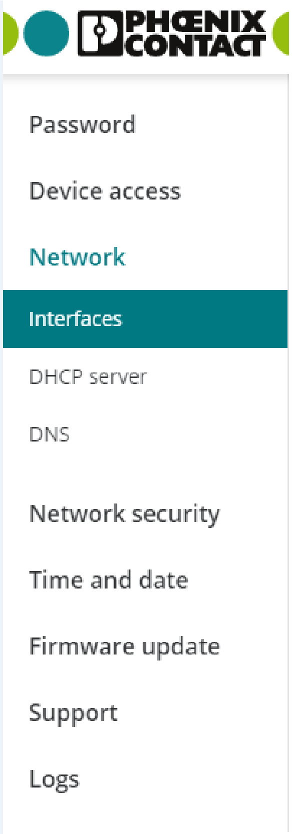


FL MGUARD 1000
Web-based management
mGuardNT 1.3.x

User manual

UM EN MGUARD NT

INSPIRING INNOVATIONS

User manual

FL MGUARD 1000 – Web-based management – mGuardNT 1.3.x

UM EN MGUARD NT, Revision 03 2020-07-09

This user manual is valid for:

Designation	Version	Order No.
FL MGUARD 1102		1153079
FL MGUARD 1105		1153078

For further information see *mGuardNT 1.3.x firmware Release Notes*.

108420_en_03

PHOENIX CONTACT GmbH & Co. KG • Flachsmarktstraße 8 • 32825 Blomberg • Germany
phoenixcontact.com

Table of contents

1 For your safety

Read this user manual carefully and keep it for future reference.

1.1 Identification of warning notes

ⓘ This symbol together with the **NOTE** signal word warns the reader of actions that might cause property damage or a malfunction.

ℹ Here you will find additional information or detailed sources of information.

1.2 Qualification of users

The use of products described in this user manual is oriented exclusively to:

– Electrically skilled persons or persons instructed by them. The users must be familiar with the relevant safety concepts of automation technology as well as applicable standards and other regulations.

– Qualified application programmers and software engineers. The users must be familiar with the relevant safety concepts of automation technology as well as applicable standards and other regulations.

1.3 Intended use

– The devices are security routers for industrial use, with integrated stateful packet inspection firewall. They are suitable for distributed protection of production cells or individual machines against manipulation.

– The devices are designed for use in industrial environments.

– The devices are intended for installation in a control cabinet.

1.4 Modifications to the product

Modifications to hardware and firmware of the device are not permitted.

– Incorrect operation or modifications to the device can endanger your safety or damage the device. Do not repair the device yourself. If the device is defective, please contact Phoenix Contact.

1.5 IT security

For Phoenix Contact devices that can be integrated in an industrial network via Ethernet, organizational and technical measures must be taken in order to protect components, networks, and systems against unauthorized access and to ensure data integrity.

Phoenix Contact recommends that the following measures should be considered at the very least.

Perform threat analyses on a regular basis.

- In order to determine whether the measures you have taken still provide adequate protection for your components, networks, and systems, a regular threat analysis is mandatory.

When planning systems, consider defense-in-depth strategies.

- Defense-in-depth strategies encompass several coordinated measures that include operators, integrators, and manufacturers.

Make sure that your software/firmware is always up to date.

- Stay informed about updates for the products used. If possible, run provided updates immediately to ensure maximum security for your product.

Deactivate unused communication channels.

- Check whether unused communication channels on the components you are using are open (e.g., SSH, SNMP, FTP, BootP, DHCP, etc.). If possible, deactivate these channels.

Restrict access rights to the device.

- Restrict access rights for components, networks, and systems to those individuals for whom authorization is strictly necessary.

Use strong passwords.

- Change default passwords during initial startup.
- If possible, use randomly generated passwords (password manager).
- Use strong passwords, e.g., at least ten characters long containing a mix of upper and lower case letters, numbers, and special characters.

Use a firewall.

- Set up a firewall in order to protect your networks and the components and systems integrated in them against unauthorized network access.
- Use a firewall to segment a network or to isolate certain components (e.g., controllers).

Do not make components and systems available in public networks.

- Avoid integrating your components and systems into public networks.
- If you have to access your components and systems via a public network, use a VPN (*Virtual Private Network*).

1.6 About this user manual

The following elements are used in this user manual:

Bold	Designations of operating elements, variable names or other accentuations
Italic	– Product, module or component designations (e.g., *tftpd64.exe*, *Config API*) – Foreign designations or proper names – Other accentuations
–	Unnumbered list
1.	Numbered list
•	Operating instructions
⇒	Result of an operation

1.7 Support

For additional information on the device as well as release notes, user assistance and software updates, visit: phoenixcontact.net/products.

In the event of problems with your device or with operating your device, please contact your supplier.

To get help quickly in the event of an error, make a snapshot of the device configuration immediately when a device error occurs, if possible. You can then provide the snapshot to the support team.

2 mGuardNT basics

2.1 Device properties and scope of functions

Table 2-1 Device properties and scope of functions

Device properties	FL MGUARD	
	1102	1105
HARDWARE		
2 net zones (network interfaces)	x	x
Ethernet via RJ45 connections (transmission speed: 10/100/1000 Mbps)	2	5
4-port Unmanaged Switch (RJ45) (*bridge mode*)	-	x
Service inputs and outputs (IOs)	x	x
NETWORK		
Stealth mode	x	x
Router mode	x	x
Packet forwarding (router mode)		
Security router	x	x
IP masquerading (NAT)	x	x
Port forwarding	x	x
1:1 NAT	x	x
Additional static routes	x	x
Network services (client/server)		
DHCP	x	x
DNS	x	x
NTP	x	x
HTTPS (WBM/*Config API*)	x	x
FIREWALL		
Stateful packet inspection firewall	x	x
Firewall (for continuous data traffic)	x	x
Device access (for incoming data traffic)	x	x
Integrity check of data packets to increase network security	x	x
Easy Protect Mode Automatic protection of connected network clients without configuration effort directly after connection of the device.	x	x
Firewall Assistant Analysis of data traffic for the automatic creation of firewall rules.	x	x

Table 2-1 Device properties and scope of functions

Device properties	**FL MGUARD**	
	1102	**1105**
Firewall test mode Analysis of data traffic for the automatic extension of existing firewall rules.	x	x
MANAGEMENT		
Administration via web-based management (WBM)	x	x
Administration via RESTful Configuration API (*Config API*)	x	x
Firmware update via WBM and *Config API*	x	x
Smart mode The access to certain management functions is implemented via the Mode button on the device and without access to a management interface.	x	x
Support tools		
TCP Dump (packet data analysis)	x	x
Ping (network analysis)	x	x
Log viewer (evaluation of log entries)	x	x
Support snapshot (status and error analysis)	x	x

2.2 Network

As a router or gateway, the device uses its network interfaces to connect subnets or net zones. For each net zone, an own IP address is configured via which the device is reachable in the network (see Section 6.1, “Network >> Interfaces”).

2.3 Firewall

Strictly speaking, the firewall of the device is a packet filter through which data packets routed through the device are analyzed and then forwarded or blocked according to the configured firewall rules (see Section 7, “Menu: Network security”).

Stateful packet inspection firewall

The mGuardNT packet filter functions as a s*tateful packet inspection* firewall. This means that response packets automatically pass through the firewall if they can be clearly assigned to a related request that was already accepted. For this reason, firewall rules are never applied to response packets.

Firewall functions

The firewall can be used and configured in different ways.

Table 2-2 Options for using the mGuard firewall

No configuration required	
Easy Protect Mode (see Section 2.3.1)	Network clients are protected against external access directly after connection of the device without the need to create firewall rules.
Configuration via web-based management (WBM) or Config API required	
Firewall (packet filter) (see Section 7.1)	Firewall rules are created and extended manually. The rules are entered and configured in the *Firewall table* of the device.
Firewall Assistant (see Section 7.2)	The *Firewall Assistant* analyzes and acquires the data traffic routed through the device for any period of time (**net zone 1 ⟵⟶ net zone 2**). The acquired packet data is used to deduce firewall rules that are automatically entered in the *Firewall table* when the *Firewall Assistant* has been stopped.
Firewall test mode (see Section 7.1, Firewall test mode)	Data traffic unintentionally rejected by the firewall can be easily identified and permitted through the automated creation of corresponding firewall rules. An alarm informs the user about the event (data traffic not acquired through an existing firewall rule).

2.3.1 Easy Protect Mode

If the device is started in *Easy Protect Mode*, it **automatically** protects all devices connected to net zone 2 (XF2–XF5) against external access (e.g., individual machines or production cells that are connected via a switch).

For additional information refer to the *“FL MGUARD 1000 – Installation and startup*” user manual, available at phoenixcontact.net/product/1153078.

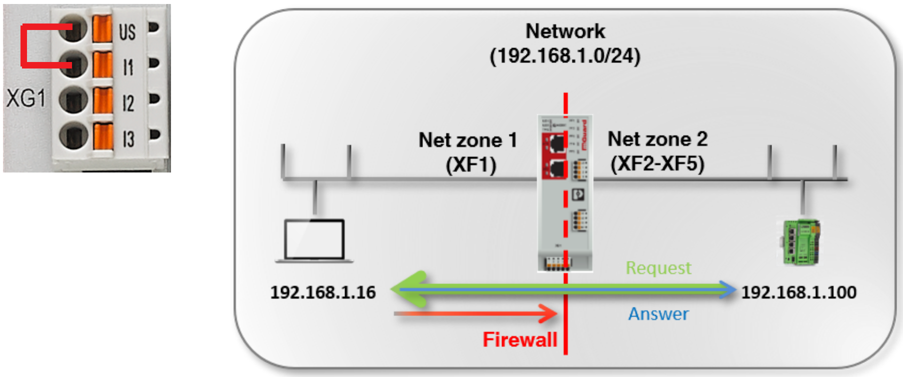


Figure 2-1 Activated *Easy Protect Mode* (via cable bridge)

The *Easy Protect Mode* is activated via a cable bridge (see Figure 2-1).

The device is integrated into the existing network via its net zones 1 and 2 or XF1 and (XF2–XF5). The existing network configuration of the connected devices does not have to be changed.

Device configuration is not required and not possible due to the missing access option via the web-based management (HTTPS).

3 Using the web-based management

3.1 Establishing a network connection to the device

Establish a connection between the configuration computer and a network interface of the device.

Default setting (network interface: XF2)

- IP address: 192.168.1.1
- Subnet mask: 24 (255.255.255.0)

For additional information refer to the "*FL MGUARD 1000 – Installation and startup*" user manual, available at phoenixcontact.net/product/1153078.

3.2 User login

A competing login of the *admin* user from several instances is not recommended and might result in loss of data.

Enter, for example, the following web address in a web browser to start the WBM:

https://192.168.1.1 (default setting: XF2)

⇒ The login page opens.

The following users can log in to the device (default setting):

- User name: *admin*
- Password: *private*

Immediately upon initial startup of the device, change the default password (see "Menu: Password" on page 23).

For additional information, refer to the "*FL MGUARD 1000 – Installation and startup"* user manual, available at phoenixcontact.net/product/1153078.

After logging in successfully, the following start page appears.

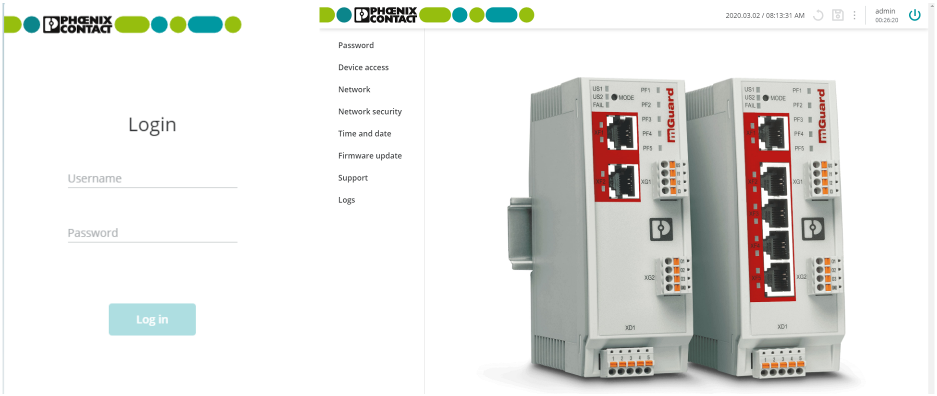


Figure 3-1 Web-based management: login page and start page

3.3 User logout

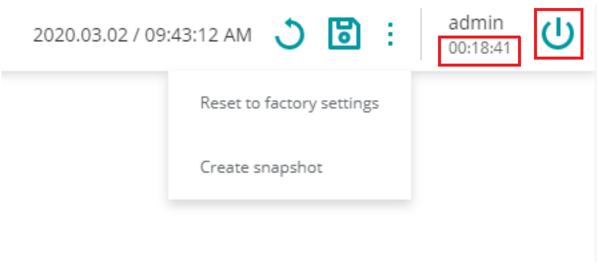


Figure 3-2 User logout

To log out the current user from the device, proceed as follows:

- Click on the ⏻ icon.

⇒ The user is logged out.

⇒ All information regarding the current session is deleted.

⇒ The user is forwarded to the login page.

Automatic logout

The user is automatically logged out if the following applies:

– The session has elapsed (*session timeout*).

– The device is restarted.

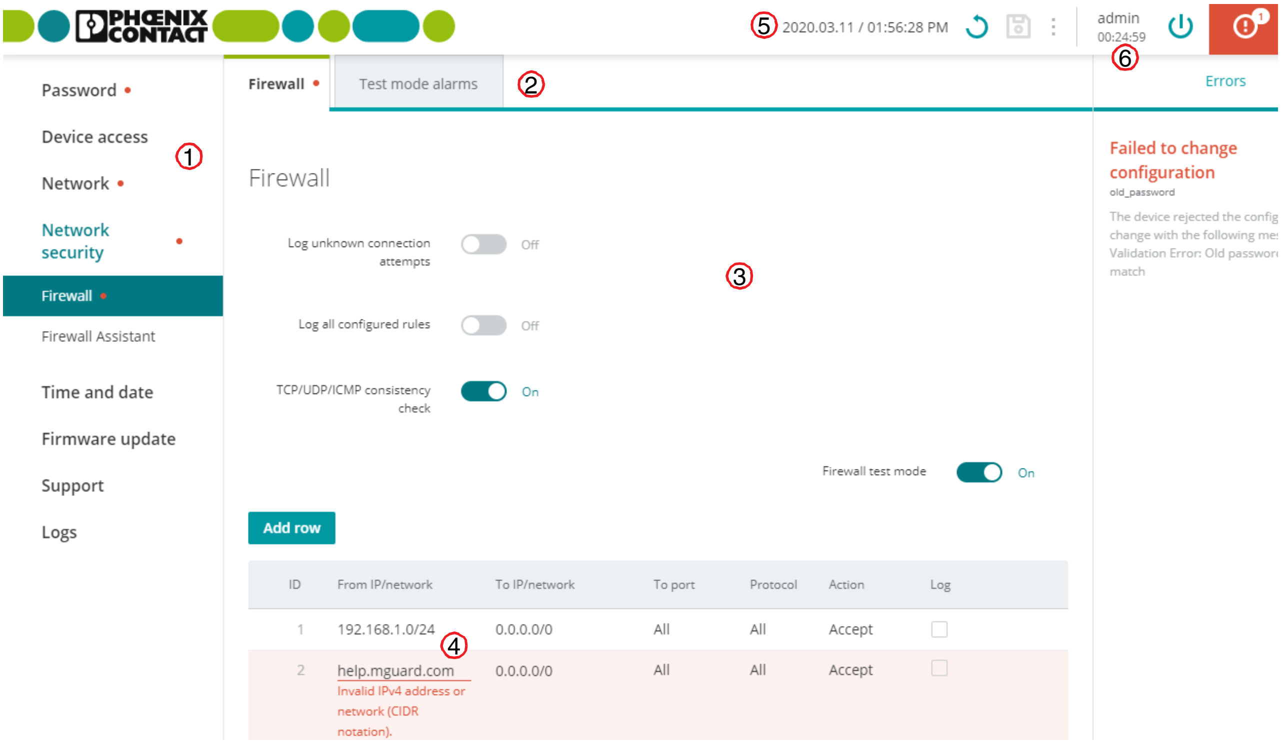
Session timeout

A logged-in user is automatically logged out once the session has elapsed (*session timeout*). The user is then forwarded to the login page if he/she tries to save a configuration change or an action.

Once the user has logged in, the timeout starts at 30 minutes. It is reset to 30 minutes if a configuration change is saved or an action carried out.

3.4 Help regarding the configuration

3.4.1 Page structure and function



Failed to change configuration
old_password
The device rejected the config change with the following me: Validation Error: Old passwor match

Firewall

Log unknown connection attempts: Off

Log all configured rules: Off

TCP/UDP/ICMP consistency check: On

Firewall test mode: On

ID	From IP/network	To IP/network	To port	Protocol	Action	Log
1	192.168.1.0/24	0.0.0.0/0	All	All	Accept	□
2	help.mguard.com Invalid IPv4 address or network (CIDR notation).	0.0.0.0/0	All	All	Accept	□

Figure 3-3 Web-based management: menu structure and page elements

Menu structure ①

Via the main and submenu structure, the individual configuration pages can be opened.

Configuration pages are often divided into several subpages that can be called via *tabs*.

Tabs ②

Tabs can be selected via the tab bar at the upper edge of the screen.

Configuration page ③

In the main window of a configuration page, the parameters of the individual variables can be changed.

The configuration page might be subdivided into several sections.

Variables ④

Variable values can be selected via a drop-down menu or a checkbox, or entered manually.

Depending on the variable, letters, numbers and/or certain special characters can be used (see Section 3.4.3). Some variables are entered into tables (e.g., 1:1 NAT rules).

System time ⑤

The current system time is displayed (format: *Coordinated Universal Time*/UTC).

Session timeout ⑥

A logged-in user is automatically logged out once the session has elapsed (*session timeout*) (see Section 3.3).

3.4.2 Icons and buttons

The following examples show icons and buttons available in the WBM.

Add row	Click on the **Add row** button to add a new table row below the last existing row.
Update	Click on the **Update** button to select and immediately use an update file.
💾	Click on the **Save** icon to apply all changes you made on a configuration page or in different menu items.
☑	Checkbox: Check the box to enable a function.
● On	Slide the switch to the **On** position to activate a function.
○ Off	Slide the switch to the **Off** position to deactivate a function.
🗑	Click on the **Waste bin** icon to delete the selected table row.
⊕	Click on the **Plus** icon to transfer the selected table row (*test mode alarms*) as a new firewall rule to the *Firewall table*.

3.4.3 Entering and changing values

Changing values

To change the value of a variable, you have to apply the change with a click on the 💾 button.

It is possible to first change several values and then apply them all with a click on the 💾 button.

Entry of impermissible values

Impermissible values of a variable cannot be applied. Usually, a corresponding error message is already displayed when an impermissible value is entered.

If impermissible entries are present, this is also indicated by a red dot ● in the menu bar (see Figure 3-3).

Correct the entries and apply the changed values with a click on the 💾 button.

3.4.4 Error messages

If an error cannot be detected during entering but only when the user tries to save the change, the adoption of all changed values is canceled.

The ❗ icon at the upper right edge of the screen indicates that one or several configuration errors are present. Click on the ❗ icon to have the corresponding error messages displayed in the right-hand page column (see Figure 3-3).

Correct the entries and apply the changed values with a click on the 💾 button.

3.4.5 Working with tables

Some mGuardNT settings are saved as a data record. In this case, the parameters and their values are entered in the table rows in the WBM.

IMPORTANT: Observe the sequence of the table rows

The sequence of the table rows is decisive for the configuration of firewall rules:

The firewall rules in the table are always queried one after the other starting from the top of the list of entries until an appropriate rule is found. Subsequent rules are then ignored.

Inserting table rows

- Click on the Add row button.

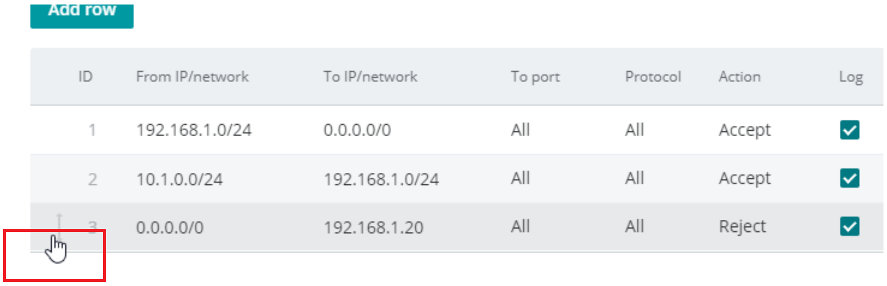
⇒ A new row is inserted below the last existing row.

- Click on the 💾 icon to apply the change.

⇒ A new data record was created in a new table row.

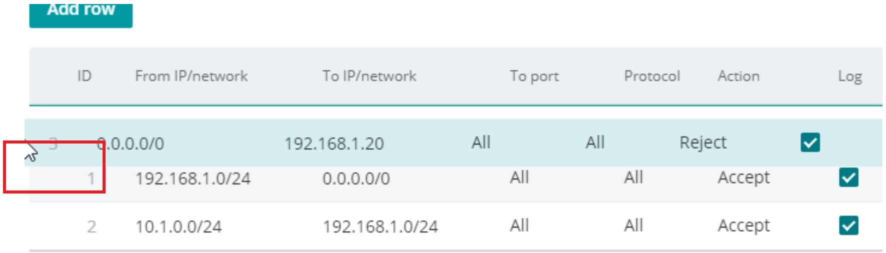
Moving table rows

- Move the mouse pointer to the left of the table row you wish to move until the pointer changes into a hand symbol.



ID	From IP/network	To IP/network	To port	Protocol	Action	Log
1	192.168.1.0/24	0.0.0.0/0	All	All	Accept	✓
2	10.1.0.0/24	192.168.1.0/24	All	All	Accept	✓
3	0.0.0.0/0	192.168.1.20	All	All	Reject	✓

- Click on the row and hold the mouse button down to drag and drop the row to the desired position.



ID	From IP/network	To IP/network	To port	Protocol	Action	Log
3	0.0.0.0/0	192.168.1.20	All	All	Reject	✓
1	192.168.1.0/24	0.0.0.0/0	All	All	Accept	✓
2	10.1.0.0/24	192.168.1.0/24	All	All	Accept	✓

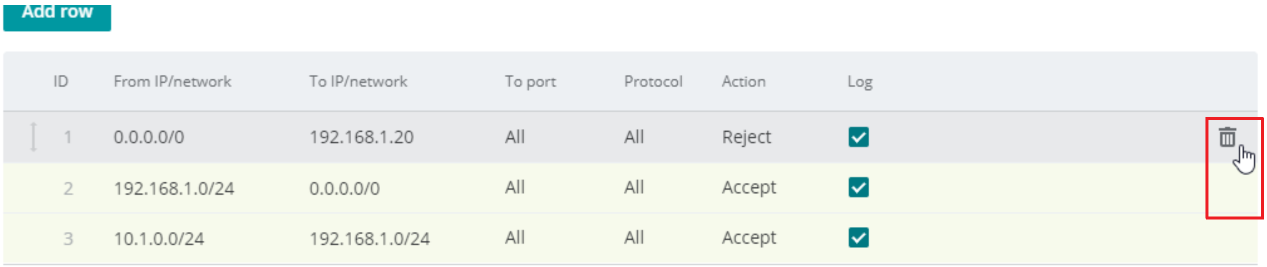
- Release the mouse button.

⇒ The row was moved to a new position.

- Click on the 💾 icon to apply the change.

Deleting table rows

- In the row you wish to delete, click on the 🗑 icon.



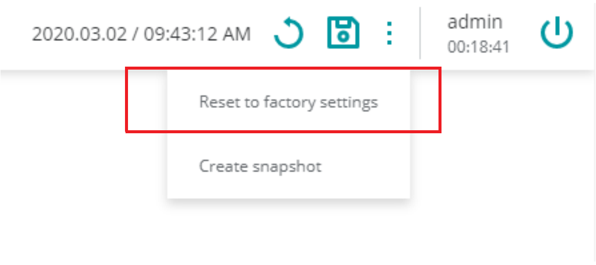
ID	From IP/network	To IP/network	To port	Protocol	Action	Log
1	0.0.0.0/0	192.168.1.20	All	All	Reject	☑
2	192.168.1.0/24	0.0.0.0/0	All	All	Accept	☑
3	10.1.0.0/24	192.168.1.0/24	All	All	Accept	☑

⇒ The row is deleted.

- Click on the 💾 icon to apply the change.

⇒ The table row and the data record were deleted.

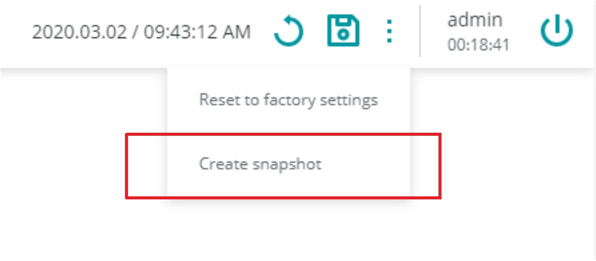
3.4.6 Resetting the device configuration to factory settings



The current configuration is deleted and reset to factory settings. The current administrator password, certificates and log entries are kept.

> To safely and irrevocably delete the configuration, you have to use the *smart mode* function “*Reset to factory settings*” (see Section 12.2).

3.4.7 Creating a snapshot



A snapshot can be used for error diagnostics and communication with the support team.

The snapshot is created and downloaded as a compressed file (in *tar.gz* format). The snapshot contains the current configuration and other system information of the device (see Table 3-1).

Table 3-1 Content of a snapshot

File name	Content/description
config	Shows the current device configuration.
bootloader_version	Shows the version of the currently installed bootloader.
conntrack	Shows the current content of the status table (*connection tracking table*).
eds	Shows current dynamic status information about certain functions of the device.
ip_addr	Shows the current network configuration of the device.
ip_neight	Shows current connection information on connected (*neighbored*) devices.
ip_link	Shows the current connection status of the network interfaces.
ip_route	Shows the current routing table.
ls_mnt_hfs	Shows the files and directories currently stored in the device's file system (/mnt/hfs).
journal	Shows the current log file of the system.
nft_ruleset	Shows the currently configured firewall rules.
nft_tables	Shows the currently configured firewall tables.
proclist	Shows the currently running processes.
serdata	Shows the serialization data that was linked to the device during creation.
services	Shows the currently started services (*systemd*) on the system.
uptime	Shows the current operating time and the load average of the system.
userid	Shows the user ID and group membership of the logged-in user.
version	Shows the currently installed firmware version.

Safety-relevant information such as passwords or cryptographic keys are not contained in the snapshot.

The time the snapshot was created is indicated in the file name as follows:

<YYYY-MM-DD_hh:mm:ss> (example: *snapshot_2019-10-09_22_00_00.tar.gz*)

3.4.8 Input: netmask and network

Netmask

The netmask can be entered in one of the following formats:

– Numeric (e.g., 24)

– Decimal (e.g., 255.255.255.0)

In the web-based management, the decimal format is automatically changed to the numeric format during entering (e.g., 255.255.0.0 --> 16).

Network

A network has to be specified in CIDR format, e.g., 192.168.1.0/24, (see Section 3.4.9).

If a network is entered in the web-based management in one of the formats shown in Table 3-2, the entry is automatically changed accordingly (see Table 3-2).

Table 3-2 Examples for the conversion of formats of networks in the WBM

Entered format	Converted format
10.1.1.1/32	10.1.1.1
10.1.1.1/24	10.1.1.0/24
10.1.1.1/16	10.1.0.0/16
10.1.1.1/8	10.0.0.0/8
10.1.1.1/0	0.0.0.0/0

3.4.9 CIDR (Classless Inter-Domain Routing)

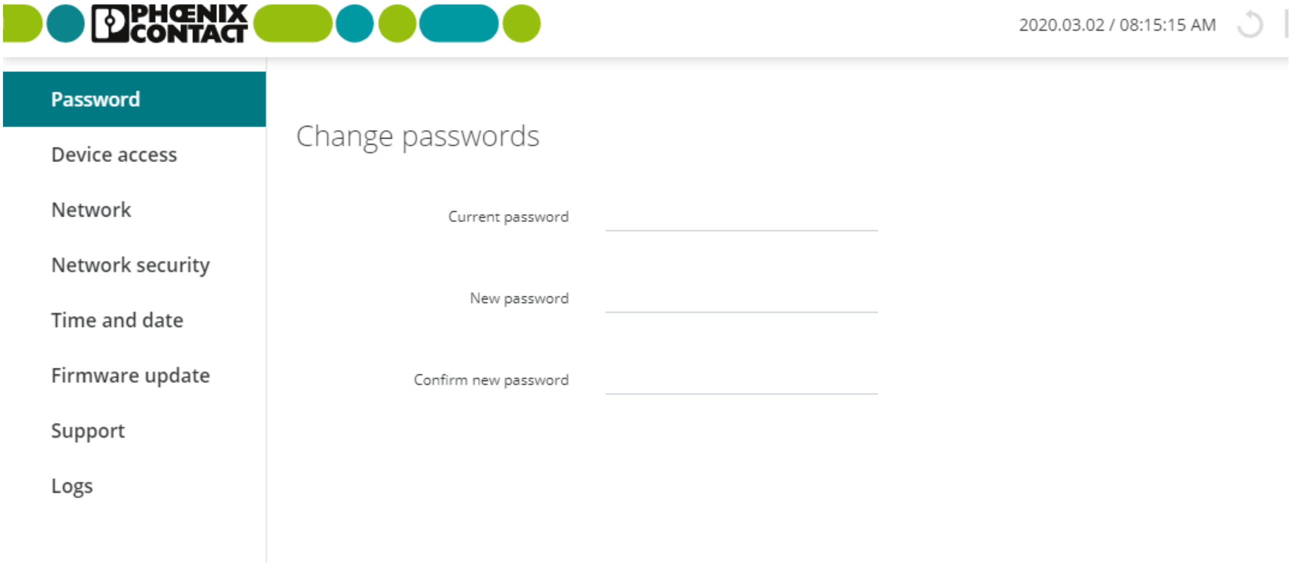
IP netmasks and CIDR combine several IP addresses to create a single address range. A range comprising consecutive addresses is handled like a network. To specify a range of IP addresses, you have to specify the address range in CIDR format (e.g., when configuring the firewall).

Table 3-3 CIDR, Classless Inter-Domain Routing

IP netmask[1]	**Binary**				**CIDR**
255.255.255.255	11111111	11111111	11111111	11111111	32
255.255.255.254	11111111	11111111	11111111	11111110	31
255.255.255.252	11111111	11111111	11111111	11111100	30
255.255.255.248	11111111	11111111	11111111	11111000	29
255.255.255.240	11111111	11111111	11111111	11110000	28
255.255.255.224	11111111	11111111	11111111	11100000	27
255.255.255.192	11111111	11111111	11111111	11000000	26
255.255.255.128	11111111	11111111	11111111	10000000	25
255.255.255.0	11111111	11111111	11111111	00000000	24
255.255.254.0	11111111	11111111	11111110	00000000	23
255.255.252.0	11111111	11111111	11111100	00000000	22
255.255.248.0	11111111	11111111	11111000	00000000	21
255.255.240.0	11111111	11111111	11110000	00000000	20
255.255.224.0	11111111	11111111	11100000	00000000	19
255.255.192.0	11111111	11111111	11000000	00000000	18
255.255.128.0	11111111	11111111	10000000	00000000	17
255.255.0.0	11111111	11111111	00000000	00000000	16
255.254.0.0	11111111	11111110	00000000	00000000	15
255.252.0.0	11111111	11111100	00000000	00000000	14
255.248.0.0	11111111	11111000	00000000	00000000	13
255.240.0.0	11111111	11110000	00000000	00000000	12
255.224.0.0	11111111	11100000	00000000	00000000	11
255.192.0.0	11111111	11000000	00000000	00000000	10
255.128.0.0	11111111	10000000	00000000	00000000	9
255.0.0.0	11111111	00000000	00000000	00000000	8
254.0.0.0	11111110	00000000	00000000	00000000	7
252.0.0.0	11111100	00000000	00000000	00000000	6
248.0.0.0	11111000	00000000	00000000	00000000	5
240.0.0.0	11110000	00000000	00000000	00000000	4
224.0.0.0	11100000	00000000	00000000	00000000	3
192.0.0.0	11000000	00000000	00000000	00000000	2
128.0.0.0	10000000	00000000	00000000	00000000	1
0.0.0.0	00000000	00000000	00000000	00000000	0

[1] Example: 192.168.1.0/255.255.255.0 corresponds to CIDR: 192.168.1.0/24

4 Menu: Password



Change passwords

Current password

New password

Confirm new password

Figure 4-1 Password: changing the password

Menu: Password

Change passwords

The administrator password is required to log in to the device via the web-based management (WBM) or the *Config API*.

After logging in for the first time, immediately change the default administrator password!

The password must contain between six and 200characters. To increase security, it should contain upper case and lower case characters, numbers, and permitted special characters.

Permitted characters (ASCII code):

!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~

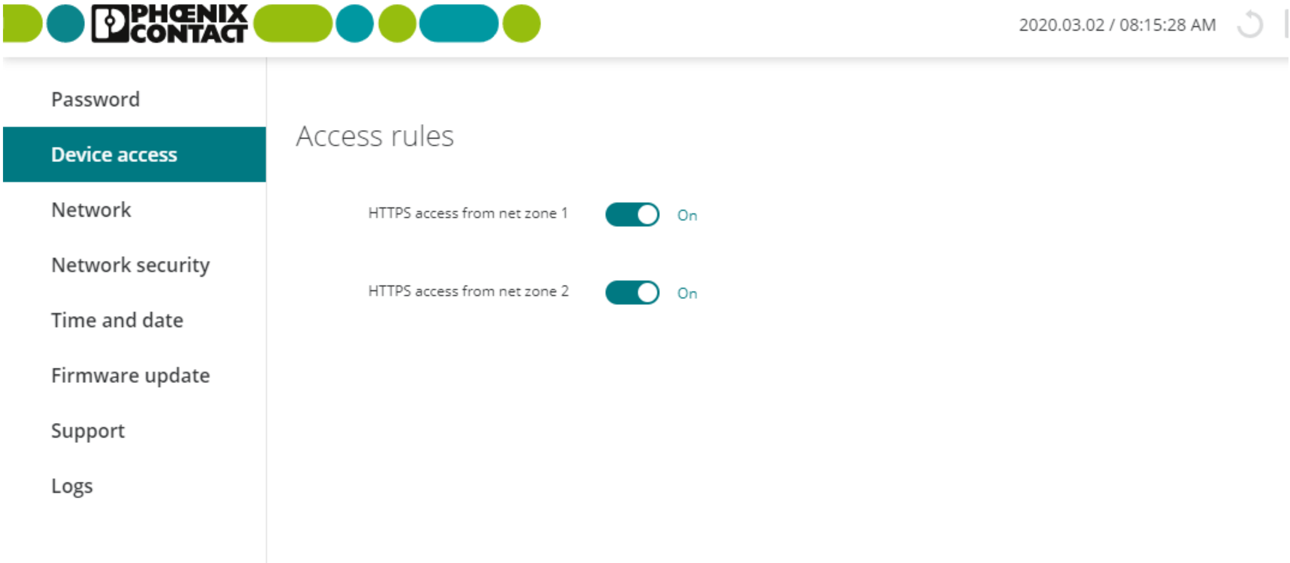
If you have forgotten your password, you have to reset the device to default settings via the *smart mode* function “*Reset to factory settings*” (see Section 12.2). All settings and the current password are then irrevocably deleted.

Default setting: *private*

> After filling in the three mandatory fields, you have to adopt the password change with a click on the 💾 button.

Current password	The current password that is to be changed.
New password	The new password.
Confirm new password	Enter the new password again.

5 Menu: Device access



Access rules

HTTPS access from net zone 1 On

HTTPS access from net zone 2 On

Figure 5-1 Device access: configuring access rules

Menu: Device access

Access rules

By means of access rules, access to the web server of the device (web-based management or *Config API*) can be limited to one of the available net zones.

Access to further active services

The access to further services provided by the device is activated and deactivated on the respective configuration pages.

- DNS server (see Section 6.3): activated for net zone 2 by default
- NTP server (see Section 8): activated for net zone 2 by default

> **NOTE: Access from the Internet**
>
> Possibly, the server can be reached from the Internet when the device is connected to the Internet via the released net zone.

HTTPS access from net zone 1

When this function is activated, access to the HTTPS server of the device is permitted from the selected net zone.

Default setting: activated

HTTPS access from net zone 2

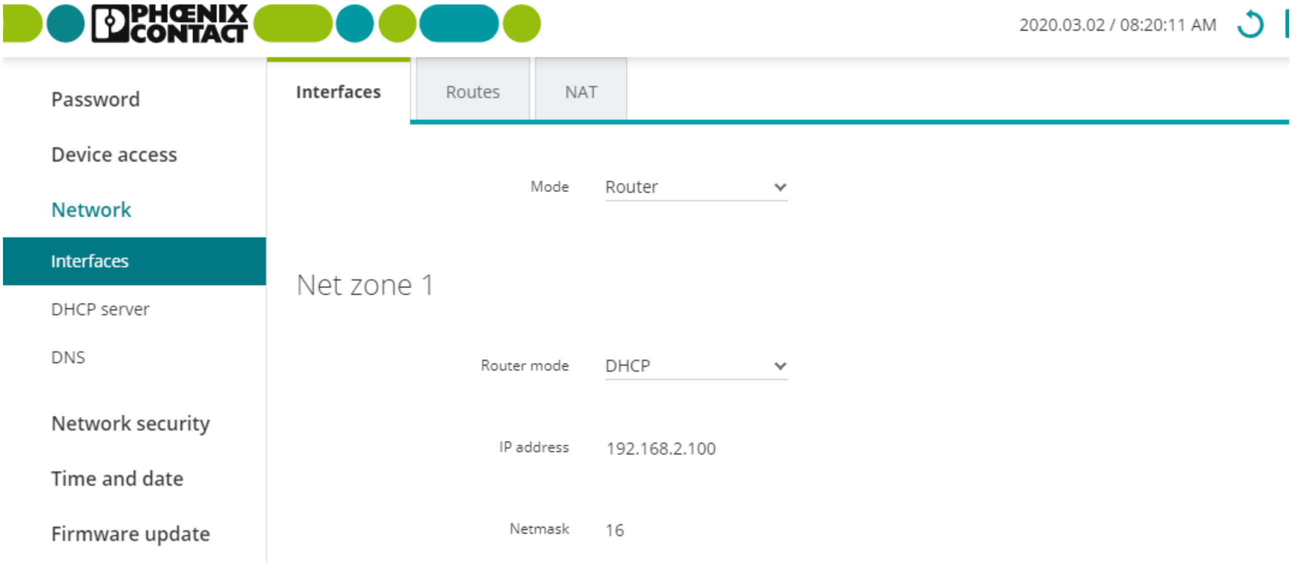
When this function is activated, access to the HTTPS server of the device is permitted from the selected net zone.

Default setting: activated

6 Menu: Network

6.1 Network >> Interfaces

6.1.1 Interfaces



Mode: Router

Net zone 1

Router mode: DHCP

IP address: 192.168.2.100

Netmask: 16

Figure 6-1 Configuring network interfaces (net zone 1/2)

Menu: Network >> Interfaces >> Interfaces		
	Mode	The device can be operated in two network modes (*Router mode* and *Stealth mode*). **Router** See *“Router mode” on page 29* **Stealth** See *“Stealth mode” on page 32*

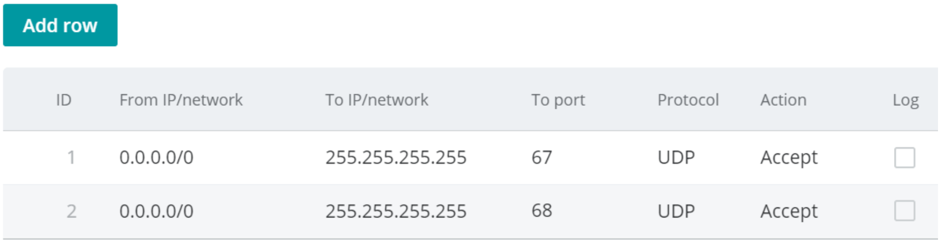
Menu: Network >> Interfaces >> Interfaces

NOTE

DHCP traffic in stealth mode

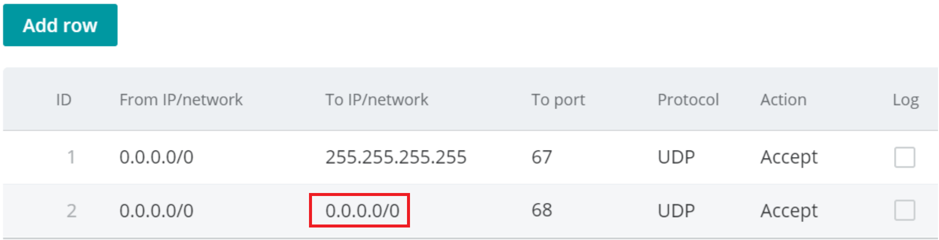
The firewall rules must be adapted so that DHCP packets can be forwarded through the device in stealth mode.

The following two rules must be entered in the *Firewall table* (see Section 7.1.1) of the device so that protected clients can retrieve their IP configuration from a DHCP server in *stealth mode*.



ID	From IP/network	To IP/network	To port	Protocol	Action	Log
1	0.0.0.0/0	255.255.255.255	67	UDP	Accept	□
2	0.0.0.0/0	255.255.255.255	68	UDP	Accept	□

If an IP configuration is still not assigned, this could be due to a non standard-compliant DHCP server. In this case, adjust the rules as follows:



ID	From IP/network	To IP/network	To port	Protocol	Action	Log
1	0.0.0.0/0	255.255.255.255	67	UDP	Accept	□
2	0.0.0.0/0	0.0.0.0/0	68	UDP	Accept	□

Menu: Network >> Interfaces >> Interfaces

Router mode

If the device is in *router mode*, it functions as a gateway between different subnets. The data traffic is routed between the two network interfaces (net zones) of the device.

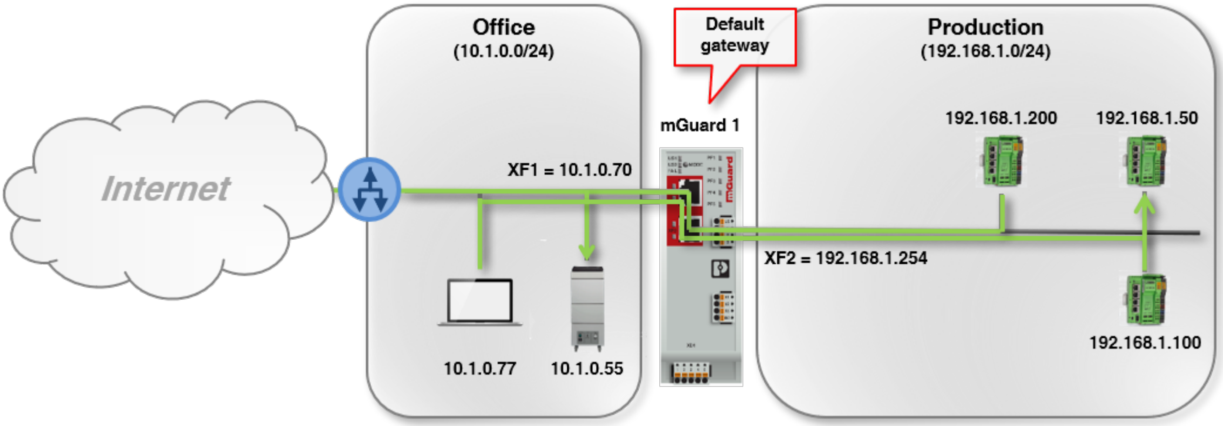


Figure 6-2 Example: *Router mode*

Clients in the subnet of one net zone (e.g., *Office*) can communicate and exchange data with clients in the subnet of the other net zone (e.g., *Production*).

The network configuration of net zone 1 (XF1) of the device can be entered statically or retrieved from a DHCP server. In net zone 2 (XF2–XF5), the device can act as a DHCP server.

The safety and firewall functions of the device are applied to incoming and routed data traffic.

Net zone 1 (XF1) (Only visible in *router mode*)	The network interfaces of the device are assigned to two different net zones which each have an individual network configuration (IPv4 address and netmask). Access to external networks or to the Internet is usually established via net zone 1 (XF1). Connected network clients in the same net zone (subnet) can access the device via the configured IP address. The network address of net zone 1 (XF1) can be statically configured on the device or assigned via DHCP. ℹ The IP address of the corresponding net zone of the device has to be indicated as the default gateway for the connected clients so that they can use the device as a gateway. ℹ NAT/IP masquerading may have to be activated on the device so that devices from one net zone can communicate with devices from other net zones or with the Internet (see “NAT” on page 35).

Menu: Network >> Interfaces >> Interfaces		
	Router mode (Configurable in *router mode*)	Mode which is used to determine how a network configuration is assigned to the net zone. **DHCP** The net zone is automatically assigned a network configuration (IP address, subnet mask and, as an option, a default gateway) by a DHCP server if a DHCP server is available in the network. **Static** The user has to manually assign a static network configuration to the net zone (IP address, subnet mask and, as an option, a default gateway). **Default setting:** DHCP
	IP address (Configurable in “*Static*” *router mode*) (Status information in “*DHCP*” *router mode*)	IP address of network interface XF1 (net zone 1). **Input format:** IPv4 address
	Netmask (Configurable in “*Static*” *router mode*) (Status information in “*DHCP*” *router mode*)	Subnet mask that defines in which subnet the device is located. **Input format:** CIDR or decimal format, e.g., 24 (= 255.255.255.0)
	Default gateway (Configurable in “*Static*” *router mode*) (Status information in “*DHCP*” *router mode*)	IP address of the default gateway to which the device sends connection requests to access unknown subnets or the Internet. A device in the subnet of net zone 1 (XF1) or in the subnet of net zone 2 (XF2–XF5) can be specified as the default gateway. An empty field without entry means that no default gateway is configured on the device. **Input format:** IPv4 address
	DNS server (Status information in “*DHCP*” *router mode*)	IP addresses of one or several DNS servers assigned by the DHCP server. A DNS server (DNS = *Domain Name System*) allows clients to resolve host names into IP addresses.

Menu: Network >> Interfaces >> Interfaces

Net zone 2 (XF2–XF5)

(Only visible in *router mode*)

The network interfaces of the device are assigned to two different net zones which each have an individual network configuration (IPv4 address/netmask).

Usually, access to the local (protected) network is established via net zone 2 (XF2–XF5).

Connected network clients in the same net zone (subnet) can access the device via the configured IP address.

The network address of net zone 2 (XF2–XF5) has to be statically configured. Unlike net zone 1 (XF1), it cannot be assigned via DHCP.

> ℹ The network address of the corresponding net zone of the device has to be specified as the default gateway for the connected clients so that they can use the device as a gateway.

> ℹ NAT/IP masquerading may have to be activated so that clients from one net zone can communicate with clients from other net zones or with the Internet (see “NAT” on page 35).

IP address

IP address of network interface XF2–XF5 (net zone 2).

Input format: IPv4 address

Default setting: 192.168.1.1

Netmask

Subnet mask that defines in which subnet the device is located.

Input format: CIDR or decimal format, e.g., 24 (= 255.255.255.0)

Default setting: 24

Menu: Network >> Interfaces >> Interfaces

Stealth mode

The *stealth mode* is used to protect one or several local clients in an existing subnet (e.g., machine controls in a production network) against unwanted network access without having to change their IP settings.

For this, the device is added between the clients and the surrounding subnet via its two network interfaces (net zones) so that the entire data traffic from and to the clients is routed through the device.

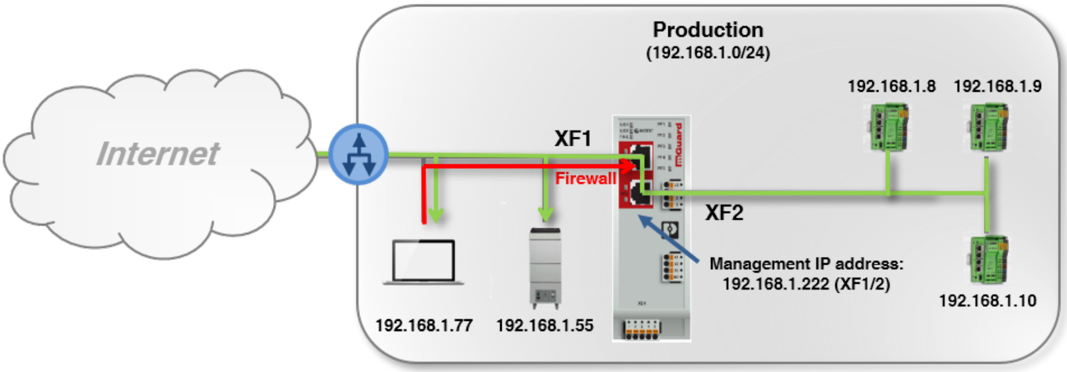


Figure 6-3 Example: *Stealth mode* (with activated firewall XF1 --> XF2)

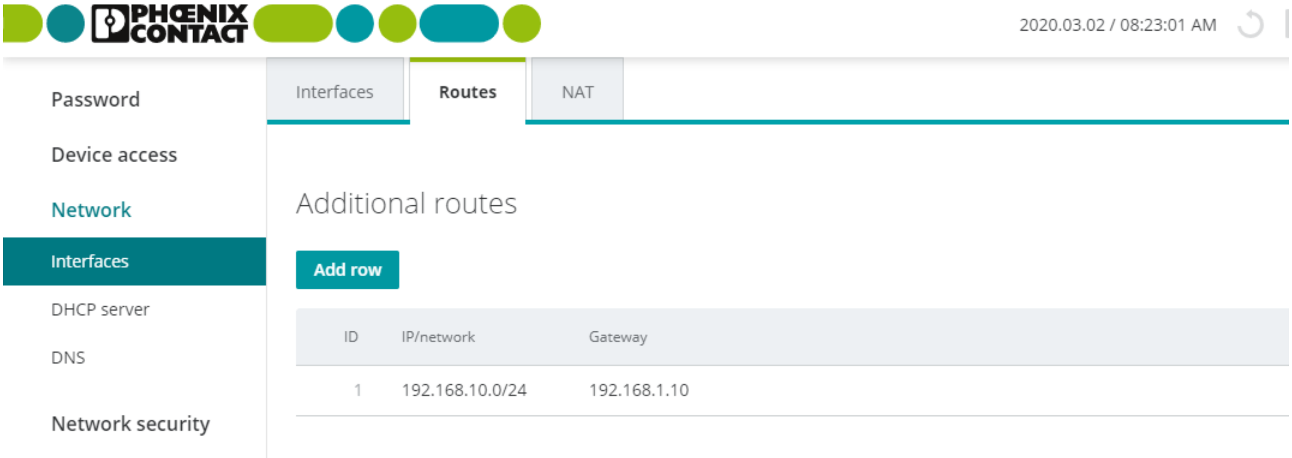
The network configuration of the connected clients does not have to be changed.

The server services DHCP, NTP and DNS server are deactivated on the device. The safety and firewall functions of the device are applied to incoming and routed data traffic (e.g., DHCP *requests*, see NOTE).

(Stealth mode) (Only visible in *stealth mode*)	**Management IP address**	IP address via which the device is available in *stealth mode* and can be managed. The management IP address is available on all network interfaces (net zones). The device is configured via the WBM or the *Config API*. **Input format:** IPv4 address **Default setting:** 192.168.1.1
	Netmask	Subnet mask that defines in which subnet the device can be reached in *stealth mode* via the management IP address. **Input format:** CIDR or decimal format, e.g., 24 (= 255.255.255.0) **Default setting:** 24

Menu: Network >> Interfaces >> Interfaces		
	Default gateway	IP address of the default gateway to which the device sends connection requests to reach unknown subnets or the Internet. In *stealth mode*, the device can thereby send requests as a client, for example, to an NTP or DNS server. If a management IP address is assigned, the default gateway of the network in which the device is located has to be specified. The default gateway can be reached via net zone 1 (XF1) and net zone 2 (XF2–XF5). **Input format:** IPv4 address **Default setting:** 192.168.1.254

6.1.2 Routes



2020.03.02 / 08:23:01 AM

Password

Device access

Network

Interfaces

DHCP server

DNS

Network security

Interfaces | Routes | NAT

Additional routes

Add row

ID	IP/network	Gateway
1	192.168.10.0/24	192.168.1.10

Figure 6-4 Configuring additional static routes

Menu: Network >> Interfaces >> Routes

Routes

(Only visible in *router mode*)

Using statically entered routes, the device can reach network destinations that are not known to its default gateway.

These destinations can also be reached by connected network clients that use the device as the default gateway.

The device forwards data packets to destinations that can be reached via the static route directly to the gateway specified in the static route.

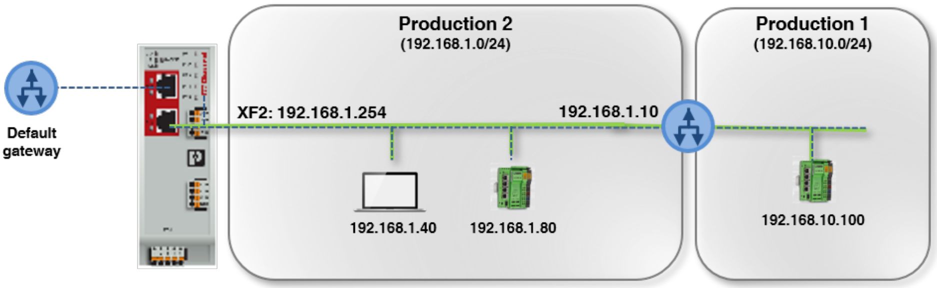


Figure 6-5 Example: additional static routes (values from Figure 6-4)

Requests from clients in *Production 2* which shall reach destinations in the subnet 192.168.10.0/24 are forwarded by the device via the static route 192.168.1.10.

IP/network

Destination (network or IP address) that shall be reached via an additional route.

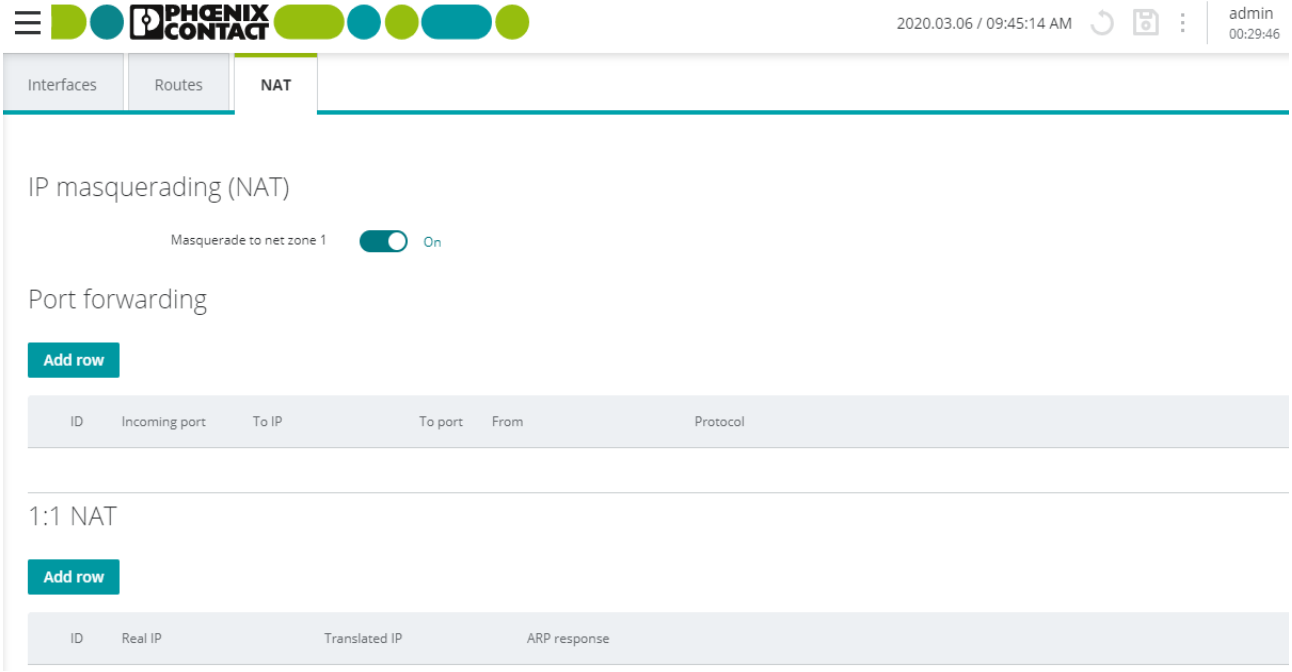
Input format: IPv4 address, IPv4 network (CIDR notation)

Gateway

IP address of the gateway via which the destination can be reached using the additional route.

Input format: IPv4 address

6.1.3 NAT



IP masquerading (NAT)

Masquerade to net zone 1 On

Port forwarding

Add row

ID	Incoming port	To IP	To port	From	Protocol

1:1 NAT

Add row

ID	Real IP	Translated IP	ARP response

Figure 6-6 Configuring IP masquerading, port forwarding and 1:1 NAT

Menu: Network >> Interfaces >> NAT

Network Address Translation (NAT)

(Only visible in *router mode*)

IP masquerading and 1:1 NAT

Network Address Translation (NAT) is used to hide the real IP address of connected network clients from external network devices.

For this, the device in its function as NAT router replaces the sender address specified in the IP header of a requesting client with

– Its own IP address (**IP masquerading (NAT)**) or
– A virtual (translated) IP address (**1:1 NAT**).

With this (translated) IP address as the sender address, the device forwards requests to external network devices. These send their response packets to the (translated) sender address, which the device then translates to the real IP address of the requesting client.

This way, for example, an entire (private) network can be hidden behind the device. The clients in the “private” network and their IP addresses remain hidden when communicating externally via the device.

See **“IP masquerading (NAT)” on page 36** and **“1:1 NAT” on page 39**.

Port forwarding

With port forwarding, data packets that are sent (from external devices) to a certain port of the device are forwarded to a defined destination IP address and a defined destination port in the (local) subnet of the device.

See **“Port forwarding” on page 37**.

Menu: Network >> Interfaces >> NAT

IP masquerading (NAT)

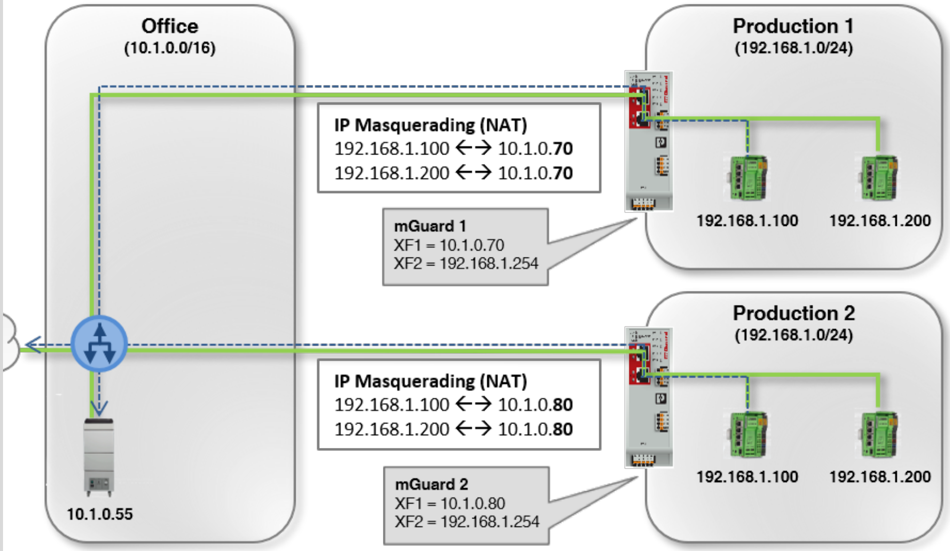
(Only visible in *router mode*)

The device replaces the real IP addresses in data packets of requesting network clients with its **own IP address** (of the outgoing interface XF1).

With this IP address as the sender address, the device forwards the requests to external network devices. These send their response packets to the IP address of the device, which then forwards the responses to the real sender addresses of the requesting clients.

For this, the connection data of the requests are saved on the device in a *connection tracking* table and compared to the connection data of the responses.

If the masked clients are to be reached from outside, the IP address of the device **cannot** be used for this. In case of external requests, the masked clients have to be contacted using their real IP address. (The network and general routing settings have to be configured accordingly.)



Requests from the **PCLs (Production)** are sent to the IP address of the **Office server (10.1.0.55)** and masked with the IP address of **the mGuard device (10.1.0.70** resp. **10.1.0.80)** as the source address.

Example

IP masquerading is often used if the “private” IP addresses cannot or should not be routed externally, for example, because a private address range such as 192.168.1.x or the internal network structure of a production network should be hidden.

This way, production cells with identical IP setting can be easily integrated into the network structure.

Masquerading into the direction of net zone 1

When this function is activated, the NAT masquerading rule is applied to data packets that leave the device via the selected network interface (XF1/net zone 1).

In the data packet, the sender's IP address is translated into the IP address of the network interface (XF1/net zone 1).

Default setting: activated

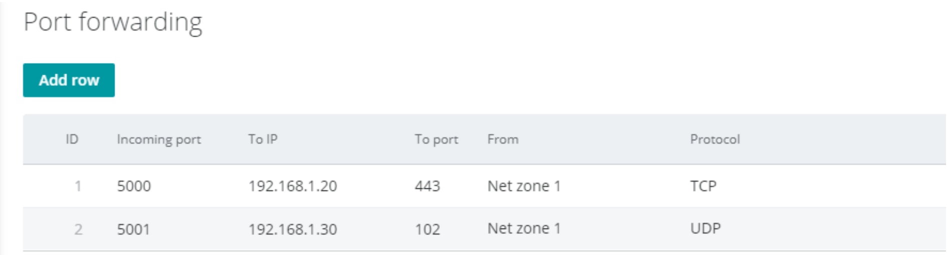
Menu: Network >> Interfaces >> NAT

Port forwarding

(Only visible in *router mode*)

With port forwarding, data packets that are sent to the IP address and to a certain port of the device are forwarded to another destination IP address and another destination port in the network.

The original destination IP address and the original destination port in the header of the incoming data packet are translated according to the port forwarding rule.



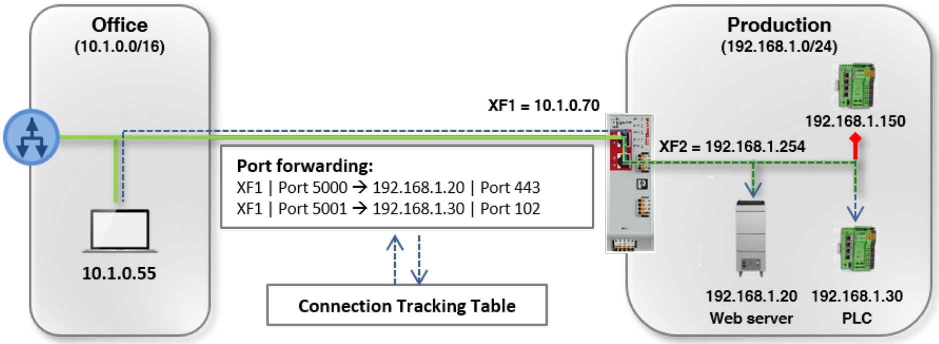
Port forwarding

Add row

ID	Incoming port	To IP	To port	From	Protocol
1	5000	192.168.1.20	443	Net zone 1	TCP
2	5001	192.168.1.30	102	Net zone 1	UDP

The translation of the header is entered in the *connection tracking* table of the device. Response packets are compared to these entries and the header files are translated back to the original values.

The firewall automatically permits the data traffic from and to the defined IP addresses and ports which was defined in a port forwarding rule.



The Office client (10.1.0.55) sends requests to the **Web server (port 443)** to the IP address **10.1.0.70** (port **5000**)
The Office Client (10.1.0.55) sends requests to the **PLC (port 102)** to the IP address **10.1.0.70** (port **5001**)

Example

Often, port forwarding is used to make individual devices or server services in a local network (e.g., web server) systematically reachable from the external network or the Internet (see figure):

- The **web server (192.168.1.20/port 443)** in the production network can be reached from the office network via the IP address of the device (**XF1 = 10.1.0.70**) and port **5000**.
- The **PLC (192.168.1.30/port 102)** in the production network can be reached from the office network via the IP address of the device (**XF1 = 10.1.0.70**) and port **5001**.

All other devices in the production network (e.g., PLC 192.168.1.150) shall not be reached from the outside. They are protected by the firewall.

Menu: Network >> Interfaces >> NAT

> **Port forwarding rules are applied before firewall rules**
>
> The rules for port forwarding are applied before the configured firewall rules for routed data traffic are applied (see Section 7).
>
> This means that a firewall rule that blocks all incoming data traffic is not applied if a port forwarding rule applies.

ID

Identification number of the rule (generated by the system)

The ID determines the order in which the rules are applied, starting with the lowest ID.

Incoming port

Network port to which the data packets have to be sent so that the rule is applied.

Data packets sent to this port are usually forwarded to the specified destination IP address (*To IP*) and the defined destination port (*To port*):

- The destination IP address in the header of the data packet is translated into the destination IP address defined in the rule (*To IP*).
- The destination port in the header of the data packet is translated into the destination port defined in the rule (*To port*).

Input format: 1 – 65535

Default setting: 1

To IP

IP address of the destination client to which the incoming data packets are forwarded if the rule is applied.

The original destination address in the header of the data packet is translated into this IP address.

Input format: IPv4 address

Default setting: 0.0.0.0

To port

Network port to which the incoming data packets are forwarded if the rule is applied.

The original destination port in the header of the data packet (see *Incoming port*) is translated into this port.

Input format: 1 – 65535

Default setting: 1

From

Net zone 1, net zone 2

Network interface (net zone) via which the data packets have to be sent to the device so that the rule is applied.

Default setting: Net zone 1

Protocol

TCP, UDP

Network protocol that has to be used for transmitting the data packets so that the rule is applied.

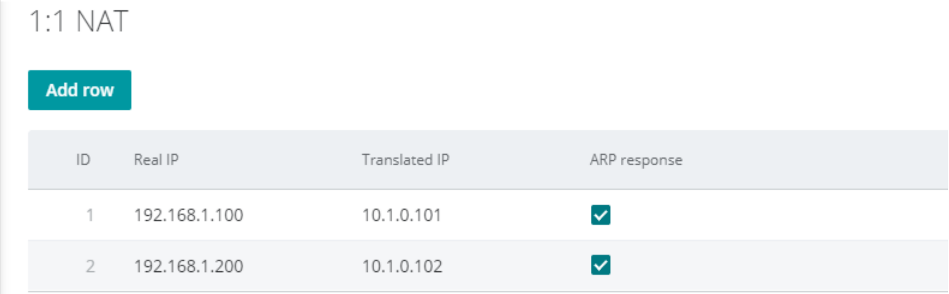
Default setting: TCP

Menu: Network >> Interfaces >> NAT

1:1 NAT

(Only visible in *router mode*)

The device translates the **real IP address** of a client (A) into a **translated IP address** which is then indicated to external network devices in the data packet as the sender address in requests from client (A).



1:1 NAT

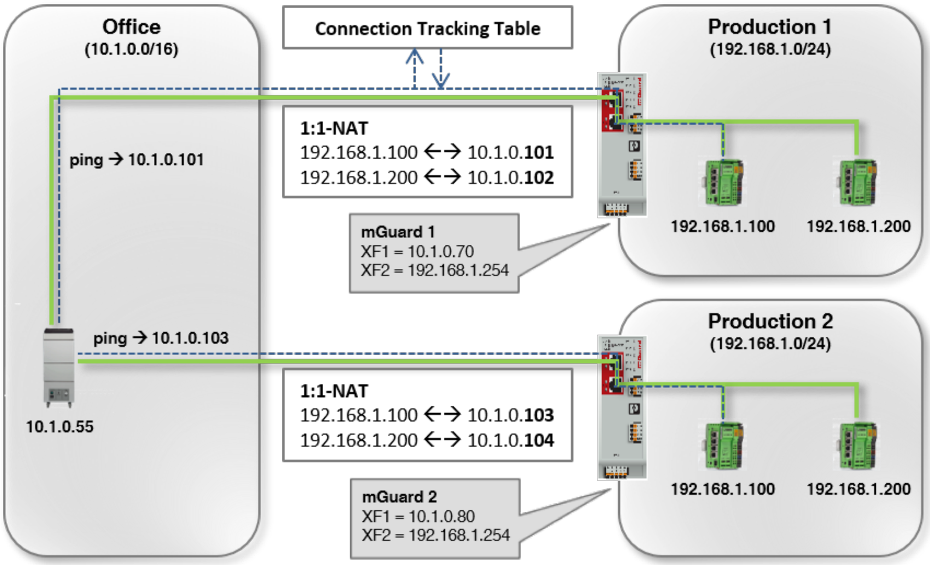
Add row

ID	Real IP	Translated IP	ARP response
1	192.168.1.100	10.1.0.101	☑
2	192.168.1.200	10.1.0.102	☑

Responses or requests from external network devices to the translated IP address of client (A) are translated by the device into the real IP address of the client (A) and forwarded to this address.

For this, the connection data of the requests are saved on the device in a *connection tracking* table and compared to the connection data of the responses.

(**Prerequisite**: The firewall of the device has to be configured in such a way that external requests are permitted.)



Example

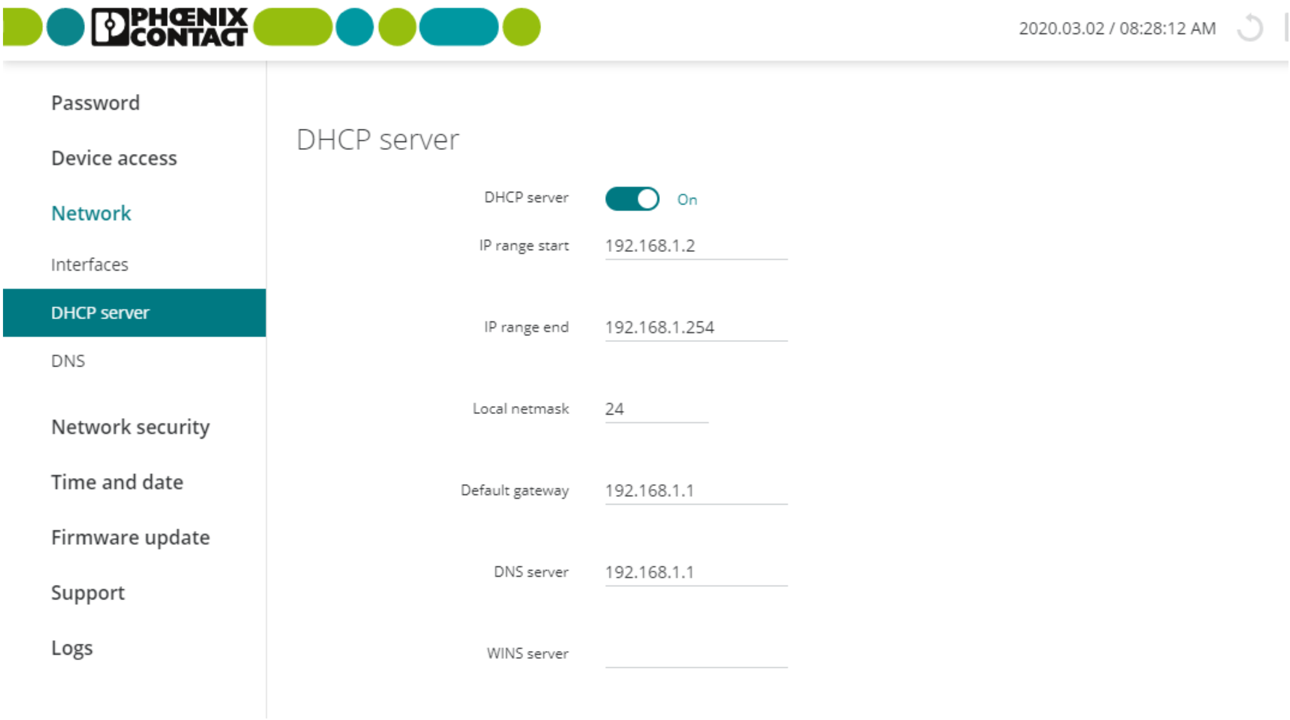
In practice, an identical IP configuration for connected machines is often used in different production cells. This would lead to address conflicts.

To solve this problem, 1:1 NAT rules can be configured on the mGuard devices. The device then replaces the respective real sender IP addresses of clients in the production network (e.g., 192.168.1.200) with translated (virtual) IP addresses from the office network (e.g., 10.1.0.102).

Communication with devices in the office network is now implemented in both directions via the translated IP addresses of the clients in the production network.

Menu: Network >> Interfaces >> NAT		
	ID	Identification number of the rule (generated by the system) The ID determines the order in which the rules are applied, starting with the lowest ID.
	Real IP	In the current version, NAT can only be applied to IP addresses, but not to networks. Real IP address of the client to whose data packets 1:1 NAT shall be applied. In the device, the real (most of the time private) IP address of the client is converted to a translated (virtual) IP address of another (most of the time public) network. The network devices will therefore see the translated IP address as the sender address of the client. This way, clients in a public network can communicate with the client in the private network. The translated IP address is indicated to them as the IP address of the client. Both networks have to use the same subnet mask. The translated IP address of the client must not be assigned in the other network. **Input format:** IPv4 address
	Translated IP	In the current version, NAT can only be applied to IP addresses, but not to networks. Translated IP address assigned to the client via 1:1 NAT instead of the real IP address. In the device, the real (most of the time private) IP address of the client is converted to a translated (virtual) IP address of another (most of the time public) network. The network devices will therefore see the translated IP address as the sender address of the client. This way, clients in a public network can communicate with the client in the private network. The translated IP address is indicated to them as the IP address of the client. Both networks have to use the same subnet mask (e.g., 24). The translated IP address must not be assigned in the other network. **Input format:** IPv4 address
	ARP response	When this function is activated, ARP requests sent to the translated IP address of a client are answered on behalf of the device. This way, it is ensured that a connected client in the private network can be reached from another network via its translated IP address without the need for manual configuration of MAC addresses. When this function is deactivated, ARP requests sent to translated IP addresses remain unanswered. **Default setting:** activated

6.2 Network >> DHCP server



DHCP server

DHCP server: On

IP range start: 192.168.1.2

IP range end: 192.168.1.254

Local netmask: 24

Default gateway: 192.168.1.1

DNS server: 192.168.1.1

WINS server:

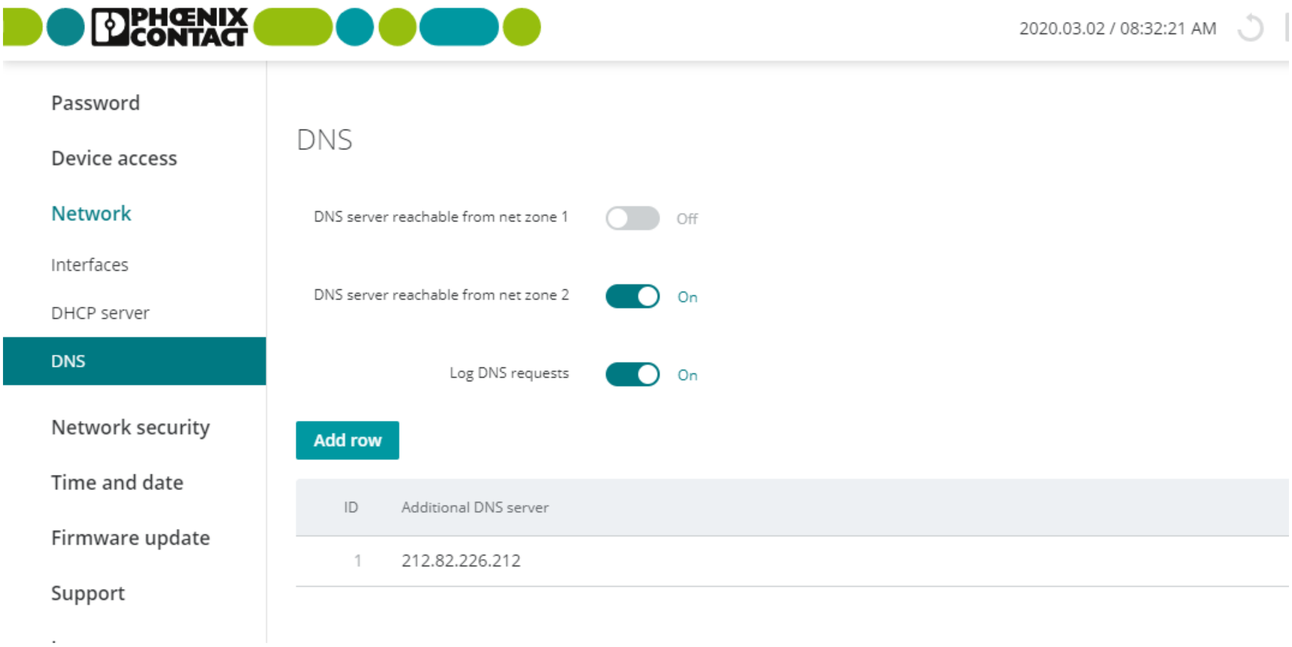
Figure 6-7 Configuring the DHCP server

Menu: Network >> DHCP server		
DHCP server	Using the *Dynamic Host Configuration Protocol* (DHCP), requesting network clients are automatically assigned a network configuration. Connected clients have to be configured in such a way that they send a DHCP request to receive a network configuration from a DHCP server. In the other case, the configuration has to be statically configured for each client.	
	DHCP server	When this function is activated, requesting clients that are connected to the device via net zone 2 are assigned a network configuration. If the DHCP server is activated, the incoming firewall of the device is automatically configured in such a way that requests by network clients to the DHCP server are accepted via the configured network interface (net zone 2) and UDP port 67. The server then assigns IP addresses from the configured IP address range to the clients. **Default setting:** activated

Menu: Network >> DHCP server		
	IP address range start	Start of the IP address range from which the DHCP server assigns IP addresses to requesting clients. The range should be chosen in such a way that the contained IP addresses can be reached in the assigned subnet (see below, “*Local netmask*”). **Input format:** IPv4 address **Default setting:** 192.168.1.2
	IP address range end	End of the IP address range from which the DHCP server assigns IP addresses to requesting clients. The range should be chosen in such a way that the contained IP addresses can be reached in the assigned subnet (see below, “*Local netmask*”). **Input format:** IPv4 address **Default setting:** 192.168.1.254
	Local netmask	Subnet mask the DHCP server assigns to requesting clients. The range from which network clients are assigned IP addresses should be chosen in such a way that the IP addresses can be reached in the assigned subnet (see above, *“IP address range start” or “IP address range end”*). **Input format:** CIDR or decimal format, e.g., 24 (= 255.255.255.0) **Default setting:** 24
	Default gateway	IP address of the default gateway the DHCP server assigns to requesting clients. Usually, this is the internal IP address of the device. **Input format:** IPv4 address **Default setting:** 192.168.1.1
	DNS server	IP address of a DNS server the DHCP server assigns to requesting clients. A DNS server (DNS = *Domain Name System*) allows clients to resolve host names into IP addresses. If the DNS server of the device shall be used, the IP address of the net zone on which this service is active has to be specified (default setting: net zone 2 = 192.168.1.1). **Input format:** IPv4 address **Default setting:** 192.168.1.1

Menu: Network >> DHCP server		
	WINS server	IP address of a WINS server the DHCP server assigns to requesting clients. A WINS server (*Windows Internet Naming Service*) allows clients to resolve host names (*NetBIOS names*) into IP addresses. **Input format:** IPv4 address **Default setting:** empty

6.3 Network >> DNS



DNS

DNS server reachable from net zone 1: Off

DNS server reachable from net zone 2: On

Log DNS requests: On

ID	Additional DNS server
1	212.82.226.212

Figure 6-8 Configuring DNS server and DNS client

Menu: Network >> DNS

DNS

If the device is to establish a connection to a peer (e.g., to an NTP server) whose address is specified in the form of a host name (i.e., *www.ntp-server.com*), the device must determine which IP address belongs to the host name.

To do this, it connects to a DNS server to query the corresponding IP address there. The IP address determined for the host name is stored in the DNS cache of the device so that it can be found directly for other host name resolutions.

Connected network clients can also use the device as a DNS server. In this case, the device responds to DNS requests from the clients by accessing its internal DNS cache.

If the connected clients receive their network configuration from the device via DHCP, the IP address of the device can be assigned automatically to the clients as a DNS server address.

DNS server reachable from net zone 1

When this function is activated, access from the selected net zone to the DNS server of the device is permitted.

> **NOTE: Access from the Internet**
>
> Possibly, the server can be reached from the Internet when the device is connected to the Internet via the released net zone.

When this function is deactivated, access to the DNS server via the selected net zone is dropped by the firewall.

Default setting: deactivated

Menu: Network >> DNS

DNS server reachable from net zone 2

When this function is activated, access from the selected net zone to the DNS server of the device is permitted.

> **NOTE: Access from the Internet**
>
> Possibly, the server can be reached from the Internet when the device is connected to the Internet via the released net zone.

Default setting: activated

Log DNS requests

When this function is activated, a log entry is created for all requests to the DNS server of the device (UDP/TCP).

Log entries can be analyzed via the *Menu: Logs* or in the *journal* file, which can be created and downloaded via a snapshot (see Section 3.4.7).

Log entries can have different prefixes (see Section 11).

Default setting: deactivated

Additional DNS server

IP address of one or several DNS servers that are queried by the device for resolving host names.

The information on a request returned by the DNS server, i.e., the resolution of a host name into an IP address, is saved to the DNS cache of the device.

Network clients sending DNS requests to the device receive the information on the name resolution from its DNS cache, which is updated if required.

Input format: IPv4 address

Please note:

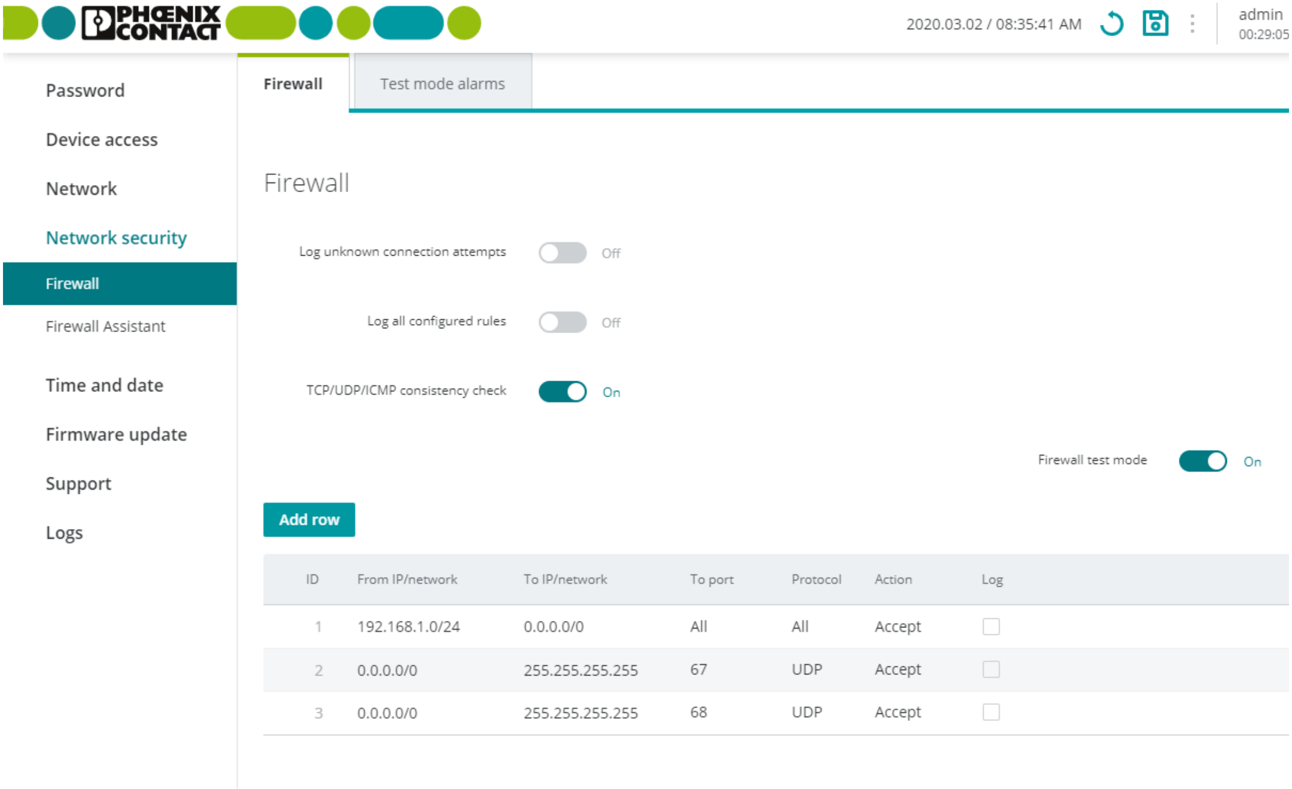
– If no user-defined DNS server is specified, the device uses a DNS server assigned via DHCP.

– If a DNS server is not assigned via DHCP either, the device uses default *Root Name Servers*.

7 Menu: Network security

7.1 Network security >> Firewall

7.1.1 Network security >> Firewall >> Firewall



Firewall

Log unknown connection attempts: Off

Log all configured rules: Off

TCP/UDP/ICMP consistency check: On

Firewall test mode: On

ID	From IP/network	To IP/network	To port	Protocol	Action	Log
1	192.168.1.0/24	0.0.0.0/0	All	All	Accept	□
2	0.0.0.0/0	255.255.255.255	67	UDP	Accept	□
3	0.0.0.0/0	255.255.255.255	68	UDP	Accept	□

Figure 7-1 Configuring firewall rules

Menu: Network security >> Firewall >> Firewall	
Firewall	Data packets that are routed through the device are analyzed by its firewall (packet filter) and then forwarded or blocked according to the configured firewall rules. Routed data traffic indicates data connections that do not terminate on the device (such as requests to the NTP server of the device) but are routed (*Router mode*) or forwarded (*Stealth mode*) by the device. The connections can also be received and forwarded on the same network interface (net zone).

Menu: Network security >> Firewall >> Firewall

Stateful packet inspection

The firewall of the device operates on the principle of the *stateful packet inspection firewall*: This means that response packets for requests that were permitted by the firewall on the way into one direction automatically pass the firewall on their way back if they can be clearly related to the request.

For this, the information on each data connection is saved to a *connection tracking* table and compared with the response packets to be able to clearly relate them to the corresponding requests.

Firewall rules are never applied to response packets.

Behavior and effects of firewall rules

1. **No rule configured:** All data packets are dropped.
2. **None of the configured rules applies:** All data packets are dropped.
3. **One rule is configured and applies:**
   The rule is applied and the configured action performed.
4. **Several rules are configured and apply:**
   The rules are queried one after the other starting from the top until an appropriate rule is found. This rule is applied and the configured action performed.
   In this case, none of the succeeding rules is considered even if they would apply.
   It is not necessary to specify a final rule that abandons all other rules.

> ℹ If a firewall is reconfigured, all existing entries in the status table (*connection tracking table*) are deleted.

Setup of firewall rules

A firewall rule comprises different parameters. Only if all configured parameters of a rule apply to a packet, the entire rule applies.

Some parameters of a rule might be configured in such a way that they always apply (e.g., *All* or *0.0.0.0/0*).

Example

From IP: *192.168.1.0/24* | To IP: *0.0.0.0/0* | Port: *All* | Protocol: *All* | Action: *Accept*

All data packets that are sent from network 192.168.1.0/24 to any destination network and destination port are accepted.

Log unknown connection attempts

When this function is activated, a corresponding log entry is created for each data connection no configured firewall rule applies to.

Log entries can be analyzed via the *Menu: Logs* or in the *journal* file, which can be created and downloaded via a snapshot (see Section 3.4.7).

Log prefix: *fw-forward-policy-*

Default setting: deactivated

Menu: Network security >> Firewall >> Firewall		
	Log all configured rules	When this function is activated, a corresponding log entry is created for each data connection to which any firewall rule applies. This also applies to rules in which logging via the "*Log*" function is deactivated. Log entries can be analyzed via the *Menu: Logs* or in the *journal* file, which can be created and downloaded via a snapshot (see Section 3.4.7). Log prefix: *fw-forward-* **Default setting:** deactivated
	TCP/UDP/ICMP consistency check	The consistency check increases the protection of connected network clients against *Denial of Service* (DoS) attacks. When this function is activated, data packets that are routed through the device and forwarded to connected network clients are checked for malicious elements: **ICMP packets** Only known ICMP code is used. **UDP packets** Destination port in the UDP packet is not equal to zero. **TCP packets** Source and destination port in the TCP packet are not equal to zero. **IPv4 packets** Protocol not set to zero. Data packets that do not meet the specified requirements are dropped by the firewall and not forwarded. **Default setting:** activated

Menu: Network security >> Firewall >> Firewall

Firewall test mode

Data traffic unintentionally blocked by the firewall can be easily identified and permitted through the automated creation of corresponding firewall rules.

NOTE: The firewall is partially deactivated.

In the *Firewall test mode*, data packets that are not detected by any of the already configured firewall rules are not dropped but forwarded instead.

Precondition

To enable the *Firewall test mode* to generate entries, the existing firewall table must not contain a final rule that blocks all data traffic.

Functionality

When the function is enabled, the firewall analyzes the (routed) traffic passed through the device.

If an already configured firewall rule applies to a data packet, the rule is applied to the data packet **as usual** (Action = *Accept, Reject* or *Drop*).

If none of the configured rules apply to a data packet, the packet is **not rejected as usual**, but forwarded.

At the same time, the user is informed about the event:

1. The device's "PF2" LED lights up red.
2. The switching output "O1" on the COMBICON connector "XG2" of the device assumes high level.
   (A connected signal lamp would light up in this case).
3. An entry is created in the *Test mode alarms* table which can be analyzed by the user.

If the data traffic that has triggered a *Test mode alarm* shall be allowed in the future, the user can automatically create a corresponding firewall rule from the respective entry in the *Test mode alarms* table (see below and Section 7.1.2).

Creating firewall rules from "Test mode alarms"

An entry in the *Test mode alarms* table can be selected and automatically inserted as a new firewall rule at the end of the existing firewall table (see Section 7.1.2).

The newly inserted rule would allow the corresponding data traffic for the future (Action = *Accept*).

Disable "Firewall test mode"

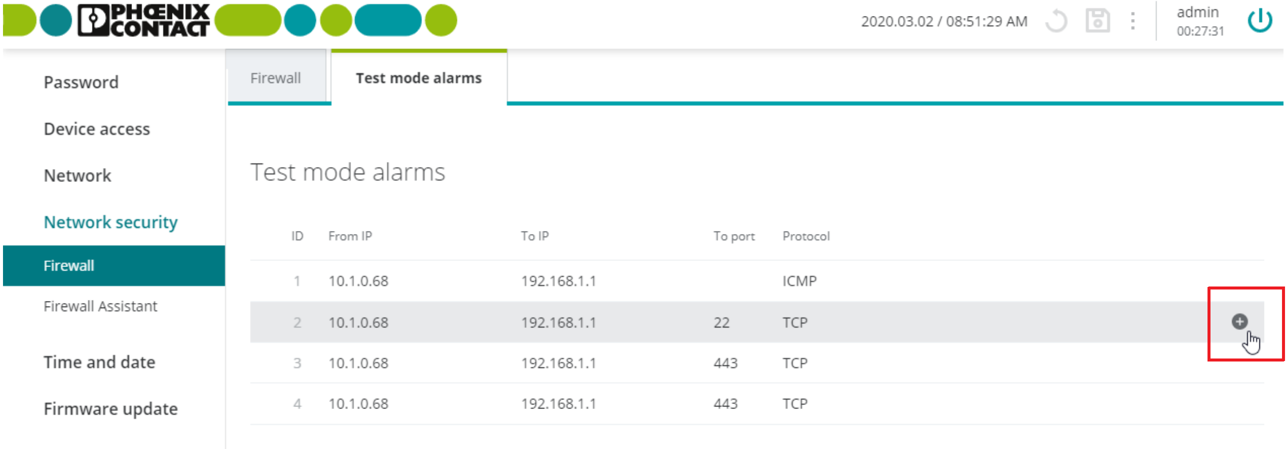
If the *Firewall test mode* is deactivated, all entries in the *Test mode alarms* table are deleted and a signaling by the LED "PF2" and the switching output "O1" is terminated.

Default setting: deactivated

Menu: Network security >> Firewall >> Firewall		
Firewall table	**ID**	Identification number of the rule (generated by the system) The ID determines the order in which the rules are queried, starting with the lowest ID.
	From IP/network	Source (network or IP address) from which the data packets have to be sent so that the rule applies in this respect. **Note:** If “0” is specified as the subnet mask, the rule applies to all sources (all IP addresses and networks) in this respect. **Input format:** IPv4 address, IPv4 network (CIDR format) **Default setting:** 192.168.1.0/24
	To IP/network	Destination (network or IP address) to which the data packets have to be sent so that the rule applies in this respect. **Note:** If “0” is specified as the subnet mask, the rule applies to all destinations (all IP addresses and networks) in this respect. **Input format:** IPv4 address, IPv4 network (CIDR format) **Default setting:** 0.0.0.0/0
	To port	Destination port to which the data packets have to be sent so that the rule applies in this respect. **Input format:** 1 – 65535, all **Note:** All = all ports **Default setting:** All
	Protocol	**TCP, UDP, ICMP, GRE, ESP, All** Network protocol that has to be used for transmitting the data packets so that the rule applies in this respect. **Note:** All = all protocols **Default setting:** All
	Action	**Accept, Reject, Drop** Action that is to be performed if all parameters configured in the access rule apply to a packet. **Accept:** The data packets may pass through. **Reject:** The data packets are rejected. The sender is informed. **Drop:** The data packets are dropped. The sender is not informed. **Default setting:** Accept

Menu: Network security >> Firewall >> Firewall		
	Log	When this function is activated, a corresponding log entry is created for each data connection this rule applies to. For rules in which the function is deactivated no log entry is created unless the function “*Log all configured rules*” is activated. Log entries can be analyzed via the *Menu: Logs* or in the *journal* file, which can be created and downloaded via a snapshot (see Section 3.4.7). Log prefix: *fw-forward-* **Default setting:** deactivated

7.1.2 Network security >> Firewall >> Test mode alarms



Test mode alarms

ID	From IP	To IP	To port	Protocol
1	10.1.0.68	192.168.1.1		ICMP
2	10.1.0.68	192.168.1.1	22	TCP
3	10.1.0.68	192.168.1.1	443	TCP
4	10.1.0.68	192.168.1.1	443	TCP

Menu: Network security >> Firewall >> Test mode alarms

Test mode alarms

(The “Test mode alarms” tab is only visible if the “Firewall test mode” is activated).

In *Firewall test mode*, the data traffic routed through the device is analyzed and a table automatically created with entries for the data packets that are not acquired by the already configured firewall rules.

The entries acquired in this table can then be selected individually and added as firewall rules at the end of the *Firewall table* of the device (menu: **Network security >> Firewall >> Firewall**, see *Firewall table*).

Added rules permit the corresponding data traffic (**Action = Accept**).

NOTE: Automatically created firewall rules are activated.

Immediately check the newly created firewall rules and adapt them according to your security requirements.

Proceed as follows:

- Check the table entries.
- Identify the firewall rules that you would like to accept considering your security requirements.
- Move the mouse pointer over the firewall rule you would like to transfer into the existing Firewall table.

⇒ The ⊕ icon will appear at the end of the row.

- Click on ⊕ to copy the rule to the Firewall table.

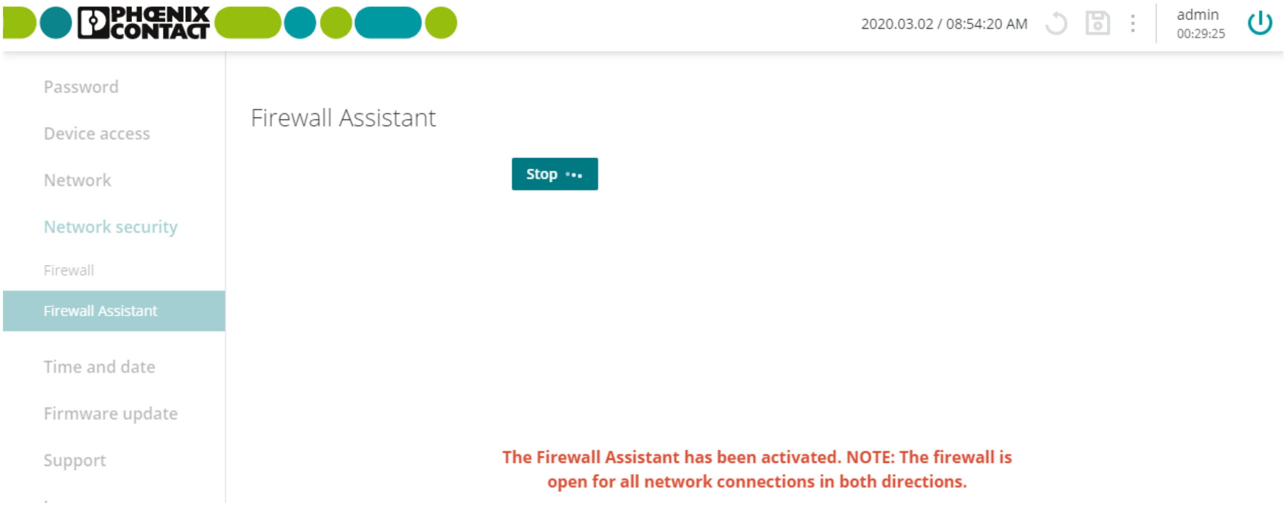
⇒ The firewall rule is inserted at the end of the Firewall table.

- Change to the **Network security >> Firewall >> Firewall** menu.
- Adapt the inserted firewall rules according to your security requirements.
- Then click on the 💾 icon to apply the change.

⇒ The newly added firewall rules are activated and immediately permit the corresponding data traffic unless superordinate rules prohibit the data traffic.

Menu: Network security >> Firewall >> Test mode alarms		
	ID	Identification number of the entry (generated by the system) The ID specifies the order in which the test mode alarms were triggered and led to an entry.
	From IP	Source (IP address) from which the data packet was sent.
	To IP	Destination (IP address) to which the data packet was sent.
	To port	Destination port to which the data packet was sent. No entry means that no destination port was specified in the data packet (e.g., ICMP data packets).
	Protocol	Network protocol that was used for transmitting the data packet. The **TCP**, **UDP**, **ICMP**, **GRE,** and **ESP** protocols are accepted. For all other protocols, the value **All** is entered.

7.2 Network security >> Firewall Assistant



The Firewall Assistant has been activated. NOTE: The firewall is open for all network connections in both directions.

If activated, the *Firewall Assistant* analyzes and acquires the data traffic routed through the device (**net zone 1** ←→ **net zone 2**).

For this, the firewall is open into both directions.

The acquired packet data is used to deduce firewall rules that are automatically entered in the Firewall table of the device when the Firewall Assistant has been stopped.

The data traffic defined in these firewall rules is allowed in the future (**Action = Accept**). All other connections are dropped.

The Firewall table created using the *Firewall Assistant* can be adapted and extended as required.

Table 7-1 Firewall Assistant: conversion of packet data into firewall rules

Header entry	Entry in firewall rule	Example
Source IP address	**From IP/network**	*10.1.1.55*
Destination IP address	**To IP/network**	*192.168.1.100*
The respective netmask of the source and destination network is not acquired. Only the individual IP addresses are acquired and accepted to the firewall rule.		
Destination port	**To port**	*443*
If no destination port is transmitted (e.g., as with the *ICMP* protocol), the value "*All*" is entered in the firewall rule.		
Protocol	**Protocol**	*TCP*
The following protocols can be accepted as values in the firewall rule: – *TCP, UDP, ICMP, GRE, ESP* For all other protocols, the value *"All"* is entered in the firewall rule.		
––	**Action**	*Accept*
In all firewall rules created via the *Firewall Assistant* or *Firewall test mode*, "*Accept*" is always entered as the action value.		

Procedure

Starting the Firewall Assistant

> **NOTE: The firewall is deactivated.**
> If the *Firewall Assistant* is activated, connected network clients are no longer protected by the firewall.

> The *Firewall Assistant* can only be started if **all firewall rules** in the *Firewall table* were previously deleted under **Network security >> Firewall >> Firewall** (see *Firewall table*).

- Click on the **Start** button to activate the Firewall Assistant.

⇒ Data traffic is analyzed and acquired.

⇒ The firewall is open into both directions.

Stopping the Firewall Assistant and creating firewall rules

> **NOTE: The automatically created firewall rules are active without prior checking.**
> Immediately check the newly created firewall rules and adapt them according to your security requirements.

- Click on the **Stop** button to deactivate the Firewall Assistant.

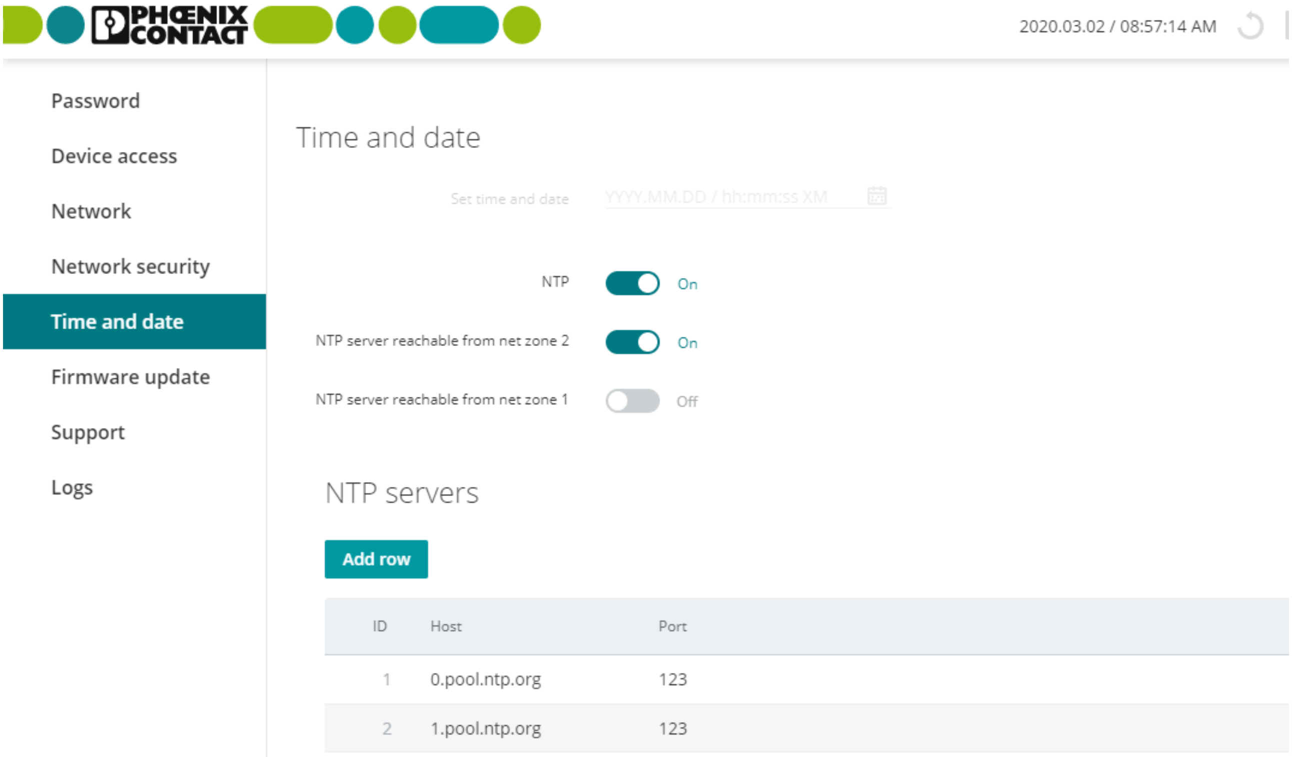
⇒ The acquired packet data is used to automatically create firewall rules, which are entered in the *Firewall table* (menu: **Network security >>Firewall >> Firewall,** see *Firewall table*).

⇒ The entered rules immediately and permanently permit the corresponding data traffic (**Action = Accept**) (see Table 7-1).

> If the created firewall rules are not visible under **Network security >> Firewall >> Firewall**, reload the page in the web browser.

The Firewall table created using the *Firewall Assistant* can be adapted and extended as required.

8 Menu: Time and date



2020.03.02 / 08:57:14 AM

Time and date

Set time and date: YYYY.MM.DD / hh:mm:ss XM

NTP: On

NTP server reachable from net zone 2: On

NTP server reachable from net zone 1: Off

NTP servers

ID	Host	Port
1	0.pool.ntp.org	123
2	1.pool.ntp.org	123

Figure 8-1 Configuring time and date

Menu: Time and date

Time and date

You can set the device system time manually or synchronize the system time using the NTP server of your choice.

> Set the time and date correctly. Otherwise, certain time-dependent activities cannot be carried out correctly by the device.

If the power supply to the device is briefly interrupted, the buffered *real-time clock* (RTC) ensures that time and date are retained and are available correctly and in the current time after a short interruption.

Set time and date

(Only visible if NTP is deactivated)

The current time and date of the device are configured and saved to the *real-time clock* (RTC).

Format: *Coordinated Universal Time* (UTC)

Permissible range:

>= 2018-01-01_00:00:00

<= 2069-01-01_00:00:00

Menu: Time and date

NTP

When the function is activated, the NTP client of the device is activated.

The NTP server of the device is only activated if access to the NTP server is at least permitted for one net zone (see below).

NTP client

When this function is activated, the device obtains its system time (time and date) from one or more NTP servers and continuously synchronizes itself with them.

The *real-time clock* (RTC) of the device is automatically synchronized with the time data obtained from the NTP servers.

Initial time synchronization can take 15 minutes or more. During this time, the device continuously compares the time data of the external NTP servers and its own system time so that they can be adjusted as accurately as possible.

NTP server

When this function is activated, connected network clients can synchronize their system time via the NTP server of the (*mGuard*)device.

Access to the NTP server can be activated or deactivated for each net zone (see below).

Default setting: activated

NTP server reachable from net zone 2

(Only visible when NTP is activated)

When this function is activated, access to the NTP server of the device is permitted from the selected net zone.

The NTP server of the device is only activated if access from at least one net zone is permitted.

> **NOTE: Access from the Internet**
> Possibly, the server can be reached from the Internet when the device is connected to the Internet via the released net zone.

Default setting: activated

NTP server reachable from net zone 1

(Only visible when NTP is activated)

When this function is activated, access to the NTP server of the device is permitted from the selected net zone.

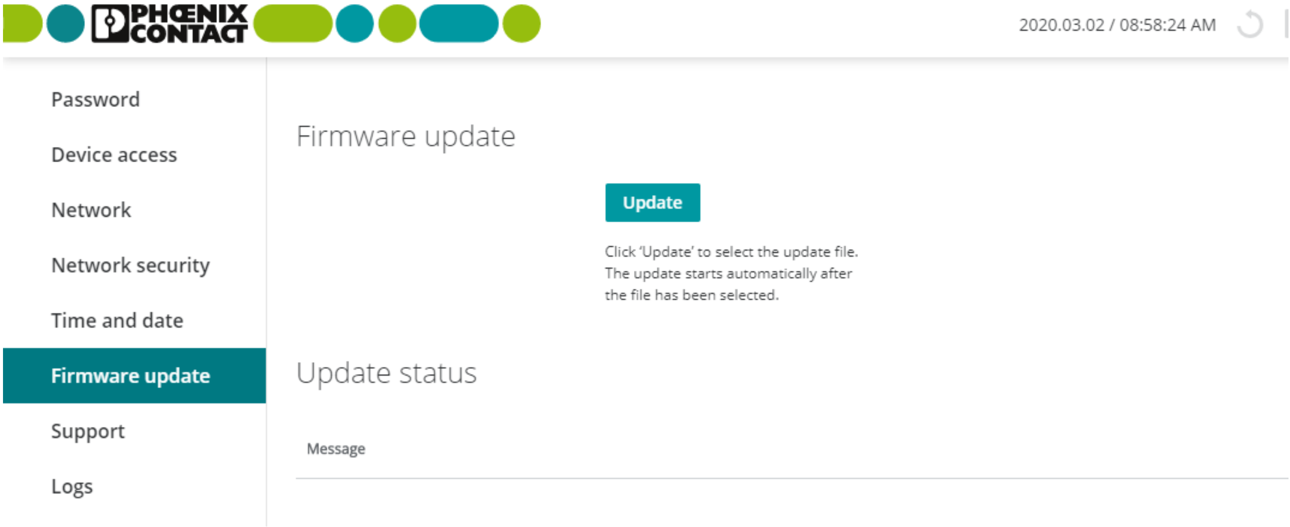
The NTP server of the device is only activated if access from at least one net zone is permitted.

> **NOTE: Access from the Internet**
> Possibly, the server can be reached from the Internet when the device is connected to the Internet via the released net zone.

Default setting: deactivated

Menu: Time and date		
NTP server	**Host**	IP address or host name of the external NTP server (time server) to which the device is to send NTP requests to obtain the current time (time and date). If several NTP servers are specified, the device automatically connects to all of them to determine the current time from all values received. **Input format:** host name or IPv4 address If host names are used, the device must be assigned one available DNS server via DHCP, or a user-defined DNS server must have been configured manually (see Section 6.3). **Default:** – 0.pool.ntp.org | Port:123 – 1.pool.ntp.org | Port:123 – 2.pool.ntp.org | Port:123 – 3.pool.ntp.org | Port:123
	Port	Port on which the external NTP server accepts NTP requests. **Default setting:** 123

9 Menu: Firmware update



Click 'Update' to select the update file. The update starts automatically after the file has been selected.

Figure 9-1 Starting the firmware update

Menu: Firmware update

Firmware update

A signed update file provided by Phoenix Contact (e.g., *mguard-image-1.3.1.mguard3.update.signed*) is uploaded from a configuration computer to the device and installed automatically.

All current settings, passwords and certificates are retained on the device. Downgrading from a higher to a lower firmware version is not possible.

> Current update files are made available for downloading in the web shop for the product:
>
> For example: phoenixcontact.net/product/1153078.
>
> As with each new firmware version safety-relevant improvements are added to the product, the latest firmware version should always be used.

Procedure

> **NOTE: Do not disconnect the power supply to the device during the update.**

- Open the **Firmware update** menu (*Firmware update* area).
- Click on the **Update** button.
- Select the update file for the firmware update.

⇒ Selecting the file automatically starts the update process.

⇒ Following successful installation of the firmware, the device restarts automatically after some seconds.

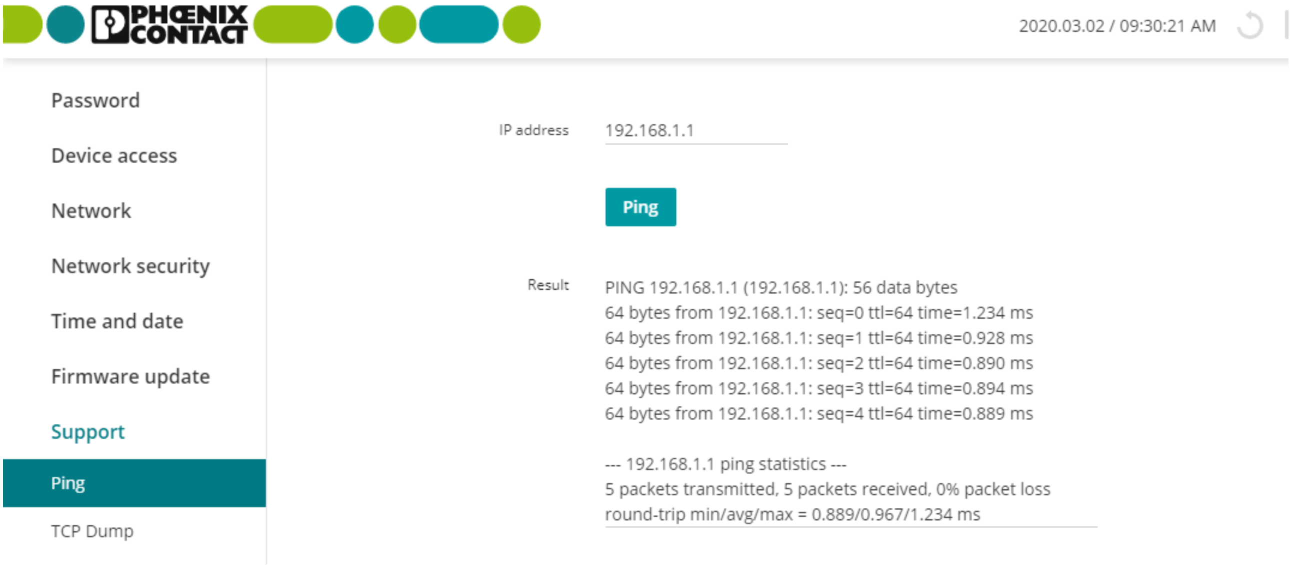
- Wait until the device has completely booted.

Update status

Shows current messages and information on the status of the firmware update.

10 Menu: Support

10.1 Support >> Ping



IP address 192.168.1.1

Result

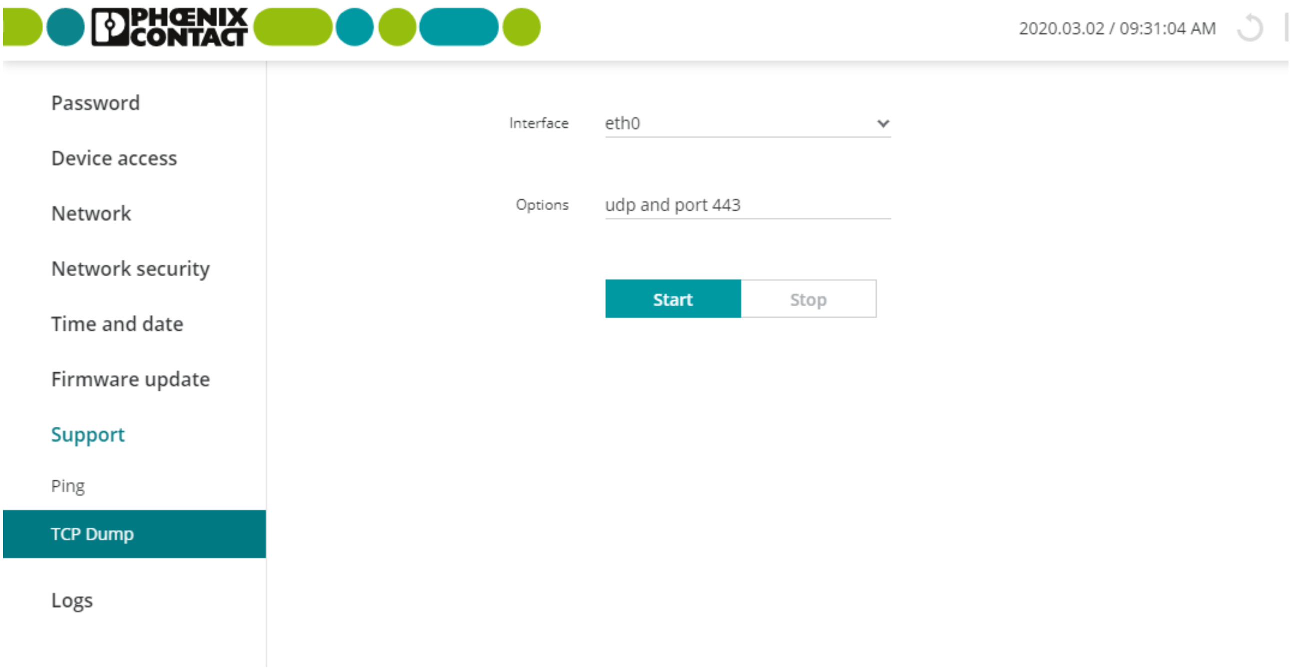
```
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: seq=0 ttl=64 time=1.234 ms
64 bytes from 192.168.1.1: seq=1 ttl=64 time=0.928 ms
64 bytes from 192.168.1.1: seq=2 ttl=64 time=0.890 ms
64 bytes from 192.168.1.1: seq=3 ttl=64 time=0.894 ms
64 bytes from 192.168.1.1: seq=4 ttl=64 time=0.889 ms

--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.889/0.967/1.234 ms
```

Figure 10-1 Support tools: Ping

Menu: Support >> Ping		
Ping	A ping request (*ICMP request*) can be used to check whether a network client is connected to an interface of the device via its IP address and can be reached via the ICMP protocol.	
	IP address	A ping request (*ICMP request*) is sent to the specified IP address of a network client. If the client can be reached via the *ICMP* protocol and any net zone of the device, it sends a response to the device. **Procedure** • Open the **Support >> Ping** menu. • Enter the IP address of the client to be checked in the field. • Click on the **Ping** button. ⇒ If the client can be reached via *ICMP*, the response from the client is displayed after a few seconds: e.g., *5 packets transmitted, 5 packets received*. ⇒ If the client cannot be reached via *ICMP*, a corresponding message is displayed: e.g., *100% packet loss*). **Input format:** IPv4 address

10.2 Support >> TCP Dump



Interface: eth0

Options: udp and port 443

Figure 10-2 Support tools: TCP Dump

Menu: Support >> TCP Dump

TCP Dump

By means of a packet analysis (*tcpdump*), the content of network packets that are sent or received via a specified network interface can be analyzed.

Filter options are used to define which network packets are to be analyzed.

The result of the analysis is saved to a file (*.*pcap*), downloaded and deleted from the device. If the device is restarted while an analysis is running, the data acquired until then is also deleted.

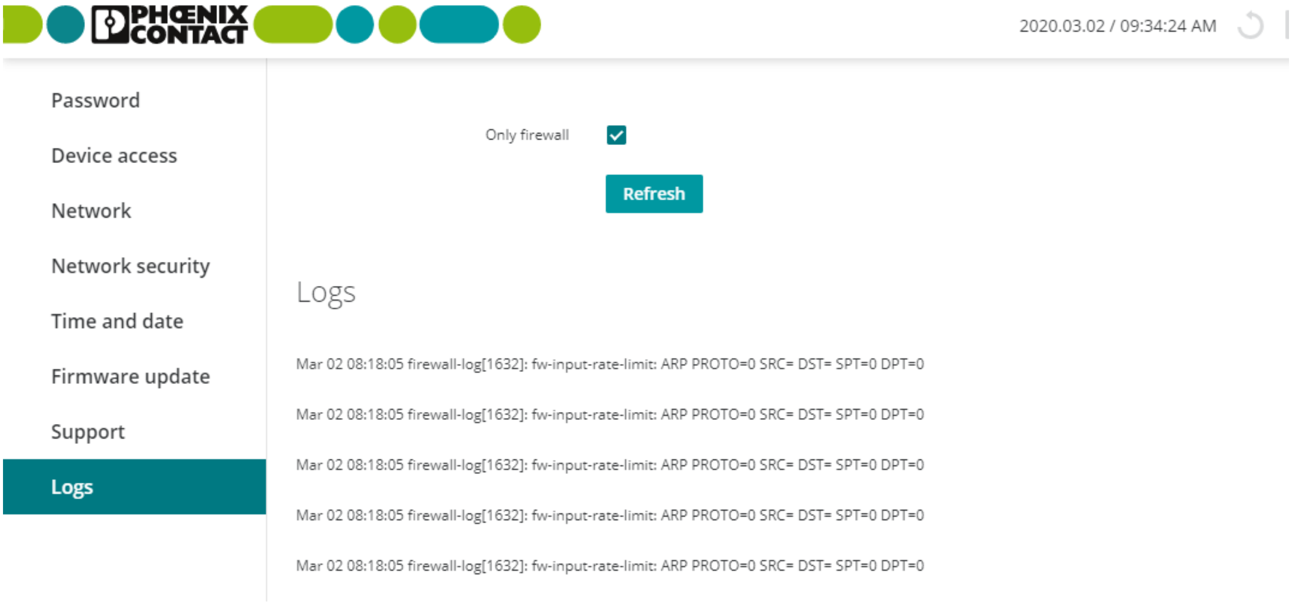
Procedure

- Open the **Support >> TCP Dump** menu.
- Select the **interface** whose network packets are to be analyzed.
- Enter the required **Options** to limit the analysis.
- To start the analysis, click on the **Start** button.
- To stop and download the analysis, click on the **Stop** button.

⇒ The result of the analysis was saved to a file (*.*pcap*), downloaded and deleted from the device.

Menu: Support >> TCP Dump		
	Interface	Only data packets that are sent or received via the selected network interface are analyzed. Net zone 1: – **eth0** Net zone 2: – **lan0** – **lan1** – **lan2** – **lan3**
	Options	Options can be used to limit the packet analysis to a selection of the elements below. Options can be linked via the logical operators “*and*, *or*, *not*”. *Example: “tcp and net 192.168.1.0/24 and not port 443”*
	Available options:	
	tcp	TCP protocol
	udp	UDP protocol
	arp	ARP protocol
	icmp	ICMP protocol
	esp	ESP protocol
	host <ip>	IPv4 address
	port <1-65535>	Network port (single port number)
	net <nw_cidr>	Network (in CIDR format, e.g., 192.168.1.0/24)
	and, or, not	Logic operators
	Start (button)	A running analysis can be started via this button.
	Stop (button)	A running analysis can be stopped via this button. The acquired packet contents are summarized in a file (*.*pcap*) and can be downloaded from the device. Afterwards, the file is deleted from the device. The time of the file download is indicated in the file name as follows: <YYYY-MM-DD_hh:mm:ss> (Example: *tcpdump_2019-10-09_22_00_00.pcap*)

11 Menu: Logs



Only firewall ☑

Logs

```
Mar 02 08:18:05 firewall-log[1632]: fw-input-rate-limit: ARP PROTO=0 SRC= DST= SPT=0 DPT=0
Mar 02 08:18:05 firewall-log[1632]: fw-input-rate-limit: ARP PROTO=0 SRC= DST= SPT=0 DPT=0
Mar 02 08:18:05 firewall-log[1632]: fw-input-rate-limit: ARP PROTO=0 SRC= DST= SPT=0 DPT=0
Mar 02 08:18:05 firewall-log[1632]: fw-input-rate-limit: ARP PROTO=0 SRC= DST= SPT=0 DPT=0
Mar 02 08:18:05 firewall-log[1632]: fw-input-rate-limit: ARP PROTO=0 SRC= DST= SPT=0 DPT=0
```

Figure 11-1 View log entries

Menu: Logs

Logs

Logging refers to the recording of messages relating to events that occurred (e.g., configuration changes, application of firewall rules, error messages).

Log entries are recorded in the RAM of the device. Once the memory space has been used up, the oldest log entries are automatically overwritten by new entries. When the device is switched off, all log entries will be deleted.

Only the first packet of data connections (e.g. UDP, TPC or ICMP) is logged (if logging is activated), since the connections are subject to *connection tracking*.

Log entries are categorized differently and marked accordingly with specific prefixes.

Firewall logging

Log entries relating to the firewall (-*fw* prefix) are created when the creation of log entries has been activated accordingly.

Log prefixes

forward = Relates to the firewall (*routing*/*stealth*) for continuous data traffic:

- **fw-forward** = A routing firewall rule was applied to a package.
- **fw-forward-policy** = A package **for which no rules have been defined** was rejected.
- **fw-forward-testmode** = Relates to entries (*Test mode alarms*) created by means of the *Firewall test mode* function.

Menu: Logs		
	input = Relates to the *incoming firewall* for accessing the device: – **fw-input** = An *incoming firewall* rule was applied to a package. – **fw-input-policy** = A package, **for which no rules have been defined**, was rejected. – **fw-input-dnscache** = Relates to accessing the DNS server of the device. – **fw-input-rate-limit** = Due to excessive access to the device during a defined period of time (e.g., via HTTPS), the data rate was throttled.	
	Firewall only	When the function is activated, only the log entries relating to the firewall (*Firewall - routing/stealth* and *incoming firewall*) will be displayed. When the function is deactivated, all log entries will be displayed. **Default setting:** activated
	Buttons	**Update** Click the **Update** button to refresh the log entries display.

12 Appendix

12.1 Using the RESTful Configuration API

The device can be configured via the web-based management, but also via the *RESTful Configuration API* (short: *Config API*).

Only experienced users should use the *Config API*.

As a machine-to-machine interface, the *RESTful Configuration API* enables automated and dynamic control and configuration of the device.

See “*FL MGUARD 1000 – RESTful Configuration API”* user manual, available at phoenixcontact.net/product/1153078).

12.2 Using smart mode

The use of *smart mode* is described in the “*FL MGUARD 1000 – Installation and startup*” user manual (UM EN FL MGUARD 1000).

Available in the download area of the corresponding product page in the Phoenix Contact web shop, for example, under phoenixcontact.net/product/1153078.

Using the *smart mode*, device functions can be called without access to one of the management interfaces of the device (WBM or *Config API*).

The following functions are available:

- Restoring the configuration access
- Restoring the factory settings (irrevocable deletion of all files)
- Update from SD card

Please observe the following notes

General terms and conditions of use for technical documentation

Phoenix Contact reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any technical changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular user documentation) does not constitute any further duty on the part of Phoenix Contact to furnish information on modifications to products and/or technical documentation. You are responsible to verify the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed.

In general, the provisions of the current standard Terms and Conditions of Phoenix Contact apply exclusively, in particular as concerns any warranty liability.

This manual, including all illustrations contained herein, is copyright protected. Any changes to the contents or the publication of extracts of this document is prohibited.

Phoenix Contact reserves the right to register its own intellectual property rights for the product identifications of Phoenix Contact products that are used here. Registration of such intellectual property rights by third parties is prohibited.

Other product identifications may be afforded legal protection, even where they may not be indicated as such.

How to contact us

Internet

Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at:
phoenixcontact.com

Make sure you always use the latest documentation.
It can be downloaded at:
phoenixcontact.net/products

Subsidiaries

If there are any problems that cannot be solved using the documentation, please contact your Phoenix Contact subsidiary.
Subsidiary contact information is available at phoenixcontact.com.

Published by

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
GERMANY

PHOENIX CONTACT Development and Manufacturing, Inc.
586 Fulling Mill Road
Middletown, PA 17057
USA

Should you have any suggestions or recommendations for improvement of the contents and layout of our manuals, please send your comments to:
tecdoc@phoenixcontact.com

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Phone: +49 5235 3-00
Fax: +49 5235 3-41200
E-mail: info@phoenixcontact.com
phoenixcontact.com

108420__en_03
Order No. —03