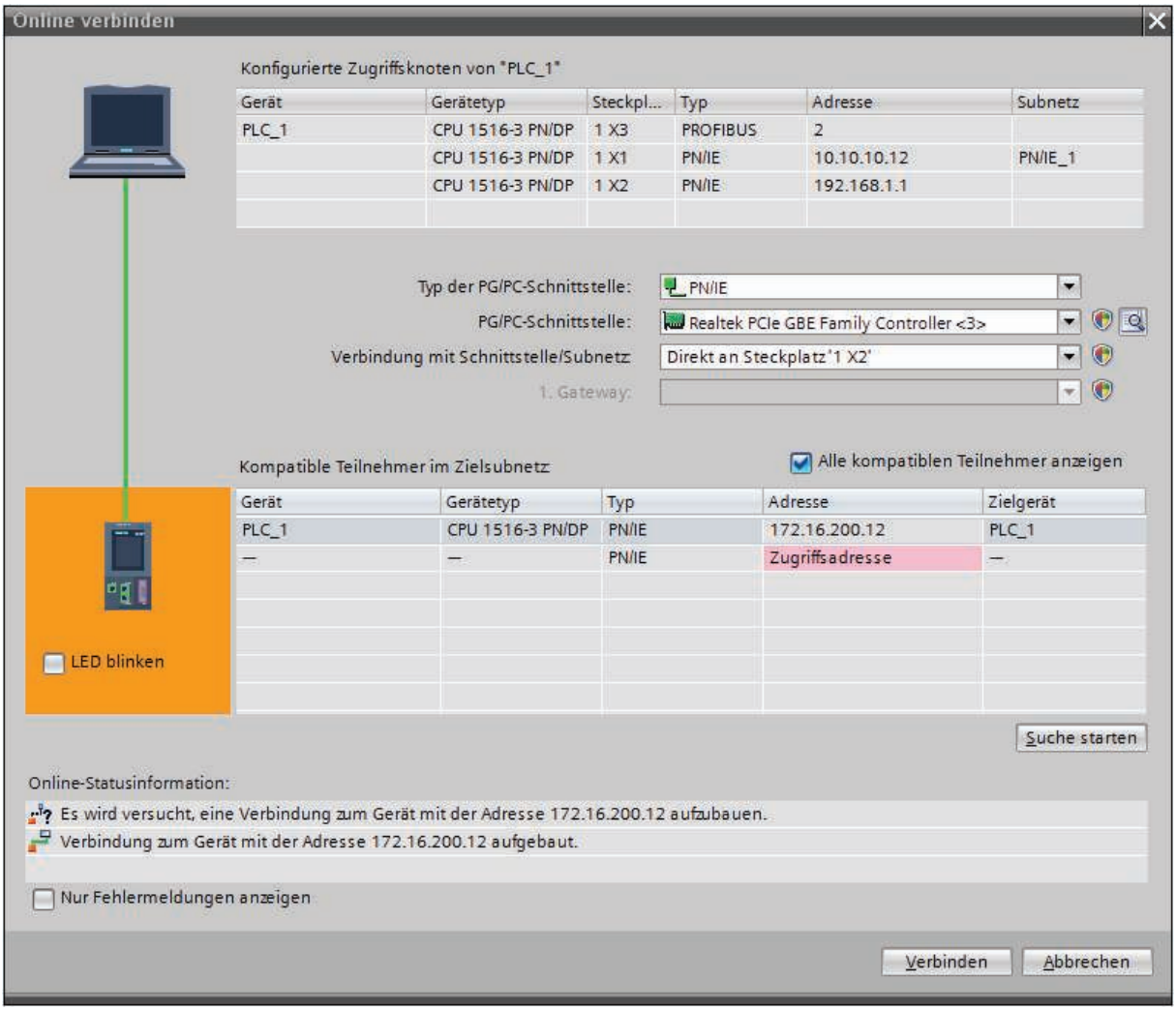
9.2 Use in the TIA portal

Here you use the function "Extended download to device" in the menu under "Online" or, where necessary, "Extended go online".





Click on "Access address" and enter the corresponding IP address. Confirm the entry by clicking on the window. An attempt is now made to establish a connection with the entered IP address.



ATTENTION

This solution can only be 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/ TIA portal always accesses the CPU with the non-adjustable port 102.

The search via the Siemens function "Accessible nodes" doesn't function through the WALL IE firewall.

9.3 Setting up a route on the PC

A Windows-PC can also be informed of the assignment of the LAN IP address to a WAN IP address as a "route" in the operating system.

To this purpose, call up the command line "CMD" with administrator rights.

The operating system is informed of a route with the following command:

```
route add 192.168.10.1 mask 255.255.255.0 10.10.1.11 metric 1
```

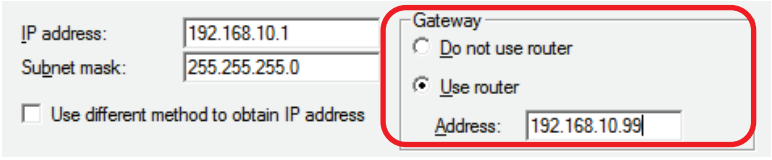
This command temporarily saves the route until the PC restart.

Use the following for permanent saving of the entered routes: `route add -p`

Display all routes: `route print`

Delete a route: `route delete 192.168.10.1`

However, in order that the responses from the CPU can also be redirected back to the PC via the WALL IE, the WALL IE must be entered as the router for the CPU in the project.



ATTENTION

This solution can only be used in the Basic NAT operating mode. This solution cannot be used with NAPT and port forwarding.

The search via the Siemens function "Accessible nodes" doesn't function through the WALL IE firewall.

10 Other functions

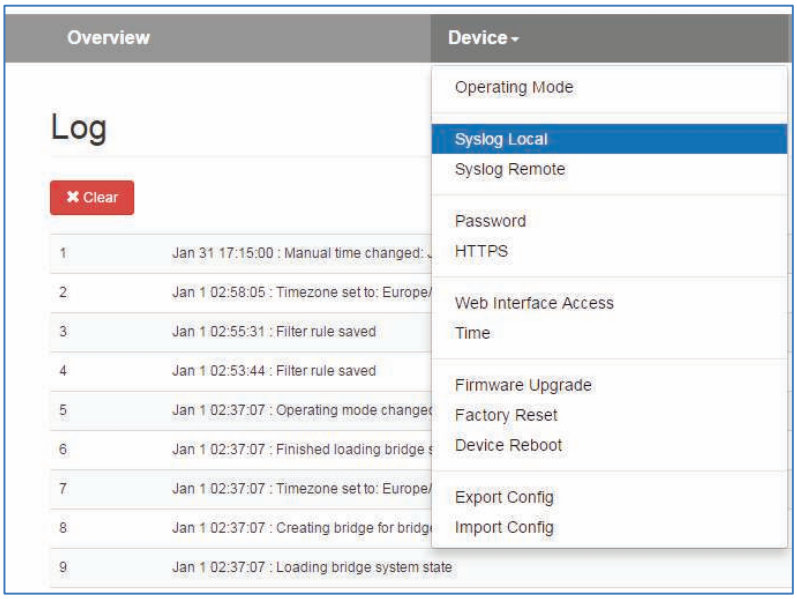
10.1 Syslog server

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. 10.5).

10.1.1 Syslog local

The local Syslog display lists the recorded events.

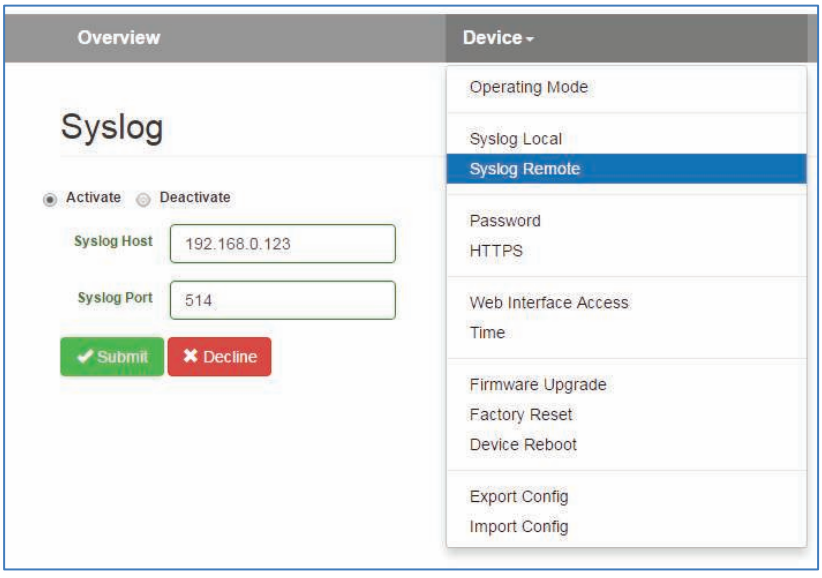
The Syslog memory can be deleted with "Clear".



10.1.2 Syslog remote

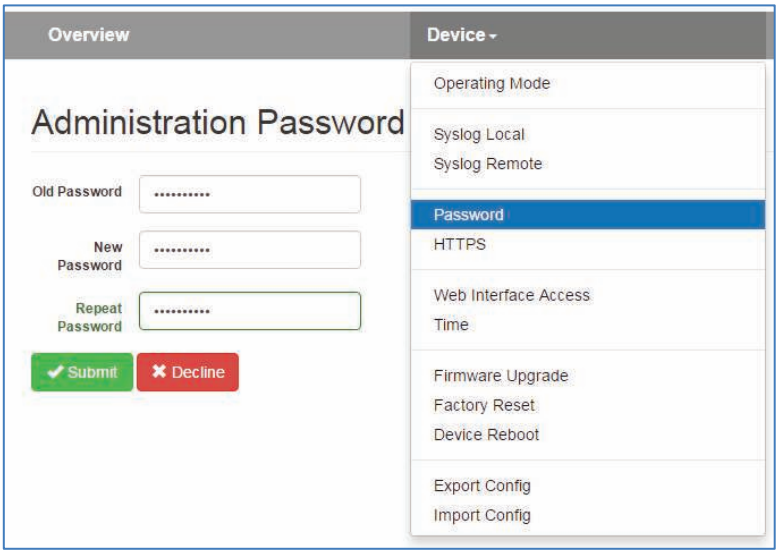
The Syslog messages can also be sent by the WALL IE to a PC through the network on which a program for Syslog recording is running.

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



10.2 Change password (Password)

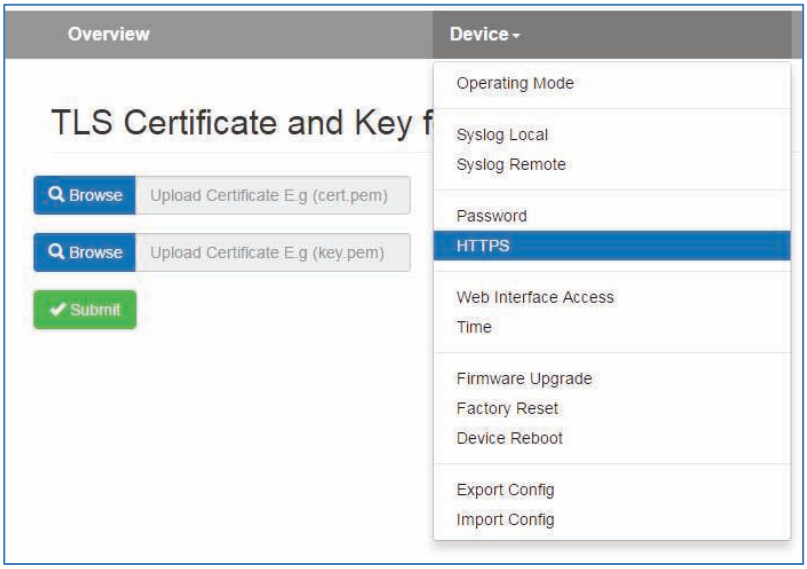
In the "Password" menu it is possible to change the password of the administrator "admin".



10.3 File certificate (HTTPS)

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

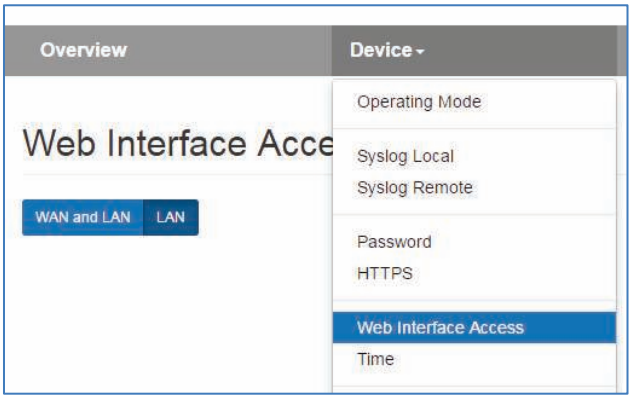
This ensures that the calling of the WALL IE configuration website, in addition to the HTTPS encoding, is also trustworthy.



10.4 Allow web interface access to WAN (Web Interface Access)

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

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



10.5 Firmware update

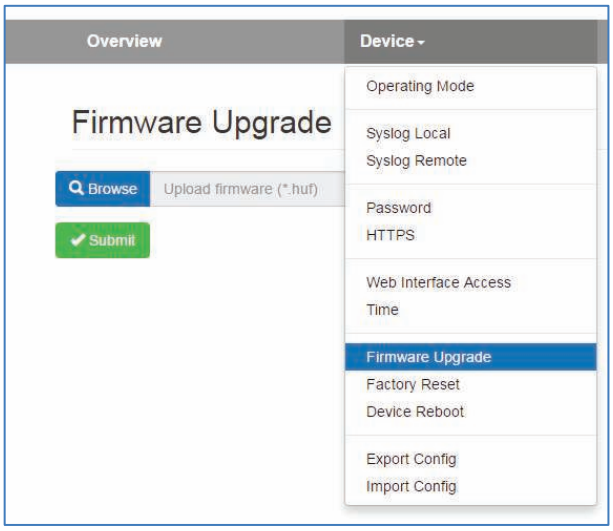
The firmware of the WALL IE can be very simply updated via the website.

You receive the firmware from the Helmholz website under www.helmholz.de or at Helmholz Support (support@helmholz.de).

The firmware comes with the file ending "HUF" and is encoded to protect you from a change.

File the firmware file on your PC and select the storage location with "Browse."

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 decoded and checked in the WALL IE. If the content is correct, the firmware is burned into the program memory and a restart of the WALL IE takes place.

ATTENTION

Operation of the WALL IE is interrupted during the update procedure.

Do not shut 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.

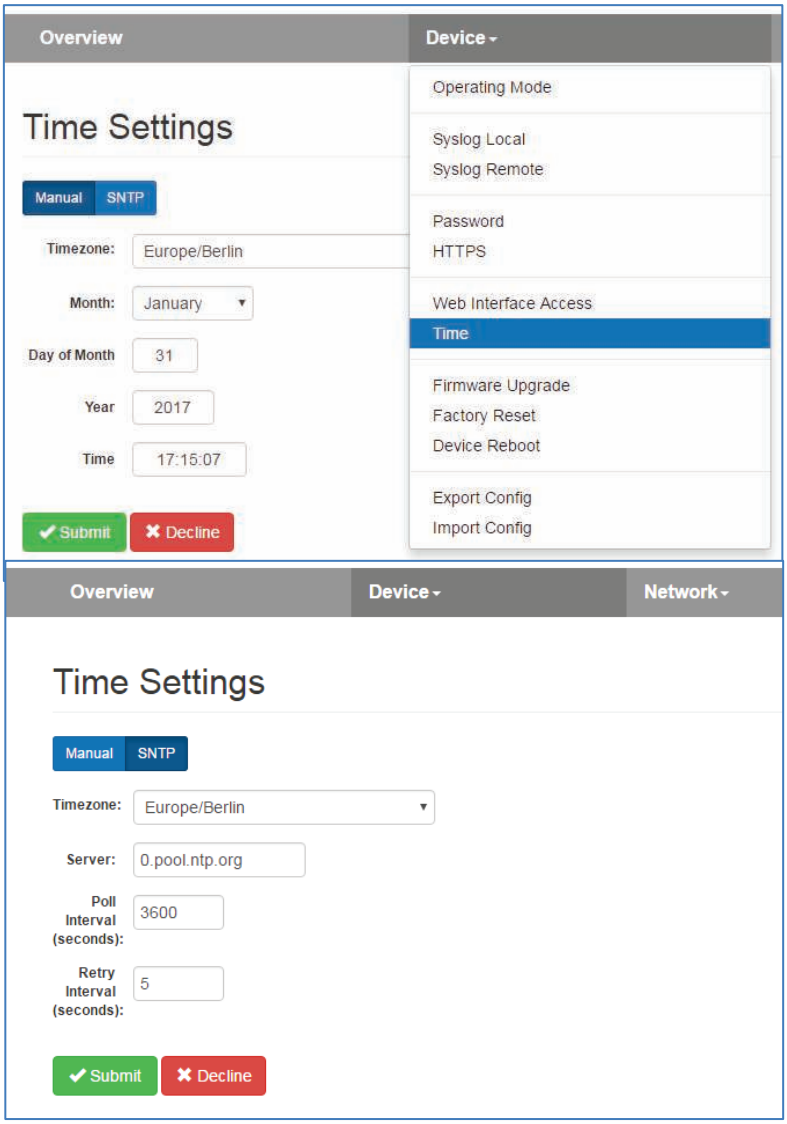
However, a "downgrade" to an older firmware version can lead to configuration errors. Carrying out a factory reset is recommended following a downgrade.

10.6 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").



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

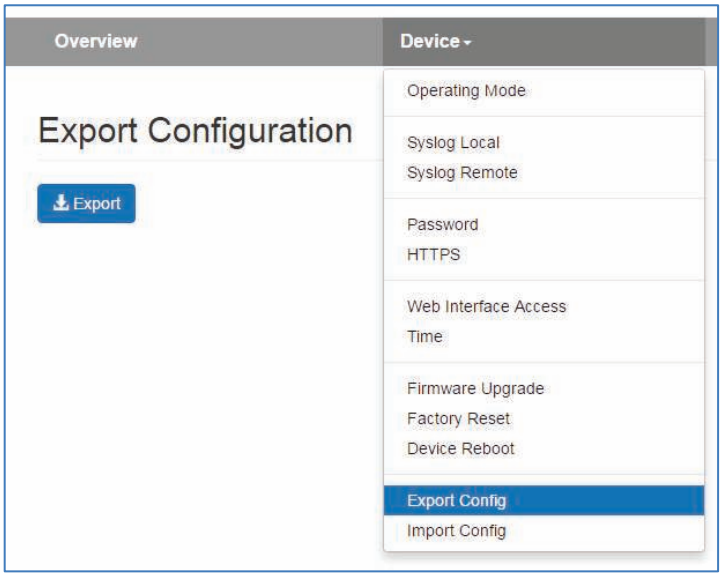
The default gateway and the DNS server must be configured in the Interface settings (see ch. 3.3) for "SNTP."

10.7 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 perform 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;
     ;
};
…
```

11 Resetting to factory settings

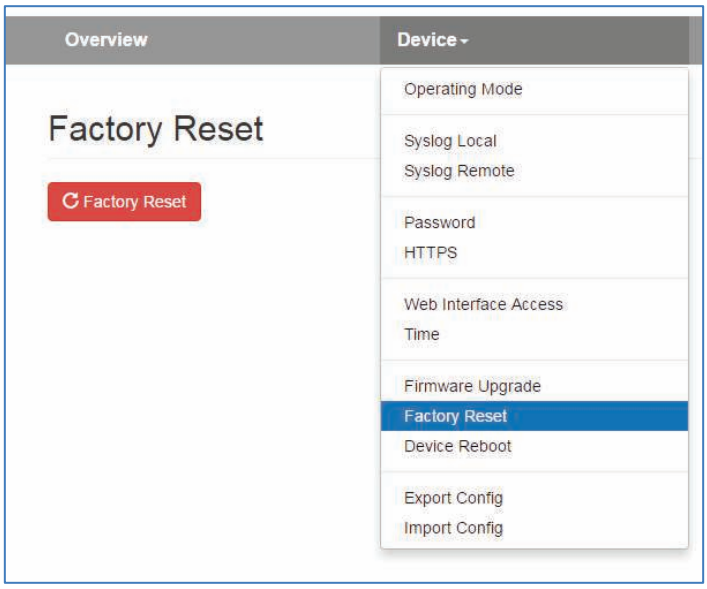
The resetting of the WALL IE to factory settings can be initiated both via the website and without access to the device with the "FCN" button.

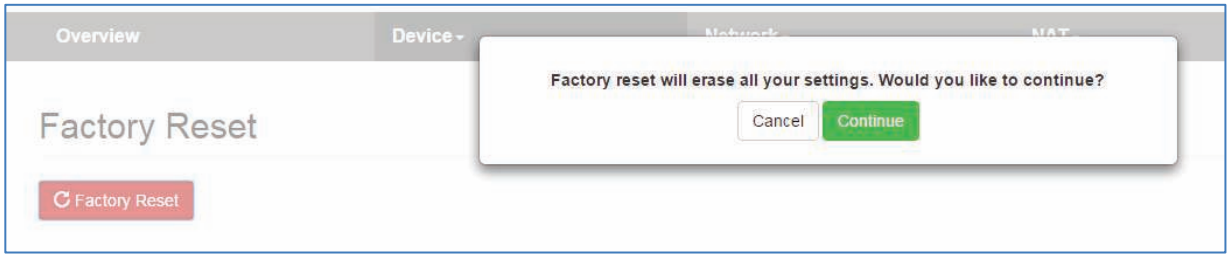
When resetting the WALL IE, the configuration is irretrievably deleted and the IP settings are set to the delivery status. The firmware remains at the current status in the process.

11.1 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.





11.2 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.

You can trigger a restart of the WALL IE with the "RST" button or switch the power off and on again.

12 Technical data

Order no.	**700-860-WAL01**
Name	WALL IE - Industrial Bridge and Firewall
Interfaces	1x WAN 10/100 Mbps
	3x LAN 10/100 Mbps, switch
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)
Voltage supply	DC 24 V (18 ... 30 V DC), SELV and limited energy circuit
Current draw	Max. 250 mA with DC 24 V
Dimensions (D x W x H)	35 mm x 59 mm x 75 mm
Weight	Approx. 160 g
Certifications	CE, UL
Noise immunity	DIN EN 61000-6-2 “EMC Immunity”
Interference emission	DIN EN 61000-6-4 “EMC Emission”
Vibration and shock resistance	DIN EN 60068-2-8:2008 “Vibration” DIN EN 60068 -27:2010 “Shock”
Protection rating	IP 20
Relative humidity	95% without condensation
Installation position	Any
Permissible ambient temperature	-40 °C to +75 °C
Transport and storage temperature	-20° C to 80° C

12.1 Dimensioned drawing