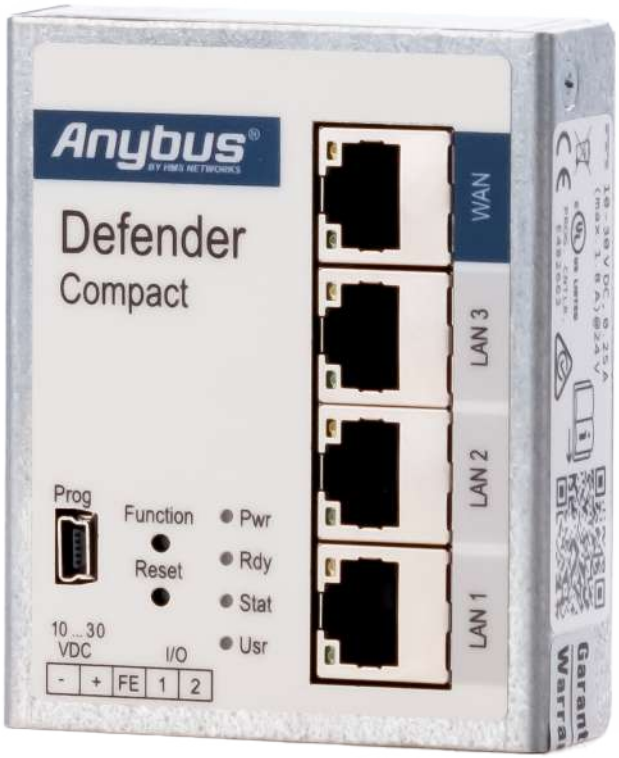
ENGLISH

Anybus® Defender Compact Manager
Instructions for use

ABD1004-NATFW
Version: 1.2.8
Publication date 2026-03-25



Important User Information

Disclaimer

The information in this document is for informational purposes only. Please inform HMS Networks of any inaccuracies or omissions found in this document. HMS Networks disclaims any responsibility or liability for any errors that may appear in this document.
HMS Networks reserves the right to modify its products in line with its policy of continuous product development. The information in this document shall therefore not be construed as a commitment on the part of HMS Networks and is subject to change without notice. HMS Networks makes no commitment to update or keep current the information in this document.
The data, examples and illustrations found in this document are included for illustrative purposes and are only intended to help improve understanding of the functionality and handling of the product. In view of the wide range of possible applications of the product, and because of the many variables and requirements associated with any particular implementation, HMS Networks cannot assume responsibility or liability for actual use based on the data, examples or illustrations included in this document nor for any damages incurred during installation of the product. Those responsible for the use of the product must acquire sufficient knowledge in order to ensure that the product is used correctly in their specific application and that the application meets all performance and safety requirements including any applicable laws, regulations, codes and standards. Further, HMS Networks will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features or functional side effects found outside the documented scope of the product. The effects caused by any direct or indirect use of such aspects of the product are undefined and may include e.g. compatibility issues and stability issues.

Copyright © 2026 HMS Networks

Contact Information

Postal address:
Box 4126
300 04 Halmstad, Sweden
E-Mail: info@hms.se

Use of open-source software

General

Our products contain, amongst others, so-called open-source software that is provided by third parties and has been published for free public use. The open-source software is subject to special open-source software licenses and the copyright of third parties.

Basically, each customer can use the open-source soft-ware freely in compliance with the licensing terms of the respective producers. The rights of the customer to use the open-source software beyond the purpose of our products are regulated in detail by the respective concerned open-source software licenses. The customer uses the open-source software freely, as provided in the respective effective license, beyond the purpose that the open-source software gets in our products. In case there is a contradiction between the licensing terms for one of our products and the respective open-source software license, the respective relevant open-source software license takes priority over our licensing terms, as far as the respective open-source software is concerned by this.

The use of the used open-source software is possible free of charge. We do not demand usage fees or any comparable fees for the use of the open-source software contained in our products. The use of the open-source software in our products by the customer is not part of the earnings we achieve with the contractual compensation.

For software that is published under the GPLv2 License, the following applies:

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 2 of the License, or (at your option) any later version. This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details. You should have received a copy of the GNU General Public License along with this program.

If not, see <https://www.gnu.org/licenses/>.

All open-source software programs contained in our products can be taken from the available list. The most important open-source software licenses are listed in the Licenses section at the end of this publication. As far as programs contained in our products are subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), the Berkeley Software Distribution (BSD), the Massachusetts Institute of Technology (MIT) or another open-source software license, which regulates that the source code must be made available, and if this software is not already delivered in source code on a data carrier with our product, we will send you this at any time upon request. If it is required to send this on a data carrier, the sending will be made against payment of a cost compensation of Euro 35,00.

Our offer to send the source code upon request ceases automatically 3 years after delivery of our product to the customer. Requests must be directed to the following address, if possible, under specification of the serial number:

HMS Networks
Box 4126
300 04 Halmstad, Sweden
E-Mail: info@hms.se

Special liability provisions

We assume no responsibility or liability if the open-source software programs included in our products are used by customers in a manner that no longer corresponds to the purpose of the contract which serves as the basis for the purchase of our products. This applies in particular to any use of the open-source software programs outside of our products. The warranty and liability provisions, which stipulate the applicable open-source software license for the corresponding open-source software, as listed below, apply to the use of open-source software beyond the contractual purpose. In particular, we are also not liable if the open-source software in our products or the entire software configuration in our products is changed. The warranty contained in the contract, which forms the basis for the purchase of our products, applies only to unchanged open-source software and the unchanged software configuration in our products.

Open-source software used

For a list of the open-source software used in our products, visit
https://www.hms-networks.com/p/abd1004-natfw-anybus-defender-compact-1004-nat-fw?tab=tab-support

Table of contents

Important User Information ..... - 2 -

Use of open-source software ..... - 3 -

Table of contents ..... - 4 -

1 General ..... - 5 -

1.1 Brief description of the Anybus Defender Compact Manager ..... - 6 -

1.2 Biref description of the industrial firewall Anybus Defender Compact ABD1004-NATFW ..... - 7 -

2 Just a few steps to the configured firewall ..... - 8 -

3 Installation of the Anybus Defender Compact manager ..... - 8 -

3.1 System requirements ..... - 8 -

3.2 Latest software version ..... - 9 -

3.3 Installing Anybus Defender Compact Manager ..... - 9 -

3.4 Location of the Anybus Defender Compact files ..... - 9 -

4 The user interface - overview ..... - 10 -

4.1 Menu bar ..... - 11 -

4.2 Access rights for the individual user levels ..... - 23 -

5 Create a project ..... - 26 -

5.1 Device project - device: The principle ..... - 28 -

5.2 Device project with or without a password? ..... - 29 -

6 Configuration ..... - 30 -

6.1 Start ..... - 31 -

6.2 Settings ..... - 50 -

6.3 Diagnosis ..... - 83 -

6.4 Reset to factory settings ..... - 84 -

7 Application examples ..... - 87 -

7.1 Network segmenting of the same network addresses ..... - 87 -

7.2 Network segmenting of dissimilar network addresses ..... - 88 -

7.3 Use of SNAT ..... - 89 -

7.4 Access to multiple devices behind the firewall ..... - 90 -

7.5 Access to individual services behind the firewall ..... - 91 -

1 General

Purpose of this documentation

This document describes the installation and configuration of the Anybus Defender Compact Manager software, version **V1.2.8**, for the ***Anybus Defender Compact*** ABD1004-NATFW industrial firewall, firmware version **V1.4.1**.

Please read carefully and store somewhere safe.

Version notes

Version	Date	Comment
V 1.1.0	Mar 19th, 2018	-
V 1.2	May 20th, 2019	General fixes and enhancements
V 1.2.1	Oct 25th, 2019	Changes to the description for devices in the hardware version HW02 *
V 1.2.2	Apr 1st, 2020	General fixes and enhancements
V 1.2.7	Sep 3rd, 2020	General fixes and enhancements Add information about "**Access rights of individual user levels**". Change when creating a device project (chapter "First start"). It is no longer mandatory to assign a project password. Description of the "operator" and "viewer" users available as of version V 1.2.7 in the "System" chapter. The device (Anybus Defender Compact) can now also be reset to its factory settings using the "admin" user. See chapter "Reset to factory settings". The network participants displayed can now be deleted in the network overview. See chapter "Packet filter> Device view (mapping table)". The column widths of the tables for "SimpleNAT", "DNAT" and in the "Packet filter" can be adjusted with the mouse pointer. In the "Diagnostics" chapter, the status of "I/0 1" and "I/0 2" is displayed in the device graphics.
1.2.7 DR01	Feb 15th, 2022	General fixes and enhancements
1.2.8	Sep 12th, 2025	Fix LAN port label mismatch in diagnosis view

Latest software/manuals and other information

Current software, manuals and further information about products for secure remote maintenance can be found in the download portal at https://www.hms-networks.com

A free version of the ***Anybus Defender Compact Manager*** can be downloaded at https://www.hms-networks.com/downloads.

1.1 Brief description of the Anybus Defender Compact Manager

The ***Anybus Defender Compact Manager*** is a configuration software that supports you in the configuration of your industrial firewall ***Anybus Defender Compact ABD1004-NATFW*** and extends the performance spectrum of the firewall.

- Improved workflow of the user
  - ° Working on several projects during one session
  - ° Settings can be changed online
  - ° Projects can be shared in encrypted project containers
- Graphical User Interface
  - ° PLC programming-like environment
  - ° View configuration and changes
  - ° See how setup and rules apply
- Learning Mode
  - ° Visualize actively communicating devices
  - ° Chose general traffic policies
  - ° Finely adjustable individual connection settings
- Interactive configuration wizard
  - ° In online or offline mode
  - ° For Bridge or Gateway operating mode

The integrated learn function of the firewall records all connections. Then, with the aid of the recorded packet table, the user decides which connections are to be permitted and disables all the others.
The function MapView aids the user in the straightforward performance of this task. This unique graphical portrayal gives the user a view of which connections are currently configured in the firewall and which net- work clients have been detected.
Additionally, the network architecture and activities can be documented with it.

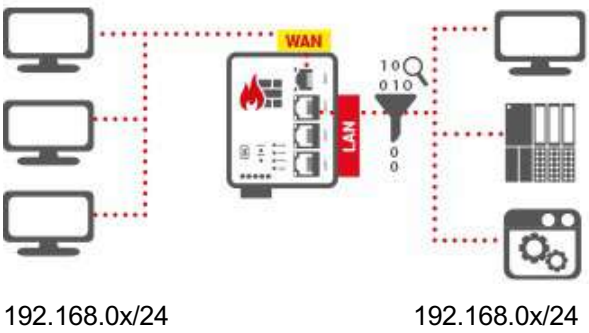
To condition the data traffic, the industrial firewall filters the permissible and forbidden data traffic based on the originating MAC/IP addresses, the destination MAC/IP addresses and the ports. Of course, all other firewall functions such as NAT, port forwarding and routing are implemented.

A free version of the ***Anybus Defender Compact Manager*** can be downloaded at https://www.hms-networks.com/downloads.

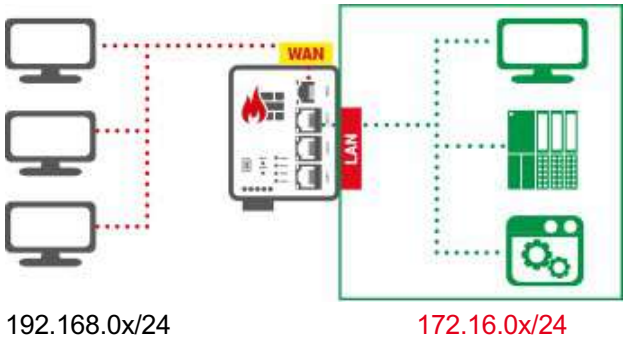
1.2 Biref description of the industrial firewall Anybus Defender Compact ABD1004-NATFW

The ***Anybus Defender Compact*** (ABD1004-NATFW) is a „self-learning“ easy-to-configure industrial firewall.
It can be used in both Bridge and Gateway mode.

Bridge mode



Gateway modus



The configuration is made via the USB interface using the

a. CLI (Command Line Interface)

b. software ***Anybus Defender Compact*** Manager

Performance characteristics

- Protects the machines in the network from attacks from the Internet.
- Easy network segmentation with controlled routing and NAT.
- Convenient learning mode makes creation of filter tables simple & easy.
- Integration into existing networks.
- Bridge or Gateway mode.
- IP, port, and protocol filters to monitor and restrict traffic.
- Configuration with secure software.
- Less attack vectors by avoiding a web interface.
- Versatile NAT functionalities, eg 1: 1 NAT, SimpleNAT and port forwarding.

Further information about the industrial firewall ***Anybus Defender Compact*** ABD1004-NATFW can be found in the "Quick start-up guide" or on our website at www.hms-networks.com.

2 Just a few steps to the configured firewall

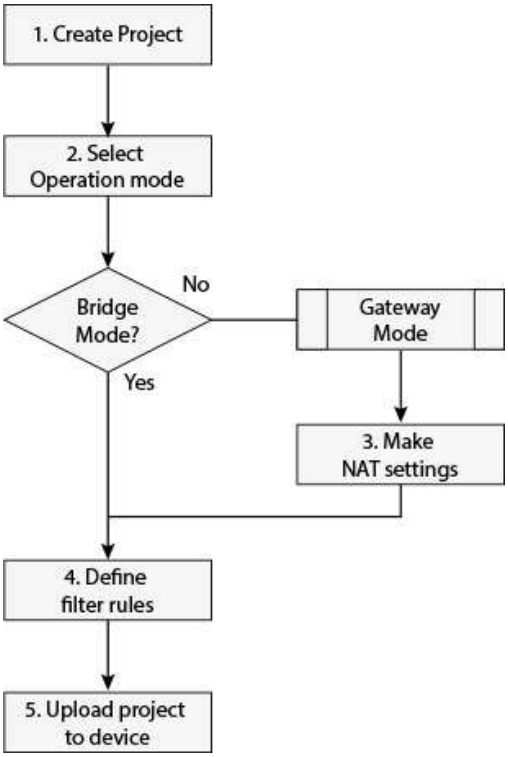
1. **Create a Project**
   Create a separate device project for each device (Anybus Defender Compact).

2. **Select operation mode**
   Depending on the application case, choose between Bridge Mode and Gateway Mode.

3. Make **NAT** settings (only gateway mode)
   Edit the NAT (Network Address Translation).

4. Define filter **mode** and create filter **rules**
   Define the global firewall settings and create the specific rules.

5. **Upload** project **settings** to device
   Connect the device to your configuration PC and upload your project settings to the device.



NOTICE

Quick Setup An interactive configuration wizard is available to help you configure the firewall.

3 Installation of the Anybus Defender Compact manager

3.1 System requirements

System requirements

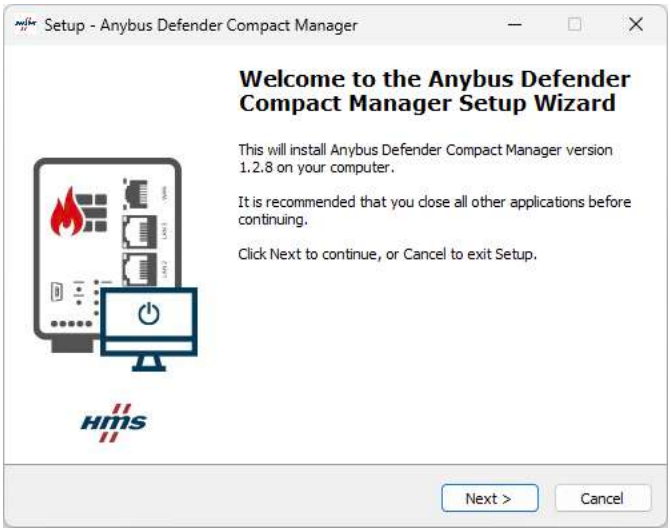
- Standard Windows PC
  - Windows 7 (32 / 64 Bit)
  - Windows 8 (64 Bit)
  - Windows 10 (64 Bit)
  - Windows 11 (64 Bit)
- Administrator rights
- At least 25 MB storage

3.2 Latest software version

a. A free version of the ***Anybus Defender Compact*** Manager can be downloaded at https://www.hms-networks.com/downloads.

b. In the **Help** menu of the ***Anybus Defender Compact*** Manager you can "**Check for updates**" and download and install the latest firmware.

3.3 Installing Anybus Defender Compact Manager



1. Start the installation by double-clicking on the installation file to run it and then following the sub- sequent instructions.
2. Click on “Next” to continue with the installation.

3.4 Location of the Anybus Defender Compact files

When installing the ***Anybus Defender Compact*** Manager on your PC, the "**abdcmngr**" folder is automatically created. This folder can be found at: **C:\Users***YouUser***\AppData\Roaming\abdcmngr**

In this directory are the subfolders:

\ drivers

\ events

\ projects

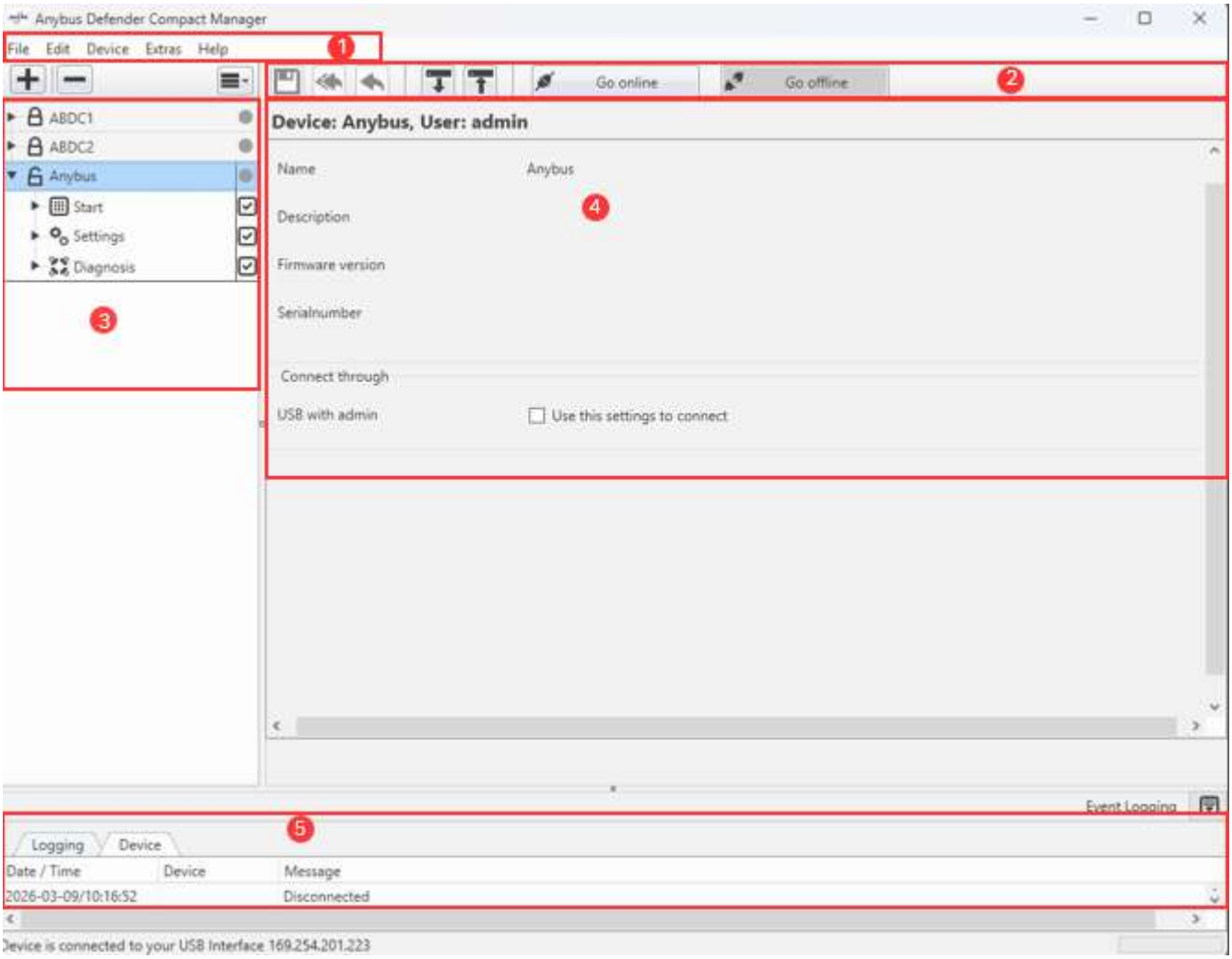
\ settings

\ updates

In the subfolder "projects", all projects with their project-related data (configuration, users, settings, etc.) are saved here.

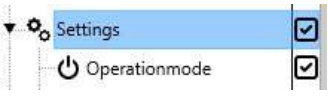
4 The user interface - overview

1. Start ***Anybus Defender Compact*** Manager via your PC's start menu or via the corresponding desktop symbol.

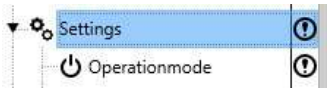


Interface layout

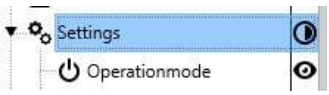
1. **Menu bar** - Miscellaneous tabs for calling submenus.
2. **Buttons** - These are used for communication with the connected devices.
3. **Configuration Menu** - Here all projects are listed with their configuration menus.
   The individual configuration areas are labelled with a symbol that signals the status of the processing.



Configuration is saved.



Configuration has been changed in the relevant menu but not yet saved in the project file.
To accept the data, the project file must be saved.

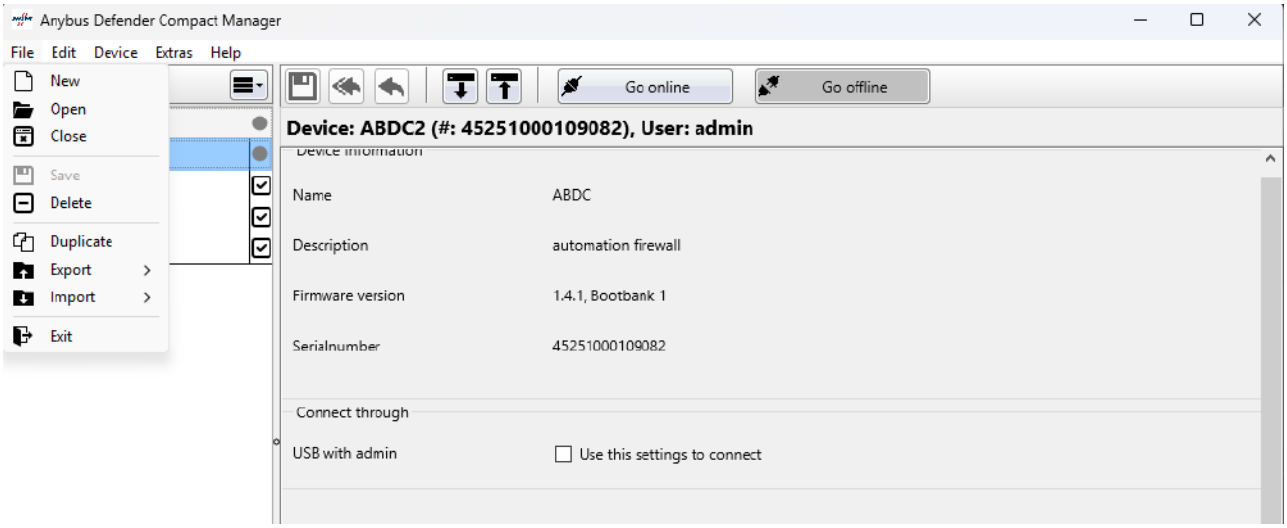


The configuration is transferred by downloading the data in the project file.
To accept the data, the project file must be saved.

4. **Main window** - The individual settings for the configuration menus are defined here.
5. **Event list** - Listing of all logged events in total or by device.

4.1 Menu bar

4.1.1 File



4.1.1.1. File > New

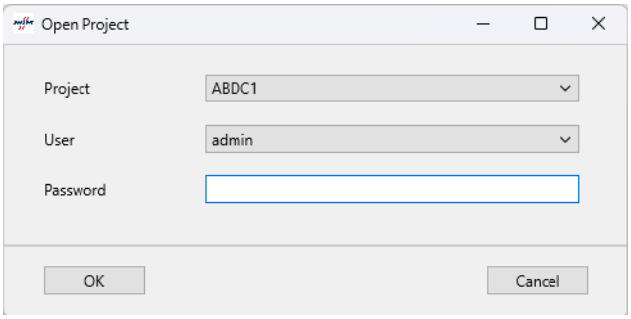
- Creation of further projects (see also "Create a project", Page 34)

4.1.1.2 File > Open

- Open a project by specification of the corresponding project password.

A project can also be selected directly in the storage area.

You can open and edit multiple projects.



An open project can be recognized by the symbol (open lock Anybus Defender Compact1) in front of the project name.

4.1.1.3 File > Close

- Close an open and selected project.

4.1.1.4. File > Safe

- Save an open and selected project.

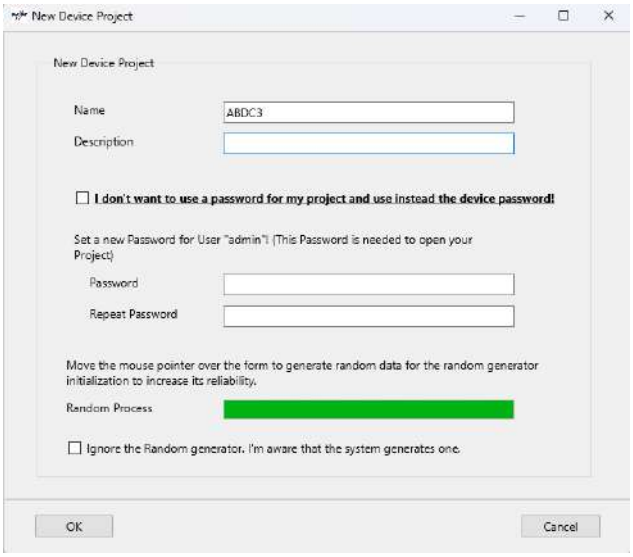
4.1.1.5 File > Delete

- Delete an open and selected project.

4.1.1.6 File > Duplicate

- Make a copy of the currently open and selected project.

Also give the project a unique name, a description (optional) and optionally set the associated project password.



NOTICE

When a project is duplicated, the entire content is copied, but a new RSA key pair is generated.

4.1.1.7 File > Export > Project

- Create a project file (* .nfp) from an open and selected project.

You can use the export function to share projects. Here, a project is distributed easily and securely in an encrypted container. This container can only be unpacked via the import function of the ***Anybus Defender Compact Manager***.

NOTICE

Please note that the keys (public kex and private key) are passed on or duplicated when sharing an exported project.

4.1.1.8 File > Export > Configuration

- Create a configuration file (* .cfg) from an open and selected project.

NOTICE

This configuration file contains the basic settings of a project and is helpful for analysis in case of support.

This configuration file contains no keys or passwords and cannot be imported back into a project.

4.1.1.9 File > Import

- Import a Project file (*.nfp).

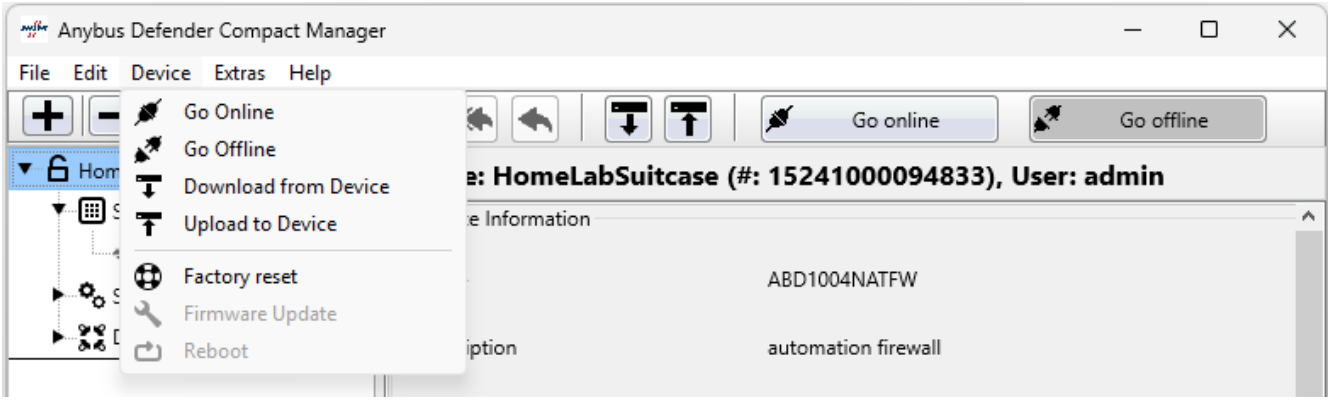
NOTICE

When importing a project (*.nfp file), a new project is automatically created on the target computer.
An existing project with the same name cannot be overwritten.
To open an imported project you need the original password.

4.1.1.10 File > Exit

- Closes the current application.

4.1.2 Device (Anybus Defender Compact hardware)



NOTICE

The following functions assume that a Device (***Anybus Defender Compact***) is connected to the same PC on which the
Anybus Defender Compact manager is also installed. Use the supplied USB cable

- When connecting to the device for the first time.
- **Anyway**, if you need to reset the device to factory settings.

- With certain settings and configurations (see details "Access rights for the individual user levels").
- And / or if the configuration access level is set to WAN / LAN inactive (see "System").

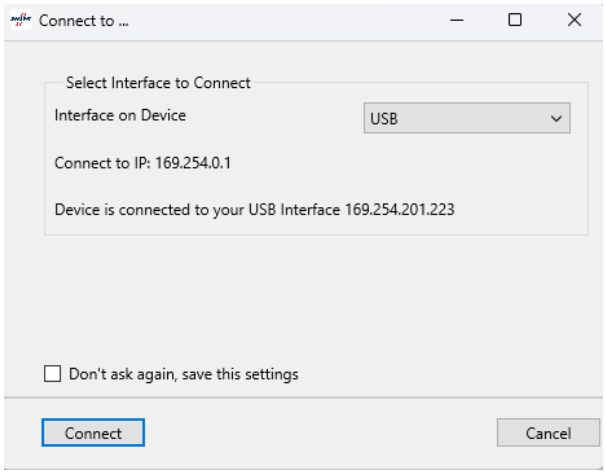
If the Configuration Access Level is set to WAN / LAN active and the access rights permit it, connect the PC and the device with a network cable.

4.1.2.1 Device > Go Online

Connect the ***Anybus Defender Compact*** via the USB interface with your PC and select

Device > Go online

Connect the Anybus Defender Compact to your PC via the USB inter- face and select **Device > Go online.**

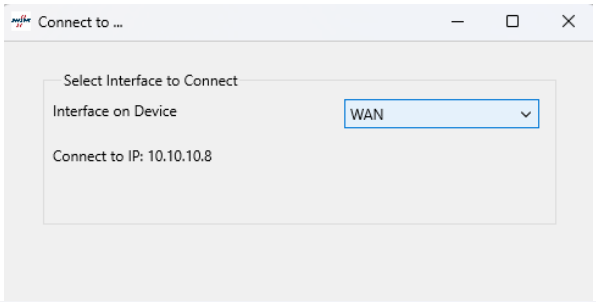


In rare cases you may need to update the USB driver for the "device to PC" connection.

Select "**Extras > Install USB Driver**" from the menu bar to update the USB driver.

Alternatively, you can establish the connection via the WAN or one of the LAN interfaces.

Please note the requirements for this, see " System" > *Configuration Access Level* and the "Access rights for the individual user levels"

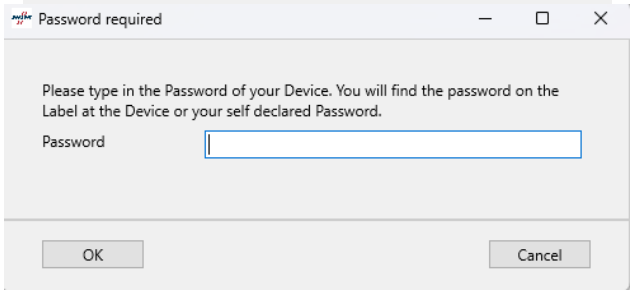


The password required for communication (device password) must be entered for the first connection to the device.

The device password is on a label on the back of the device.

Please note that the password is case-sensitive.

The changed device password can then be used for later connections.



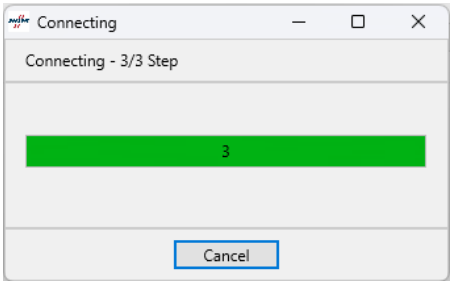
NOTICE

If you have created your project with a project password, you no longer need a password after Project-Device pairing.

NOTICE

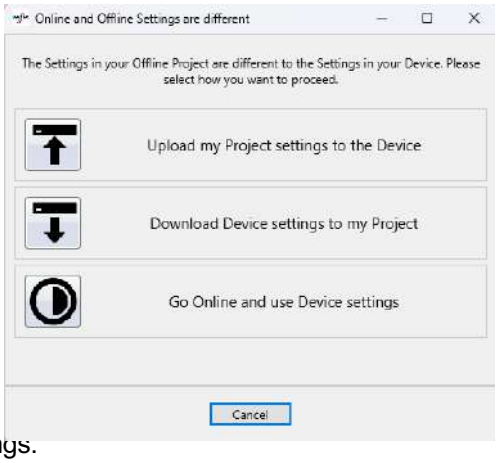
After the first connection from a Project to a Device (Go online) **and** uploading the Project settings to the Device, the **Project-Device Pairing** is complete.

The ***Anybus Defender Compact*** establishes a connection to the connected Device.



If the device settings differ from the Project settings, you can specify here how the different data states should be handled.

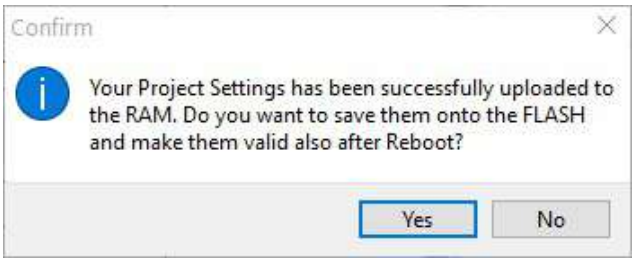
Select the desired process or click on “Cancel” to remain offline:



Upload my Project settings to the Device

- The Device settings are overwritten by the Project settings.

In the following message: "*Your Project Settings has been successfully uploaded to the RAM. Do you want to save them onto the FLASH and make them valid also after Reboot?*" you decide whether the data should be stored permanently or temporarily on the device.



- **Yes** = The settings are permanently stored on the device and are retained beyond a device restart.
- **No** = The settings are saved only temporarily (until a device restart).

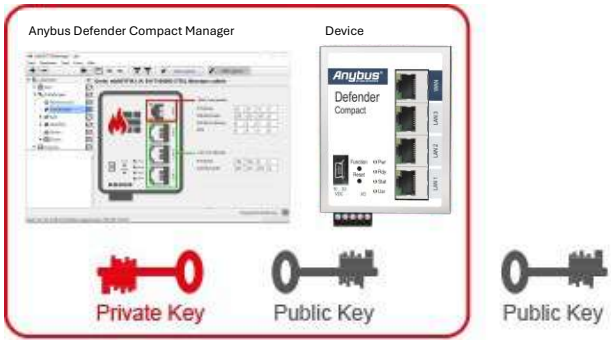
NOTICE

After the first connection from a Project to a Device (Go online) **and** uploading the Project settings to the Device, the **Project-Device Pairing** is complete.

After **Project-Device Pairing**, the "Public Key" is saved in the device and the device password is no longer active.

Access to the pairing takes place via the existing Project password.

The device password is required again if you want to reset the device to its factory settings.



Download Device settings to my Project

- After a confirmation prompt, the project settings are overwritten by the device settings.

Go Online and use Device settings

- With this selection you can edit the device settings directly.
- From here you can

  - upload the Project settings to the Device

  - download the Device settings to your Project

- If you go offline without making any changes, the Project settings will be restored.

4.1.2.2 Device Go Offline

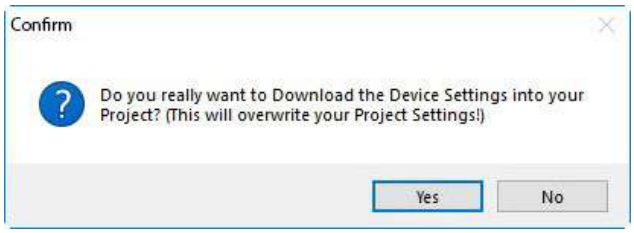
- The connection to the Device is disconnected and you are working again with the Project settings.

4.1.2.3 Device > Download Device Settings

Download from Device

This will download the device settings to the Project.

After confirming the security message with "Yes", the project settings are overwritten by the device settings.

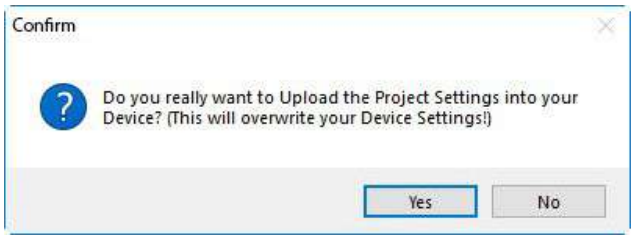


4.1.2.4 Device > Upload Project Settings to the Device

Upload to Device

Here, the Project settings are uploaded to the connected Device.

After confirming the security message with "Yes", the Device settings are overwritten by the Project settings.



4.1.2.5 Device > Factory reset

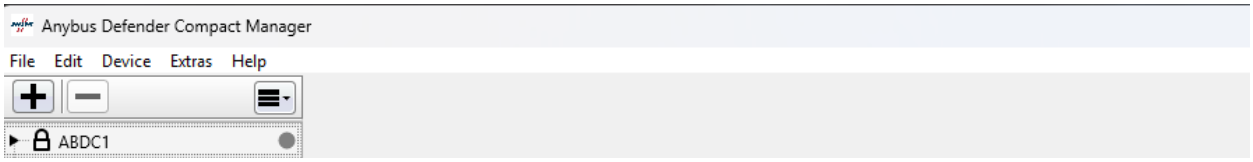
NOTICE

The ***Anybus Defender Compact*** is only reset to its factory settings by the user "factory reset" and only via the USB interface.

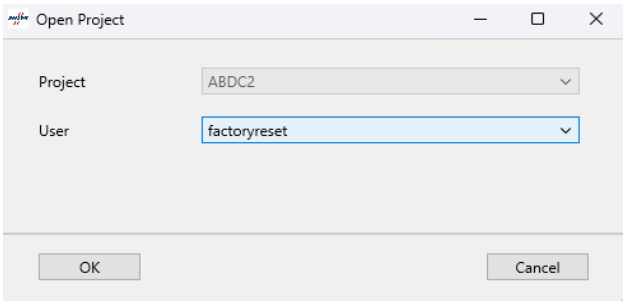
If you are logged in as the "admin" user, you can also carry out the action directly without having to log out and log in again with the user "factoryreset".

Furthermore, you always need the original device password for this action, even if the device is already paired or the device password has been changed.

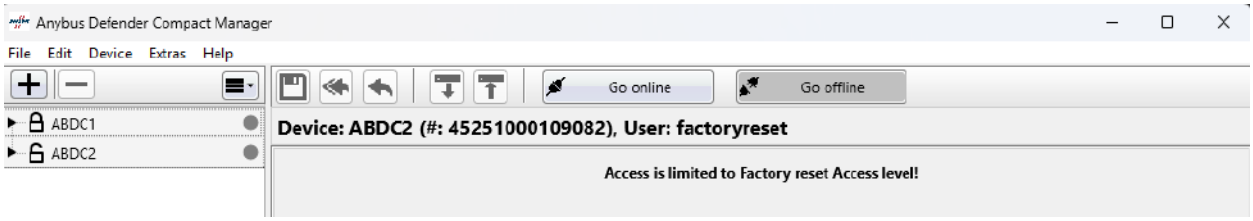
1. Select the project file that is paired with the device (***Anybus Defender Compact***) that should be reset to its factory set- tings.



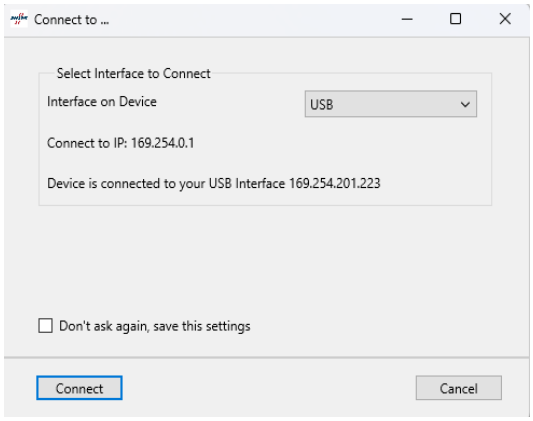
2. Select user "admin" or "factoryreset" and confirm with "OK".



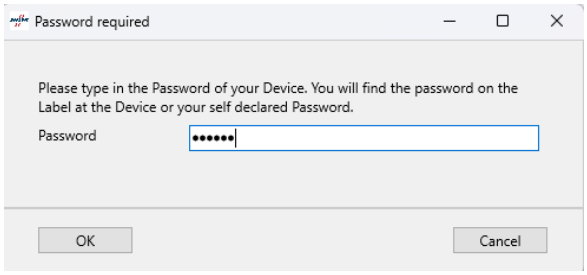
3. Click on the button “Go Online" in the main menu.



4. Make sure that "USB" is selected for the interface to be connected and click on "Connect".

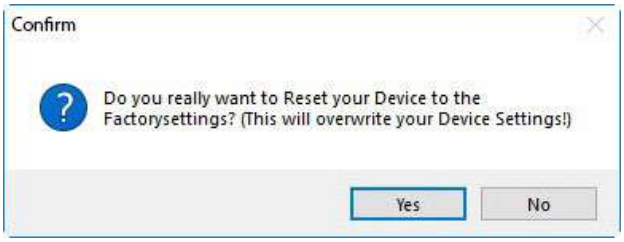


5. Now enter the device-specific password (see label on the device) and confirm with "OK" to establish the connection.
   The device password is always needed for this action, even if the device is already paired.

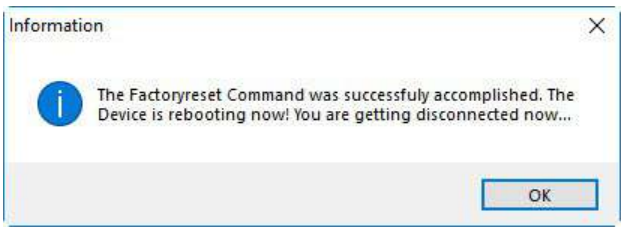


6. Select the function "Factory reset" via the "Device" menu.

7. Confirm the query about overwriting the device settings by clicking “Yes” to reset to the factory settings.



8. Confirm the information window with "OK" to complete the action.



4.1.2.6 Device> Firmware Update

Firmware Update

When firmware update, the Anybus Defender Compact Manager represents the central exchange between the auto-update server and the Device (Anybus Defender Compact).

NOTICE

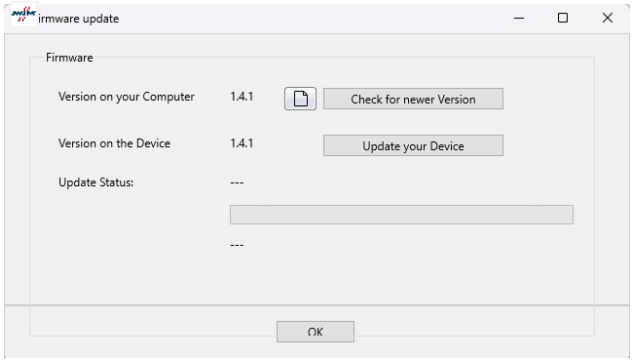
This feature is only active when the device is online.

Device is online - Project settings and device settings are **equal**.

Device is online - Project settings and device settings are **different**.

When executing the function, the "version on your computer" and the "version on the device" (Anybus Defender Compact) are displayed.

- By clicking on the "Check for newer version" button, a connection to the auto-update server will be established, if the internet connection is established.



- If a newer firmware version is offered on the auto-update server, you can execute the download with "Yes".

NOTICE

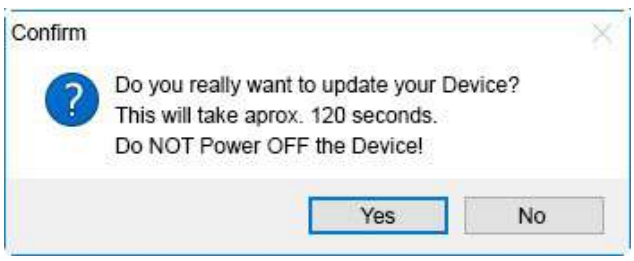
The firmware is automatically saved to "C:\Users*yourUser*\AppData\Roaming\abdcmngr\updates\" on your computer.

If you are not able or you do not want to connect to the auto-update server, you can save a newer firmware version* on your computer.

By clicking on the symbol , you can navigate to this saved firmware file (eg 1-1-1-fwnf.swu). By simply clicking (left-click) the firmware file, it will be moved to the "downloads" folder.

* The latest firmware version for the industrial firewall ***Anybus Defender Compact*** can be found here: https://www.hms-networks.com/p/abd1004-natfw-anybus-defender-compact-1004-nat-fw?tab=tab-support.

- Click "Update your device" to start installing the new firmware on your Device.



NOTICE

You must NOT switch **off** your Device during installation.

NOTICE

After successful installation, the Device must be restarted.

4.1.2.7 Device > Reboot

Reboot

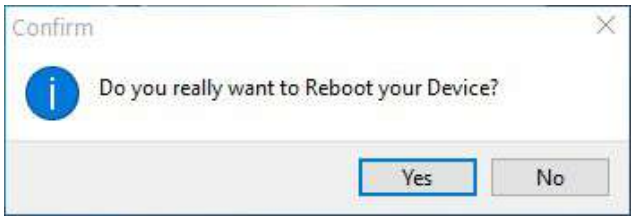
NOTICE

This feature is only active when the device is online.

Go online Device is online - Project settings and device settings are **equal**.

Go online Device is online - Project settings and device settings are **different**.

- Confirm with “Yes” if you really want to reboot your device.



- Confirm once again with “Yes” so that the device reboots.
  The connection is broken in doing so.

Restart directly on the device via Reset button

Regardless of whether the device is online or offline, you can initiate a restart by pressing the Reset button on the front of the device.

4.1.3 Extras

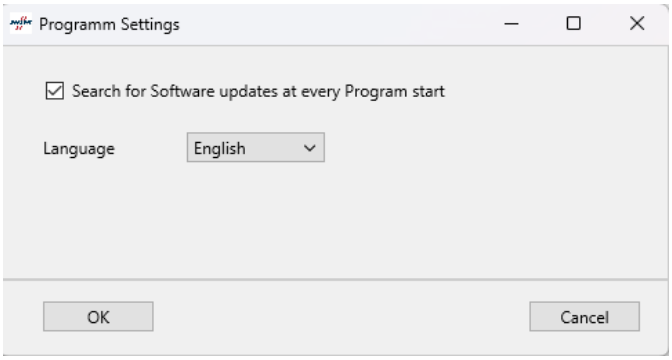
4.1.3.1 Extras > Settings

Search for software update after every program start

By default, the ***Anybus Defender Compact*** manager checks for avail- able software updates on the auto-update server every time the program starts.

By deactivating the checkbox, you deactivate the automatic search.

Use the "**Help > Check for Updates**" menu to manually search for existing software updates on the Auto Update server.

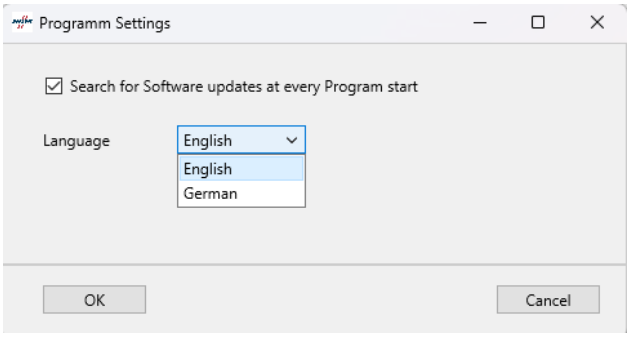


NOTICE

For the search for software updates on the auto-update server, an internet connection is generally necessary.

Setting the program language

Use the pull-down menu to select the language of the program interface (English, German).



4.1.3.2 Extras > Install USB-Driver

In rare cases, you may need to update the USB driver for the "Device-to-PC" connection.

Click " Install USB-Driver" to update the USB driver.

NOTICE

When installing the Anybus Defender Compact Manager, the USB driver was included

on C:\Users*YourUser*\AppData\Roaming\abdcmngr\drivers

4.1.4 Help

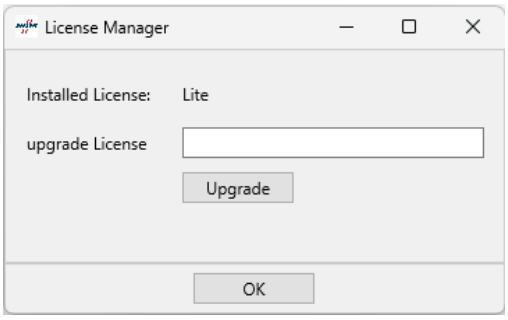
Check for updates

Here, provided you have an Internet connection, you can check whether the latest version of ***Anybus Defender Compact*** Manager is installed.

License

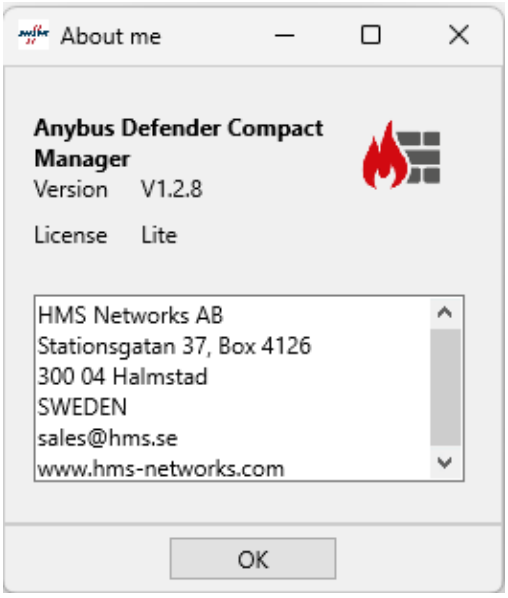
NOTICE

The Lite version ***Anybus Defender Compact*** Manager is sufficient for general configuration of your device.



About me

This is where you obtain information about the installed software (version, license) and our contact details.



4.2 Access rights for the individual user levels

	User level							
	admin (0)		operator (1)		viewer (2)		factoryreset (9)	
Configuration interface →	USB	LAN/ WAN	USB	LAN/ WAN	USB	LAN/ WAN	USB	LAN/ WAN
Action ↓								
Device								
Go online	E	E	E	E	E	E	E	-
Go offline	E	E	E	E	E	E	E	-
Download	E	E	E	E	E	E	-	-
Upload	E	E	E	E	-	-	-	-
Factory reset	E	-	-	-	-	-	E	-

NOTICE

The ***Anybus Defender Compact*** is only reset to its factory settings by the user "factory reset" and only via the USB interface.

If you are logged in as the "admin" user, you can also carry out the action directly without having to log out and log in again with the user "factoryreset".

Furthermore, you always need the original device password for this action, even if the device is already paired or the device password has been changed.

Firmware Update	E	E	E	E	-	-	-	-
Reboot	E	E	E	E	E	E	E	-

E = execute; - = no access

NOTICE

The users "admin" and "factoryreset" are created by default and cannot be deactivated or changed.

The "operator" and "viewer" users are created (activated or deactivated) in the System > " Access - edit authentication method for individual users" menu.

	User level							
	admin (0)		operator (1)		viewer (2)		factoryreset (9)	
Configuration interface →	USB	LAN/ WAN	USB	LAN/ WAN	USB	LAN/ WAN	USB	LAN/ WAN
Function ↓								
Start	R/W	-	-	-	-	-	-	-
Quick Setup	R/W	-	-	-	-	-	-	-
Settings	R/W	R	R	R	R	R	-	-
Operation mode	R/W	R	R	R	R	R	-	-
Interfaces	R/W	R	R	R	R	R	-	-
NAT	R/W	R/W	R/W	R/W	R	R	-	-
SNAT	R/W	R/W	R/W	R/W	R	R	-	-
Simple NAT	R/W	R/W	R/W	R/W	R	R	-	-
Network NAT	R/W	R/W	R/W	R/W	R	R	-	-
DNAT	R/W	R/W	R/W	R/W	R	R	-	-
Packet filter	R/W	R/W	R/W	R/W	R	R	-	-
Filter mode	R/W	R/W	R/W	R/W	R	R	-	-
Rules	R/W	R/W	R/W	R/W	R	R	-	-
Routes	R/W	R/W	R/W	R/W	R	R	-	-
System	R/W	R/W	R	R	R	R	-	-
Access	R/W	R/W	R/W*	R	R/W*	R	-	-
Time	R/W	R/W	R	R	R	R	-	-
Syslog	R/W	R/W	R	R	R	R	-	-
NetCap	R/W	R/W	R	R	R	R	-	-
Diagnosis	R	R	R	R	R	R	-	-
Loggings	R	R	R	R	R	R	-	-

W = write; R = read only; - = no access; * only change password

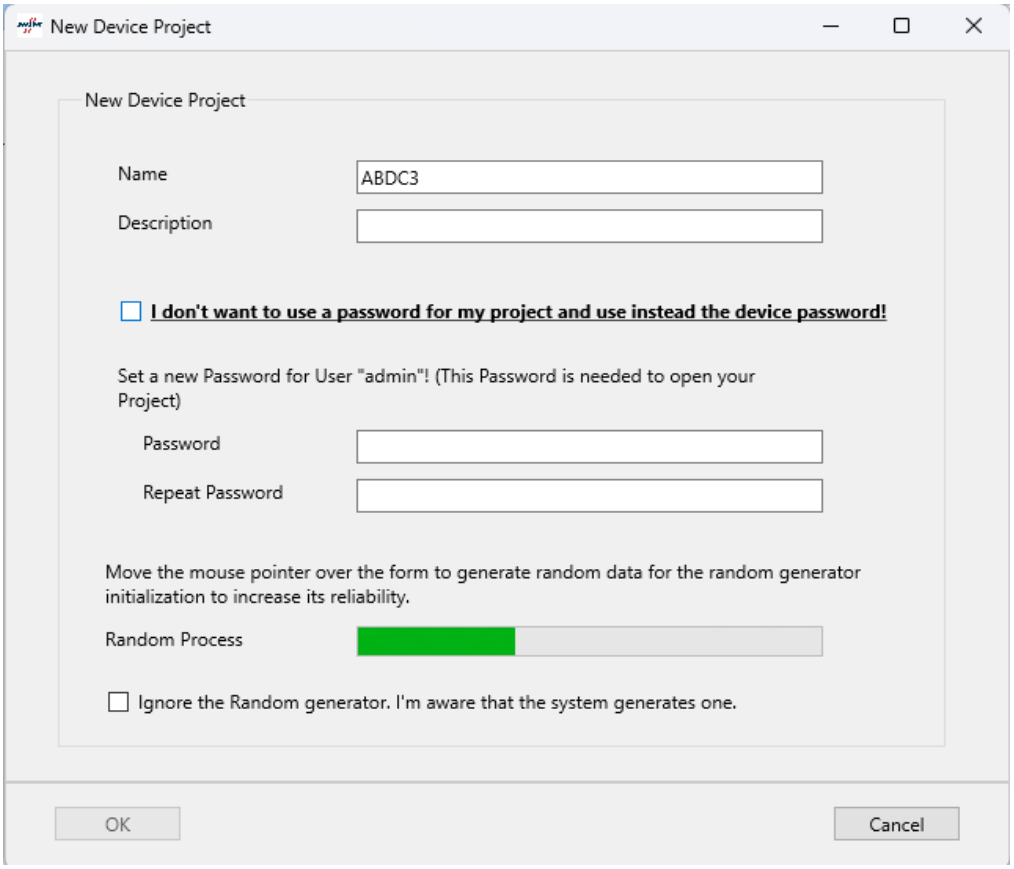
	User level			
	admin (0)	operator (1)	viewer (2)	factoryreset (9)
Action ↓				
File	E	E	E	E
New	E	E	E	E
Open	E	E	E	E
Close	E	E	E	E
Save	E	E	-	-
Delete	E	E	-	-
Duplicate	E	E	-	-
Export	E	E	-	-
Project	E	E	-	-
Configuration	E	E	-	-
Import	E	E	E	E
Project	E	E	E	E
Configuration	E	E	-	-
Exit	E	E	E	E
Edit	E	E	E	-
Expand all	E	E	E	-
Collapse all	E	E	E	-
Extras	E	E	E	E
Settings	E	E	E	E
Install USB Driver	E	E	E	E
Help	E	E	E	E
Check for Updates	E	E	E	E
License	E	E	E	E
About	R	R	R	E

E = execute; R = read only; - = no access

5 Create a project

Start ***Anybus Defender Compact*** Manager via your PC's start menu or via the corresponding desktop symbol. During the first Start you are requested to create a new project.

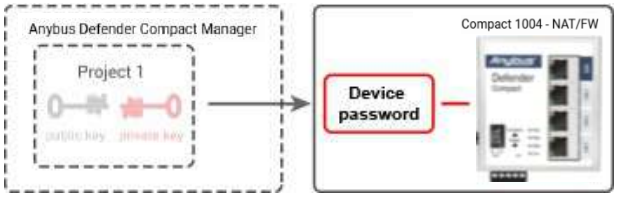
You can create additional device projects via **File >** **New**.



Name	**Mandatory field** for assigning a unique name to this project. When specifying the name, only the following numbers and/or letters are permitted: **0** to **9**, **A** to **Z**, **a** to **z** - **without** any spaces.
Description	**Optional field** for a short description of this project.
I don't want to use a password...	If you activate this **checkbox**, no password is required to open this project.

The following applies to projects **without** a password:

- **No** password is required to open the project.
- When the configuration is first transferred from the project to the device, there is **no** Project-Device Pairing.
- For communication, the **current device password** must be entered every time a connection is established to the device.

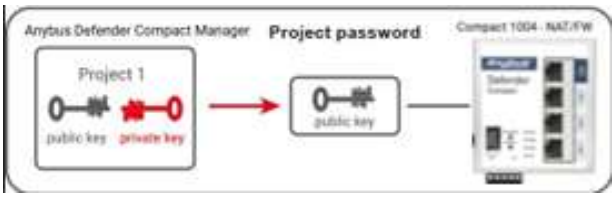


ATTENTION: If you do not use a password for a device project, this project can be opened and edited / changed at any time!

Password **Repeat Password**	If you want to protect the project with a password, assign a password (min. 8 characters) for the user "admin" here. When a password is assigned, RSA encryption is active and the project can only be opened / edited after entering the password.

The following applies to projects **with** a password:

- A password is required to open the project.
- The first time the configuration is transferred from the project to the device, a **Project-Device Pairing** takes place.
- After the project-device pairing has taken place, the current device password is no longer active. **No additional password** needs to be entered for communication with the device.



Random Process	Move your mouse over the form field to generate an additional random value for calculation of a security key. This value is added to the algorithm of the random generator as an additional “unknown” factor. In this way back calculation of the generated security key is nearly impossible.
Ignore the Random generator...	Optionally, you can suppress generation of the additional value by confirmation of this checkbox. In this case, only the random value generated by the PC's operating system is used.

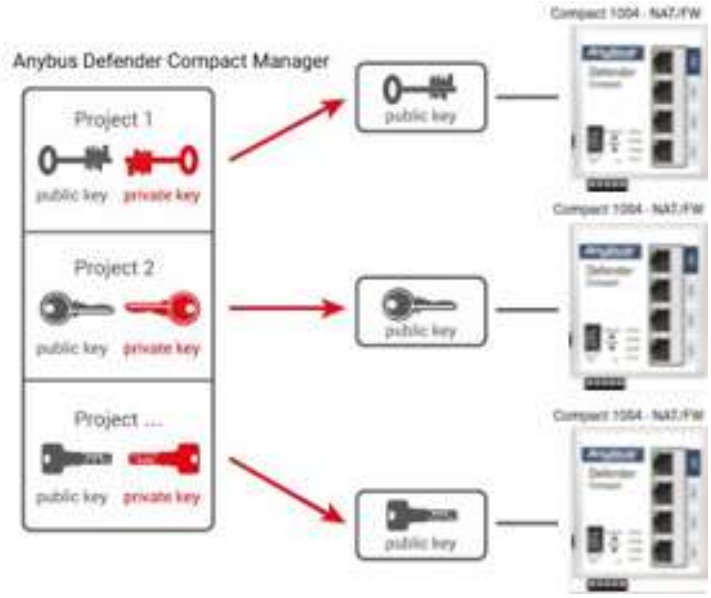
Click on the "**OK**" button to confirm the entry

The ***Anybus Defender Compact*** manager generates a corresponding project folder and starts with its user interface.

5.1 Device project - device: The principle

Device project - device: The principle

The Anybus Defender Compact manager supports you with the configuration of the industrial firewall Anybus Defender Compact ABD1004-NATFW.



For each device (Anybus Defender Compact) you create an encrypted device project with the Anybus Defender Compact manager.

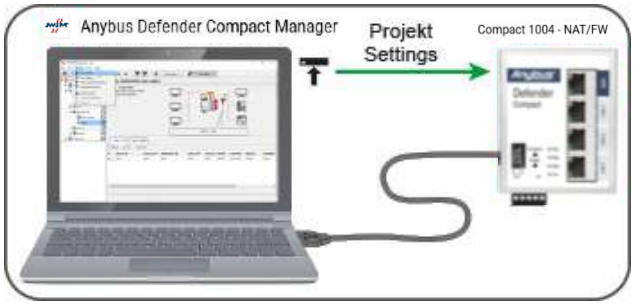
=> File > New

You can protect each device project with an individual project password.

A device project contains, among other things, also the PKI (Public Key Infrastructure).
The "private key" is protected by the device password.

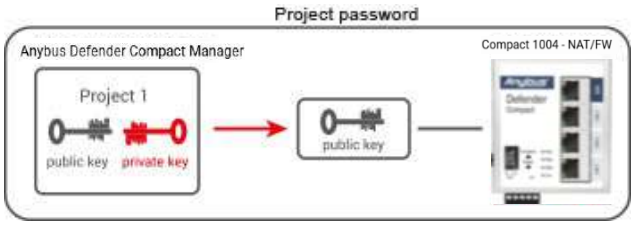
You can make all device settings "**offline**" in the device project and transfer them to the device at any time. The first transfer is called a **Project-Device Pairing**.

After Project-Device Pairing, the "Public Key" is saved in the device and the device password is no longer active.



You now only need the project password to open / edit the device project and to communicate with the "Device".

The device password is required again if you want to reset the device to its factory settings.

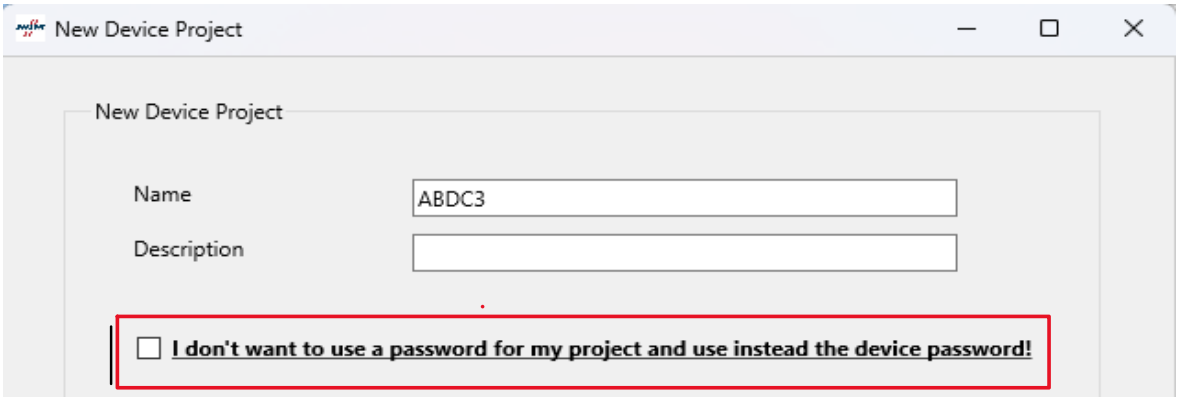


NOTICE

The possible number of devices (Anybus Defender Compact ABD1004-NATFW) that can be managed in the NETFIX Manager is theoretically unlimited.

The only possible restriction: Each open project uses approx. 2 MB RAM.

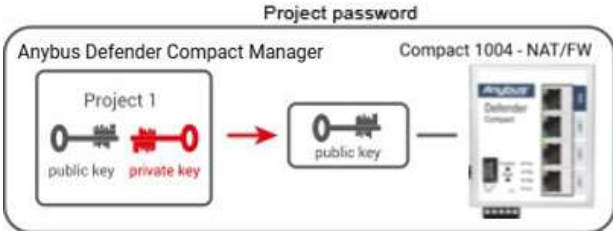
5.2 Device project with or without a password?



"I don't want to use a password for my project and use instead the device password!"

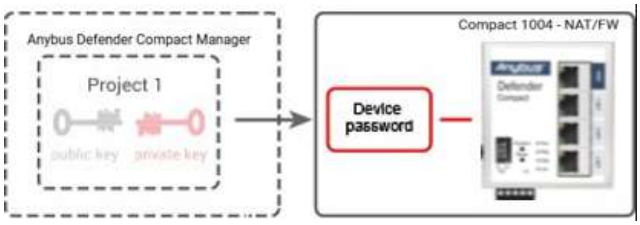
With this checkbox you specify whether a device project should be created with or without a project password.

Device project with password



- A password is required to open the project

Device project without password



- **No** password is required to open the project.

- The first time the configuration is transferred from the project to the device, a **Project-Device Pairing** takes place.
- When the configuration is first transferred from the project to the device, there is **no** Project-Device Pairing.
- After the project-device pairing has taken place, the current device password is no longer active. **No additional password** needs to be entered for communication with the device.

For communication, the **current device password** must be entered every time a connection is established to the device.

NOTICE

ATTENTION: If you do not use a password for a device project, this project can be opened and edited / changed at any time!

NOTICE

The original device password is definitely required again if you want to reset the device to its factory settings.

6 Configuration

NOTICE

Before you begin with the configuration, you should be clear in which operating mode - bridge mode or gateway mode - you want to use / use the industrial firewall ***Anybus Defender Compact***.
See " Operation mode - general"

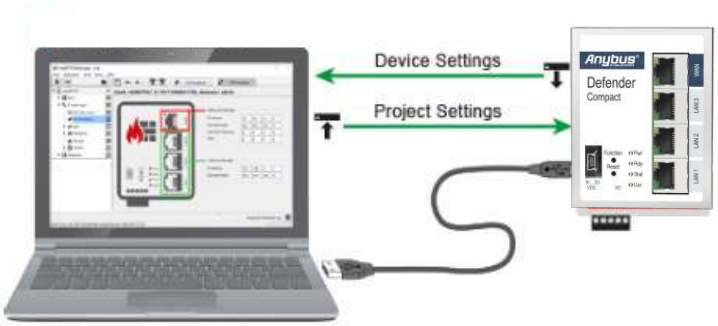
NOTICE

The configuration always takes place within a project

- either offline = project settings
- or online, directly on the device (***Anybus Defender Compact***) = device settings.

Different data states can be synchronized at any time.

- Download Device Settings
- Upload Project Settings to the Device



Select the project to be configured

- via "File > Open",
- or direct selection in the configuration menu.

Enter the required project password and confirm with "OK”

6.1 Start

Under the menu item **Start** you can chose between

Quick Setup => continue with **Quick Setup** menu

and

Advanced => continue with **Operation mode** menu

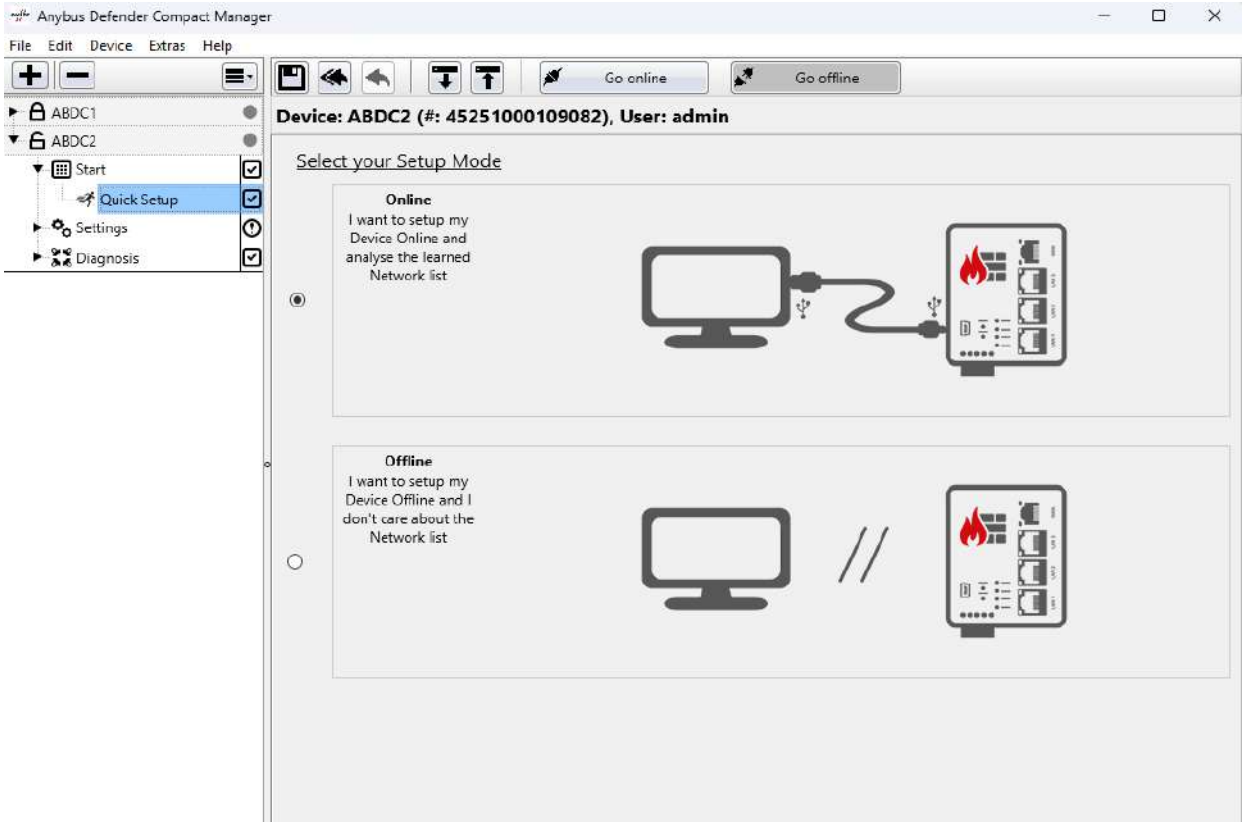
You will be automatically forwarded to the **Settings > Operating mode** menu.

6.1.1 Quick Setup / Configuration Wizard

In the Quick Setup, an assistant guides you through all relevant settings.

Because you have to make various decisions during configuration (e.g. Setup Mode, Operation Mode, NAT Mode, etc.), the configuration wizard is variable.

The menus to be edited during the configuration are explained in detail in the chapter "Settings".

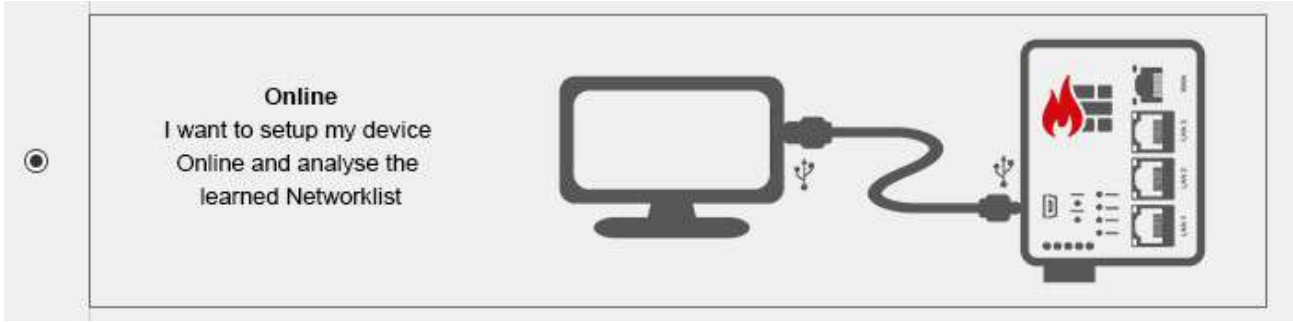


First of all, you have to decide whether you want to configure **Online** or **Offline**.

Choose one of the two configuration methods and click "**Next**".

6.1.1.1 Setup Mode - Online

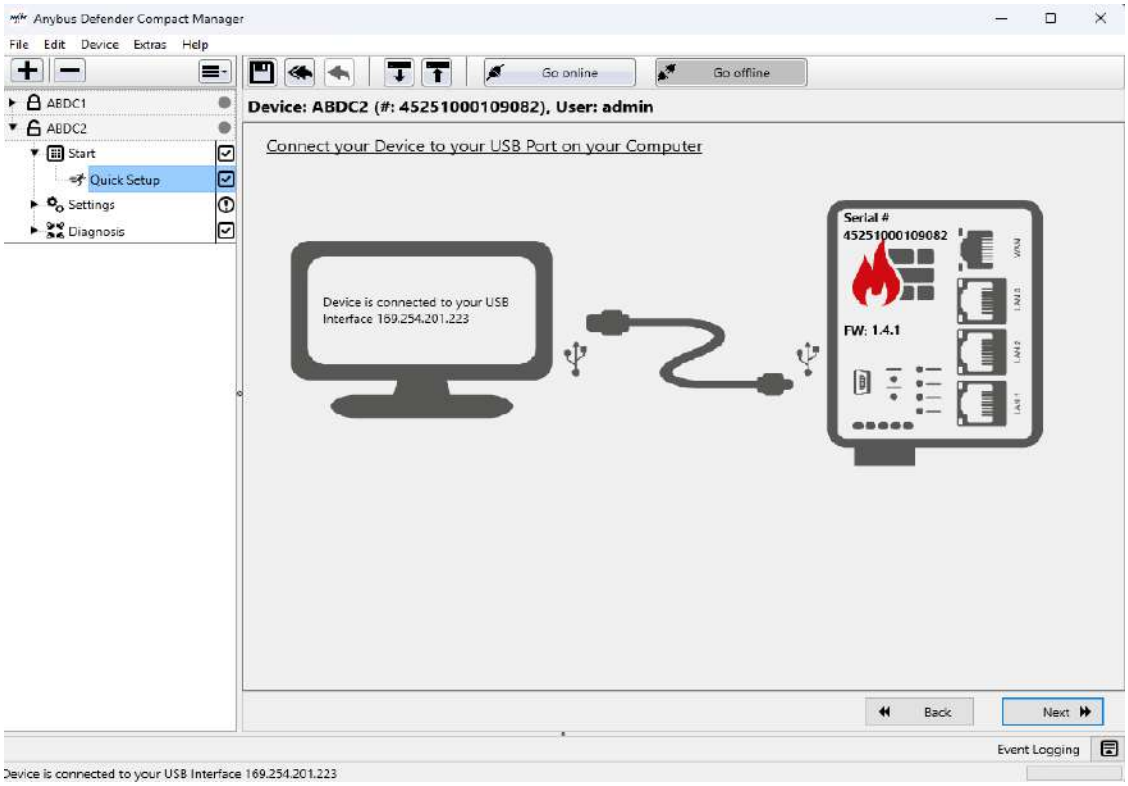
Online



NOTICE

For Online configuration, the following conditions must be met:

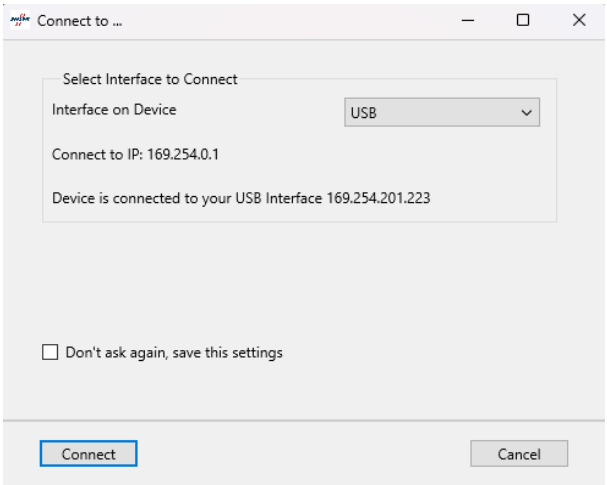
- The device (***Anybus Defender Compact***) is connected to the same PC on which the Anybus Defender Compact manager is installed.
- The device is integrated in the network structure to be monitored.



In rare cases, you may need to update the USB driver for the "device to PC" connection. To do this, click the "Install USB Driver" button.

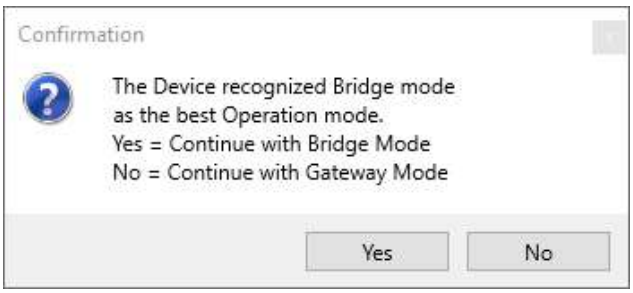
Click on "**Next**"

Click on "**Connect**"



"The Device recognized Bridge mode as the best Operation mode.
Yes = Continue with Bridge Mode
No = Continue with Gateway Mode"

Confirm the message by selecting "**Yes**" or "**No**".



As soon as the device has been integrated into the network structure and is switched on, it automatically starts recording the network data. In a network list (Mapview) all reachable network subscribers are listed.

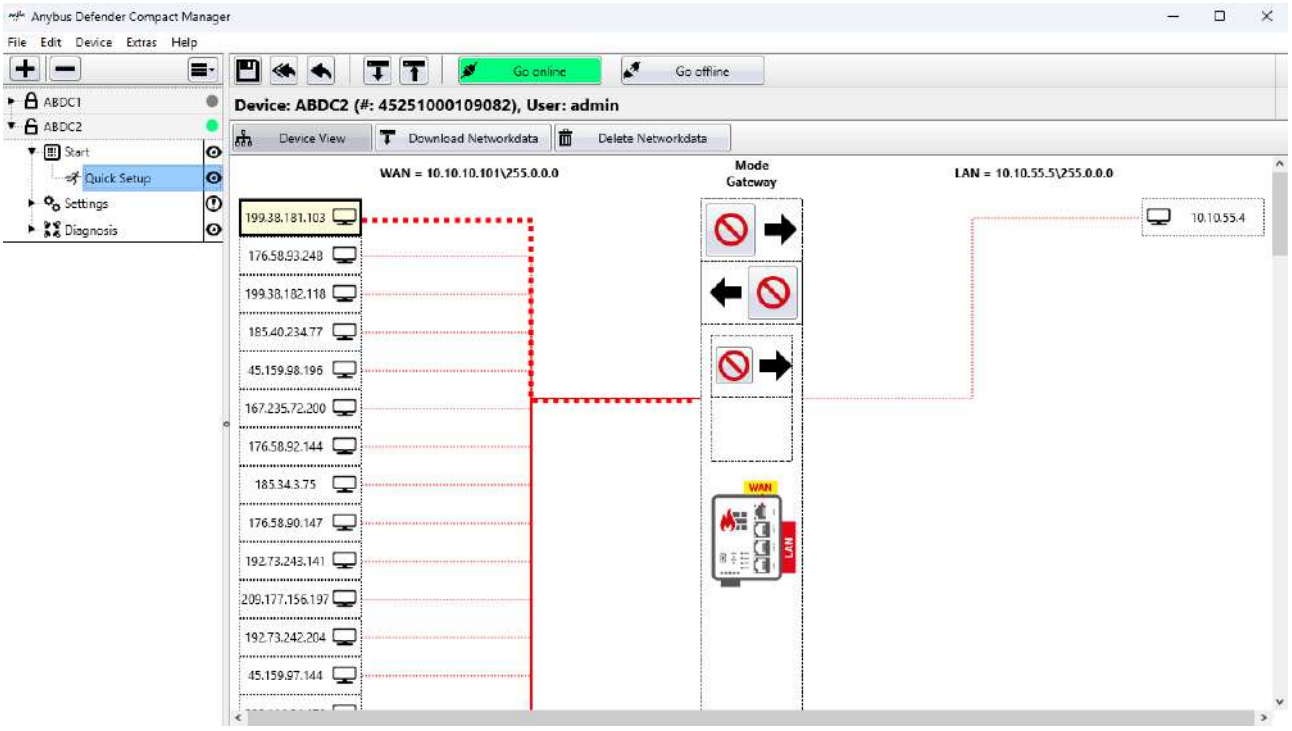


Image 1: Example of a network list

From here, you can analyze the network data and - with just a click of the mouse - allow and block connections.

If no reachable participants have been detected, a message appears: "*There are no learned Networkdata on the Device. You can skip the Mapview and follow with the device settings.*"

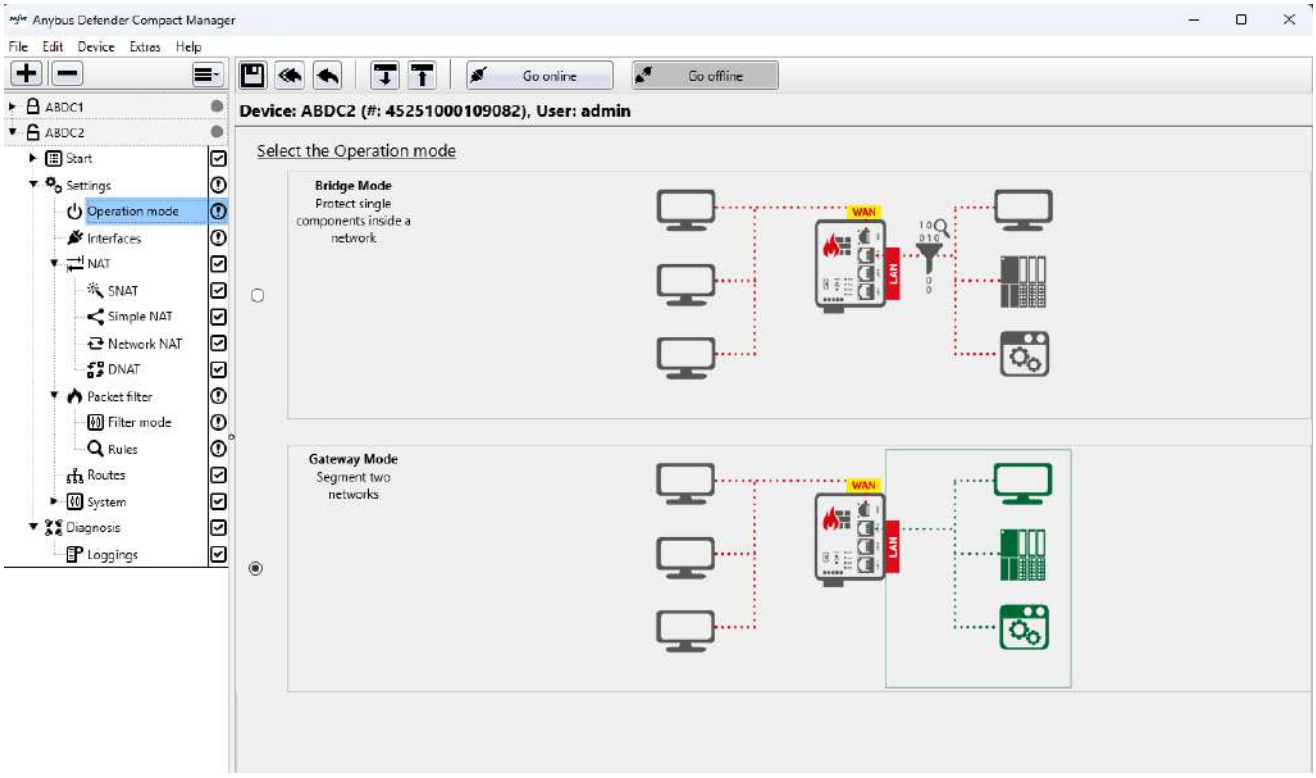
More information about the network list can be found in the chapter **Packet filter** (" Packet filter")

6.1.1.2 Setup Mode - Offline

For offline configuration, the device (***Anybus Defender Compact***) neither needs to be connected to the computer nor integrated into a network structure.

You can upload the configuration (Project Settings) to the device at any time - provided the device is connected to the configuration computer.

Clicking on “**Next**” leads you through all the menus relevant for the configuration (see also from " Settings").

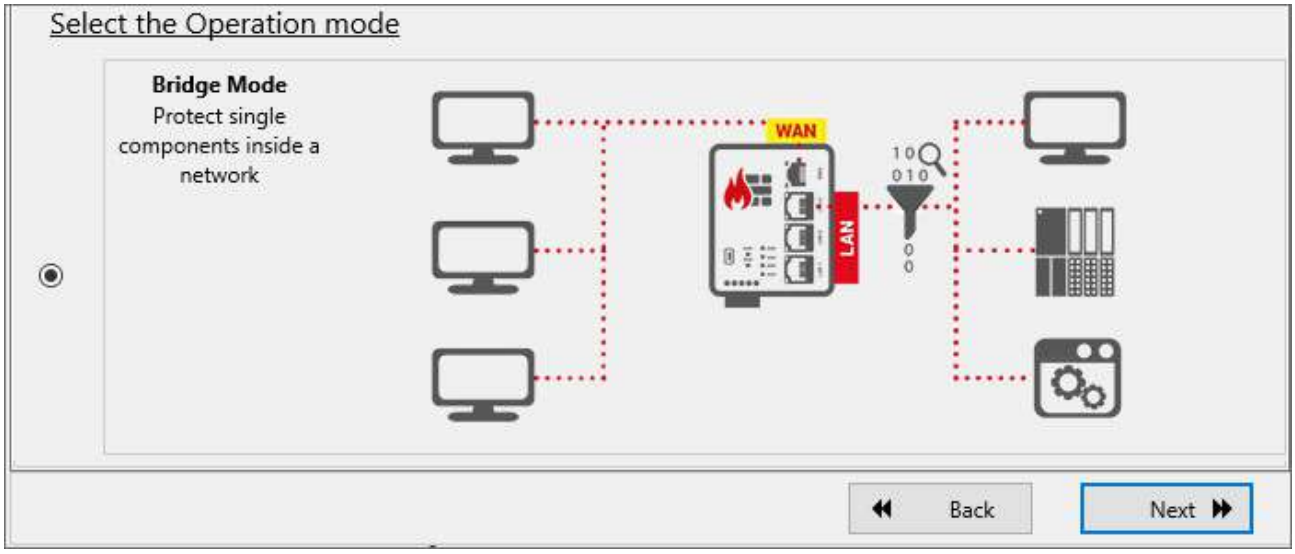


Here you select the operating mode (Bridge mode or Gateway mode) for which the device is to be configured.

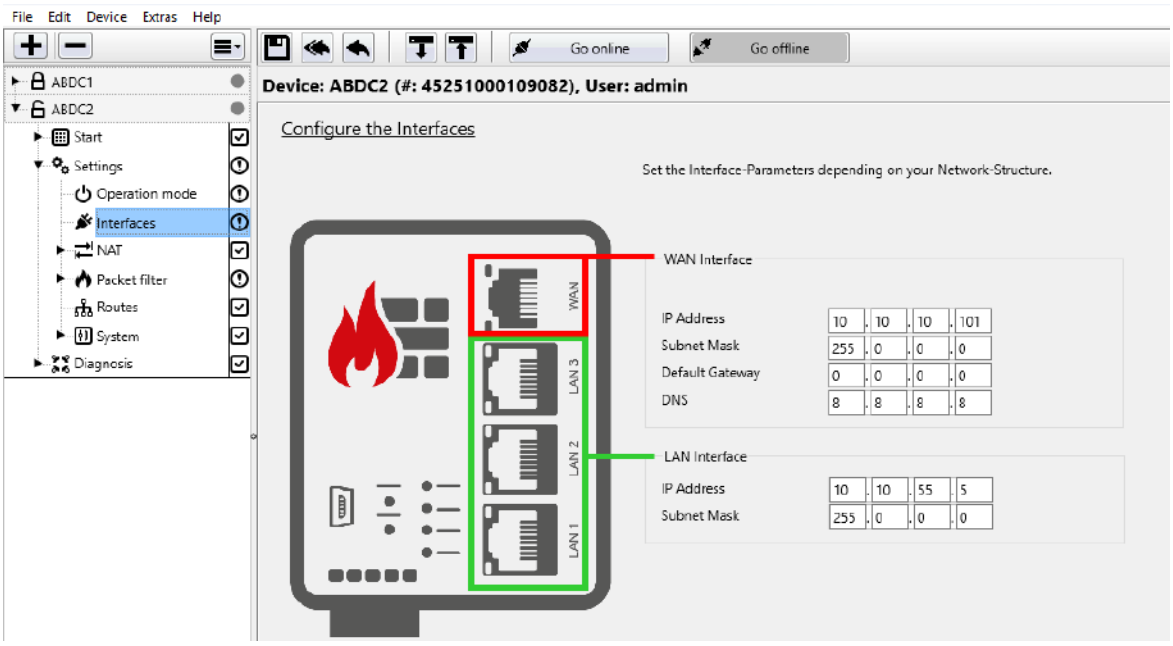
Operation mode	Function	Description
Bridge Mode	Individual components within a network are protected.	In bridge mode the firewall is easily integrated into existing networks that are in the same network segment. As supplied, it can be installed without any network modifications and immediately starts learning the current data traffic. It protects WAN <> LAN data exchange using a packet filter. The firewall integrates transparently and no IP address assignment is necessary for the device.
Gateway Mode	Two networks are segmented.	In gateway mode, both WAN and LAN are assigned a defined IP address and in this way segment the networks. Here functions such as NAT and forwarding can be used to route data traffic to subordinate networks. Here too, the packet filter can be used to control WAN <> LAN data exchange. Here too, learning mode simplifies the creation of filter tables.
	NOTICE	
	In Gateway Mode, the networks in the IP address space must be different.	

6.1.1.2.1 Quick Setup - Bridge Mode

Bridge Mode



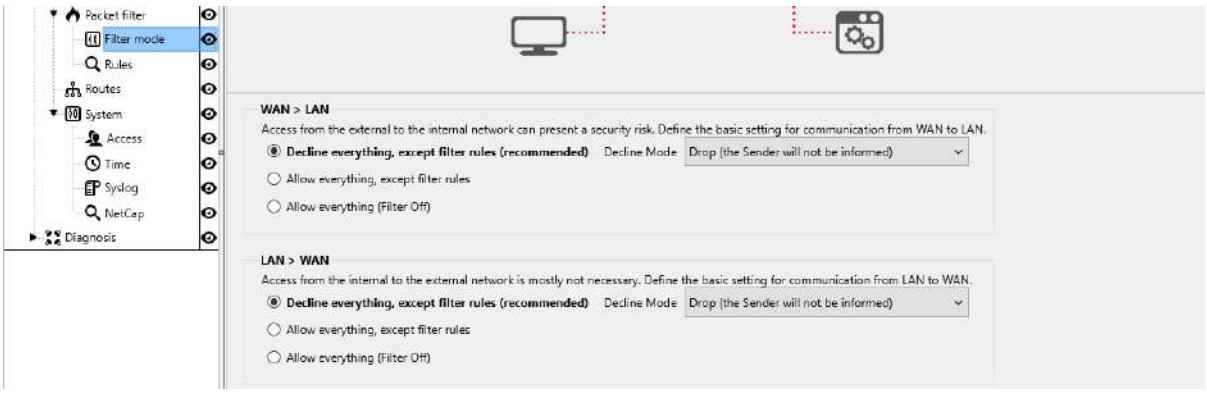
After clicking "**Next**" you will be prompted to configure the LAN / WAN interface.



WAN / LAN Interface	
Label	Description
disable Interface	Checkbox to activate / deactivate the WAN / LAN interface. If the WAN / LAN interface is disabled, it cannot be set as a Configuration Access Level. Settings already made under " System" are deactivated and cannot be changed.

WAN / LAN Interface	
IP Address **Subnet Mask**	The assignment of an IP address / subnet mask is only necessary if the device is to be accessible via IP. For example, for future changes (configuration) via Ethernet or if other services such as Syslog / SNTP are to be used. If you do not enter an IP address, the Anybus Defender Compact is not visible in the network.
Default Gateway	A default gateway is required if • devices from the network want to connect to the Internet, • when integrating devices from the LAN over the WAN into other networks. If this is not desired, the default value "0.0.0.0" must be retained.
DNS	The assignment of a **DNS** server (for SNTP service) is also possible.

After clicking on "**Next**" you will be redirected to the setting of the Filter mode.



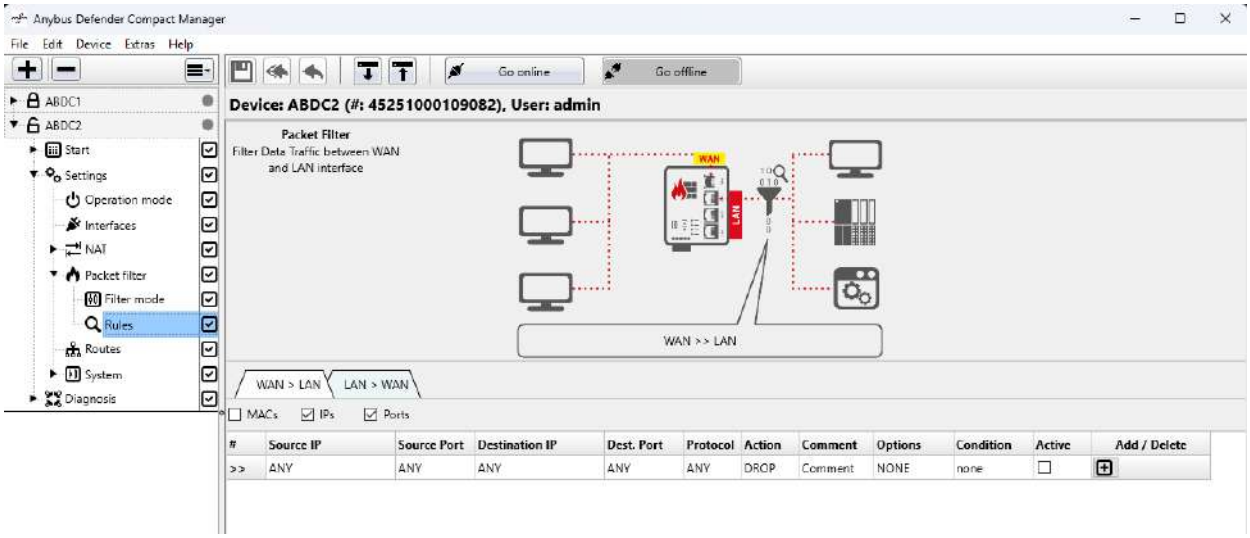
Select the appropriate rules under the desired communication directions (WAN > LAN or LAN > WAN).

- **Decline everything**, except filter rules (recommended) - so-called *whitelisting*
  - Drop (the sender will not be informed)
  - Reject (the sender will be informed via the ICMP Protocol)
- **Allow everything** except filter rules (see " Rules", Page 85) - so-called *blacklisting*
  Here all packets are accepted at the end of the filter table. The filter sorts but is effectively only off.
- **Allow everything** (**Filter Off**)
  All filters are inactive here and the data transfer is completely accepted.

NOTICE

Further information can be found in the "Packet filter > Filter mode" settings menu.

Click "**Next**" to create the firewall rules.



Here you create the individual rules for the firewall ruleset; both **WAN > LAN** and **LAN > WAN**.

A set of rules consists of the settings in the **Filter mode** and the set of **Rules** created.

The policy processes / checks both incoming packets as well as the response packets generated by the network participant and allows allowed connections to pass through the firewall (ACCEPT) or blocks (DROP, REJECT) unauthorized connections.

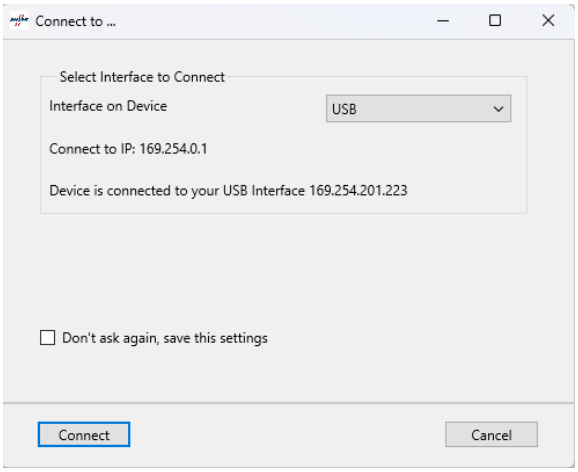
NOTICE

Further information is available in the Settings menu "Packet filter > Rules".

Click on "**Next**" to load the created configuration into the device.

In rare cases, you may need to update the USB driver for the "device to PC" connection. To do this, click the "Install USB Driver" button.

Click on "**Connect**"



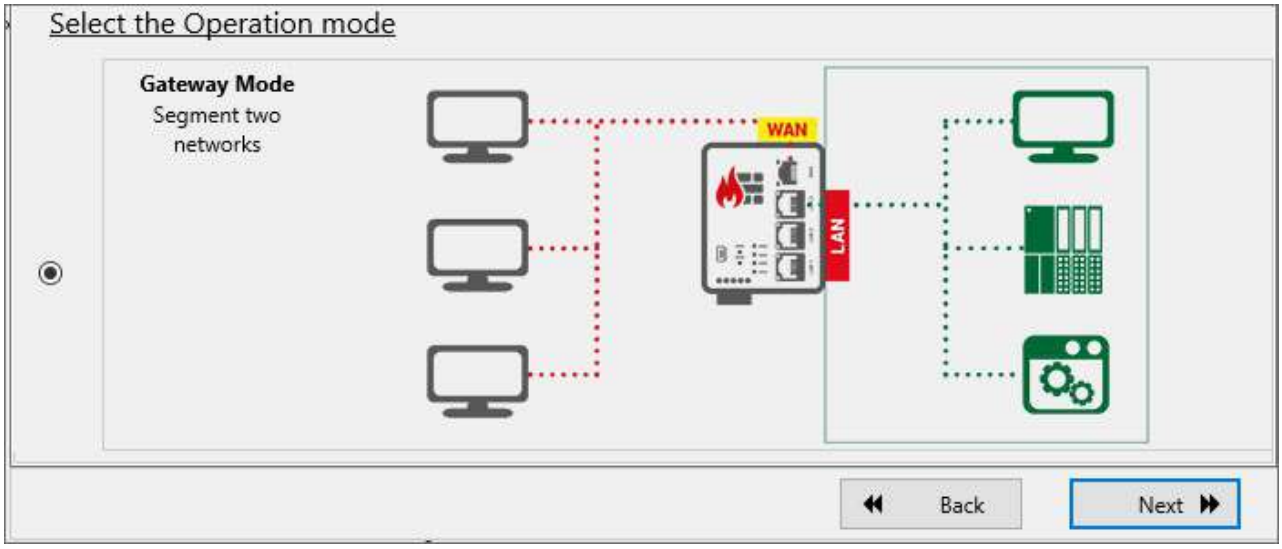
The password required for communication (device password) must be entered for the first connection to the device.

The device password is on a label on the back of the device.

Please note that the password is case-sensitive.

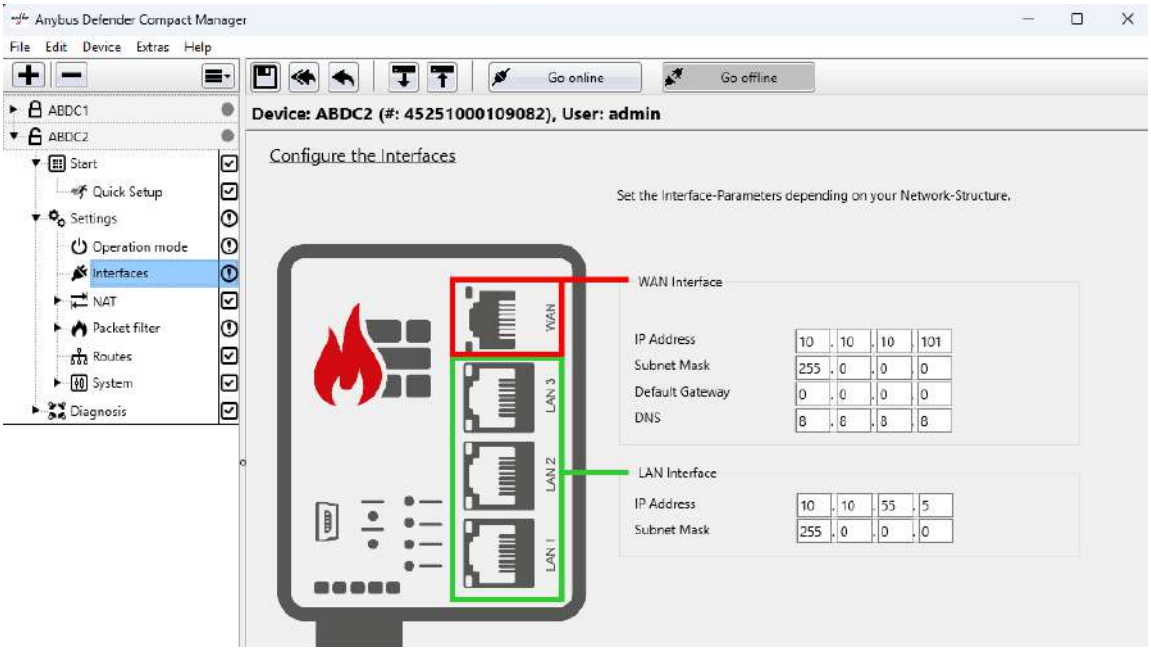
6.1.1.2.2 Quick Setup - Gateway Mode

Gateway Mode



After clicking "**Next**" you will be prompted to configure the WAN and the LAN interface.

Configuration of the WAN and the LAN interface

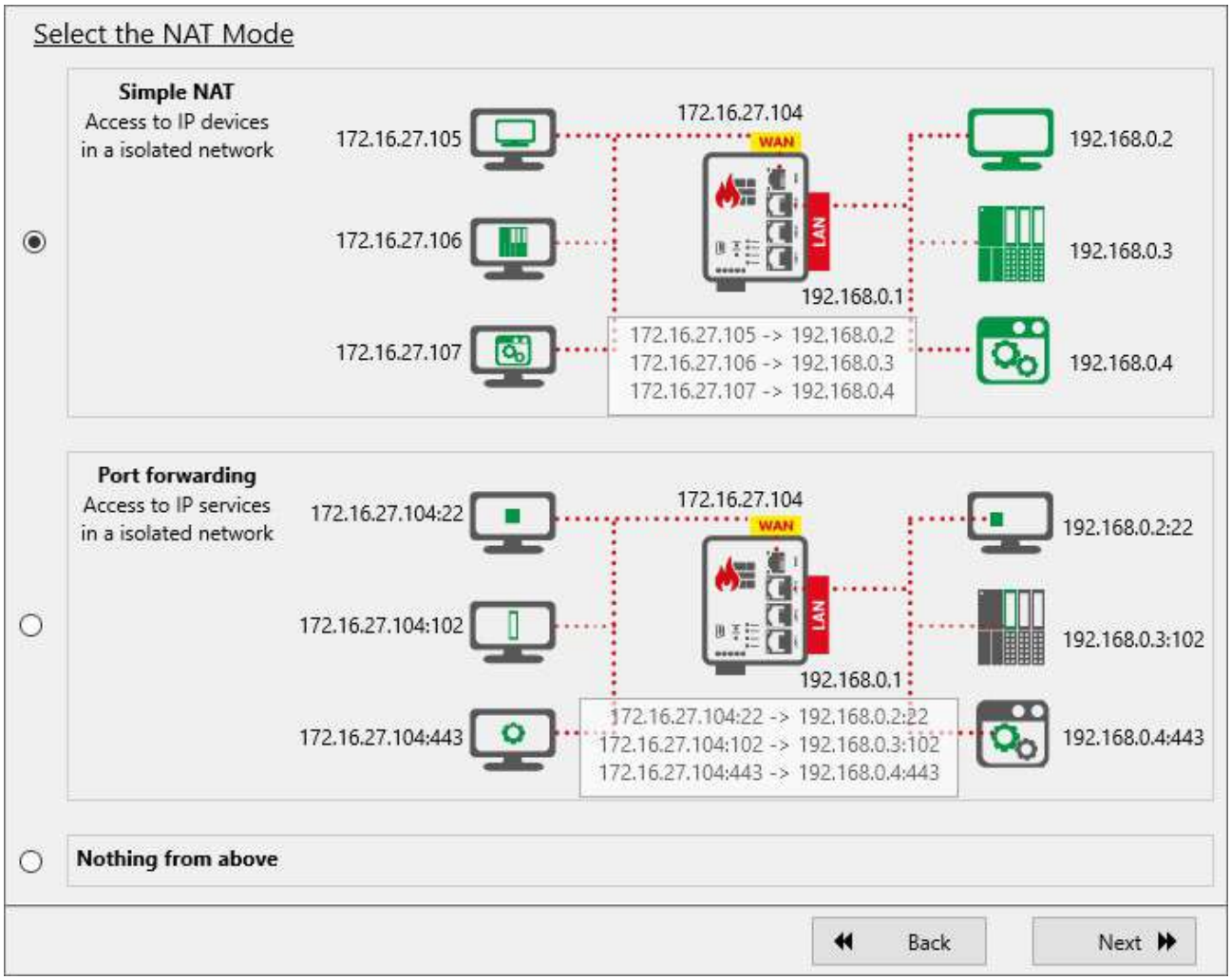


WAN Interface	
Label	Description
IP Address	Enter the appropriate values for the network on the WAN side here.
Subnet Mask	
Default Gateway	A default gateway is required if • devices from the network want to connect to the Internet.
DNS	The assignment of a **DNS** server (for SNTP service) is also possible.

LAN Interface	
Label	Description
IP Address	Enter the appropriate values for the network on the LAN side here.
Subnet Mask	

After clicking on "**Next**" you will get to the NAT mode selection menu.

Select NAT mode



You can choose from:

- "**Simple NAT**" - Access to IP devices in an isolated network
- "**Port forwarding**" (DNAT) - Access to IP services in an isolated network
- "**Nothing from above**"

Make your selection and confirm it by clicking on "**Next**"

"Simple NAT"

NOTICE

Use Simple NAT to access an IP address from network B (LAN) 1:1 on network A (WAN).

With this function, a network participant in the LAN can be directly addressed via a WAN IP address. As it were, the IP address of a LAN participant with an IP address from the WAN area is mirrored in the WAN. This does not require a virtual IP address, as is usual with a NAT function.

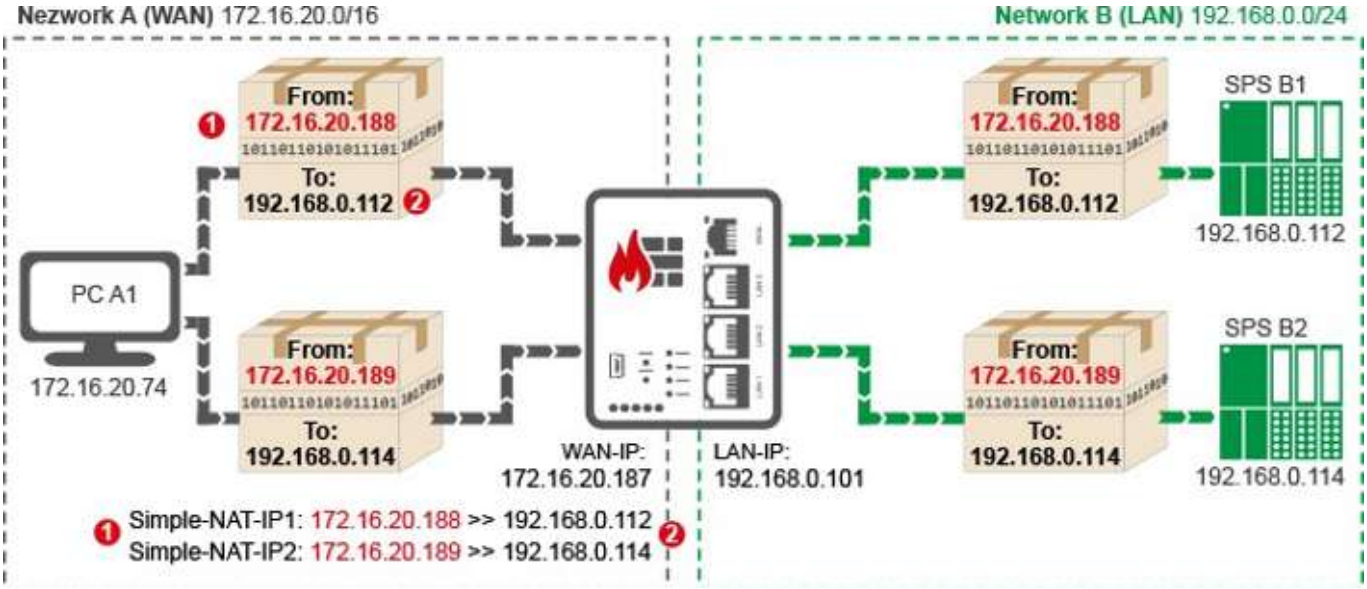


Image 2: Example: Data packet delivery to two subscribers using Simple-NAT from WAN to LAN

To do this, enter in the address assignment table

1 a free WAN Ethernet address from the WAN network and

2 and the LAN IP address of the recipient from the LAN network to be "NATed" with.

NOTICE

You need a separate WAN IP address for each receiver (network subscriber in the LAN network).

NOTICE

If one of the network participants to be reached has no or a wrong (inappropriate) gateway entry and can therefore not send a response to an delivered data packet, you must also activate the "WAN to LAN" function in the SNAT.

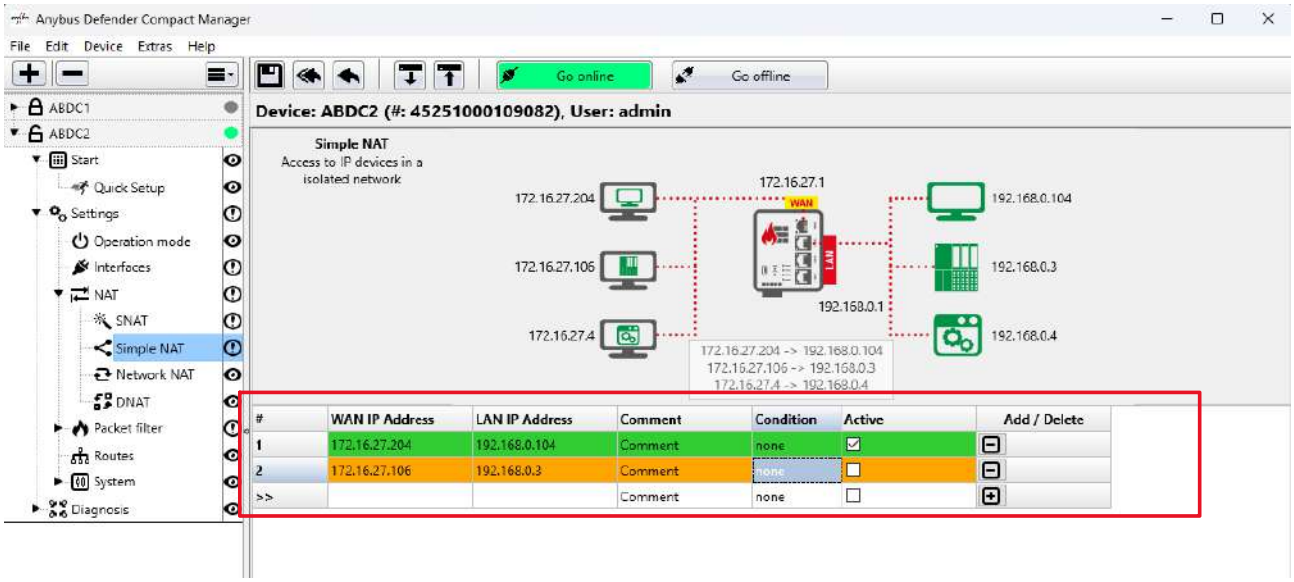


Image 3: Address assignment table

Label	Description
WAN IP-Address	Enter a free WAN IP address from the WAN network.
LAN IP-Address	Enter the IP address of the recipient from the LAN network.
Comment	Here you can enter a comment for the defined assignment.
Condition	Selection field for specifying the condition when a rule is or remains active. You can choose from: **DIN1-High**, **DIN1-Low**, **DIN2-High**, **DIN2-Low** or **NONE**. By wiring (high / low) DI1 or DI2 (digital inputs of the Anybus Defender Compact), you can dynamically deactivate and reactivate a SimpleNAT filter rule. If you select NONE, the rule remains unaffected.

NOTICE

Only active packet filter rules are transferred to the device. That means: A rule can only be deactivated and reactivated by a signal change at a digital input (high -> low or low -> high).

Active	Checkbox for activating / deactivating the assignment.
Add/Delete	Click on the plus icon ⊞ to add the mapping. Click on the minus icon ⊟ to delete an assignment.

TIP

You can easily set the column widths of the table with the mouse.

NOTICE

As soon as you have added and activated an assignment, the rule for this assignment is automatically entered and activated under **Packet filter** > **Rules** > WAN > LAN.

Image 4: Example entries in address assignment table

#	WAN IP Address	LAN IP Address	Comment	Condition	Active	Add / Delete
1	172.16.27.204	192.168.0.104	Comment	none	☑	⊟
2	172.16.27.106	192.168.0.3	Comment	none	☐	⊟
>>			Comment	none	☐	⊞

Image 5: Related entries in the firewall rules WAN>LAN

WAN > LAN | LAN > WAN

☐ MACs ☑ IPs ☑ Ports

#	Source IP	Source Port	Destination IP	Dest. Port	Protocol	Action	Comment	Options	Condition	Active	Add / Delete
1	172.16.27.204	ANY	192.168.0.104	ANY	ANY	ACCEPT	SimpleNAT:17	NONE	none	☑	⊟
2	172.16.27.106	ANY	192.168.0.3	ANY	ANY	DROP	Comment	NONE	none	☐	⊟
>>	ANY	ANY	ANY	ANY	ANY	DROP	Comment	NONE	none	☐	⊞

After clicking on "**Next**" you will be redirected to the setting of the Filter mode.

"Port forwarding" (DNAT)

NOTICE

DNAT stands for Destination NAT. This changes the destination of the data packet.

With port forwarding, a single port can be forwarded to a specific IP address specifying the port.
Port forwarding is available from WAN to LAN as well as LAN to WAN.

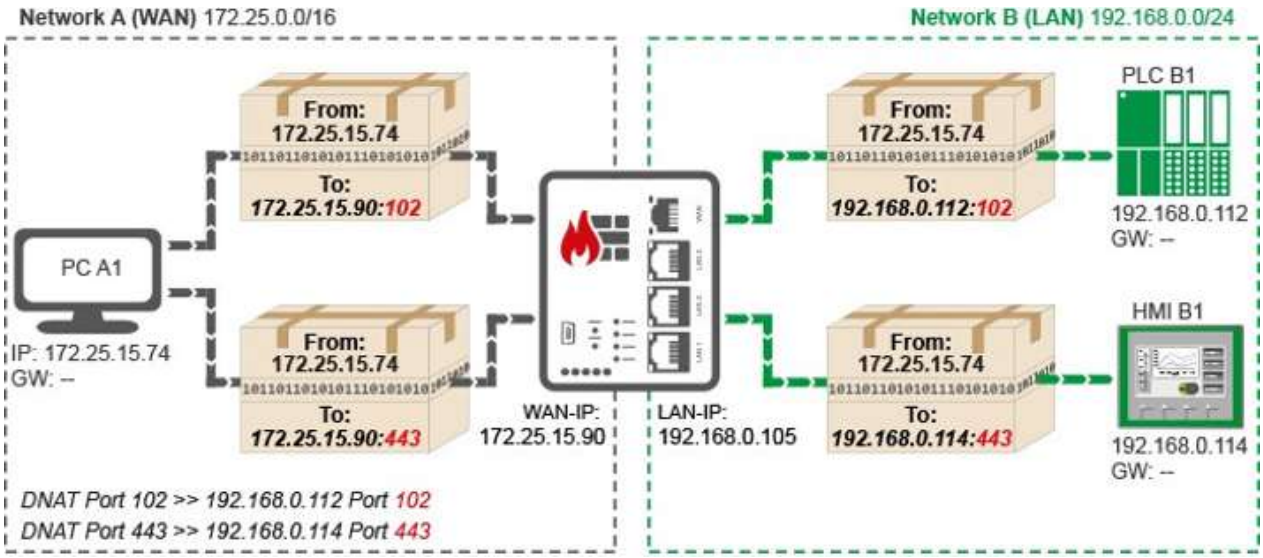


Image 6: Example diagram of a DNAT from WAN to LAN
PLC B1 (programming port 102) and HMI B2 (web server port 443) should be accessible via PC A1.

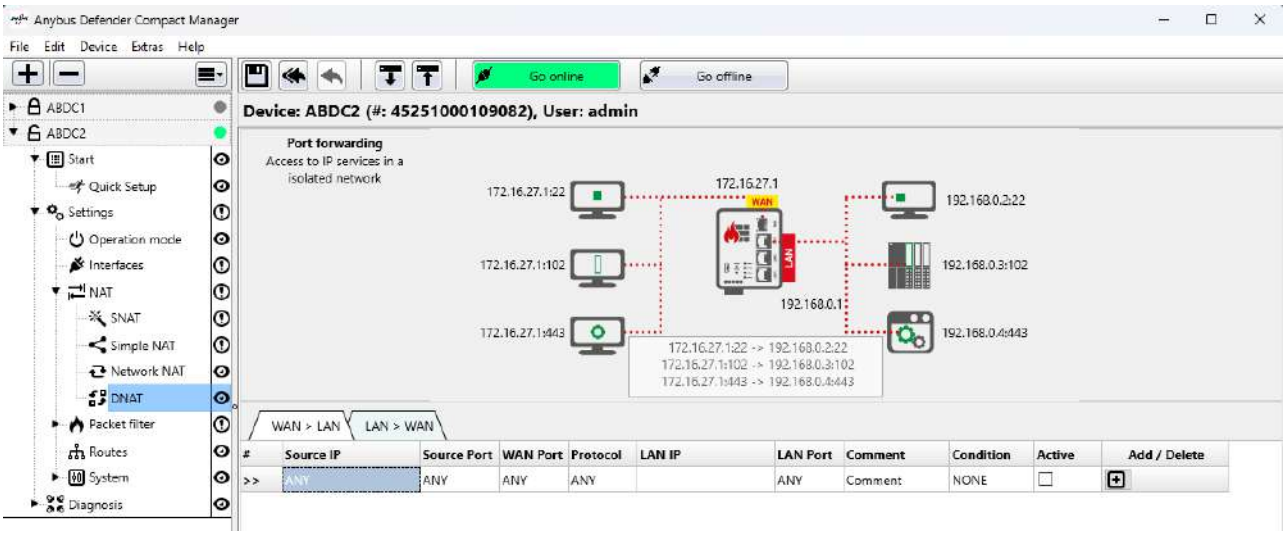
WAN > LAN | LAN > WAN

#	Source IP	Source Port	WAN Port	Protocol	LAN IP	LAN Port	Comment	Condition	Active	Add/Delete
1	172.25.15.74	ANY	102	TCP	192.168.0.112	102	Comment	DI1-High	☑	⊟
2	172.25.15.74	ANY	443	TCP	192.168.0.114	443	Comment	DI1-High	☐	⊟
>>	ANY	ANY	ANY	ANY	ANY	ANY	Comment	NONE	☐	⊞

Image 7: Related address assignment table with the selection WAN > LAN

NOTICE

An entry in the address assignment table is only effective if the relevant "**Active**" checkbox is checked. An active entry is highlighted in green.



WAN > LAN | LAN > WAN

#	Source IP	Source Port	WAN Port	Protocol	LAN IP	LAN Port	Comment	Condition	Active	Add/Delete
1	172.25.15.74	ANY	102	TCP	192.168.0.112	102	Comment	DI1-High	☑	⊟
>>	ANY	ANY	ANY	ANY	ANY	ANY	Comment	NONE	☐	⊞

Image 8: Example address assignment table with WAN > LAN selected

Label	Description
Source IP	IP address of the sender of the data packets.
Source Port	The specification of a port serves for a better overview. With ANY there is no restriction.
WAN Port	WAN port of the firewall.

NOTICE

The entry of the WAN port is important because this port is forwarded to the LAN IP / port.

A WAN port = ANY is technically possible, but not useful. Then everything will be forwarded.

Protocol	Selection of the permitted protocol • ANY (all) • ICMP • UDP • TCP
LAN IP	IP address of the subscriber (receiver) in the LAN network.
LAN Port	Port of the subscriber (receiver) in the LAN network.
Comment	Here you can enter a comment for the defined port forwarding.
Condition	Selection field for specifying the condition when a rule is or remains active. You can choose from: **DIN1-High**, **DIN1-Low**, **DIN2-High**, **DIN2-Low** or **NONE**. By wiring (high / low) DI1 or DI2 (digital inputs of the Anybus Defender Compact), you can dynamically de- activate and reactivate a DNAT rule. If you select NONE, the rule remains unaffected.

NOTICE

Only active packet filter rules are transferred to the device. That means: A rule can only be deactivated and reactivated by a signal change at a digital input (high -> low or low -> high).

Active	By confirming the checkbox the port forwarding is active. The relevant line in the assignment table is highlighted in green.

Label	Description
Source IP	IP address of the sender of the data packets.
Source Port	The specification of a port serves for a better overview. With ANY there is no restriction.
LAN Port	LAN port of the firewall.

Label	Description

NOTICE

The entry of the LAN port is important because this port is forwarded to the WAN IP / port.

A LAN port = ANY is technically possible, but not useful. Then everything will be forwarded.

Protocol	Selection of the permitted protocol • ICMP • UDP • TCP
WAN IP	IP address of the subscriber (receiver) in the WAN network.
WAN Port	Port of the subscriber (receiver) in the WAN network.
Comment	Here you can enter a comment for the defined port forwarding.

Condition	Selection field for specifying the condition when a rule is or remains active. You can choose from: **DIN1-High**, **DIN1-Low**, **DIN2-High**, **DIN2-Low** or **NONE**. By wiring (high / low) DI1 or DI2 (digital inputs of the Anybus Defender Compact), you can dynamically de- activate and reactivate a DNAT rule. If you select NONE, the rule remains unaffected.

NOTICE

Only active packet filter rules are transferred to the device. That means: A rule can only be deactivated and reactivated by a signal change at a digital input (high -> low or low -> high).

Active	By confirming the checkbox the port forwarding is active. The relevant line in the assignment table is highlighted in green.

Add/Delete	
	Click on the plus symbol adds an entry in the table.
	Click on the minus icon removes an entry from the table.

TIP

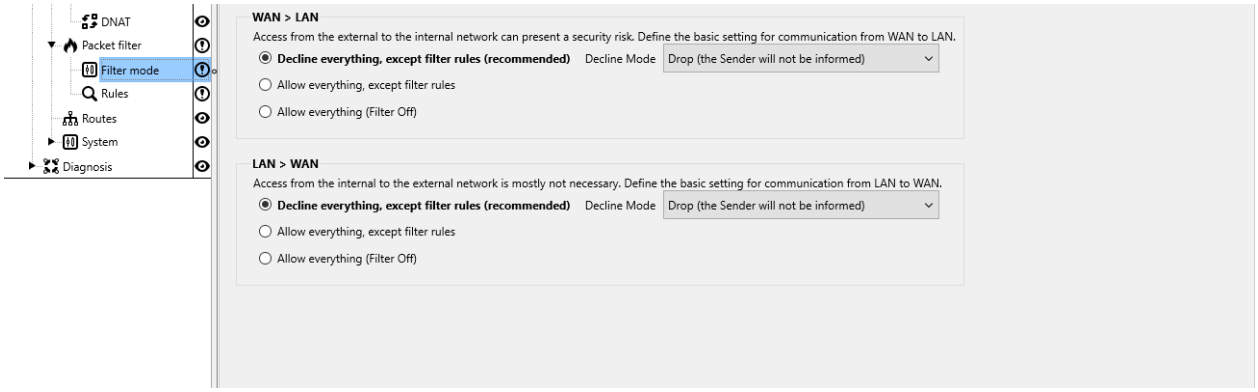
You can easily set the column widths of the table with the mouse.

After clicking on "**Next**" you will be redirected to the setting of the Filter mode.

"Nothing from above"

After clicking on "**Next**" you will be redirected to the setting of the Filter mode.

Set filter mode



Select the appropriate rules under the desired communication directions (WAN > LAN or LAN > WAN).

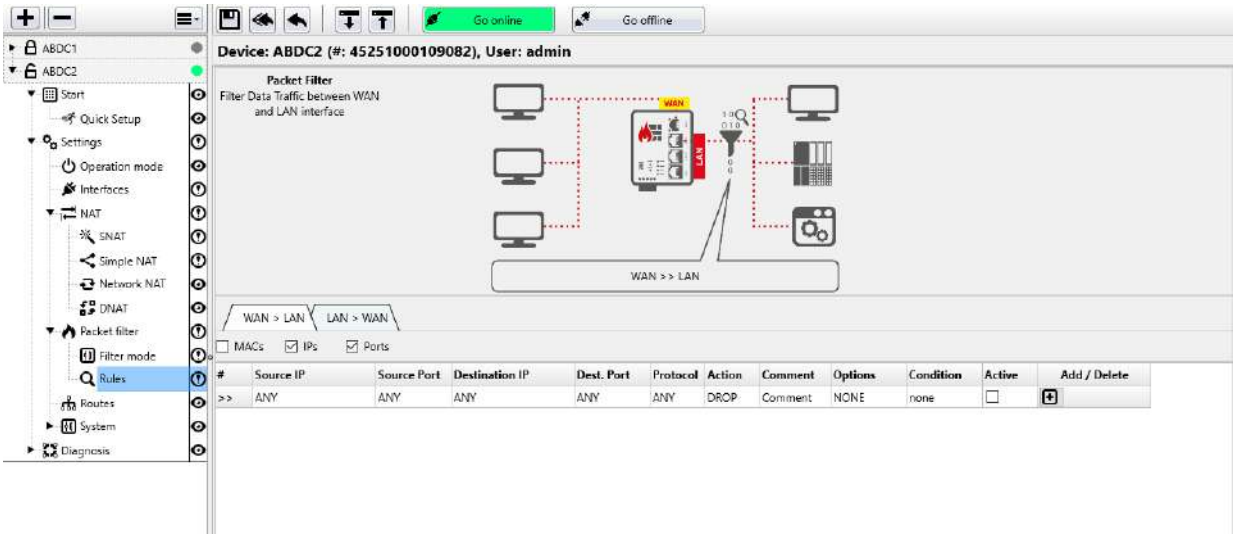
- **Decline everything**, except filter rules (recommended) - so-called *whitelisting*
  - Drop (the sender will not be informed)
  - Reject (the sender will be informed via the ICMP Protocol)
- **Allow everything** except filter rules (see " Rules", Page 85) - so-called *blacklisting*
  Here all packets are accepted at the end of the filter table. The filter sorts but is effectively only off.
- **Allow everything** (**Filter Off**)
  All filters are inactive here and the data transfer is completely accepted.

NOTICE

Further information can be found in the "Packet filter > Filter mode" settings menu.

Click "**Next**" to create the firewall rules.

Create firewall rules



Here you create the individual rules for the firewall ruleset; both **WAN > LAN** and **LAN > WAN**.

A set of rules consists of the settings in the **Filter mode** and the set of **Rules** created.

The policy processes / checks both incoming packets as well as the response packets generated by the network participant and allows allowed connections to pass through the firewall (ACCEPT) or blocks (DROP, REJECT) unauthorized connections.

NOTICE

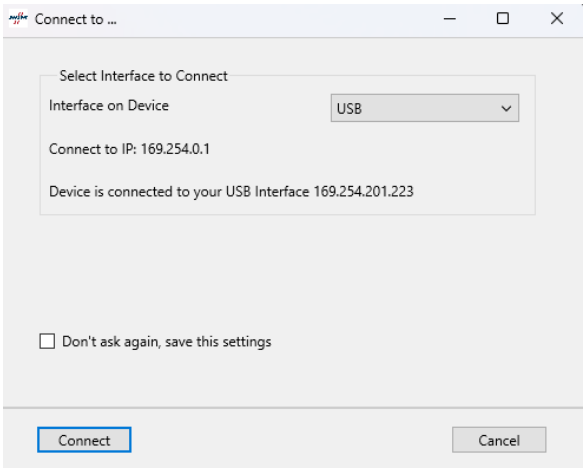
Further information is available in the Settings menu "Packet filter > Rules".

Click on "**Next**" to load the created configuration into the device.

Upload the configuration to the device

In rare cases, you may need to update the USB driver for the "device to PC" connection. To do this, click the "Install USB Driver" button.

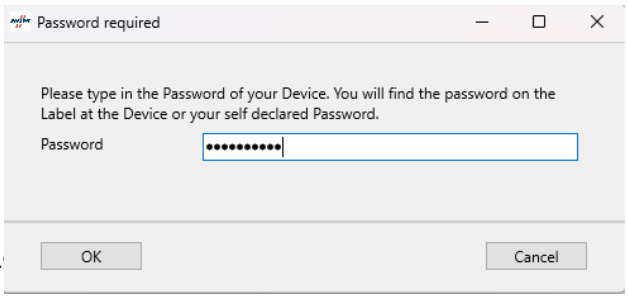
Click on "**Connect**"



The password required for communication (device password) must be entered for the first connection to the device.

The device password is on a label on the back of the device.

Please note that the password is case-sensitive.



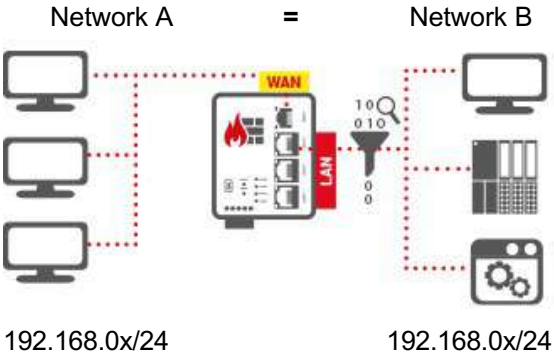
6.2 Settings

6.2.1 Operation mode - general

The ***Anybus Defender Compact*** can be operated either in bridge mode or in gateway mode.

6.2.2 Bridge mode (condition as supplied)

Bridge mode



Without any network changes, the ***Anybus Defender Compact*** protects the data exchange between WAN <> LAN by means of a packet filter.
In bridge mode the firewall is easily integrated into existing networks that are in the same network segment - ideal for upgrades.
The firewall integrates transparently and no IP address specification is necessary.

Exemplary use cases

⇨ **Protection of machines that are already connected to the network**
In bridge mode, the ***Anybus Defender Compact*** makes it easy to control traffic without having to make changes to the network.

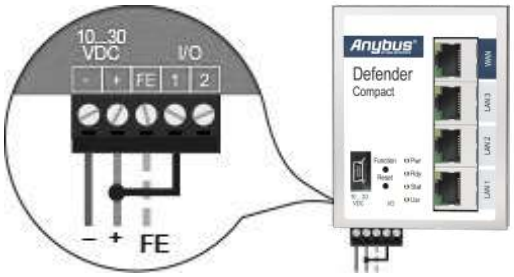
⇨ **Securing of sensitive network components**
To achieve a good IT security standard, controls must be continuously updated. However, this would significantly interfere with running processes and be completely inappropriate.

By activating the ***Anybus Defender Compact*** as an external cyber security watchdog, the PLC security can be in- creased without continually having to implement updates.

NOTICE

By default, the ***Anybus Defender Compact*** is set to bridge mode with packet filter enabled - security by default. The transitions WAN <> LAN are blocked.

By bridging input I/O **1** and P **+** (I/O **1** is thus activated), the packet filter is **inactive** after the ***Anybus Defender Compact*** has been booted - **for the duration of the initial configuration**. That is, the transitions WAN <> LAN are open. The data traffic is detected immediately as soon as the de- vice (***Anybus Defender Compact***) in your network is connected to the desired location.



The bridging of input I/O **1** is ignored after the initial configuration and can only be used again after the ***Anybus Defender Compact*** has been reset to its factory settings.
You should choose the default setting with bridged input I/O **1** if at least one of the two conditions applies.

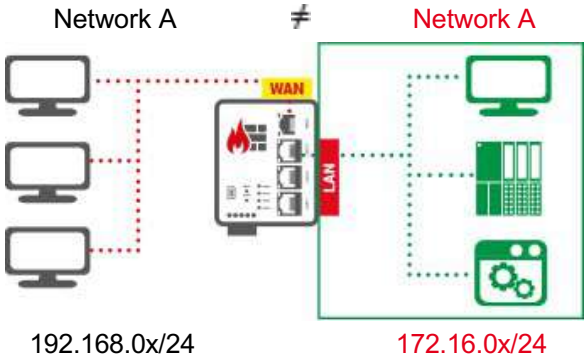
a. You want to make the configuration at a later time
   and already perform the installation
   and not influence the existing network.

b. You want to use the learning function of the ***Anybus Defender Compact*** in order to be able to read out the detected network traffic later during the configuration.

6.2.3 Gateway mode

Gateway mode allows individual areas of a network to be separated. Here too, learning mode simplifies the creation of filter tables.

Gateway mode



In Gateway mode, both WAN and LAN are assigned a defined IP address and in this way segment the networks. Here functions such as NAT (see " NAT settings (gateway mode only)") and forwarding (see " Routes to networks on the WAN side (Gateway mode only)") can be used to route data traffic to sub- ordinate networks. Here too, the packet filter can be used to control WAN <> LAN data exchange.

Example use cases

⇨ **Avoiding address conflicts when installing new machines**
The integration of a new machine in an existing production network can cause address conflicts and render machine installation more laborious and expensive.

Using the ***Anybus Defender Compact***, machine installations can be simplified and shortened. At the same time, internal network conventions are complied with.

⇨ **Easy access to devices in an isolated network segment**
Access to machines in isolated segments can be difficult or even impossible.

With simple NAT, ***Anybus Defender Compact*** easily routes the addresses from the WAN to the LAN side. All that is necessary is for the so-called mapping table to be filled out.

⇨ **Isolating network segments with high data traffic**
Modern communication protocols cause a high data volume.

With ***Anybus Defender Compact***, network segments can be isolated, data traffic locally limited and the bandwidth of the corporate network protected.

6.2.4 Application cases - possible Operating mode and recommended feature

Based on the following table, you can assign the recommended feature of the ***Anybus Defender Compact*** for different applications.

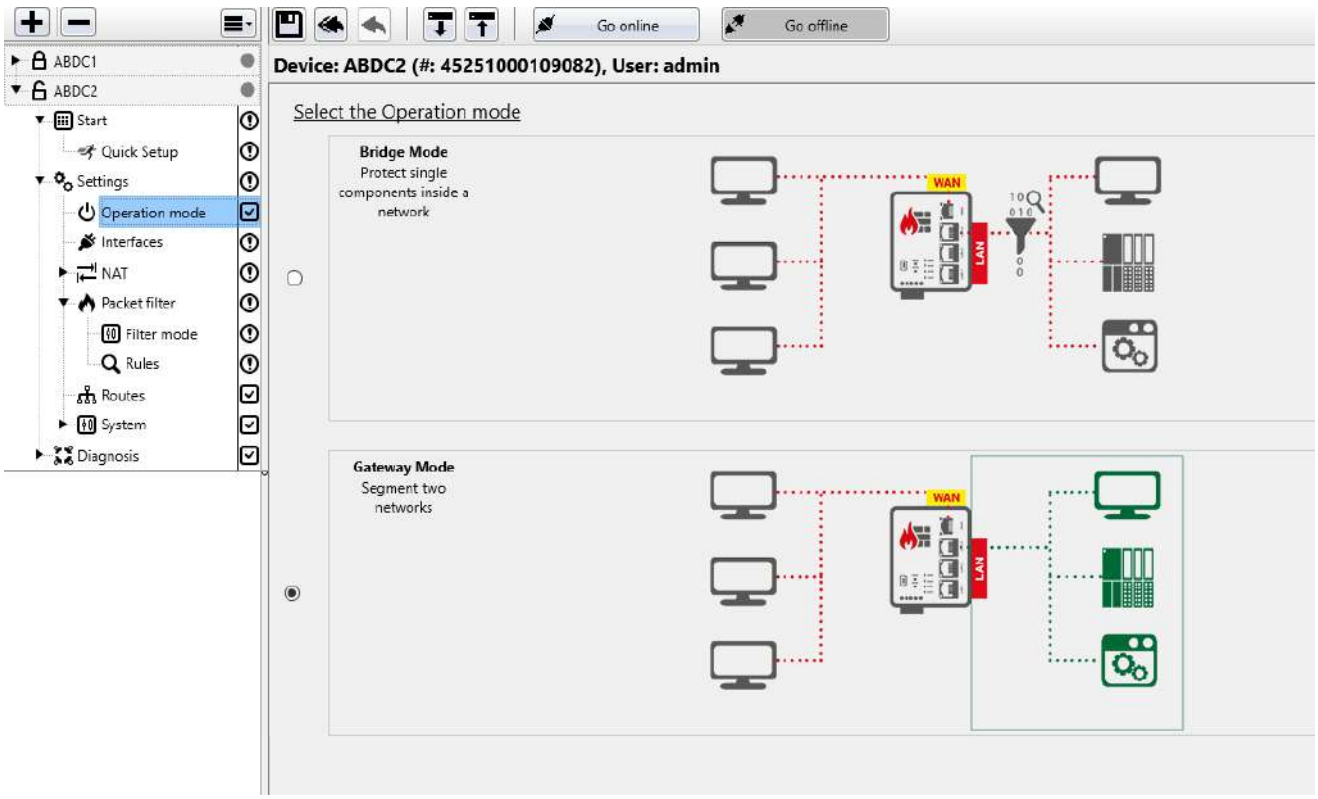
Application	Operation mode	Feature
Avoiding address conflicts when installing new machines	Gateway mode	Simple NAT, Network NAT, port forwarding (see " NAT settings (gateway mode only)", Page 67)
Easy access to devices in an isolated network segment	Gateway mode	Simple NAT (see " Simple NAT (Access to IP devices in an isolated network)", Page 71)
Securing of the internal machine network	Gateway mode	Firewall, packet filter (see " Packet filter", Page 80)
Isolating network segments with high data traffic	Gateway mode	Routes (static routes) (see " Routes to networks on the WAN side (Gateway mode only)", Page 90)
Protection of machines that are already connected to the network	Bridge mode, Gateway mode	Firewall, packet filter (see " Packet filter", Page 80)
Restriction of network access	Bridge mode, Gateway mode	Firewall, packet filter (see " Packet filter", Page 80)
Securing of sensitive network components	Bridge mode	Firewall, packet filter (see " Packet filter", Page 80)

6.2.5 Which function is available in which operating mode?

The following functions are available in the **Settings** menu, depending on the selected operating mode:

Function	**Operating mode**	
	Bridge mode	Gateway mode
NAT	–	✓
SNAT	–	✓
Simple-NAT	–	✓
Network-NAT	–	✓
DNAT	–	✓
Packetfilter	✓	✓
Filtermode	✓	✓
Rules	✓	✓
Routes	–	✓

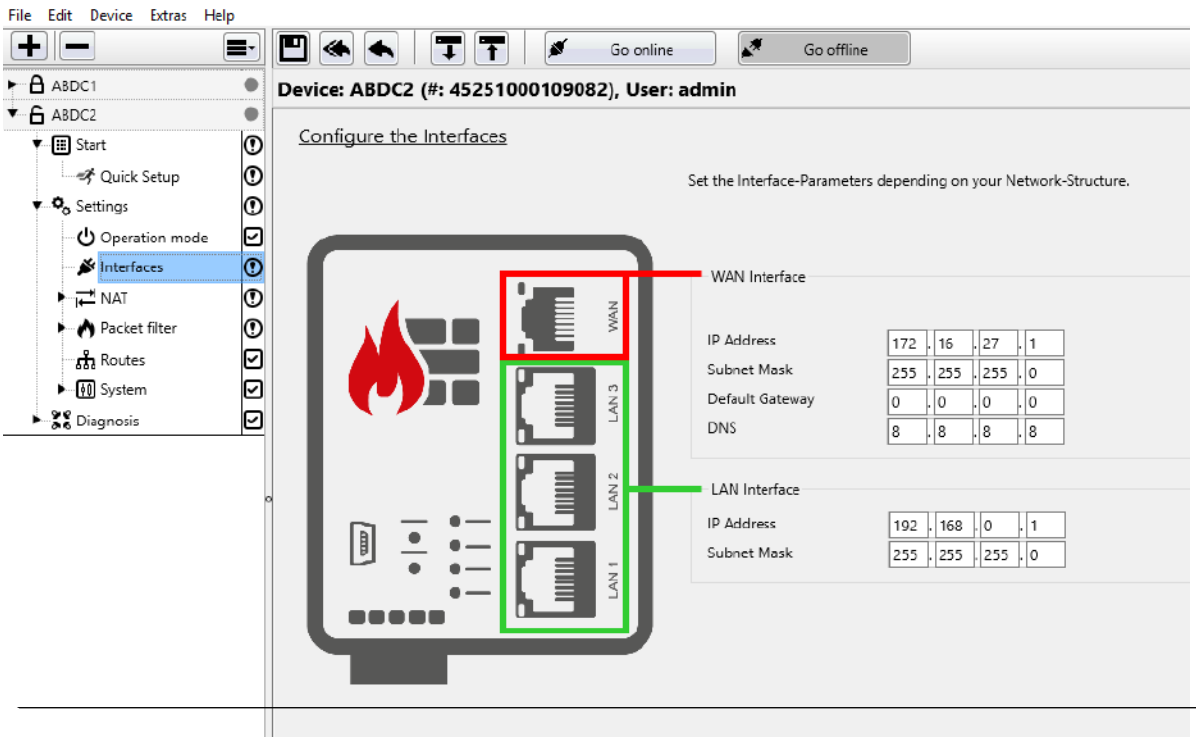
6.2.6 Select Operating mode



Here you select the operating mode (Bridge mode or Gateway mode) for which the device is to be configured.

6.2.7 Interfaces

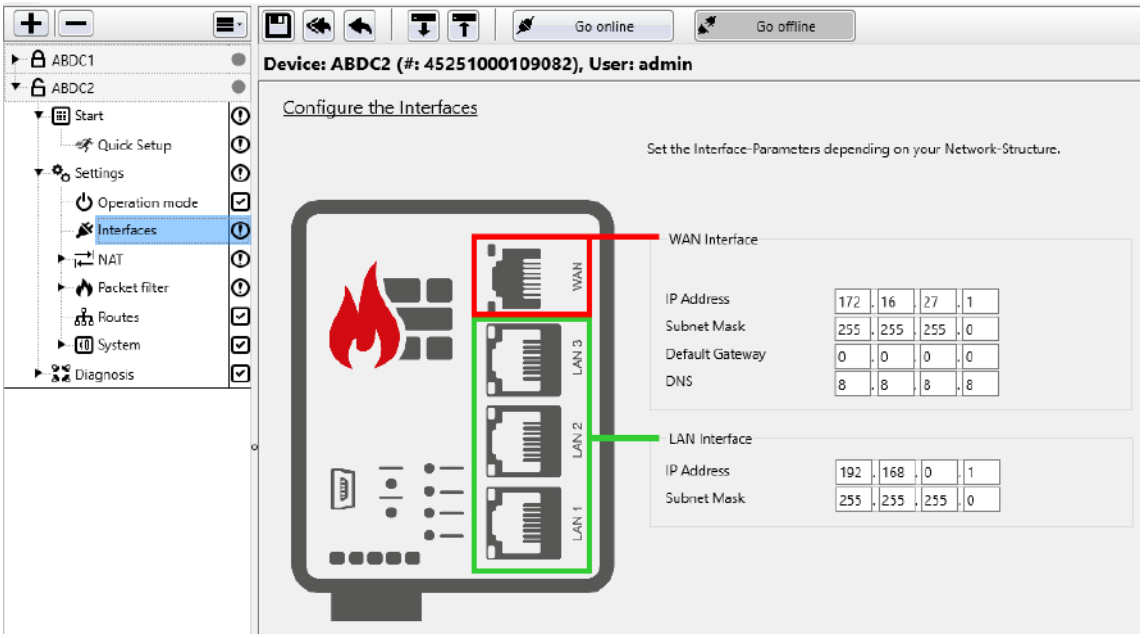
Bridge Mode



WAN / LAN Interface

Label	Description
disable Interface	Checkbox to activate / deactivate the WAN / LAN interface. If the WAN / LAN interface is disabled, it cannot be set as a Configuration Access Level. Settings already made under "System" are deactivated and cannot be changed.
IP Address **Subnet Mask**	The assignment of an IP address / subnet mask is only necessary if the device is to be accessible via IP. For example, for future changes (configuration) via Ethernet or if other services such as Syslog / SNTP are to be used. If you do not enter an IP address, the Anybus Defender Compact is not visible in the network.
Default Gateway	A default gateway is required if • devices from the network want to connect to the Internet, • when integrating devices from the LAN over the WAN into other networks. If this is not desired, the default value "0.0.0.0" must be retained.
DNS	The assignment of a **DNS** server (for SNTP service) is also possible.

Gateway Mode



WAN Interface	
Label	Description
IP Address	Enter the appropriate values for the network on the WAN side here.
Subnet Mask	
Default Gateway	A default gateway is required if • devices from the network want to connect to the Internet.
DNS	The assignment of a **DNS** server (for SNTP service) is also possible.

LAN Interface	
Label	Description

IP Address	Enter the appropriate values for the network on the LAN side here.
Subnet Mask	

6.2.8 NAT settings (gateway mode only)

NAT (Network Address Translation) is the umbrella term for the automatic replacement of address information (IP addresses) inside packets.

As a result of the replacement functionality, this only functions for addresses of different networks A and B.

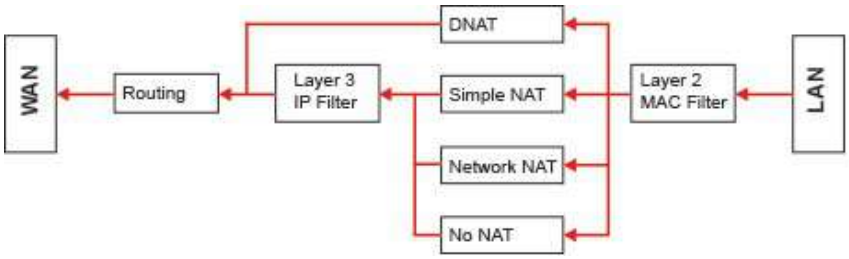


Image 9: Traffic WAN> LAN Schema

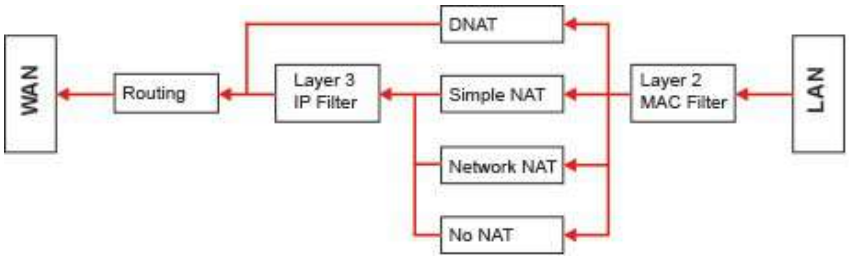


Image 10: Traffic LAN> WAN Schema

- Ports for NTP and DNS of the local service on the device are hard coded in the packet filter if one of these services is enabled.
- **The WAN-IP of the Anybus Defender Compact cannot be pinged by default. This must be released in the filter.**
- If a DNAT rule is specified, it is automatically bypassed at the layer 3 packet filter. The exception is layer 2 (MAC filter). If this is active or a rule specified including MAC address, a corresponding rule can also supplement the DNAT rule.
- Layer 3 packet filter (IP filter) is independent of the set filter mode (whitelisting, blacklisting, etc.).
- Layer 2 packet filter (MAC filter) is switched off by default.
  - Bridge mode
    Broadcast, PROFINET and other layer 2 protocols are passed through.
  - Gateway mode

    Only IP packets are accepted, i.e. Broadcast, PROFINET and other layer 2 protocols are **NOT** passed through.

- MAC filter
  As soon as a MAC address is entered in the filter table, the MAC filter is activated, i.e. the layer 2 packet filter then follows the setting from the firewall filter mode (whitelisting, blacklisting, etc.).

NOTICE

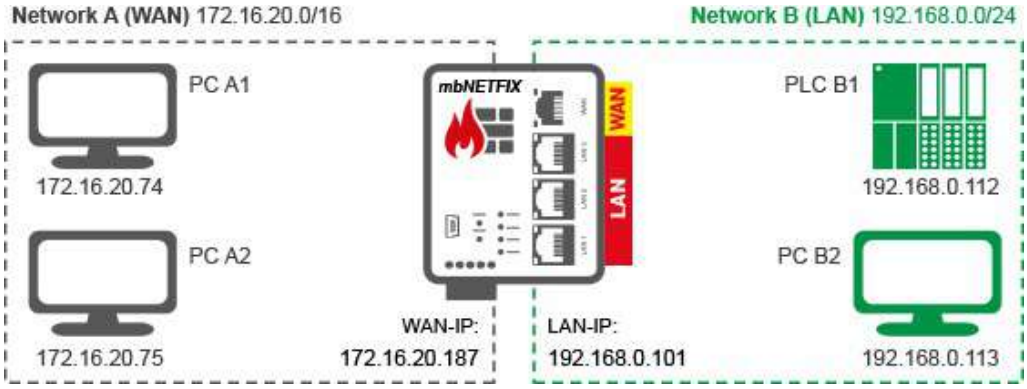
If the packet filter is operated in the "whitelisting" filter mode **and** the MAC filter (Layer 2) is activated, **only** packets that the MAC filter accepts reach the IP filter (Layer 3).

Arrangement

For the description of the individual menus / functions and examples, the following is defined:

The network on the **WAN** side = Network A (172.16.20.0/16)
The WAN IP of the firewall = 172.16.20.187

The network on the **LAN** side = Network **B** (192.168.0.0/24)
The LAN-IP of the firewall = 192.168.0.101



6.2.8.1 SNAT (Source Network Address Translation)

Use SNAT if the network subscriber to be reached is outside the network area of the sender, has no or an incorrect (inappropriate) gateway entry and can therefore not send a reply to an delivered data packet.

For SNAT, the sender IP address of all packets, e.g. from network A (WAN), exchanged against the LAN interface address of the firewall (network B).

Since the receiver in network B does not see the original sender IP address, but the LAN interface address of the own network, no gateway is necessary for the packet response.

This means: the receiver sends the answer to the LAN interface of its own network. Since the firewall "remembered" the IP traffic due to the SNAT, it replaces the packet address with the original sender address.

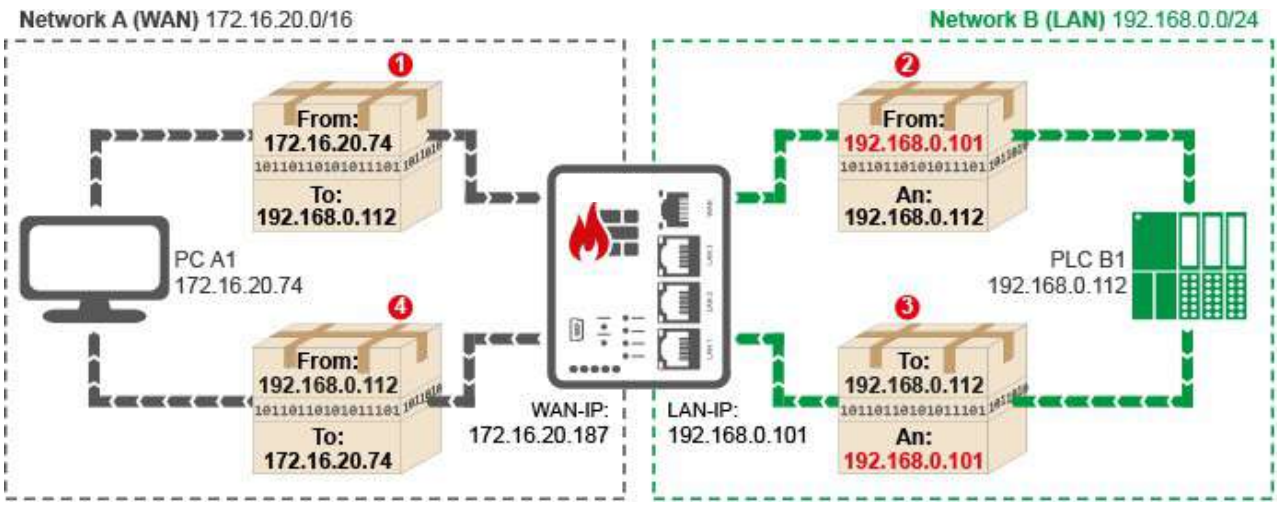


Image 11: Example: Data packet shipment via SNAT from WAN to LAN

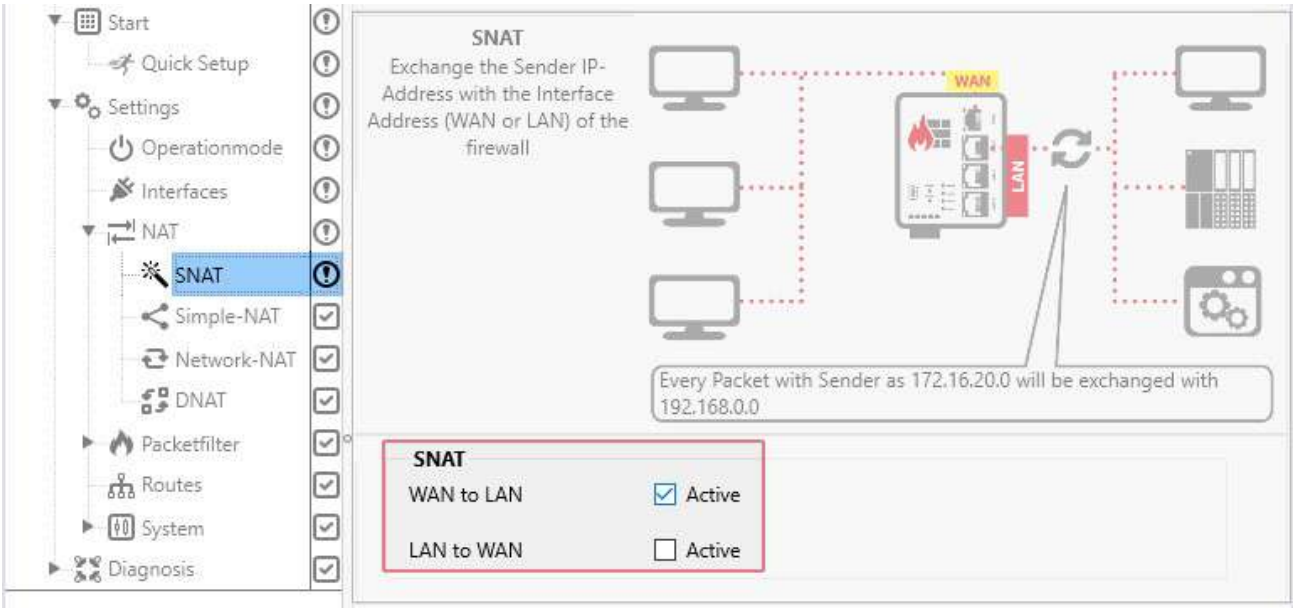
1. PC A1 (IP 172.16.20.74) on the WAN side sends a data packet to PLC B1 (IP 192.168.0.112) on the LAN side.

2. Since SPS B1 does not have a valid gateway entry, it could not send a response packet to the original IP.

Therefore, in the firewall, the sender IP (IP 172.16.20.74) is replaced by the interface IP of the firewall on the LAN side (IP 192.168.0.101) and the packet is delivered to the PLC B1.

3. The answer packet of SPS B1 is addressed to the LAN-IP IP 192.168.0.101.

4. When transferring to the WAN side, the original IP address of PC A1 (172.16.20.74) is reinstated in the firewall and the packet is delivered.



By clicking on the respective "Active" checkbox you determine the corresponding direction (WAN to LAN or LAN to WAN).

NOTICE

In addition, you must still enable the communication to the individual nodes in the **Packet filter** !

6.2.8.2 Simple NAT (Access to IP devices in an isolated network)

NOTICE

Use Simple NAT to access an IP address from network B (LAN) 1:1 on network A (WAN).

With this function, a network participant in the LAN can be directly addressed via a WAN IP address. As it were, the IP address of a LAN participant with an IP address from the WAN area is mirrored in the WAN. This does not require a virtual IP address, as is usual with a NAT function.

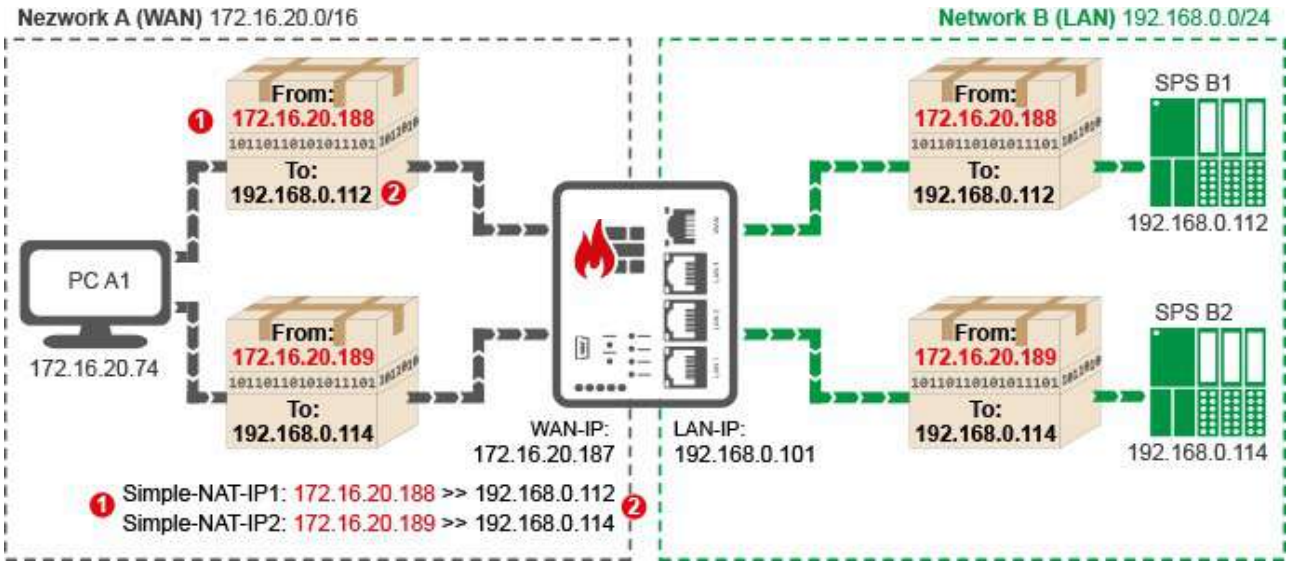


Image 12: Example: Data packet delivery to two subscribers using Simple-NAT from WAN to LAN

To do this, enter in the address assignment table

1. a free WAN Ethernet address from the WAN network and

2. and the LAN IP address of the recipient from the LAN network to be "natted" with.

NOTICE

You need a separate WAN IP address for each receiver (network subscriber in the LAN network).

NOTICE

If one of the network participants to be reached has no or a wrong (inappropriate) gateway entry and can therefore not send a response to an delivered data packet, you must also activate the "WAN to LAN" function in the SNAT.

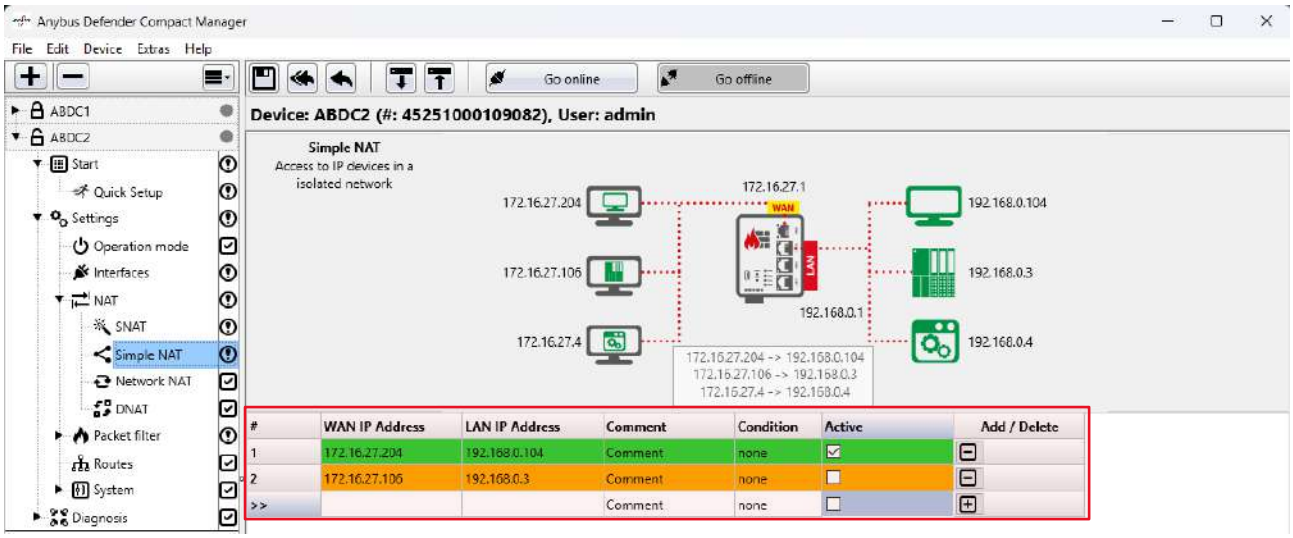


Image 13: Address assignment table

Label	Description
WAN IP-Address	Enter a free WAN IP address from the WAN network.
LAN IP-Address	Enter the IP address of the recipient from the LAN network.
Comment	Here you can enter a comment for the defined assignment.
Condition	Selection field for specifying the condition when a rule is or remains active. You can choose from: **DIN1-High**, **DIN1-Low**, **DIN2-High**, **DIN2-Low** or **NONE**. By wiring (high / low) DI1 or DI2 (digital inputs of the Anybus Defender Compact), you can dynamically deactivate and reactivate a SimpleNAT filter rule. If you select NONE, the rule remains unaffected.

NOTICE

Only active packet filter rules are transferred to the device. That means: A rule can only be deactivated and reactivated by a signal change at a digital input (high -> low or low -> high).

Active	Checkbox for activating / deactivating the assignment.
Add/Delete	Click on the plus icon ⊞ to add the mapping. Click on the minus icon ⊟ to delete an assignment.

TIP

You can easily set the column widths of the table with the mouse.

NOTICE

As soon as you have added and activated an assignment, the rule for this assignment is automatically entered and activated under **Packet filter** > **Rules** > WAN > LAN.

#	WAN IP Address	LAN IP Address	Comment	Condition	Active	Add / Delete
1	172.16.27.204	192.168.0.104	Kommentar	DI1-High	☑	⊖
2	172.16.27.106	192.168.0.3	Kommentar	DI1-High	☐	⊖
>>			Kommentar	none	☐	⊕

Image 14: Example entries in address assignment table

WAN > LAN | LAN > WAN

☐ MACs ☑ IPs ☐ Ports

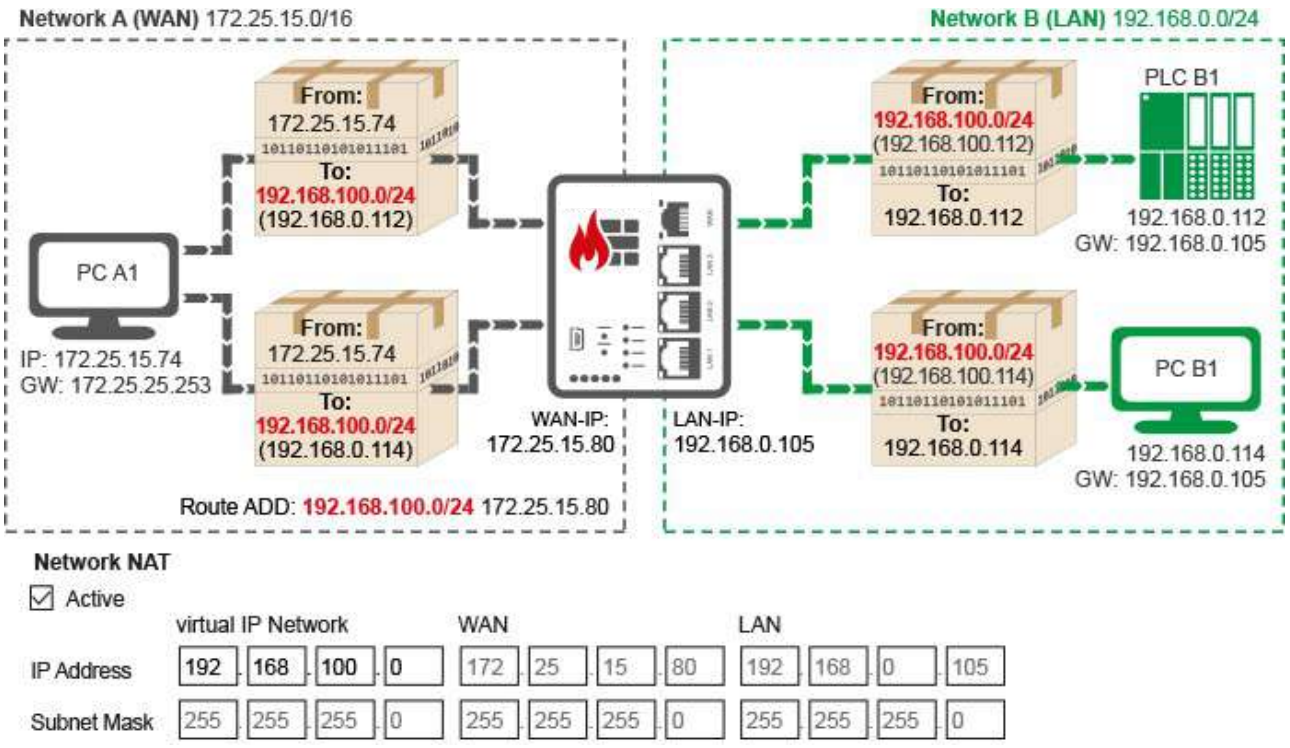
#	Source IP	Destination IP	Protocol	Action	Comment	Options	Condition	Active	Add / Delete
1	ANY	192.168.0.104	ANY	ACCEPT	SimpleNAT:17	NONE	DI1-High	☑	⊖
2	ANY	192.168.0.3	ANY	ACCEPT	SimpleNAT:17	NONE	DI1-High	☐	⊖
>>	ANY	ANY	ANY	DROP	Comment	NONE	none	☐	⊕

Image 15: Related entries in the firewall rules WAN>LAN

6.2.8.3 Network NAT

NOTICE

Use Network NAT to reach an IP range (complete or partial) from Network B (LAN) 1: 1 in Network A (WAN).



With the network NAT function, the entire area or a subarea of the LAN network can be addressed directly via a virtual network. It is almost an IP address of a LAN participant with an IP address mirrored from the virtual network.

Each network participant from the LAN uses a separate IP address from the virtual network.

The host part of each virtual IP address is the same as the host part of the real recipient address.

Conditions for Network NAT:

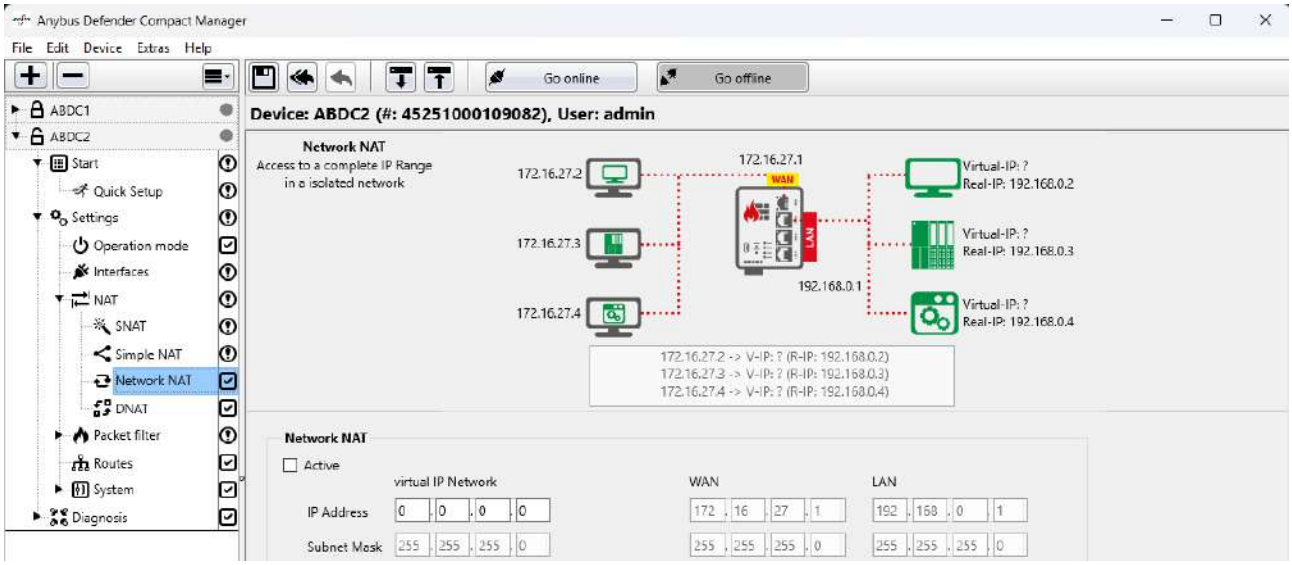
- The virtual network must not be in the same address range as the WAN or LAN network.
- Each network participant needs a corresponding gateway entry.

NOTICE

If a network subscriber from the LAN network has no or a wrong (inappropriate) gateway entry, you must additionally activate the SNAT function "WAN to LAN".

Simultaneous activation of Network-NAT and SNAT "LAN to WAN" is not possible.

- The communication between the individual participants must also be released in the packet filter.
  Here, the real IP addresses of the LAN side must be used for the packet filter.
  That is, if you define the destination IPs from "WAN to LAN", you will need to use the IPs of the LAN side, not the NAT IPs (virtual IPs).



Label	Description
Aktiv	Check box for enabling/disabling this function.
Virtual IP Network	Enter a free network address as a virtual IP network here.
WAN	Here the WAN and LAN interface of the Anybus Defender Compact is displayed.
LAN	

6.2.8.4. DNAT (port forwarding)

Access to IP services in an isolated network

NOTICE

DNAT stands for Destination NAT. This changes the destination of the data packet.

With port forwarding, a single port can be forwarded to a specific IP address specifying the port.
Port forwarding is available from WAN to LAN as well as LAN to WAN.

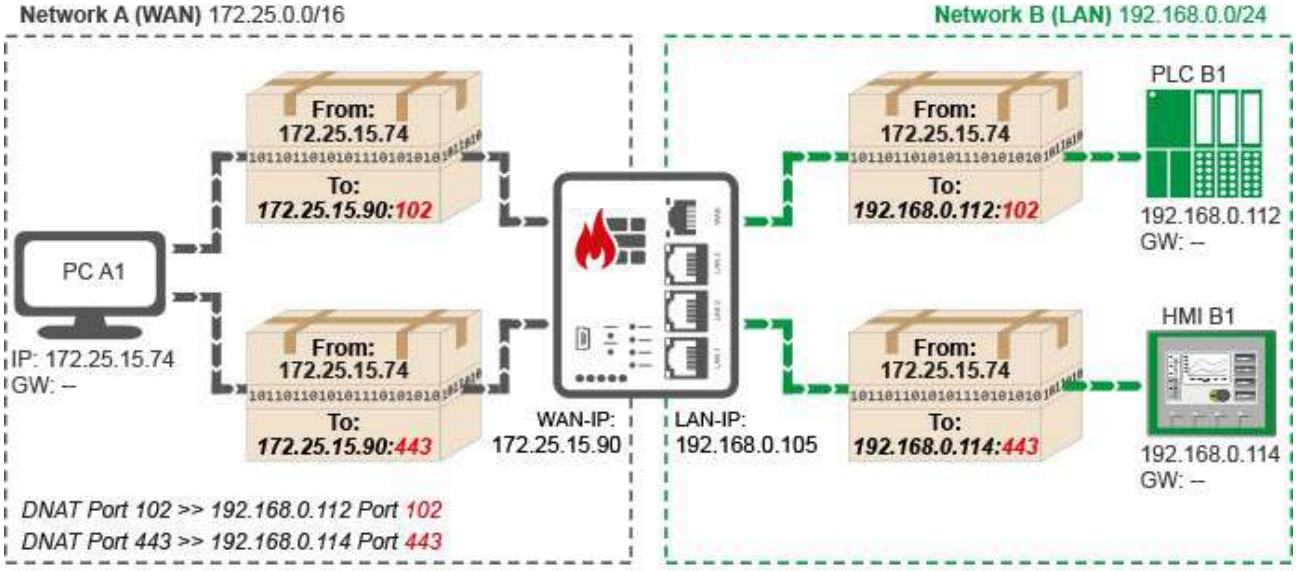


Image 16: Example diagram of a DNAT from WAN to LAN
PLC B1 (programming port 102) and HMI B2 (web server port 443) should be accessible via PC A1.

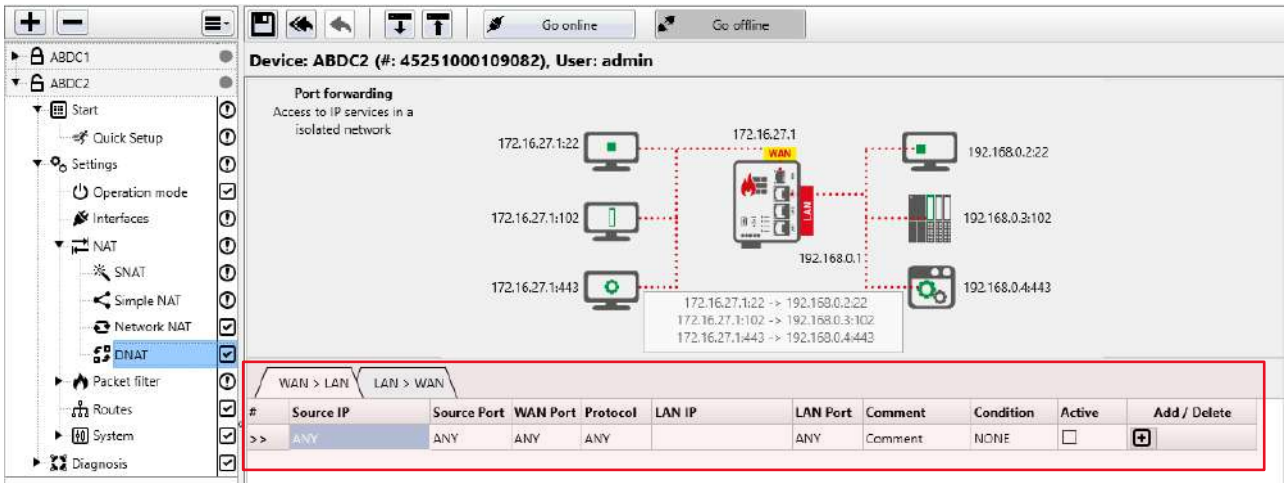
WAN > LAN | LAN > WAN

#	Source IP	Source Port	WAN Port	Protocol	LAN IP	LAN Port	Comment	Condition	Active	Add/Delete
1	172.25.15.74	ANY	102	TCP	192.168.0.112	102	Comment	DI1-High	☑	⊟
2	172.25.15.74	ANY	443	TCP	192.168.0.114	443	Comment	DI1-High	☐	⊟
>>	ANY	ANY	ANY	ANY	ANY	ANY	Comment	NONE	☐	⊞

Image 17: Related address assignment table with the selection WAN > LAN

NOTICE

An entry in the address assignment table is only effective if the relevant "**Active**" checkbox is checked. An active entry is highlighted in green.



WAN > LAN

WAN > LAN | LAN > WAN

#	Source IP	Source Port	WAN Port	Protocol	LAN IP	LAN Port	Comment	Condition	Active	Add/Delete
1	172.25.15.74	ANY	102	TCP	192.168.0.112	102	Comment	DI1-High	☑	⊟
>>	ANY	ANY	ANY	ANY	ANY	ANY	Comment	NONE	☐	⊞

Image 18: Example address assignment table with WAN > LAN selected

Label	Description
Source IP	IP address of the sender of the data packets.
Source Port	The specification of a port serves for a better overview. With ANY there is no restriction.
WAN Port	WAN port of the firewall.

NOTICE

The entry of the WAN port is important because this port is forwarded to the LAN IP / port.

A WAN port = ANY is technically possible, but not useful. Then everything will be forwarded.

Protocol	Selection of the permitted protocol • ANY (all) • ICMP • UDP • TCP
LAN IP	IP address of the subscriber (receiver) in the LAN network.
LAN Port	Port of the subscriber (receiver) in the LAN network.
Comment	Here you can enter a comment for the defined port forwarding.

Label	Description
Condition	Selection field for specifying the condition when a rule is or remains active. You can choose from: **DIN1-High**, **DIN1-Low**, **DIN2-High**, **DIN2-Low** or **NONE**. By wiring (high / low) DI1 or DI2 (digital inputs of the Anybus Defender Compact), you can dynamically de- activate and reactivate a DNAT rule. If you select NONE, the rule remains unaffected.

NOTICE

Only active packet filter rules are transferred to the device. That means: A rule can only be deactivated and reactivated by a signal change at a digital input (high -> low or low -> high).

Active	By confirming the checkbox the port forwarding is active. The relevant line in the assignment table is highlighted in green.

LAN > WAN

Label	Description
Source IP	IP address of the sender of the data packets.
Source Port	The specification of a port serves for a better overview. With ANY there is no restriction.
LAN Port	LAN port of the firewall.

NOTICE

The entry of the LAN port is important because this port is forwarded to the WAN IP / port.

A LAN port = ANY is technically possible, but not useful. Then everything will be forwarded.

Protocol	Selection of the permitted protocol • ICMP • UDP • TCP
WAN IP	IP address of the subscriber (receiver) in the WAN network.
WAN Port	Port of the subscriber (receiver) in the WAN network.
Comment	Here you can enter a comment for the defined port forwarding.
Condition	Selection field for specifying the condition when a rule is or remains active. You can choose from: **DIN1-High**, **DIN1-Low**, **DIN2-High**, **DIN2-Low** or **NONE**. By wiring (high / low) DI1 or DI2 (digital inputs of the Anybus Defender Compact), you can dynamically de- activate and reactivate a DNAT rule. If you select NONE, the rule remains unaffected.

NOTICE

Only active packet filter rules are transferred to the device. That means: A rule can only be deactivated and reactivated by a signal change at a digital input (high -> low or low -> high).

Active	By confirming the checkbox the port forwarding is active. The relevant line in the assignment table is highlighted in green.

Add/Delete	
	Click on the plus symbol adds an entry in the table.
	Click on the minus icon removes an entry from the table.

TIP

#	Source IP	Source Port	WAN Port	Protocol	LAN IP	LAN Port	Comment	Condition	Active
>>	ANY	ANY	ANY	ANY		ANY	Comment	NONE	☐

You can easily set the column widths of the table with the mouse.

6.2.9 Packet filter

Packet filters, also called **network filters**, filter the incoming and outgoing data traffic in a computer network. This usually serves both the protection of the network against attackers and the protection against unintentionally outgoing data packets.

In a firewall rule, you define which traffic is permitted or forbidden by a firewall. Depending on the sender, delivery address and protocol allowed data packets may pass (ACCEPT), forbidden data packets are rejected (REJECT) or discarded (DROP).

Here you can

a. use the **Filter mode** to restrict all traffic between the WAN and LAN networks

b. and define under **Rules** the communication of individual network subscribers.

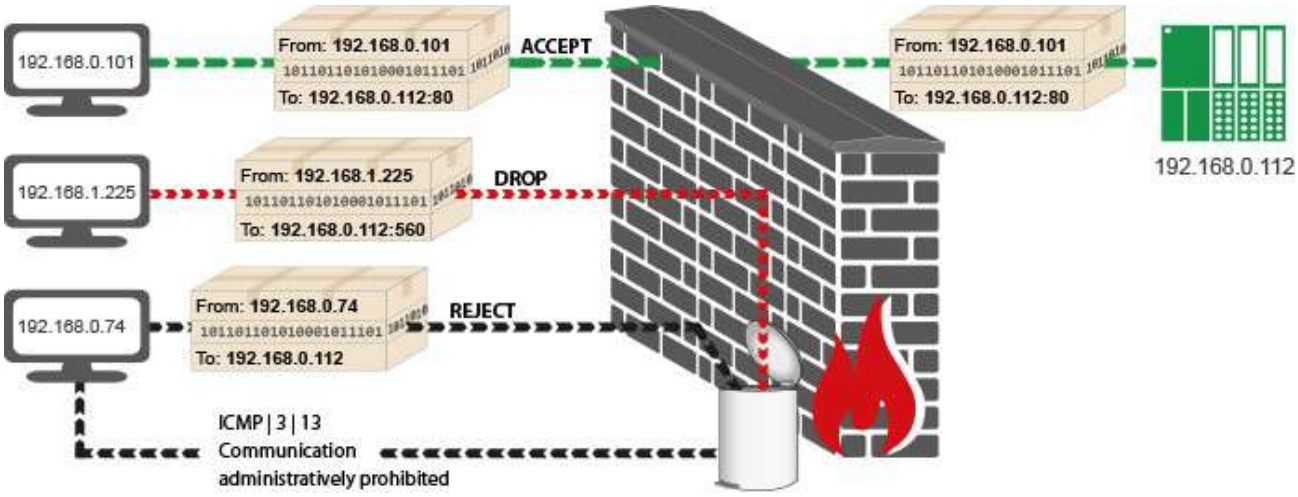


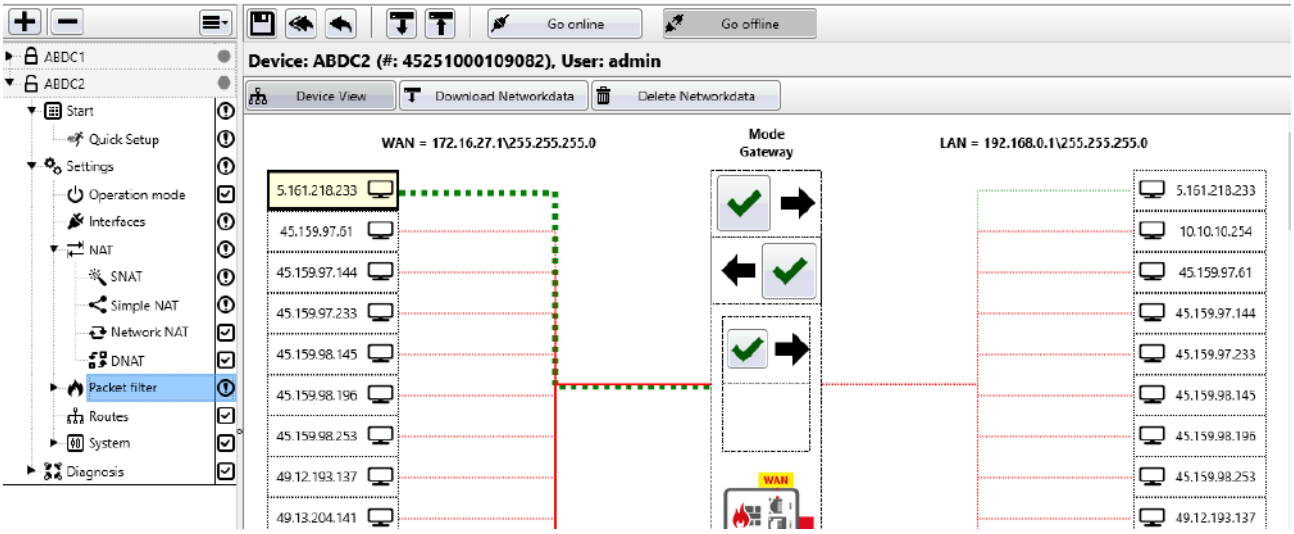
Image 19: Sample graphic for a packet filter WAN > LAN

#	Source-IP	Source-Port	Destination-IP	Dest. Port	Protocol	Action	Comment
1	192.168.0.101	ANY	192.168.0.112	80	TCP	ACCEPT	allowed connection (accept)
2	192.168.1.225	ANY	192.168.0.112	560	UDP	DROP	unauthorized connection (drop)
3	192.168.0.74	ANY	ANY	ANY	ANY	REJECT	unauthorized connection (reject)

Table 1: Sample rules WAN > LAN

Device View (Mapping Table)

Image 20: Device view of detected / learned network participants / network communication



In the device view, the recognized (detected) network participants and the learned network communication are displayed in a mapping table.

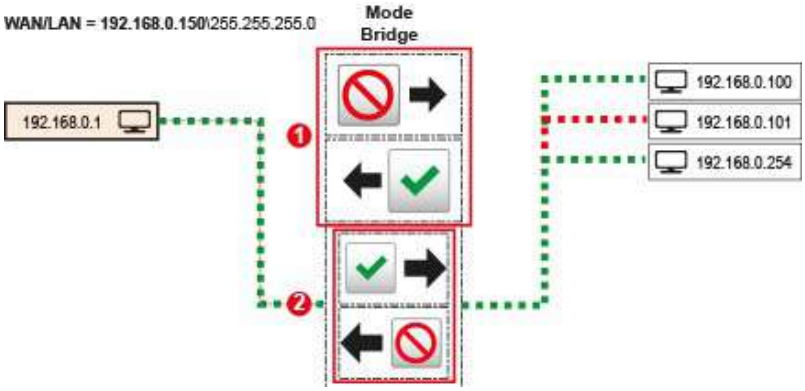
Prerequisites for displaying the mapping table:

- The firewall (Anybus Defender Compact) must be integrated in the network structure and
- the firewall must be in online mode.

By clicking on the "**Download Networkdata**" button, the device view is updated, and additionally detected network participants are listed.

With just a click of the mouse In the device view, you can

1. set the filter modes for the data router of WAN> LAN and LAN> WAN and
2. the communication of individual network nodes with just a click of the mouse.



By clicking on the "**Delete Networkdata**" button, the display of the device participants is deleted.

Click on "**Download Networkdata**", the current network participants are displayed again.

Control of the complete data traffic - Filtermode

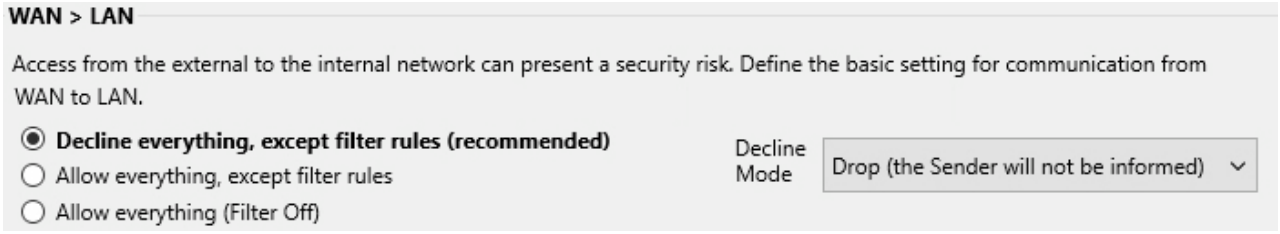
1 The control of the data traffic takes place over the switches / for the respective direction.

Example:

Clicking the switch → ("All traffic from WAN to LAN is allowed") changes the switch setting

→ ("All traffic from WAN to LAN is blocked")

At the same time, WAN>LAN **Filtermode** changes to "Decline everything except filter rules (recommended)".

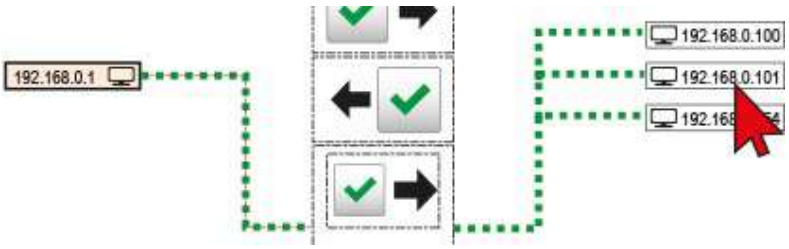


Communication of individual network participants - Rules

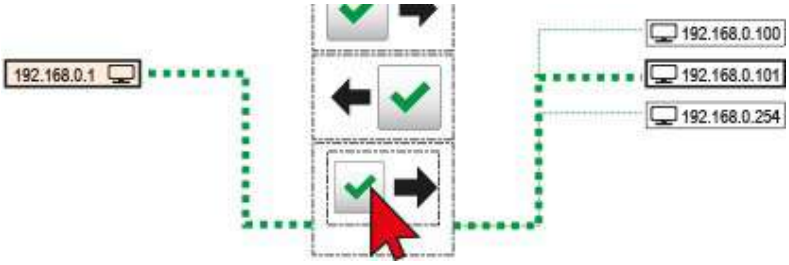
The communication of individual network subscribers is determined by the switches / for the respective direction and the respective entry of a network subscriber 192.168.0.101

Example:

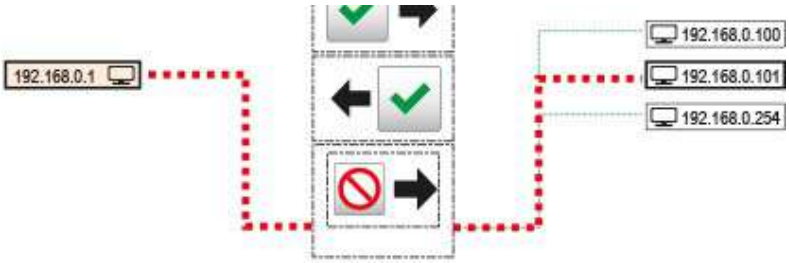
Click the entry of the network subscriber for whom you want to create / change a rule.



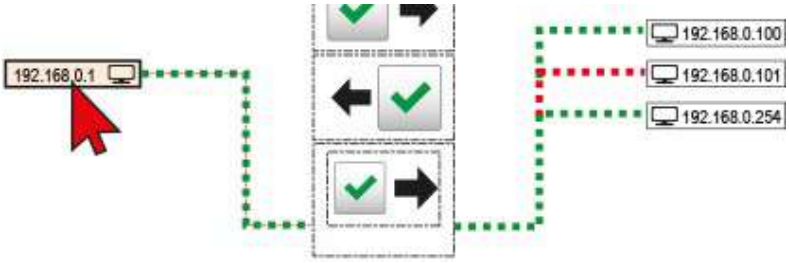
Click on the button to create / change the rule between the network device 192.168.0.101 and 192.168.0.1.



The traffic between 192.168.0.101 and 192.168.0.1 is now blocked.



After clicking on the network participant in the WAN network, the entire device view is displayed again.



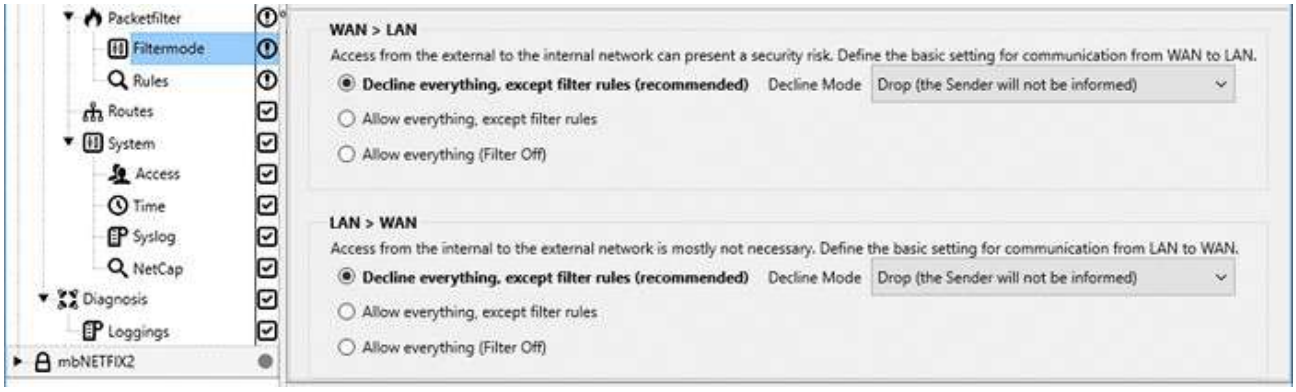
The entries under **Rules** then look like this for WAN> LAN traffic:

WAN > LAN | LAN > WAN

#	Source IP	Source Port	Destination IP	Dest. Port	Protocol	Action	Comment	Active	Add/Delete
1	192.168.0.1	ANY	192.168.0.1	ANY	ICMP	ACCEPT	@1	☑	⊟
2	192.168.0.1	ANY	192.168.0.101	80	TCP	DROP	@1	☑	⊟
3	192.168.0.1	ANY	192.168.0.101	ANY	ICMP	DROP	@1	☑	⊟
4	192.168.0.1	ANY	192.168.0.101	137	UDP	DROP	@1	☑	⊟
5	192.168.0.1	ANY	192.168.0.100	137	UDP	ACCEPT	@1	☑	⊟

6.2.9.1 Filter mode

Filter mode is part of the firewall policy. Here you regulate the general procedure of all data packets arriving at the firewall.



1. Select the appropriate rules under the desired communication directions (WAN > LAN or LAN > WAN).

Select the appropriate rules under the desired communication directions (WAN > LAN or LAN > WAN).

- **Decline everything**, except filter rules (recommended) - so-called *whitelisting*
  - Drop (the sender will not be informed)
  - Reject (the sender will be informed via the ICMP Protocol)

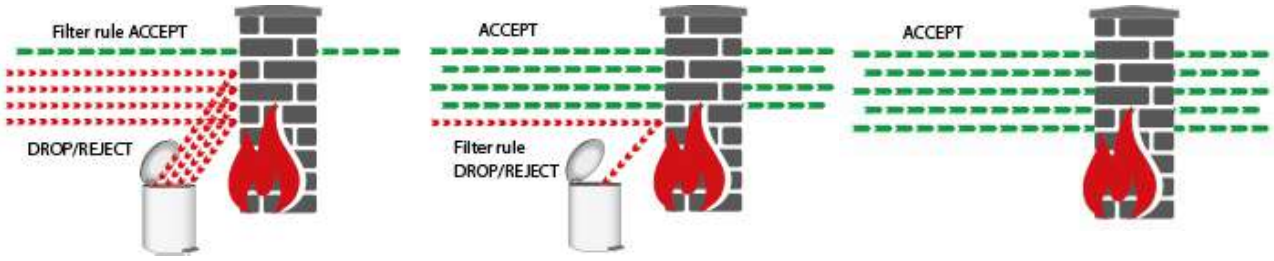
- **Allow everything** except filter rules (see " Rules", Page 85) - so-called *blacklisting*
  Here all packets are accepted at the end of the filter table. The filter sorts but is effectively only off.
- **Allow everything** (**Filter Off**)
  All filters are inactive here and the data transfer is completely accepted.

Filter mode

Decline everything, except filter rules (recommended) - **Whitelisting**

Allow everything, except filter rules - **Blacklisting**

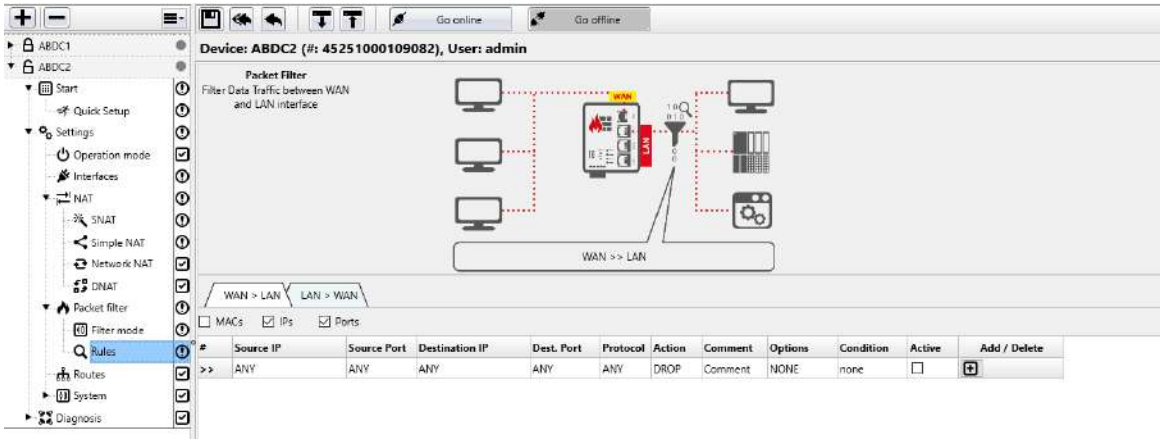
Allow everything (filter OFF)



Decline Mode

- **Drop** (the sender will not be informed)
  If this option is selected, it means that no data packets can pass.
  The packets are deleted immediately.
  The sender is not notified about the whereabouts of the data packets.
- **Reject** (the sender will be informed with ICMP)
  If this option is selected, the data packets are rejected.
  The sender is notified that the data packets have been rejected.

6.2.9.2. Rules



Here you create the individual rules for the firewall ruleset; both **WAN > LAN** and **LAN > WAN**.

A set of rules consists of the settings in the **Filter mode** and the set of **Rules** created.

The policy processes / checks both incoming packets as well as the response packets generated by the network participant and allows allowed connections to pass through the firewall (ACCEPT) or blocks (DROP, REJECT) unauthorized connections.

NOTICE

The firewall rules are evaluated from top to bottom. Exception rules that affect individual Mac or IP addresses should therefore be at the top.

General

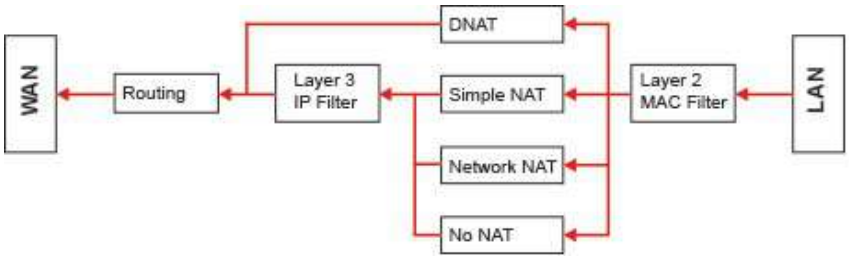


Image 21: Traffic WAN> LAN Schema

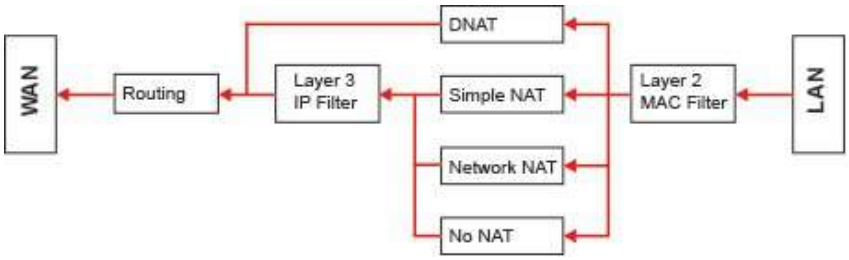


Image 22: Traffic LAN> WAN Schema

- Ports for NTP and DNS of the local service on the device are hard-coded in the packet filter if one of these services is enabled.
- **The WAN-IP of the Anybus Defender Compact can not be pinged by default. This must be released in the filter.**
- If a DNAT rule is specified, it is automatically bypassed at the layer 3 packet filter. The exception is layer 2 (MAC filter). If this is active or a rule specified including MAC address, a corresponding rule can also supplement the DNAT rule.
- Layer 3 packet filter (IP filter) is independent of the set filter mode (whitelisting, blacklisting, etc.).
- Layer 2 packet filter (MAC filter) is switched off by default.
  - Bridge mode
    Broadcast, PROFINET and other layer 2 protocols are passed through.
  - Gateway mode

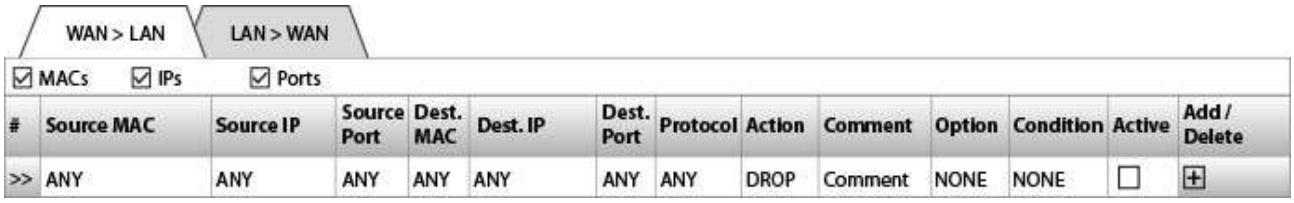
    Only IP packets are accepted, i.e. Broadcast, PROFINET and other layer 2 protocols are **NOT** passed through.

- MAC filter
  As soon as a MAC address is entered in the filter table, the MAC filter is activated, i.e. the layer 2 packet filter then follows the setting from the firewall filter mode (whitelisting, blacklisting, etc.).

NOTICE

If the packet filter is operated in the "whitelisting" filter mode **and** the MAC filter (Layer 2) is activated, **only** packets that the MAC filter accepts reach the IP filter (Layer 3).

Create a Rule



1. Select the appropriate tab (WAN > LAN or LAN > WAN) to define the required rules.

2. Using the "MACs", "IPs" and "Ports" checkboxes, you can hide and / or display the associated columns as required.

3. Fill out the required fields by entering values or selecting.

NOTICE

To reset a rule entry to ANY after a change / incorrect entry,

a. highlight the relevant field and press the "Delete" key on your keyboard

or

b. delete the complete entry => ANY will be automatically entered again.

4. Click on "Add / Delete" to add or delete a rule.

TIP

You can easily set the column widths of the table with the mouse.

Designation	Description
Source MAC	MAC address (physical address) of the network subscriber from which a data packet originates. **NOTICE** MAC addresses must be entered in the format "AA-BB-CC-DD-EE-FF" (numbers in hexa-decimal).
Source IP	IP address of the network subscriber from which a data packet originates.
Source Port	Port no. of the network subscriber from which a data packet originates.
Destination MAC	MAC address (physical address) of the network subscriber to which a data packet is addressed.
Destination IP	IP address of the network subscriber to which a data packet is addressed.
Destination Port	Port no. to which the network subscriber listens to which a data packet is addressed.

Protocol	Selection of the permitted protocol • ANY (all) • ICMP • UDP • TCP
Action	Selection of the action, how to proceed with a data package • ACCEPT • REJECT (The sender is informed by ICMP package.) • DROP (The package is discarded without notifying the sender.)
Comment	Here you can enter a comment on a defined rule.
Option	Selection field for using the FTP helper. In addition to control port 21, the FTP server can also use dynamic ports. By selecting this function, dynamic ports are recognized on the packet filter, via which the data connection is then established.
Condition	Selection field for specifying the condition when a rule is or remains active. You can choose from: **DIN1-High**, **DIN1-Low**, **DIN2-High**, **DIN2-Low** or **NONE**. By wiring (high / low) DI1 or DI2 (digital inputs of the Anybus Defender Compact), you can dynamically de- activate and reactivate a packet filter rule. If you select NONE, the rule remains unaffected.

NOTICE

Only active packet filter rules are transferred to the device. That means: A rule can only be deactivated and reactivated by a signal change at a digital input (high -> low or low -> high).

Active	Checkbox to activate / deactivate a rule.
Add / Delete	After confirming with this button, the rule will be included in the ruleset / deleted from the ruleset.

WAN > LAN | LAN > WAN

☑ MACs ☑ IPs ☑ Ports

#	Source MAC	Source IP	Source Port	Dest. MAC	Dest. IP	Dest. Port	Protocol	Action	Comment	Option	Condition	Active	Add / Delete
1	ANY	ANY	ANY	ANY	ANY	ANY	ANY	DROP	Comment	NONE	DI1-High	☐	⊟
2	9C-EB-E8-84-3D-5E	ANY	ANY	ANY	ANY	ANY	ANY	DROP	Comment	NONE	DI1-High	☑	⊟
3	ANY	192.168.0.101	ANY	ANY	192.168.0.112	80	TCP	DROP	Comment	NONE	NONE	☑	⊟
>>	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ACCEPT	Comment	NONE	NONE	☐	⊞

Image 23: Example Rules: **Allow everything** except filter rules (blacklisting) - direction = **WAN > LAN**

As soon as a rule has been added, it receives a serial number and can be active (highlighted in green) or inactive (highlighted in orange).

NOTICE

When defining a rule, there is no plausibility check.

Avoid defining rules that cancel each other or block all traffic.

Example

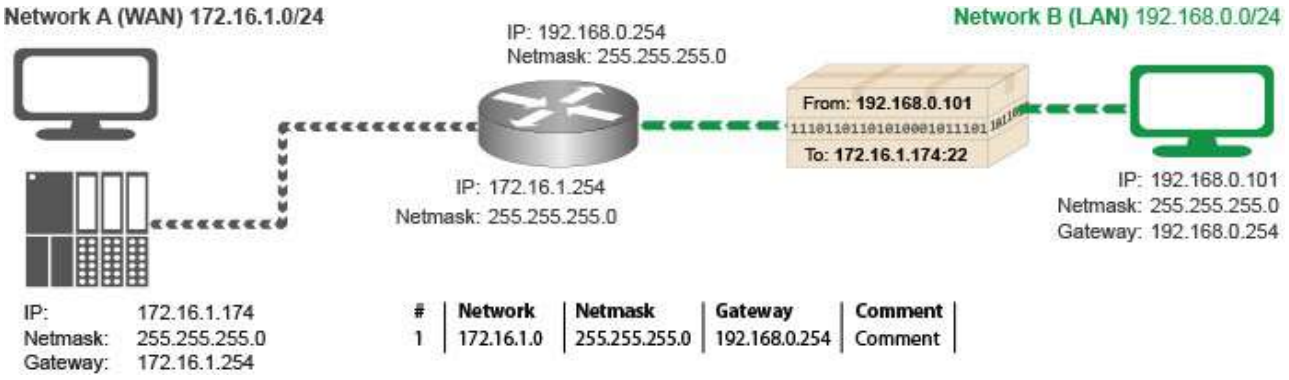
In the filter mode, "**Allow everything except filter rules**" (blacklisting) and the direction **WAN > LAN** is selected.

Rule #1 if active, would override the filter mode setting and block all traffic.

Rule #2 drops all data packets sent from a specific device/network adapter with MAC address 9C-EB-E8-84-3D-5E.

Regel #3 discards all data packets sent from the IP address 192.168.0.101
and addressed to a network participant with the IP 192.168.0.112
and this device is listening to the port no. 80
and the transmission protocol used is TCP.

6.2.10 Routes to networks on the WAN side (Gateway mode only)



The ***Anybus Defender Compact*** provides, via static routes, the access from the LAN network to any subscribers in the WAN network, including isolated network segments.

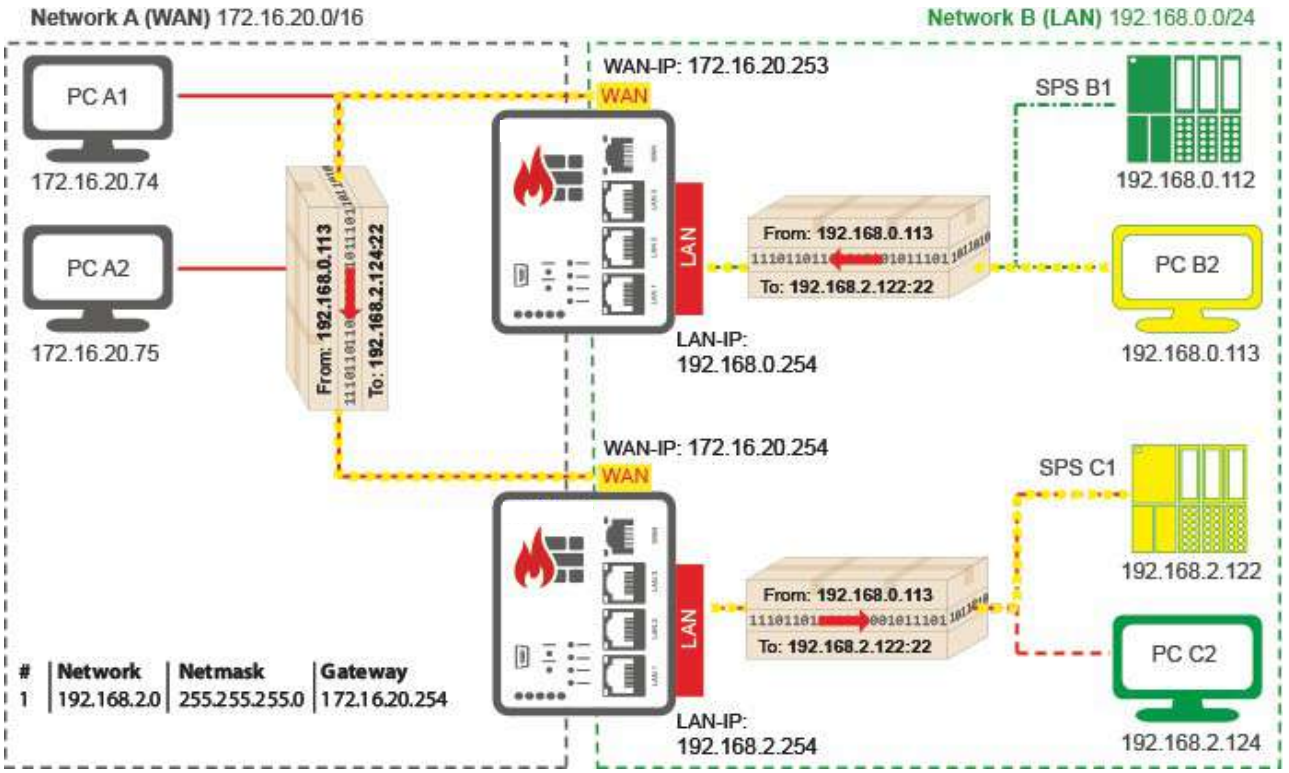
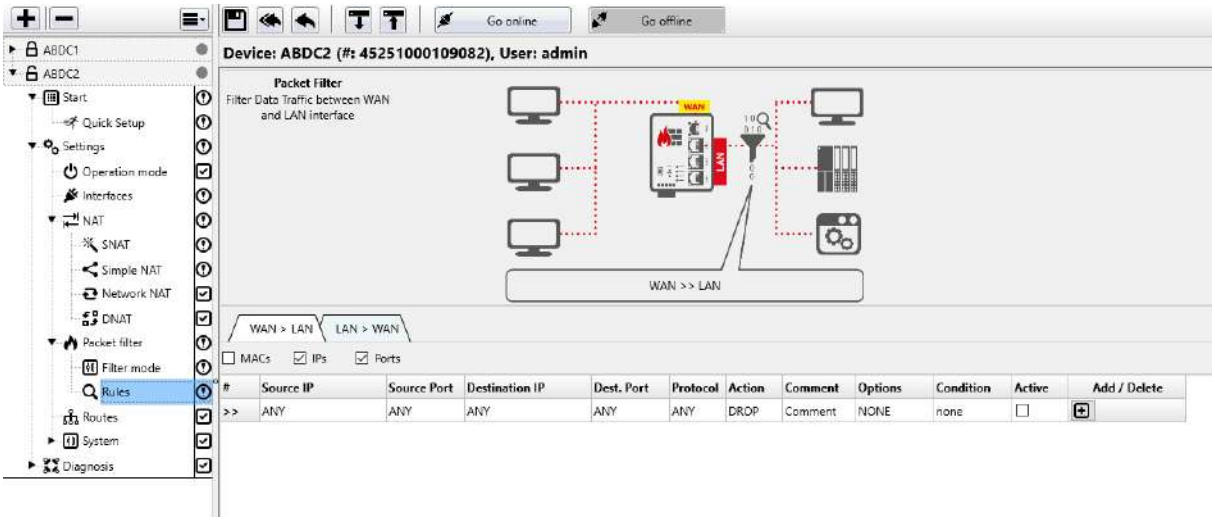


Image 24: Example: PC B2 from network A accesses PLC C1 via the routing. PLC C1 is a network participant in WAN subnet C.

Add route

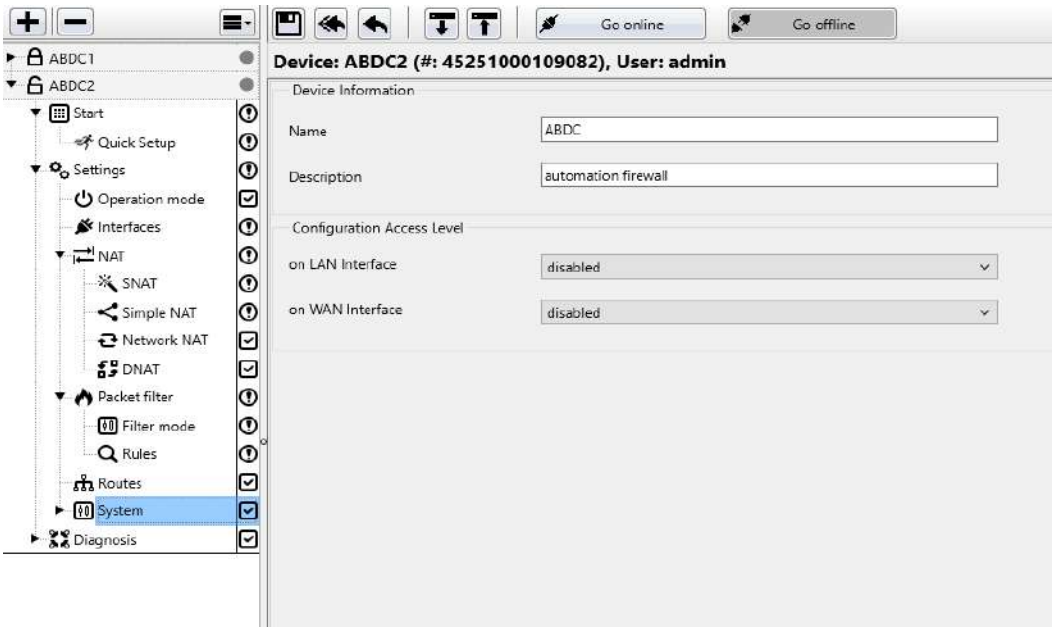


1. Enter the necessary information in the input fields.

2. By clicking on the "Add / Delete" button, add a route or delete an existing route.

Designation	Description
Network	Specification of the network to be reached.
Netmask	Specification of the subnet mask of the network to be reached.
Gateway	Specification of the corresponding gateway to the receiver network.
Comment	Here you can leave a comment on the defined route.
Active	By confirming the checkbox, the route will be activated.

6.2.11 System



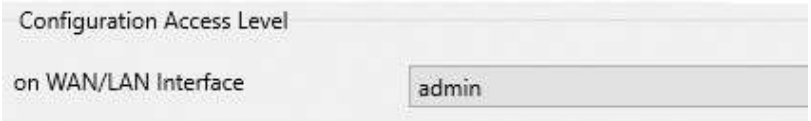
Device Information

Here you can change the name of the device and add a description.

Configuration Access Level

Depending on the selected operating mode (bridge or gateway mode), you can regulate the access authorization for the device configuration via the WAN and / or LAN interfaces here.

- If bridge mode is selected, the authorization to configure via the WAN and LAN interfaces can only be assigned to one user.



- In gateway mode, the configuration permission for the WAN and LAN interfaces can be split between two different users.

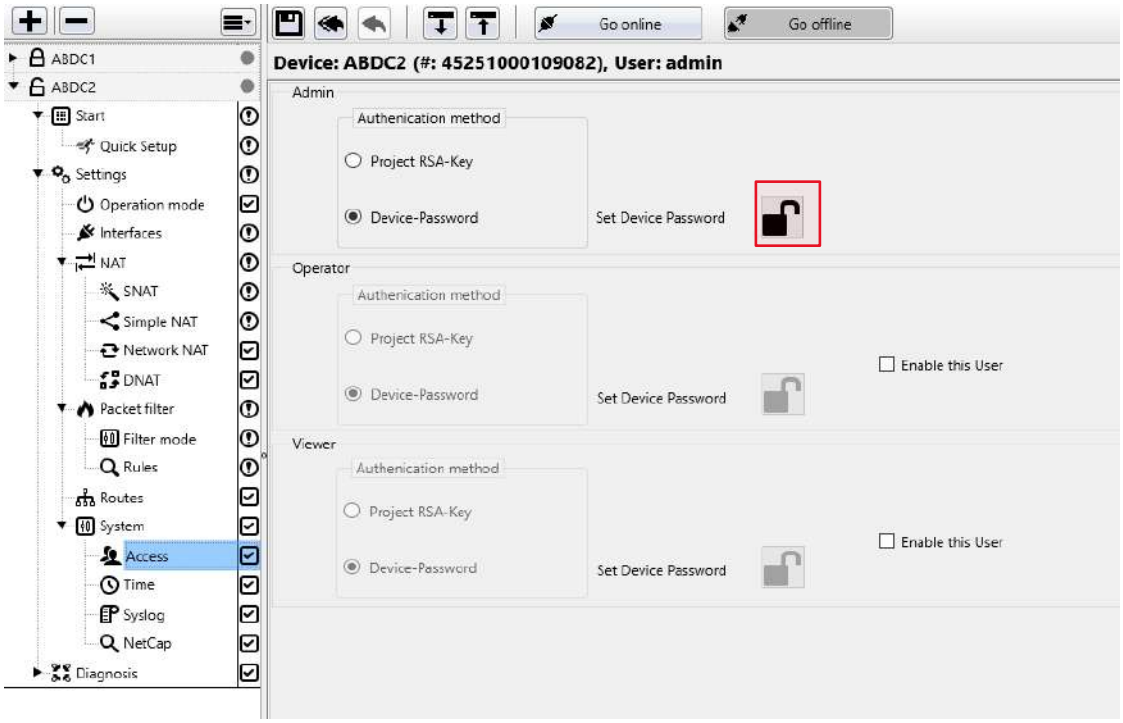
The following choices / users are available:

- **disabled**
  The device is configured exclusively via the USB interface.
- **admin, operator und viewer**
  The users named here receive the corresponding rights according to the table "Access rights for the individual user levels" after their login.
- **operator and viewer**
  The „Operator“ user has the possibility to add/delete/edit the “NAT”, “Packet filter” and “Routes” rules. Any other setting cannot be edited and can only be viewed.
- **viewer**
  The „Viewer“ user is only able to view the whole configuration but has no writing-access to any setting.

NOTICE

A detailed description of the access rights can be found in the chapter
"Access rights for the individual user levels"

6.2.11.1 Access - edit authentication method for individual users



Admin - Operator - Viewer

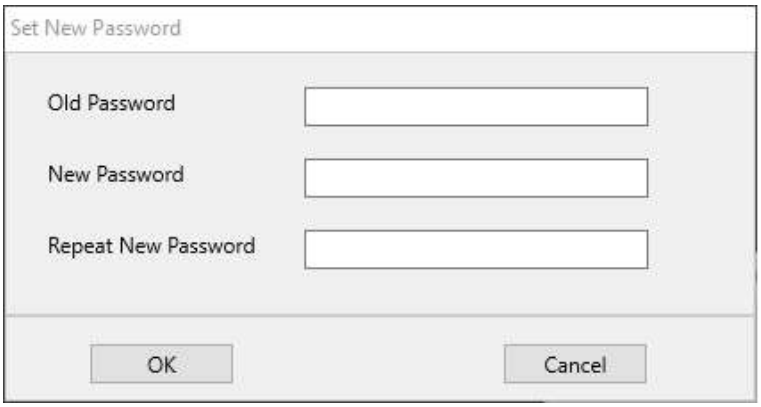
Here you can change the project password for this project.

Here you can

- Set a project password (project RSA key) for this project or change the existing password.
- Set / change the device password.
- Activate user (operator / viewer).

6.2.11.1.1 Set / change project password

1. In the main window, click the lock icon next to "Set Project Password".
2. Enter the old password* and a new password. And repeat the input of the new password.



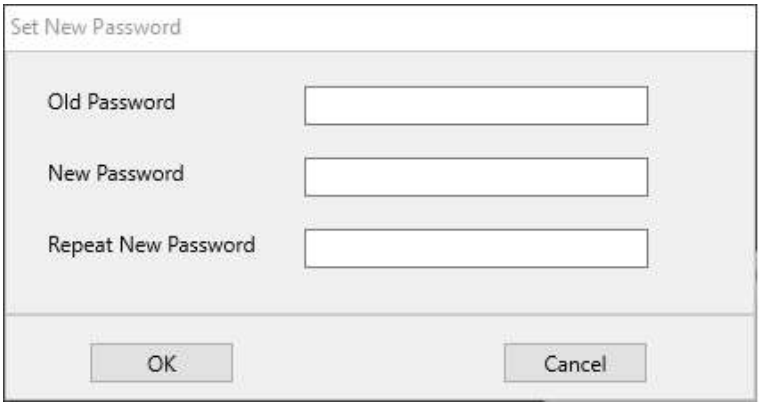
3. Click OK to save the change.

6.2.11.1.2 Set / change device password

NOTICE

To change the device password, the device (Anybus Defender Compact) must be connected to the configuration PC and ready for operation. And you have to "Go online" with the Anybus Defender Compact.

1. In the main window, click the lock icon next to "Set Device Password".
2. Enter the old password* and a new password. And repeat the input of the new password.



3. Click OK to save the change.

* Entering the old password is only necessary if the password is changed.

6.2.11.1.3 Activate user (operator / viewer)

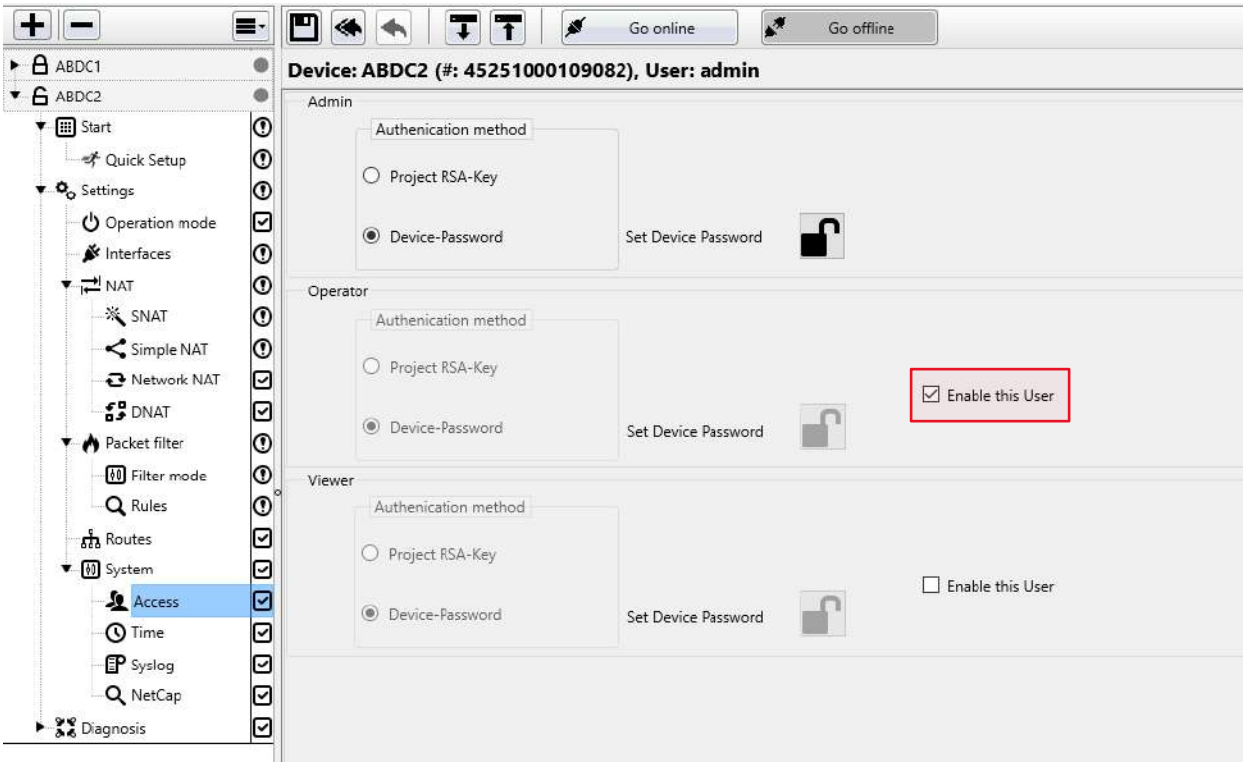
Operator - Viewer

For each project file, two additional users with corresponding rights can be assigned / activated.

- **Operator**
  The „Operator“ user has the possibility to add / delete / edit the “NAT”, “Packet filter” and “Routes” rules. Any other setting cannot be edited and can only be viewed.
- **Viewer**
  The „Viewer“ user is only able to view the whole configuration but has no writing-access to any setting.

NOTICE

A detailed description of the access rights can be found in the chapter
"Access rights for the individual user levels"



Activate the checkbox of the respective user you want to activate.

NOTICE

Activation / deactivation of users (operator, viewer) can only be carried out by the Admin user.

⇨ This User does not exist yet.
Would you like to create it?

Click on "**Yes**"

⇨ You enabled the user operator.
Please reset the password for this user when you are Online!

Click on "**Ok**"

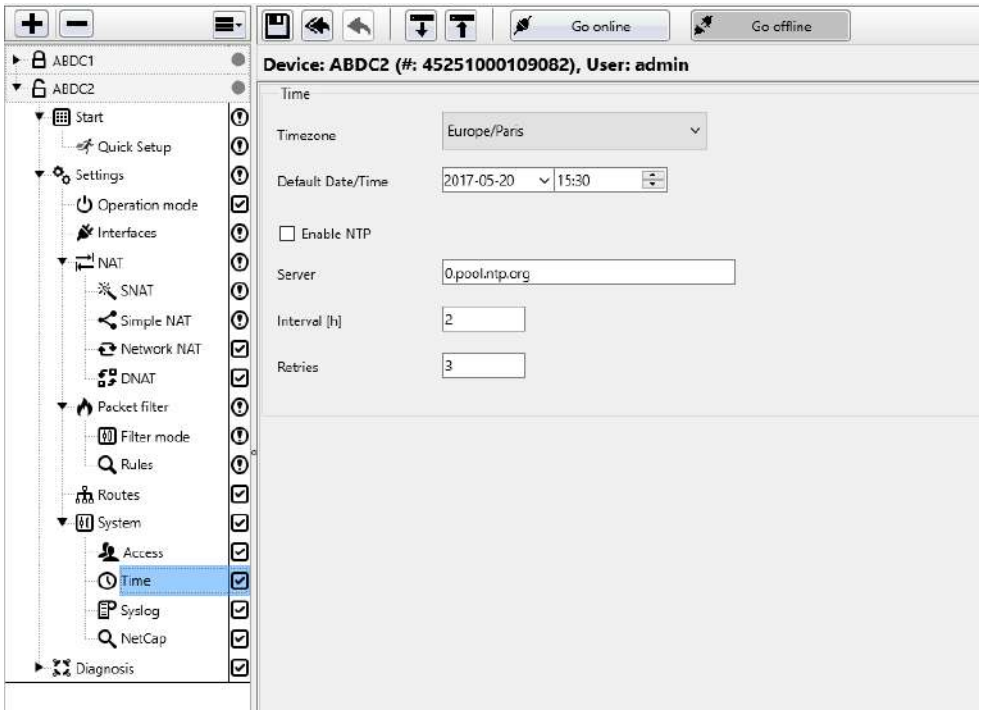
Deactivate user

Deactivate the checkbox of the user you want to delete.

NOTICE

If you deactivate an activated user again, this user is deleted. Set passwords are lost.

6.2.11.2 Time



This is where you select the time zone to be used in your device.

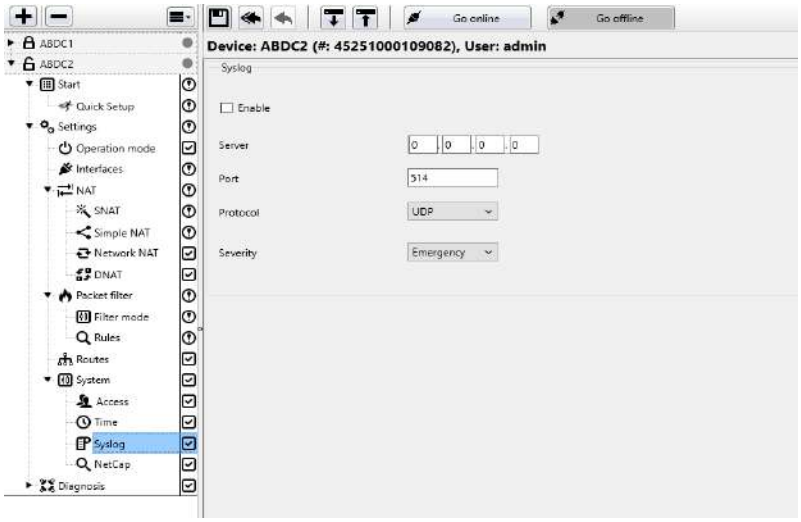
Additionally, you can also specify a default date and a time.

NTP

Optionally, you can also assign an NTP server for synchronizing the time.

1. To do so, click on the NTP checkbox.
2. Specify the server address, the interval in hours between synchronizations and the number of retries.

6.2.11.3. Syslog



Using an external log server system logging of Anybus Defender Compact can be outsourced. The Syslog server records all events with a date and time. The time must be set so that the Syslog server can log all configuration changes and user logins (see " Time").

1. Activate the Syslog server.
2. Enter the server address and the port to be used.
3. Then select the protocol and the desired notification level (severity).

Protocol

- UDP
- TCP

Notification level (severity)

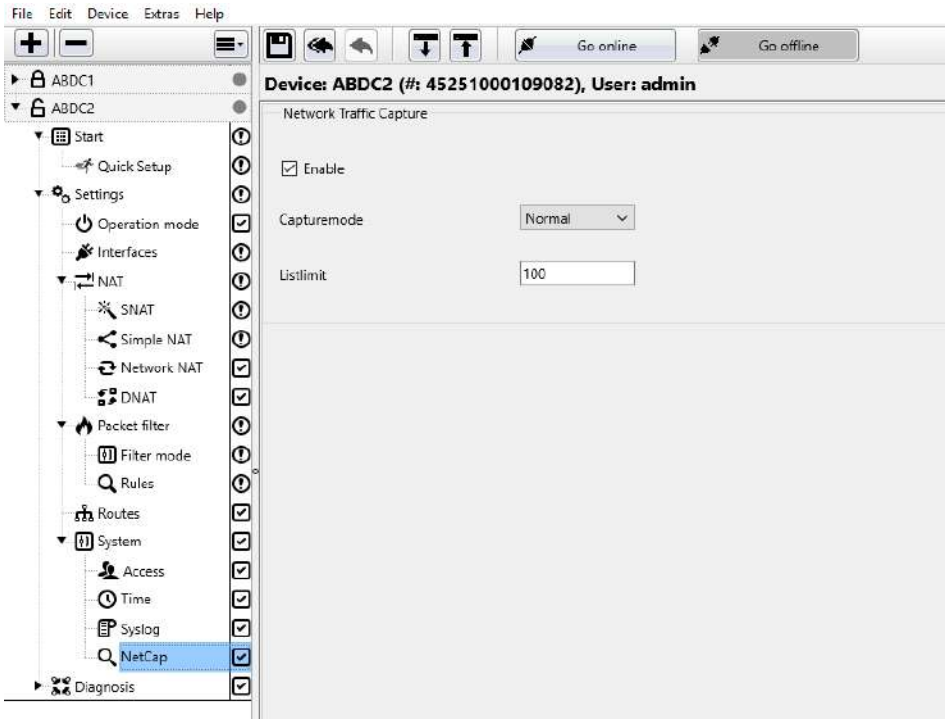
Here you can select a notification level to be logged.

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informational

NOTICE

Dependent on the selection, all higher priority levels are also automatically logged.

6.2.11.4 NetCap



Here you can specify if and how much network data should be recorded.

Active (enabled by default)

- Checkbox to activate / deactivate the function

Capture mode (under development)

- Normal
- Mode 1
- .....
- Mode 9

List limit (default = 100)

- Here you set the max. Number of detected network participants to be listed in the device view (mapping table).

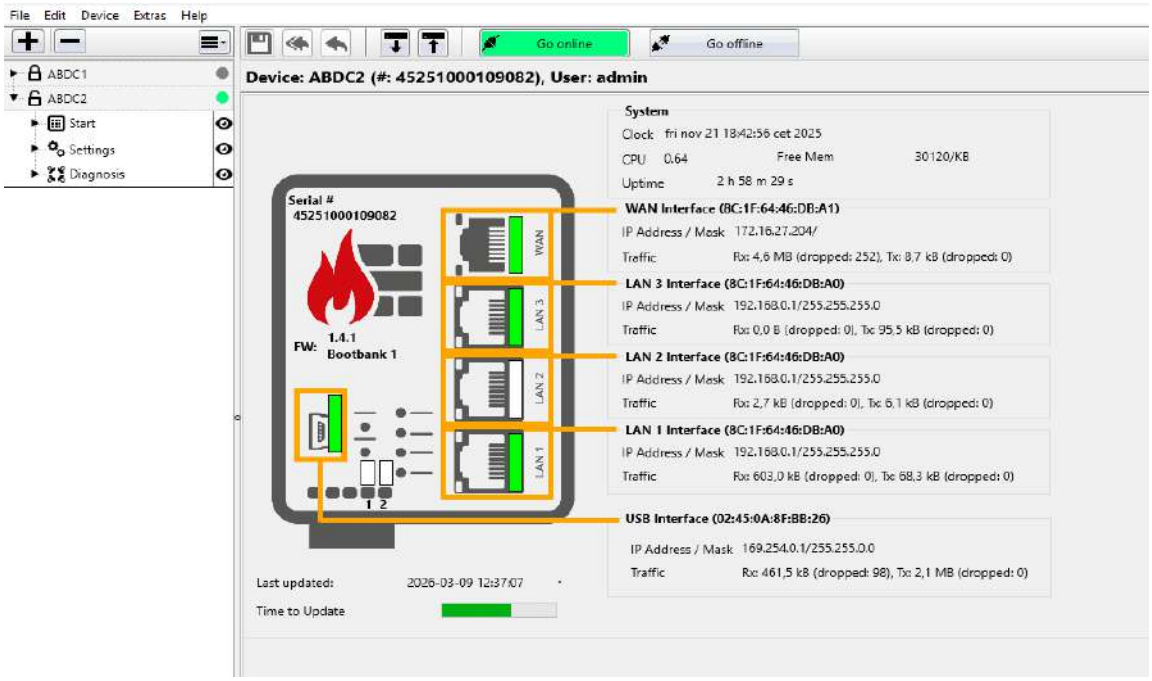
6.2.12 Data exchange

NOTICE

After all configuration work is completed, the data must be uploaded onto your device (see "**Error! Reference source not found.**").

6.3 Diagnosis

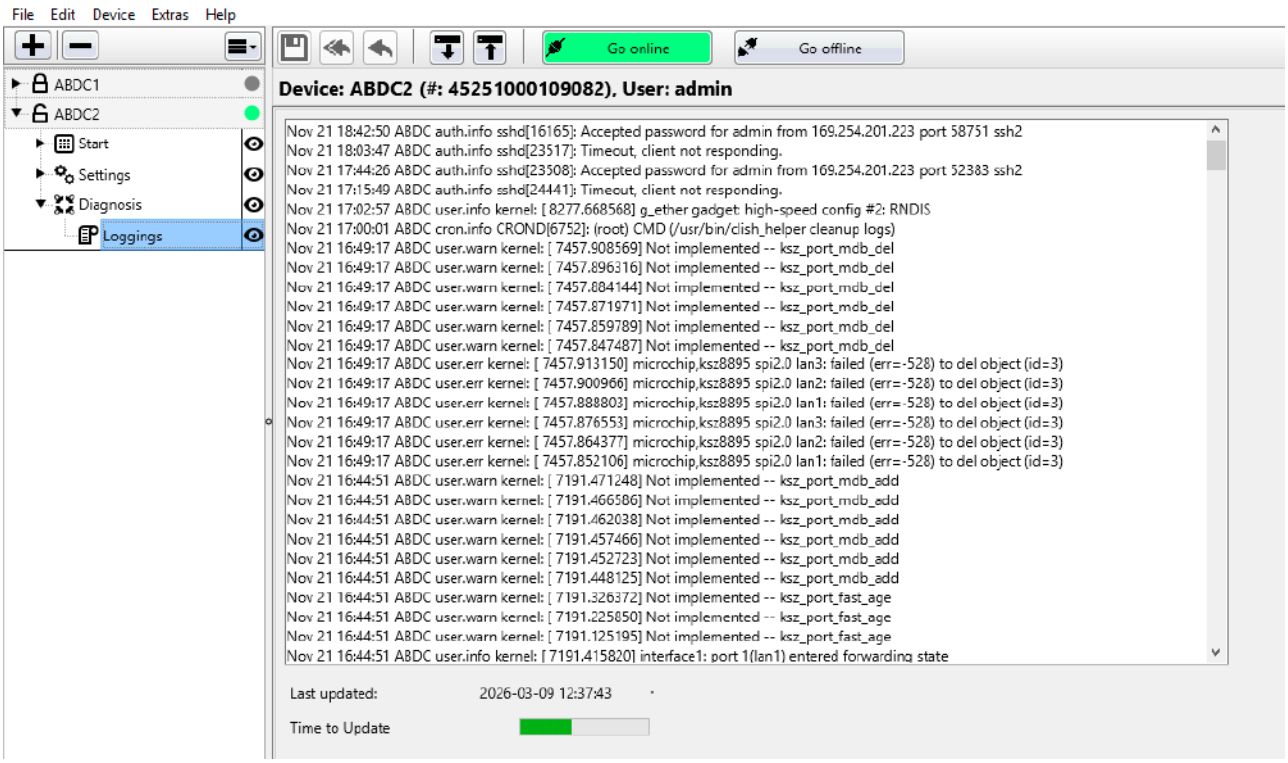
An overview of the device data is displayed here.



Information about:

- System
- WAN Interface
- LAN 1 ... LAN 3 Interface
- USB Interface
- Status of input 1 and input 2 (green = input is connected)

6.3.1 Loggings



All events that have occurred are logged and saved in Anybus Defender Compact.

The tabs “Loggings” and “Device” are opened to view the individual events.

NOTICE

The last 1000 entries are always displayed (rolling update system).

6.4 Reset to factory settings

NOTICE

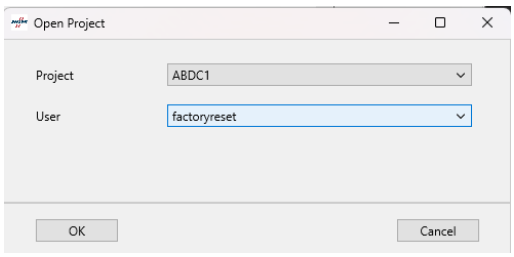
The ***Anybus Defender Compact*** is only reset to its factory settings by the user "factory reset" and only via the USB interface.

If you are logged in as the "admin" user, you can also carry out the action directly without having to log out and log in again with the user "factoryreset".

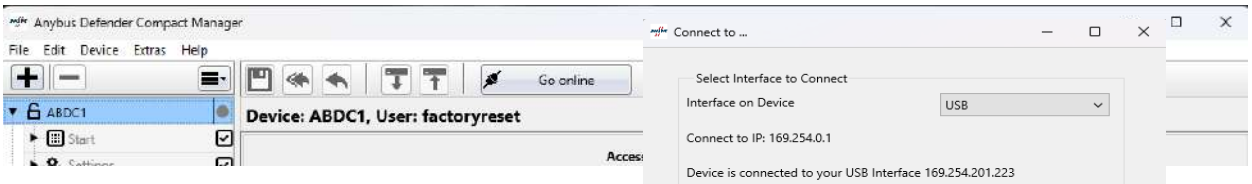
Furthermore, you always need the original device password for this action, even if the device is already paired or the device password has been changed.

1. Select the project file that is paired with the device (***Anybus Defender Compact***) that should be reset to its factory set- tings.

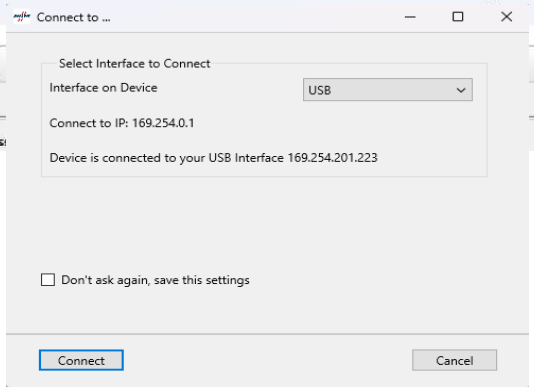
2. Select user "admin" or "factoryreset" and confirm with "OK".



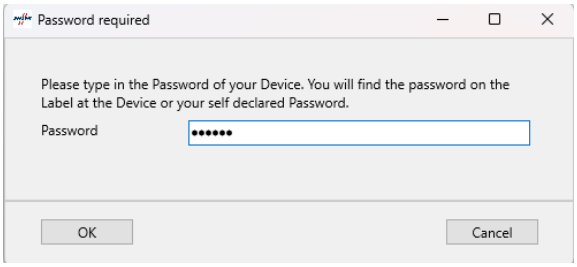
3. Click on the button “Go Online" in the main menu.



4. Make sure that "USB" is selected for the interface to be connected and click on "Connect".

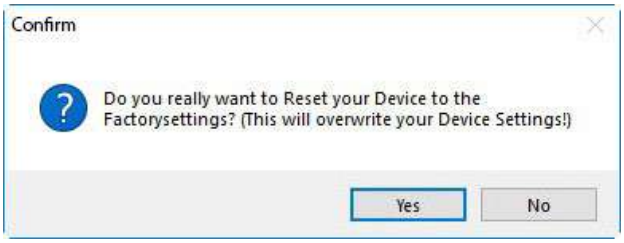


5. Now enter the device-specific password (see label on the device) and confirm with "OK" to establish the connection.
   The device password is always needed for this action, even if the device is already paired.

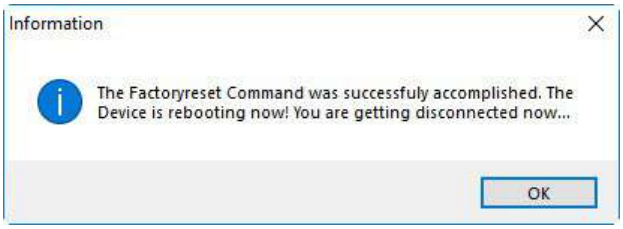


6. Select the function "Factory reset" via the "Device" menu.

7. Confirm the query about overwriting the device settings by clicking “Yes” to reset to the factory settings.

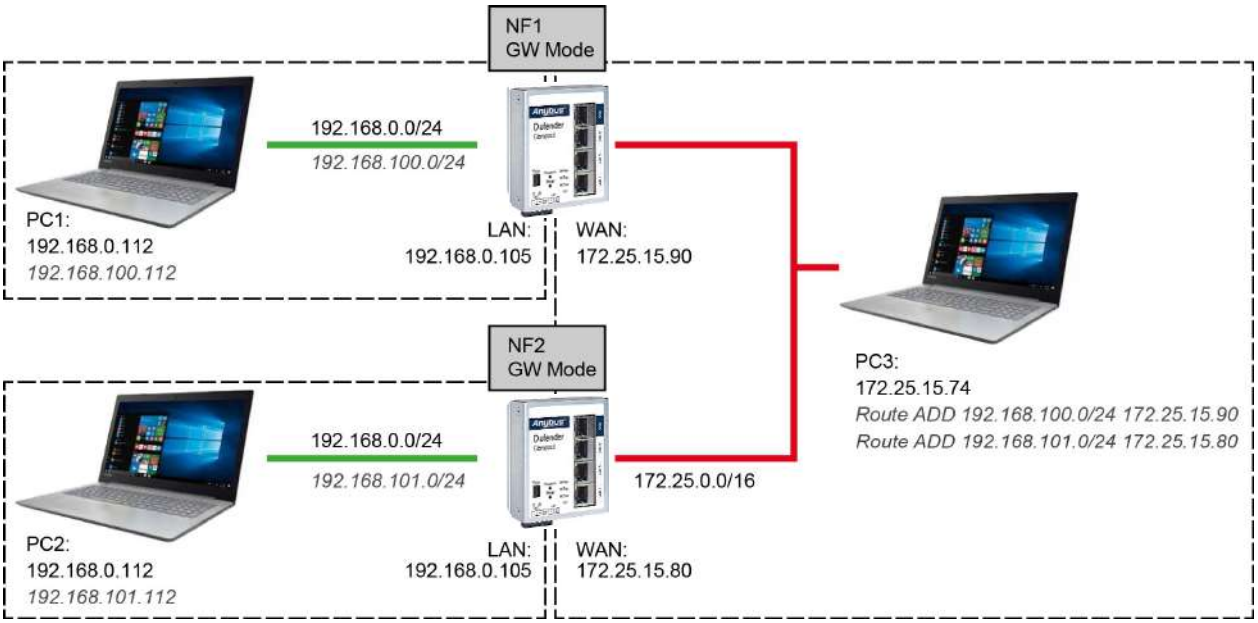


8. Confirm the information window with "OK" to complete the action.



7 Application examples

7.1 Network segmenting of the same network addresses



Devices

- PC1: IP: 192.168.0.112/24, Gateway: 192.168.0.105
- PC2: IP: 192.168.0.112/24, Gateway: 192.168.0.105
- PC3: IP: 172.25.15.74/16, Gateway: 172.25.25.253

Anybus Defender Compact

- NF1
  Network NAT: 192.168.100.0/24
  Static Routes: Network 192.168.101.0/24 via Gateway 172.25.15.80
- NF2
  Network NAT: 192.168.101.0/24
  Static Routes: Network 192.168.100.0/24 via Gateway 172.25.15.90

NOTICE

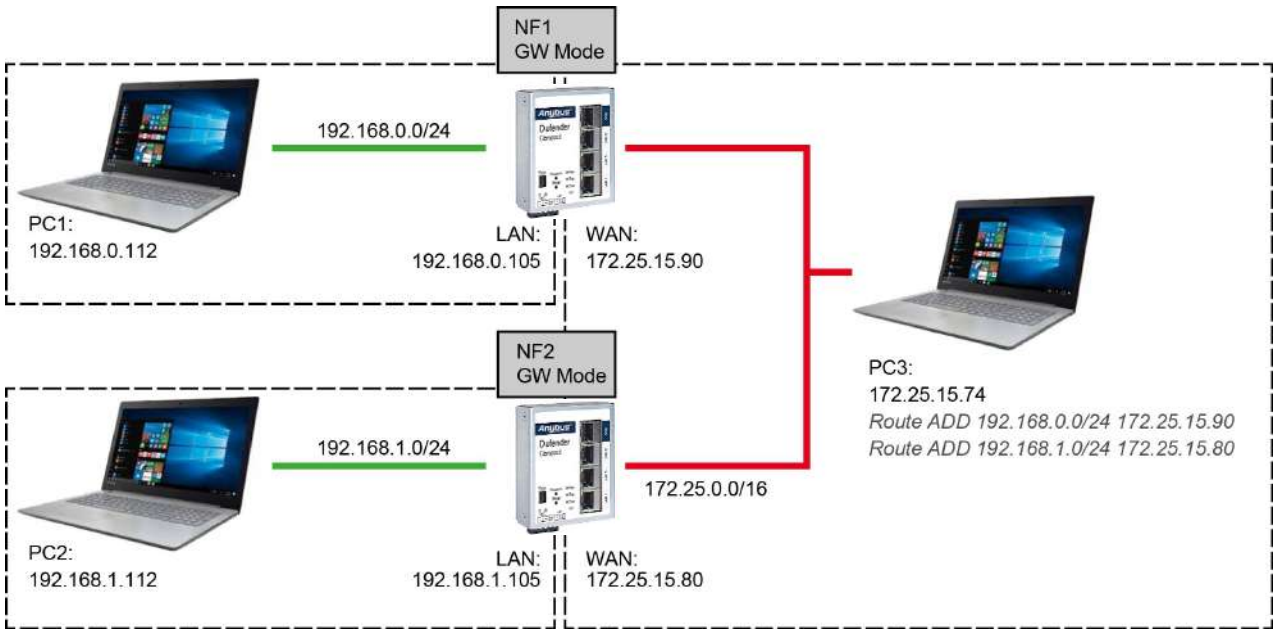
In addition, communication to the individual clients must also be approved in the packet filter!

E.g. to PING from PC1: 192.168.0.112 (192.168.100.112) to PC2: 192.168.0.112 (192.168.101.112), the ICMP protocol must be enabled in the LAN > WAN packet filter of NF1 and also in the WAN > LAN packet filter of NF2.

Consequently, it must first go “out” from NF1 before it can be incoming at NF2.

A gateway must be entered for both PC1 and PC2, as they would like to route into other networks. In principle the SNAT “WAN to LAN” function can also be enabled here, if for example only direction PC1 to PC2 is required. Consequently no gateway need be entered on PC2. Then in NF2, SNAT “WAN to LAN” must be activated.

7.2 Network segmenting of dissimilar network addresses



Devices

- PC1: IP: 192.168.0.112/24, Gateway: 192.168.0.105
- PC2: IP: 192.168.1.112/24, Gateway: 192.168.1.105
- PC3: IP: 172.25.15.74/16, Gateway: 172.25.25.253

Anybus Defender Compact

- NF1
  Static Routes: Network 192.168.1.0/24 via Gateway 172.25.15.80
- NF2
  Static Routes: Network 192.168.0.0/24 via Gateway 172.25.15.90

NOTICE

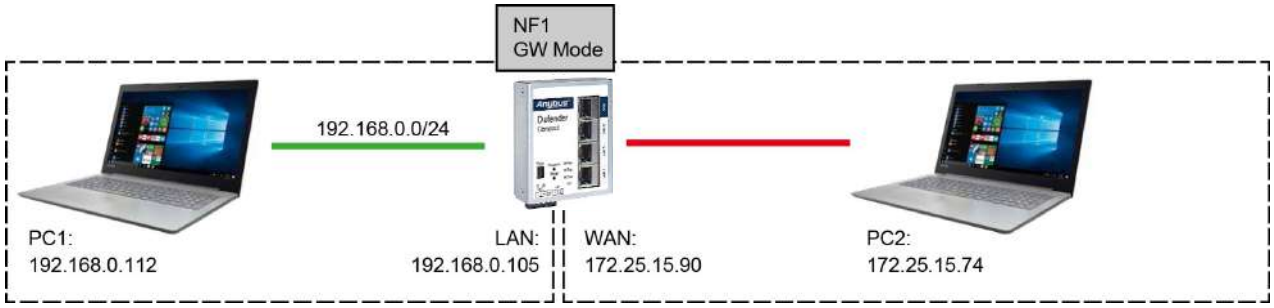
In addition, communication to the individual clients must also be approved in the packet filter!

E.g. to PING from PC1: 192.168.0.112 to PC2: 192.168.112, the ICMP protocol must be enabled in the LAN > WAN packet filter of NF1 and also in the WAN > LAN packet filter of NF2.

Consequently, it must first go “out” from NF1 before it can be incoming at NF2.

A gateway must be entered for both PC1 and PC2, as they would like to route into other networks. In principle the SNAT “WAN to LAN” function can also be enabled here, if for example only direction PC1 to PC2 is required. Consequently no gateway need be entered on PC2. Then in NF2, SNAT “WAN to LAN” must be activated.

7.3 Use of SNAT



Example 1: PC1 has gateway entry and PC2 does not

Devices

- PC1: IP: 192.168.0.112/24, Gateway: 192.168.0.105
- PC2: IP: 172.25.15.74/16, Gateway: -----

Anybus Defender Compact

- NF1
  SNAT WAN to LAN: disabled
  SNAT LAN to WAN: active

Example 2: PC2 has gateway entry and PC1 does not

Devices

- PC1: IP: 192.168.0.112/24, Gateway: -----
- PC2: IP: 172.25.15.74/16, Gateway: 172.25.15.90

Anybus Defender Compact

- NF1
  SNAT WAN to LAN: active
  SNAT LAN to WAN: disabled

SNAT WAN to LAN

Replaces the sender address of each IP packet that goes from WAN to LAN with the LAN IP. In the above case a PING goes from 172.25.15.74 to 192.168.0.112. However, PC1 does not see the sender address 172.25.15.74, rather 192.168.0.105. As the sender address is thus in a network, it is not necessary to use a gateway. I.e. PC1 sends the answer to 192.168.0.105. Because of the SNAT, the NF1 has noted the IP traffic and converts the response back to the original IP addresses.

SNAT LAN to WAN

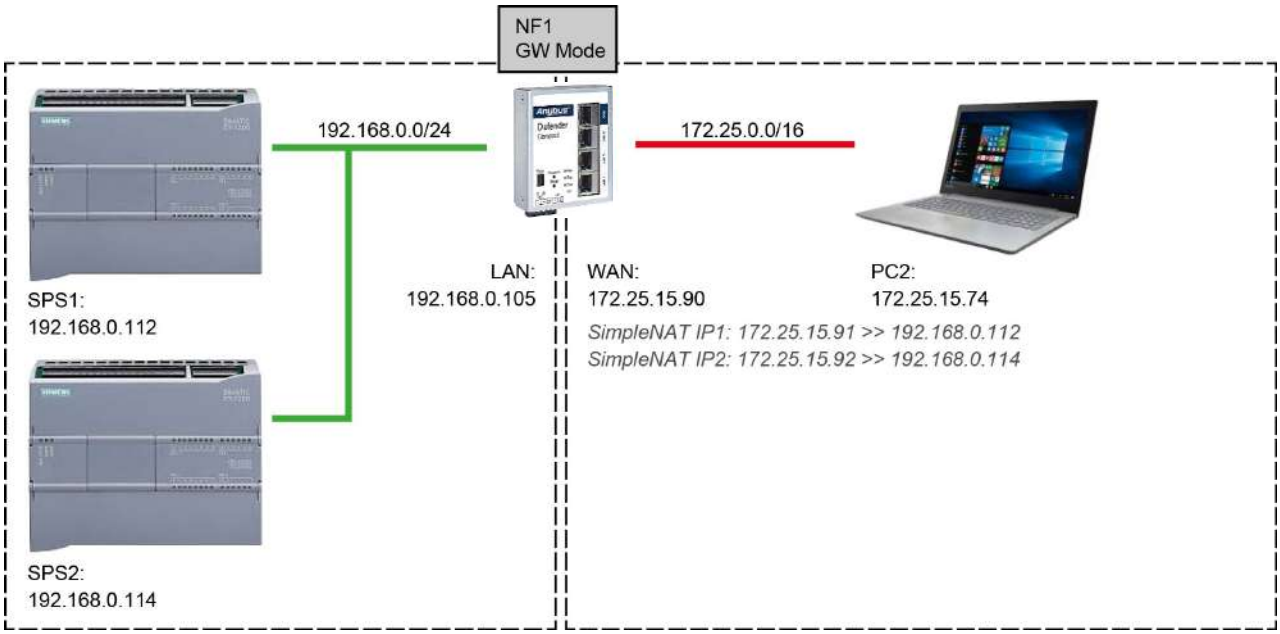
The same as WAN to LAN, only in the opposite direction.

NOTICE

In addition, communication to the individual clients must also be approved in the packet filter!

E.g. to PING from PC1: 192.168.0.112 to PC2: 172.25.15.74, the ICMP protocol must be enabled in the LAN > WAN packet filter of NF1.

7.4 Access to multiple devices behind the firewall



Example:

Both PLCs should be accessible via PC2 via their own IP addresses. Port forwarding (DNAT) is not possible here because especially with a Siemens PLC, the port assignment cannot be made in PC2.

Devices

- SPS1: IP: 192.168.0.112/24, Gateway: -----
- PLC2: IP: 192.168.0.114/24, Gateway: -----
- PC2: IP: 172.25.15.74/16, Gateway: -----

Anybus Defender Compact (NF1)

- SNAT WAN to LAN: active
- SNAT LAN to WAN: disabled
- Simple NAT: 172.25.15.91 >> 192.168.0.112
- Simple NAT: 172.25.15.92 >> 192.168.0.114
- Packet Filter: ANY >> 192.168.0.112, Port 102, ACCEPT
- Packet Filter: ANY >> 192.168.0.114, Port 102, ACCEPT

SNAT WAN to LAN

- Replaces the sender address of each IP packet that goes from WAN to LAN with the LAN IP address.

Simple NAT

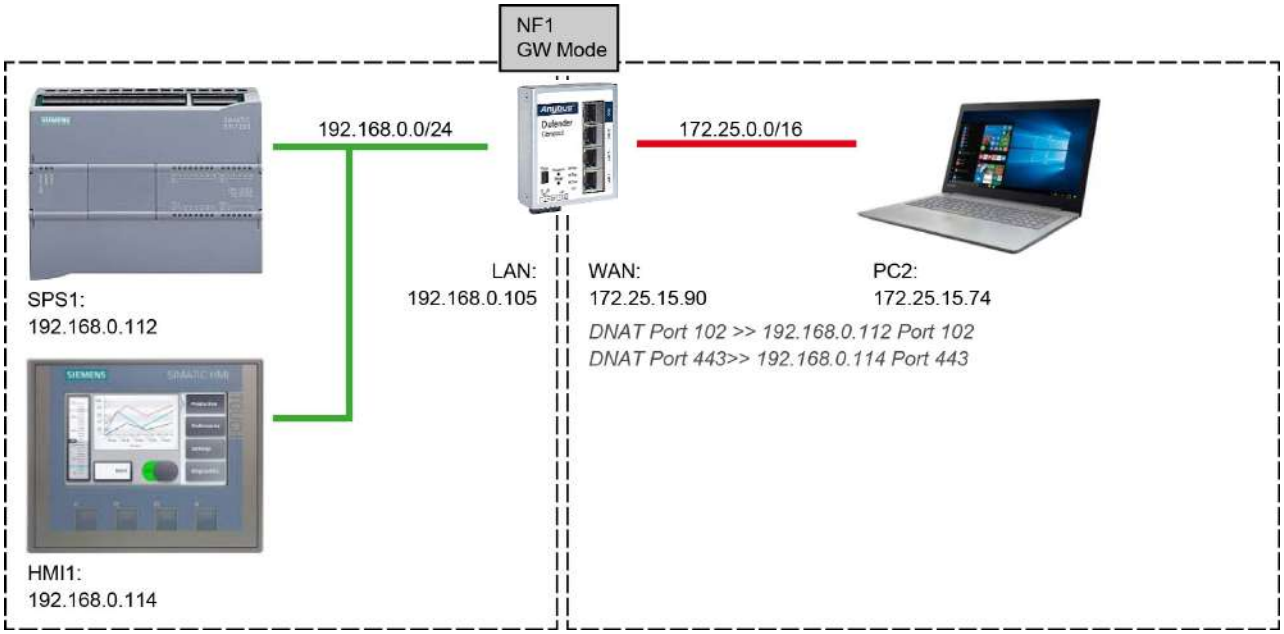
- Here the destination address is rerouted to another destination address.
  Specifically for the above case, each packet that has the destination address 172.25.15.91 is rerouted or changed to the destination address 192.168.0.112. The same occurs for 172.25.15.92 to 192.168.0.114.
  In this way, the PLCs can be directly accessed via a WAN IP address in the WAN network.

NOTICE

In addition, communication to the individual clients must also be approved in the packet filter!

E.g. to PING from PC1: 192.168.0.112 to PC2: 172.25.15.74, the ICMP protocol must be enabled in the LAN > WAN packet filter of NF1.

7.5 Access to individual services behind the firewall



Example:

SPS1 (Programmed port 102) and HMI1 (webserver port 443) should be accessible via PC2.

Devices

- SPS1: IP: 192.168.0.112/24, Gateway: -----
- HMI1: IP: 192.168.0.114/24, Gateway: -----
- PC2: IP: 172.25.15.74/16, Gateway: -----

Anybus Defender Compact (NF1)

- SNAT WAN to LAN: active
- SNAT LAN to WAN: disabled
- DNAT: TCP 102 >> 192.168.0.112 TCP 102
- DNAT: TCP 443 >> 192.168.0.114 TCP 443
-

SNAT WAN to LAN

- Replaces the sender address of each IP packet that goes from WAN to LAN with the LAN IP address.

DNAT

- Here the destination address and the destination port are rerouted to another destination address and destination port.
  Specifically for the above case, each packet that has the destination 172.25.15.90, TCP 102 is rerouted to the destination 192.168.0.112, TCP102. The same occurs for 172.25.15.90, TCP 443 to 192.168.0.114, TCP 443. This ensures that the PLC and the HMI are each accessibly via their own port of the firewall WAN IP.
  Here, the advantage in comparison with other systems is that port 443 is not used as a web service in the firewall and thus is available if such routing is required.

Packet Filter

- No setting is required here as all DNAT entries bypass the packet filter, as they already contain all necessary filter functions. In principle, however, a DROP can be entered, for example, for defined MAC ad- dresses.

NOTICE

In addition, communication to the individual clients must also be approved in the packet filter!

E.g. to PING from PC1: 192.168.0.112 to PC2: 172.25.15.74, the ICMP protocol must be enabled in the LAN > WAN packet filter of NF1.