



Quick Start Guide WALL IE / WALL IE PLUS, Industrial NAT Gateway/Firewall

Version
15 en

Order number:

WALL IE	700-860-WAL01	as of firmware V 1.10.100
WALL IE PLUS	700-862-WAL01	as of firmware V 1.00.000

Content

1	Safety instructions	3
2	Introduction	4
3	Connecting the WALL IE	5
4	Initial access to the web interface	6
5	Main view	7
6	Choosing the operating mode	7
6.1	The NAT operating mode	7
6.2	The Bridge operating mode	8
7	Application „NAT“	9
7.1	Adjustment of the IP addresses in the NAT operating mode	9
7.2	Setting up “Basic NAT” rules	10
7.3	Packet filter “WAN to LAN”	11
7.4	Packet filter “LAN to WAN”	12
7.5	SNAT	13
7.6	NAPT	14
7.7	Portforwarding	15
8	Application “Bridge”	16
8.1	Adjustment of the IP addresses in the bridge operating mode	16
8.2	Packet filter “WAN to LAN”	17
8.3	Packet filter “LAN to WAN”	18
9	Firmware update	19
10	LEDs status information	20
10.1.1	WALL IE (700-860-WAL01)	20
10.1.2	WALL IE PLUS (700-862-WAL01)	20
11	Function of the buttons	20
12	Technical data	21

1 Safety instructions

Target audience



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. 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.

Intended use



The device has a protection rating of IP 20 (open type) 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 operation, the doors of control boxes/cabinets must be closed and possibly locked during operation.

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!

Operation



ATTENTION
forbidden.

Successful and safe operation of the device requires proper transport, storage, setup, assembly, installation, commissioning, operation, and maintenance. Operate the device only in flawless condition. The permissible operating conditions and performance limits (technical data) must be adhered to. Retrofits, changes, or modifications to the device are strictly

Security



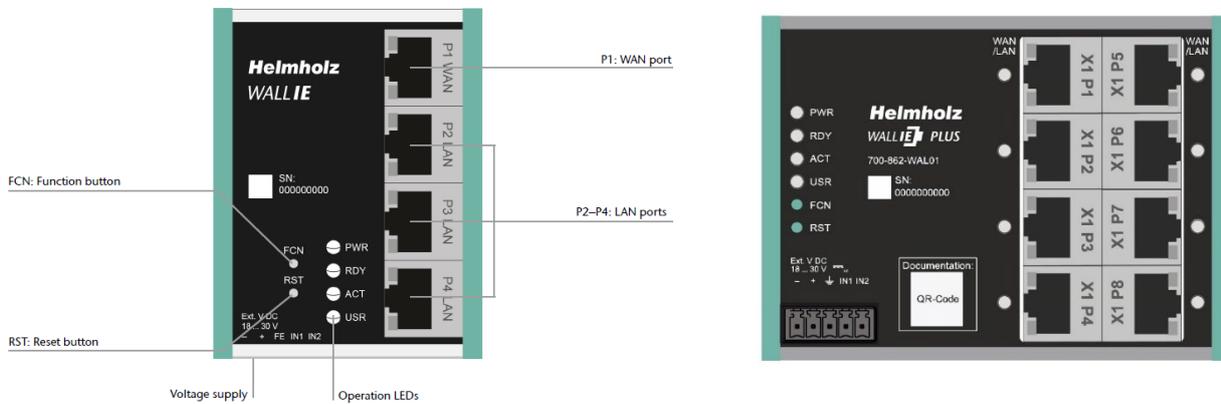
ATTENTION

The device is a network infrastructure component and therefore an important element in the security consideration of a plant. When using the device, therefore, observe the relevant recommendations to prevent unauthorized access to installations and systems. Further information on this can be found in the device manual.

2 Introduction

WALL IE, the Industrial NAT Gateway and Firewall, simply integrates machine networks into the high-level production or company network using network segmentation, packet and MAC address filtering.

Currently, the product range consists of two variants: **WALL IE (700-860-WAL01)** and **WALL IE PLUS (700-862-WAL01)**. Unless otherwise noted, this document describes functions that support both devices equally.



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 below.

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

This document explains the initial commissioning of the WALL IE using the "NAT" and "Bridge" application examples. Only the most important settings are explained.

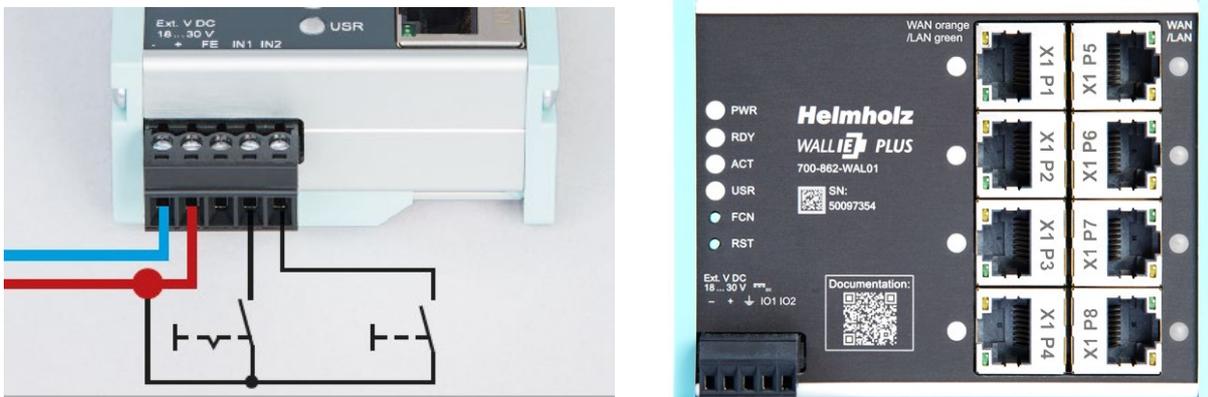


For a detailed description of all functions and important safety instructions, please refer to the WALL IE manual. This can be found at www.helmholz.de or scan the QR code directly.



3 Connecting the WALL IE

The WALL IE must be supplied with DC 24 V at the wide range input 18-30 V DC via the supplied connector plug. The connection (FE) is for the functional earth. Connect it properly to the reference potential. The WALL IE is designed exclusively for operation with safety extra-low voltage (SELV/PELV).



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

The RJ45 sockets "X1 P1" to "X1 P8" of the WALL IE PLUS (700-862-WAL01) can be assigned to the network WAN or LAN as desired. In the factory setting, port P1 is set for WAN and ports P2-P8 for LAN. The LEDs next to the port indicate the assignment, orange for WAN and green for LAN. Setting the assignment of the ports for WAN and LAN is possible in the web interface. More detailed information can be found in the manual.

The inputs IN1 and IN2 have no function in the current firmware version but will be available for external switching of firewall rules in a later firmware version.



NOTE

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



NOTE

The device may only be operated with power supplies that meet the specifications of EN/IEC 60950-1 for power sources of limited capacity. Otherwise, the device must be operated in an enclosure that meets the requirements of a fire protection enclosure according to EN/IEC 60950-1.

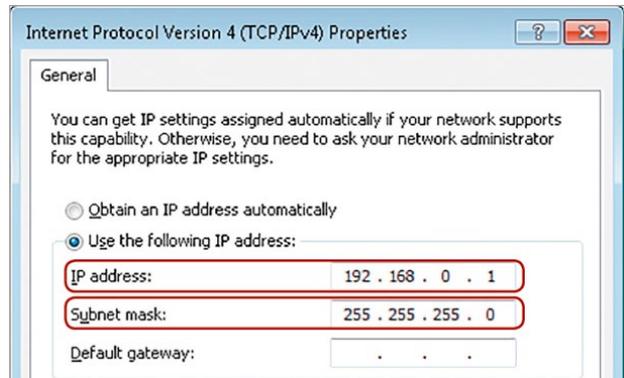
4 Initial access to the web interface

The WALL IE is delivered from the factory with the IP address 192.168.0.100 and the subnet mask 255.255.255.0 on the LAN side. Access to the web interface is possible with the WALL IE (700-860-WAL01) via the LAN ports P2 - P4. With the WALL IE PLUS (700-862-WAL01), access is possible via the ports P2 - P8 or via all ports whose LED lights up green in the delivery state.

The IP address of your network adapter must first be set in accordance with the IP subnet of the WALL IE: Start → Settings → Network and Internet → Change Adapter settings → 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.

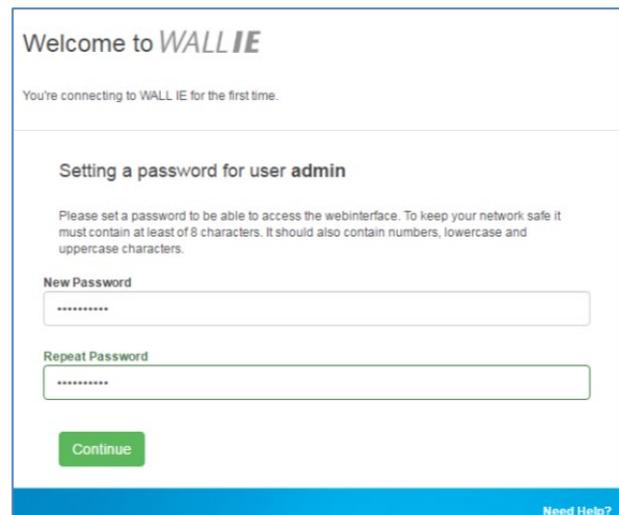
With the first login you will be requested to set a password for the “admin” user.

The password must contain at least 8 characters and can be up to 128 characters long, it can contain special characters and numbers. With the button "Continue" the password will be saved in the device and you will be redirected to the "Overview" page of the WALL IE.

The main user is always “admin”.

In addition to the main user, 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.



NOTE

Please memorize the password carefully! For security reasons, there is no way to reset the password without setting the device to factory settings.

5 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.

Overview | Logout | Help

WALL IE
NAT Gateway/Firewall

Helmholz®
COMPATIBLE WITH YOU

Overview Device - Network - NAT - Packet Filter -

Overview

Live Statistics

Uptime 0 days 23:01:17

System Time 2/1/1970 01:16:53

Current User admin

Device Configuration

Timezone Europe/Berlin

Operating Mode NAT

INTERFACE

DNS 10.10.1.250

GATEWAY 10.10.1.251

DHCP Server OFF

Software

Firmware Version V1.08.200

Linux Kernel Version 4.9.4

Open Source Software Licenses

Hardware

Serial Number 00000293

Order Number 700-860-WAL01

Hardware Revision 1-1

LAN MAC Address 24-EA-40-0F-01-25

WAN MAC Address 24-EA-40-0E-01-25

www.helmholz.de



NOTE

Please check the WALL IE website for a newer firmware version. The firmware update is described on page 19.

Firmware link: <http://www.helmholz.de/goto/700-860-WAL01#tab-software>



6 Choosing the operating mode

Depending on the application for the WALL IE, the operating mode must be defined at the beginning. WALL IE supports two basic modes of operation: NAT and Bridge.

6.1 The NAT operating mode

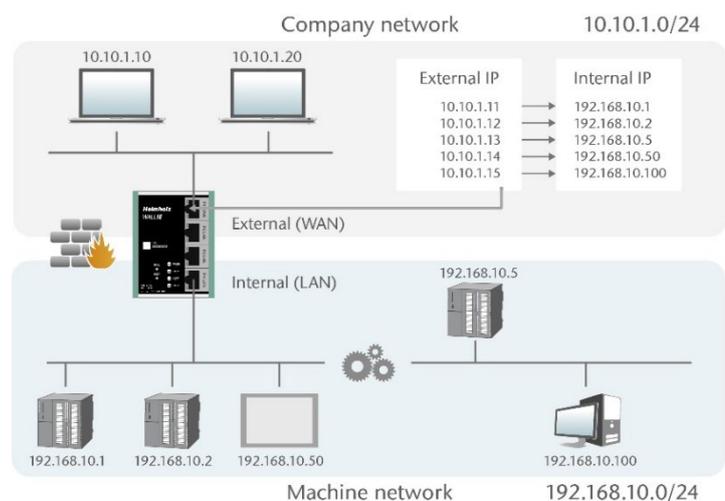
When an automation cell with preset IP addresses is to be incorporated into a company network with other IP addresses, the IP addresses of the machine must normally all be set again.

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 company network.

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

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

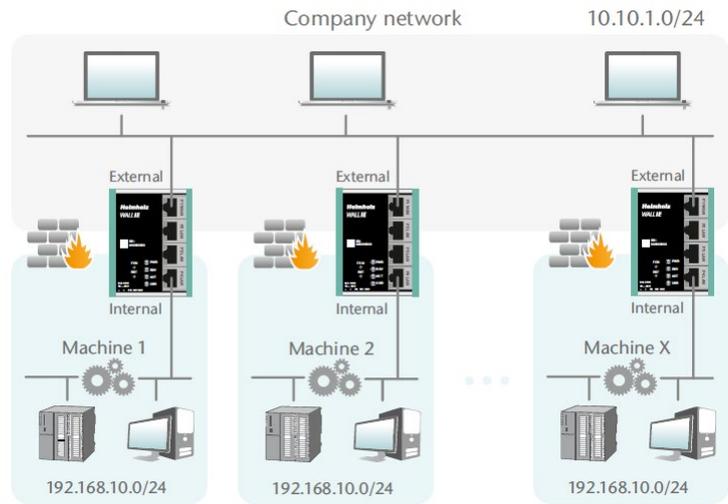


Basic NAT, also known as “1:1 NAT” or “Static NAT”, is the translation of individual IP addresses or of complete IP address ranges.

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

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

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



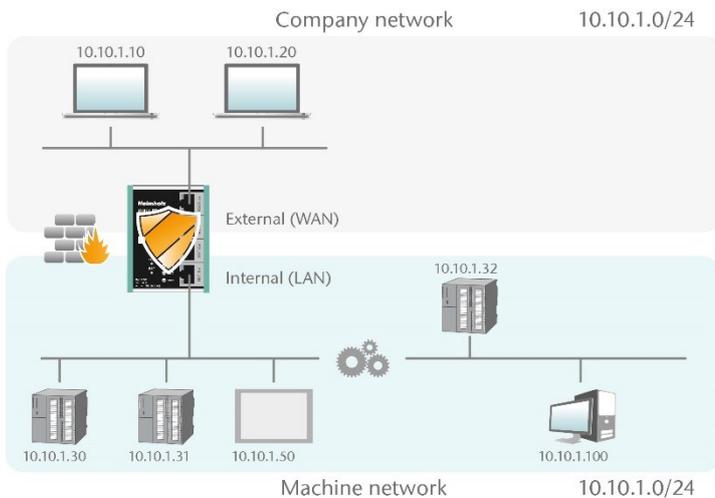
If “NAT” is your planned application case, please continue reading on page 9.

6.2 The Bridge operating mode

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

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

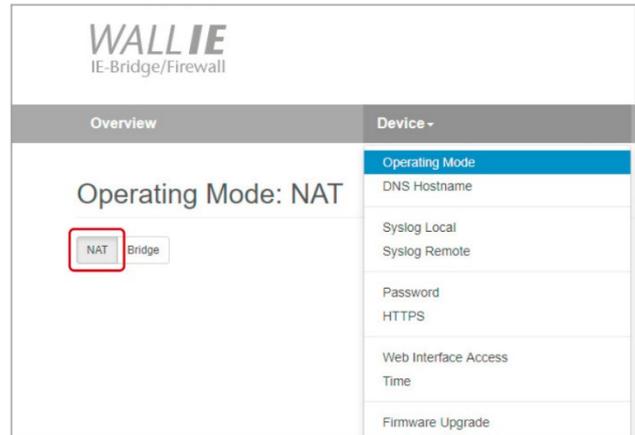
This allows the separation of part of the company network without using different network addresses.



If “bridge” is your planned application case, please continue reading on page 16.

7 Application „NAT“

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

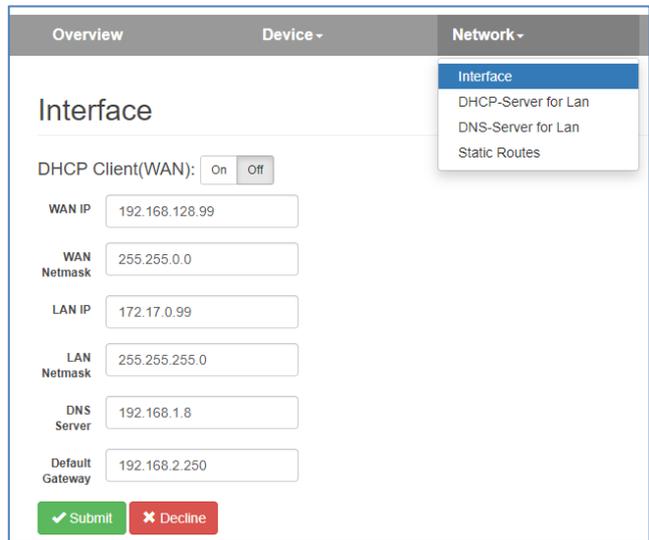


7.1 Adjustment of the IP addresses in the NAT operating mode

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. It is necessary to indicate a DNS server for the SNTP service.

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



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



ATTENTION

If you change the LAN IP address, you may need to reopen the WALL IE web page on the browser under the new IP address and log in again.

7.2 Setting up “Basic NAT” rules

To use Basic NAT functionalities, the operating mode of the WALL IE must be set to "NAT". Select the "NAT" menu and the "Basic NAT" submenu. Enter the first rule and save it using the  button.



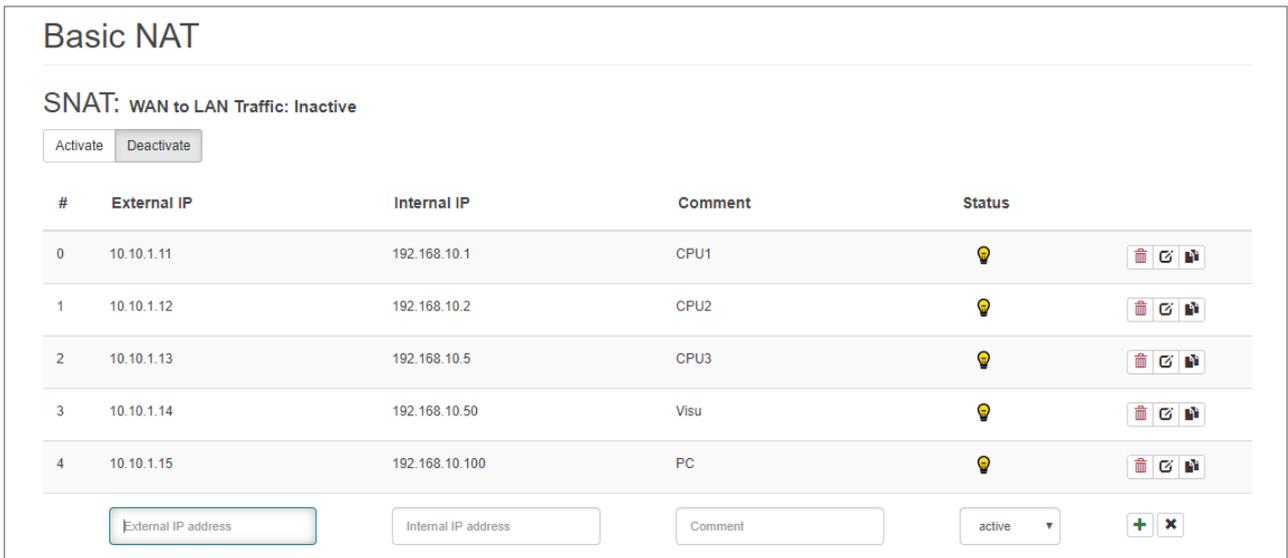
Basic NAT

SNAT: WAN to LAN Traffic: Inactive

Activate Deactivate

#	External IP	Internal IP	Comment	Status
0	10.10.1.11	192.168.10.1	CPU1	active

The "External IP" is a free IP address from the WAN IP address range. This must not have been assigned to any other Ethernet station (in the WAN) yet! The "Internal IP" is the existing IP address of the network node in the machine (LAN). As “Comment” any text can be entered. With this 'additional WAN interface' the address conversion ("natting") to the entered LAN IP (the target device) is then realized in the WALL IE.



Basic NAT

SNAT: WAN to LAN Traffic: Inactive

Activate Deactivate

#	External IP	Internal IP	Comment	Status
0	10.10.1.11	192.168.10.1	CPU1	🔆
1	10.10.1.12	192.168.10.2	CPU2	🔆
2	10.10.1.13	192.168.10.5	CPU3	🔆
3	10.10.1.14	192.168.10.50	Visu	🔆
4	10.10.1.15	192.168.10.100	PC	🔆

External IP address Internal IP address Comment active

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

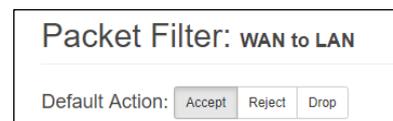
 = Rule is inactive, a click on the lamp symbol changes the rule status to active

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



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



Packet Filter: WAN to LAN

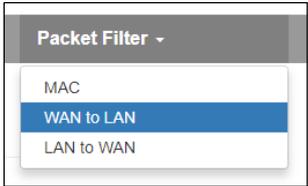
Default Action: Accept Reject Drop

7.3 Packet filter “WAN to LAN”

The packet filters can be used to restrict access between the company network (WAN) and the machine network (LAN). For example, it can be configured that only certain subscribers from the company network are allowed to exchange data with defined subscribers from the automation cell.

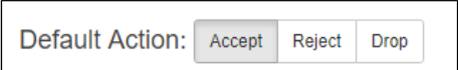
The following filter criteria on layers 3 and 4 are available: IPv4 addresses, protocol (TCP/UDP/ICMP), and ports.

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

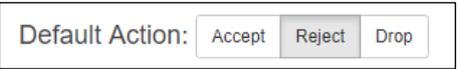


With the “Default Option” you can set whether all frames are generally allowed (“Accept”) and only special packets are filtered (“Blacklisting”), or whether all frames are generally prohibited (“Reject” / “Drop”) and only those frames are allowed to pass through that correspond with the filter rules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

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

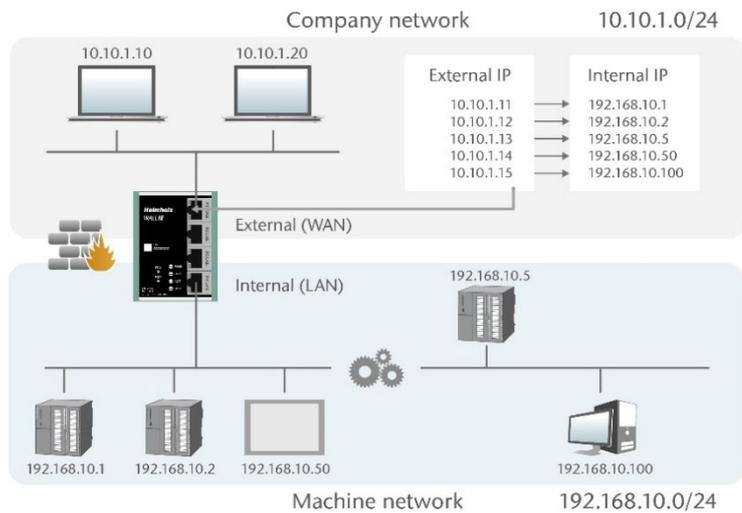


In order to limit access to the machine network to certain participants in the WAN, set the default action to “Reject” or “Drop”. In the case of prohibited frames from the WAN, “Reject” sends an error message in response, while “Drop” rejects the frame without sending an error message.

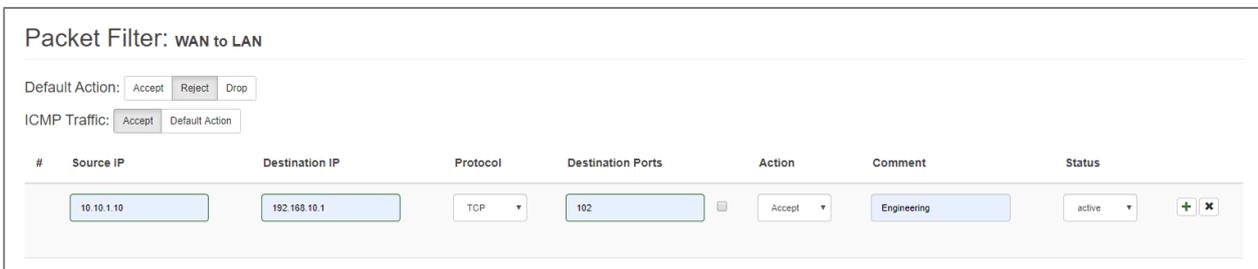


Example: A PC in the company network (WAN) has the IP address 10.10.1.11 (e.g. a visualization).

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 company network (WAN).

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

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

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

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

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

3	10.10.1.1-10.10.1.9	192.168.10.1	TCP	1.65535	Accept	Many	🟡
4	10.10.1.200	192.168.10.1-192.168.10.200	TCP	1.65535	Accept	All LAN access	🟡

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).

7.4 Packet filter “LAN to WAN”

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

The screenshot shows the configuration page for a Packet Filter named "LAN to WAN". At the top, there are tabs for Overview, Device, Network, NAT, and Packet Filter. The Packet Filter tab is active, showing a dropdown menu with options: MAC, WAN to LAN, and LAN to WAN (which is selected). Below the menu, the "Default Action" is set to "Accept" (with "Reject" and "Drop" as options). The "ICMP Traffic" is set to "Accept" (with "Default Action" as an option). A table below shows the filter rule configuration with columns for #, Source IP, Destination IP, Protocol, Destination Ports, Action, Comment, and Status. Below the table is a form for adding a new rule with fields for Source IP address, Destination IP address, Protocol (set to TCP), Destination Ports, Action (set to Accept), Comment, and Status (set to active).

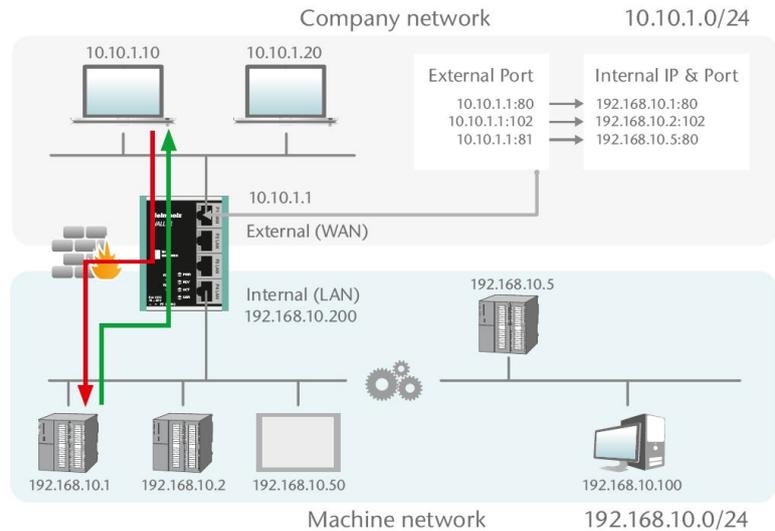
General rule can be changed by setting the "Default Action" to "Reject" or "Drop". In addition to general rule, filtering can be further customized using specific packet filter rules."

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

7.5 SNAT

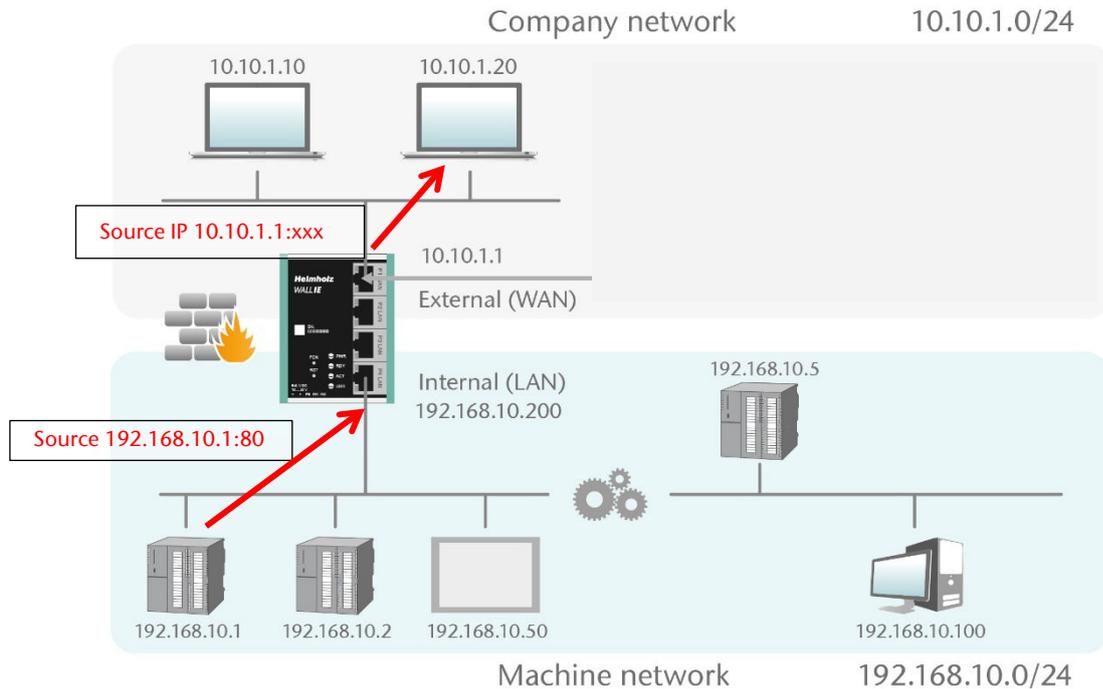
The function “SNAT (Source NAT)” transparently forwards incoming traffic from the WAN side to the LAN network. To all packets, forwarded on LAN side by WALL IE, source IP address is replaced with WALL IE LAN IP address.

Therefore, none of the LAN participants needs the 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.



7.6 NAPT

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



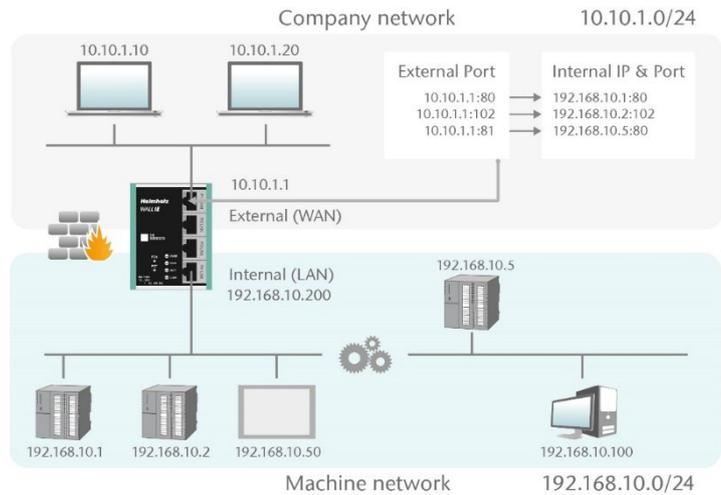
In order for the communication from LAN to WAN to work when NAPT is activated, the WALL IE LAN IP address must be entered as gateway in all devices on the LAN!

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

7.7 Portforwarding

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.



Overview
Device ▾
Network ▾
NAT ▾
Packet Filter ▾

Basic NAT

NAPT

NAPT

NAPT: LAN to WAN Traffic: Inactive

Port Forwarding: WAN (10.10.1.99) to LAN Traffic

#	Protocol	External Port	Internal IP	Internal Port	Comment	Status
0	TCP	81	192.168.10.1	80	CPU1	💡 🗑️ 📧 🖨️

TCP ▾

active ▾
+
×

Protocol: “TCP” or “UDP”

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

Internal IP: IP address of device connected to LAN.

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

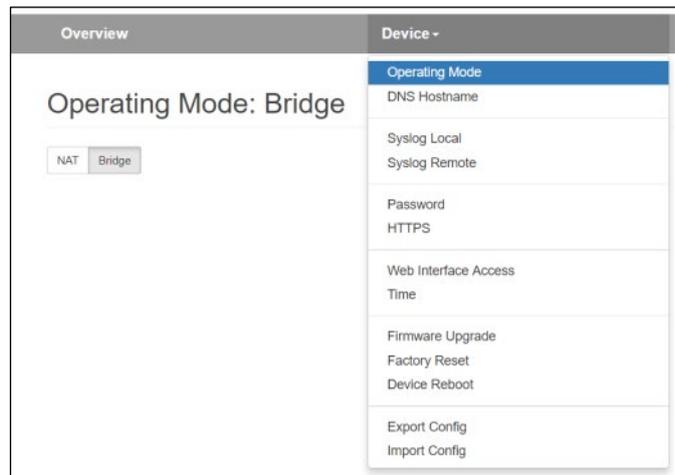
Comment: Freely definable comment.



"Portforwarding" and "Basic NAT" can be used simultaneously in NAT operating mode. If the default action for the "WAN to LAN" packet filters is set to "Reject" or "Drop", corresponding filter rules for access must also be created for each port forwarding entry.

8 Application “Bridge”

To activate the bridge operating mode, select the "Operating Mode" menu item in the "Device" menu and set it to "Bridge".

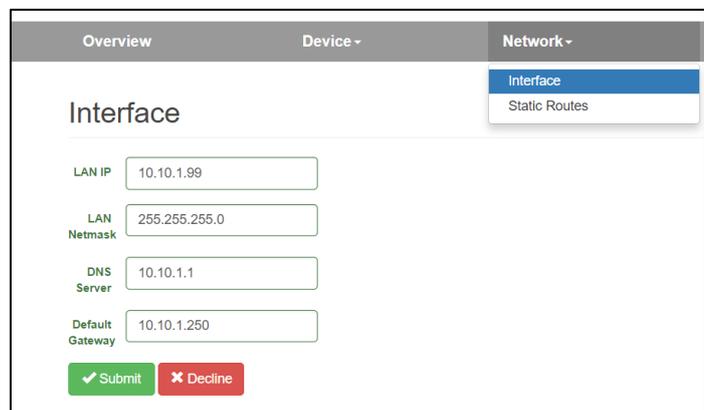


8.1 Adjustment of the IP addresses in the bridge operating mode

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

A DNS server and a default gateway can also be 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.

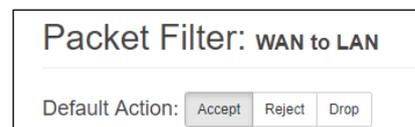
The entry is saved with the “Submit” button and the IP settings are thus activated immediately. The current entry is rejected without acceptance with “Decline”.



NOTE

If you change the LAN IP address, you may need to reopen the WALL IE web page on the browser under the new IP address and log in again.

In bridge mode, all ports are initially blocked for "WAN-to-LAN" data traffic for security reasons! To allow access, packet filter rules must be created or the "Default Action" for the packet filters must be set to "Accept".



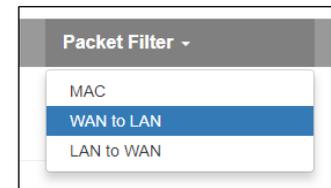
LAN to WAN traffic is always enabled by default but can also be restricted by packet filters or the default action.

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

8.2 Packet filter “WAN to LAN”

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

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



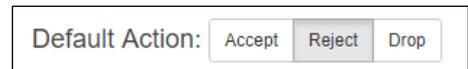
Select the “WAN to LAN” menu point in the “Packet Filter” menu.

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

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

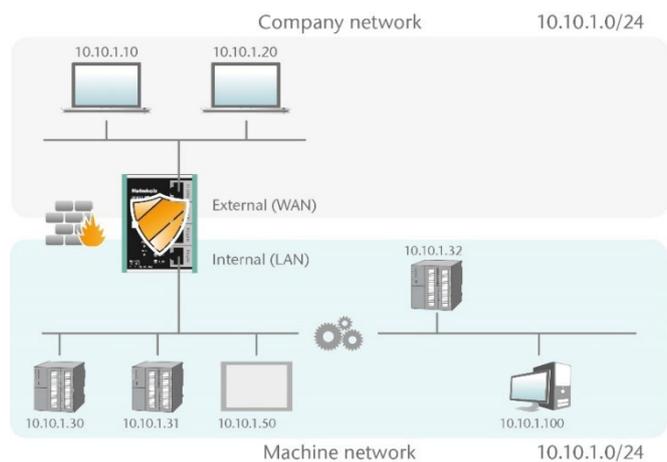


In order to limit access to the machine network to certain participants in the WAN, set the default action to “Reject” or “Drop”. In the case of prohibited frames from the WAN, “Reject” sends an error message in response, while “Drop” rejects the frame without sending an error message.



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

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



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

Packet Filter: WAN to LAN

Default Action: Accept Reject Drop

ICMP Traffic: Accept Default Action

#	Source IP	Destination IP	Protocol	Destination Ports	Action	Comment	Status
	10.10.1.10	10.10.1.30	TCP	102	Accept	CPU1	active

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

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

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

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

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

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

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

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

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

8.3 Packet filter “LAN to WAN”

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

The screenshot displays the configuration for a packet filter rule named "LAN to WAN". At the top, there are tabs for "Overview", "Device", "Network", and "Packet Filter", with "Packet Filter" being the active tab. Below the tabs, the rule name "Packet Filter: LAN to WAN" is shown. There are two rows of buttons: "Default Action" with options "Accept", "Reject", and "Drop"; and "ICMP Traffic" with options "Accept" and "Default Action". Below these is a table with columns: "#", "Source IP", "Destination IP", "Protocol", "Destination Ports", "Action", "Comment", and "Status". The table contains one row with input fields for "Source IP address", "Destination IP address", a dropdown for "TCP", a text field for "Ports", a dropdown for "Accept", a text field for "Comment", and a dropdown for "active". To the right of the table are plus and minus icons.

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

9 Firmware update

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



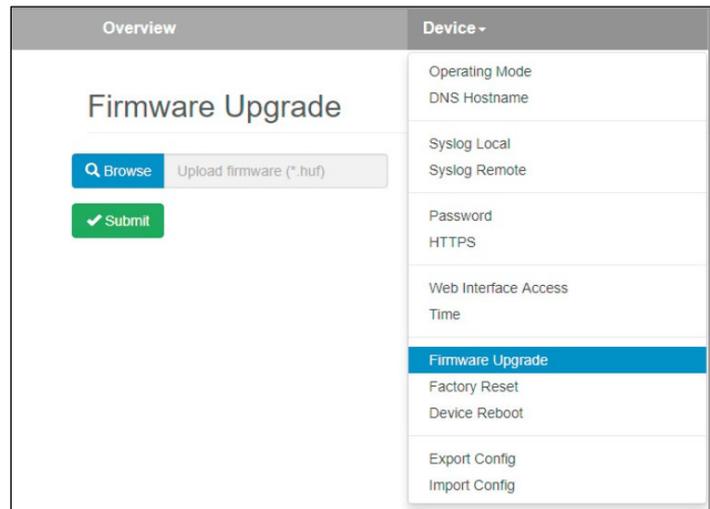
Link to firmware: <http://www.helmholz.de/goto/700-860-WAL01#tab-software> or scan the QR code.

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

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

The firmware file is then transferred to the WALL IE. This can take up to 1 minute.

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



ATTENTION

During the update process, the operation of the WALL IE is interrupted. Do not switch off the device during the update process..



NOTE

The configuration of the WALL IE is retained when updating to a higher version, as far as this is technically possible. However, a "downgrade" to an older firmware version can lead to configuration errors. It is recommended to perform a factory reset after a downgrade.



NOTE

After a firmware update it may be necessary to clear the browser cache once to update outdated JavaScript elements of the WALL IE website.

10 LEDs status information

10.1.1 WALL IE (700-860-WAL01)

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



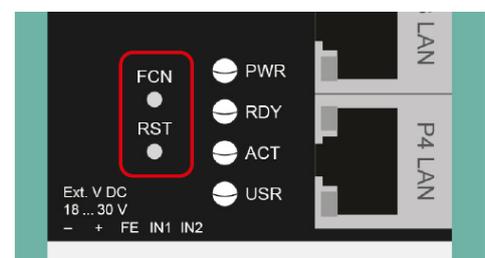
10.1.2 WALL IE PLUS (700-862-WAL01)

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



11 Function of the buttons

The "FCN" button can be used to reset the WALL IE to **factory settings**. The "FCN" button must be held down during the start-up phase of the WALL IE. The successful resetting of the parameters and settings is acknowledged by the "USR" LED lighting up during the boot process. The "FCN" button can then be released.



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

12 Technical data

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

Order no.	700-862-WAL01
Name	WALL IE PLUS, Industrial NAT Gateway/Firewall
Dimensions (D x W x H)	34.5 x 101.5 x 75.5 mm
Weight	approx. 230 g
WAN/LAN interface	
Number	8, switched
Type	100Base-Tx/1000Base-T
Connection	RJ45 socket
Transmission rate	100/1000 Mbps
Operating modes	Bridge, NAT (Basic NAT, NAPT)
Packet filter	IPV4 addresses, protocol (TCP/UDP), ports ("WAN to LAN" and "LAN to WAN" separate), MAC addresses (black & whitelisting)
Status indicator	4 LEDs function status, 8 LEDs Ethernet status
Voltage supply	24 V DC, 18–30 V DC
Current draw	max. 275 mA at 24 V DC
Power dissipation	max. 6,7 W
Ambient conditions	
Installation position	Any
Ambient temperature	0 °C ... +60 °C
Transport and storage temperature	-40 °C ... +85 °C
Relative air humidity	95 % r H without condensation
Pollution degree	2
Protection rating	IP20
Certification	CE
RoHS	Yes
REACH	Yes



NOTE

The contents of this Quick Start Guide have been checked by us so as to ensure that they match the hardware and software described. However, we assume no liability for any existing differences, as these cannot be fully ruled out. The information in this Quick Start Guide is, however, updated on a regular basis. When using your purchased products, please make sure to use the latest version of this Quick Start Guide, which can be viewed and downloaded on the Internet from www.helmholz.de.

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.

Our customers are important to us, we are happy to receive suggestions and ideas for improvement. If you have any questions regarding the use of the product, please contact Helmholz Support by phone or send an e-mail to support@helmholz.de.

All trademarks shown or mentioned in this document are the property of their respective owners or manufacturers. The representation and naming serve exclusively to explain the use and setting options of the products documented here.