Helmholz
COMPATIBLE WITH YOU

WALL IE - Industrial NAT Gateway and Firewall

Manual

Version 6 | 4/8/20 | as of firmware V 1.08.400

Manual order number: 900-860-WAL01

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

Notes

All rights reserved, including those related to the translation, reprinting, and reproduction of this manual or of parts thereof.

No part of this manual may be reproduced, processed, duplicated, or distributed in any form (photocopy, microfilm, or any other methods), even for training purposes or with the use of electronic systems, without written approval from Helmholz GmbH & Co. KG.

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.

Copyright © 2020 by

Helmholz GmbH & Co. KG

Hannberger Weg 2 | 91091 Großenseebach

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

Windows is a registered trademark of Microsoft Corporation.

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

Contents

1 General 6

1.1 Target audience for this manual 6

1.2 Safety instructions 6

1.3 Note symbols and signal words 7

1.4 Intended use 8

1.5 Improper use 8

1.6 Installation 9

1.6.1 Access restriction 9

1.6.2 Electrical installation 9

1.6.3 Protection against electrostatic discharges 9

1.6.4 Overcurrent protection 9

1.6.5 EMC protection 9

1.6.6 Operation 9

1.6.7 Liability 9

1.6.8 Disclaimer of liability 10

1.6.9 Warranty 10

1.6.10 Recycling / WEEE 10

2 Security recommendations 11

3 Overview 12

3.1 Setup 12

3.2 Connection of the power supply 13

3.3 LEDs status information 13

4 Initial access to the web interface 14

4.1 Initial registration 15

4.2 Main view 16

4.2.1 Menu overview 17

4.2.2 Responsive design 17

5 Choosing the operating mode 18

5.1 The NAT operating mode 18

5.2 The Bridge operating mode 19

6 Application case NAT 20

6.1 Adjustment of the IP addresses in the NAT operating mode 20

6.2 Activate DHCP client at the WAN interface 21

6.3 Setting up “Basic NAT” rules ... 22
6.4 Packet filter “WAN to LAN” ... 24
6.5 ICMP Traffic “WAN to LAN” ... 26
6.6 Packet filter “LAN to WAN” ... 27
6.7 ICMP Traffic “LAN to WAN” ... 27
6.8 SNAT ... 28
6.9 NAPT ... 29
6.10 Port forwarding ... 30
7 Application case Bridge ... 32
7.1 Activate Bridge mode ... 32
7.2 Adjustment of the IP addresses in the bridge operating mode ... 32
7.3 Packet filter “WAN to LAN” ... 33
7.4 ICMP Traffic “WAN to LAN” ... 35
7.5 Packet filter “LAN to WAN” ... 36
7.6 ICMP Traffic “LAN to WAN” ... 36
8 MAC address filtering ... 37
9 Static routes ... 38
10 Use with Simatic Step 7 / TIA portal ... 39
10.1 Application with step 7 ... 40
10.2 Use in the TIA portal ... 41
11 Other functions ... 43
11.1 DHCP server for LAN ... 43
11.2 Host name (WAN) ... 44
11.3 Syslog server ... 45
11.3.1 Syslog local ... 45
11.3.2 Syslog remote ... 45
11.4 Change password / User management ... 46
11.5 File certificate (HTTPS) ... 48
11.6 Allow web interface access over WAN network (Web Interface Access) ... 48
11.7 Time settings (Time) ... 49
11.8 Export/import of configuration ... 50
12 Firmware update ... 51
13 Resetting to factory settings ... 52
13.1 Resetting to factory settings via the website ... 52

13.2 Resetting to factory settings with button 52
14 FAQ 53
15 Technical data 54
15.1 Dimensioned drawing 55

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

HAZARD

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

WARNING

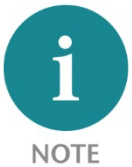
If the hazard warning is ignored, there is a probable danger to life and health of people from electrical voltage.

CAUTION

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

ATTENTION

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



NOTE

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 that 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 that 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 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.

1.6.10 Recycling / WEEE

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.

The electrical devices described in this document are to be recycled. According to Directive 2012/19 / EU on waste electrical and electronic equipment (WEEE), they must not be disposed of by municipal waste disposal companies.

2 Security recommendations

WALL IE is a network infrastructure component, and thus an important element in the security considerations of a system or network. When using WALL IE, therefore please consider the following recommendations in order to prohibit unauthorized access to plants and systems.

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 concept with corresponding products, such as the WALL IE.

You can find extensive information, for example, in the “ICS Security Compendium” of the Federal Office for Information Security (BSI):
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ICS/ICS-Security_compendium.html

Physical access:

- Limit physical access to components of relevance to security to qualified personnel.

Security of the software:

- Always keep the firmware of all communications components up to date.
- Inform yourself regularly of firmware updates for the product.
  You can find information on that in chapter 12.
- Only activate protocols and functions you really need

Passwords:

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

3 Overview

WALL IE, the Industrial NAT Gateway and Firewall, simply integrates machine networks into the superior production network using network segmentation, packet and MAC address filtering.

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.

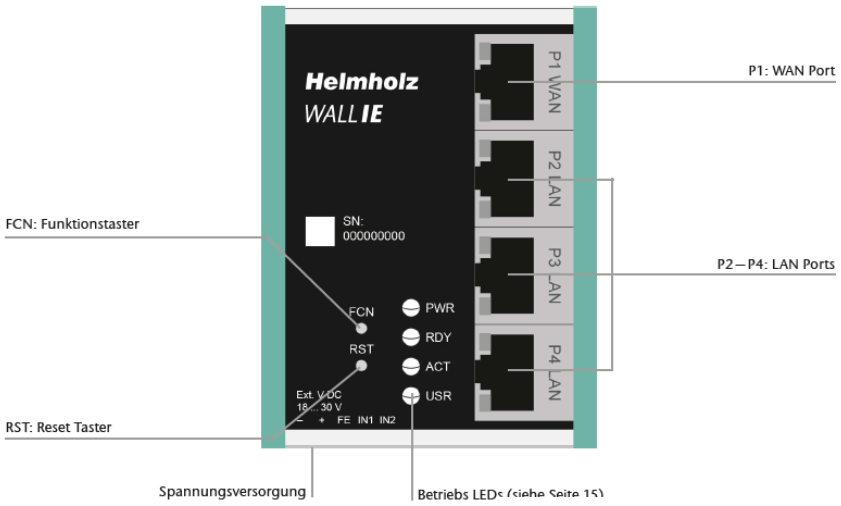
In the **Bridge operating mode**, the WALL IE network bridge is active in an IPv4 subnetwork. In contrast with normal switches, packet filtering is possible in this operating mode. This means that the restriction of access to individual areas of your network can be achieved without having to use different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

Features of the WALL IE:

- NAT (Basic NAT, SNAT, NAPT and port forwarding) for network segmentation
- Bridge functionality for securing network areas with identical IPv4 address ranges
- 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

3.1 Setup

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

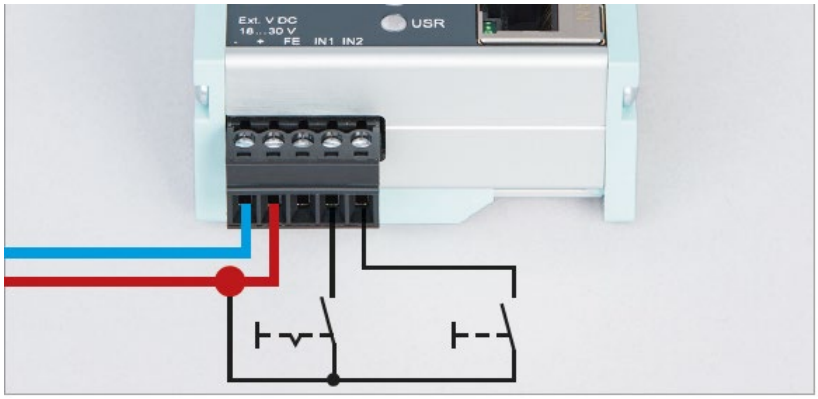


A reset to factory settings can be initiated with the function button (FCN) (see ch. 12). The reset button (RST) initiates a restart of the WALL IE.

3.2 Connection of the power supply

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. Connect this correctly with the reference potential.

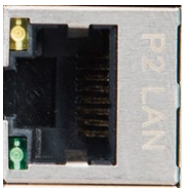
The RJ45 “P1 WAN” socket is for the connection of the external network. The RJ45 “P2 LAN –P4 LAN” sockets are switched and are for the connection of the internal network.



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.

3.3 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	Flashing light	Reset to works setting activated
RJ45 LEDs	Green (Link)	Connected
	Orange (Act)	Data transfer at the port

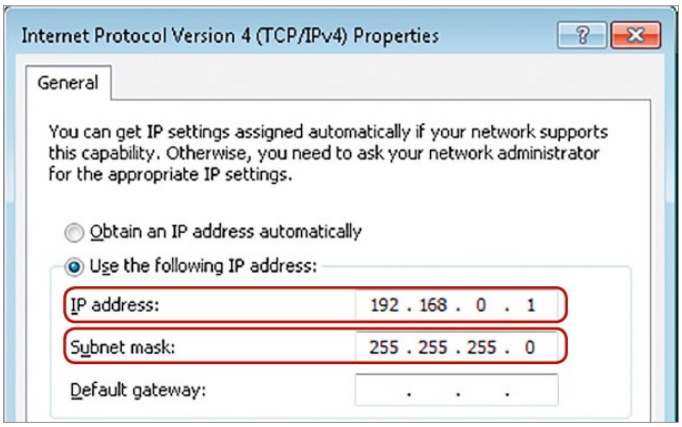


4 Initial access to the web interface

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 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

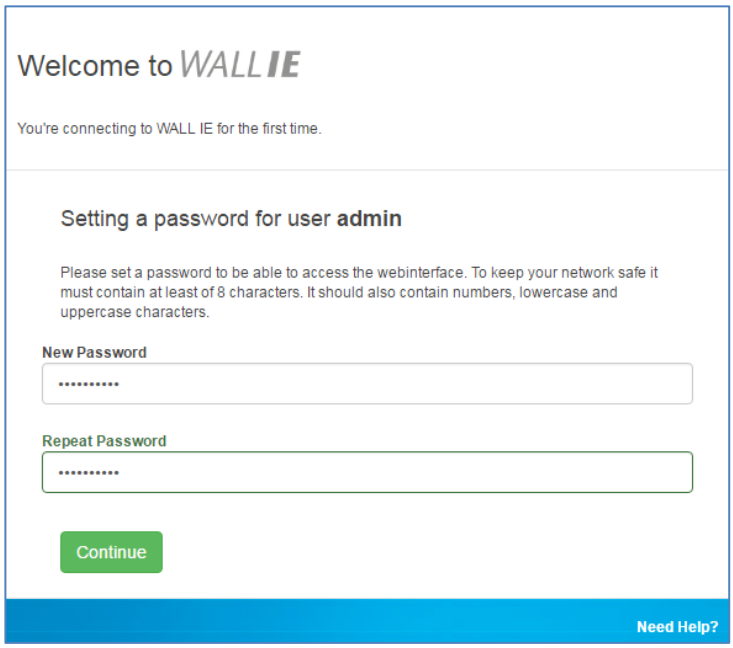
You will be prompted to set a password with the initial registration.

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.

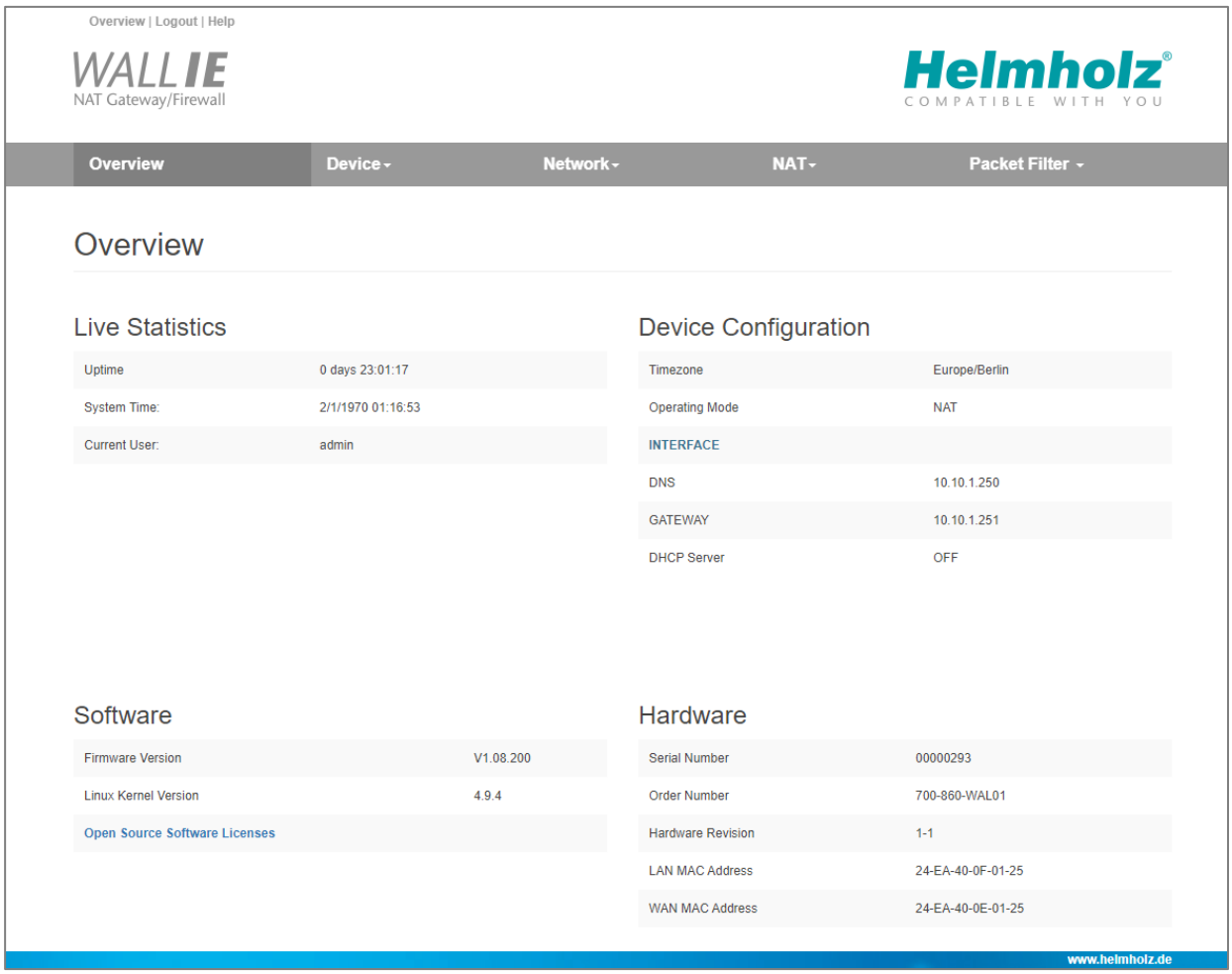


ATTENTION

Please note the password well! 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.

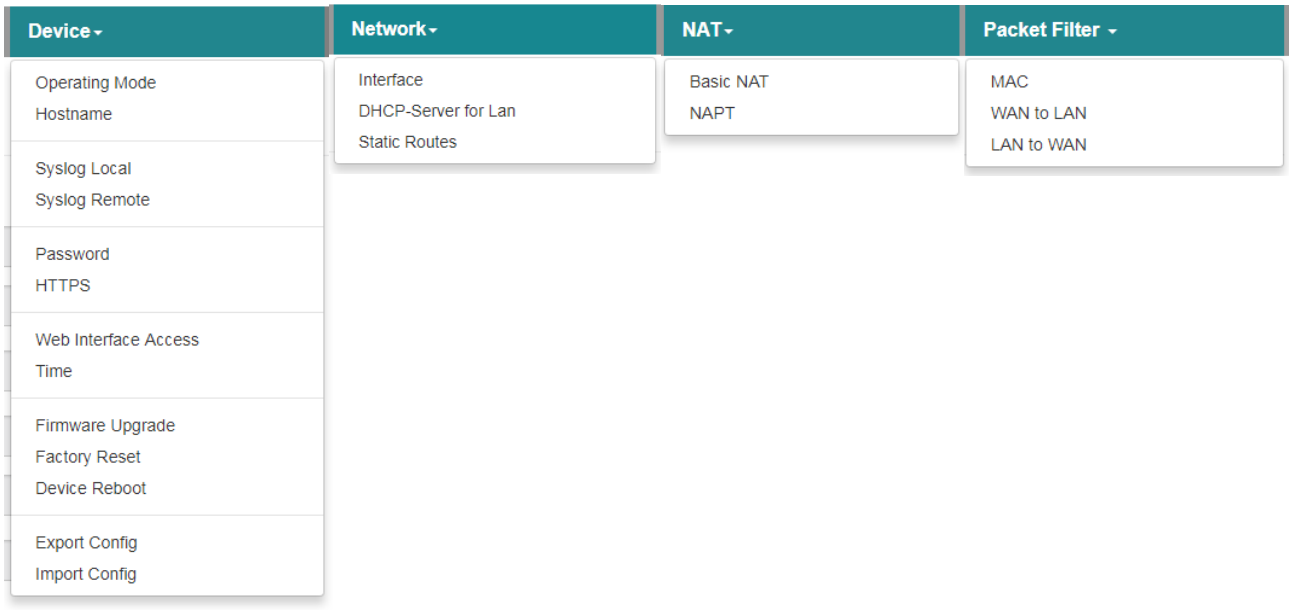


NOTE

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

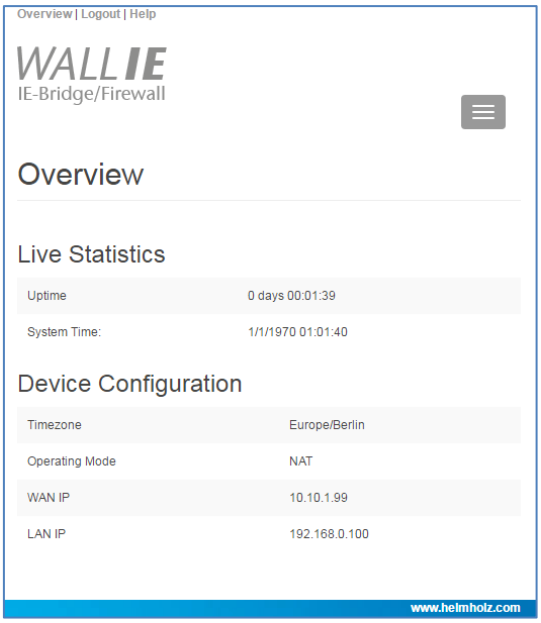
Link to firmware:
http://www.helmholz.de/goto/700-860-WAL01#tab-software

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.

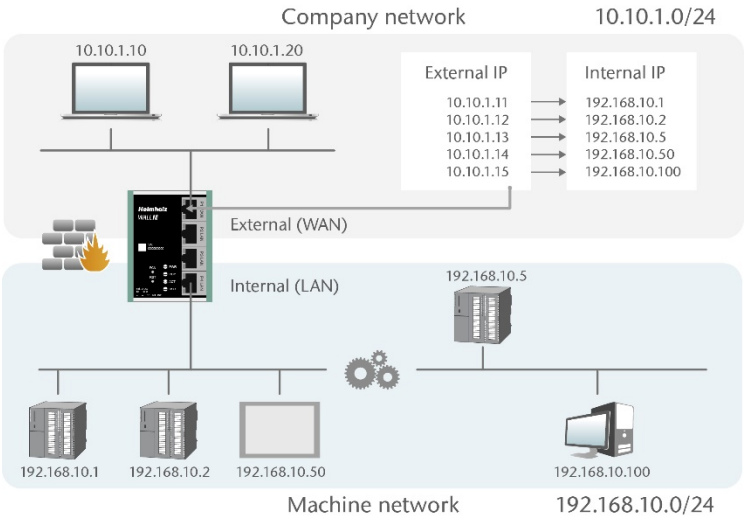
5 Choosing the operating mode

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 production network with other IP addresses, 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 production network.



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

Packet filters and MAC address filters can also be used to estimate the data transfer permitted.

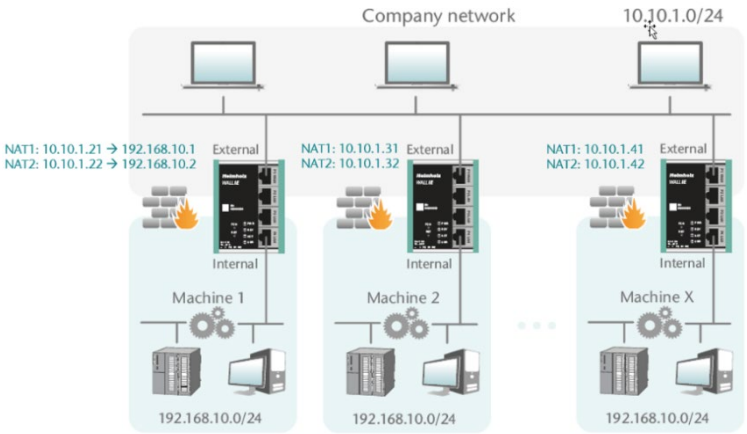
Broadcast traffic is generally filtered at the WALL IE, which means that the time behavior of the machine network is not impaired by the production network.

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 that packets 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 production network.

Each automation cell can in this case be assigned a different, free IP address from the production network.



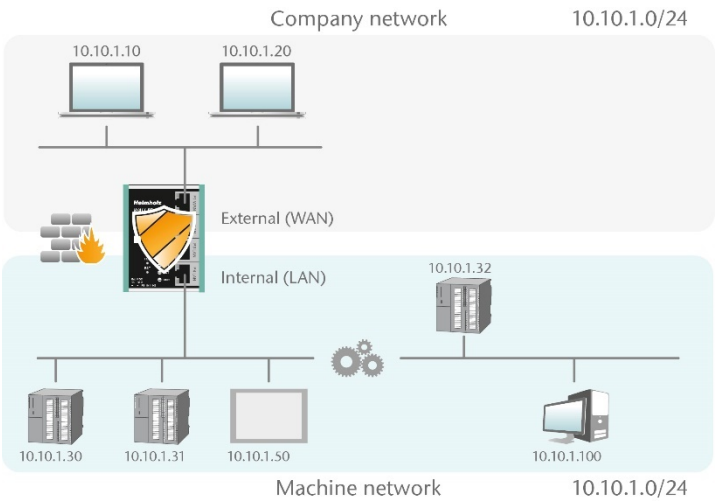
If “NAT” is your planned application case, please continue reading in chapter 6.

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 production network. The IP addresses in the production 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.

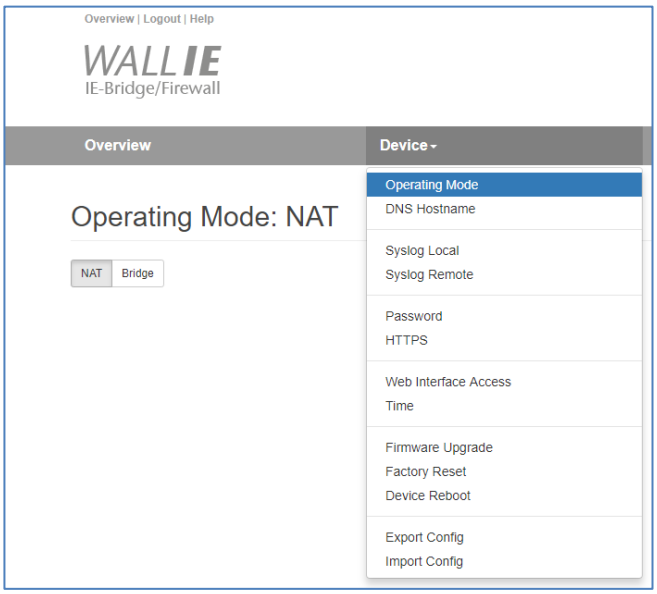
This allows the separation of part of the production network without using different network addresses.



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

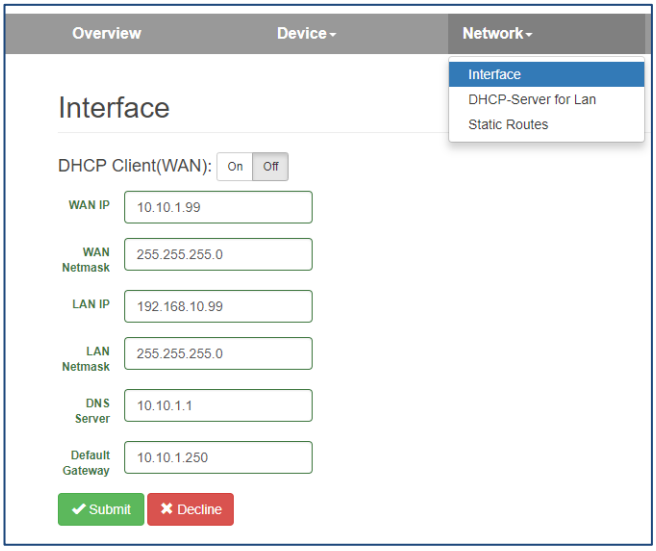
6 Application case NAT

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 indicated. 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 standard gateway can also be acquired per 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”.

A DNS server can also be indicated where necessary. It is necessary to indicate a DNS server for the SNTP service (see ch. 11.7).

ATTENTION

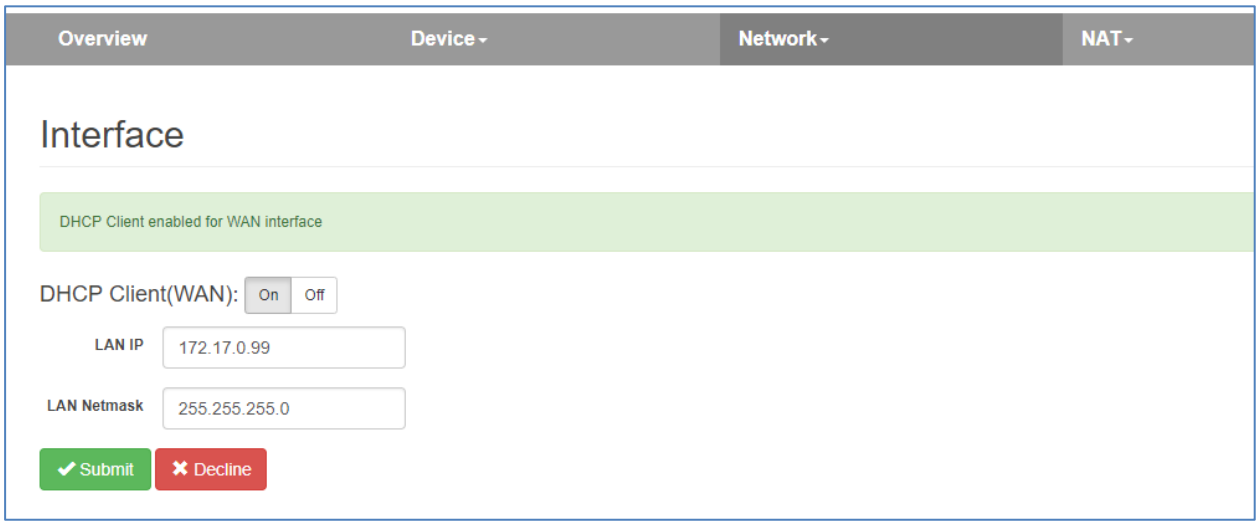
When you change the LAN IP address, you may need to reopen the website of the WALL IE in the browser using the new IP address and log in again.

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.

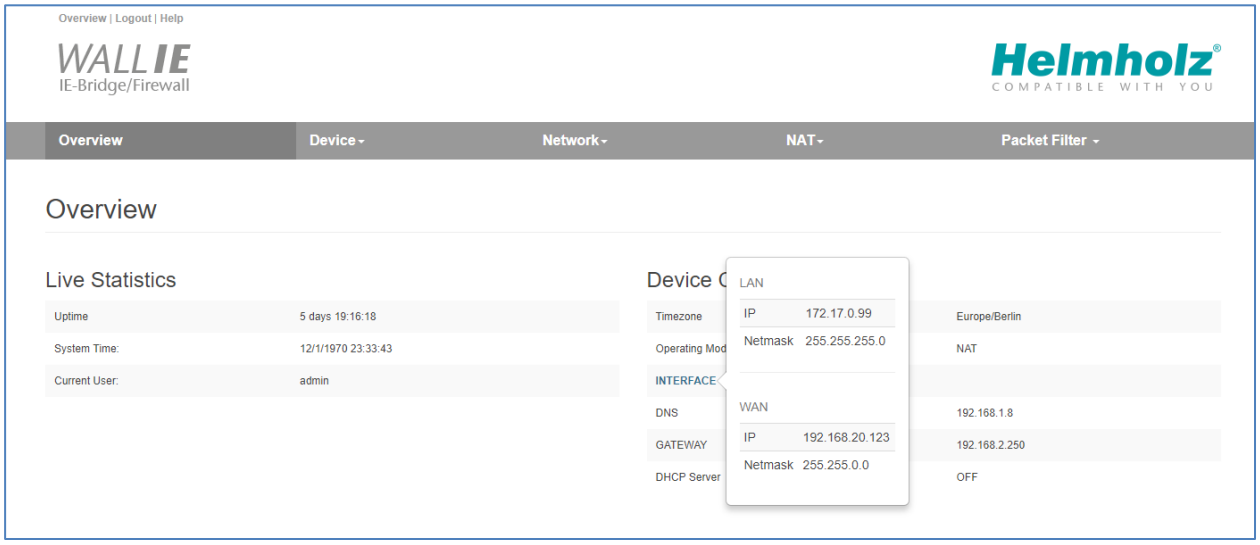
6.2 Activate DHCP client at the WAN interface

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.

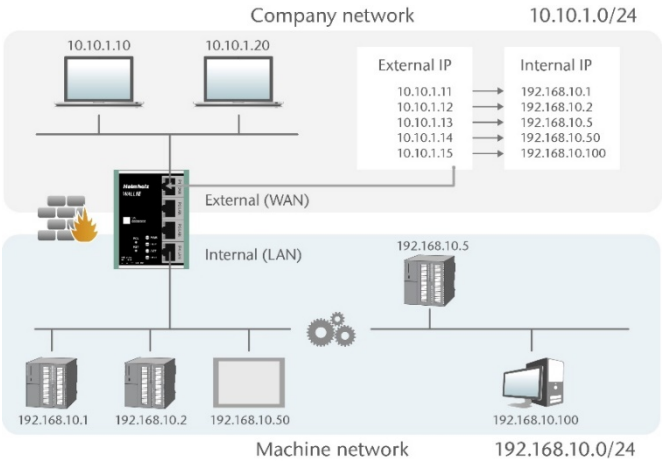
The IP settings acquired from the DHCP client are made visible on the overview page by clicking on “INTERFACE”.

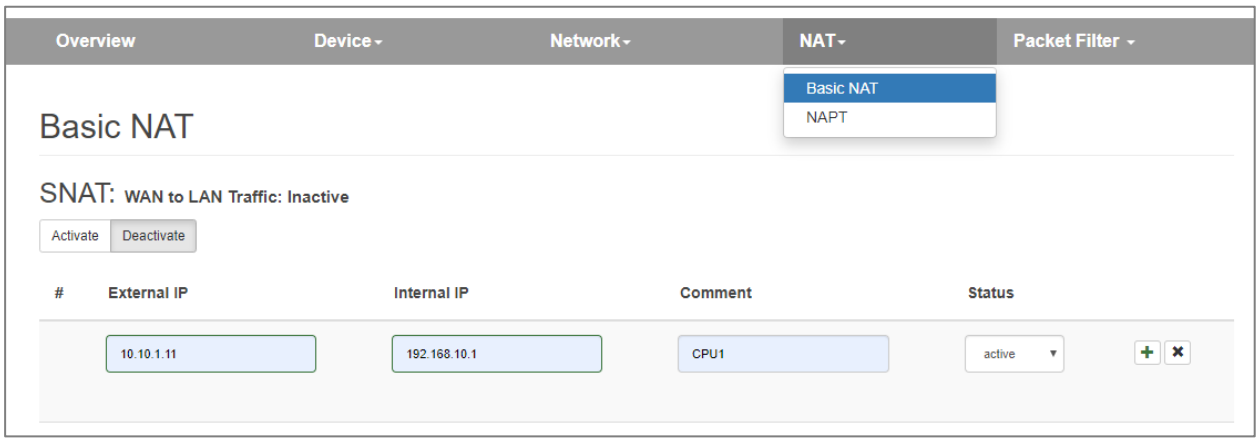


6.3 Setting up “Basic NAT” rules

In order that the entry of “Basic NAT” rules is possible, WALL IE must be in the operating mode “NAT”.

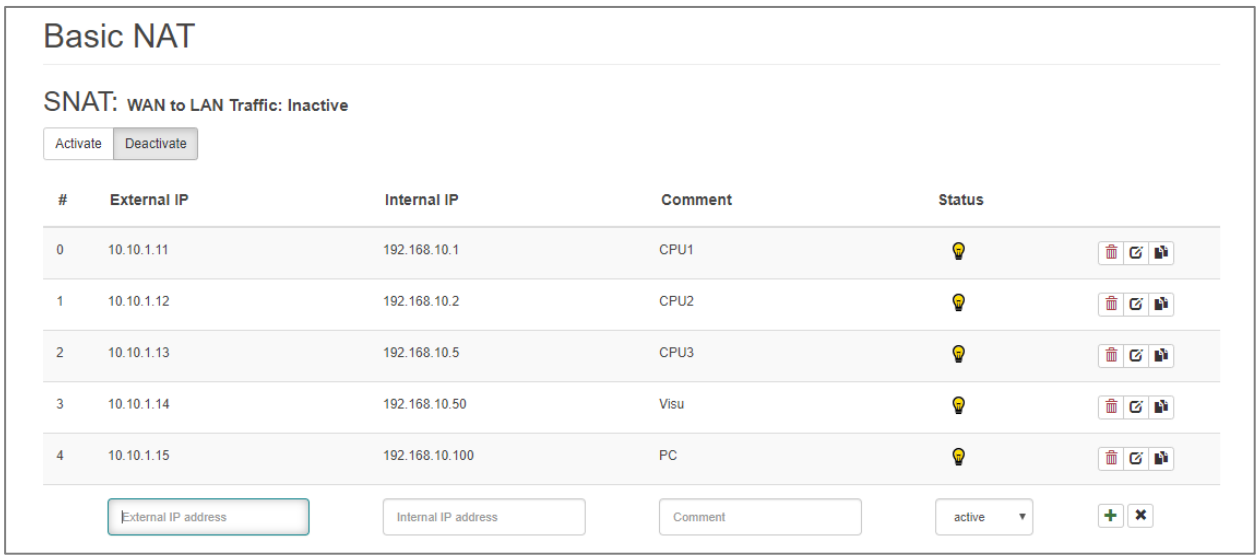
Then select the “NAT” menu and the sub-menu “Basic NAT”. Enter the first rule and save it with the button.





The “External IP” is the IP address under which the network participant of the machine becomes visible in the production network (WAN). The “Internal IP” is the IP address of the network participant in the machine (LAN). Any text can be entered as a comment.

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

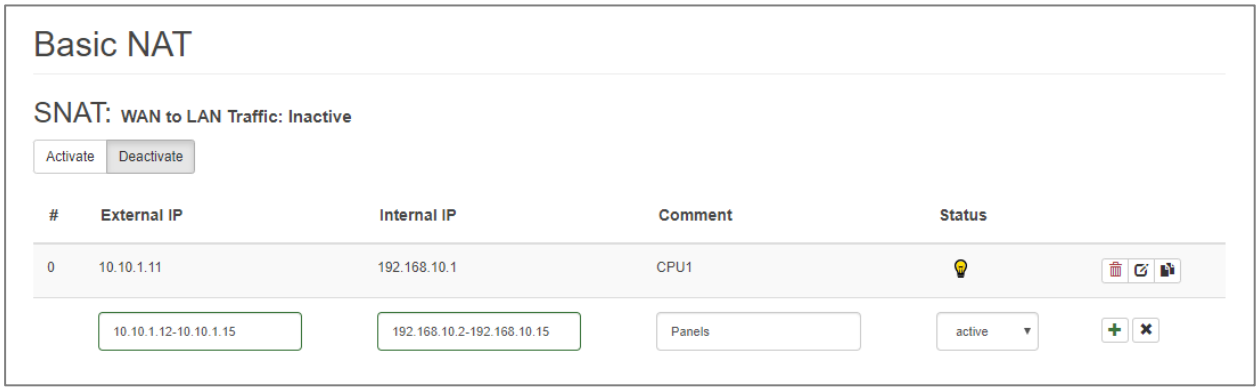


Status: = Rule is active; a click on the lamp symbol changes the rule status to inactive

= 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!

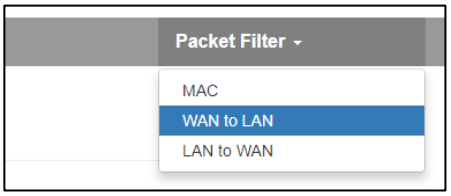
In order to enable access, packet filter rules must be created or the default action for the packet filters be set to “Accept”. See the following chapter.

The “LAN to WAN” data transfer is initially always released but can also be limited by packet filters 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 production network (WAN) and the machine network (LAN).

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

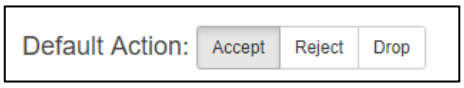
The following filter criteria on layers 3 and 4 are available: IPv4 addresses, protocol (TCP/UDP), and ports.

The packet filters are always also available in the direction “LAN to WAN”, see chapter 0.

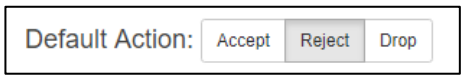
Select the “WAN to LAN” menu point in the “Packet Filter” menu.

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”.

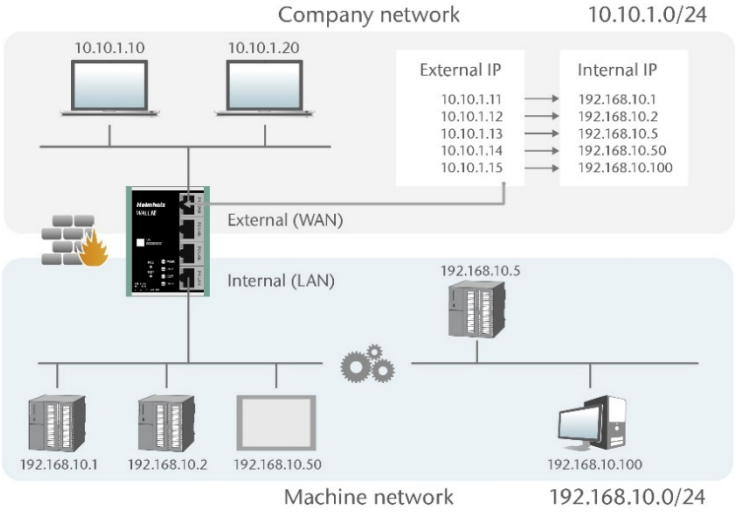


In order to limit access to the machine network to certain participants in the WAN, set the default action to “Reject” or “Drop”. In the case of prohibited frames from the WAN, “Reject” sends an error message in response, while “Drop” rejects the frame without sending an error message.

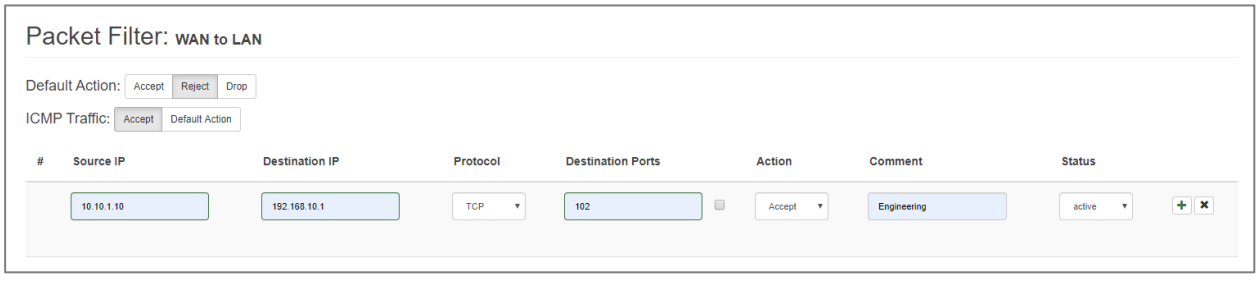


Example: A PC in the production network (WAN) has the IP address 10.10.1.11 (e.g. a visualization).

This PC should be able to access the CPU with the IP address 192.168.10.1 within the LAN via the port 102 with the help of the TCP protocol.



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

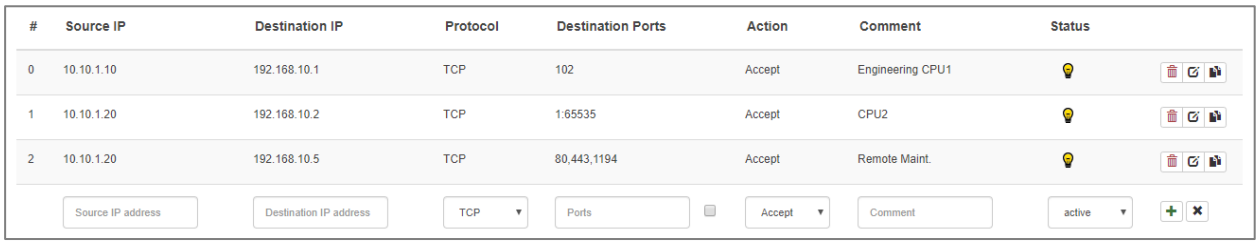


Source IP indicates the IP address of the active device in the production network (WAN). **Destination IP** the addressed device in the machine network (LAN).

The filter rules can be defined for one protocol type with **protocol** "TCP" or "UPD".

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".

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	

Action defines whether this rule allows communication ("Accept"), rejects with error message ("Reject"), or simply rejects ("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”

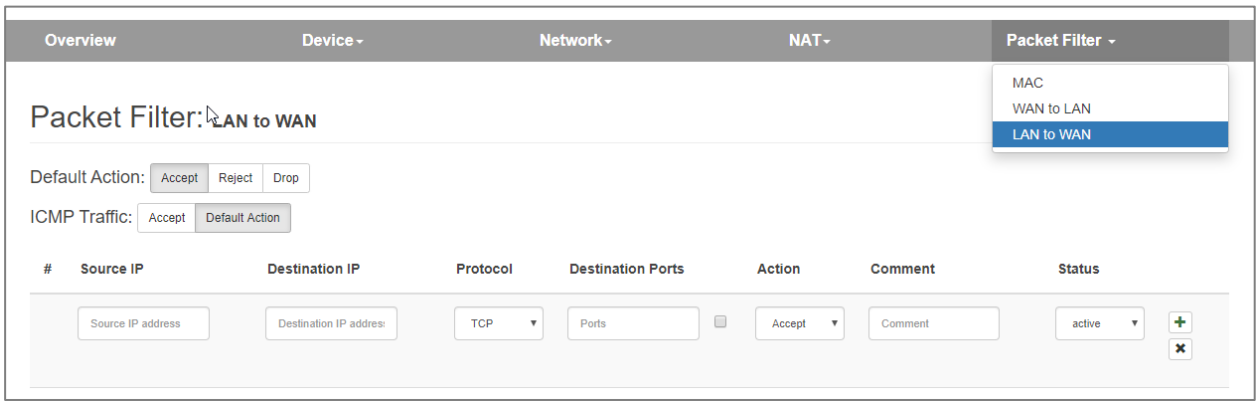
The Internet Control Message Protocol (ICMP) serves the purpose of exchanging information and error messages via the Internet protocol IPv4. Typical ICMP frames include “ping” or “traceroute”.

With the “ICMP Traffic” option, you can generally allow the directing of ICMP frames from the WAN to the LAN network (“Accept”) or, depending upon the packet filters, prohibit this (“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 of any kind are allowed through.

6.6 Packet filter “LAN to WAN”

In the basic state, data traffic is permitted for devices from the machine network (LAN) to the production network (WAN) without limitations (“Default Action”: “Accept”).



In the “LAN to WAN” packet filter, the communication of devices in LAN with devices in the production network (WAN) or into the Internet is completely prohibited or is blocked or allowed for particular devices.

The entry of the filter rules corresponds to the packet filters “WAN to LAN”, except that the source IP is now the LAN IP and the destination IP addresses a device in the WAN.

ATTENTION

In the event that devices in the LAN should communicate with devices in the production network, “SNAT” should be activated in “Basic NAT” settings.

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”

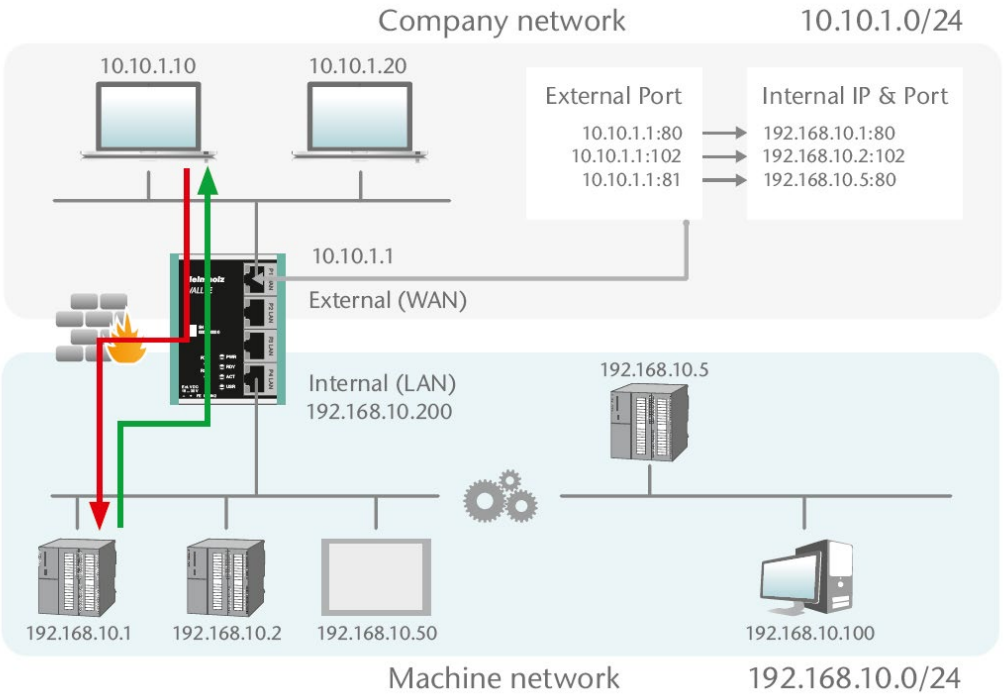
With the “ICMP Traffic” option, you can generally allow the directing of ICMP frames from the LAN to the WAN network (“Accept”) or, depending upon the packet filters, prohibit this (“Default Action”).

If, for example, the packet filters “Default Action” are set to “Reject” or “Drop”, and ICMP Traffic to “Default Action”, then no ICMP frames of any kind are allowed through.

6.8 SNAT

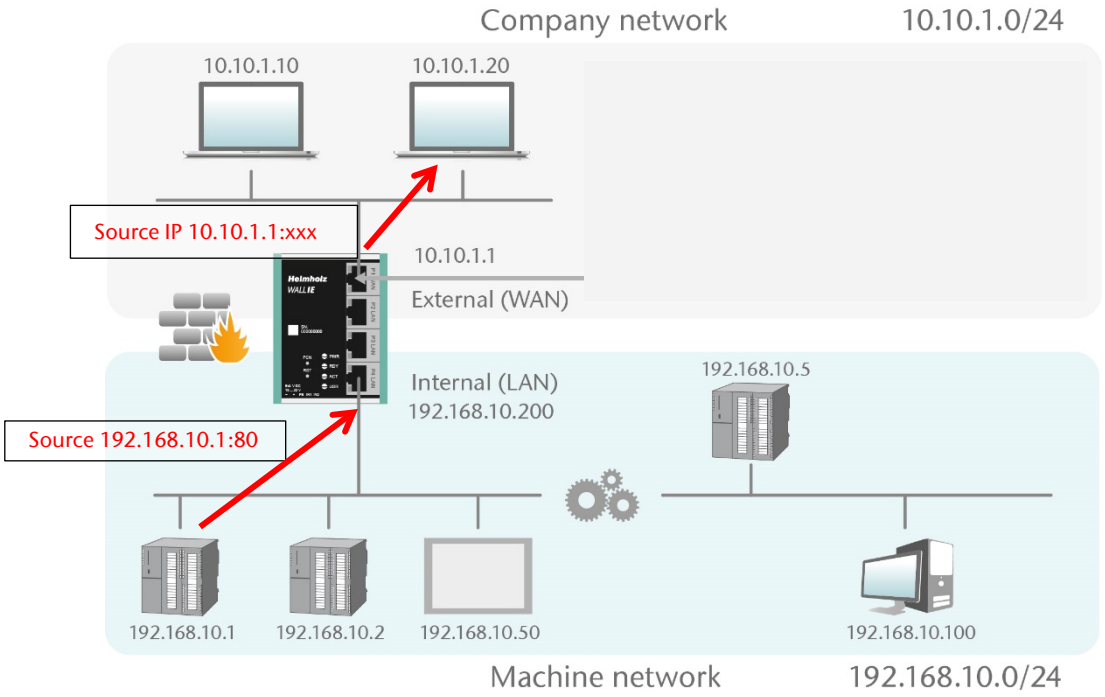
The function “SNAT (Source NAT)” transparently forwards incoming traffic from the WAN side to the LAN network. All data packets sent to the LAN are sent to the IP address of the WALL IE.

Therefore, none of the LAN participants needs the WALLIE 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.

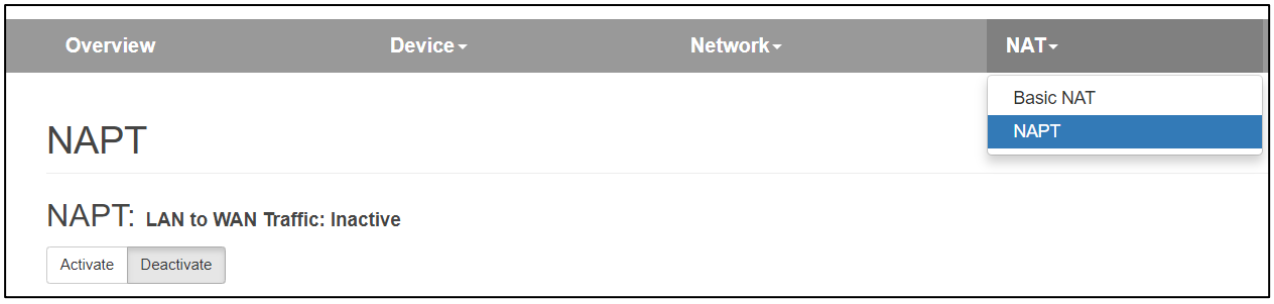


6.9 NAPT

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



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 administer the implementation to the IP addresses of the WAN network and looks after the assignment of the response.



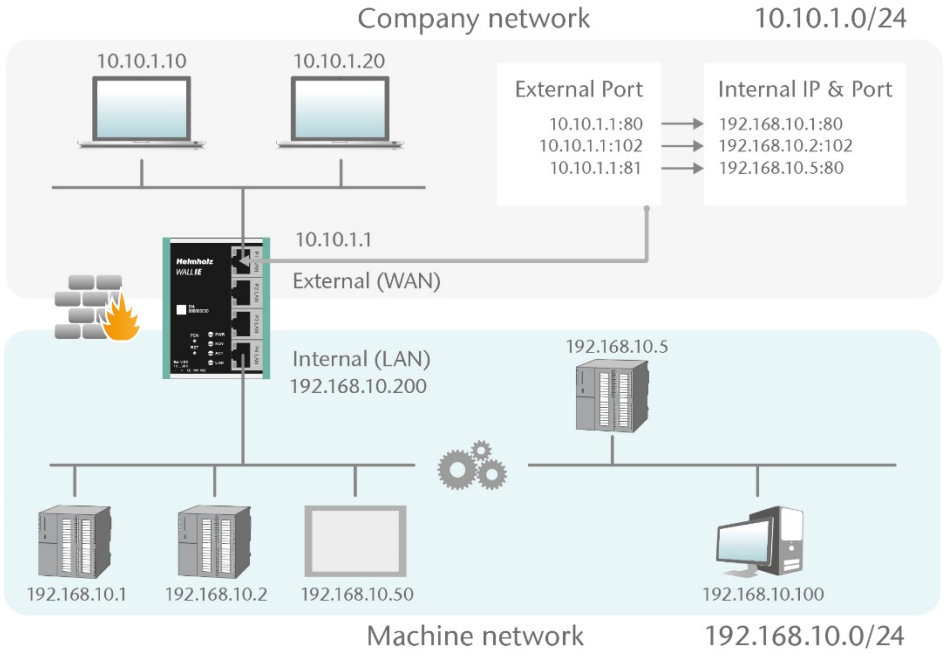
ATTENTION

In order that the communication with activated NAPT from the LAN to WAN functions, WALL IE LAN IP address must be set as a default gateway for every device connected to LAN.

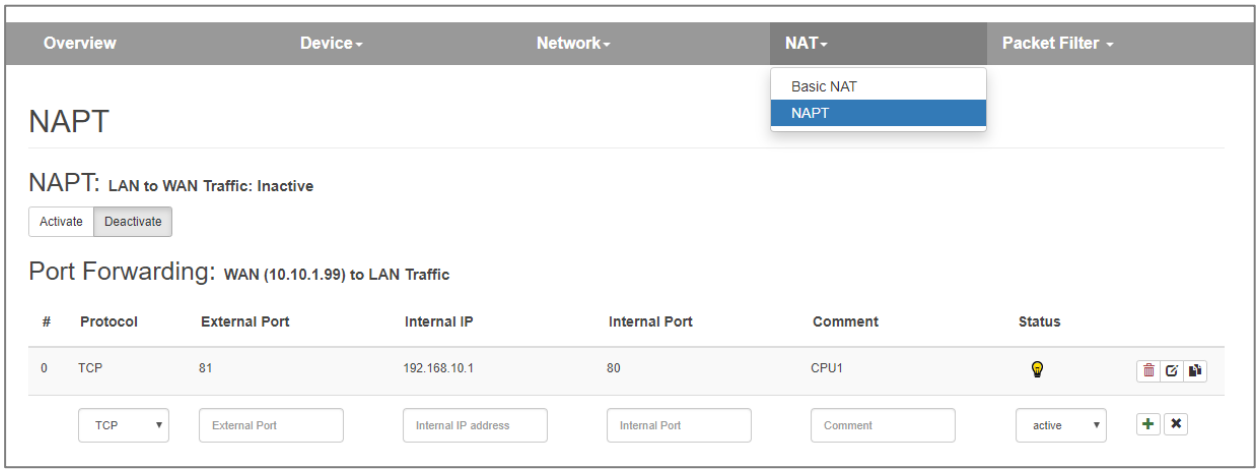
If the **NAPT** option is deactivated, the query packets from the LAN are forwarded from the LAN to the WAN with their original sender IP and sender port.

6.10 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 192.168.10.5 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: The port under which the frames in the WAN under the address of the WALL IE are received.

Internal IP: The IP address to be addressed in the machine network (LAN).

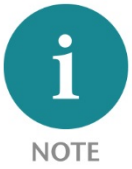
Internal Port: The port of the device to be addressed in the machine network (LAN).

Comment: Freely definable comment.

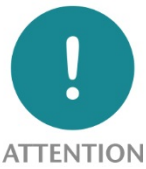
Status: = Rule is active; a click on the lamp symbol changes the rule status to inactive

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

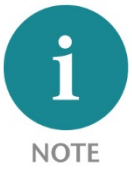
Possible actions: delete a rule edit a rule copy a rule



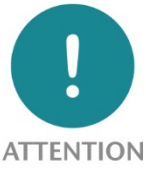
"Port forwarding" and "Basic NAT" can be used simultaneously in the NAT operating mode.



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.



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 11.6).

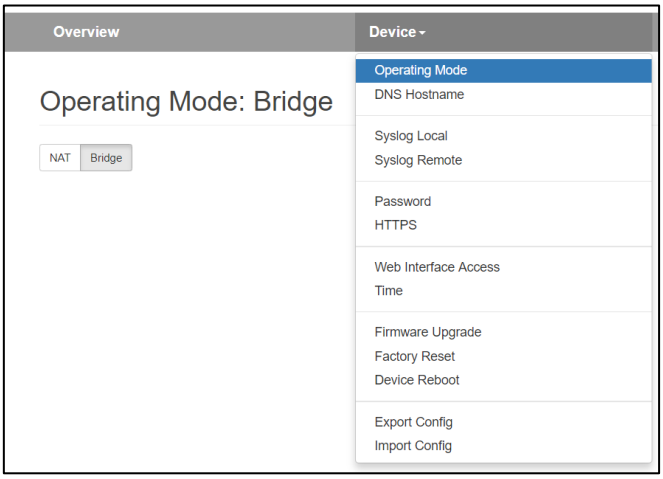


A maximum of 128 port forwarding entries can be created.

7 Application case 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”.

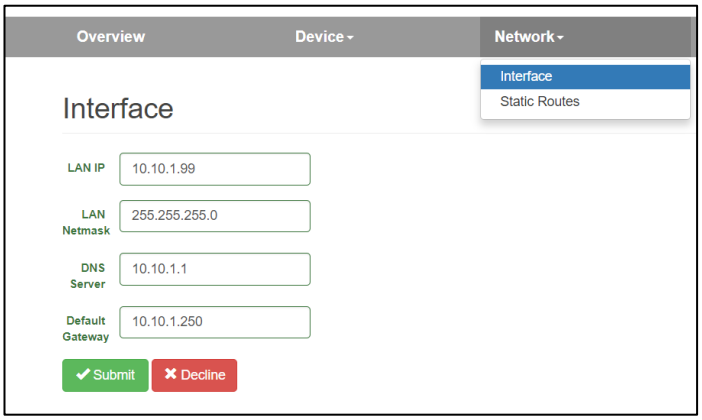


7.2 Adjustment of the IP addresses in the bridge operating mode

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

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

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

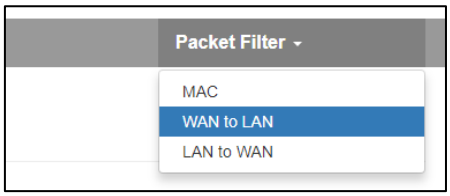
In the bridge mode, all ports are initially blocked for “WAN-to-LAN” data transfer for security reasons!

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 production network (WAN) and the machine network (LAN).



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

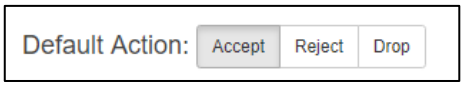
The following filter criteria on layers 3 and 4 are available: IPv4 addresses, protocol (TCP/UDP), and ports.

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

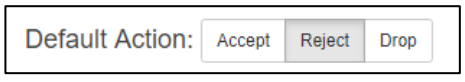
Select the “WAN to LAN” menu point in the “Packet Filter” menu.

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”.

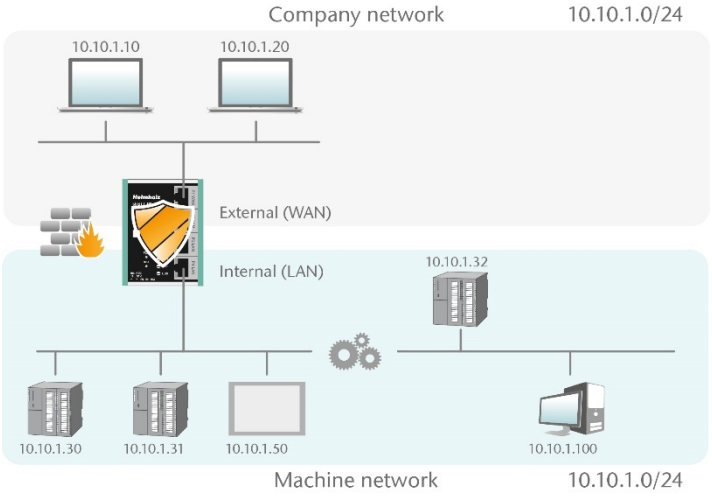


In order to limit access to the machine network to certain participants in the WAN, set the default action to “Reject” or “Drop”. In the case of prohibited frames from the WAN, “Reject” sends an error message in response, while “Drop” rejects the frame without sending an error message.

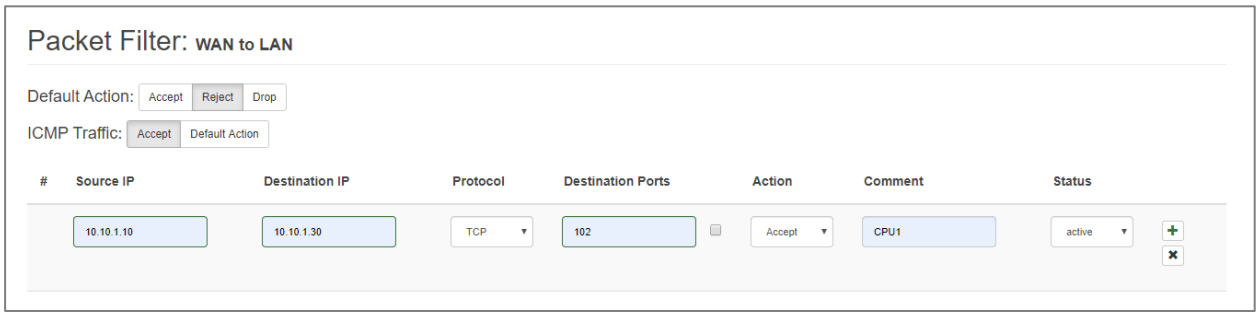


Example: A PC in the production network (WAN) has the IP address 10.10.1.11 (e.g. a visualization).

This PC should be able to access the CPU with the IP address 10.10.1.30 within the LAN via the port 102 with the help of the TCP protocol.



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



Source IP indicates the IP address of the active device in the production 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" or "UPD".

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	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".

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 rejects ("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.

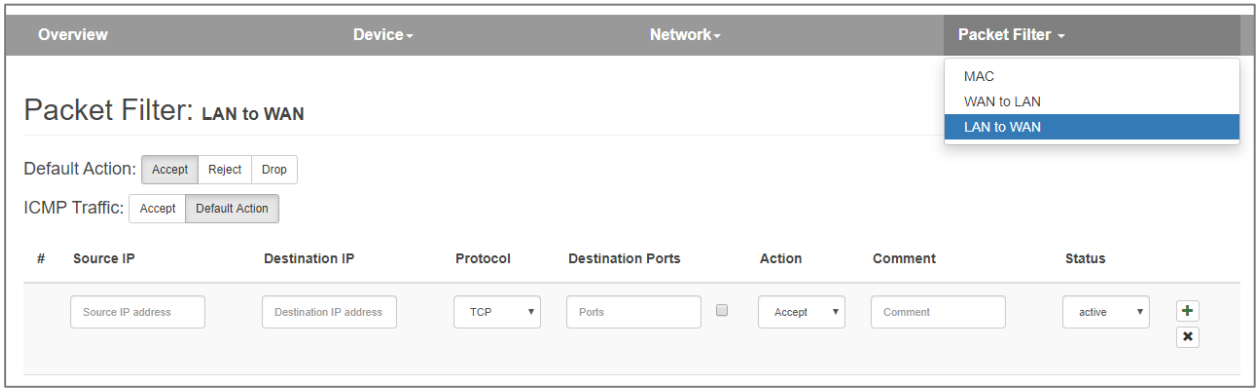
7.4 ICMP Traffic “WAN to LAN”

With the “ICMP Traffic” option, you can generally allow the directing of ICMP frames from the WAN to the LAN network (“Accept”) or, depending upon the packet filters, prohibit this (“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 of any kind are allowed through.

7.5 Packet filter “LAN to WAN”

In the basic state, data traffic is permitted for devices from the machine network (LAN) to the production network (WAN) without limitations (“Default Action”: “Accept”).



In the “LAN to WAN” packet filter, the communication of devices in LAN with devices in the production network (WAN) can be completely prohibited or be blocked or allowed for particular devices.

7.6 ICMP Traffic “LAN to WAN”

With the “ICMP Traffic” option, you can generally allow the directing of ICMP frames from the LAN to the WAN network (“Accept”) or, depending upon the packet filters, prohibit this (“Default Action”).

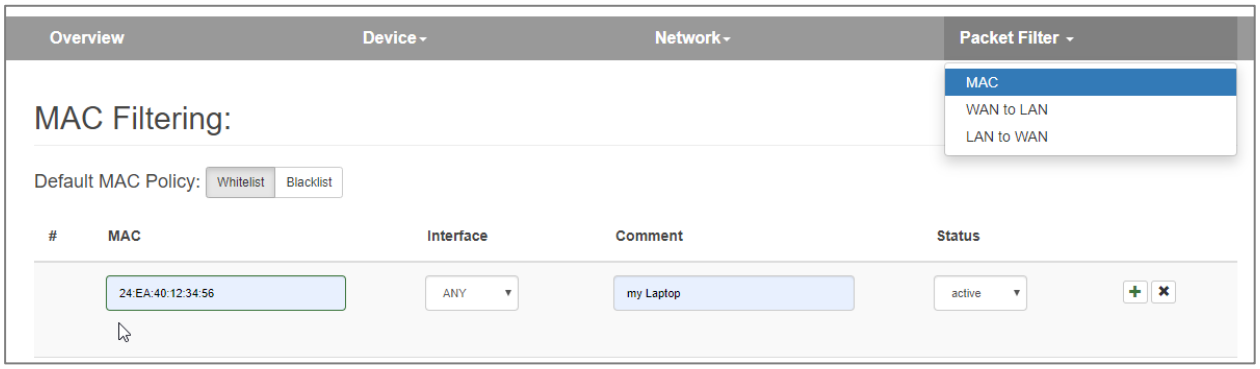
If, for example, the packet filters “Default Action” are set to “Reject” or “Drop”, and ICMP Traffic to “Default Action”, then no ICMP frames of any kind are allowed through.

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 sides.



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.

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

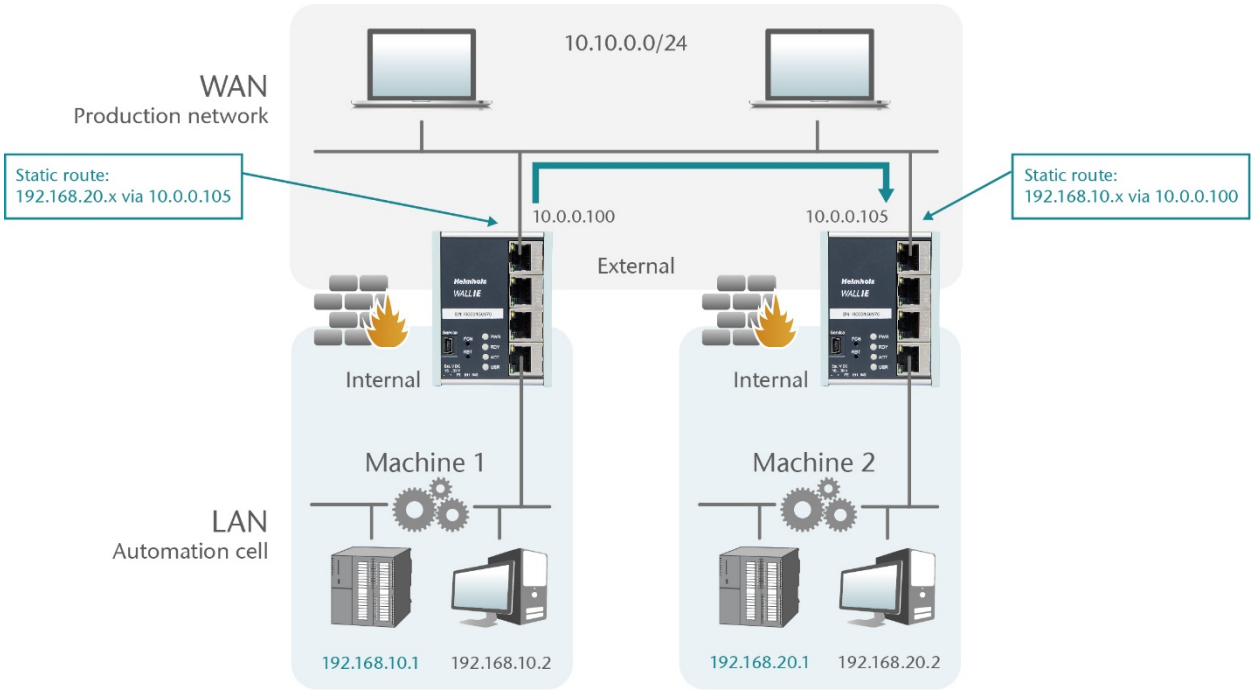
In the NAT mode, the MAC filtering is only carried out WHEN the MAC address is also indicated in the IP header of the packet. Layer 2 frames are not forwarded in the NAT mode.

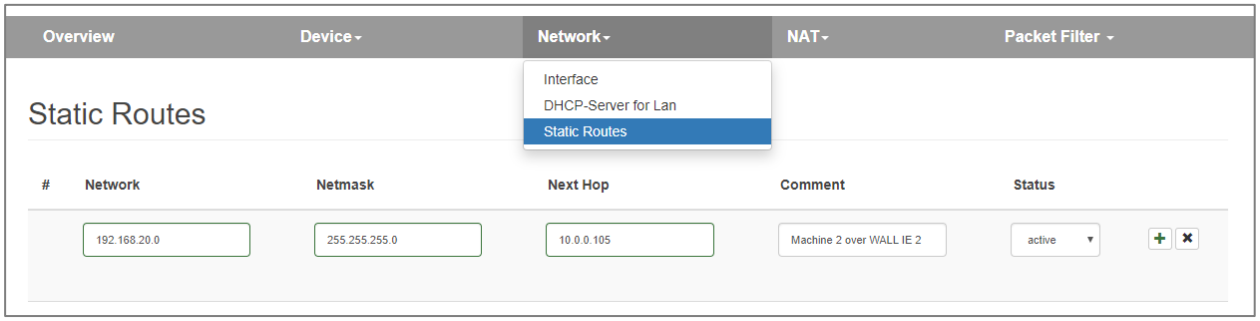
The MAC filtering takes place on layer 2 in the bridge mode.

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

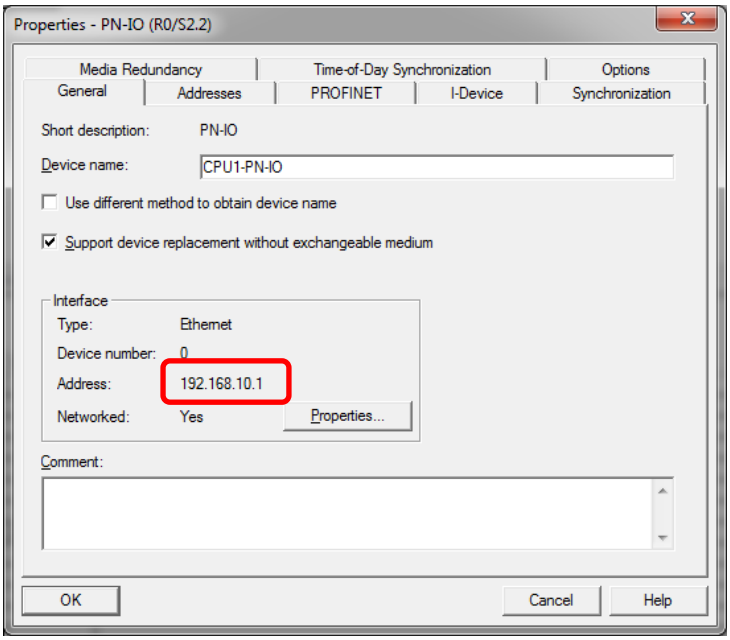
In order to enable the return route of the answer, a route for the IP address of the WALL IE of machine 1 must also be set up in the remote gateway (Machine 2)!

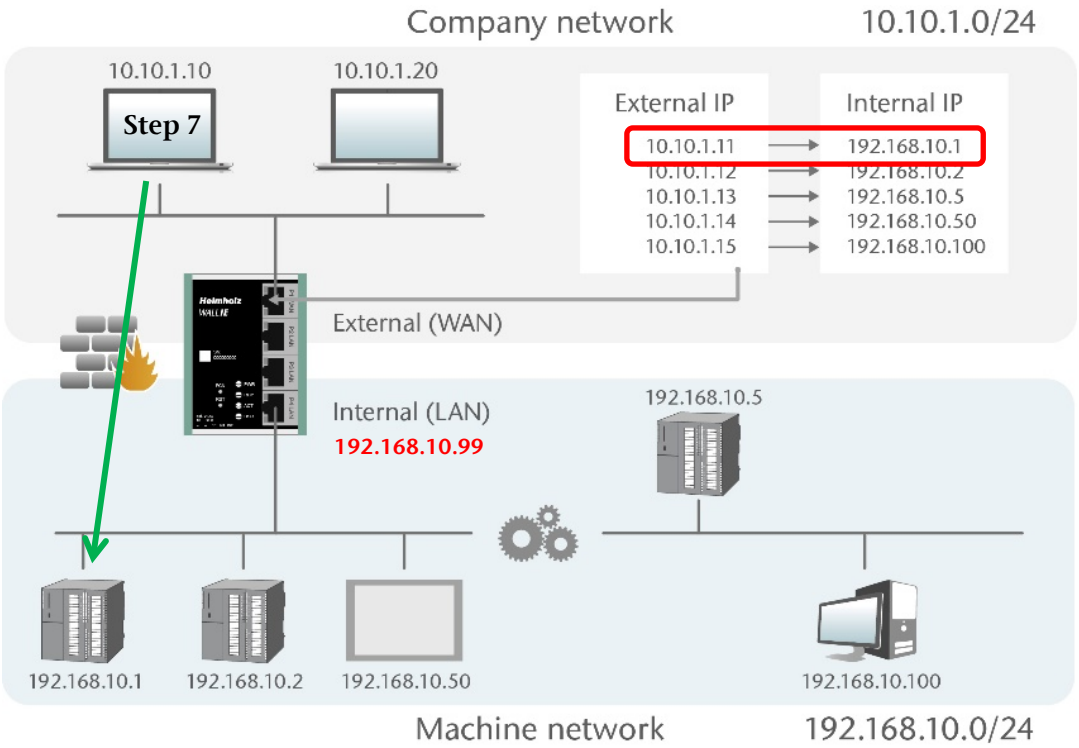
10 Use with Simatic Step 7 / TIA portal

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.

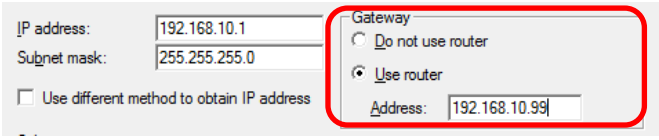




10.1 Application with step 7

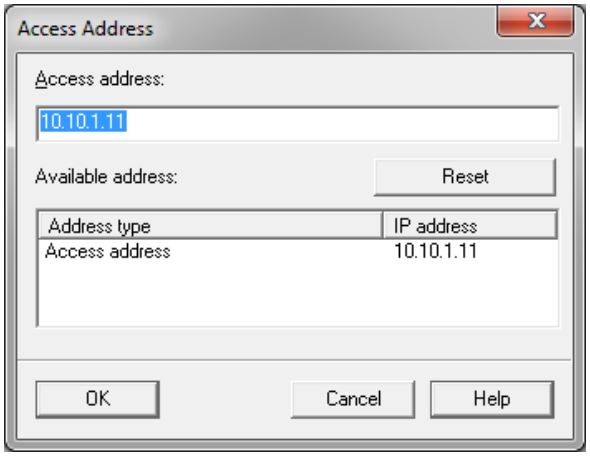
Step 7 offers the possibility to access a CPU and to use an IP address other than that set in the project in the process.

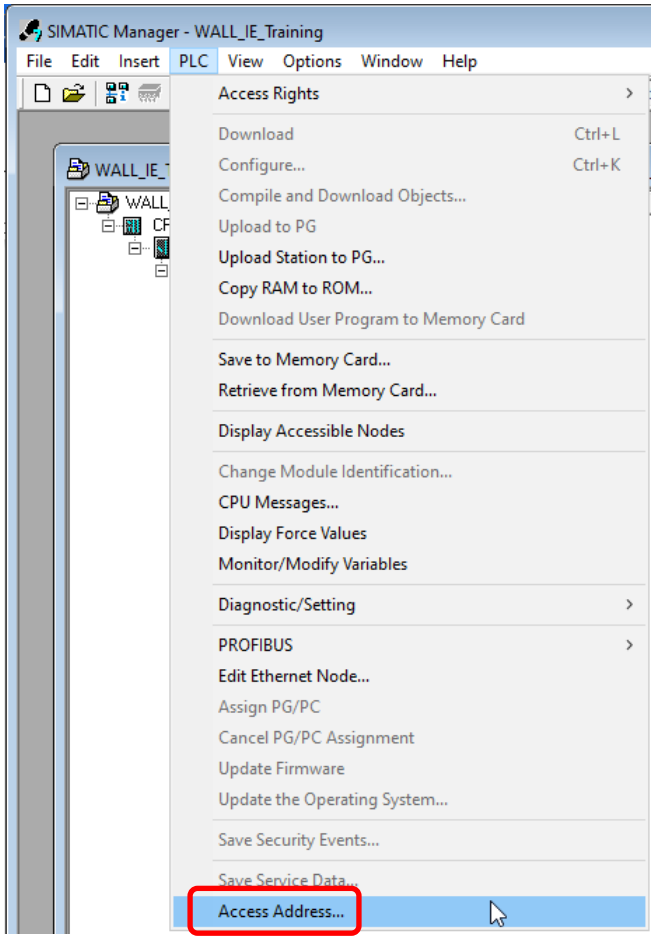
In order to be able to redirect the responses from the CPU back to the engineering station in the WAN via the WALL IE, either the SNAT function must be activated in WALL IE under "Basic NAT" or the WALL IE must be entered as the router for the CPU in the project.



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

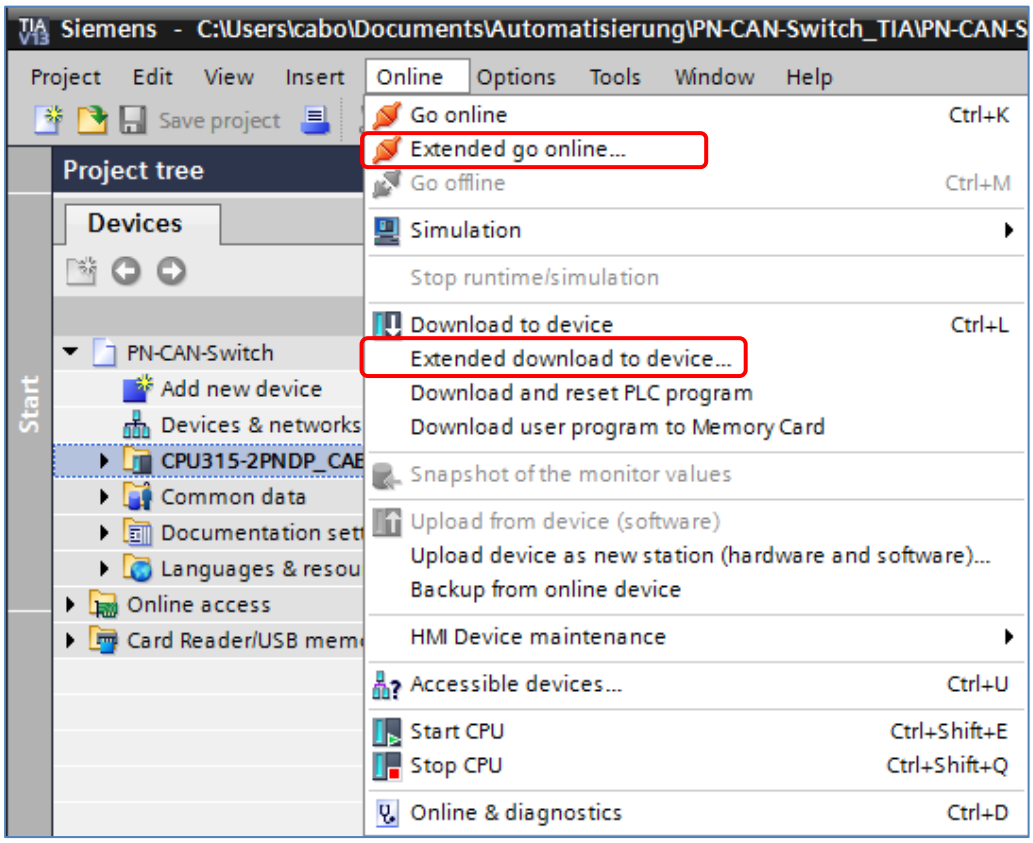
This solution can only be sensibly used in the Basic NAT operating mode. In the case of NAPT with port forwarding, only one CPU can be reached, as the Simatic Manager always accesses the CPU with the non-adjustable port 102.

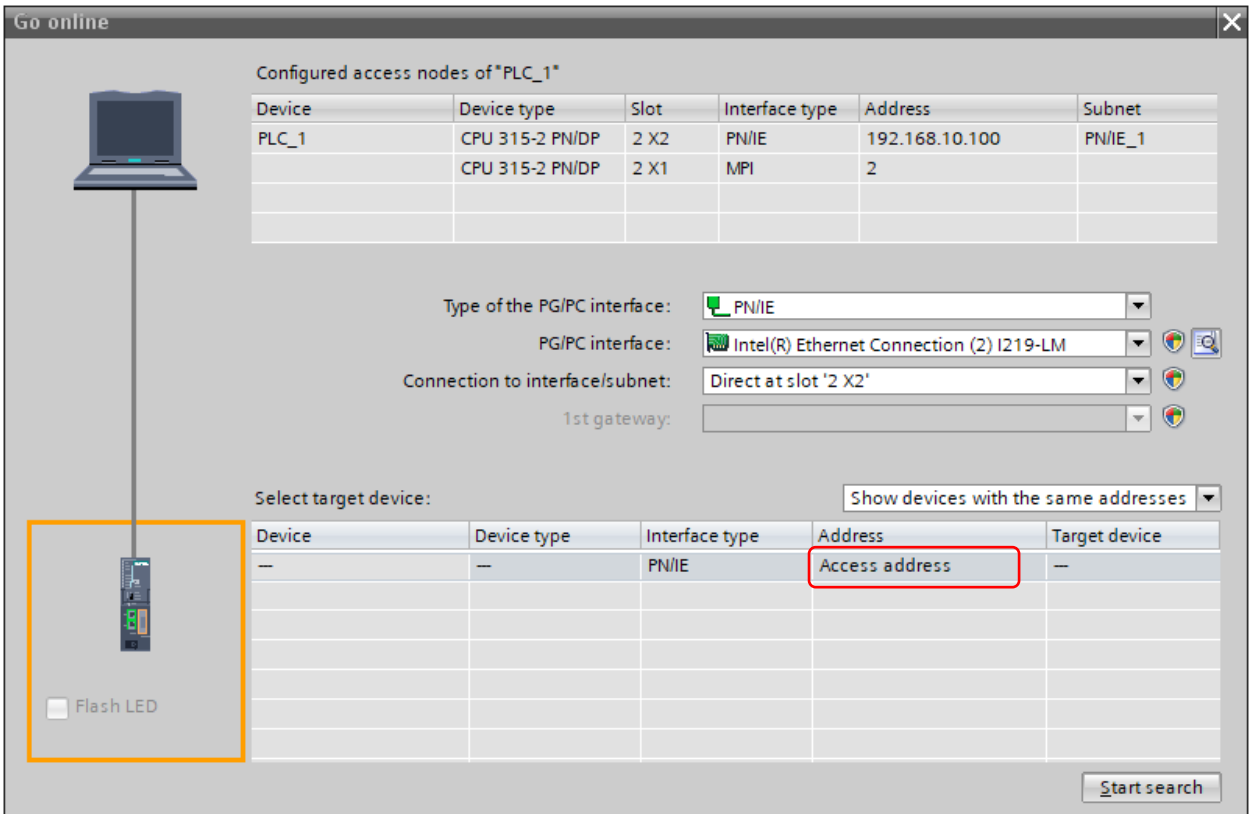
The search via the Siemens function “reachable participants” doesn’t function through the WALL IE firewall.

PROFINET RT frames are not routed through by WALL IE!

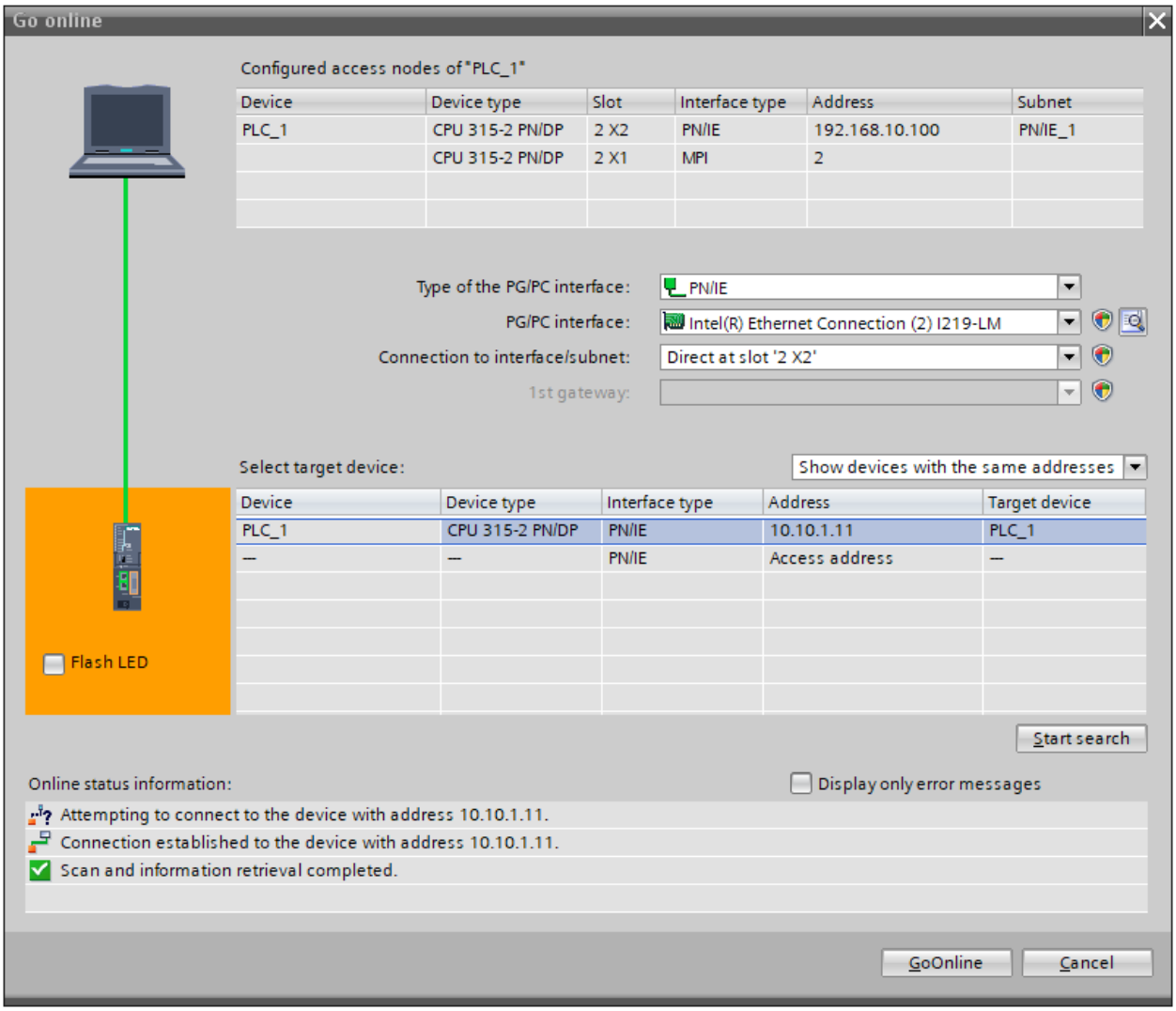
10.2 Use in the TIA portal

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.

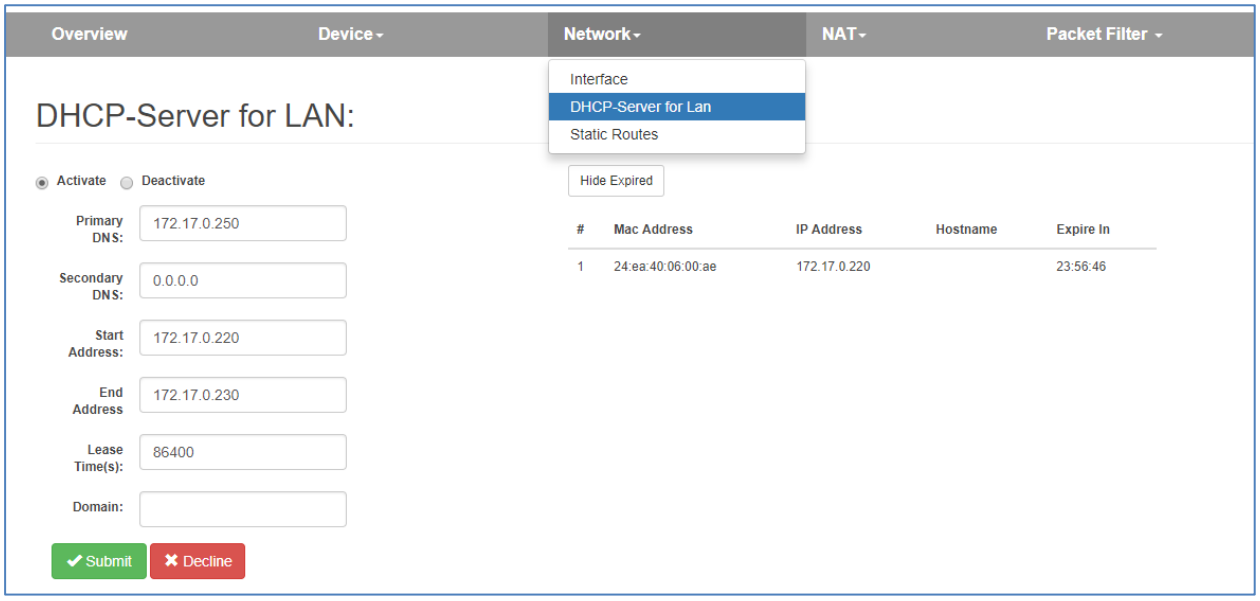
The search via the Siemens function “reachable participants” function does not work through the WALL IE firewall.

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: DNS server in the LAN for the assignment of the device name, after the WALL IE DHCP server has assigned the IP address to the device.

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

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

Lease Time (s): Time in seconds until the DHCP entry is rejected when the device is no longer logged in. 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: DHCP clients provided by the DHCP server become part of a domain, in which every network device can be identified by the indication of its device domain. DNS server entry for the device must be present in it.

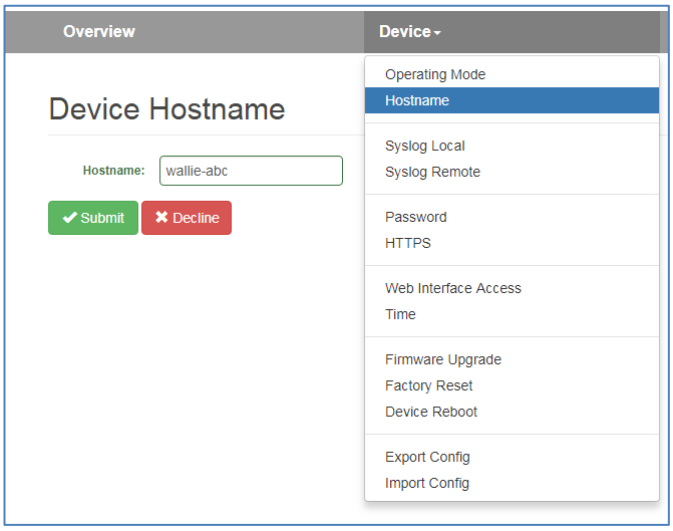
On the right side of the website there is a table of the IP addresses assigned by the DHCP server with the affiliated device MAC addresses.

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

11.2 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.



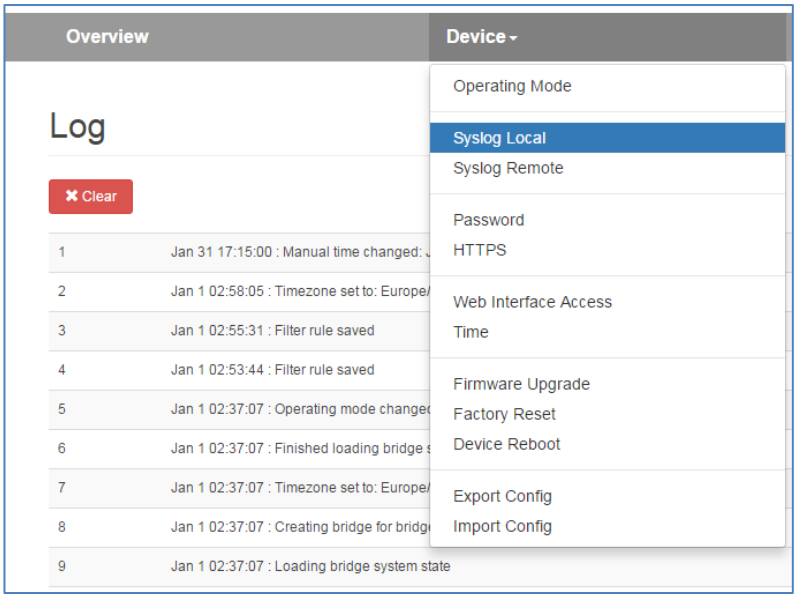
11.3 Syslog server

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. 11.7).

11.3.1 Syslog local

The local Syslog display lists the recorded events.

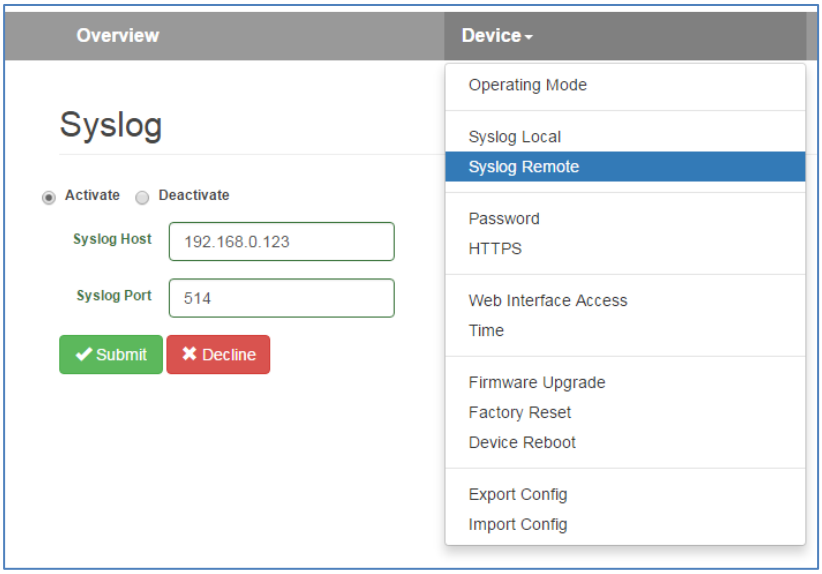
The Syslog memory can be deleted with “Clear”.



11.3.2 Syslog remote

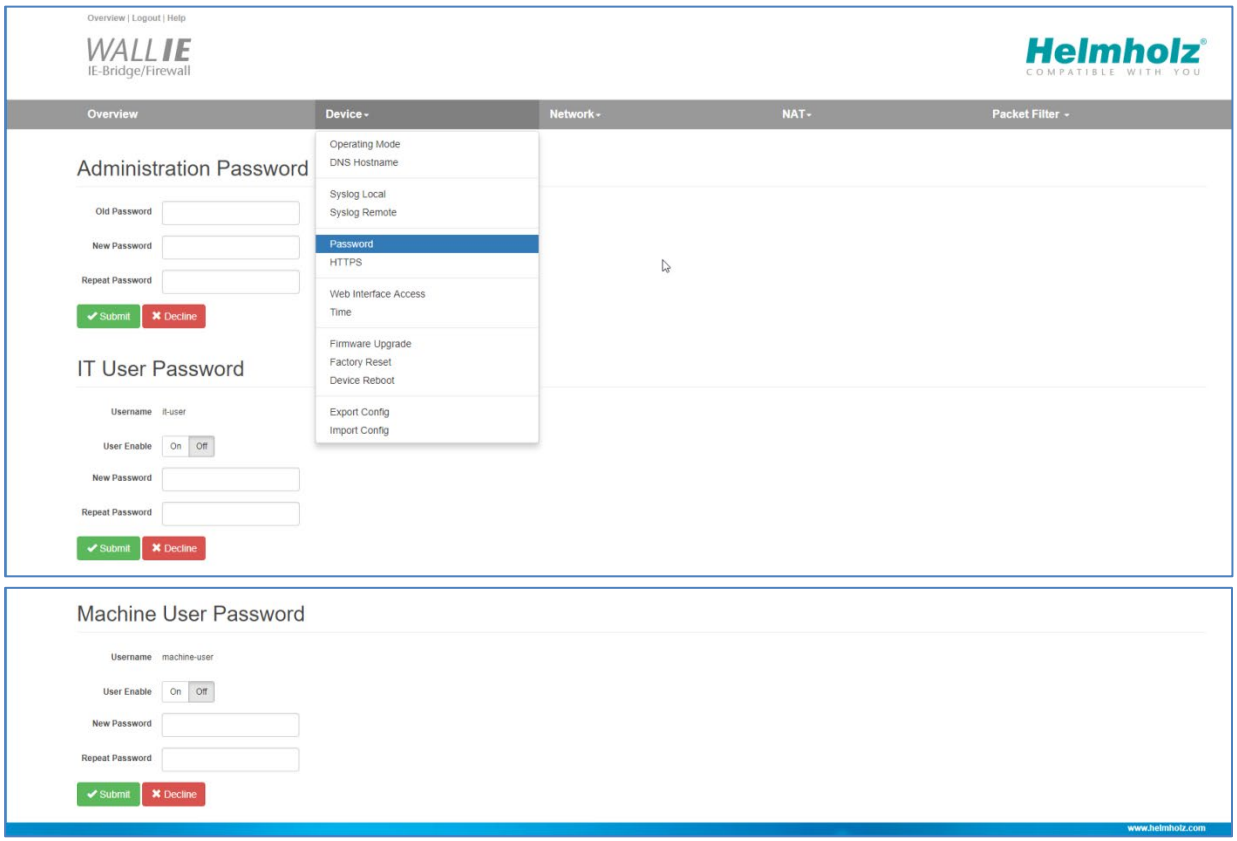
The Syslog messages can also be sent by the WALL IE to a PC through the network on which a program for Syslog recording is running.

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



11.4 Change password / 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:

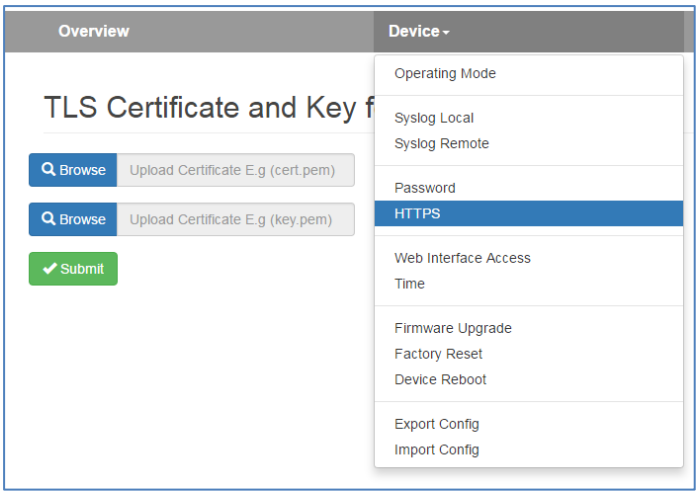
- Access to the WALL IE exclusively via the LAN interface
- Change to the settings of the DHCP server
- Changing of the Basic NAT/NAPT rules and settings

- 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”

11.5 File certificate (HTTPS)

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

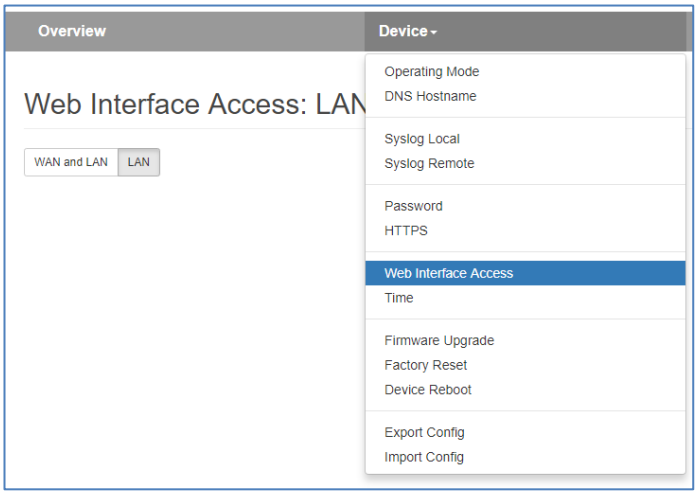
This ensures that the calling up of the WALL IE configuration website, in addition to the HTTPS encoding, is also trustworthy.



11.6 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".

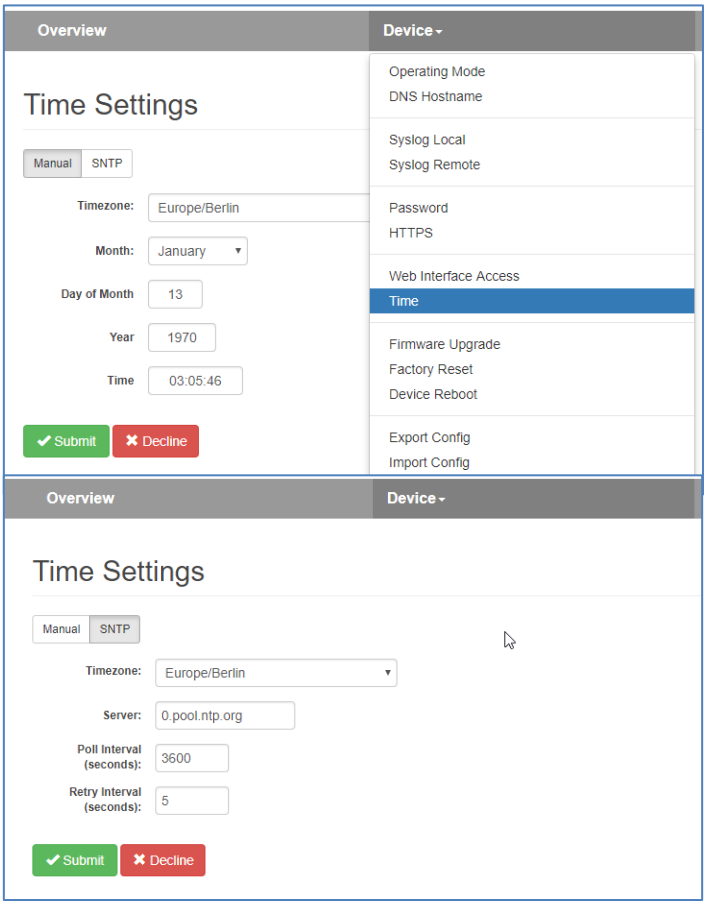


11.7 Time settings (Time)

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

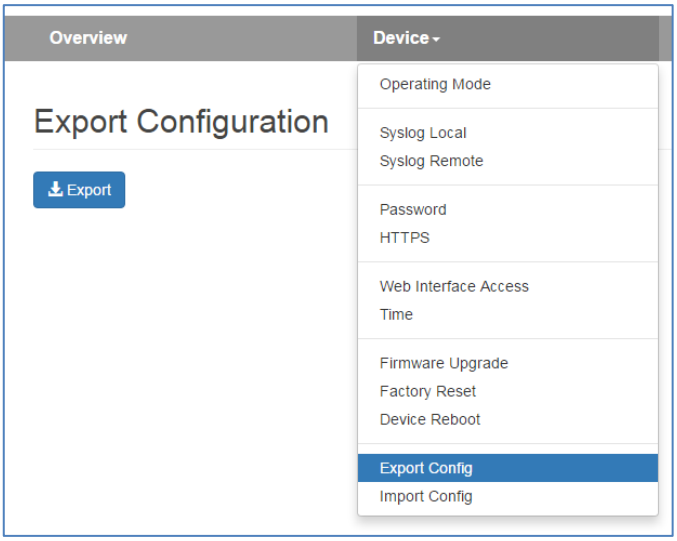
For “SNTP”, the default gateway and the DNS server must be configured in the interface settings in order that the SNTP service can reach the NTP server in the Internet

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

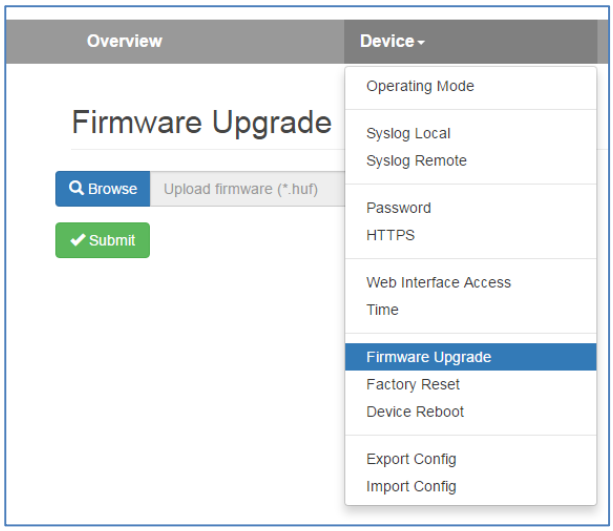
Link to the current firmware:
http://www.helmholz.de/goto/700-860-WAL01#tab-software

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

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 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

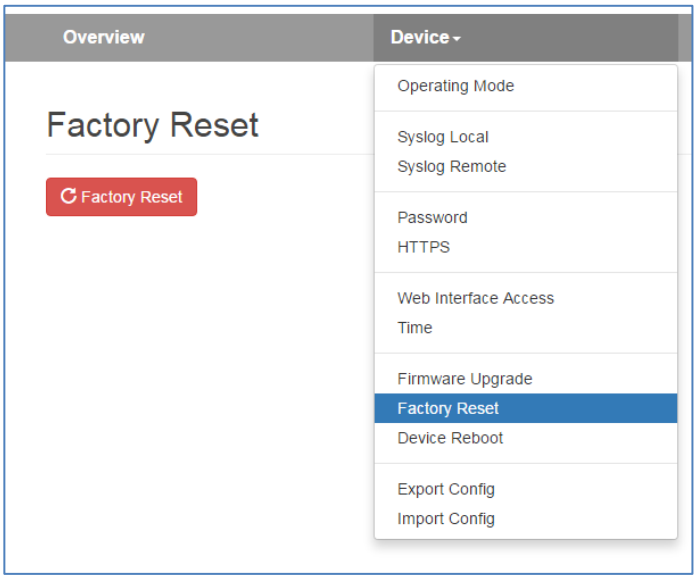
The resetting of the WALL IE to factory settings can be initiated both via the website and without access to the device with the “FCN” button.

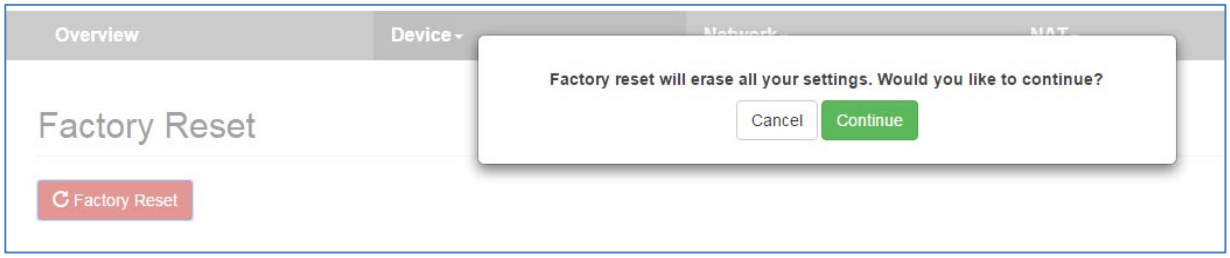
When resetting the WALL IE, the configuration is irretrievably deleted and the IP settings are set to the delivery status. The firmware remains at the current status in the process.

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.

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

14 FAQ

Are broadcasts or multicasts allowed through the WALL IE?

WALL IE is a TCP/IP NAT or Bridge device. It works on layers 3 and 4. Broadcasts and multicasts are blocked at WALL IE in both directions (LAN→WAN and WAN→LAN). The blocking of broadcasts thus also 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 blocked by the WALL IE.

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?

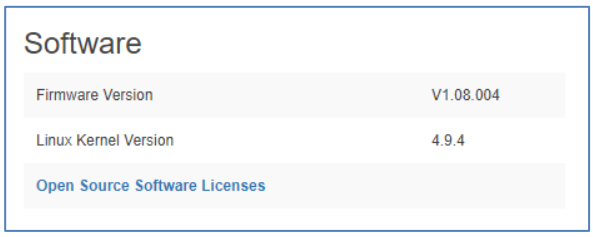
No, the WALL IE always only has one current configuration. However, it is possible to deactivate or activate individual packet filter rules or NAT entries via the lamp symbol. It is also possible to export, edit and import a WALL IE configuration again.

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.

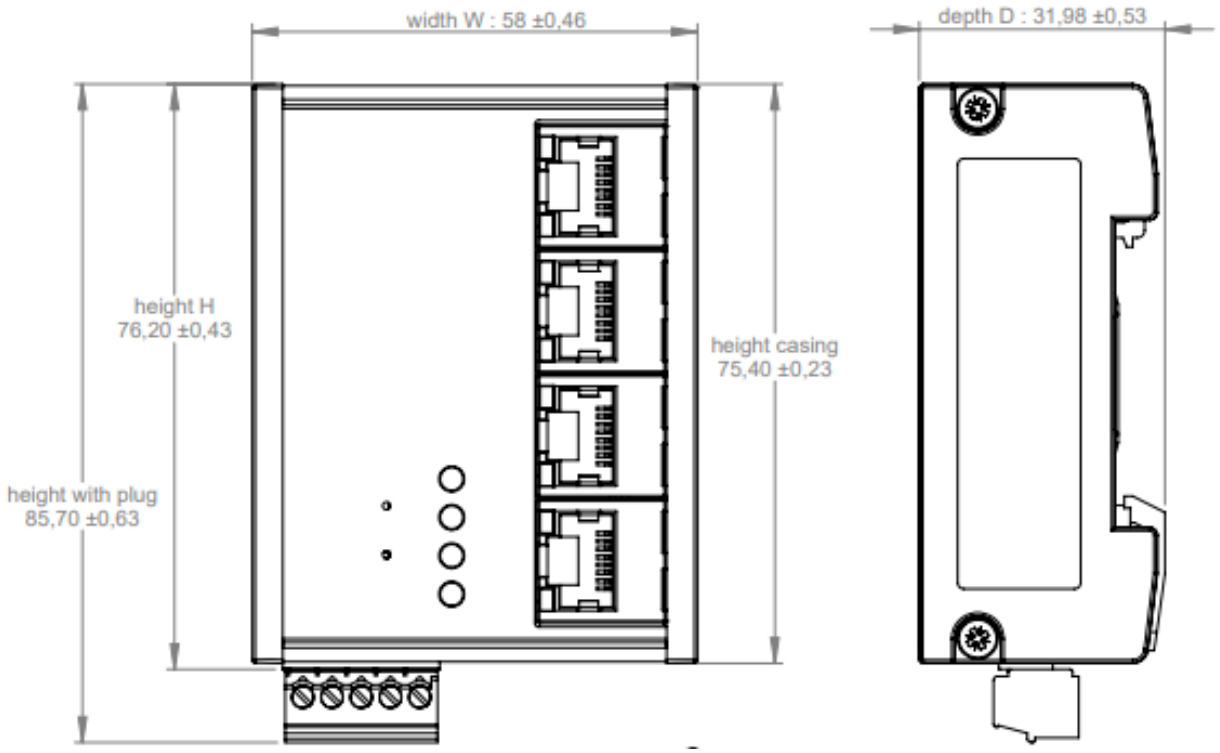
The most recent firmware can be downloaded at the website www.helmholz.de.

The installation of the firmware is described in chapter 12.



http://www.helmholz.de/goto/700-860-WAL01#tab-software

15 Technical data

Order no.	**700-860-WAL01**
Name	WALL IE
Scope of delivery	WALL LTE, Quick Start Guide
Dimensions (D x W x H)	32,5 x 58,5 x 76,5 mm
Weight	Approx. 130 g
WAN interface	
Number	1
Type	10 Base-T/100 Base-T
Connection	RJ45 socket
Transmission rate	10/100 Mbps
LAN interface	
Number	3, switched
Type	10 Base-T/100 Base-T
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
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	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
CE	
RoHS	Yes
REACH	Yes

15.1 Dimensioned drawing