Configuration of the mGuard security appliances
Firmware 8.9

User Manual

PHOENIX CONTACT
INSPIRING INNOVATIONS

User Manual

Configuration of the mGuard security appliances (Reference Manual)

Firmware 8.9

2025-06-05

Designation: UM EN MGUARD 8.9

Revision: 19

Order No.: —

This user manual is valid for the mGuard software release 8.9 when using devices of the mGuard product range (for further information see mGuard firmware – Version 8.9.x – Release Notes):

FL MGUARD RS4000 TX/TX (VPN)
FL MGUARD RS4000 TX/TX VPN-M
FL MGUARD RS4000-P
FL MGUARD RS2000 TX/TX VPN
FL MGUARD RS2000 TX/TX-B
FL MGUARD RS4004 TX/DTX (VPN)
FL MGUARD RS2005 TX VPN
FL MGUARD CORE TX (VPN)
TC MGUARD RS4000 3G VPN
TC MGUARD RS2000 3G VPN
TC MGUARD RS4000 4G VPN
TC MGUARD RS2000 4G VPN
TC MGUARD RS4000 4G VZW VPN
TC MGUARD RS2000 4G VZW VPN
TC MGUARD RS4000 4G ATT VPN
TC MGUARD RS2000 4G ATT VPN
FL MGUARD CENTERPORT
mGuard centerport 2U (Innominate)
FL MGUARD GT/GT (VPN)
FL MGUARD PCI(E)4000 (VPN)
FL MGUARD SMART2 (VPN)
FL MGUARD DELTA TX/TX (VPN)

Please observe the following notes

User group of this manual

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

– Qualified electricians or persons instructed by them, who are familiar with applicable standards and other regulations regarding electrical engineering and, in particular, the relevant safety concepts.
– Qualified application programmers and software engineers, who are familiar with the safety concepts of automation technology and applicable standards.

Explanation of symbols used and signal words

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety measures that follow this symbol to avoid possible injury or death.

There are three different categories of personal injury that are indicated with a signal word.

DANGER This indicates a hazardous situation which, if not avoided, will result in death or serious injury.

WARNING This indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION This indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

This symbol together with the signal word **NOTE** and the accompanying text alert the reader to a situation which may cause damage or malfunction to the device, hardware/software, or surrounding property.

This symbol and the accompanying text provide the reader with additional information or refer to detailed sources of information.

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

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

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.

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.

Table of Contents

1 mGuard basics

The mGuard protects IP data links by combining the following functions:

- Industrial security network router (with built-in 4 or 5-port switch and DMZ port depending on the model).
- VPN router for secure data transmission via public networks (hardware-based DES, 3DES, and AES encryption, IPsec and OpenVPN protocol).
- Configurable firewall for protection against unauthorized access. The dynamic packet filter inspects data packets using the source and destination address and blocks undesired data traffic.

1.1 Basic properties of the mGuards

The mentioned properties are not guaranteed properties, as they are basically dependent on the respective device and on installed licenses.

Network features

- Stealth (auto, static, multi), router (static, DHCP client), PPPoE (for DSL), PPTP (for DSL), and modem
- VLAN
- DHCP server/relay on the internal and external network interfaces
- DNS cache on the internal network interface
- Dynamic routing (OSPF)
- GRE tunneling
- Administration via HTTPS and SSH
- Optional conversion of DSCP/TOS values (Quality of Service)
- Quality of Service (QoS)
- LLDP
- MAU management
- SNMP

Firewall features

- Stateful packet inspection
- Anti-spoofing
- IP filter
- L2 filter (only in stealth mode)
- NAT with FTP, IRC, and PPTP support (only in “Router” network mode)
- 1:1 NAT (only in “Router” network mode)
- Port forwarding (not in “Stealth” network mode)
- Individual firewall rules for different users (user firewall)
- Individual rule records as action (target) of firewall rules (apart from user firewall or VPN firewall)

Anti-virus features

- CIFS integrity check of network drives for changes to specific file types (e.g., executable files)

VPN features (IPsec)

- Protocol: IPsec (tunnel and transport mode, XAuth/Mode Config)
- IPsec encryption in hardware with DES (56 bits), 3DES (168 bits), and AES (128, 192, 256 bits)
- Packet authentication: MD5, SHA-1, SHA-265, SHA-384, SHA-512

- Internet Key Exchange (IKE) with main and quick mode
- Authentication via:
  - Pre-shared key (PSK)
  - X.509v3 certificates with public key infrastructure (PKI) with certification authority (CA), optional certificate revocation list (CRL), and the option of filtering by subject

  or
  - Remote certificate, e.g., self-signed certificates
- Detection of changing peer IP addresses via DynDNS
- NAT traversal (NAT-T)
- Dead Peer Detection (DPD): detection of IPsec connection aborts
- IPsec/L2TP server: connection of IPsec/L2TP clients
- IPsec firewall and 1:1 NAT
- Default route via VPN tunnel
- Data forwarding between VPNs (hub and spoke)
- Depending on the license: up to 250 VPN tunnels, in the case of mGuard centerport (Innominate)/FL MGUARD CENTERPORT up to 3000 active VPN tunnels
- Hardware acceleration for encryption in the VPN tunnel (except for mGuard centerport (Innominate)/FL MGUARD CENTERPORT)

VPN features (OpenVPN)

- OpenVPN client
- OpenVPN encryption with Blowfish, AES (128, 192, 256 bits)
- Dead Peer Detection (DPD)
- Authentication via user identifier, password or X.509v3 certificate
- Detection of changing peer IP addresses via DynDNS
- OpenVPN firewall and 1:1 NAT
- Routes via VPN tunnels can be configured statically and learned dynamically
- Data forwarding between VPNs (hub and spoke)
- Depending on the license: up to 50 VPN tunnels

Additional features

- Remote Logging
- VPN/firewall redundancy (depending on the license)
- Administration using SNMP v1 - v3 and Phoenix Contact Device Manager (mGuard device manager (FL MGUARD DM))
- PKI support for HTTPS/SSH remote access
- Can act as an NTP and DNS server via the LAN interface
- Compatible with mGuard Secure Cloud
- Plug-n-Protect technology
- Tracking and time synchronization via GPS/GLONASS positioning system (product-dependent)
- COM Server

Support

In the event of problems with your mGuard, please contact your supplier.

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

1.2 Typical application scenarios

This section describes various application scenarios for the mGuard.

- Stealth mode (Plug-n-Protect)
- Network router
- DMZ (demilitarized zone)
- VPN gateway
- WLAN via VPN tunnel
- Resolving network conflicts
- Mobile router via integrated mobile network modem

1.2.1 Stealth mode (Plug-n-Protect)

In **stealth mode**, the mGuard can be positioned between an individual computer and the rest of the network.

The settings (e.g., for firewall and VPN) can be made using a web browser under the URL https://1.1.1.1/.

No configuration modifications are required on the computer itself.

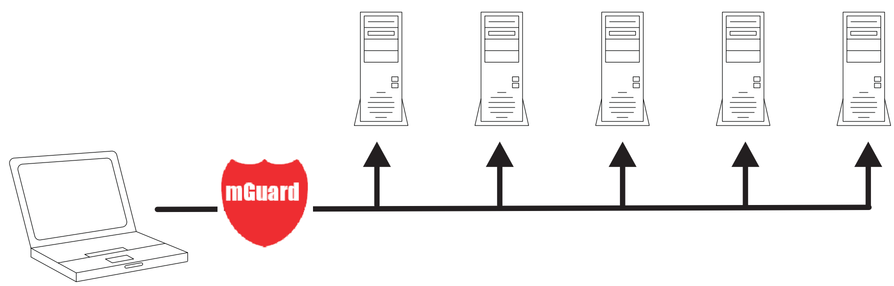


Figure 1-1 Stealth mode (Plug-n-Protect)

1.2.2 Network router

When used as a **network router**, the mGuard can provide the Internet connection for several computers and protect the company network with its firewall.

One of the following network modes can be used on the mGuard:

- *Router*, if the Internet connection is, for example, via a DSL router or a permanent line.
- *PPPoE*, if the Internet connection is, for example, via a DSL modem and the PPPoE protocol is used (e.g., in Germany).
- *PPTP*, if the Internet connection is, for example, via a DSL modem and the PPTP protocol is used (e.g., in Austria).
- *Modem*, if the Internet connection is via a serial connected modem (compatible with Hayes or AT command set).
- *Built-in mobile network modem*, mobile router via integrated mobile network modem

For computers in the Intranet, the mGuard must be specified as the default gateway.

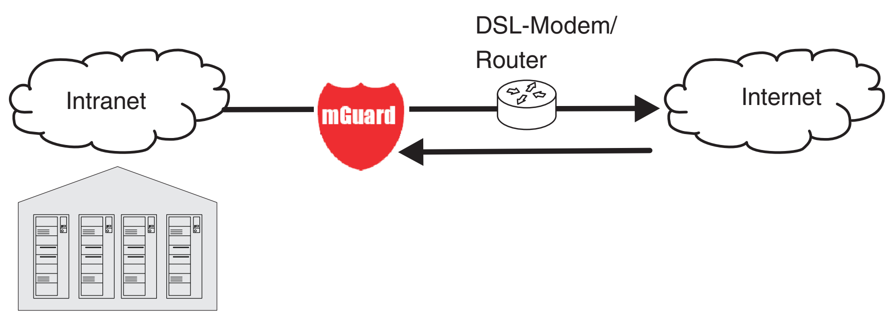


Figure 1-2 Network router

1.2.3 DMZ

A **DMZ** (demilitarized zone) is a protected network that is located between two other networks. For example, a company's website may be in the DMZ so that new pages can only be copied to the server from the Intranet via FTP. However, the pages can be read from the Internet via HTTP.

IP addresses within the DMZ can be public or private, and the mGuard, which is connected to the Internet, forwards the connections to private addresses within the DMZ by means of port forwarding.

A DMZ scenario can be established either between two mGuards (see Figure 1-3) or via a dedicated DMZ port of the TC MGUARD RS4000 3G, TC MGUARD RS4000 4G or FL MGUARD RS4004.

The DMZ port is only supported in router mode and requires at least one IP address and a corresponding subnet mask. The DMZ does not support any VLANs.

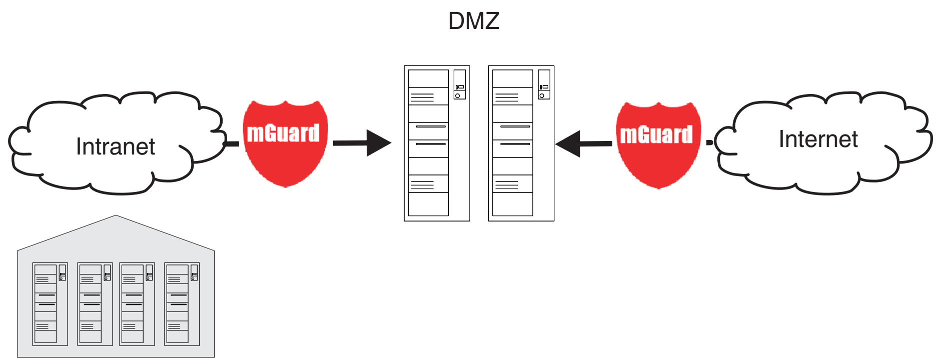


Figure 1-3 DMZ

1.2.4 VPN gateway

The **VPN gateway** provides company employees with encrypted access to the company network from home or when traveling. The mGuard performs the role of the VPN gateway.

IPsec-capable VPN client software must be installed on the external computers or failing that, the computer is equipped with an mGuard.

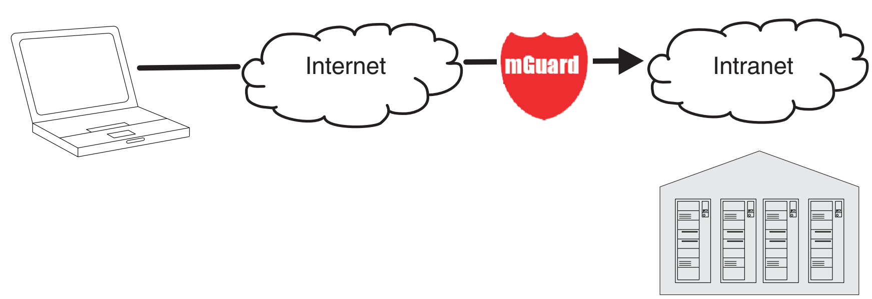


Figure 1-4 VPN gateway

1.2.5 WLAN via VPN

WLAN via VPN is used to connect two company buildings via a WLAN path protected using IPsec. The adjacent building should also be able to use the Internet connection of the main building.

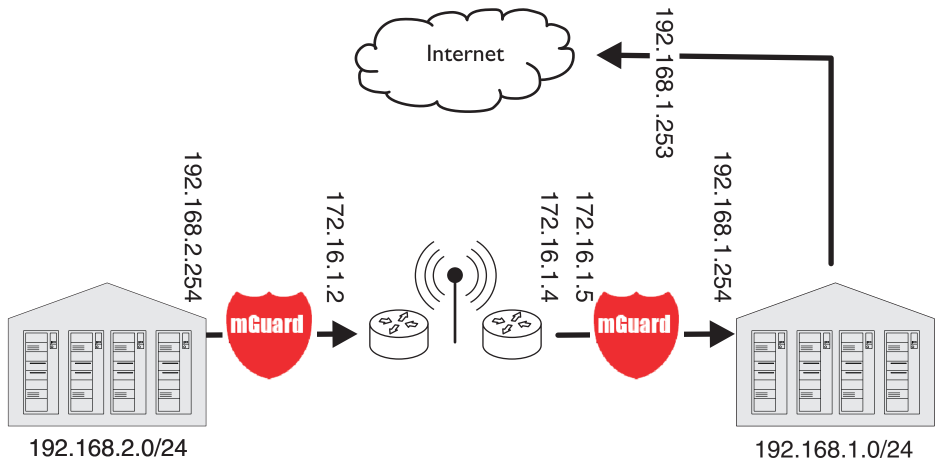


Figure 1-5 WLAN via VPN

In this example, the mGuards were set to *router* mode and a separate network with 172.16.1.x addresses was set up for the WLAN.

To provide the adjacent building with an Internet connection via the VPN, a default route is set up via the VPN:

Tunnel configuration in the adjacent building

Connection type	Tunnel (network <-> network)
Address of the local network	192.168.2.0/24
Address of the remote network	0.0.0.0/0

In the main building, the corresponding counterpart is configured:

Tunnel configuration in the main building

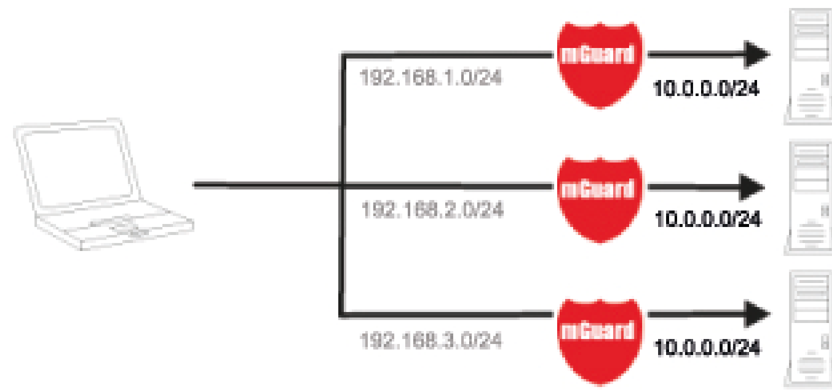
Connection type	Tunnel (network <-> network)
Local network	0.0.0.0
Address of the remote network	192.168.2.0/24

The default route of an mGuard usually uses the WAN port. However, in this case the Internet can be accessed via the LAN port:

Default gateway in the main building:

IP address of the default gateway	192.168.1.253

1.2.6 Resolving network conflicts



Resolving network conflicts

In the example, the networks on the right-hand side should be accessible to the network or computer on the left-hand side. However, for historical or technical reasons the networks on the right-hand side overlap.

The 1:1 NAT feature of the mGuard can be used to translate these networks to other networks, thereby resolving the conflict.

(1:1 NAT can be used in normal routing and in IPsec tunnels and in OpenVPN connections.)

2 Configuration help

2.1 Secure encryption

The mGuard generally offers the option to use different encryption and hash algorithms.

> Some of the algorithms available are dated and are no longer regarded as reliable. This is why they are not to be recommended. Due to downwards compatibility, they can continue to be selected and used in mGuard.

In the following areas of the mGuard, the user must ensure that secure encryption and hash algorithms are used:

– IPsec VPN connections
– OpenVPN connections
– Shell Access (SSH)
– HTTPS Web Access (TLS/SSL)
– Encrypted State Synchronization of redundancy pairs (up to 8.7.1)

The secure use of encryption is explained in the following sections.

Further information can for example be found in the technical directive of the Federal office for information security: “BSI TR-02102 Cryptographic procedure: recommendations and key lengths”.

Using secure encryption and hash algorithms

Phoenix Contact recommends using encryption and hash algorithms according to the following table.

The following generally applies: the longer the key length (in bits), which is used in the encryption algorithm (specified by the appended number), the more secure it is.

Encryption	**Algorithm**	**Use**
	AES-256 AES-192 AES-128	Recommended
	3DES Blowfish	Do not use, if possible
	DES	Do not use
Hash/checksum	**Hash function**	**Use**
	SHA-512 SHA-384 SHA-256	Recommended
	SHA-1	Do not use, if possible
	MD5	Do not use

Use of secure SSH clients

Establishing encrypted SSH connections to the mGuard is initiated by the SSH client used. If the SSH client uses dated and thus insecure encryption algorithms, these are generally accepted by the mGuard.

Always use **Current SSH clients** (e.g. *putty*), to avoid use of weak encryption algorithms.

Use of secure web browsers

Establishing encrypted HTTPS connections (TLS/SSL) to the mGuard is initiated by the web browser used. If the web browser uses dated and thus insecure encryption algorithms, these are generally accepted by the mGuard.

Always use **Current web browsers** to avoid use of weak encryption algorithms.

Creation of secure X.509 certificates

X.509 certificates are generated using various software tools.

Always use **Current program versions** of the software tools to avoid use of weak encryption algorithms when creating X.509 certificates. The MD5 hash algorithm should not be used and SHA-1 not used as far as possible.

When creating X.509 certificates, use **key lengths of at least 2048 bits**.

Use of X.509 certificates instead of Pre-Shared Keys (PSK)

Pre-shared key (PSK) authentication in VPN connections is considered insecure and should no longer be used. For security reasons, use X.509 certificates for authentication.

2.2 Suitable web browsers

The device is configured via a graphic user interface in the web browser.

Always use **Current web browsers** to avoid use of weak encryption algorithms.

Current versions of the following web browsers are supported:
- Mozilla Firefox
- Google Chrome
- Microsoft Edge

Limitation of login attempts

In the event of a Denial of Service attack, services are intentionally made unable to function. To prevent this type of attack, the mGuard is provided with a throttle for different network requests.

This feature is used to count all the connections going out from one IP address and using a specific protocol. When a certain number of connection attempts is counted, the throttle becomes effective. The throttle is reset if there are no further connection attempts for 30 seconds.

The number of connection attempts that lead to activation of the throttle depends on the protocol used:
- 32 when using HTTPS
- 6 when using SSH, SNMP, COM server

2.3 User roles

root	User role without restrictions
admin	Administrator
netadmin	Administrator for the network only
audit	Auditor/tester
mobile	Sending text messages

The predefined users (*root*, *admin*, *netadmin*, *audit*, and *mobile*) have different permissions.
- The *root* user has unrestricted access to the mGuard.
- The *admin* user also has unrestricted functional access to the mGuard, however the number of simultaneous SSH sessions is limited.
- Permissions are explicitly assigned to the *netadmin* user via the mGuard device manager (FL MGUARD DM). This user only has read access to the other functions. Passwords and private keys cannot be read by this user.
- The *audit* user only has read access to all functions. By default, the *audit* user role can only be activated via the mGuard device manager (FL MGUARD DM), in the same way as *netadmin*.
- The *mobile* user can send text messages with the mGuard using a CGI script. Further functions cannot be accessed by the *mobile* user (see "CGI interface" on page 457).

2.4 Input help during configuration (system messages)

With firmware 8.0 or later, modified or invalid entries are highlighted in color on the web interface.

System messages which explain why an entry is invalid, for example, are also displayed.

> In order to support this, JavaScript must be enabled in the web browser used.

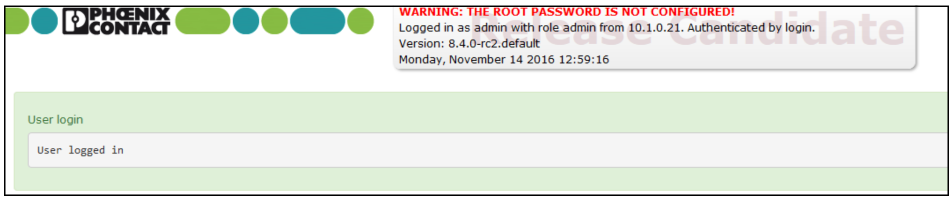


Figure 2-1 Example system message

- **Modified entries** are highlighted in **green** on the relevant page and in the associated menu item until the changes are applied or reset. In the case of tables, it is only indicated that a table row has been modified or removed; the modified value is not indicated.
- **Invalid entries** are highlighted in **red** on the relevant page and tab and in the associated menu item.

The modified or invalid entries remain highlighted even when you close a menu.

When necessary, information relating to the system is displayed at the top of the screen.

2.5 Using the web interface

You can click on the desired configuration via the menu on the left-hand side, e.g., “Management, Licensing”.

The page is then displayed in the main window – usually in the form of one or more tab pages – where settings can be made. If the page is organized into several tab pages, you can switch between them using the *tabs* at the top.

Working with tab pages

– You can make the desired entries on the corresponding tab page (see also "Working with sortable tables" on page 25).
– You can return to the previously accessed page by clicking on the **“Back”** button located at the bottom right of the page, if available.

Modifying values

If you modify the value of a variable on the web interface, the change will not be applied until you click on the **Save** icon. The variable name for the modified variable is then displayed in green.

In order to make it easier to trace the changes, the full menu path for the modified variable is also displayed in green: Menu >> Submenu >> Tab page >> Section >> Variable.

Entry of impermissible values

If you enter an impermissible value (e.g., an impermissible number in an IP address) and click on the **Save** icon, the relevant variable name is displayed in red and an error message is usually displayed.

In order to make it easier to trace the error, the full menu path for the modified variable is also displayed in red: Menu >> Submenu >> Tab page >> Section >> Variable.

Entry of a timeout

A timeout can be entered in three ways:
– In seconds [ss]
– In minutes and seconds [mm:ss]
– In hours, minutes, and seconds [hh:mm:ss]

The three possible values are each separated by a colon. If only one value is entered, it will be interpreted as seconds, two values as minutes and seconds, three values as hours, minutes and seconds. The values for minutes and seconds may be greater than 59. After the values have been applied, they will always be shown as [hh:mm:ss] regardless of the format they were entered in (if you enter 90:120 for example, it will be shown as 1:32:00).

Global icons

The following icons are located at the top of every page:

Logout

To **log out** after configuration access to the mGuard.

If the user does not log out, he/she is logged out automatically if there has been no further activity and the time period specified by the configuration has elapsed. Access can only be restored by logging in again.

Reset

Reset to the original values. If you have entered values on one or more configuration pages and have not yet activated them (by clicking on **Save**), you can reset the modified values to the original values by clicking on **Reset**.

Save

To apply the settings on the device, you must click on **Save**.

Please note that changes made elsewhere (highlighted in green) will also be applied.

Session timeout

01:29:53

Displays the time remaining until the logged in user will be logged out of the web interface. Clicking on the time display resets the timeout time to the configured output value (see "Management >> Web Settings >> General" on page 70).

Online help

Link to the **online help** for the installed firmware version.

The online help can only be accessed when an Internet connection is established and the firewall is set accordingly.

Clicking on the icon opens the corresponding section of the mGuard firmware user manual for the page contents in a new tab/window of the web browser.

The mGuard firmware user manual is also available in a **PDF version** and can be downloaded on the corresponding product pages at phoenixcontact.net/products or help.mguard.com.

Working with sortable tables

Many settings are saved as data records. Accordingly, the adjustable parameters and their values are presented in the form of table rows. If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. Therefore, note the order of the entries, if necessary. The order can be changed by moving table rows up or down.

With tables you can:

– Insert rows to create a new data record with settings (e.g., the firewall settings for a specific connection)
– Move rows (i.e., re-sort them)
– Delete rows to delete the entire data record

Inserting rows

1. Click on the ⊕ **Insert Row** icon in the row below which a new row is to be inserted.
2. A new row is inserted below the selected row.
   The inserted row is displayed in green until the change has been applied.

Moving rows

1. Move the mouse pointer over the row number (seq.) of the row that you wish to move.
   The mouse pointer changes to a cross .
2. Left-click in the desired row and hold down the mouse button.
   The row is deleted from the existing sequence.
3. With the mouse, move the selected row to the desired position.
   A border around the target row shows where the row will be inserted.
4. Release the mouse button.
5. The row is moved to the position marked with a box.

Deleting rows

1. Click on the **Delete Row** icon in the row that you wish to delete.
2. Then click on the **Save** icon to apply the change.

2.6 CIDR (Classless Inter-Domain Routing)

IP netmasks and CIDR are methods of notation that combine several IP addresses to create a single address area. An area comprising consecutive addresses is handled like a network.

To specify an area of IP addresses for the mGuard, e.g., when configuring the firewall, it may be necessary to specify the address area in CIDR format. In the table below, the left-hand column shows the IP netmask, while the right-hand column shows the corresponding CIDR format.

IP netmask	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

Example: 192.168.1.0/255.255.255.0 corresponds to CIDR: 192.168.1.0/24

2.7 Network example diagram

The following diagram shows how IP addresses can be distributed in a local network with subnetworks, which network addresses result from this, and how the details regarding additional internal routes may look for the mGuard.

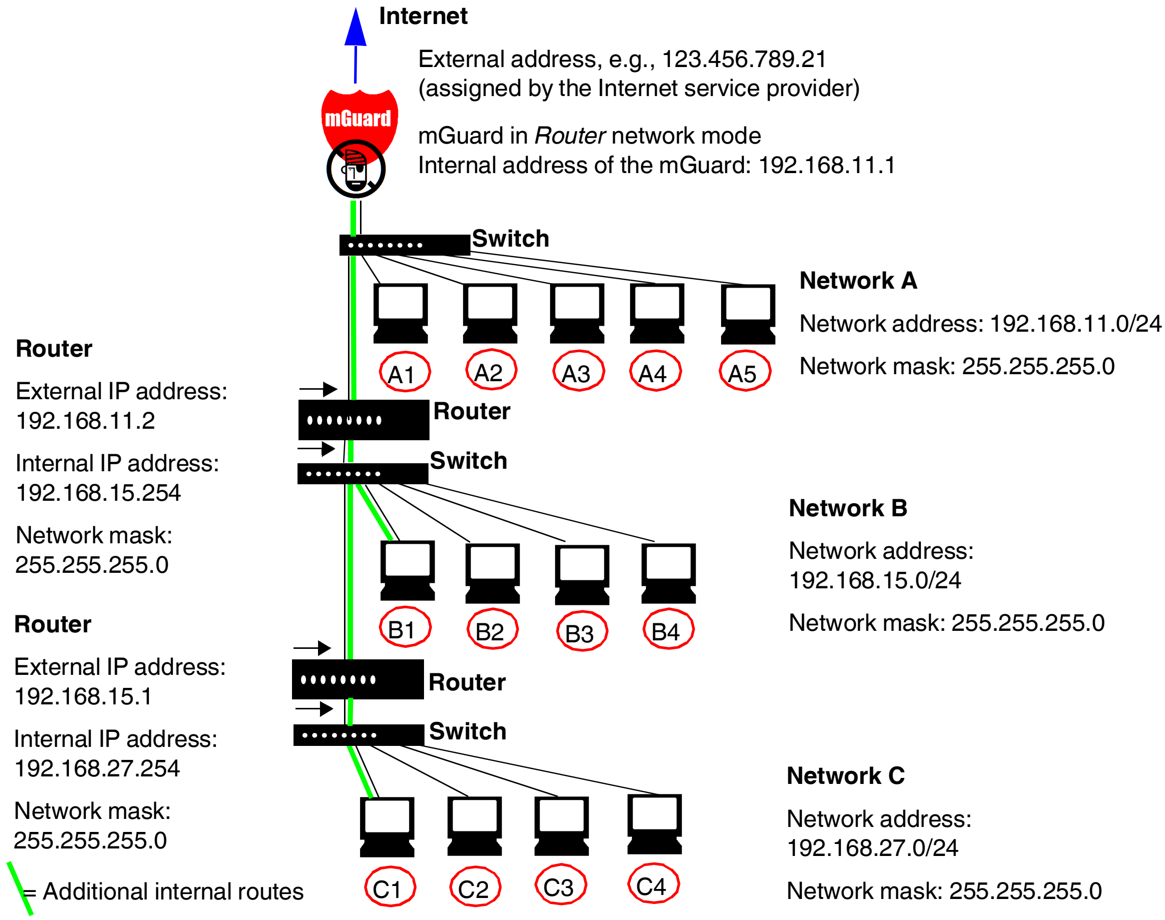


Table 2-1 Network example diagram

Network A	**Computer**	**A1**	**A2**	**A3**	**A4**	**A5**
	IP address	192.168.11.3	**192.168.11.4**	**192.168.11.5**	**192.168.11.6**	**192.168.11.7**
	Network mask	255.255.255.0	**255.255.255.0**	**255.255.255.0**	**255.255.255.0**	**255.255.255.0**
Network B	**Computer**	**B1**	**B2**	**B3**	**B4**	**Additional internal routes** Network: 192.168.15.0/24 Gateway: 192.168.11.2 Network: 192.168.27.0/24 Gateway: 192.168.11.2
	IP address	192.168.15.2	**192.168.15.3**	**192.168.15.4**	**192.168.15.5**	
	Network mask	255.255.255.0	**255.255.255.0**	**255.255.255.0**	**255.255.255.0**	
Network C	**Computer**	**C**	**C2**	**C3**	**C4**	
	IP address	192.168.27.1	**192.168.27.2**	**192.168.27.3**	**192.168.27.4**	
	Network mask	255.255.255.0	**255.255.255.0**	**255.255.255.0**	**255.255.255.0**	

2.8 LED status indicator and blinking behavior

With the help of built-in LED diodes, mGuard devices indicate different system states. This can be status, alarm or error messages.

Detailed information on the LEDs can be found in the Appendix (see "LED status indicator and blinking behavior" on page 459).

3 Changes compared to the previous version

3.1 Overview of the changes in Version 8.9

For a more detailed overview of the changes, see *mGuard-Firmware Version 8.9.x – Release Notes*.

The following functions have been added to or removed from firmware Version 8.9:

– Time synchronization with some NTP clients, especially PLC systems, can be optimized (see variable "‘discard minimum1‘" on page 50).
– The establishment of a data connection via the cellular modem can be optimized (see variable "Data roaming" on page 165).

3.2 Overview of the changes in Version 8.8

For a more detailed overview of the changes, see *mGuard-Firmware Version 8.8.x – Release Notes*.

The following functions have been added to or removed from firmware Version 8.8:

– Filtering TCP packages with set URGENT flag
– Encrypted state synchronization in activated firewall and VPN redundancy is no longer supported

Filtering TCP packages with set URGENT flag

IT security experts have discovered eleven vulnerabilities in the real-time operating system VxWorks (*URGENT/11*). Six of the vulnerabilities allow an attacker to install and execute code on affected devices (*Remote Code Execution*):

– CVE-2019-12256
– CVE-2019-12257
– CVE-2019-12255
– CVE-2019-12260
– CVE-2019-12261
– CVE-2019-12263

Pre-connected mGuard devices can use their firewall functionality to protect affected devices from related attacks (see detailed description at phoenixcontact.com).

mGuard-Firmware version 8.8.0 provides a new function for this purpose which can be used to block TCP packets that have an URGENT flag set in the TCP header (see Section 8.1.7: *Block URGENT-flagged TCP traffic*).

Encrypted state synchronization in activated firewall and VPN redundancy is no longer supported

With mGuard firmware 8.8.0, the "Encrypted State Synchronization" in activated firewall and VPN redundancy is no longer available.

An update to firmware version 8.8.0 is only possible if the function "Encrypted State Synchronization" has been deactivated before.

3.3 Overview of the changes in Version 8.7

For a more detailed overview of the changes, see *mGuard-Firmware Version 8.7.x – Release Notes*.

The following functions have been added to firmware Version 8.7:

- QoS features in VPN connections are no longer supported
- New versions of the MEM PLUG configuration memory are supported

QoS features in VPN connections are no longer supported

The following *Quality of Service* features have been removed and are no longer supported in VPN connections:

- *Egress Queues (VPN)*
- *Egress Rules (VPN)*

New versions of the MEM PLUG configuration memory are supported

New versions of the MEM PLUG external configuration memory with higher capacity for the FL MGUARD GT/GT device are supported.

3.4 Overview of the changes in Version 8.6

For a more detailed overview of the changes, see *mGuard-Firmware Version 8.6.x – Release Notes*.

The following functions have been added to firmware Version 8.6:

- The BusyBox program was updated
- SNMPv3 user name and password can be changed
- Simplified search for firewall rules on the basis of log entries
- NTP time synchronization via VPN
- In "Autodetect" stealth mode, the mGuard can use the DNS server of its (protected) client
- DHCP server on the DMZ- interface
- SSH remote access for the user root can be deactivated

The BusyBox program was updated

The BusyBox program was updated to Version 1.26.1.

Users who run UNIX service programs or shell scripts (e.g., rollout scripts) on the mGuard should check them for changed behavior.

SNMPv3 user name and password can be changed

The SNMPv3 user name "*admin*" specified in earlier mGuard versions can be changed via the web interface, an ECS configuration, or a rollout script. The same applies for the corresponding SNMPv3 password (see "Management >> SNMP" on page 96).

Simplified search for firewall rules on the basis of log entries

Clicking a log entry of the network security log opens the configuration page containing the firewall rule that caused the log entry (see "Logging >> Browse Local Logs" on page 413).

NTP time synchronization via VPN

The request from the NTP server for time synchronization can be performed via a VPN tunnel if a suitable one is configured (see "NTP server" on page 50).

In "Autodetect" stealth mode, the mGuard can use the DNS server of its (protected) client

In "*Autodetect"* stealth mode the mGuard can automatically determine the used DNS server of its (protected) client, and can also use it. For this, "*Provider defined (i. e. via PPPoE or DHCP)"* must be selected in the DNS settings as nameserver (see "Servers to query" on page 206).

DHCP server on the DMZ- interface

The mGuard can function as DHCP server on the DMZ interface and automatically assign a network configuration to querying clients via the DHCP protocol (see "DMZ DHCP" on page 216).

SSH remote access for the user root can be deactivated

SSH access via the external interface (WAN) can be deactivated for the user "*root*" (see "Enable SSH access as user root" on page 54).

3.5 Overview of the changes in Version 8.5

For a more detailed overview of the changes, see *mGuard-Firmware Version 8.5.x – Release Notes*.

The following functions have been added to firmware Version 8.5:

– Proxy authentication by means of VPN Path Finder
– SNMP trap “Service input/CMD”
– TLS authentication in OpenVPN connections
– Firewall functionality in mGuard devices of the RS2000 series
– The CIFS Anti-Virus Scan Connector function is no longer required
– 1:1 NAT in OpenVPN connections
– COM server functionality extended

Proxy authentication by means of VPN Path Finder

The Path Finder function of the gateway being initiated supports the proxy authentication mechanisms: “**NTLM**”, “**Basic**”.

SNMP trap “Service input/CMD”

The new hardware-based “**Service-input/CMD**” trap is sent if a service input/CMD is switched by a switch or button.

TLS authentication in OpenVPN connections

OpenVPN connections can also be protected by exchanging static pre-shared keys (TLS-PSK).

1:1 NAT in OpenVPN connections

A local 1:1 NAT can be used in OpenVPN connections.

Firewall functionality in mGuard devices of the RS2000 series

The previous functionality of the “2-click firewall” for mGuard devices from the RS2000 series has been extended. The creation of firewall rules and use of IP and port groups is now possible. Firewall access is recorded and represented in log files.

The CIFS Anti-Virus Scan Connector function is no longer required

The CIFS AV Scan Connector function is no longer required.

COM server functionality extended

The COM server functionality for the serial interface also supports packet lengths of 7 bits.

3.6 Overview of the changes in Version 8.4

The following functions have been added to firmware Version 8.4:

– Support for the LTE mobile network modem (4G)
– Automatic login with CDMA mobile network provider
– Restart of the mGuard via text message
– Modbus TCP (Deep Packet Inspection)
– Use of host names in IP groups (firewall rules)
– Restricted access (internal/external) for the mGuard NTP server
– Modified recovery procedure
– Log entry for CMD contact

Support for the LTE mobile network modem (4G)

mGuard devices with built-in LTE mobile network modem (4G) are supported.

Automatic login with CDMA mobile network provider

Login and activation of a device previously registered with the CDMA mobile network provider (Verizon – USA) is carried out automatically when the mobile network connection to the provider is established for the first time ("Mobile network cdma2000 OTASP Registration" on page 161).

Restart of the mGuard via text message

mGuard devices with integrated mobile network function can be restarted (rebooted) with a text message and the token contained in it (see "Restart" on page 120).

Modbus TCP (Deep Packet Inspection)

The mGuard can inspect incoming and outgoing Modbus TCP connections (Deep Packet Inspection), i.e., usually connections to TCP port 502, and filter them if required.

The rules for filtering Modbus TCP packets are configured in Modbus TCP rule records. These rule records can be selected in the following firewall tables as actions: general packet filter / DMZ / GRE / IPsec VPN / OpenVPN client / PPP (see "Modbus TCP" on page 284).

Use of host names in IP groups (firewall rules)

Host names can also be specified in IP groups in addition to IP addresses (DNS-based firewall rules).

The use of host names is therefore possible in firewall tables where IP groups can be selected (see "IP/Port Groups" on page 275): general packet filter / DMZ / GRE / IPsec VPN / OpenVPN client / NAT / user firewall.

Restricted access (internal/external) for the mGuard NTP server

Incoming requests to the NTP server of the mGuard via any interface can be restricted by means of firewall rules (see "Enable NTP time synchronization" on page 50).

Modified recovery procedure

Before performing the recovery procedure, the current device configuration is stored in a new configuration profile (“Recovery DATE”). Following the recovery procedure, the device starts with the default settings. The previously active configuration can be restored with or without changes via the recovery configuration profile.

Log entry for CMD contact

Switching a CMD contact (CMD 1–3) using the connected switch or button generates a log entry.

3.7 Overview of the changes in Version 8.3

The following functions have been added to firmware Version 8.3:

- Establishing OpenVPN connections
- Dynamic routing (OSPF)
- Support for GRE tunnels
- Support for the Path Finder function of the mGuard Secure VPN Client
- Use of IP and port groups
- New access check and modified test report creation (logging) for CIFS
- Improved display of the VPN status (IPsec)
- Improved timeout behavior for VPN connections
- New VPN license model
- Improved use of configuration profiles
- Optional use of the proxy server by the secondary external interface
- Support for XAuth and Mode Config (iOS support)

Establishing OpenVPN connections

As an OpenVPN client, the mGuard can establish VPN connections to peers which support OpenVPN as the server (see "OpenVPN Client menu" on page 365).

Dynamic routing (OSPF)

Support for the OSPF (Open Shortest Path First) dynamic routing protocol. As an OSPF router, the mGuard can dynamically learn the routes of neighboring OSPF routers and distribute its own as well as learned routes. This simplifies the configuration of complex network structures, since fewer routes have to be entered statically (see "Network >> Dynamic Routing" on page 221).

The OSPF routes can be learned and distributed via every selected interface (internal, external, DMZ) as well as via IPsec connections (with the aid of a GRE tunnel in the case of IPsec).

Support for GRE tunnels

The mGuard supports the use of GRE tunnels. It is therefore possible to encapsulate other network protocols and transport them in the form of a tunnel via the Internet Protocol (IP). This also enables the dynamic distribution of OSPF routes via IPsec connections (see "Network >> GRE Tunnel" on page 225).

Support for the Path Finder function (mGuard Secure VPN Client)

The “Path Finder” function enables the connection to be established by the mGuard Secure VPN Client when it is located behind a proxy server or a firewall (see "TCP encapsulation with enabled “Path Finder” function" on page 318).

Use of IP and port groups

IP and port groups enable the easy creation and management of firewall and NAT rules in complex network structures.

IP addresses, IP areas, and networks can be grouped in IP groups and identified by a name. Likewise, ports or port ranges can be grouped in port groups.

If a firewall or NAT rule is created, instead of IP addresses/IP areas or ports/port ranges, the IP or port groups can be selected directly in the corresponding fields and assigned the rule (see "IP/Port Groups" on page 275).

New access check and modified test report creation (logging) for CIFS

Access check

In order to prevent a comprehensive integrity check being aborted due to the absence of access permissions to the destination drive, access permission can be checked before the actual scan. This access check is much faster and generates a test report which can be downloaded and analyzed. If all access permissions are present, the integrity check can then be performed (see "CIFS Integrity Monitoring >> CIFS Integrity Checking" on page 300).

Test report (log file)

The old results of the integrity check are not deleted from the test report when a new test is performed. The new results are simply added to the report. When the report reaches a specified file size, it is stored as a backup file and a new test report is created. When this test report also reaches a specified file size, the backup file is overwritten with the new report and another report is created (see "Report" on page 307).

Improved display of the VPN status (IPsec)

The status page for displaying information about VPN connections has been revised. The status of all VPN connections is clearly displayed ("IPsec VPN >> IPsec Status" on page 363).

New VPN license model

The new VPN license model allows tunnel groups to be created with all VPN licenses.

The license no longer limits the number of tunnels established, but instead the number of connected peers (VPN peers). If several tunnels are established to a peer, only one peer is counted, which is an improvement over the old model.

The license status, i.e., the total number of licensed peers and the number of licensed peers currently used, is clearly shown in the “IPsec VPN” and “OpenVPN Client” menus.

Improved use of configuration profiles

Before the settings of saved configuration profiles are applied, the changes to the current configuration can be shown and therefore checked. The changes can be applied unmodified. However, individual settings can also be freely modified before being applied (see "Configuration Profiles" on page 91).

Improved timeout behavior for VPN connections

A timeout can stop a VPN connection that was started via a button on the web interface, text message, a switch, a pushbutton or the script nph-vpn.cgi. This VPN connection is terminated after the timeout has elapsed and is set to the “Stopped” state.

A VPN connection that is initiated (established) by data traffic is also terminated by a timeout. However, this VPN connection is not set to the “Stopped” state after the timeout has elapsed, instead it remains in the “Started” state. When data traffic resumes, the VPN connection is established again. This function is particularly useful when using the mobile interface (3G).

Support for XAuth and Mode Config (iOS support)

The mGuard now supports the “Extended Authentication” (XAuth) authentication mode and the frequently required “Mode Config” protocol extension, including split tunneling as server and as client (e.g., support of Apple iOS). Network settings and DNS and WINS configurations are communicated to the IPsec client by the IPsec server (see "Mode Configuration" on page 331).

Optional use of the proxy server by the secondary external interface

If a proxy server is used, the secondary external interface may be exempted from its use. This can be useful if the secondary external interface is a mobile network modem (3G) (see "Network >> Proxy Settings" on page 219).

3.8 Overview of the changes in Version 8.1

The following functions have been added to firmware Version 8.1.

- User firewall in VPN connections
- Dynamic activation of the firewall rules
- Function extension of the service contacts
- OPC Inspector for Deep Packet Inspection for OPC Classic
- Extended DynDNS providers
- New mode for pre-shared key (PSK) authentication method
- On the web interface, dynamic modifications are displayed in gray.
- Verbose logging of modems

User firewall in VPN connections

The user firewall can be used within VPN connections.

A VPN connection in which the user firewall rules apply can now be selected for the user firewall (under Network Security >> User Firewall >> User Firewall Templates).

Dynamic activation of the firewall rules (conditional firewall)

The firewall rules can now be activated via an external event:

- **A button on the web interface** (under Network Security >> Packet Filter >> Rule Records)
- **An API command line** that is activated using the name or the row ID.
  /Packages/mguard-api_0/mbin/action fwrules/[in]active <ROWID>
- /Packages/mguard-api_0/mbin/action_name fwrules/[in]active <NAME>
- **An externally connected pushbutton/switch** (for mGuards that allow connection, see "Dynamic activation of the firewall rules (conditional firewall)" on page 38)
- **The starting or stopping of a VPN connection**. It can be set whether a started or stopped VPN connection activates or deactivates the firewall rule record. Successful establishment of the VPN connection is not important. (The VPN connection can be started via a button on the web interface, text message, a switch, a pushbutton, data traffic or the script nph-vpn.cgi.)
- **Incoming text message** (for TC MGUARD RS4000/RS2000 3G only). See "Token for text message trigger" under Network Security >> Packet Filter >> Rule Records.
- **CGI interface**. The CGI script “nph-action.cgi may” can be used to control firewall rule records.

If the status of the firewall rule records changes, an e-mail can be sent automatically. In the case of the TC MGUARD RS4000/RS2000 3G, a text message can also be sent in such an event.

Function extension of the service contacts

Service contacts (service I/Os) can be connected to some mGuards.

– TC MGUARD RS4000/RS2000 3G
– FL MGUARD RS4000/RS2000
– FL MGUARD RS
– FL MGUARD GT/GT

A pushbutton or an on/off switch can be connected to **inputs CMD 1-3**. The pushbutton or on/off switch is used to establish and release predefined VPN connections or the defined firewall rule records.

For the VPN connections it can be set whether the VPN connection is to be switched via one of the service contacts (IPsec VPN >> Connections >> Edit >> General). If a switch is connected, the switch behavior can also be inverted.

For the firewall rule records it can be set whether a rule is to be switched via one of the service contacts or if a VPN connection is to be switched (Network Security >> Packet Filter >> Rule Records).

In this way, one or more freely selectable VPN connections or firewall rule records can be switched. A mixture of VPN connections and firewall rule records is also possible.

The web interface displays which VPN connections and which firewall rule records are connected to an input (Management >> Service I/O >> Alarm output).

In addition, the behavior of **outputs ACK 1-3** can be set on the web interface (Management >> Service I/O >> Alarm output).

Outputs ACK 01-2 can be used to monitor specific VPN connections or firewall rule records and to display them using LEDs.

Alarm output ACK 03 monitors the function of the mGuard and therefore enables remote diagnostics.

The alarm output reports the following, if it has been activated.

– Failure of the redundant supply voltage
– Monitoring of the link status of the Ethernet connections
– Monitoring of the temperature state
– Monitoring of the connection status of the internal modem

OPC Inspector for Deep Packet Inspection for OPC Classic

When using the OPC Classic network protocol, interconnected firewalls virtually have no effect. In addition, conventional NAT routing cannot be used.

When the OPC Classic function is activated, the OPC packets are monitored (see "OPC Inspector" on page 288).

The TCP ports that are negotiated during the connection opened first are detected and opened for OPC packets. If no OPC packets are transmitted via these ports within a configurable timeout, they are closed again. If the OPC validity check is activated, only OPC packets must be transmitted via OPC Classic port 135.

Additional functions

Extended DynDNS providers

– When establishing VPN connections, it is useful if the devices obtain their IP address via a DynDNS service.

  More DynDNS providers are supported in Version 8.1.

New mode for pre-shared key authentication method

When selecting the pre-shared key (PSK) authentication method, “Aggressive Mode” can be selected (under IPsec VPN >> Connections >> Edit >> Authentication).

On the web interface, dynamic modifications are highlighted gray.

Status messages are displayed on the web interface and updated continuously. To identify these dynamic entries more easily, they are displayed in gray.

Verbose logging of modems

Only for mGuards that have an internal or external modem or that are capable of mobile communication (under Logging >> Settings).

3.9 Overview of the changes in Version 8.0

The following functions have been added to firmware Version 8.0.

Configuration extensions

- Improved CIFS Integrity Monitoring (see "New in CIFS Integrity Monitoring" on page 42)
- Integrated **COM server** for mGuard platforms with serial interface (see "New in CIFS Integrity Monitoring" on page 42)
- Configurable **multicast support** for devices with internal switch in order to send data to a group of receivers without the transmitter having to send it multiple times (see "Multicast" on page 196)
- **VPN extensions** (see "VPN extensions" on page 42).
- **Dynamic web interface** for configuration. Incorrect entries are highlighted in color and help is also offered in the form of system messages.
- Support for 100 Mbps SFPs for FL MGUARD GT/GT. SFPs are hot-swap-capable interfaces for Ethernet or fiber optics in different forms.

Support for mGuard platforms TC MGUARD RS4000 3G and TC MGUARD RS2000 3G

- Support for **mobile network and positioning functions** (see "Network >> Mobile Network" on page 156)
- **Support for integrated Managed and Unmanaged Switches** (see "Network >> Ethernet" on page 194)
- Support for a dedicated **DMZ port** (only TC MGUARD RS4000 3G)

  The DMZ port can be set so that it forwards packets to the internal, external or secondary external interface.
  The DMZ port is only supported in router mode and requires at least one IP address and a corresponding subnet mask. The DMZ does not support any VLANs.

Removed functions

- HiDiscovery support
- The “Save” button which only applied changes for the current page has been removed. Changes are made across all pages.

New in CIFS Integrity Monitoring

Time schedule

The time schedule has been improved in Version 8.0. Now more than one scan per day is possible. Continuous scanning can also be set.

If the scan takes longer than planned, it is aborted. However you can adjust the settings so that a scan is started regularly.

Extended display of the current status

Each row of the CIFS Integrity Monitoring also displays the following information.
- The status of the scanned network drives
- The result of the last scan or the progress of the current scan

The menu in the web interface has been extended so that you can now see the status of each scan. The progress indicator shows the number of checked files.

VPN extensions

Status of the VPN connections

The setting for the VPN connection is now divided into “Disabled”, “Started”, and “Stopped”. The “Disabled” setting ignores the VPN connection, as if it were not configured. This also means it cannot be dynamically enabled/disabled. The other two settings determine the status of the VPN connection when restarting the connection or booting.

In Version 8.0, the VPN connections can be started or stopped via a button on the web interface, via text message, an external switch or the script nph-vpn.cgi. This takes into account all VPN connections. Packets that correspond to a VPN connection that is not disabled are forwarded when the connection is established or discarded if the connection is not established. VPN connections which were set to “Active: No” in the previous versions are now interpreted as “Disabled”.

Unique names

In Version 8.0, the names of VPN connections are made unique. During the update, a hash or unique number is added to names that are duplicated.

Timeout for the VPN connection

You can set a timeout which aborts the VPN connection if it has been started via a text message, nph-vpn.cgi script or the web interface. VPN connections which have been started by an explicit request via an application are not affected.

Source-based routing

VPN tunnels which only differ in their source network can now be configured.

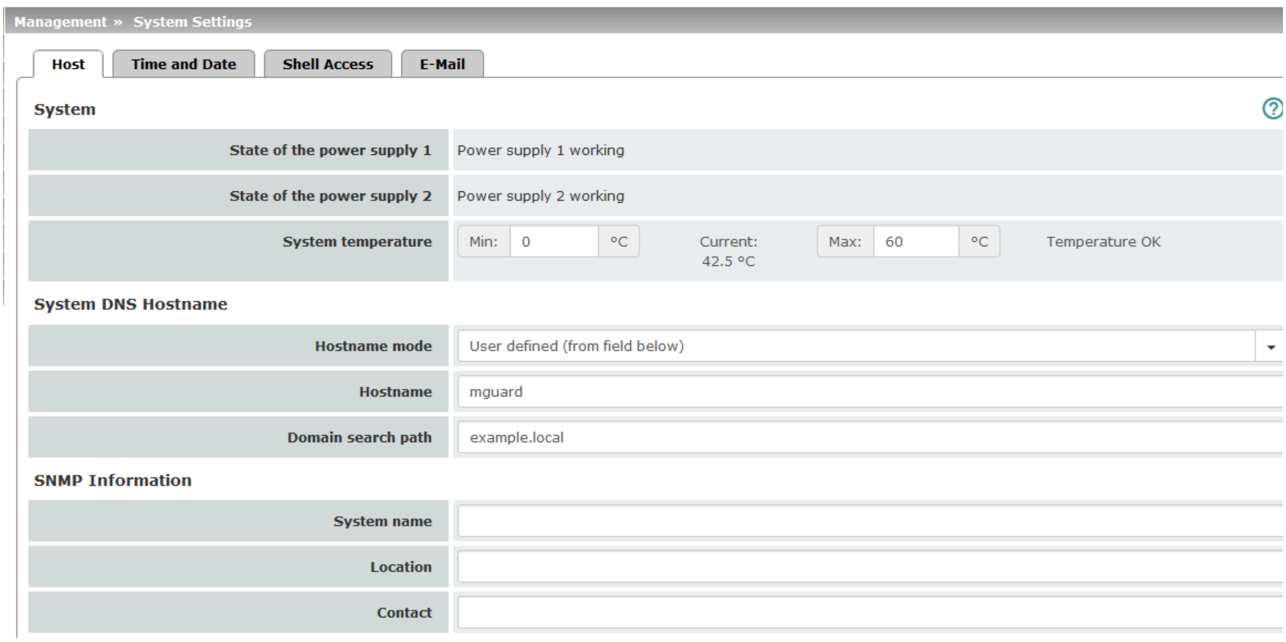
From Version 8.0, the VPN configuration permits a remote network with different local networks in one configuration. The VPN tunnel groups are extended so that they permit an established VPN connection to select only one subnetwork from the local network. In previous versions, this was only possible for remote networks.

4 Management menu

> For security reasons, we recommend you change the default root and administrator passwords during initial configuration (see "Authentication >> Administrative Users" on page 231). A message informing you of this will continue to be displayed at the top of the page until the passwords are changed.

4.1 Management >> System Settings

4.1.1 Host

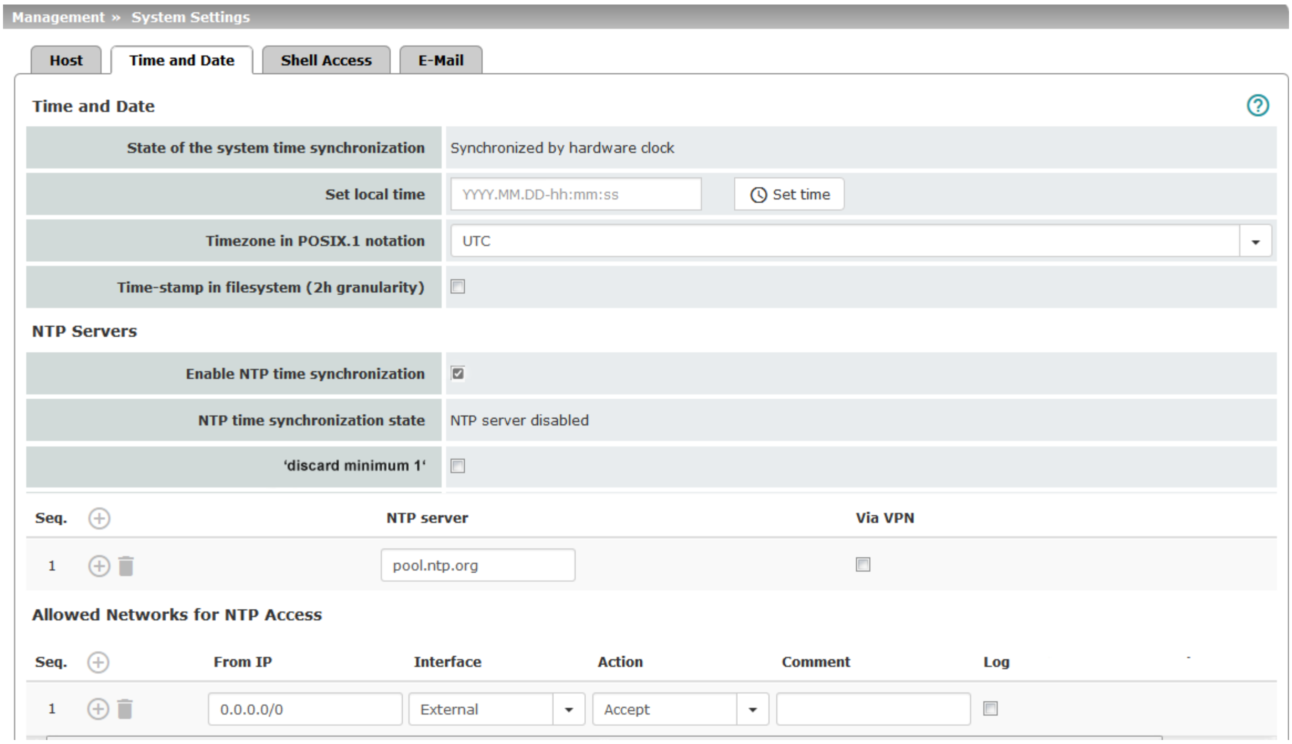


Management >> System Settings >> Host		
System	**Power supply 1/2** (Only TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4000, FL MGUARD RS4004, mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD RS, FL MGUARD GT/GT)	State of both power supply units (model depedent with redundant power supply) **Note** (FL MGUARD CENTERPORT): In order for the power supply status (power supply 1/2) to be displayed correctly in the WBM, the (redundant) power supply must already have been connected correctly before the device is switched on. If this is not the case, it is necessary to shut down the device and disconnect the power supply completely from the device for at least 30 seconds. Then reconnect the power supply correctly to the device and restart it.
	System temperature (°C)	An SNMP trap is triggered if the temperature exceeds or falls below the specified temperature range.
	CPU temperature (°C) (only mGuard centerport (Innominate), FL MGUARD CENTERPORT, not with firmware 7.6.0)	An SNMP trap is triggered if the temperature exceeds or falls below the specified temperature range.

Management >> System Settings >> Host [...]		
	System use notification	Freely selectable text for a system use notification that is displayed before logging on at the mGuard device (maximum 1024 characters). Is displayed for: – Login per SSH login – Login via the serial console – Login via the web interface (web UI). The (repeated) display of the message can be disabled by the customer using a suitable SSH. **Default setting:** *The usage of this mGuard security appliance is reserved to authorized staff only. Any intrusion and its attempt without permission is illegal and strictly prohibited.*
System DNS Hostname	**Hostname mode**	You can assign a name to the mGuard using the *Hostname mode* and *Hostname* fields. This name is then displayed, for example, when logging in via SSH (see "Management >> System Settings" on page 43, "Shell Access" on page 53). Assigning names simplifies the administration of multiple mGuard devices. **User defined (from field below)** (Default) The name entered in the *Hostname* field is the name used for the mGuard. If the mGuard is running in *Stealth* mode, the “User defined” option must be selected under “Hostname mode”. **Provider defined (e.g., via DHCP)** If the selected network mode permits external setting of the host name, e.g., via DHCP, the name supplied by the provider is assigned to the mGuard.
	Hostname	If the “User defined” option is selected under *Hostname mode*, enter the name that should be assigned to the mGuard here.
	Domain search path	This option makes it easier for the user to enter a domain name. If the user enters the domain name in an abbreviated form, the mGuard completes the entry by appending the domain suffix that is defined here under “Domain search path”.
SNMP Information	**System name**	A name that can be freely assigned to the mGuard for administration purposes, e.g., “Hermes”, “Pluto”. (Under SNMP: sysName)
	Location	A description of the installation location that can be freely assigned, e.g., “Hall IV, Corridor 3”, “Control cabinet”. (Under SNMP: sysLocation)
	Contact	The name of the contact person responsible for the mGuard, ideally including the phone number. (Under SNMP: sysContact)
Keyboard (Only mGuard centerport (Innominate), FL MGUARD CENTERPORT)	The settings for using a keyboard can only be made for the mGuard centerport (Innominate) and FL MGUARD CENTERPORT devices.	

Management >> System Settings >> Host [...]		
	Keyboard assignment	Selection list for selecting the appropriate keyboard layout.

4.1.2 Time and Date



Set the time and date correctly. Otherwise, certain time-dependent activities cannot be started by the mGuard (see "Time-controlled activities" on page 47).

Management >> System Settings >> Time and Date	
Time and Date	You can set the mGuard system time manually and assign the appropriate time zone or synchronize the system time using the NTP server of your choice. The system time can also be set via GPS/GLONASS on TC MGUARD RS4000/RS2000 3G (see "Positioning System" on page 172) Set the time and date correctly. Otherwise, certain time-dependent activities cannot be started by the mGuard (see "Time-controlled activities" on page 47). Connected devices can use the mGuard as an NTP server. Please note, that for security reasons the NTP version *NTP v1* is not supported by the mGuard.

Management >> System Settings >> Time and Date [...]		
	State of the system time	Indicates whether the mGuard system time has ever been synchronized with a valid time during mGuard runtime.

> If the display indicates that the mGuard system time has not been synchronized, the mGuard does not perform any time-controlled activities.

Devices without built-in clock always start in “Not synchronized” mode. Devices with a built-in clock usually start in “Synchronized by hardware clock” mode.

The state of the clock only returns to “Not synchronized” if the firmware is reinstalled on the device or if the built-in clock has been disconnected from the power for too long.

Power supply of the built-in clock is ensured by the following components:

- **Capacitor** (only TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS),
- **Battery** (only mGuard centerport (Innominate), FL MGUARD CENTERPORT, mGuard delta (Innominate))
- **Rechargeable battery** (only FL MGUARD RS4000/RS2000, FL MGUARD RS4004/RS2005, FL MGUARD SMART2, FL MGUARD PCI(E)4000, FL MGUARD DELTA)

  In the case of the FL MGUARD RS4000/RS2000, the rechargeable battery lasts at least five days.

Time-controlled activities

- **Time-controlled pick-up of configuration from a configuration server:**

  This is the case when the *Time schedule* setting is selected under the *Management >> Central Management*, *Configuration Pull* menu item for the **Pull schedule** setting (see "Management >> Configuration Profiles" on page 90, "Configuration Pull" on page 110).
- **Interruption of the connection at a certain time using PPPoE network mode:**

  This is the case when **Network Mode** is set to PPPoE under the *Network >> Interfaces, General* menu item, and **Automatic Re-connect** is set to Yes (see *"PPPoE" on page 141*).
- **Acceptance of certificates when the system time has not yet been synchronized:**

  This is the case when the *Wait for synchronization of the system time* setting is selected under the Authentication >> Certificates,Certificate Settings menu item for the **Check the validity period of certificates and CRLs** option (see Authentication >> Certificates and"Certificate Settings" on page 246).
- **CIFS integrity check:**

  The regular, automatic check of the network drives is only started when the mGuard has a valid time and date (see section below).

Management >> System Settings >> Time and Date [...]		
	The system time can be set or synchronized by various events: – **Synchronized by hardware clock**: the mGuard has a built-in clock which has been synchronized with the current time at least once. The display shows whether the clock is synchronized. A synchronized built-in clock ensures that the mGuard has a synchronized system time even after a restart. – **Synchronized manually**: the administrator has defined the current time for the mGuard runtime by making a corresponding entry in the **Set local time** field. – **Synchronized by file system time-stamp**: the administrator has set the **Time-stamp in filesystem** setting to *Yes*, and has either transmitted the current system time to the mGuard via NTP (see below under *NTP Servers*) or has entered it under **Set local time**. The system time of the mGuard is then synchronized using the time stamp after a restart (even if it has no built-in clock). The time might be set exactly again afterwards via NTP. – **Synchronized by Network Time Protocol NTP**: the administrator has activated NTP time synchronization under **NTP Servers**, has entered the address of at least one NTP server, and the mGuard has established a connection with at least one of the specified NTP servers. If the network is working correctly, this occurs a few seconds after a restart. The display in the **NTP time synchronization state** field may only change to “Synchronized” much later (see the explanation below under **NTP time synchronization state**). – **Synchronized by GPS/GLONASS data**: TC MGUARD RS4000/RS2000 3G can set and synchronize the system time via the positioning system (GPS/GLONASS) (under "Network >> Mobile Network >> Positioning System").	
	Set local time	Here you can set the time for the mGuard, if no NTP server has been set up or the NTP server cannot be reached. You should also set the local system time if the "Network >> Mobile Network >> Positioning System" menu item is set to “Yes” under the positioning system (under "Network >> Mobile Network >> Positioning System"). The date and time are specified in the format YYYY.MM.DD-HH:MM:SS: YYYY Year MM Month DD Day HH Hour MM Minute SS Second

Management >> System Settings >> Time and Date [...]		
	Timezone in POSIX.1 notation	If a current local time (that differs from Greenwich Mean Time) is to be displayed as the *current system time*, you must enter the number of hours that your local time is ahead of or behind Greenwich Mean Time. You can select your location from the drop-down list (daylight savings time is usually automatically taken into consideration). Alternatively, you can set it manually as follows: **Example**: in Berlin, the time is one hour ahead of GMT. Therefore, enter: CET-1. In New York, the time is five hours behind Greenwich Mean Time. Therefore, enter: CET+5. The only important thing is the -1, -2 or +1, etc. value as only these values are evaluated – not the preceding letters. They can be “CET” or any other designation, such as “UTC”. If you wish to display Central European Time (e.g., for Germany) and have it automatically switch to/from daylight savings time, enter: CET-1CEST,M3.5.0,M10.5.0/3
	Time-stamp in filesystem	If this function is activated, the mGuard writes the current system time to its memory every two hours. If the mGuard is switched off and then on again, a time from this two-hour time slot is displayed, not a time on January 1, 2000.
NTP Servers	The mGuard can act as the NTP server for external computers (NTP = Network Time Protocol). In this case, the computers should be configured so that the address of the mGuard is specified as the NTP server address. By default, the NTP server of the mGuard device is disabled. After starting the NTP server, access is possible via the internal interface (LAN interface). Firewall rules can be used to enable or restrict access via all available interfaces. If the mGuard is operated in *Stealth* mode, the management IP address of the mGuard (if this is configured) must be used for the computers, or the IP address 1.1.1.1 must be entered as the local address of the mGuard. For the mGuard to act as the NTP server, it must obtain the current date and the current time from an NTP server (= time server). To do this, the address of at least one NTP server must be specified. This feature must also be activated.	

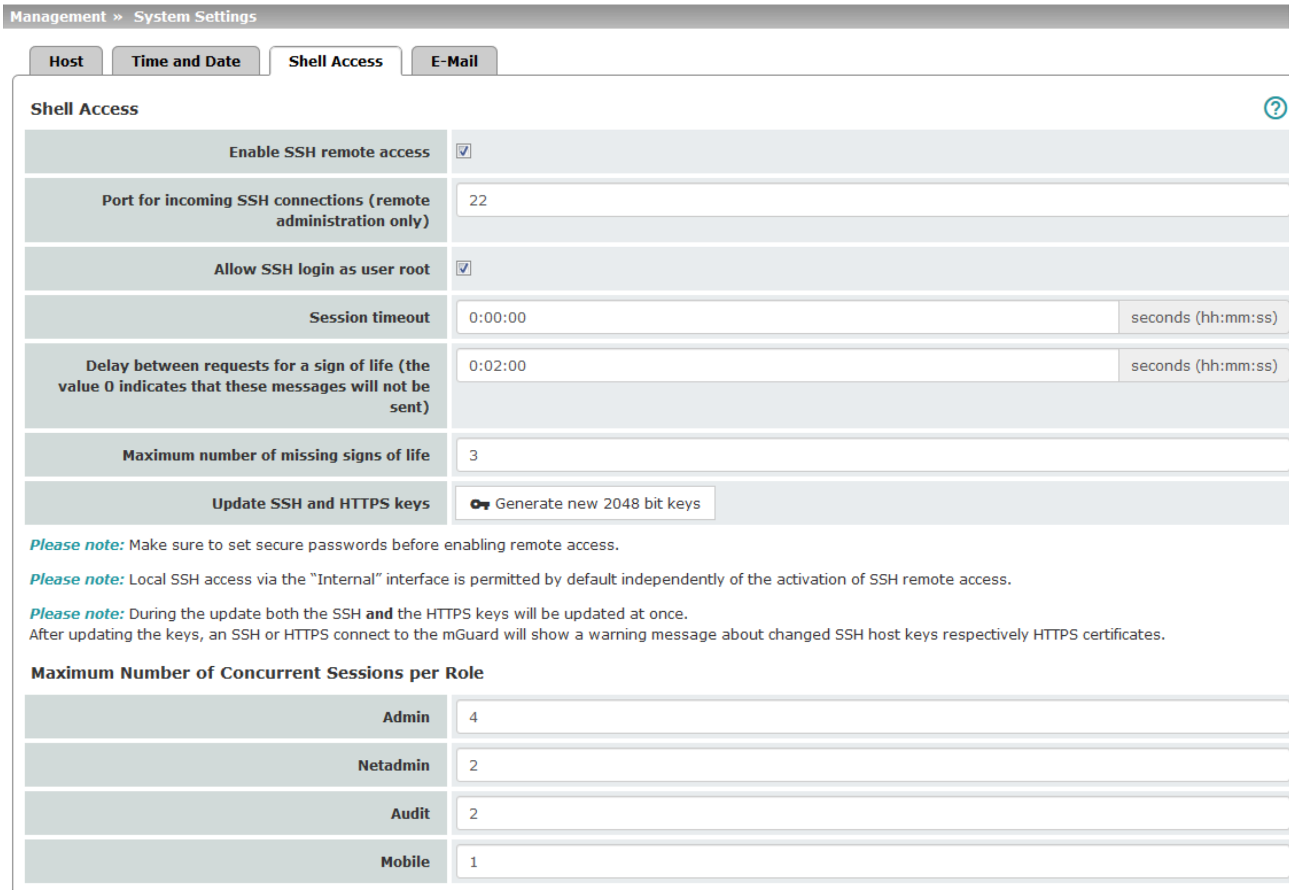
Management >> System Settings >> Time and Date [...]		
	Enable NTP time synchronization	If this function is activated, the mGuard obtains the date and time from one or more time server(s) and synchronizes itself with it or them. Initial time synchronization can take up to 15 minutes. During this time, the mGuard continuously compares the time data of the external time server and that of its own time so that this can be adjusted as accurately as possible. Only then can the mGuard act as the NTP server for the computers connected to its LAN interface and provide them with the system time. An initial time synchronization with the external time server is performed after every booting process, unless the mGuard has a built-in clock (for *TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G*, *FL MGUARD RS4004/RS2005, FL MGUARD RS4000/RS2000, FL MGUARD PCI(E)4000, FL MGUARD DELTA*, *FL MGUARD GT/GT*, and for *FL MGUARD SMART2)*. After initial time synchronization, the mGuard regularly compares the system time with the time servers. Fine adjustment of the time is usually only made in the second range.
	NTP time synchronization state	Displays the current NTP status. Shows whether the NTP server running on the mGuard has been synchronized with the configured NTP servers to a sufficient degree of accuracy. If the system clock of the mGuard has never been synchronized prior to activation of NTP time synchronization, then synchronization can take up to 15 minutes. The NTP server still changes the mGuard system clock to the current time after a few seconds, as soon as it has successfully contacted one of the configured NTP servers. The system time of the mGuard is then regarded as synchronized. Fine adjustment of the time is usually only made in the second range.
	‘discard minimum1‘	Enabling this option can improve time synchronization with some NTP clients, especially PLC systems. Additionally, the refresh interval on the PLC system should be increased to the maximum possible value (e.g. 86400 seconds).
	NTP server	Enter one or more time servers from which the mGuard should obtain the current time. If several time servers are specified, the mGuard will automatically connect to all of them to determine the current time.

Management >> System Settings >> Time and Date [...]		
	Via VPN	The NTP server's request is – **where possible** – carried out via a VPN tunnel (IPsec VPN or OpenVPN). **Prerequisite**: A suitable VPN tunnel is available. If no suitable VPN tunnel is available, traffic is always sent **unencrypted via the default gateway**. A suitable VPN tunnel is available if the remote peer belongs to the remote network of a configured VPN tunnel and the mGuard has an internal IP address that belongs to the local network of the same VPN tunnel. **Please note:** **For IPsec VPN connections**, the "Via VPN" function must be activated so that the traffic is routed through a suitable IPsec VPN tunnel. **For OpenVPN connections**, traffic is always routed via a suitable OpenVPN tunnel even if the function is deactivated.
Allowed Networks for NTP access (when “Enable NTP time synchronization” function is activated)	When the **Enable NTP time synchronization** function is activated, external devices can access the NTP server of the mGuard. By default, it can only be accessed via the internal interface (LAN interface). **NOTE: The device may be accessible via external networks.** Depending on the settings, the services of the device may be accessible via external networks or the internet. Make sure that access is only possible if it is desired. Otherwise, configure your network accordingly to prevent such access. If no rules are set or if no rule applies, the following default settings apply: – NTP access via *Internal* is permitted. – NTP access via *External*, External 2, *DMZ* , GRE, Dial-in, and *VPN* is denied. Specify the monitoring options according to your requirements. **NOTE:** If you want to deny access via *Internal*, you must implement this explicitly by means of corresponding firewall rules, for example, by specifying *Drop* as the action. The table lists the firewall rules that have been set up. These apply for incoming data packets of an NTP access attempt. If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored.	

Management >> System Settings >> Time and Date [...]		
	From IP	Enter the address of the computer or network from which access is permitted or forbidden in this field. The following options are available: – An IP address. – To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 26). – **0.0.0.0/0** means all addresses.
	Interface	**Internal / External / External 2 / DMZ / VPN / GRE / Dial-in**[1] Specifies to which interface the rule should apply. If no rules are set or if no rule applies, the following default settings apply: – NTP access is permitted via *Internal*. – NTP access via *External*, *External 2, DMZ, VPN, Dial-in*, and *GRE* is denied. Specify the monitoring options according to your requirements. **NOTE:** If you want to deny access via *Internal*, you must implement this explicitly by means of corresponding firewall rules, for example, by specifying *Drop* as the action.
	Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back and the sender is informed of their rejection. (In *Stealth* mode, *Reject* has the same effect as *Drop*.) **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts.
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – activate *Log* function – Should not be logged – deactivate *Log* function (default)

[1] *External 2* and *Dial-in* are only for devices with a serial interface (see "Network >> Interfaces" on page 127).

4.1.3 Shell Access



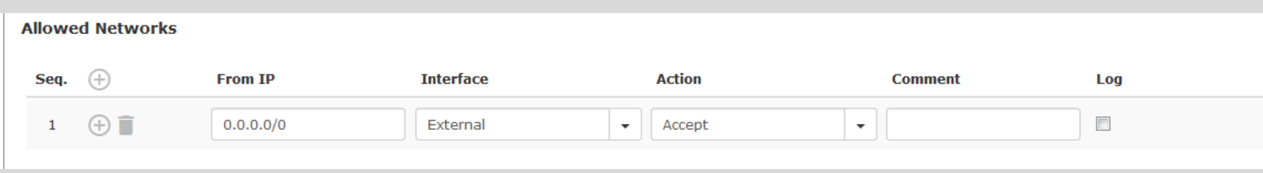
The mGuard must not be simultaneously configured via web access, shell access or SNMP. Simultaneous configuration via the different access methods might lead to unexpected results.

Management >> System Settings >> Shell Access		
Shell Access	You can configure the mGuard via the web interface or via the command line (shell). Access to the command line is via the serial interface or SSH. Always use **Current SSH clients** (e.g. *putty*), to avoid use of weak encryption algorithms. If you need to make changes to the authentication procedure, you should subsequently restart the mGuard, in order to safely end existing sessions with no longer valid certifications or passwords. When **SSH remote access** is activated, the mGuard can be configured **from remote computers** using the command line. **SSH remote access** is deactivated by default. It can be activated and restricted to selected networks. **NOTE: The device may be accessible via external networks.** Depending on the settings, the services of the device may be accessible via external networks or the internet. Make sure that access is only possible if it is desired. Otherwise, configure your network accordingly to prevent such access. **NOTE:** Local SSH access via the “Internal” interface is permitted by default independently of the activation of SSH remote access. The **Enable SSH remote access** function must be activated and the firewall rules for the internal interface must then be defined accordingly in order to specify differentiated access options on the mGuard via the internal interface (see "Allowed Networks" on page 57). **NOTE:** If remote access is enabled, make sure that secure passwords are defined for *root* and *admin* users. If you need to make changes to the password for *root* or *admin*, you should subsequently restart the mGuard, in order to safely end existing sessions with no longer valid certifications or passwords.	
	Enable SSH remote access	Activate the function to enable SSH remote access. SSH access via the *Internal* interface (i.e., from the directly connected LAN or from the directly connected computer) can be enabled independently of the activation of this function. Following activation of the remote access, access is possible via *Internal*, *VPN*, and *Dial-in*. The firewall rules for the available interfaces must be defined accordingly in order to specify differentiated access options on the mGuard (see "Allowed Networks" on page 57).
	Enable SSH access as user root	**Standard: enabled** If the function is activated, the user "*root*" can log onto the device via SSH access.

Management >> System Settings >> Shell Access [...]		
	Port for incoming SSH connections (remote administration only) (Only if SSH remote access is activated)	**Default: 22** If this port number is changed, the new port number only applies for access via the *External, External 2, DMZ, VPN, GRE,* and *Dial-in* interface. In Stealth mode, incoming traffic on the port specified is no longer forwarded to the client. In Router mode with NAT or port forwarding, the port number set here has priority over the rules for port forwarding. Port number 22 still applies for internal access. The remote peer that implements remote access may have to specify the port number defined here during login. Example: If this mGuard can be accessed over the Internet via address 123.124.125.21 and default port number 22 has been specified for remote access, you may not need to enter this port number in the SSH client (e.g., PuTTY or OpenSSH) of the remote peer. If a different port number has been set (e.g., 2222), this must be specified, e.g.: ssh -p 2222 123.124.125.21
	Session timeout	Specifies after what period of inactivity (in hh:mm:ss) the session is automatically terminated, i.e., automatic logout. When set to 0 (default setting), the session is not terminated automatically. The specified value is also valid for shell access via the serial interface instead of via the SSH protocol. The effect of the “Session timeout” setting is temporarily suspended if the processing of a shell command exceeds the number of seconds set. In contrast, the connection can also be aborted if it is no longer able to function correctly, see "Delay between requests for a sign of life" on page 56.

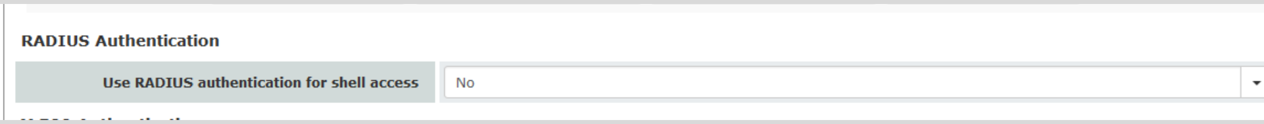
Management >> System Settings >> Shell Access [...]		
	Delay between requests for a sign of life	**Default: 120 seconds (00:02:00)** Values from 0 seconds to 1 hour can be set. Positive values indicate that the mGuard is sending a request to the peer within the encrypted SSH connection to find out whether it can still be accessed. This request is sent if no activity was detected from the peer for the specified number of seconds (e.g., due to network traffic within the encrypted connection). The value 0 means that no requests for a sign of life are sent. The value entered here relates to the functionality of the encrypted SSH connection. As long as it is working properly, the SSH connection is not terminated by the mGuard as a result of this setting, even when the user does not perform any actions during this time. As the number of simultaneously open sessions is limited (see *"Maximum number of concurrent sessions per role" on page 57*), it is important to terminate sessions that have expired. Therefore, the request for a sign of life is preset to 120 seconds for Version 7.4.0 or later. If a maximum of three requests for a sign of life are issued, this causes an expired session to be detected and removed after six minutes. In previous versions, the preset was “0”. If it is important not to generate additional traffic, you can adjust the value. When “0” is set in combination with *Concurrent Session Limits*, subsequent access may be blocked if too many sessions are interrupted but not closed as a result of network errors. The entry can be in seconds [ss], minutes and seconds [mm:ss] or hours, minutes, and seconds [hh:mm:ss].
	Maximum number of missing signs of life	Specifies the maximum number of times a sign of life request to the peer may remain unanswered. For example, if a sign of life request should be made every 15 seconds and this value is set to 3, the SSH connection is deleted if a sign of life is still not detected after approximately 45 seconds.
	Update SSH and HTTPS keys	**Generate new 2048 bit keys** Keys that have been generated using an older firmware version might be weak and should be renewed. • Click on this button to generate a new key. • Note the fingerprints of the new keys generated. • Log in via HTTPS and compare the certificate information provided by the web browser.

Management >> System Settings >> Shell Access [...]	
Maximum number of concurrent sessions per role	You can limit the number of users who may access the mGuard command line simultaneously. The “*root*” user always has unrestricted access. The number of access instances for administrative user roles (*admin, netadmin, audit,* and *mobile*) can be limited individually. The *netadmin* and *audit* authorization levels relate to access rights with the mGuard device manager (FL MGUARD DM). The restriction does not affect existing sessions; it only affects newly established access instances. Approximately 0.5 MB of memory are required for each session. **Admin** — 2 to 2147483647 At least two simultaneously permitted sessions are required for the “*admin*” *role* to prevent it from having its access blocked. **Netadmin** — 0 to 2147483647 When “0” is set, no session is permitted. The “*netadmin*” user is not necessarily used. **Audit** — 0 to 2147483647 When “0” is set, no session is permitted. The “*audit*” user is not necessarily used. **Mobile** — 0 to 2147483647 When “0” is set, no session is permitted. The “*mobile*” user is not necessarily used.
Allowed Networks (Only active if **Enable SSH remote access** is activated)	SSH access to the mGuard command line can be restricted to selected interfaces and networks by means of firewall rules. The rules apply for incoming data packets and can be configured for all interfaces depending on the license and device. The rules specified here only take effect if the **Enable SSH remote access** function is activated. Access via *Internal* is also possible if this function is deactivated. If you want to deny access via *Internal*, you must implement this explicitly by means of corresponding firewall rules, for example, by specifying *Drop* as the action. If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored. **The following options are available:**



Management >> System Settings >> Shell Access [...]		
	From IP	Enter the address of the computer or network from which access is permitted or forbidden in this field. The following options are available: IP address: **0.0.0.0/0** means all addresses. To specify an address area, use CIDR format, see "CIDR (Classless Inter-Domain Routing)" on page 26.
	Interface (This option varies depending on the device and licenses installed.)	**Internal / External / External 2 / DMZ / VPN / GRE / Dial-in** *External 2* and *Dial-in* are only for devices with a serial interface, see "Network >> Interfaces" on page 127. Specifies to which interface the rule should apply. If no rules are set or if no rule applies, the following default settings apply: SSH access is permitted via *Internal, VPN,* and *Dial-in*. Access via *External*, *External 2*, *DMZ,* and *GRE* is denied. Specify the access options according to your requirements. **NOTE:** If you want to deny access via *Internal, VPN,* or *Dial-in*, you must implement this explicitly by means of corresponding firewall rules, for example, by specifying *Drop* as the action. **To prevent your own access being blocked**, you may have to permit access simultaneously via another interface explicitly with *Accept* before clicking on the **Save** button to activate the new setting. Otherwise, if your access is blocked, you must carry out the recovery procedure.
	Action	Options: – **Accept** means that the data packets may pass through. – **Reject** means that the data packets are sent back and the sender is informed of their rejection. (In *Stealth* mode, *Reject* has the same effect as *Drop*.) – **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts.
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – activate *Log* function – Should not be logged – deactivate *Log* function (default)

Management >> System Settings >> Shell Access [...]	
RADIUS authentication (This menu item is not included in the scope of functions for TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005 or FL MGUARD RS2000.)	Users can be authenticated via a RADIUS server when they log in. This also applies for users who want to access the mGuard via shell access using SSH or a serial console. The password is checked locally in the case of predefined users *(root, admin, netadmin, audit,* and *mobile*).



Use RADIUS authentication for shell access

If set to **No**, the passwords of users who log in via shell access are checked via the local database on the mGuard.

Select **Yes** for users to be authenticated via a RADIUS server. This also applies for users who want to access the mGuard via shell access using SSH or a serial console. The password is only checked locally in the case of predefined users *(root, admin, netadmin, audit,* and *mobile*).

The *netadmin* and *audit* authorization levels relate to access rights with the mGuard device manager (FL MGUARD DM).

Under **X.509 Authentication**, if you set **Enable X.509 certificates for SSH access** to **Yes**, the X.509 authentication method can be used as an alternative. Which method is actually used by the user depends on how the user uses the SSH client.

> If you need to make changes to the authentication procedure, you should subsequently restart the mGuard, in order to safely end existing sessions with no longer valid certifications or passwords.

When setting up RADIUS authentication for the first time, select **Yes**.

> You should only select **As only method for password authentication** if you are an experienced user, as doing so could result in all access to the mGuard being blocked.

If you do intend to use the **As only method for password authentication** option when setting up RADIUS authentication, we recommend that you create a “Customized Default Profile” which resets the authentication method.

The predefined users *(root, admin, netadmin, audit,* and *mobile)* are then no longer able to log into the mGuard via SSH or serial console.

There is one exception: it it still possible to perform authentication via an externally accessible serial console by correctly entering the local password for the *root* user name.

Management >> System Settings >> Shell Access

X.509 Authentication

(This menu item is not included in the scope of functions for TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005 or FL MGUARD RS2000.)

X.509 certificates for SSH clients

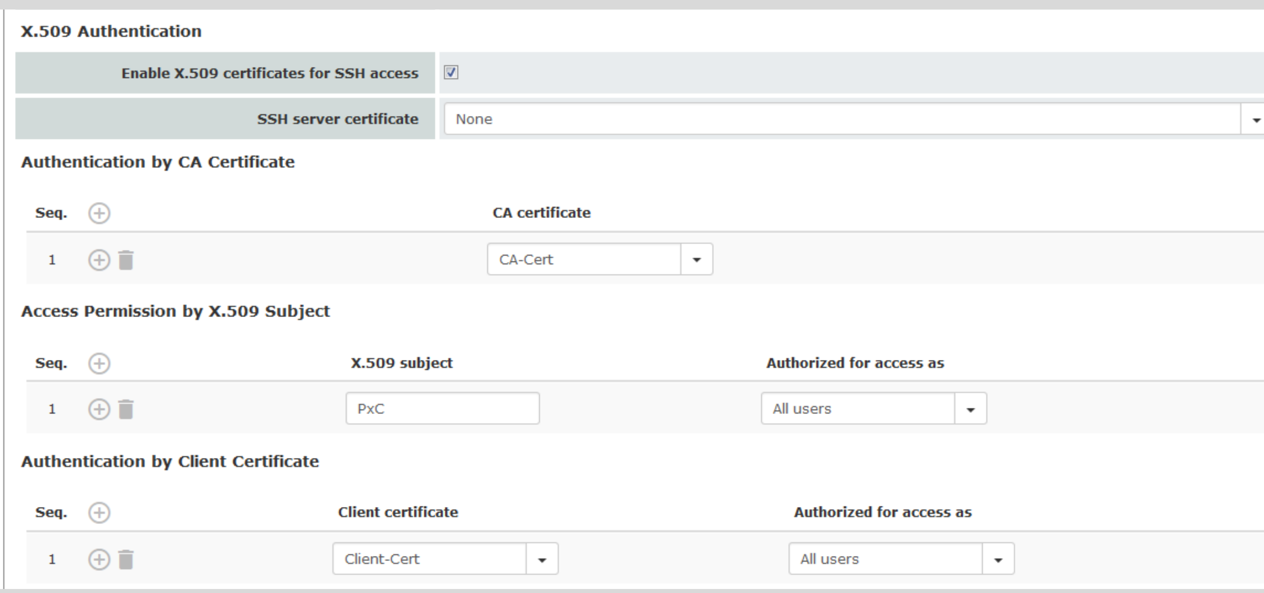
The mGuard supports the authentication of SSH clients using X.509 certificates. It is sufficient to configure CA certificates that are required for the establishment and validity check of a certificate chain. This certificate chain must exist between the CA certificate on the mGuard and the X.509 certificate shown to the SSH client (see "Shell Access" on page 53).

If the validity period of the client certificate is checked by the mGuard (see "Certificate Settings" on page 246), new CA certificates must be configured on the mGuard at some point. This must take place before the SSH clients use their new client certificates.

If CRL checking is activated (under Authentication >> Certificates >> Certificate Settings), one URL (where the corresponding CRL is available) must be maintained for each CA certificate. The URL and CRL must be published before the mGuard uses the CA certificates in order to confirm the validity of the certificates shown by the VPN partners.

> The rules specified here only take effect if the **Enable SSH remote access** function is activated. Access via *Internal* is also possible if this function is deactivated.
>
> If you want to deny access via *Internal*, you must implement this explicitly by means of corresponding firewall rules, for example, by specifying *Drop* as the action.

> If you need to make changes to the authentication procedure, you should subsequently restart the mGuard, in order to safely end existing sessions with no longer valid certifications or passwords.



Management >> System Settings >> Shell Access [...]		
	Enable X.509 certificates for SSH access	**If the function is deactivated**, then only conventional authentication methods (user name and password or private and public keys) are permitted, not the X.509 authentication method. **If the function is activated**, then the X.509 authentication method can be used in addition to conventional authentication methods (as also used when the function is deactivated). If the function is activated, the following must be specified: – How the mGuard authenticates itself to the SSH client according to X.509, see **SSH server certificate (1)** – How the mGuard authenticates the remote SSH client according to X.509, see **SSH server certificate (2)**
	SSH server certificate (1)	**Specifies how the mGuard identifies itself to the SSH client.** Select one of the machine certificates from the selection list or the *None* entry. **None** When *None* is selected, the SSH server of the mGuard does not authenticate itself to the SSH client via the X.509 certificate. Instead, it uses a server key and thus behaves in the same way as older versions of the mGuard. If one of the machine certificates is selected, this is also offered to the SSH client. The client can then decide whether to use the conventional authentication method or the method according to X.509. The selection list contains the machine certificates that have been loaded on the mGuard under the *Authentication >> Certificates* menu item (see *Page 241*).
	SSH server certificate (2)	**Specifies how the mGuard authenticates the SSH client** The following definition relates to how the mGuard verifies the authenticity of the SSH client. The table below shows which certificates must be provided for the mGuard to authenticate the SSH client if the SSH client shows one of the following certificate types when a connection is established: – A certificate signed by a CA – A self-signed certificate For additional information about the table, see Section *"Authentication >> Certificates"* .

Authentication for SSH

The peer shows the following:	Certificate (specific to individual), **signed by CA**	Certificate (specific to individual), **self-signed**
The mGuard authenticates the peer using:		
	All CA certificates that form the chain to the root CA certificate together with the certificate shown by the peer PLUS (if required) Client certificates (remote certificates), **if** used as a filter	Client certificate (remote certificate)

According to this table, the certificates that must be provided are the ones the mGuard uses to authenticate the relevant SSH client.

The following instructions assume that the certificates have already been correctly installed on the mGuard (see *"Authentication >> Certificates"*).

> If the use of revocation lists (CRL checking) is activated under the *"Authentication >> Certificates"* , *Certificate Settings* menu item, each certificate signed by a CA that is “shown” by SSH clients is checked for revocations.

Management >> System Settings >> Shell Access

Authentication by CA Certificate

This configuration is only necessary if the SSH client shows a certificate signed by a CA.

All CA certificates required by the mGuard to form the chain to the relevant root CA certificate with the certificates shown by the SSH client must be configured.

The selection list contains the CA certificates that have been loaded on the mGuard under the *"Authentication >> Certificates"* menu item.

> If you need to make changes to the authentication procedure, you should subsequently restart the mGuard, in order to safely end existing sessions with no longer valid certifications or passwords.

Access Permission by X.509 Subject

Enables a filter to be set in relation to the contents of the *Subject* field in the certificate shown by the SSH client. It is then possible to restrict or enable access for SSH clients, which the mGuard would accept in principle based on certificate checks:

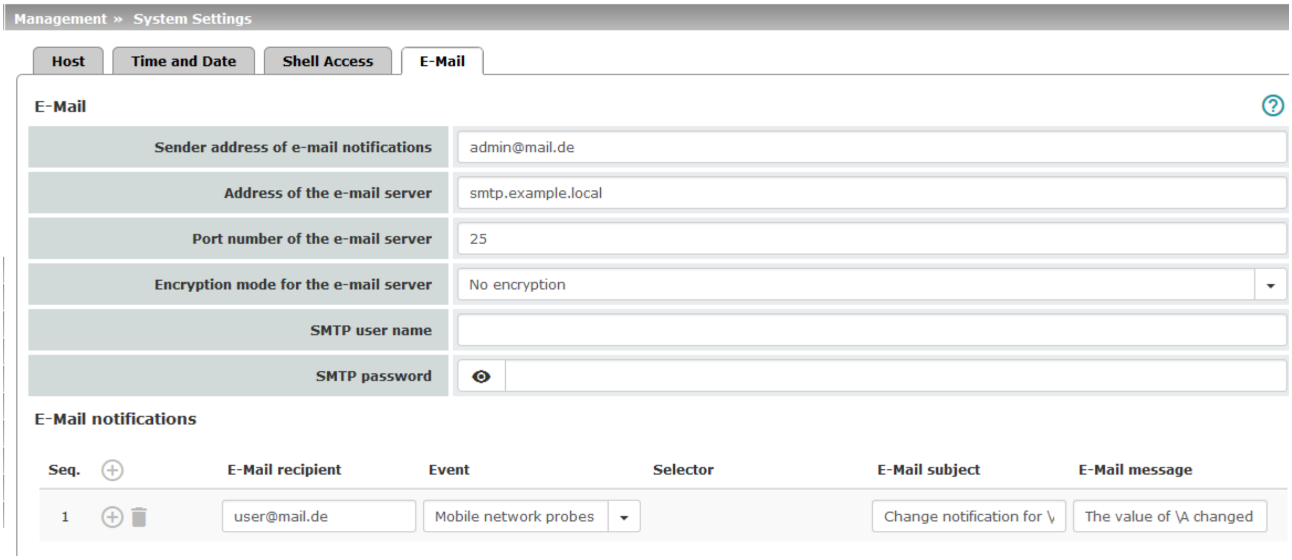
– Restricted access to certain *subjects* (i.e., individuals) and/or to *subjects* that have certain attributes or
– Access enabled for all subjects (see glossary under *"Subject, certificate" on page 453)*

> The *X.509 subject* field must not be empty.

Management >> System Settings >> Shell Access [...]		
	Access enabled for all subjects (i.e., individuals): An * (asterisk) in the *X.509 subject* field can be used to specify that all subject entries in the certificate shown by the SSH client are permitted. It is then no longer necessary to identify or define the subject in the certificate. **Restricted access to certain subjects (i.e., individuals) or to subjects that have certain attributes:** In the certificate, the certificate owner is specified in the *Subject* field. The entry is comprised of several attributes. These attributes are either expressed as an object identifier (e.g., 132.3.7.32.1) or, more commonly, as an abbreviation with a corresponding value. Example: CN=John Smith, O=Smith and Co., C=US If certain subject attributes have very specific values for the acceptance of the SSH client by the mGuard, then these must be specified accordingly. The values of the other freely selectable attributes are entered using the ***** (asterisk) wildcard. Example: CN=*, O=*, C=US (with or without spaces between attributes) In this example, the attribute “C=US” must be entered in the certificate under “Subject”. It is only then that the mGuard would accept the certificate owner (subject) as a communication partner. The other attributes in the certificates to be filtered can have any value. If a subject filter is set, the number (but not the order) of the specified attributes must correspond to that of the certificates for which the filter is to be used. Please note that the filter is case-sensitive. Several filters can be set and their sequence is irrelevant.	
	Authorized for access as	**All users / root / admin / netadmin / audit / mobile** Additional filter which specifies that the SSH client has to be authorized for a specific administration level in order to gain access. When establishing a connection, the SSH client shows its certificate and also specifies the system user for which the SSH session is to be opened (*root, admin, netadmin, audit, mobile*). Access is only granted if the entries match those defined here. Access for all listed system users is possible when *All users* is set. The *netadmin* and *audit* setting options relate to access rights with the mGuard device manager (FL MGUARD DM).

Management >> System Settings >> Shell Access [...]		
	Authentication by Client Certificate	Configuration is required in the following cases: – SSH clients each show a self-signed certificate. – SSH clients each show a certificate signed by a CA. Filtering should take place: access is only granted to a user whose certificate copy is installed on the mGuard as the remote certificate and is provided to the mGuard in this table as the *Client certificate*. This filter is **not** subordinate to the *Subject* filter. It resides on the same level and is allocated a logical OR function with the *Subject* filter. The entry in this field defines which client certificate (remote certificate) the mGuard should adopt in order to authenticate the peer (SSH client). The client certificate can be selected from the selection list. The selection list contains the client certificates that have been loaded on the mGuard under the *"Authentication >> Certificates"* menu item. If you need to make changes to the authentication procedure, you should subsequently restart the mGuard, in order to safely end existing sessions with no longer valid certifications or passwords. The client must use exactly this certificate to authenticate itself. Further information from the certificate (validity period, issuer and subject) will not be considered during the examination.
	Authorized for access as	**All users / root / admin / netadmin / audit / mobile** Filter which specifies that the SSH client has to be authorized for a specific administration level in order to gain access. When establishing a connection, the SSH client shows its certificate and also specifies the system user for which the SSH session is to be opened (*root, admin, netadmin, audit, mobile*). Access is only granted if the entries match those defined here. Access for all listed system users is possible when *All users* is set. The *netadmin* and *audit* setting options relate to access rights with the mGuard device manager (FL MGUARD DM).

4.1.4 E-Mail



Management >> System Settings >> E-Mail		
E-mail (Make sure that the e-mail settings for the mGuard are correctly configured)	You can configure the mGuard to send e-mails via an e-mail server. Should certain events occur, notifications in plain text or machine-readable format can be sent to recipients that can be freely selected.	
	Sender address of e-mail notifications	E-mail address which is displayed as the sender from mGuard.
	Address of the e-mail server	Address of the e-mail server
	Port number of the e-mail server	Port number of the e-mail server
	Encryption mode for the e-mail server	**No encryption / TLS encryption / TLS encryption with StartTLS** Encryption mode for the e-mail server
	SMTP user name	User identifier (login)
	SMTP password	Password for the e-mail server
E-Mail notifications	Any e-mail recipients can be linked to predefined events and a freely definable message. The list is processed from top to bottom.	
	E-Mail recipient	Specifies the e-mail address.
	Event	When the selected event occurs or the event is configured for the first time, the linked recipient address is selected and the event is sent to them as an e-mail. An e-mail message can also be stored and sent. Some of the events listed depend on the hardware used. A complete list of all events can be found under "Event table" on page 66.

Management >> System Settings >> E-Mail [...]		
	Selector	Configured VPN connections (IPsec VPN / OpenVPN) or firewall rule records that are to be monitored by email can be selected here.
	E-Mail subject	Text appears in the subject line of the e-mail The text is freely definable. You can use blocks from the event table which can be inserted as placeholders in plain text (\A and \V) or in machine-readable format (\a and \v). Time stamps in the form of a placeholder (\T or \t (machine readable)) can also be inserted.
	E-Mail message	Here you can enter the text that is sent as an e-mail. The text is freely definable. You can use blocks from the event table which can be inserted as placeholders in plain text (\A and \V) or in machine-readable format (\a and \v). Time stamps in the form of a placeholder can also be inserted in plain text (\T) or machine-readable format (\t).

Time stamp

Table 4-1 Time stamp examples

Plain text \T	Machine readable \t (according to RFC-3339)
Monday, April 22, 2016 13:22:36	2016-04-22T11:22:36+0200

Event table

Table 4-2 Event table

Plain text		Machine readable	
\A = event	**\V = value**	**\a = event**	**\v = value**
State of the ECS	Not present	/ecs/status	1
	Removed		2
	Present and in sync		3
	Not in sync		4
	Inserted		5
	Generic error		8
Connectivity check result of the internal interface	Connectivity check succeeded	/redundancy/cc/int/ok	yes
	Connectivity check failed		no
Connectivity check result of the external interface	Connectivity check succeeded	/redundancy/cc/ext1/ok	yes
	Connectivity check failed		no
Validity of the positional data	Positioning data not valid	/gps/valid	no
	Positioning data valid		yes
Telephone number and message of an incoming text message		/gsm/incoming_sms	

Table 4-2 Event table

Plain text		Machine readable	
\A = event	\V = value	\a = event	\v = value
Roaming state of the mobile network engine	Registered to home network	/gsm/roaming	no
	Registered to foreign network		yes
	Not registered		unknown
Registration state to the mobile network	Not registered to mobile network	/gsm/service	no
	Registered to mobile network		yes
Currently selected SIM slot	Using SIM 1	/gsm/selected_sim	1
	Using SIM 2		2
	SIM interface disabled		0
Mobile network fallback SIM activity	Normal operation (primary SIM)	/gsm/sim_fallback	no
	Fallback mode (secondary SIM)		yes
Mobile network probes	Network probes are disabled	/gsm/network_probe	disabled
	Network probes are enabled		enabled
	Network probes failed		failed
	Network probes succeeded		succeeded
State of the alarm output	Alarm output closed / high [OK]	/ihal/contact	close
	Alarm output is open / low [FAILURE]		open
Reason for activating the alarm output	No alarm	/ihal/contactreason	
	No network link on external interface		link_ext
	No network link on internal interface		link_int
	Power supply 1 out of order		psu1
	Power supply 2 out of order		psu2
	Board temperature exceeding configured bounds		temp
	Redundancy connectivity check failed		ccheck
	The internal modem is offline		modem
	No network link on LAN2		link_swp0
	No network link on LAN3		link_swp1
	No network link on LAN1		link_swp2
	No network link on LAN4		link_swp3
	No network link on LAN5		link_swp4
	No network link on DMZ		link_dmz
State of the power supply 1	Power supply 1 working	/ihal/power/psu1	ok
	Power supply 1 out of order		fail
State of the power supply 2	Power supply 2 working	/ihal/power/psu2	ok
	Power supply 2 out of order		fail
State of the input/CMD 1	Service input/CMD1 activated	/ihal/service/cmd1	on
	Service input/CMD1 deactivated		off

Table 4-2 Event table

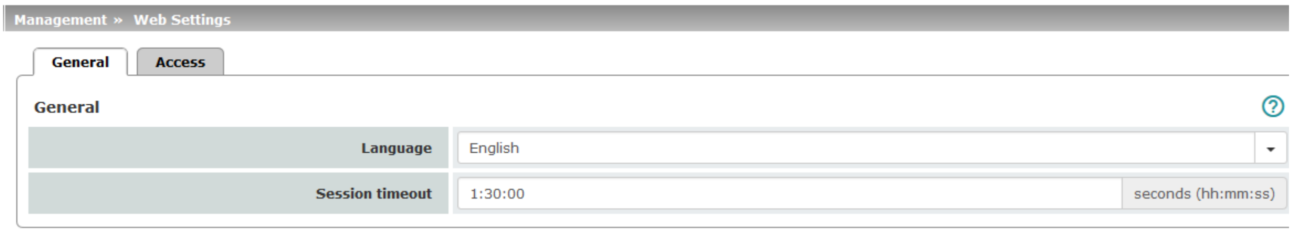
Plain text		Machine readable	
\A = event	**\V = value**	**\a = event**	**\v = value**
State of the input/CMD 2	Service input/CMD2 activated	/ihal/service/cmd2	on
	Service input/CMD2 deactivated		off
State of the input/CMD 3	Service input/CMD3 activated	/ihal/service/cmd3	on
	Service input/CMD3 deactivated		off
Board temperature	Temperature OK	/ihal/tempera-ture/board_alarm	ok
	Temperature too hot		hot
	Temperature too cold		cold
Temporary state of the secondary external inter-face	On standby	/network/ext2up	no
	Temporarily up		yes
Modem network connec-tion state State of the modem	Not connected	/network/mo-dem/state	offline
	Dialing		dialing
	Online		online
	Initialized waiting		init
Status of redundancy	The redundancy controller starts up	/redundancy/status	booting
	No sufficient connectivity		faulty
	No sufficient connectivity and waiting for a component		faulty_waiting
	Synchronizing with active device		outdated
	Synchronizing with active device and waiting for a component		outdated_waiting
	On standby		on_standby
	On standby and waiting for a component		on_standby_waiting
	Becoming active		becomes_active
	Actively forwarding network traffic		active
	Actively forwarding network traffic and waiting for a component		active_waiting
	Going on standby		becomes_standby
IPsec VPN connection preparation state	Stopped	/vpn/con/*/armed	no
	Started		yes
IPsec SA state of the VPN connection	No IPsec SAs established	/vpn/con/*/ipsec	down
	Not all IPsec SAs established		some
	All IPsec SAs established		up
Activation state of a fire-wall rule record	The state of the firewall rule records has changed	/fwrules/*/state	inactive
			active

Table 4-2 Event table

Plain text		Machine readable	
\A = event	**\V = value**	**\a = event**	**\v = value**
OpenVPN connection activation state	Stopped	/openvpn/con/*/armed	no
	Started		yes
OpenVPN connection state	Down	/openvpn/con/*/state	down
	Established		up

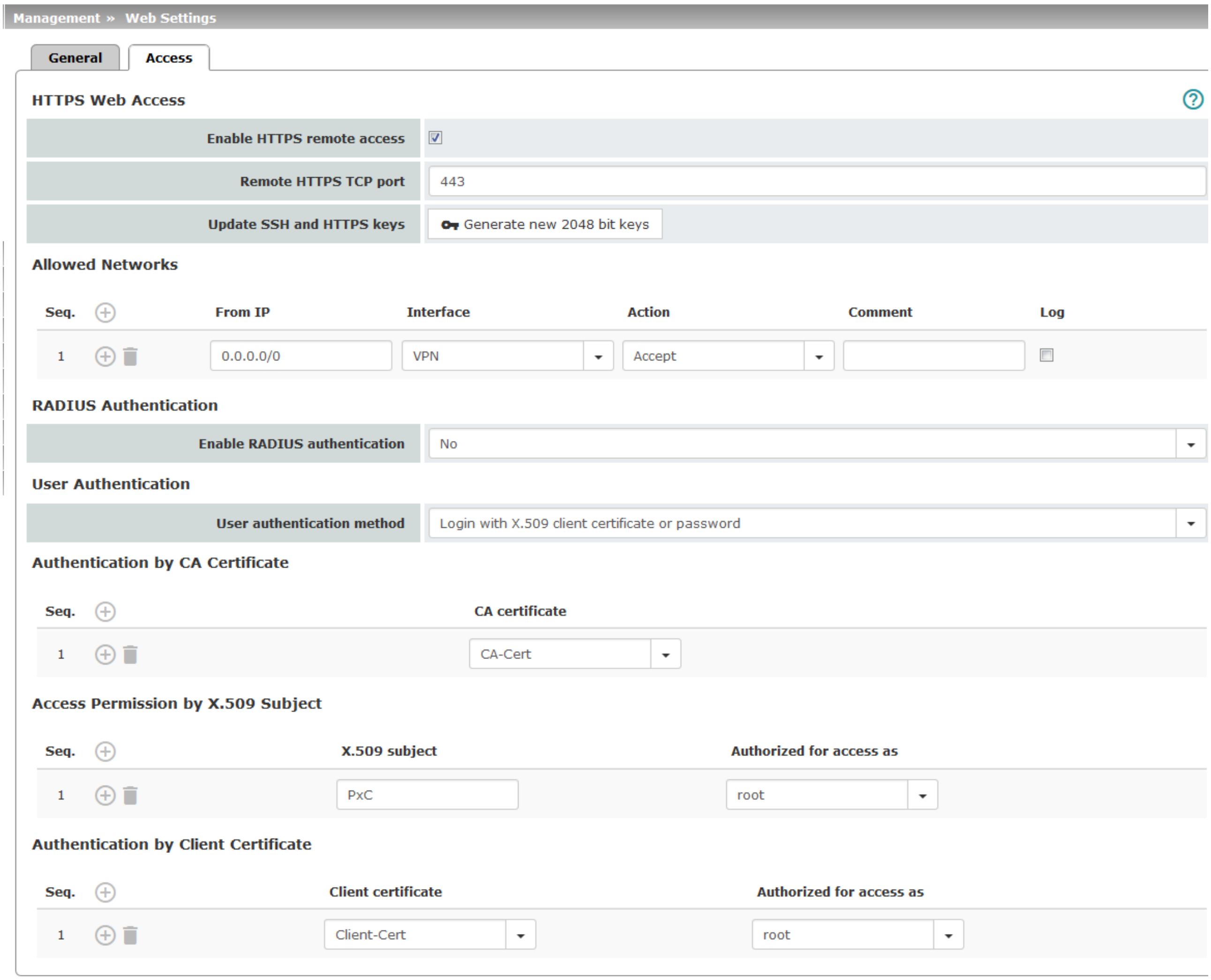
4.2 Management >> Web Settings

4.2.1 General



Management >> Web Settings >> General		
General	**Language**	If **Automatic** is selected in the list of languages, the device uses the language setting of the computer's web browser.
	Session timeout	Specifies the period of inactivity after which the user will be automatically logged out of the mGuard web interface. Possible values: 15 to 86400 seconds (= 24 hours) The entry can be in seconds [ss], minutes and seconds [mm:ss] or hours, minutes, and seconds [hh:mm:ss].

4.2.2 Access

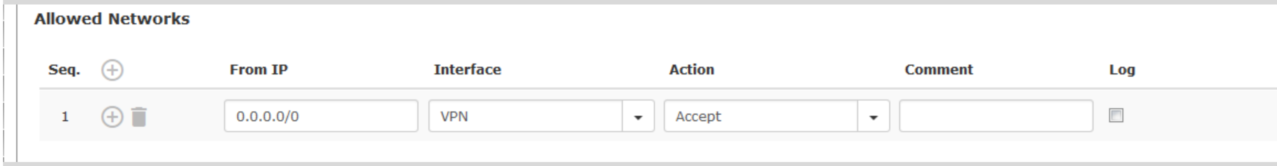


The mGuard must not be simultaneously configured via web access, shell access or SNMP. Simultaneous configuration via the different access methods might lead to unexpected results.

Management >> Web Settings >> Access	
HTTPS Web Access	When HTTPS remote access is activated, the mGuard can be configured **from remote computers** via its web interface. Access is via a web browser (e.g., Mozilla Firefox, Google Chrome, Microsoft Internet Explorer). Always use **Current web browsers** to avoid use of weak encryption algorithms. If you need to make changes to the authentication procedure, you should subsequently restart the mGuard, in order to safely end existing sessions with no longer valid certifications or passwords. **HTTPS remote access** is deactivated by default. Once activated it can be restricted to selected interfaces and networks. **NOTE: The device may be accessible via external networks.** Depending on the settings, the services of the device may be accessible via external networks or the internet. Make sure that access is only possible if it is desired. Otherwise, configure your network accordingly to prevent such access. **NOTE:** Local HTTPS access via the “Internal” interface is permitted by default independently of the activation of HTTPS remote access. The **Enable HTTPS remote access** function must be activated and the firewall rules for the internal interface must then be defined accordingly in order to specify differentiated access options on the mGuard via the internal interface (see "Allowed Networks" on page 73). **NOTE:** If remote access is enabled, make sure that secure passwords are defined for *root* and *admin* users. If you need to make changes to the password for *root* or *admin*, you should subsequently restart the mGuard, in order to safely end existing sessions with no longer valid certifications or passwords.
	Enable HTTPS remote access: Activate the function to enable HTTPS remote access. HTTPS access via the *Internal* interface (i.e., from the directly connected LAN or from the directly connected computer) can be enabled independently of the activation of this function. Following activation of the remote access, access is possible via *Internal*, *VPN*, and *Dial-in*. The firewall rules for the available interfaces must be defined accordingly in order to specify differentiated access options on the mGuard (see "Allowed Networks" on page 73). In addition, the authentication rules under **User authentication** must be set, if necessary.

Management >> Web Settings >> Access [...]		
	Remote HTTPS TCP port	**Default: 443** If this port number is changed, the new port number only applies for access via the *External, External 2, DMZ, VPN*, *GRE*, and *Dial-in* interface. Port number 443 still applies for internal access. In Stealth mode, incoming traffic on the port specified is no longer forwarded to the client. In Router mode with NAT or port forwarding, the port number set here has priority over the rules for port forwarding. The remote peer that implements remote access may have to specify the port number defined here after the IP address when entering the address. **Example:** if this mGuard can be accessed over the Internet via address 123.124.125.21 and port number 443 has been specified for remote access, you do not need to enter this port number after the address in the web browser of the remote peer. If a different port number is used, it should be entered after the IP address, e.g.: https://123.124.125.21:442/
	Update SSH and HTTPS keys	**Generate new 2048 bit keys** Keys that have been generated using an older firmware version might be weak and should be renewed. • Click on this button to generate a new key. • Note the fingerprints of the new keys generated. • Log in via HTTPS and compare the certificate information provided by the web browser.
Allowed Networks (Only active if **Enable HTTPS remote access** is activated)	HTTPS access to the mGuard can be restricted to selected interfaces and networks by means of firewall rules. The rules specified here only take effect if the **Enable HTTPS remote access** function is activated. Access via *Internal* is also possible if this function is deactivated. If you want to deny access via *Internal*, you must implement this explicitly by means of corresponding firewall rules, for example, by specifying *Drop* as the action. If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored. **The following options are available:**	

Management >> Web Settings >> Access [...]



From IP

Enter the address of the computer or network from which access is permitted or forbidden in this field.

IP address: **0.0.0.0/0** means all addresses. To specify an address area, use CIDR format – see "CIDR (Classless Inter-Domain Routing)" on page 26.

Interface

(This option varies depending on the device and licenses installed.)

Internal / External / External 2 / DMZ / VPN / GRE / Dial-in[1]

Specifies to which interface the rule should apply.

If no rules are set or if no rule applies, the following **default settings** apply:

- HTTPS access is permitted via *Internal, VPN*, and *Dial-in*.
- HTTPS acess via *External*, *External 2*, *DMZ*, and *GRE* is denied.

Specify the access options according to your requirements.

> If you want to deny access via *Internal, VPN* or *Dial-in*, you must implement this explicitly by means of corresponding firewall rules, for example, by specifying *Drop* as the action. **To prevent your own access being blocked**, you may have to permit access simultaneously via another interface explicitly with *Accept* before clicking on the **Save** button to activate the new setting. Otherwise, if your access is blocked, you must carry out the recovery procedure.

Action

- **Accept** means that the data packets may pass through.
- **Reject** means that the data packets are sent back and the sender is informed of their rejection. (In *Stealth* mode, *Reject* has the same effect as *Drop*.)
- **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts.

Comment

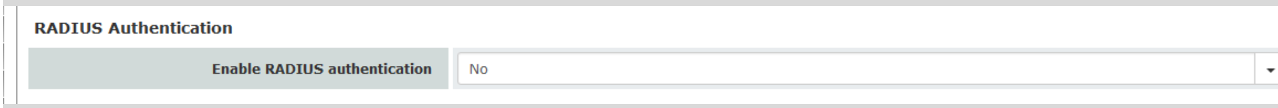
Freely selectable comment for this rule.

Log

For each individual firewall rule, you can specify whether the use of the rule:

- Should be logged – activate *Log* function
- Should not be logged – deactivate *Log* function (default)

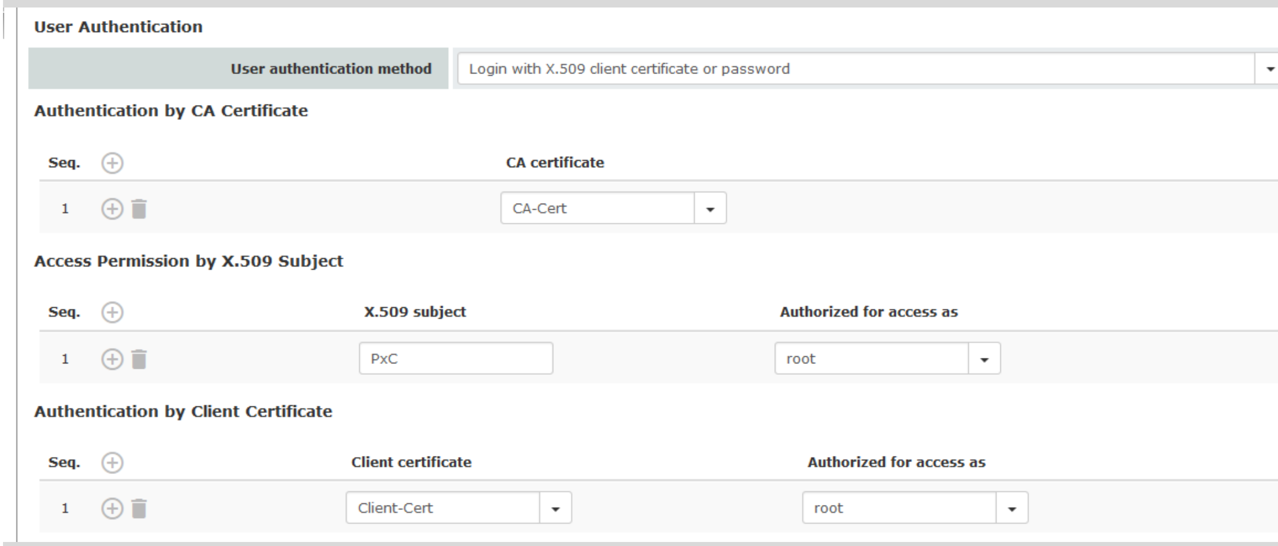
Management >> Web Settings >> Access [...]		
RADIUS authentication (This menu item is not included in the scope of functions for TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005 or FL MGUARD RS2000.)	Users can be authenticated via a RADIUS server when they log in. The password is only checked locally in the case of predefined users *(root, admin, netadmin, audit, mobile,* and *user*).	



	Enable RADIUS authentication	If the function is activated, the passwords of users who log in via HTTPS are checked via the local database. The **User authentication method** can only be set to **Login restricted to X.509 client certificate** if **No** is selected. Select **Yes** for users to be authenticated via the RADIUS server. The password is only checked locally in the case of predefined users (*root*, *admin*, *netadmin*, *audit, mobile,* and *user*). If you need to make changes to the authentication procedure, you should subsequently restart the mGuard, in order to safely end existing sessions with no longer valid certifications or passwords. The *netadmin* and *audit* authorization levels relate to access rights with the mGuard device manager (FL MGUARD DM). You should only select **As only method for password authentication** if you are an experienced user, as doing so could result in all access to the mGuard being blocked. When setting up RADIUS authentication for the first time, select **Yes**. If you do intend to use the **As only method for password authentication** option when setting up RADIUS authentication, we recommend that you create a “Customized Default Profile” which resets the authentication method. If you have selected RADIUS authentication as the only method for checking the password, it may no longer be possible to access the mGuard. For example, this may be the case if you set up the wrong RADIUS server or convert the mGuard. The predefined users (*root*, *admin*, *netadmin*, *audit, mobile,* and *user*) are then no longer accepted.

1 *External 2* and *Dial-in* are only for devices with a serial interface (see "Network >> Interfaces" on page 127).

Management >> Web Settings >> Access	
User Authentication (This menu item is not included in the scope of functions for TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005 or FL MGUARD RS2000.)	You can specify whether the mGuard user authenticates their login with a password, an X.509 user certificate or a combination of the two. If you need to make changes to the authentication procedure, you should subsequently restart the mGuard, in order to safely end existing sessions with no longer valid certifications or passwords.



Management >> Web Settings >> Access[...]		
Specifies how the local mGuard authenticates the remote peer	**User authentication method**	**Login with password** Specifies that the remote mGuard user must use a password to log into the mGuard. The password is specified under the *Authentication >> Administrative Users* menu (see *Page 231*). The option of RADIUS authentication is also available (see Page 238). If you need to make changes to the authentication procedure or change passwords, you should subsequently restart the mGuard in order to safely end existing sessions with no longer valid certifications or passwords. Depending on which user identifier is used to log in (user or administrator password), the user has the appropriate rights to operate and/or configure the mGuard accordingly. **Login with X.509 client certificate or password** User authentication is by means of login with a password (see above) or The user’s web browser authenticates itself using an X.509 certificate and a corresponding private key. Additional details must be specified below. The use of either method depends on the web browser of the remote user. The second option is used when the web browser provides the mGuard with a certificate. **Login restricted to X.509 client certificate** The user's web browser must use an X.509 certificate and the corresponding private key to authenticate itself. Additional details must be specified here. Before enabling the *Login restricted to X.509 client certificate* option, you must first select and test the *Login with X.509 client certificate or password* option. Only switch to *Login restricted to X.509 client certificate* when you are sure that this setting works. **Otherwise your access could be blocked.** Always take this precautionary measure when modifying settings under **User Authentication**.

If the following **User authentication methods** are defined:
- *Login restricted to X.509 client certificate*
- *Login with X.509 client certificate or password*

You must then specify how the mGuard authenticates the remote user according to X.509.

The table below shows which certificates must be provided for the mGuard to authenticate the user (access via HTTPS) if the user or their web browser shows one of the following certificate types when a connection is established:
- A certificate signed by a CA
- A self-signed certificate

For additional information about the table, see "Authentication >> Certificates" on page 241.

X.509 authentication for HTTPS

The peer shows the following:	Certificate (specific to individual), **signed by CA**[1]	Certificate (specific to individual), **self-signed**
The mGuard authenticates the peer using:	⇕	⇕
	All CA certificates that form the chain to the root CA certificate together with the certificate shown by the peer PLUS (if required) Client certificates (remote certificates), **if** used as a filter	Client certificate (remote certificate)

1 The peer can additionally provide sub-CA certificates. In this case, the mGuard can form the set union for creating the chain from the CA certificates provided and the self-configured CA certificates. The corresponding root certificate must always be available on the mGuard.

According to this table, the certificates that must be provided are the ones the mGuard uses to authenticate a remote user (access via HTTPS) or their web browser.

The following instructions assume that the certificates have already been correctly installed on the mGuard (see "Authentication >> Certificates" on page 241).

> If the use of revocation lists (CRL checking) is activated under the Authentication >> Certificates*, Certificate Settings* menu item, each certificate signed by a CA that is “shown” by the HTTPS clients must be checked for revocations.

Management >> Web Settings >> Access		
	Authentication by CA Certificate	This configuration is only necessary if the user (access via HTTPS) shows a certificate signed by a CA. If you need to make changes to the authentication procedure, you should subsequently restart the mGuard, in order to safely end existing sessions with no longer valid certifications or passwords. All CA certificates required by the mGuard to form the chain to the relevant root CA certificate with the certificates shown by the user must be configured. If the web browser of the remote user also provides CA certificates that contribute to forming the chain, then it is not necessary for these CA certificates to be installed on the mGuard and referenced at this point. However, the corresponding root CA certificate must be installed on the mGuard and made available (referenced) at all times. When selecting the CA certificates to be used or when changing the selection or the filter settings, you must first select and test the *Login with X.509 client certificate or password* option as the *User authentication method* before enabling the (new) setting. Only switch to *Login restricted to X.509 client certificate* when you are sure that this setting works. **Otherwise your access could be blocked.** Always take this precautionary measure when modifying settings under **User Authentication**.
	Access Permission by X.509 Subject	Enables a filter to be set in relation to the contents of the *Subject* field in the certificate shown by the web browser/HTTPS client. It is then possible to restrict or enable access for the web browser/HTTPS client, which the mGuard would accept in principle based on certificate checks: – Restricted access to certain *subjects* (i.e., individuals) and/or to *subjects* that have certain attributes or – Access enabled for all subjects (see glossary under "Subject, certificate" on page 453) The *X.509 subject* field must not be left empty.

Management >> Web Settings >> Access [...]

Access enabled for all subjects (i.e., individuals):

An * (asterisk) in the *X.509 subject* field can be used to specify that all subject entries in the certificate shown by the web browser/HTTPS client are permitted. It is then no longer necessary to identify or define the subject in the certificate.

Restricted access to certain subjects (i.e., individuals) and/or to subjects that have certain attributes:

In the certificate, the certificate owner is specified in the *Subject* field. The entry is comprised of several attributes. These attributes are either expressed as an object identifier (e.g., 132.3.7.32.1) or, more commonly, as an abbreviation with a corresponding value.

Example: CN=John Smith, O=Smith and Co., C=US

If certain subject attributes have very specific values for the acceptance of the web browser by the mGuard, then these must be specified accordingly. The values of the other freely selectable attributes are entered using the ***** (asterisk) wildcard.

Example: CN=*, O=*, C=US (with or without spaces between attributes)

In this example, the attribute “C=US” must be entered in the certificate under “Subject”. It is only then that the mGuard would accept the certificate owner (subject) as a communication partner. The other attributes in the certificates to be filtered can have any value.

> If a subject filter is set, the number (but not the order) of the specified attributes must correspond to that of the certificates for which the filter is to be used.
>
> Please note that the filter is case-sensitive.

> Several filters can be set and their sequence is irrelevant.

With HTTPS, the web browser of the accessing user does not specify which user or administrator rights it is using to log in. These access rights are assigned by setting filters here (under “Authorized for access as”).

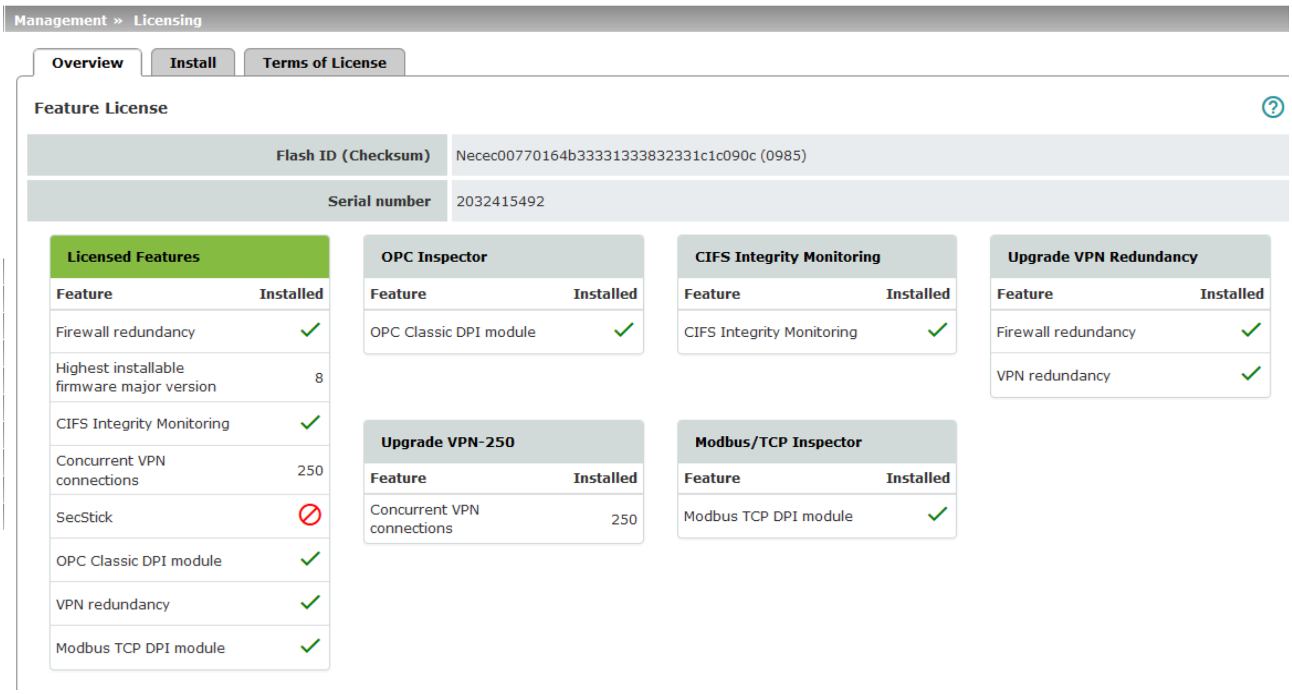
This has the following result: if there are several filters that “let through” a certain user, then the first filter applies.

Management >> Web Settings >> Access [...]		
		The user is assigned the access rights as defined by this filter. This could differ from the access rights assigned to the user in the subsequent filters. If client certificates are selected as the authentication method, then they have priority over the filter settings here.
	Authorized for access as	**root / admin / netadmin / audit / user / mobile** Specifies which user or administrator rights are granted to the remote user. For a description of the *root, admin, mobile,* and user authorization levels, see "Authentication >> Administrative Users" on page 231. The *netadmin* and *audit* authorization levels relate to access rights with the mGuard device manager (FL MGUARD DM).
	Authentication by Client Certificate	Configuration is required in the following cases: – Remote users each show a self-signed certificate. – Remote users each show a certificate signed by a CA. Filtering should take place: access is only granted to a user whose certificate copy is installed on the mGuard as the remote certificate and is provided to the mGuard in this table as the *Client certificate*. If used, this filter has priority over the *Subject* filter in the table above. The entry in this field defines which remote certificate the mGuard should adopt in order to authenticate the peer (web browser of the remote user). The client certificate can be selected from the selection list. The selection list contains the client certificates that have been loaded on the mGuard under the "Authentication >> Certificates" menu item. If you need to make changes to the authentication procedure, you should subsequently restart the mGuard, in order to safely end existing sessions with no longer valid certifications or passwords.
	Authorized for access as	**root / admin / netadmin / audit / user / mobile** Specifies which user or administrator rights are granted to the remote user. For a description of the *root, admin, mobile, and user* authorization levels, see "Authentication >> Administrative Users" on page 231. The *netadmin* and *audit* authorization levels relate to access rights with the mGuard device manager (FL MGUARD DM).

4.3 Management >> Licensing

You can obtain additional optional licenses from your supplier.

4.3.1 Overview



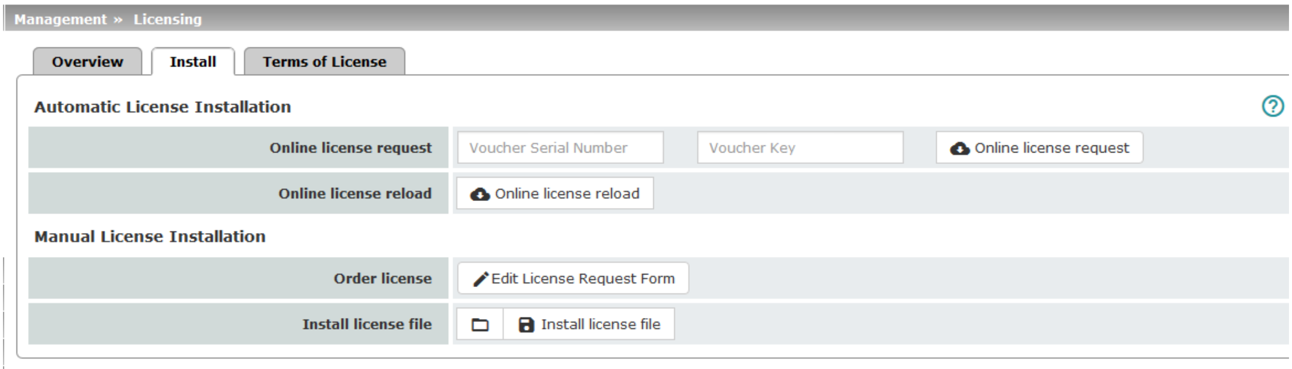
With mGuard Version 5.0 or later, licenses remain installed even after the firmware is flashed.

However, licenses are still deleted when devices with older firmware versions are flashed to Version 5.0.0 or later. Before flashing, the license for using the new update must then first be obtained so that the required license file is available for the flashing process.

This applies to major release upgrades, e.g., from Version 4.x.y to Version 5.x.y to Version 6.x.y.

Management >> Licensing >> Overview		
Basic settings	**Feature License**	Shows which functions are included with the installed mGuard licenses (e.g., the number of possible VPN tunnels or whether remote logging is supported).

4.3.2 Install



A VPN 1000 and VPN 3000 license can only be installed on the mGuard centerport (Innominate) and FL MGUARD CENTERPORT.

More functions can be added later to the mGuard license you have obtained.

You will find a voucher serial number and a voucher key in the voucher included with the mGuard. The voucher can also be obtained separately. They can be used to request the required feature license file, which you can install once you receive it.

Management >> Licensing >> Install		
Automatic License Installation	**Online license request**	Enter the serial number printed on the voucher and the corresponding voucher key, then click on the "**Online license request**" button. The mGuard now establishes a connection via the Internet and installs the corresponding license on the mGuard if the voucher is valid.
	Online license reload	This option can be used if the licenses installed on the mGuard have been deleted. Click on the "**Online license reload**" button. The licenses that were previously issued for this mGuard are then retrieved from the server via the Internet and installed.
Manual License Installation	**Order license**	After clicking on the "**Edit license request form**" button, an online form is displayed, which can be used to order the desired license. Enter the following information in the form: – **Voucher Serial Number**: the serial number printed on your voucher – **Voucher Key**: the voucher key on your voucher – **Flash Id:** this is entered automatically – **Serialnumber:** this is entered automatically After sending the form, the license file is made available for download and can be installed on the mGuard (see "Install license file").

Management >> Licensing >> Install[...]		
	Install license file	To install a license, first save the license file as a separate file on your computer, then proceed as follows: • Click on the “No file selected” button. • Select the desired license file (*.lic). Click on the “**Install license file**” button.

4.3.3 Terms of License

Lists the licenses of the external software used on the mGuard. The software is usually open-source software (for the current list see also Application Note AH EN MGUARD2 LICENSES "Free and Open Source Software" (available in the PHOENIX CONTACT Web Shop e.g. at phoenixcontact.net/product/2700634).

Management » Licensing

Overview | Install | Terms of License

mGuard Firmware License Information

The mGuard incorporates certain free and open software. Some license terms associated with this software require that Innominate Security Technologies AG provides copyright and license information, see below for details.

All the other components of the mGuard Firmware are Copyright © 2001-2016 by Innominate Security Technologies AG.

Last reviewed on 2015-07-29 for the mGuard 8.3.0 release.

atv	BSD style
bcron	GNU GPLv2
bglibs	GNU GPLv2
bridge-utils	GNU GPLv2
busybox	GNU GPLv2
c-ares	MIT derivate license, BSD style, and GNU GPLv2
conntrack	GNU GPLv2
curl	MIT/X derivate license
djbdns	Public Domain, D. J. Bernstein
ebtables	GNU GPLv2
e2fsprogs	EXT2 filesystem utilities: GNU GPLv2 lib/ext2fs: LGPLv2 lib/e2p: LGPLv2 lib/uuid: BSD style
eject	GNU GPLv2
fnord	GNU GPLv2
FreeS/WAN, Openswan	GNU GPLv2/LGPLv2 md2: Derived from the RSA Data Security, Inc. MD2 Message Digest Algorithm. md5: Derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm. libdes: BSD style libcrypto: BSD style Eric Young, BSD style OpenSSL libaes: BSD style zlib: zlib license raij: BSD style
hdparm	BSD style
HTML Utilities	BSD style
inadyn	GNU GPLv2
iproute2	GNU GPLv2
ipset	GNU GPLv2
iptables	GNU GPLv2
kbd	GNU GPLv2
lcdproc	GNU GPLv2
libcap	BSD style
libfuse	GNU GPLv2/LGPLv2
libgmp	GNU GPLv2/LGPLv2
liblzo2	GNU GPLv2
libmnl	GNU GPLv2/LGPLv2
libnetfilter_acct	GNU GPLv2/LGPLv2
libnetfilter_conntrack	GNU GPLv2
libnetfilter_cthelper	GNU GPLv2
libnetfilter_cttimeout	GNU GPLv2
libnetfilter_log	GNU GPLv2
libnetfilter_queue	GNU GPLv2
libnfnetlink	GNU GPLv2
linux	GNU GPLv2
mai-interface	Contains code derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm.
mai-script	Contains code derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm.
mguard-apps-gpl	GNU GPLv2

4.4 Management >> Update

Whether or not an mGuard device can be updated to the current firmware version or another depends on its hardware architecture, the installed firmware version, and the installed licenses.

Update information can be found in the **Release Notes** for the relevant firmware version and in the **Application Note** *Update and flash FL/TC MGUARD devices* (available in the PHOENIX CONTACT Web Shop or at help.mguard.com).

An update to mGuard firmware version 8.8.x is only possible from firmware version 8.6.1 or later.

An update to mGuard firmware version 8.6.1 is possible from all firmware versions starting with 7.6.0.

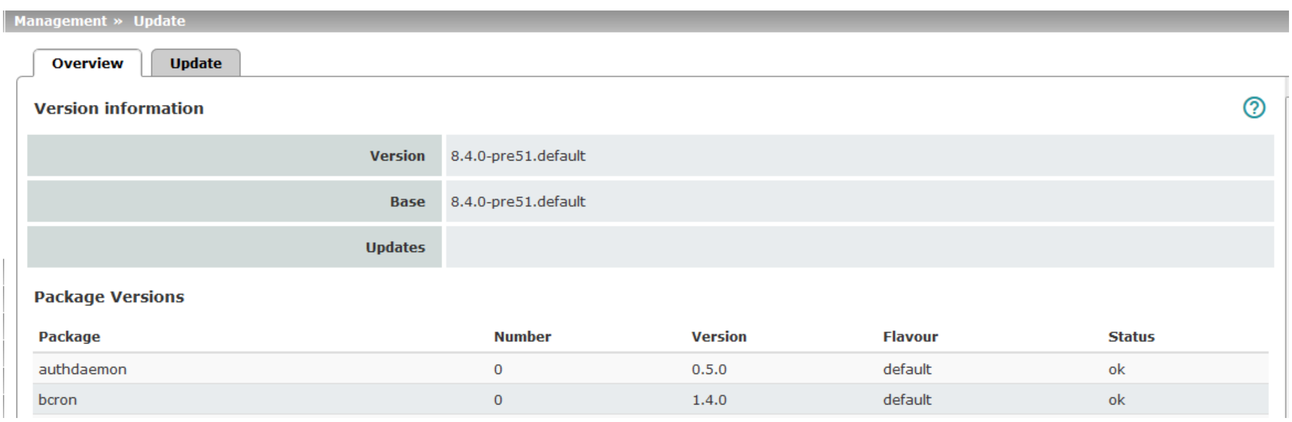
Devices with mobile network engine and installed **mGuard firmware <= 8.3.x** get the **mGuard firmware update** and the **firmware update for the mobile network engine** in two automatic, consecutive steps. This update can therefore take several minutes (indicated by the LED running light in the area of the mobile phone unit).

NOTE: The mobile network engine may be damaged if the update process is interrupted.

Do not switch the device off or interrupt the power supply to the device during the update process.

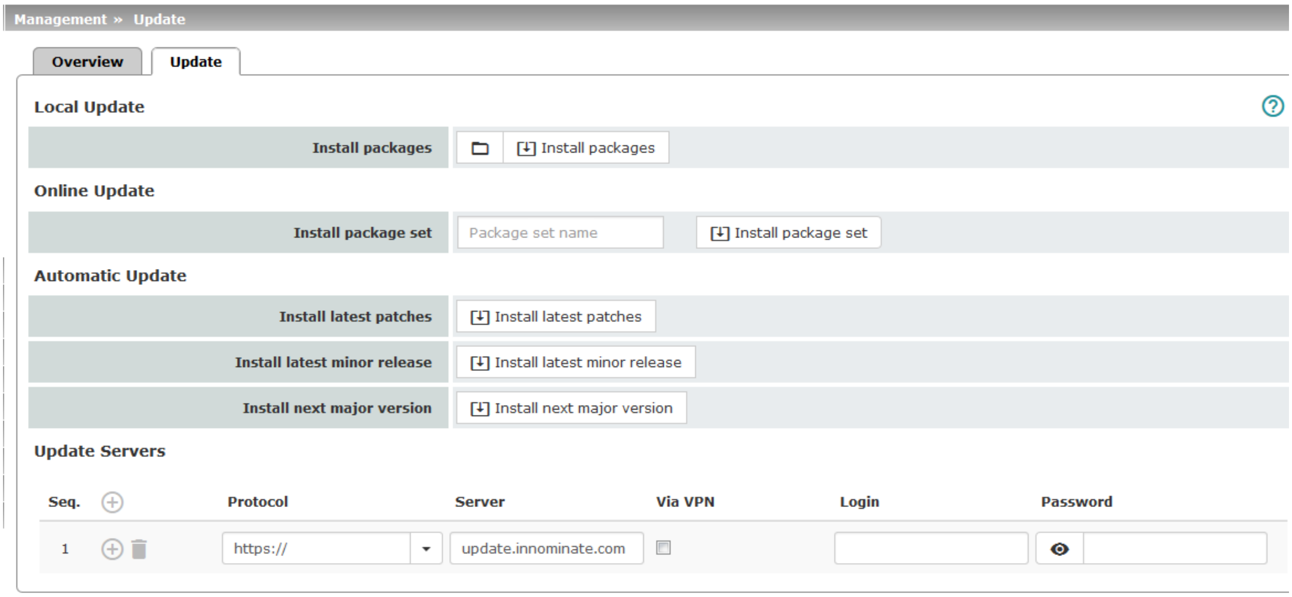
A running light for the three LEDs (signal strength) next to the antenna connections of the device indicates that an update is in progress.

4.4.1 Overview



Management >> Update >> Overview		
Version information	Lists information about the firmware version of the mGuard.	
	Version	The current software version of the mGuard.
	Base	The software version that was originally used to flash this mGuard.
	Updates	List of updates that have been installed on the base.
Package Versions	Lists the individual software modules of the mGuard. This information may be needed if support is required.	

4.4.2 Update



Firmware updates with firewall redundancy enabled

NOTE: Only the inactive device of a redundancy pair can be updated.

Procedure

- Update the inactive device of the redundancy pair first.
  After a successful update, this device automatically becomes active.
- Now start the update for the other, now inactive, device.
- Check whether both devices have been successfully updated.

Updating the firmware

There are two options for performing a firmware update:

1. You have the current package set file on your computer (the file name ends with ".tar.gz") and you perform a local update.
2. The mGuard downloads a firmware update of your choice from the update server via the Internet and installs it.

NOTE: Do not interrupt the power supply to the mGuard during the update process. Otherwise, the device could be damaged and may have to be reactivated by the manufacturer.

Depending on the size of the update, the process may take several minutes.

A message is displayed if a restart is required after completion of the update.

Management >> Update		
Local Update	**Install packages**	To install the packages, proceed as follows: • Click on the **No file selected** icon, select the file and open it. The file name of the update file depends on the device platform and the currently installed firmware version (see also **Application Note** Update FL_TC MGUARD devices – AH EN MGUARD UPDATE). **Example**: *update-8.{0-5}-8.6.1.default.mpc83xx.tar.gz* • Then click on the **Install packages** button. The following applies to devices with mobile network engine and installed **mGuard firmware version <= 8.3.x**: A local update to **mGuard firmware version 8.4.0 or later** cannot be performed, as the modem firmware update required for this cannot be carried out locally. In this case, carry out an **Online Update** or **Flash Update**.
Online Update	**Install package set**	To perform an online update, proceed as follows: • Make sure that there is at least one valid entry under **Update Servers**. You should have received the necessary details from your licensor. • Enter the name of the package set. The name of the package set depends on the currently installed firmware version (see also **Application Note** Update FL_TC MGUARD devices – AH EN MGUARD UPDATE). **Example**: *update-8.{0-5}-8.6.1.default* • Then click on the **Install package set** button.
Automatic Update	This is a version of the online update where the mGuard independently determines the required package set. With mGuard firmware Version 8.4 or later, an automatic update via the configured update server can also be started on the command line (see "Command line tool „mg“" on page 458). – Authorized users: *root* and *admin* – Command: *mg update*, parameter: *major* | *minor* | *patches* Successful implementation or any errors that occur will be documented in the log file: */var/log/psm-sanitize.*	
	Install latest patches	Patch releases resolve errors in previous versions and have a version number which only changes in the third digit position. Version 8.0.**1** is a patch release for Version 8.0.**0**.
	Install latest minor release	Minor and major releases supplement the mGuard with new properties or contain changes that affect the behavior of the mGuard. Their version number changes in the first or second digit position. Version 8.**1.0** is a minor release for Version 8.**0.1**.

Management >> Update [...]		
	Install next major version	Version **8**.6.0 is a major release for Version **7**.6.8.
Update Servers	Specify from which servers an update may be performed.	

> The list of servers is processed from top to bottom until an available server is found. The order of the entries therefore also specifies their priority.

> All configured update servers must provide the same updates.

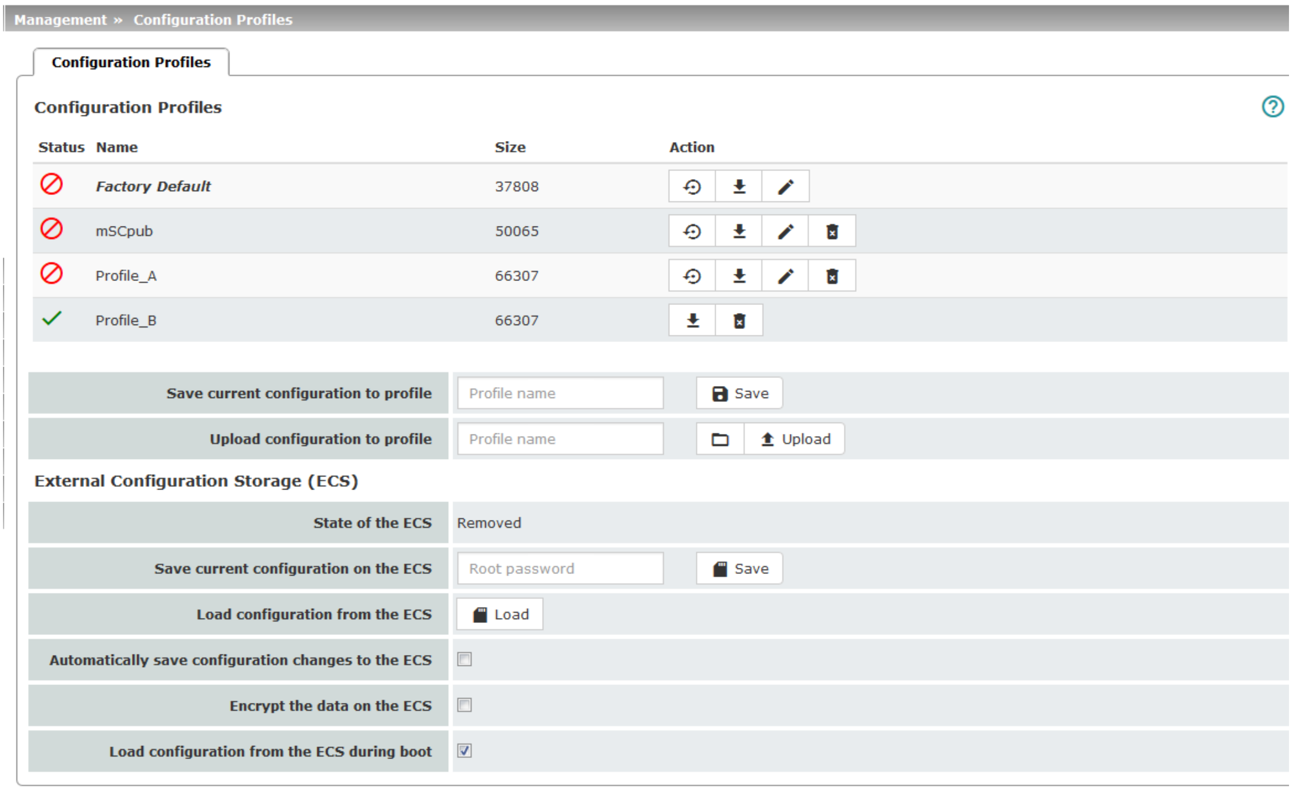
> It is not necessary to enter the login information (login + password) if the factory default update server (https://update.innominate.com) is used.

The following options are available:

Protocol	The update can be performed via HTTPS, HTTP, FTP or TFTP.
Server	Host name or IP address of the server that provides the update files.
Via VPN	The update server's request is – **where possible** – carried out via a VPN tunnel (IPsec VPN or OpenVPN). **Prerequisite**: A suitable VPN tunnel is available. If no suitable VPN tunnel is available, traffic is always sent **unencrypted via the default gateway**. A suitable VPN tunnel is available if the remote peer belongs to the remote network of a configured VPN tunnel and the mGuard has an internal IP address that belongs to the local network of the same VPN tunnel. **Please note:** **For IPsec VPN connections**, the "Via VPN" function must be activated so that the traffic is routed through a suitable IPsec VPN tunnel. **For OpenVPN connections**, traffic is always routed via a suitable OpenVPN tunnel even if the function is deactivated.
Login	Login for the server.
Password	Password for login.

4.5 Management >> Configuration Profiles

4.5.1 Configuration Profiles



You can save the settings of the mGuard as a configuration profile under any name on the mGuard. It is possible to create multiple configuration profiles. You can then switch between different profiles as required, for example, if the mGuard is used in different environments.

Furthermore, you can also save the configuration profiles as files on your configuration computer. Alternatively, these configuration files can be loaded onto the mGuard and activated.

In addition, you can restore the *Factory Default* settings at any time.

Certain models also allow the configuration profiles to be stored on external configuration storage (ECS).

– **SD card:** TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4004/RS2005, FL MGUARD RS4000/RS2000, FL MGUARD DELTA, FL MGUARD PCI(E)4000, FL MGUARD CENTERPORT
– **V.24/USB memory stick:** mGuard centerport (Innominate)
– **MEM PLUG**: FL MGUARD GT/GT
  Unencrypted configuration profiles can be stored on an external configuration memory (**MEM PLUG**) which can be connected to the M12 socket of the mGuard.
  The MEM PLUG is available in two version with different memory capacities (FL MEM PLUG and FL MEM PLUG 2).
  The memory capacity of a MEM PLUG is smaller than the memory capacity of the mGuard device.

Complex configurations, e.g. with a huge number of configured firewall rules and/or VPN connections, can lead to large configuration profiles, for which the storage capacity of a MEM PLUG is not sufficient.

Use FL MEM PLUG 2 with higher capacity (order number: 1032962) to back up your configurations in order to minimize the risk of insufficient memory capacity.

> When a configuration profile is saved, the passwords used for authenticating administrative access to the mGuard (Root password, Admin password, SNMPv3 password) are not saved.

> It is possible to load and activate a configuration profile that was created under an older firmware version. However, the reverse is not true – a configuration profile created under a newer firmware version should not be loaded and will be rejected.

Encrypted configuration memory

From mGuard firmware version 7.6.1, configuration profiles can be encrypted on the mGuard for platform 2 mGuard devices (not on FL MGUARD GT/GT). This makes rollout easier.

You can save several mGuard configurations on an SD card and then use it to start up all mGuards. During the startup process, the mGuard finds the relevant valid configuration on the SD card. This is loaded, decrypted, and used as the valid configuration (see "Encrypt the data on the ECS" on page 95.)

Recovery procedure

With firmware 8.4.0 or later, before performing the recovery procedure, the current device configuration is stored in a new configuration profile (“Recovery DATE”). Following the recovery procedure, the device starts with the default settings.

Following the recovery procedure, the configuration profile with the designation “Recovery DATE” appears in the list of configuration profiles and can be restored with or without changes.

Management >> Configuration Profiles

Configuration Profiles

At the top of the page there is a list of the configuration profiles that are stored on the mGuard, e.g., the *Factory Default* configuration profile. If any configuration profiles have been saved by the user (see below), they will be listed here.

Active configuration profile: the configuration profile that is currently enabled has an *Active* symbol at the start of the entry. If a configuration is modified in such a way that it corresponds to a stored configuration profile, the *Active* symbol appears next to it after the changes have been applied.

Configuration profiles that are stored on the mGuard can be:

– Enabled (Restore profile)
– Downloaded as a file on the connected configuration computer
– Viewed and edited (Edit profile)
– Deleted
– Downloaded as an atv file

Download configuration profile as an atv file

- Click on the name of the configuration profile in the list.

  The configuration profile is downloaded as an atv file and can be analyzed with a text editor.

Management >> Configuration Profiles [...]	
	View and edit configuration profile before restoring it (Edit profile) • Click on the **Edit profile** icon to the right of the configuration profile name. The configuration profile is loaded, but not activated yet. All entries that contain changes to the configuration currently used are highlighted in green on the relevant page and in the associated menu path. The changes displayed can be applied as they are or with further modifications, or they can be discarded: – To apply the entries for the loaded profile (with further modifications, where applicable), click on the **Save** icon. – To discard all changes, click on the **Reset** icon. **Enable the factory default or a configuration profile saved on the mGuard by the user (Restore profile)** • Click on the **Restore profile** icon to the right of the configuration profile name. The corresponding configuration profile is restored without a safety prompt being displayed and is activated immediately. **Save configuration profile as a file on the configuration computer** • Click on the **Download profile** icon to the right of the configuration profile name. • In the dialog box that is displayed, where appropriate specify the file name and storage location where the configuration profile is to be saved as a file. (The file name can be freely selected.) **Delete configuration profile** • Click on the **Delete profile** icon to the right of the configuration profile name. The profile is deleted irrevocably without a safety prompt being displayed. The *Factory Default* profile cannot be deleted.
	Save current configuration to profile — **Save current configuration as a profile on the mGuard** • Enter the desired profile name in the *Profile name* field next to “Save current configuration to profile”. • Click on the **Save** button. The configuration profile is saved on the mGuard. The profile name appears in the list of configuration profiles stored on the mGuard.

Management >> Configuration Profiles [...]		
	Upload configuration to profile	**Upload a configuration profile that has been saved to a file on the configuration computer** **Requirement**: a configuration profile has been saved on the configuration computer as a file according to the procedure described above. • Enter the desired profile name that is to be displayed in the *Profile name* field next to "**Upload configuration to profile**". • Click on the **No file selected** icon and select and open the relevant file in the dialog box that is displayed. • Click on the **Upload** button. The configuration profile is loaded on the mGuard, and the name assigned in step 1 appears in the list of profiles that are stored. Configuration profiles with settings that are actually identical may differ slightly in size (bytes) due to technical reasons. This behavior occurs when certain entries, e.g., date information, comments, permissions or firmware versions differ when the profile is created/applied.
External Configuration Storage (ECS)	Configuration profiles stored on the mGuard can be exported to external configuration storage (ECS) from where they can be imported onto mGuard devices again. Depending on the device used and the technical requirements, various types of external configuration storage can be used as the storage medium (e.g., SD cards or USB flash drives). The exported file has the file extension "ecs.tgz". Technical requirements of SD cards: – FAT file system on the first partition SD cards certified and approved by Phoenix Contact: see section „Accessories" on the product pages at phoenixcontact.net/products To import the file onto an mGuard device, the SD card or the USB flash drive must be inserted in or connected to the mGuard. The configuration can be: – Automatically loaded, decrypted, and used as the active configuration when the device is started – Loaded and activated via the web interface The configuration on the external storage medium also contains the encrypted passwords (hashed) for the users *root*, *admin*, *netadmin*, *audit*, and *user*, as well as for the SNMPv3 user. These passwords are also loaded when loading from an external storage medium.	

Management >> Configuration Profiles [...]		
	State of the ECS	The current state is updated dynamically. (See "State of the ECS" in "Event table" on page 66).
	Save current configuration on the ECS (Only for TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4004/RS2005, FL MGUARD RS4000/RS2000, FL MGUARD GT/GT, FL MGUARD DELTA, FL MGUARD PCI(E)4000, mGuard centerport (Innominate), and FL MGUARD CENTERPORT)	When replacing the original device with a replacement device, the configuration profile of the original device can be applied using the ECS. To do so, the replacement device must still use “root” as the password for the “root” user. If the root password on the replacement device is not “root”, this password must be entered in the **“Root password”** field. Click on the **Save** button to apply the entry. The memory capacity of the MEM PLUGs is smaller than the memory capacity of the mGuard device. Complex configurations, e.g. with a huge number of configured firewall rules and/or VPN connections, can lead to large configuration profiles, for which the storage capacity of a MEM PLUGS is not sufficient. Use FL MEM PLUG 2 (order number: 1032962) to back up your configurations in order to minimize the risk of insufficient memory capacity.
	Load configuration from the ECS	If there is a configuration profile on an inserted or connected ECS storage medium, clicking on the “**Load**” button imports it to the mGuard where it is enabled as the active profile. The loaded configuration profile does not appear in the list of configuration profiles stored on the mGuard.

Management >> Configuration Profiles [...]		
	Automatically save configuration changes to the ECS (Only for TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4004/RS2005, FL MGUARD RS4000/RS2000, FL MGUARD GT/GT, FL MGUARD DELTA, FL MGUARD PCI(E)4000, mGuard centerport (Innominate), FL MGUARD CENTERPORT)	When the function is activated, the configuration changes are automatically saved to the ECS, i.e., the ECS always stores the profile currently used. **NOTE: Do not save any further configuration changes if storing the last configuration change on the ECS has not yet been successfully completed.** Storing the configuration on an ECS, especially on the MEM PLUG, can take several minutes depending on the configuration. **Storing the configuration on the MEM PLUG 2 usually takes 16 minutes or longer.** Further configuration changes that are made and applied during the current storage process will not be automatically saved on the ECS. They may be lost if an "old" configuration is loaded from the ECS when booting the device. The mGuard only uses the automatically stored configuration profiles on startup if the original password (“root”) is still set on the mGuard for the “root” user. Configuration changes are made even if the ECS is disconnected, full or defective. The corresponding error messages are displayed in the Logging menu (see "Logging >> Browse Local Logs" on page 413). Activation of the new setting extends the response time of the user interface when changing any settings.
	Encrypt the data on the ECS (Only for TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4004/RS2005, FL MGUARD RS4000/RS2000, FL MGUARD PCI(E)4000, FL MGUARD DELTA, mGuard centerport (Innominate), and FL MGUARD CENTERPORT)	When the function is activated, the configuration changes are encrypted and stored on an ECS. From mGuard firmware version 7.6.1, configuration profiles can be encrypted on the mGuard for platform 2 mGuard devices (not on FL MGUARD GT/GT). This makes mGuard rollout easier. You can save several mGuard configurations on an SD card (or also on a USB stick in the case of mGuard centerport (Innominate)) and then use it to start up all mGuards. During the startup process, the mGuard finds the relevant valid configuration on the configuration storage. This is loaded, decrypted, and used as the valid configuration.
	Load configuration from the ECS during boot	When the function is activated, the ECS is accessed when booting the mGuard. The configuration profile is loaded from the ECS onto the mGuard, decrypted if necessary, and used as the valid configuration. The loaded configuration profile does not automatically appear in the list of configuration profiles stored on the mGuard.

4.6 Management >> SNMP

> The mGuard must not be simultaneously configured via web access, shell access or SNMP. Simultaneous configuration via the different access methods might lead to unexpected results.

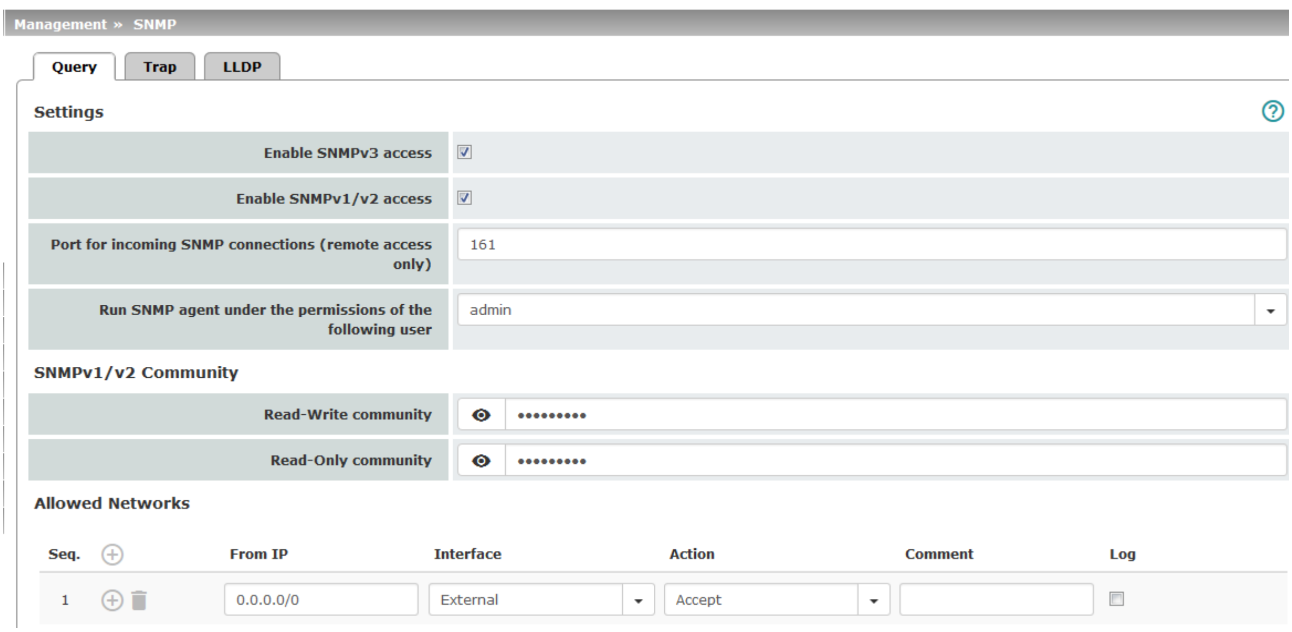
The Simple Network Management Protocol (SNMP) is primarily used in more complex networks to monitor or configure the state and operation of devices.

With mGuard firmware 8.4 or later, it is also possible to execute *Actions* on the mGuard using the SNMP protocol. Documentation of the actions that can be executed is available via the corresponding MIB file.

MIB file

To configure, monitor or control the mGuard via an SNMP client using the SNMP protocol, the corresponding MIB file must be imported into the SNMP client. MIB files are provided in a ZIP file together with the firmware or firmware updates. They can be downloaded from the manufacturer's website via the corresponding product pages: phoenixcontact.net/products.

4.6.1 Query



SNMP is available in several releases: SNMPv1/SNMPv2 and SNMPv3.

The older versions (SNMPv1/SNMPv2) do not use encryption and are not considered to be secure. The use of SNMPv1/SNMPv2 is therefore not recommended.

SNMPv3 is significantly better in terms of security, but not all management consoles support this version yet.

> Processing an SNMP request may take more than one second. However, this value corresponds to the default timeout value of some SNMP management applications.
>
> - If you experience timeout problems, set the timeout value of your management application to values between 3 and 5 seconds.

Management >> SNMP >> Query		
Settings	**Enable SNMPv3 access**	Activate the function if you wish to allow monitoring of the mGuard via SNMPv3. Following activation of the remote access, access is possible via *Internal*, *Dial-in*, and *VPN*. The firewall rules for the available interfaces must be defined on this page under **Allowed Networks** in order to specify differentiated access and monitoring options on the mGuard. Access via SNMPv3 requires authentication with a user name and password. The default setting for the access data is as follows: **User name**: admin **Password**: SnmpAdmin (It is case-sensitive.) From mGuard firmware Version 8.6.0, the SNMPv3 access data **user name** and **password** can be changed via the web interface, an ECS configuration, or a rollout script. Administration of SNMPv3 users via SNMPv3 USM is not possible. The changed user name and password can be saved on an **ECS** and restored from there. If the current configuration is saved in an **ATV configuration profile**, only the SNMPv3 user name and **not** the password is saved in the configuration profile. Archiving the profile does not change the SNMPv3s password currently on the mGuard. The addition of further SNMPv3 users is not currently supported. MD5 is used for the authentication process; DES is supported for encryption.

Management >> SNMP >> Query [...]		
	Enable SNMPv1/v2 access	Activate the function if you wish to allow monitoring of the mGuard via SNMPv1/v2. You must also enter the login data under **SNMPv1/v2 Community**. Following activation of the remote access, access is possible via *Internal*, *Dial-in*, and *VPN*. The firewall rules for the available interfaces must be defined on this page under **Allowed Networks** in order to specify differentiated access and monitoring options on the mGuard.
	Port for incoming SNMP connections	Default: 161 If this port number is changed, the new port number only applies for access via the *External, External 2, DMZ, VPN, GRE,* and *Dial-in* interface. Port number 161 still applies for internal access. In Stealth mode, incoming traffic on the port specified is no longer forwarded to the client. In Router mode with NAT or port forwarding, the port number set here has priority over the rules for port forwarding. The remote peer that implements remote access may have to specify the port number defined here when entering the address.
	Run SNMP agent under the permissions of the following user	**admin / netadmin** Specifies which permissions are used to run the SNMP agent.
SNMPv3 access data	**User name**	Changes the currently assigned SNMPv3 user name.
	Password	Changes the currently assigned SNMPv3 password. The password can only be written but not read out (*write only*). The changed user name and password can be saved in an **ECS file** and restored from there. If the current configuration is saved in an **ATV configuration profile**, only the SNMPv3 user name, and **not** the password is taken on in the configuration profile. Archiving the profile does not change the SNMPv3s password currently on the mGuard.

Management >> SNMP >> Query [...]		
SNMPv1/v2 Community	**Read-Write community**	Enter the required login data in this field.
	Read-Only community	Enter the required login data in this field.
Allowed Networks	Lists the firewall rules that have been set up. These apply for incoming data packets of an SNMP access attempt. **NOTE: The device may be accessible via external networks.** Depending on the settings, the services of the device may be accessible via external networks or the internet. Make sure that access is only possible if it is desired. Otherwise, configure your network accordingly to prevent such access. The rules specified here only take effect if the **Enable SNMPv3 access** or **Enable SNMPv1/v2 access** function is activated. If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored.	
	From IP	Enter the address of the computer or network from which access is permitted or forbidden in this field. The following options are available: – An IP address. – To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 26). – **0.0.0.0/0** means all addresses.
	Interface	**Internal / External / External 2 / DMZ / VPN / GRE / Dial-in**[1] Specifies to which interface the rule should apply. If no rules are set or if no rule applies, the following default settings apply: – SNMP access is permitted via *Internal, VPN,* and *Dial-in*. – SNMP access via *External*, *External 2*, *DMZ,* and *GRE* is denied. Specify the monitoring options according to your requirements. **NOTE:** If you want to deny access via *Internal, VPN* or *Dial-in*, you must implement this explicitly by means of corresponding firewall rules, for example, by specifying *Drop* as the action.

Management >> SNMP >> Query [...]		
	Action	**Accept** means that the data packets may pass through.
		Reject means that the data packets are sent back and the sender is informed of their rejection. (In *Stealth* mode, *Reject* has the same effect as *Drop*.)
		Drop means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts.
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – activate *Log* function – Should not be logged – deactivate *Log* function (default)

[1] *External 2* and *Dial-in* are only for devices with a serial interface (see "Network >> Interfaces" on page 127).

4.6.2 Trap


Management » SNMP
Query
Trap
LLDP
Basic Traps
SNMP authentication
Link up/down
Coldstart
Admin connection attempt (SSH, HTTPS)
Admin access (SSH, HTTPS)
New DHCP client
Hardware-related Traps
Chassis (power, signal relay)
Service input/CMD
Agent (external config storage, temperature)
CIFS Integrity Traps
Successful integrity check of a CIFS share
Failed integrity check of a CIFS share
Found a (suspicious) difference on a CIFS share
Redundancy Traps
Status change
User Firewall Traps
User firewall traps
VPN Traps
IPsec connection status changes
L2TP connection status changes
SEC-Stick traps
SEC-Stick connection status changes
Mobile Network Traps
Incoming text message and network supervision
Trap Destinations
Seq.
Destination IP
Destination port
Destination name
Destination community

In certain cases, the mGuard can send SNMP traps. SNMP traps are only sent if the SNMP request is activated.

The traps correspond to SNMPv1. The trap information for each setting is listed below. A more detailed description can be found in the MIB that belongs to the mGuard.

> If SNMP traps are sent to the peer via a VPN tunnel, the IP address of the peer must be located in the network that is specified as the **Remote** network in the definition of the VPN connection.
>
> The internal IP address must be located in the network that is specified as **Local** in the definition of the VPN connection (see IPsec VPN >> Connections >> Edit >> General).

- If the IPsec VPN >> Connections >> Edit >> General, **Local** option is set to **1:1 NAT** (see Page 338), the following applies:
  The internal IP address must be located in the specified local network.
- If the IPsec VPN >> Connections >> Edit >> General, **Remote** option is set to **1:1 NAT** (see Page 340), the following applies:
  The IP address of the remote log server must be located in the network that is specified as **Remote** in the definition of the VPN connection.

Management >> SNMP >> Trap		
Basic Traps	**SNMP authentication**	**Trap description** – enterprise-oid : mGuardInfo – generic-trap : authenticationFailure – specific-trap : 0 Sent if an unauthorized station attempts to access the mGuard SNMP agent.
	Link up/down	**Trap description** – enterprise-oid : mGuardInfo – generic-trap : linkUp, linkDown – specific-trap : 0 Sent when the connection to a port is interrupted (linkDown) or restored (linkUp).
	Cold restart	**Trap description** – enterprise-oid : mGuardInfo – generic-trap : coldStart – specific-trap : 0 Is sent after a cold restart or warm start.
	Admin connection attempt (SSH, HTTPS)	**Trap description** – enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : mGuardHTTPSLoginTrap (1) – additional : mGuardHTTPSLastAccessIP Is sent if someone has tried successfully or unsuccessfully (e.g., using an incorrect password) to open an HTTPS session. The trap contains the IP address from which the attempt was issued.

Management >> SNMP >> Trap [...]		
		– enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : mGuardShellLoginTrap (2) – additional : mGuardShellLastAccessIP Is sent when someone opens the shell via SSH or the serial interface. The trap contains the IP address of the login request. If this request was sent via the serial interface, the value is 0.0.0.0.
	Admin access (SSH, HTTPS)	**Trap description** – enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapSSHLogin – additional : mGuardTResSSHUsername mGuardTResSSHRemoteIP Is sent when someone accesses the mGuard via SSH. – enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapSSHLogout – additional : mGuardTResSSHUsername mGuardTResSSHRemoteIP Is sent when access to the mGuard via SSH is terminated.
	New DHCP client	**Trap description** – enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : 3 – additional : mGuardDHCPLastAccessMAC Is sent when a DHCP request is received from an unknown client.
Hardware-related Traps (Only TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4004/RS2005, FL MGUARD RS4000/RS2000, FL MGUARD RS)	**Chassis (power, signal relay)**	**Trap description** – enterprise-oid : mGuardTrapSenderIndustrial – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapIndustrialPowerStatus (2) – additional : mGuardTrapIndustrialPowerStatus Sent when the system registers a power failure. – enterprise-oid : mGuardTrapSenderIndustrial – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapSignalRelais (3) – additional : mGuardTResSignalRelaisState (mGuardTEsSignlalRelaisReason, mGuardTResSignal RelaisReasonIdx) Sent after the signal contact is changed and indicates the current status (0 = Off, 1 = On).

Management >> SNMP >> Trap [...]		
	Service input/CMD	**Trap description** – enterprise-oid : mGuardTrapCMD – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapCMDStateChange (1) – additional : mGuardCMDState Is sent if a service input/CMD is switched by a switch or button. A trap is sent during every switching procedure.
	Agent (external config storage, temperature)	**Trap description** – enterprise-oid : mGuardTrapIndustrial – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapIndustrialTemperature (1) – additional : mGuardSystemTemperature, mGuardTrapIndustrialTempHiLimit, mGuardTrapIndustrialLowLimit Indicates the temperature in the event of the temperature exceeding the specified limit values. – enterprise-oid : mGuardTrapIndustrial – genericTrap : enterpriseSpecific – specific-trap : mGuardTrapAutoConfigAdapterState (4) – additional : mGuardTrapAutoConfigAdapter Change Is sent after access to the ECS.
FL MGUARD BLADE controller traps (Only FL MGUARD BLADE)	**Blade status change** (Blade switch, failure)	**Trap description** – enterprise-oid : mGuardTrapBladeCTRL – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapBladeCtrlPowerStatus (2) – additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlPowerStatus Is sent when the power supply status of the blade pack changes. – enterprise-oid : mGuardTrapBladeCTRL – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapBladeCtrlRunStatus (3) – additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlRunStatus Is sent when the blade run status changes.

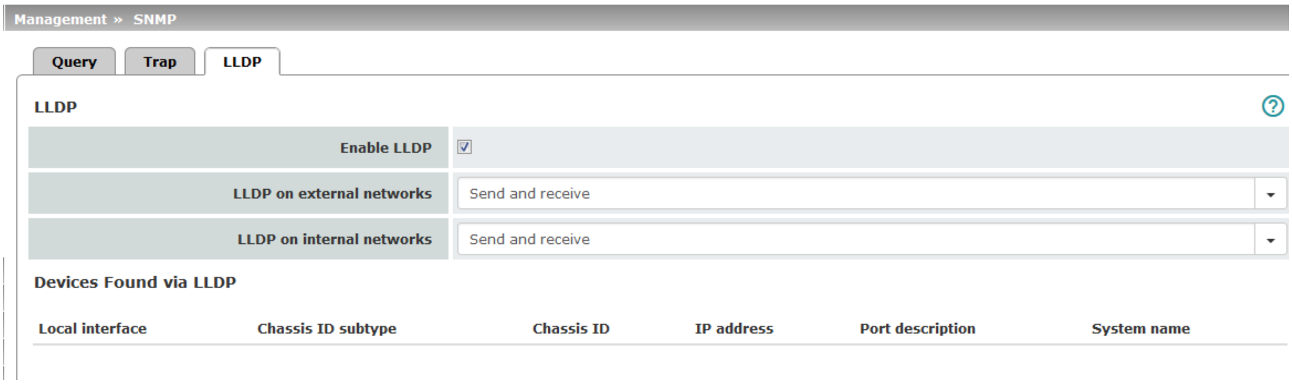
Management >> SNMP >> Trap [...]		
	Blade reconfiguration (Backup/restore)	**Trap description** – enterprise-oid : mGuardTrapBladeCtrlCfg – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapBladeCtrlCfgBackup (1) – additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlCfgBackup Is sent when configuration backup is triggered for the FL MGUARD BLADE controller. – enterprise-oid : mGuardTrapBladeCtrlCfg – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapBladeCtrlCfgRestored 2 – additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlCfgRestored Is sent when configuration restoration is triggered from the FL MGUARD BLADE controller.
CIFS Integrity Traps (Not for TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000)	**Successful integrity check of a CIFS share**	**Trap description** – enterprise-oid : mGuardTrapCIFSScan – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapCIFSScanInfo (1) – additional : mGuardTResCIFSShare, mGuardTResCIFSScanError, mGuardTResCIFSNumDiffs Is sent if the CIFS integrity check has been successfully completed.
	Failed integrity check of a CIFS share	**Trap description** – enterprise-oid : mGuardTrapCIFSScan – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapCIFSScanFailure (2) – additional : mGuardTResCIFSShare, mGuardTResCIFSScanError, mGuardTResCIFSNumDiffs Is sent if the CIFS integrity check has failed.
	Found a (suspicious) difference on a CIFS share	**Trap description** – enterprise-oid : mGuardTrapCIFSScan – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapCIFSScanDetection (3) – additional : mGuardTResCIFSShare, mGuardTResCIFSScanError, mGuardTResCIFSNumDiffs Is sent if the CIFS integrity check has detected a deviation.

Management >> SNMP >> Trap [...]		
Redundancy Traps (Not for TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000)	**Status change**	**Trap description** – enterprise-oid : mGuardTrapRouterRedundancy – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapRouterRedBackupDown – additional : mGuardTResRedundacyBackup-Down This trap is sent when the backup device (secondary mGuard) cannot be reached by the master device (primary mGuard). (The trap will only be sent if ICMP checks are activated.) – enterprise-oid : mGuardTrapRouterRedundancy – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapRRedundancyStatus-Change – additional : mGuardRRedStateSSV, mGuardRRedStateACSummary, mGuardRRedStateCCSummary, mGuardRRedStateStateRepSummary Is sent when the status of the HA cluster has changed.
Userfirewall traps (Not for TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000)	**Userfirewall traps**	**Trap description** – enterprise-oid : mGuardTrapUserFirewall – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapUserFirewallLogin (1) – additional : mGuardTResUserFirewallUsername, mGuardTResUserFirewallSrcIP, mGuardTResUserFirewallAuthenticationMethod Is sent when a user logs into the user firewall. – enterprise-oid : mGuardTrapUserFirewall – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapUserFirewallLogout (2) – additional : mGuardTResUserFirewallUsername, mGuardTResUserFirewallSrcIP, mGuardTResUserFirewallLogoutRea-son Is sent when a user logs out of the user firewall. – enterprise-oid : mGuardTrapUserFirewall – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapUserFirewallAuthError TRAP-TYPE (3) – additional : mGuardTResUserFirewallUsername, mGuardTResUserFirewallSrcIP, mGuardTResUserFirewallAuthenticationMeth-od Is sent in the event of an authentication error.

Management >> SNMP >> Trap [...]		
VPN Traps	**IPsec connection status changes**	**Trap description** – enterprise-oid : mGuardTrapVPN – genericTrap : enterpriseSpecific – specific-trap : mGuardTrapVPNIKEServerStatus (1) – additional : mGuardTResVPNStatus Is sent when the IPsec IKE server is started or stopped. – enterprise-oid : mGuardTrapVPN – genericTrap : enterpriseSpecific – specific-trap : mGuardTrapVPNIPsecConnStatus (2) – additional : mGuardTResVPNName, mGuardTResVPNIndex, mGuardTResVPNPeer, mGuardTResVPNStatus, mGuardTResVPNType, mGuardTResVPNLocal, mGuardTResVPNRemote Is sent when the status of an IPsec connection changes. – enterprise-oid : mGuard – generic-trap : enterpriseSpecific – specific-trap : mGuardTrapVPNIPsecConnStatus Is sent when a connection is established or aborted. It is not sent when the mGuard is about to accept a connection request for this connection.
	L2TP connection status changes	**Trap description** – enterprise-oid : mGuardTrapVPN – genericTrap : enterpriseSpecific – specific-trap : mGuardTrapVPNL2TPConnStatus (3) – additional : mGuardTResVPNName, mGuardTResVPNIndex, mGuardTResVPNPeer, mGuardTResVPNStatus, mGuardTResVPNLocal, mGuardTResVPNRemote Is sent when the status of an L2TP connection changes.
Mobile Network Traps (Only TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G)	**Incoming SMS and connection supervision**	Enables traps for the mobile network connection. Traps are sent when a text message is received or the mobile network connection drops.
Trap Destinations	Traps can be sent to multiple destinations.	
	Destination IP	IP address to which the trap should be sent.
	Destination port	Default: 162 Destination port to which the trap should be sent.

Management >> SNMP >> Trap [...]		
	Destination name	Optional name for the destination. Does not affect the generated traps.
	Destination community	Name of the SNMP community to which the trap is assigned.

4.6.3 LLDP



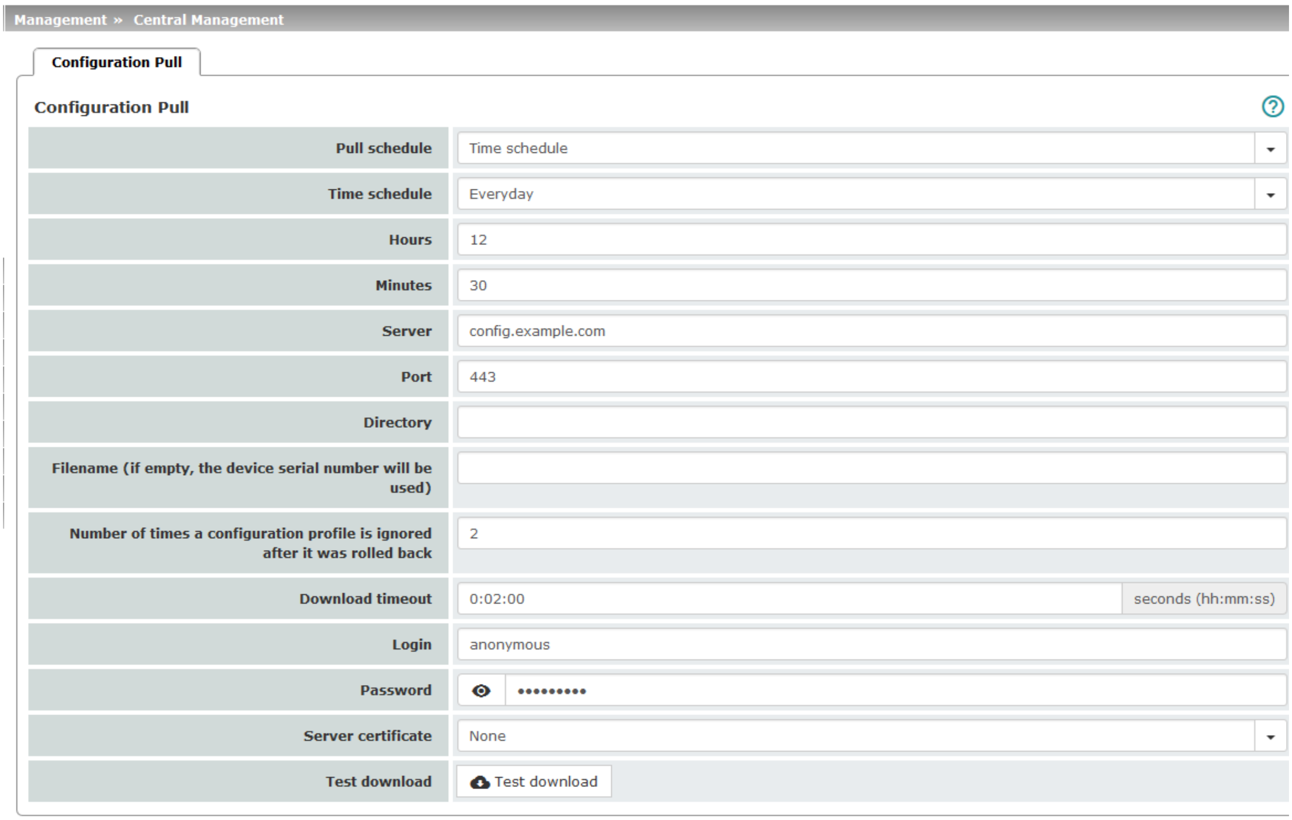
LLDP (Link Layer Discovery Protocol, IEEE 802.1AB/D13) uses suitable request methods to automatically obtain information about the network infrastructure. A system that uses LLDP can be configured so that it listens for or sends LLDP information. There are no requests for or responses to LLDP information.

As a transmitter, the mGuard periodically sends unsolicited multicasts to Ethernet level (Layer 2) in configured time intervals (typically ~30 s).

Management >> SNMP >> LLDP		
LLDP	**Enable LLDP**	The LLDP service or agent can be globally activated or deactivated here.
	LLDP on external networks	You can select whether the mGuard only **receives** or **sends and receives** LLDP information from external and/or internal networks.
	LLDP on internal networks	(See above)
Devices	**Devices Found via LLDP**	**Local interface** Local interface via which the device was found. **Chassis ID subtype** Unique chassis ID subtype of the computer found. **Chassis ID** A unique ID of the computer found; typically one of its MAC addresses. **IP address** IP address of the computer found. This can be used to perform administrative activities on the computer via SNMP. **Port description** A textual description of the network interface via which the computer was found. **System name** Host name of the computer found.

4.7 Management >> Central Management

4.7.1 Configuration Pull



The mGuard can retrieve new configuration profiles from an HTTPS server in adjustable time intervals, provided that the server makes them available to the mGuard as files (file extension: .atv). If the configuration provided differs from the current configuration of the mGuard, the available configuration is automatically downloaded and activated.

Management >> Central Management >> Configuration Pull		
Configuration Pull	**Schedule**	Here, specify whether (and if so, when and at what intervals) the mGuard should attempt to download and apply a new configuration from the server. To do this, open the selection list and select the desired value. The following also applies for all time-based controls: the mGuard also attempts to download a new configuration from the server after every restart. When **Never** is selected, the mGuard makes no attempt to download a configuration from the server. When **Once at boot** is selected, the mGuard attempts to download a configuration from the server after every restart. When **Time schedule** is selected, a new field is shown below. In this field, specify whether the new configuration should be downloaded from the server daily or regularly on a certain weekday, and at what time. Time-controlled download of a new configuration is only possible if the system time has been synchronized (see "Management >> System Settings" on page 43, "Time and Date" on page 46). Time control sets the selected time based on the configured time zone. When **Every xx min/h** is selected, the mGuard attempts to download a configuration from the server at the specified time intervals.
	Server	IP address or host name of the server that provides the configurations.
	Port	Port via which the server can be accessed.
	Directory	The directory (folder) on the server where the configuration is located.
	File name	The name of the file in the directory defined above. If no file name is defined here, the serial number of the mGuard is used with file extension ".atv".
	Number of times a configuration profile is ignored after it was rolled back	Default: 2 After retrieving a new configuration, it is possible that the mGuard may no longer be accessible after applying the new configuration. It is then no longer possible to implement a new remote configuration to make corrections. In order to prevent this, the mGuard performs the following check:
	Procedure As soon as the retrieved configuration is applied, the mGuard tries to connect to the configuration server again based on the new configuration. It then attempts to download the newly applied configuration profile again. If successful, the new configuration remains in effect.	

Management >> Central Management >> Configuration Pull [...]	
	If this check is unsuccessful for whatever reason, the mGuard assumes that the newly applied configuration profile is faulty. The mGuard remembers the MD5 total for identification purposes. The mGuard then performs a rollback. Rollback means that the last (working) configuration is restored. This assumes that the new (non-functioning) configuration contains an instruction to perform a rollback if a newly loaded configuration profile is found to be faulty according to the checking procedure described above. When the mGuard makes subsequent attempts to retrieve a new configuration profile periodically after the time defined in the **Pull schedule** field (and **Time schedule**) has elapsed, it will only accept the profile subject to the following selection criterion: the configuration profile provided **must differ** from the configuration profile previously identified as faulty for the mGuard and which resulted in the rollback. (The mGuard checks the MD5 total stored for the old, faulty, and rejected configuration against the MD5 total of the new configuration profile offered.) If this selection criterion is **met**, i.e., a newer configuration profile is offered, the mGuard retrieves this configuration profile, applies it, and checks it according to the procedure described above. It also disables the configuration profile by means of rollback if the check is unsuccessful. If the selection criterion is **not met** (i.e., the same configuration profile is being offered), the selection criterion remains in force for all further cyclic requests for the period specified in the **Number of times...** field. If the specified number of times elapses without a change of the configuration profile on the configuration server, the mGuard applies the unchanged new (“faulty”) configuration profile again, despite it being “faulty”. This is to rule out the possibility that external factors (e.g., network failure) may have resulted in the check being unsuccessful. The mGuard then attempts to connect to the configuration server again based on the new configuration that has been reapplied. It then attempts to download the newly applied configuration profile again. If this is unsuccessful, another rollback is performed. The selection criterion is enforced again for the further cycles for loading a new configuration as often as is defined in the **Number of times...** field. If the value in the **Number of times...** field is specified as **0**, the selection criterion (the offered configuration profile is ignored if it remains unchanged) will never be enforced. As a result, the second of the following objectives could then no longer be met. This mechanism has the following objectives: 1. After applying a new configuration, it must be ensured that the mGuard can still be configured from a remote location. 2. When cycles are close together (e.g., **Pull schedule** = 15 minutes), the mGuard must be prevented from repeatedly testing a configuration profile that might be faulty at intervals that are too short. This can hinder or prevent external administrative access, as the mGuard might be too busy dealing with its own processes. 3. External factors (e.g., network failure) must be largely ruled out as a reason why the mGuard considers the new configuration to be faulty.

Management >> Central Management >> Configuration Pull [...]

Download timeout

Default: 2 minutes (00:02:00)

Specifies the maximum timeout length (period of inactivity) when downloading the configuration file. The download is aborted if this time is exceeded. If and when a new download is attempted depends on the setting of Pull Schedule (see above).

The entry can be in seconds [ss], minutes and seconds [mm:ss] or hours, minutes, and seconds [hh:mm:ss].

Login

Login (user name) that the HTTPS server requests.

Password

Password that the HTTPS server requests.

> The following special characters must **not** be used in the password: ' ` \ " $ [ ] ? * ; < > | & !

Server certificate

The certificate that the mGuard uses to check the authenticity of the certificate “shown” by the configuration server. It prevents an incorrect configuration from an unauthorized server from being installed on the mGuard.

The following may be specified here:

- A self-signed certificate of the configuration server or
- The root certificate of the CA (certification authority) that issued the server certificate. This is valid when the configuration server certificate is signed by a CA (instead of self-signed).

> If the stored configuration profiles also contain the private VPN key for the VPN connection(s) with PSK, the following conditions must be met:

- The password should consist of at least 30 random upper and lower case letters and numbers (to prevent unauthorized access).
- The HTTPS server should only grant access to the configuration of this individual mGuard using the login and password specified. Otherwise, users of other mGuard devices could access this individual device.

> The IP address or the hostname specified under Server must be the same as the server certificate's common name (CN).
>
> Self-signed certificates should not use the “key-usage” extension.

Management >> Central Management >> Configuration Pull [...]		
		To install a certificate, proceed as follows: Requirement: the certificate file must be saved on the connected computer. • Click on **Browse...** to select the file. • Click on **Import**.
	Download test	Click on the **Test download** button to test whether the specified parameters are correct without actually saving the modified parameters or activating the configuration profile. The result of the test is displayed in the right-hand column. Ensure that the profile on the server does not contain unwanted variables starting with "GAI_PULL_", as these overwrite the applied configuration.

4.8 Management >> Service I/O

This menu is **only** available on the **TC MGUARD RS4000/RS2000 3G**, **TC MGUARD RS4000/RS2000 4G**, **FL MGUARD RS4004/RS2005**, **FL MGUARD RS4000/RS2000**, **FL MGUARD RS**, and **FL MGUARD GT/GT**.

Service contacts (service I/Os) can be connected to some mGuards.

- **TC MGUARD RS4000/RS2000 3G,**
- **TC MGUARD RS4000/RS2000 4G**
- **FL MGUARD RS4004/RS2005**
- **FL MGUARD RS4000/RS2000**
- **FL MGUARD RS**
- **FL MGUARD GT/GT**

Connection of the service contacts is described in the user manual for the devices (UM EN MGUARD DEVICES).

Input/CMD 1, CMD 2, CMD 3

A pushbutton or an on/off switch can be connected to the inputs. One or more freely selectable VPN connections or firewall rule records can be switched via the corresponding switch. A mixture of VPN connections and firewall rule records is also possible. The web interface displays which VPN connections and which firewall rule records are connected to this input.

The pushbutton or on/off switch is used to establish and release predefined VPN connections or to activate defined firewall rule records.

Signal contact (signal output) ACK 1, 2

You can set whether to monitor specific VPN connections or firewall rule records and to display them using LEDs.

If VPN connections are being monitored, an illuminated LED indicates that VPN connections are established.

Alarm output ACK 3

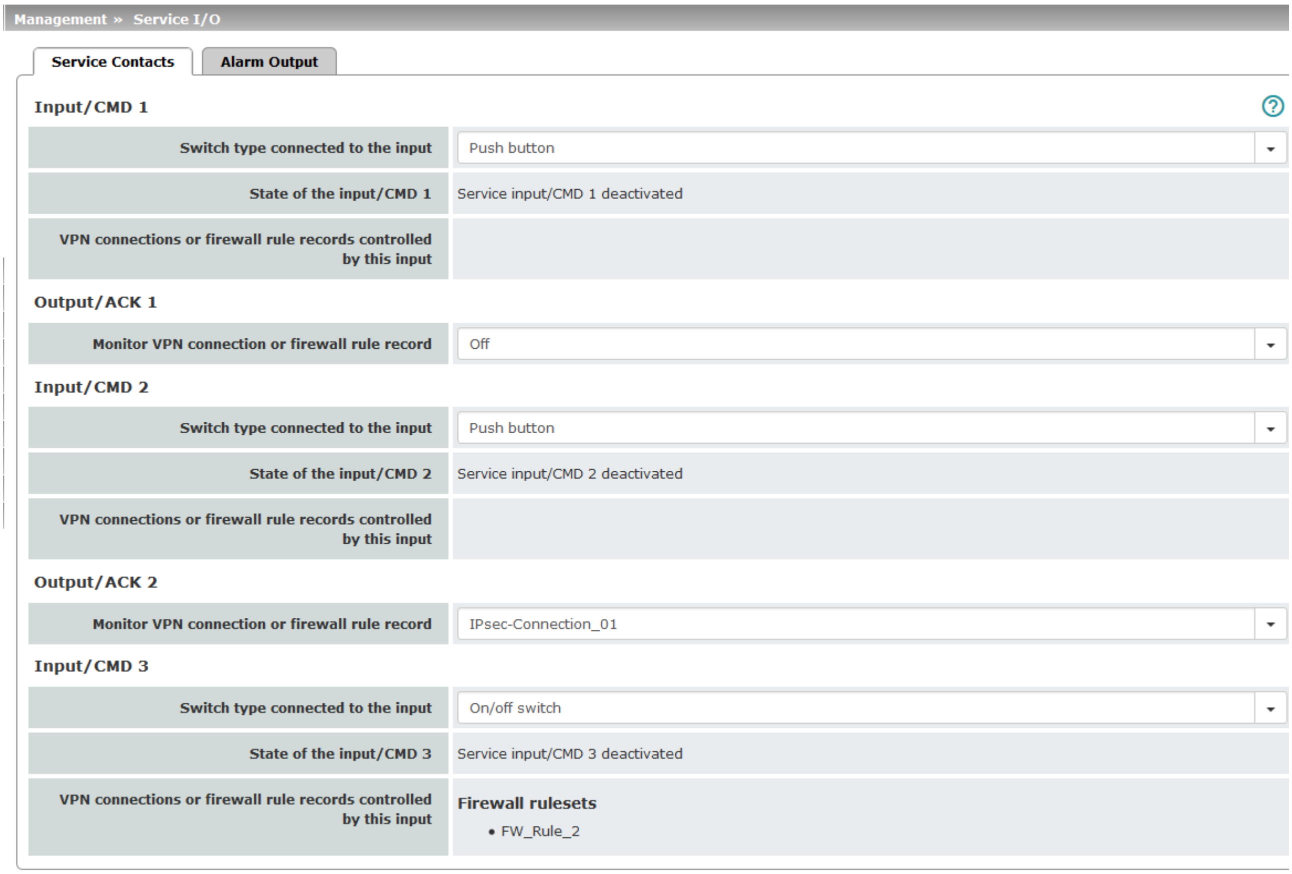
The alarm output monitors the function of the mGuard and therefore enables remote diagnostics.

The corresponding LED lights up red if the alarm output changes to the low level due to an error (inverted control logic).

The alarm output reports the following, if it has been activated.

- Failure of the redundant power supply
- Monitoring of the link status of the Ethernet connections
- Monitoring of the temperature state
- Monitoring of the connection status of redundancy
- Monitoring of the connection status of the internal modem

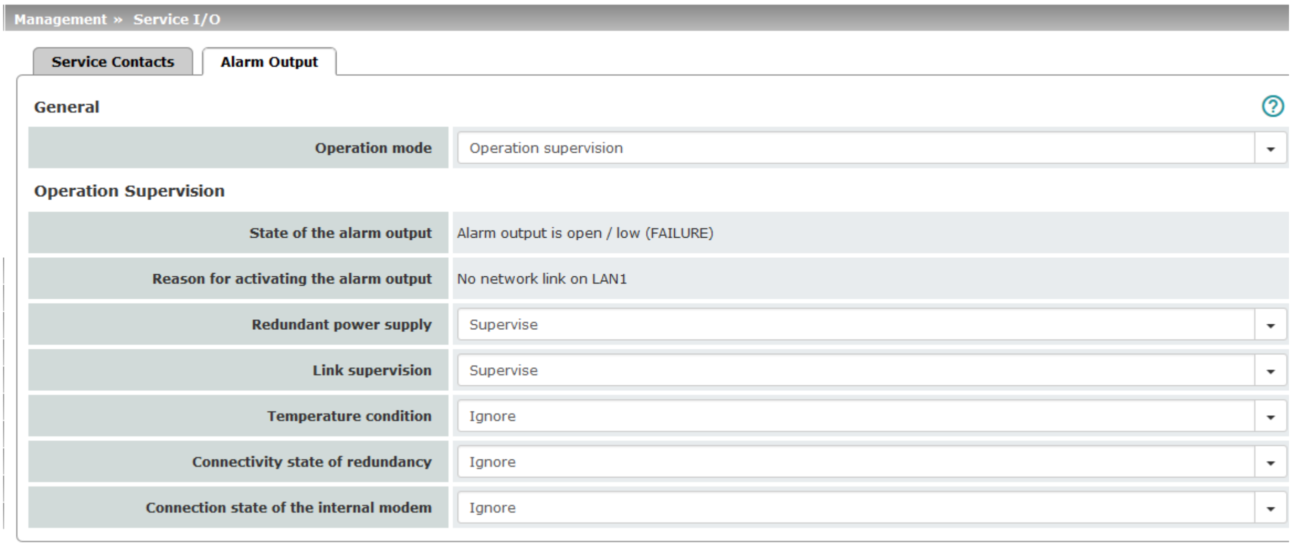
4.8.1 Service Contacts



Management >> Service I/O >> Service Contacts		
Input/CMD 1-3	**Switch type connected to the input**	**Push button / On/off switch** Select the type of switch connected.
	State of the input/CMD 1-3	Displays the state of the connected switch. When editing the VPN connection, the switch must be selected under "Controlling service input" (under “*"IPsec VPN >> Connections >> Edit >> General"* ” or *"OpenVPN Client >> Connections >> Edit >> General"*).

Management >> Service I/O >> Service Contacts[...]		
	VPN connections or firewall rule records controlled by this input	The FL MGUARD RS4000/RS2000, TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4004/RS2005, FL MGUARD RS and FL MGUARD GT/GT have connections to which external pushbuttons or an on/off switch and actuators (e.g., a signal lamp) can be connected. The pushbutton or on/off switch can be used to: – Start or stop configured VPN connections – Activate or deactivate configured firewall rule records The events that are controlled by the input can be configured here: 1. **IPsec VPN:** *"IPsec VPN >> Connections >> Edit >> General"* 2. **OpenVPN:** *"OpenVPN Client >> Connections >> Edit >> General"* 3. **Firewall rule record:** *Network Security >> Packet Filter >> Rule Records*
Output/ACK 1-2	**Monitor VPN connection or firewall rule record**	**Off/VPN connection/firewall rule record** The state of the selected VPN connection or the selected firewall rule record is indicated via the associated signal contact (ACK output).

4.8.2 Signaling output

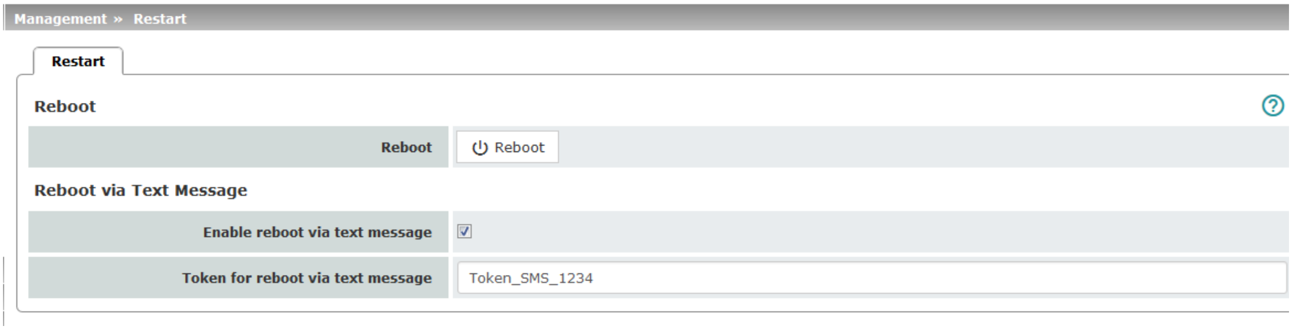


Management >> Service I/O >> Alarm output		
General	**Operating mode**	**Operation supervision / Manual setting** The alarm output can be controlled automatically using **Operation supervision** (default) or **Manual setting**.
	Manual setting	**Closed / Open (Alarm)** The desired state of the alarm output (for function control) can be selected here: If the state is manually set to **Open (Alarm)**, the FAULT LED does not light up red (no alarm).
Operation Supervision	**Current state**	Displays the state of the alarm output.
	Redundant power supply	If set to **Ignore**, the state of the power supply does not influence the alarm output. If set to **Supervise**, the alarm output is opened if either of the two supply voltages fails.
	Link supervision	**Ignore / Supervise** Monitoring of the link status of the Ethernet connections. If set to **Ignore**, the link status of the Ethernet connections does not influence the alarm output. If set to **Supervise**, the alarm output is opened if one link does not indicate connectivity. Set the links to be monitored under *Network >> Ethernet >> MAU Settings* in the *Link supervision* menu.

Management >> Service I/O >> Alarm output [...]		
	Temperature condition	The alarm output indicates overtemperature and undertemperature. The permissible range is set under *"System temperature (°C)"* in the *Management >> System Settings >> Host* menu. If set to **Ignore**, the temperature does not influence the signal contact. If set to **Supervise**, the alarm output is opened if the temperature is not within the permissible range.
	Connection state of the internal modem	Only if an internal modem is available and switched on (TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, and FL MGUARD RS with internal analog modem or ISDN modem). If set to **Ignore**, the connection status of the internal modem does not influence the alarm output. If set to **Supervise**, the alarm output is opened if the internal modem does not have a connection.
	Connectivity state of redundancy	Only if the **Redundancy** function is used (see Section 17). If set to **Ignore**, the connectivity check does not influence the alarm output. If set to **Supervise**, the alarm output is opened if the connectivity check fails. This is regardless of whether the mGuard is active or in standby mode.

4.9 Management >> Restart

4.9.1 Restart



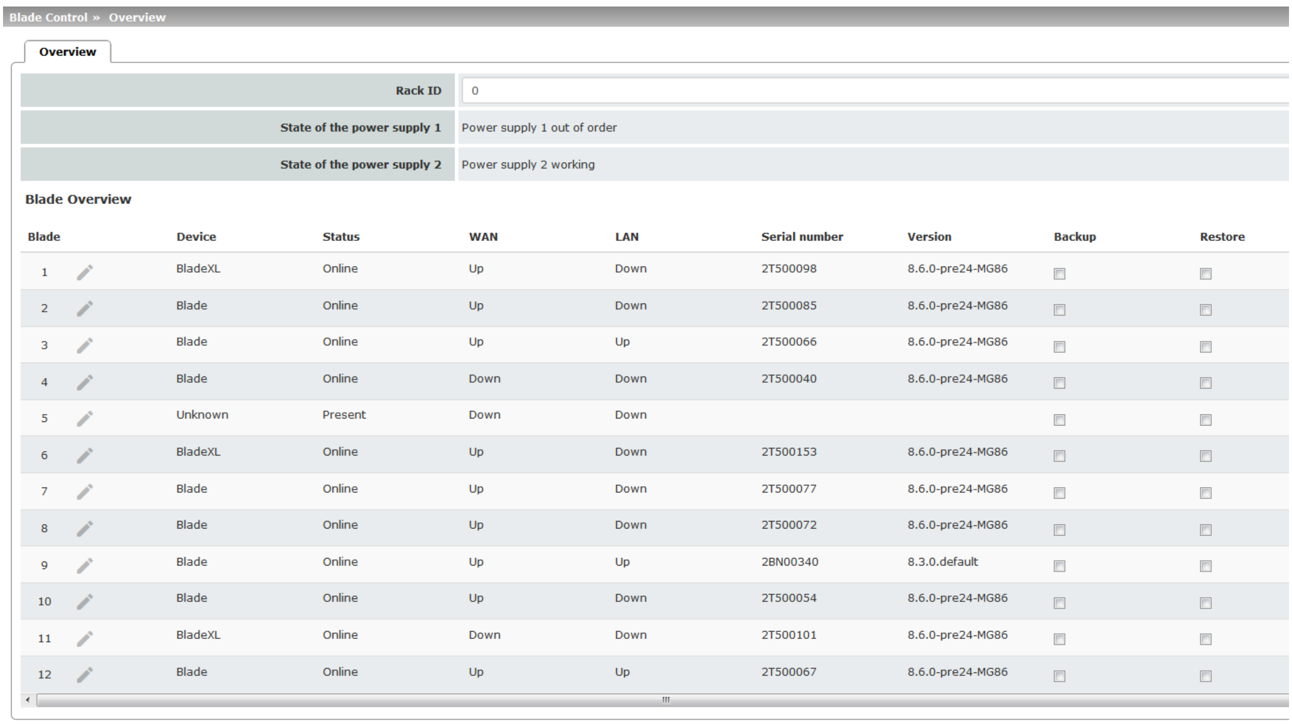
Management >> Restart >> Reboot		
Reboot	**Reboot**	Click on the "**Reboot**" button to restart (reboot) the mGuard. The device requires approx. 60 seconds to restart. A restart has the same effect as a temporary interruption to the power supply. The mGuard is switched off and back on again. A restart is required in the event of an error. It may also be required after a software update.
Reboot via Text Message (Only TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G)	**Enable reboot via text message**	With mGuard firmware Version 8.4 or later, it is possible to restart (reboot) the mGuard via text message. When the **function is activated**, the mGuard can be restarted (rebooted) via an incoming text message. The text message must contain the "*system/reboot*" command followed by a configured token (see below). Example: *system/reboot* mytoken1234 When the **function is deactivated**, a restart via text message is not possible (default).
	Token for reboot via text message	Token for restarting the mGuard via text message.

5 Blade Control menu

> Configuration of the **FL MGUARD BLADE controller** is not possible in mGuard firmware Version 8.4 and 8.5.

> This menu is only available on the **FL MGUARD BLADE controller**. For reasons of compatibility, always use the latest blade slide-in module as the controller.

5.1 Blade Control >> Overview


Blade Control » Overview

Overview

Rack ID	0
State of the power supply 1	Power supply 1 out of order
State of the power supply 2	Power supply 2 working

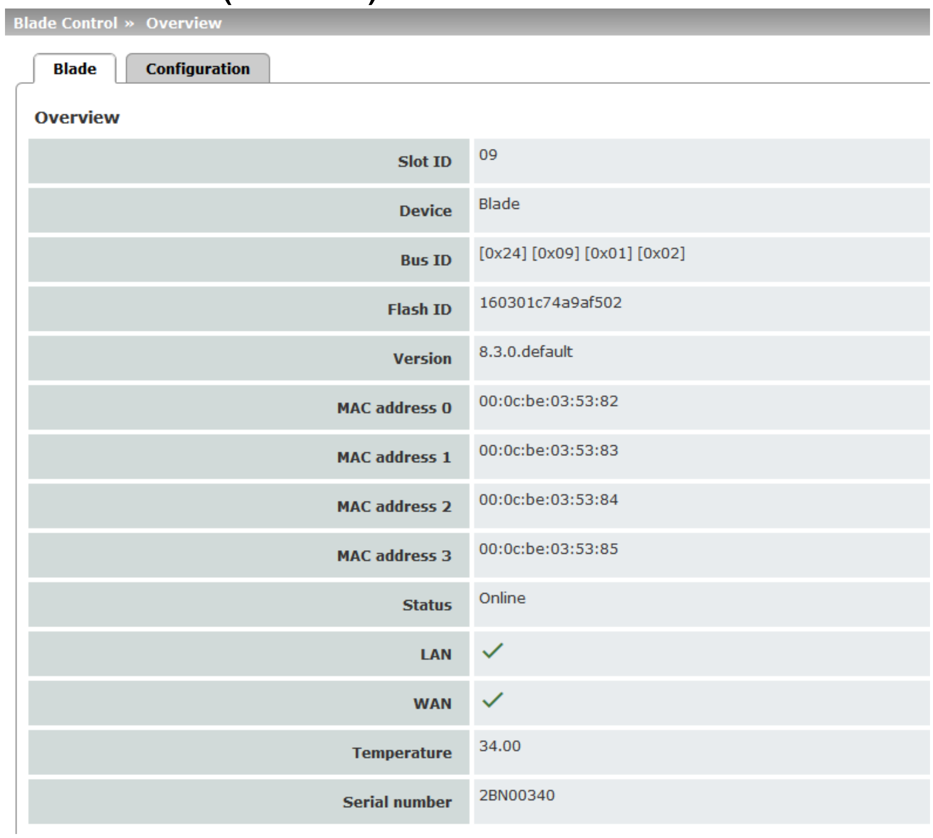
Blade Overview

Blade	Device	Status	WAN	LAN	Serial number	Version	Backup	Restore
1	BladeXL	Online	Up	Down	2T500098	8.6.0-pre24-MG86		
2	Blade	Online	Up	Down	2T500085	8.6.0-pre24-MG86		
3	Blade	Online	Up	Up	2T500066	8.6.0-pre24-MG86		
4	Blade	Online	Down	Down	2T500040	8.6.0-pre24-MG86		
5	Unknown	Present	Down	Down				
6	BladeXL	Online	Up	Down	2T500153	8.6.0-pre24-MG86		
7	Blade	Online	Up	Down	2T500077	8.6.0-pre24-MG86		
8	Blade	Online	Up	Down	2T500072	8.6.0-pre24-MG86		
9	Blade	Online	Up	Up	2BN00340	8.3.0.default		
10	Blade	Online	Up	Down	2T500054	8.6.0-pre24-MG86		
11	BladeXL	Online	Down	Down	2T500101	8.6.0-pre24-MG86		
12	Blade	Online	Up	Up	2T500067	8.6.0-pre24-MG86		

Blade Control >> Overview >> Overview		
Overview	**Rack ID**	The ID of the rack where the blade is located. This value can be configured for all blades on the controller.
	State of the power supply P1/P2	Status of power supply units P1 and P2. – Power supply 1/2 working – Power supply 1/2 out of order
Overview of blades	**Blade**	Number of the slot where the blade is installed.
	Device	Device name, e.g., “blade” or “blade XL”.

Blade Control >> Overview >> Overview[...]		
	Status	– **Online** (the device in the slot is operating correctly) – **Present** (a device is in the slot but not yet ready) – **Absent** (the slot is empty) – **Config changed** (the device configuration has changed) – **Config download** (the device's configuration profile is copied to the Blade Controller) – **Config upload** (the configuration profile is copied from the Blade Controller to the device)
	WAN	Status of the WAN port.
	LAN	Status of the LAN port.
	Serial number	Serial number of the mGuard.
	Version	Software version of the mGuard.
	Backup	**Backup**: automatic configuration backup on the controller is activated or deactivated for this slot.
	Restore	**Restore**: automatic configuration restoration (new configuration) after replacing the blade is activated or deactivated for this slot.

5.1.1 Blade (in slot #...)

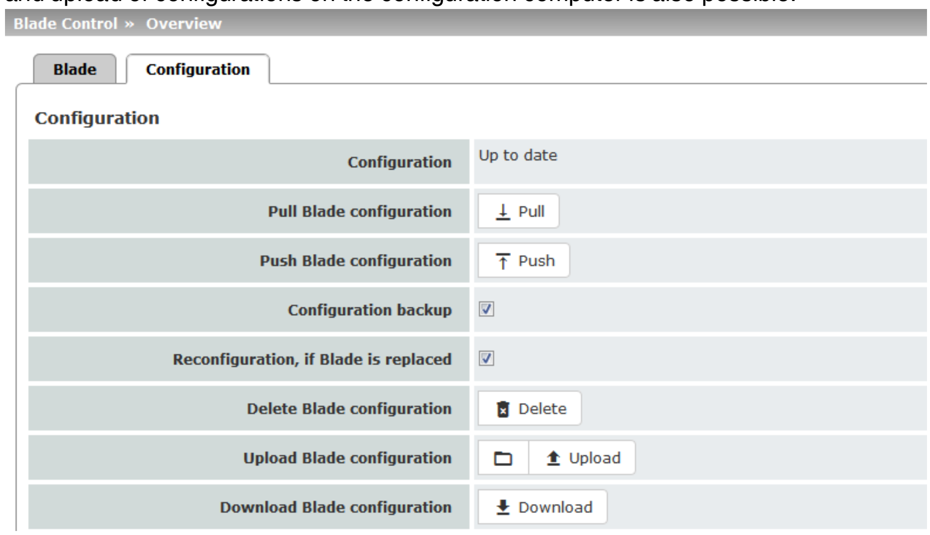


Click the **Edit row** icon to open an overview page with status information on the blade in the selected slot.

Blade Control >> Overview >> Blade (for blade in slot #...)		
Overview	**Slot ID**	The number or Slot ID of the slot used in the blade rack.
	Device	Name/Device name of the device, e.g., “blade” or “blade XL”
	Bus ID	ID of this slot on the control bus of the bladebase.
	Flash ID	Flash ID of the flash memory of the mGuard.
	Version	Version of the software installed on the mGuard.
	MAC address (0 ... 3)	All MAC addresses reserved for this mGuard.
	Status	mGuard status.
	LAN	Status of the LAN interface
	WAN	Status of the WAN interface
	Temperature	Temperature of the device. *N/A* is displayed for devices that have no temperature sensor.
	Serial number	Serial number of the mGuard.

5.1.2 Configuration

On the **Configuration** tab, configurations of the blade can be saved in the selected slot on the controller, or played back in the blade. This process can be automatic. The download and upload of configurations on the configuration computer is also possible.



Blade Control >> Overview >> Configuration		
Configuration	**Configuration**	Displays the status of the stored configuration for the blade in this slot: – No configuration file provided – Up to date – Outdated – File will be copied – Blade change detected – [---] (No blade available)
	Pull Blade configuration	The configuration of the blade in this slot is saved on the blade controller (*Pull*).
	Push Blade configuration	The configuration of the blade stored on the blade controller is played back on the blade (*Push*), and used. If the blade was reconfigured after a manual configuration backup *(Pull)*, but the new configuration was not saved again by means of *Push* on the blade controller, the configuration stored on the controller is out of date. The status of the configuration is displayed as **"outdated"**. In this case, ensure that the desired configuration is saved on the blade controller (*Pull* command).

Blade Control >> Overview >> Configuration		
	Configuration backup	When the function is activated, the configuration changes made on the blade are automatically saved on the blade controller. This corresponds to manual saving by means of *Pull* command (see above).
	Reconfiguration, if Blade is replaced	After replacing the blade in this slot, the configuration stored on the blade controller is automatically transferred to the new device in this slot.
	Delete blade configuration	Deletes the configuration stored on the blade controller for the device in this slot.
	Upload blade configuration	Uploads a configuration profile stored on the local configuration PC for this slot onto the blade controller.
	Download blade configuration	Downloads a configuration profile stored on the blade controller for this slot onto the local configuration PC.

6 Network menu

6.1 Network >> Interfaces

The mGuard has the following interfaces with external access:

	Ethernet: internal: LAN external: WAN	Serial interface	Built-in modem	Serial console via USB[1]
FL MGUARD RS4000/RS2000	**Yes**	**Yes**	**No**	**No**
FL MGUARD RS4004	**LAN: 4** **WAN: 1** **DMZ: 1**	**Yes**	**No**	**No**
FL MGUARD RS2005	**LAN: 5** **WAN: 1**	**Yes**	**No**	**No**
TC MGUARD RS4000 3G, TC MGUARD RS4000 4G	**LAN: 4** **WAN: 1** **DMZ: 1**	**Yes**	**Yes**	**No**
TC MGUARD RS2000 3G, TC MGUARD RS2000 4G	**LAN: 4** **WAN: no** **DMZ: no**	**Yes**	**Yes**	**No**
FL MGUARD CENTERPORT	**LAN: 1** **WAN: 1** **DMZ: 1**	**Yes**	**No**	**No**
FL MGUARD SMART2	**Yes**	**No**	**No**	**Yes**
FL MGUARD GT/GT, FL MGUARD RS, FL MGUARD PCI 533/266, FL MGUARD BLADE, FL MGUARD DELTA, mGuard centerport (Innominate), mGuard delta (Innominate)	**Yes**	**Yes**	**No**	**No**
FL MGUARD PCI(E)4000	**Yes**	**No**	**No**	**No**
FL MGUARD RS (ISDN/analog)	**Yes**	**Yes**	**Yes**	**No**
FL MGUARD SMART 533/266	**Yes**	**No**	**No**	**No**

1 See "Serial console via USB" on page 191.

The LAN port is connected to a stand-alone computer or the local network (internal). The WAN port is used to connect to the external network. For devices with a serial interface, the connection to the external network can also or additionally be established via the serial interface using a modem. Alternatively, the serial interface can also be used as follows: for PPP dial-in into the local network or for configuration purposes. For devices with a built-in modem (analog modem or ISDN terminal adapter), the modem can also be used to combine access options.

The details for this must be configured on the *General, Dial-out, Dial-in* and *Modem/Console* tabs. For a more detailed explanation of the options for using the serial interface (and a built-in modem), see "Modem" on page 184.

Connecting the network interface

The mGuard platforms have DTE interfaces. Connect the mGuards to the DTE interface using an Ethernet crossover cable. Here auto MDIX is permanently switched on, so it does not matter if the auto negotiation parameter is disabled.

MAC addresses

The MAC address of the WAN interface determined by the manufacturer is indicated on the type label of the device. The other MAC addresses (LAN/DMZ [optional]) can be calculated as follows:

– **WAN interface**: see type label.
– **LAN interface**: MAC address of the WANinterface incremented by 1 (**WAN + 1**).
  Devices with integrated switch: all switch ports use the same MAC address.
– **DMZ interface**: MAC address of the WAN interface incremented by 6 (**WAN + 6**).

Example:

– WAN: 00:a0:45:eb:28:9d
– LAN: 00:a0:45:eb:28:9e
– DMZ: 00:a0:45:eb:28:a3

6.1.1 Overview of "Router" network mode

> Default setting for TC MGUARD RS4000/RS2000 4G,
> TC MGUARD RS4000/RS2000 3G, FL MGUARD RS4004/RS2005,
> FL MGUARD GT/GT, mGuard centerport (Innominate), FL MGUARD CENTERPORT,
> FL MGUARD BLADE-Controller, mGuard delta (Innominate)

If the mGuard is in *Router* mode, it acts as the gateway between various subnetworks and has both an external interface (WAN port) and an internal interface (LAN port) with at least one IP address.

WAN port

The mGuard is connected to the Internet or other “external” parts of the LAN via its WAN port.

– FL MGUARD SMART2: the WAN port is the Ethernet socket.

LAN port

The mGuard is connected to a local network or a stand-alone computer via its LAN port:

– FL MGUARD SMART2: the LAN port is the Ethernet connector.
– In *Power-over-PCI mode*, the LAN port is the LAN socket of the FL MGUARD PCI(E)4000, FL MGUARD PCI(E)4000, FL MGUARD PCI 533/266.

As in the other modes, firewall and VPN security functions are available (depending on license).

> If the mGuard is operated in *Router* mode, it must be set as the default gateway on the locally connected computers.
>
> This means that the IP address of the mGuard LAN port must be specified as the default gateway address on these computers.

> NAT should be activated if the mGuard is operated in *Router* mode and establishes the connection to the Internet (see "Network >> NAT" on page 198).
>
> Only then can the computers in the connected local network access the Internet via the mGuard. If NAT is not activated, it is possible that only VPN connections can be used.

In *Router* network mode, a secondary external interface can also be configured (see "Secondary External Interface" on page 149).

There are several Router modes, depending on the Internet connection:

– Static
– DHCP
– PPPoE
– PPTP
– Modem
– Built-in modem / Built-in mobile network modem

Router Mode: Static

The external IP-settings are fixed.

Router Mode: DHCP

The external IP-settings are requested by the mGuard and assigned by an external DHCP server.

Router Mode: PPPoE

PPPoE mode corresponds to Router mode with DHCP but with one difference: the PPPoE protocol, which is used by many DSL modems (for DSL Internet access), is used to connect to the external network (Internet, WAN). The external IP address, which the mGuard uses for access from remote peers, is specified by the provider.

> If the mGuard is operated in *PPPoE* mode, the mGuard must be set as the default gateway on the locally connected computers.
>
> This means that the IP address of the mGuard LAN port must be specified as the default gateway address on these computers.

> If the mGuard is operated in *PPPoE* mode, NAT must be activated in order to access the Internet.
>
> If NAT is not activated, it is possible that only VPN connections can be used.

For the further configuration of *PPPoE* network mode, see "PPPoE" on page 141.

Router Mode: PPTP

Similar to *PPPoE* mode. For example, in Austria the PPTP protocol is used instead of the PPPoE protocol for DSL connections.

(PPTP is the protocol that was originally used by Microsoft for VPN connections.)

> If the mGuard is operated in *PPTP* mode, the mGuard must be set as the default gateway on the locally connected computers.
>
> This means that the IP address of the mGuard LAN port must be specified as the default gateway on these computers.

> If the mGuard is operated in *PPTP* mode, NAT should be activated in order to access the Internet from the local network (see "Network >> NAT" on page 198).
>
> If NAT is not activated, it is possible that only VPN connections can be used.

For the further configuration of *PPTP* network mode, see "PPTP" on page 142.

Router Mode: Modem

> Only for *FL MGUARD RS4000/RS2000, TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4004/RS2005*, *mGuard centerport (Innominate)*, *FL MGUARD CENTERPORT*, FL MGUARD RS, *FL MGUARD BLADE, mGuard delta (Innominate), FL MGUARD DELTA*

If *Modem* network mode is selected, the external Ethernet interface of the mGuard is deactivated and data traffic is transferred to and from the WAN via the externally accessible serial interface (serial port) of the mGuard.

An external modem, which establishes the connection to the telephone network, is connected to the serial interface. The connection to the WAN or Internet is then established via the telephone network (by means of the external modem).

If the address of the mGuard is changed (e.g., by changing the network mode from *Stealth* to *Router*), the device can only be accessed via the new address. If the configuration is changed via the LAN port, confirmation of the new address is displayed before the change is applied. If configuration changes are made via the WAN port, no confirmation is displayed.

If the mode is set to *Router*, *PPPoE* or *PPTP* and you then change the IP address of the LAN port and/or the local netmask, make sure you specify the correct values. Otherwise, the mGuard may no longer be accessible under certain circumstances.

For the further configuration of *Built-in mobile network modem / Built-in modem / Modem* network mode, see "Dial-out" on page 174.

After selecting *Modem* as the network mode, specify the required parameters for the modem connection on the **Dial-out** and/or **Dial-in** tab (see "Dial-out" on page 174 and "Dial-in" on page 181).

In *Modem* network mode, the serial interface of the mGuard is not available for the PPP dial-in option or for configuration purposes (see "Modem" on page 184).

Enter the connection settings for an external modem on the Modem tab page (see "Modem" on page 184).

Router Mode: Built-in modem

Only used for FL MGUARD RS devices **with** a built-in modem or ISDN terminal adapter.

If *Built-in modem* network mode is selected, the external Ethernet interface of the mGuard is deactivated and data is transferred to and from the WAN via the built-in modem or built-in ISDN terminal adapter of the mGuard. This must be connected to the telephone network. The connection to the Internet is then established via the telephone network.

After selecting *Built-in modem*, the fields for specifying the modem connection parameters are displayed.

For the further configuration of *Built-in modem / Modem* network mode (see "Dial-out" on page 174).

Router Mode: Built-in mobile network modem

Only for TC MGUARD RS4000/RS2000 3G and TC MGUARD RS4000/RS2000 4G.

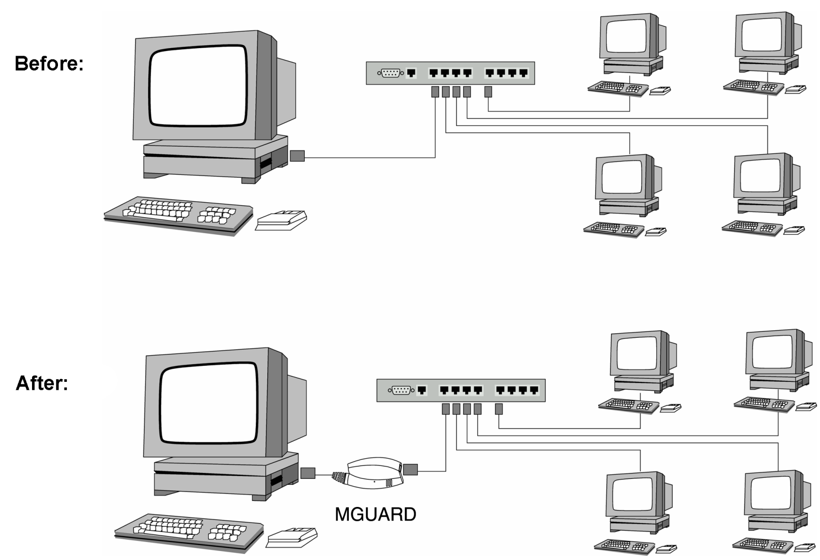
If *Built-in mobile network modem* is selected as the network mode, data traffic is routed via the built-in mobile network modem instead of the WAN port of the mGuard.

For the further configuration of *Built-in modem / Modem* network mode (see "Dial-out" on page 174).

6.1.2 Overview of "Stealth" network mode

Default setting for FL MGUARD RS4000/RS2000, FL MGUARD RS, FL MGUARD SMART2, FL MGUARD PCI(E)4000, FL MGUARD PCI(E)4000, FL MGUARD PCI 533/266, FL MGUARD DELTA

Stealth mode (Plug-n-Protect) is used to protect a stand-alone computer or a local network with the mGuard. Important: if the mGuard is in *Stealth* network mode, it is inserted into the existing network (see figure) without changing the existing network configuration of the connected devices.



(There may be as well LAN on the left side.)

The mGuard analyzes the network traffic and independently configures its network connection accordingly. It works transparently and therefore cannot be detected in the network without configured management IP address. Connected computers keep their network configuration and must not be reconfigured.

As in the other modes, firewall and VPN security functions are available (depending on licence).

Externally supplied DHCP data is allowed through to the connected computer.

In *Single-Stealth* mode, a firewall installed on the computer must be configured to allow ICMP echo requests (ping), if the mGuard is to provide services such as VPN, DNS, NTP, etc.

In *Stealth* mode, the mGuard uses internal IP address 1.1.1.1. This can be accessed from the computer if the default gateway configured on the computer is accessible.

In the *Stealth* configurations **"Autodetect"** and **"Static"**, it is not possible to establish a VPN-connection originating from the internal client through the mGuard.

In *Stealth* network mode, a secondary external interface can also be configured (see "Secondary External Interface" on page 149).

Stealth configurations

Autodetect

The mGuard analyzes the outgoing network traffic and independently configures its network connection accordingly. It operates transparently.

> For the use of certain functions (e.g. automatic updates, licence updates or establishment of VPN-connections), it is required that the mGuard makes its own requests of external servers, even in stealth mode.
>
> These requests are only possible when the locally connected computer permits ping requests. Configure its security settings accordingly.

Static

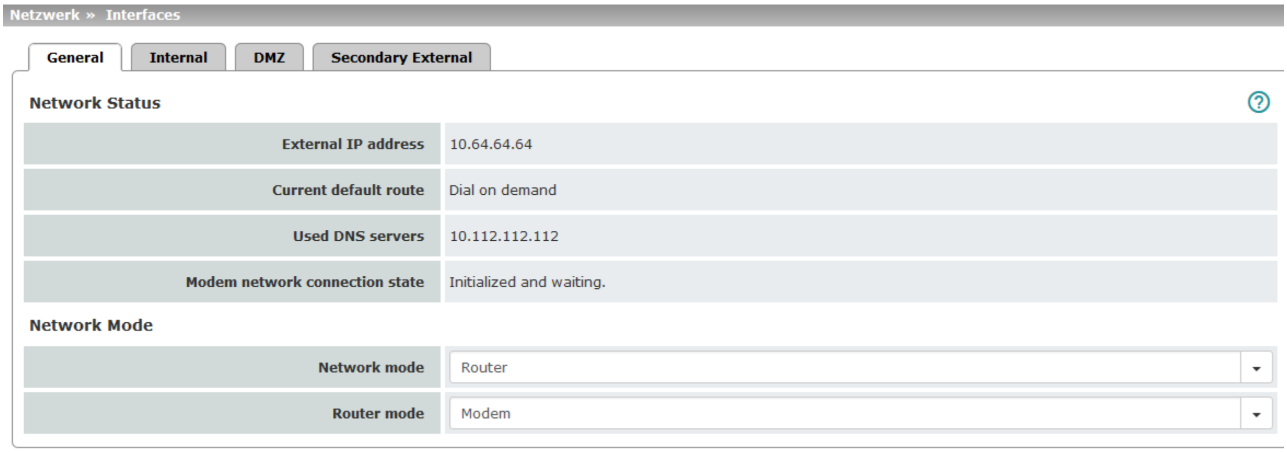
If the mGuard cannot analyze the network traffic, e.g., because the locally connected computer only receives data and does not send it, then *Stealth configuration* must be set to **Static**. In this case, further input fields are available for Static Stealth Configuration.

Multiple clients (default setting)

As with **Autodetect**, but it is possible to connect more than one computer to the LAN port (secure port) of the mGuard, meaning that multiple IP addresses can be used at the LAN port (secure port) of the mGuard.

For the further configuration of *Stealth* network mode, see "Stealth" on page 145.

6.1.3 General



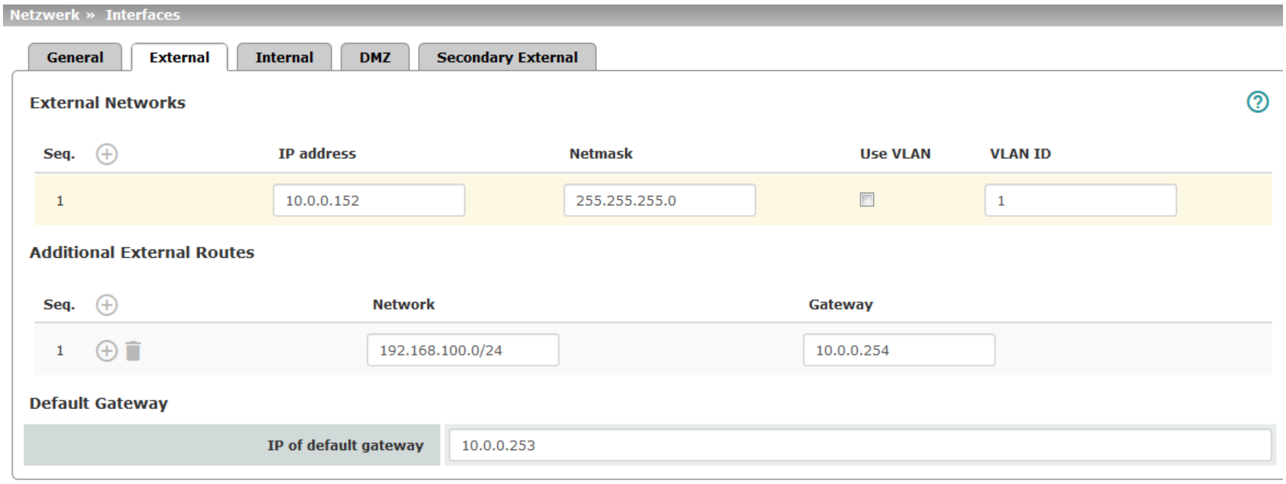
Network >> Interfaces >> General		
Network Status	**External IP address**	Display only: the addresses via which the mGuard can be accessed by devices from the external network. They form the interface to other parts of the LAN or to the Internet. If the transition to the Internet takes place here, the IP addresses are usually assigned by the Internet service provider (ISP). If an IP address is assigned dynamically to the mGuard, the currently valid IP address can be found here. In *Stealth* mode, the mGuard adopts the address of the locally connected computer as its external IP.
	Secondary external IP address (Only if the secondary external interface is activated)	Display only: the addresses via which the mGuard can be accessed by devices from the external network via the secondary external interface.
	Current default route	Display only: the IP address that the mGuard uses to try to reach unknown networks is displayed here. If a default route has not been specified, the field is left empty.
	Used DNS servers	Display only: the names of the DNS servers used by the mGuard for name resolution are displayed here. This information can be useful, for example, if the mGuard is using the DNS servers assigned to it by the Internet service provider.
	Connection status of modem to data network (Only for devices with an internal modem)	Displays the status of the internal modem (mobile network modem of the TC MGUARD RS4000/RS2000 3G / TC MGUARD RS4000/RS2000 4G and the internal analog modem for the FL MGUARD RS).

Network >> Interfaces >> General [...]		
Network mode	**Network mode**	**Router / Stealth** The mGuard must be set to the network mode that corresponds to its connection to the network. Depending on which network mode the mGuard is set to, the page will change together with its configuration parameters. “Stealth” network mode is not available for the **TC MGUARD RS2000 3G** and **TC MGUARD RS2000 4G**, as it does not have a wired WAN interface. See also: "Overview of "Router" network mode" on page 129 and "Overview of "Stealth" network mode" on page 132.
	Depending on the network mode selected and the mGuard device, different setting options are available on the web interface:	
	Router Mode (Only if "**Router**" network mode was selected)	**Static / DHCP / PPPoE / PPTP / Modem[1] / Built-in modem[1] / Built-in mobile network modem[1]** For a detailed description, see: – "Router Mode: Static" on page 130 – "Router Mode: DHCP" on page 130 – "Router Mode: PPPoE" on page 130 and "PPPoE" on page 141 – "Router Mode: PPTP" on page 130 and "PPTP" on page 142 – "Router Mode: Modem" on page 130 and "Dial-out" on page 174

Network >> Interfaces >> General [...]		
	Stealth configuration (Only if "**Stealth**" network mode was selected)	**Autodetect / Static / Multiple clients** **Autodetect** The mGuard analyzes the network traffic and independently configures its network connection accordingly. It operates transparently. For the use of certain functions (e.g. automatic updates, licence updates or establishment of VPN-connections), it is required that the mGuard makes its own requests of external servers, even in stealth mode. These requests are only possible when the locally connected computer permits ping requests. Configure its security settings accordingly. **Static** If the mGuard cannot analyze the network traffic, e.g., because the locally connected computer only receives data and does not send it, then ***Stealth configuration*** must be set to **Static**. In this case, further input fields are available for Static Stealth Configuration at the bottom of the page. **Multiple clients** (Default) As with **Autodetect**, but it is possible to connect more than one computer to the LAN port (secure port) of the mGuard, meaning that multiple IP addresses can be used at the LAN port (secure port) of the mGuard.
	Autodetect: ignore NetBIOS over TCP traffic on TCP port 139 (Only with **Autodetect** Stealth configuration)	If a Windows computer has more than one network card installed, it may alternate between the different IP addresses for the sender address in the data packets it sends. This applies to network packets that the computer sends to TCP port 139 (NetBIOS). As the mGuard determines the address of the computer from the sender address (and therefore the address via which the mGuard can be accessed), the mGuard would have to switch back and forth, and this would hinder operation considerably. To avoid this, activate the function if the mGuard has been connected to a computer that has these properties.

1 *M*odem / Built-in modem / Built-in mobile network modem is not available for all mGuard models (see "Network >> Interfaces" on page 127).

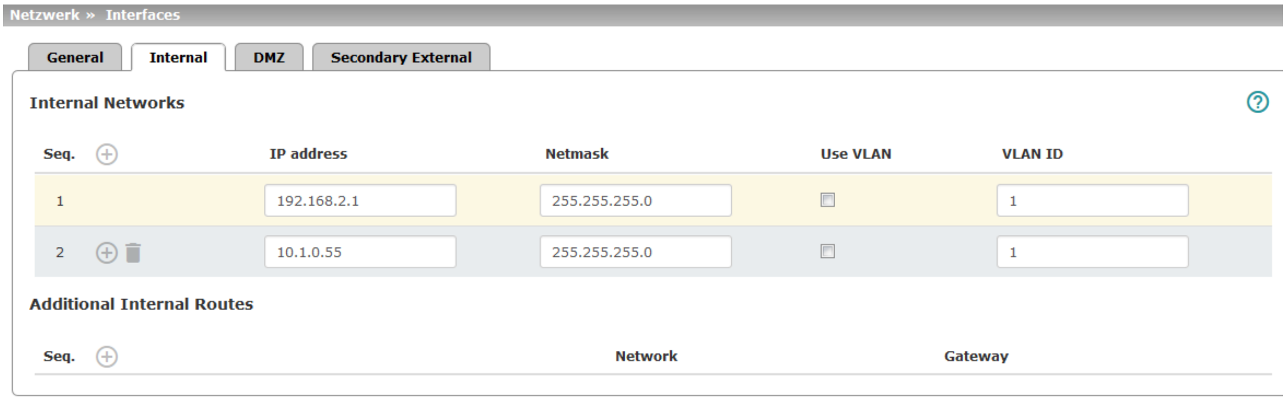
6.1.4 External



Network >> Interfaces >> External (network mode = "Router", router mode = "Static")		
External Networks	The addresses via which the mGuard can be accessed by external devices that are located behind the WAN port. If the transition to the Internet takes place here, the external IP address of the mGuard is assigned by the Internet service provider (ISP).	
	IP address	IP address via which the mGuard can be accessed via its WAN port.
	Netmask	The netmask of the network connected to the WAN port.
	Use VLAN	If the IP address should be within a VLAN, activate the function.
	VLAN ID	– A VLAN ID between 1 and 4095. – For an explanation of the term "VLAN", please refer to the glossary on page 456. – If you want to delete entries from the list, please note that the first entry cannot be deleted.
	OSPF area (Only if **OSPF** is activated)	Links the static addresses/routes of the external network interface to an OSPF area (see "Network >> Dynamic Routing" on page 221). An OSPF area cannot be assigned to the WAN interface in **"DHCP" router mode**.
Additional External Routes	In addition to the default route via the default gateway specified below, additional external routes can be specified.	
	Network	Specify the network in CIDR format (see "Network >> Dynamic Routing" on page 221).
	Gateway	The gateway via which this network can be accessed. See also "Network example diagram" on page 27.

Network >> Interfaces >> External (network mode = "Router", router mode = "Static") [...]		
Default gateway	**IP of default gateway**	The IP address of a device in the local network (connected to the LAN port) or the IP address of a device in the external network (connected to the WAN port) can be specified here. If the mGuard establishes the transition to the Internet, this IP address is assigned by the Internet service provider (ISP). If the mGuard is used within the LAN, the IP address of the default gateway is assigned by the network administrator. If the local network is not known to the external router, e.g., in the event of configuration via DHCP, specify your local network under Network >> NAT (see Page 198).

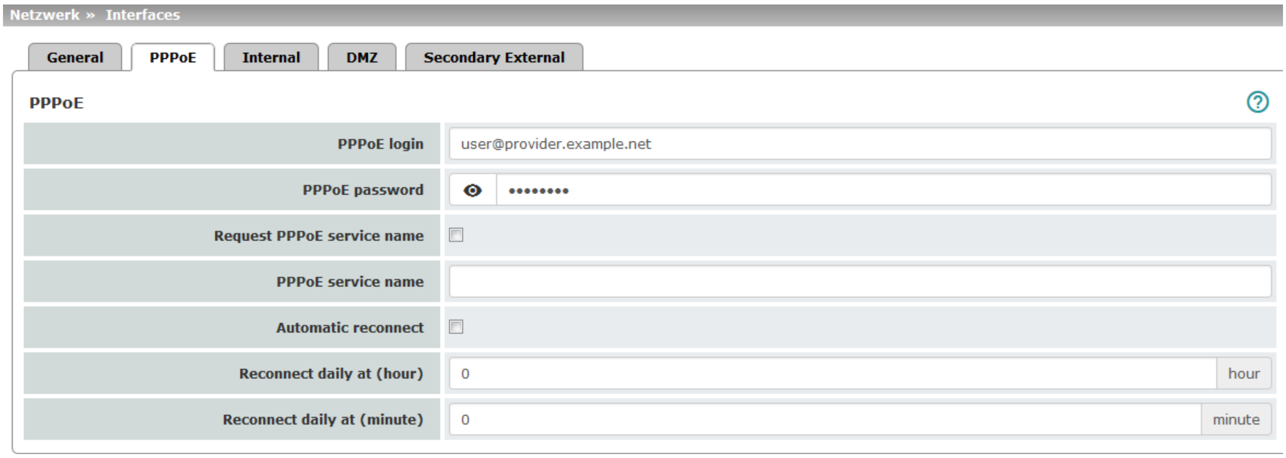
6.1.5 Internal



Network >> Interfaces >> Internal (Network mode = "Router")		
Internal Networks	**IP address**	The internal IP is the IP address via which the mGuard can be accessed by devices in the locally connected network. The default settings in **Router**/**PPPoE**/**PPTP**/**Modem** mode are as follows: – IP address: **192.168.1.1** – Netmask: **255.255.255.0** You can also specify other addresses via which the mGuard can be accessed by devices in the locally connected network. For example, this can be useful if the locally connected network is divided into subnetworks. Multiple devices in different subnetworks can then access the mGuard via different addresses.
	IP address	IP address via which the mGuard can be accessed via its LAN port.
	Netmask	The netmask of the network connected to the LAN port.
	Use VLAN	If the IP address should be within a VLAN, activate the function.
	VLAN ID	– A VLAN ID between 1 and 4095. – For an explanation of the term "VLAN", please refer to the glossary on page 456. – If you want to delete entries from the list, please note that the first entry cannot be deleted.
	OSPF area (Only if **OSPF** is activated)	Links the static addresses/routes of the internal network interface to an OSPF area (see "Network >> Dynamic Routing" on page 221). An OSPF area cannot be assigned to the WAN interface in **"DHCP" router mode**.
Additional Internal Routes	Additional routes can be defined if further subnetworks are connected to the locally connected network.	

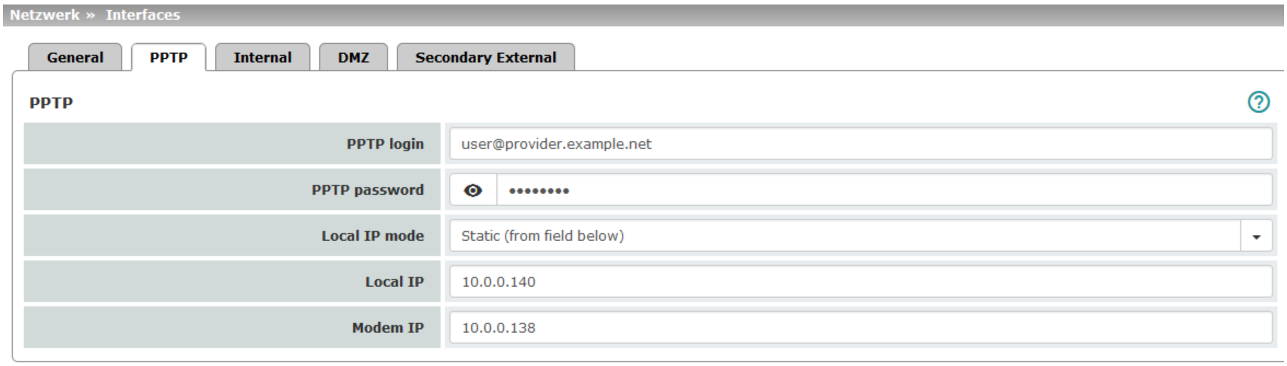
Network >> Interfaces >> Internal (Network mode = "Router") [...]		
	Network	Specify the network in CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 26).
	Gateway	The gateway via which this network can be accessed. See also "Network example diagram" on page 27.

6.1.6 PPPoE



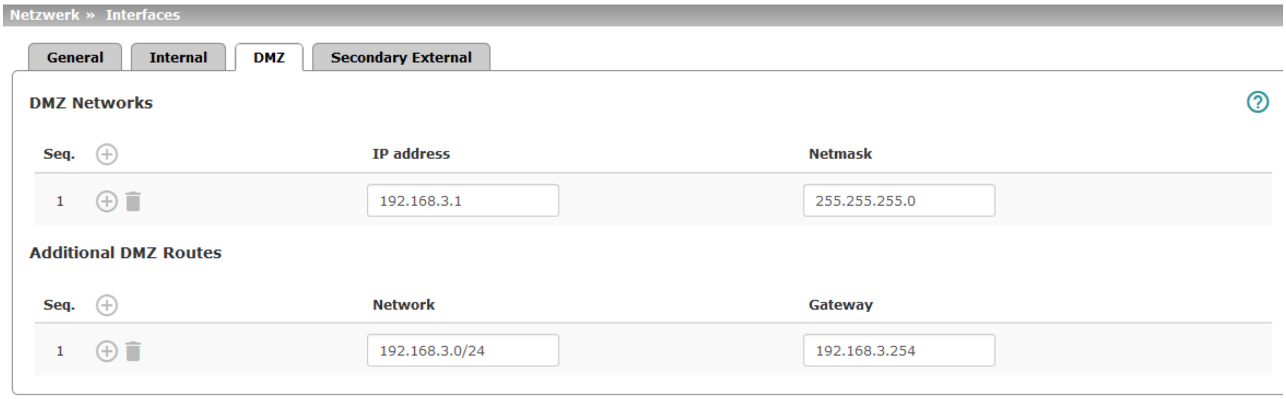
Network >> Interfaces >> PPPoE (Network mode = "Router", router mode = "PPPoE")		
PPPoE	For access to the Internet, the Internet service provider (ISP) provides the user with a user identifier (login) and password. These are requested when you attempt to establish a connection to the Internet.	
	PPPoE login	The user identifier (login) that is required by the Internet service provider (ISP) when you attempt to establish a connection to the Internet.
	PPPoE password	The password that is required by the Internet service provider when you attempt to establish a connection to the Internet.
	Request PPPoE service name	When the function is activated, the PPPoE client of the mGuard requests the service name specified below from the PPPoE server. Otherwise, the PPPoE service name is not used.
	PPPoE service name	PPPoE service name
	Automatic Reconnect	When the function is activated, you must specify the time in the **Reconnect daily at** field. This feature is used to schedule Internet disconnection and reconnection (as required by many Internet service providers) so that they do not interrupt normal business operations. When this function is enabled, it only takes effect if synchronization with a time server has been carried out (see "Management >> System Settings" on page 43, "Time and Date" on page 46).
	Reconnect daily at (hour)	Specified time (hour) at which the *Automatic Reconnect* function (see above) should be performed.
	Reconnect daily at (minute)	Specified time (minute) at which the *Automatic Reconnect* function (see above) should be performed.

6.1.7 PPTP



Network >> Interfaces >> PPTP (Network mode = "Router", router mode = "PPTP")		
PPTP	For access to the Internet, the Internet service provider (ISP) provides the user with a user identifier (login) and password. These are requested when you attempt to establish a connection to the Internet.	
	PPTP login	The user identifier (login) that is required by the Internet service provider when you attempt to establish a connection to the Internet.
	PPTP password	The password that is required by the Internet service provider when you attempt to establish a connection to the Internet.
	Local IP mode	**Static / Via DHCP** **Via DHCP** If the address data for access to the PPTP server is provided by the Internet service provider via DHCP, select this option. In this case, no entry is required under **Local IP**. **Static (from field below)** If the address data for access to the PPTP server is **not** supplied by the Internet service provider via DHCP, the local IP address must be specified.
	Local IP	The IP address via which the mGuard can be accessed by the PPTP server.
	Modem IP	IP address of the PPTP server of the Internet service provider.

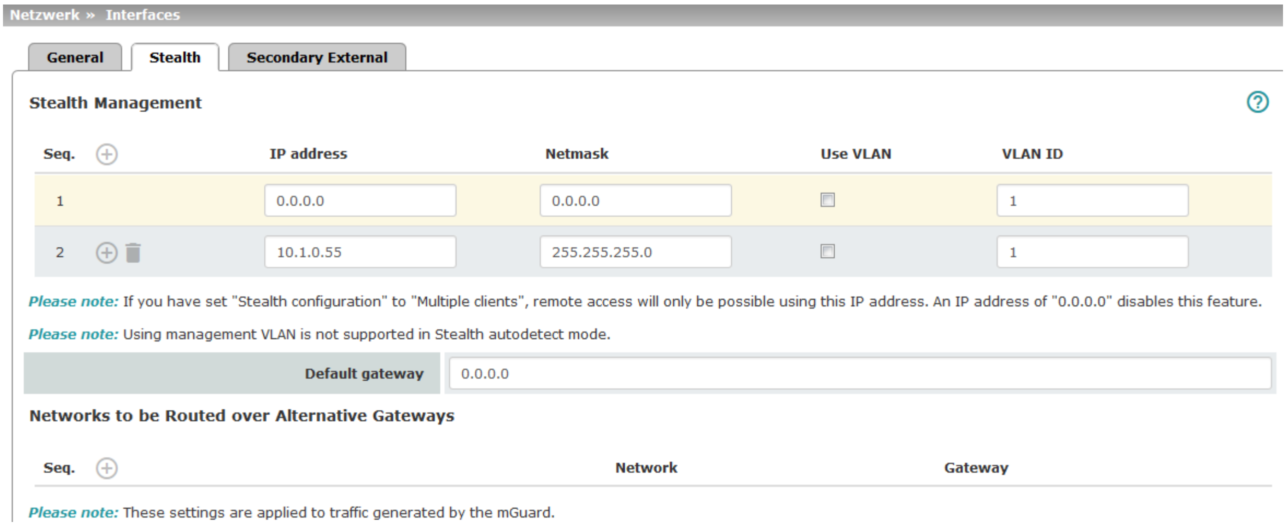
6.1.8 DMZ



Network >> Interfaces >> DMZ (Network mode = "Router")		
DMZ Networks (Only for TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004, FL MGUARD CENTERPORT)	**IP addresses**	IP address via which the mGuard can be accessed by devices in the network connected to the DMZ port. The DMZ port is only supported in router mode and requires at least one IP address and a corresponding subnet mask. The DMZ does not support any VLANs. In **"Router" network mode**, every newly added table line has default settings: – IP address: **192.168.3.1** – Netmask: **255.255.255.0** You can also specify other addresses via which the mGuard can be accessed by devices in the networks connected to the DMZ port. For example, this can be useful if the network connected to the DMZ port is divided into subnetworks. Multiple devices in different subnetworks can then access the mGuard via different addresses.
	IP address	IP address via which the mGuard can be accessed via its DMZ port. Default: 192.168.3.1
	Netmask	The netmask of the network connected to the DMZ port. Default: 255.255.255.0
	OSPF area (Only if **OSPF** is activated)	Links the static addresses/routes of the DMZ network interface to an OSPF area (see "Network >> Dynamic Routing" on page 221). An OSPF area cannot be assigned to the WAN interface in **“DHCP” router mode**.
Additional DMZ Routes	Additional routes can be defined if further subnetworks are connected to the DMZ.	

Network >> Interfaces >> DMZ (Network mode = "Router")[...]		
	Network	Specify the network in CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 26). Default: 192.168.3.0/24
	Gateway	The gateway via which this network can be accessed. See also "Network example diagram" on page 27. Default: 192.168.3.254

6.1.9 Stealth



Network >> Interfaces >> Stealth (“Stealth” network mode)	
Stealth Management	Additional Management IP addresses for the administration of the mGuard can be specified here. If: – The **Multiple clients** option is selected under *Stealth configuration* – The client does not answer ARP requests – No client is available Remote access via HTTPS, SNMP, and SSH is **only** possible using this address. With *static* Stealth configuration, the *Stealth Management IP Address* can always be accessed, even if the network card of the client PC has not been activated. If the secondary external interface is activated (see "Secondary External Interface" on page 149), the following applies: If the routing settings are such that data traffic to the **Stealth Management IP Address** would be routed via the secondary external interface, this would be an exclusion situation, i.e., the mGuard could no longer be administered locally. To prevent this, the mGuard has a built-in mechanism that ensures that in such an event the Stealth Management IP Address can still be accessed by the locally connected computer (or network).

Network >> Interfaces >> Stealth ("Stealth" network mode) [...]		
	IP address	Management IP address via which the mGuard can be accessed and administered. **In Stealth mode "Autodetect" the following applies:** If a Management IP Address is assigned, the default gateway of the network in which the mGuard is located must be specified. The IP address "0.0.0.0" deactivates the management IP address. Change the management IP address first before specifying any additional addresses.
	Netmask	The netmask of the IP address above.
	Use VLAN	This option only applies if you set the "Stealth configuration" option to "Multiple clients". IP address and netmask of the VLAN port. If the IP address should be within a VLAN, activate the function. In Stealth mode, VLAN cannot be used when the redundancy function is activated at the same time.
	VLAN ID	This option only applies if you set the "Stealth configuration" option to "Multiple clients". – A VLAN ID between 1 and 4095. – An explanation can be found under "VLAN" on page 456. – If you want to delete entries from the list, please note that the first entry cannot be deleted. In Stealth mode "Multiple Clients", the external DHCP server of the mGuard cannot be used if a VLAN ID is assigned as the management IP.
	Default gateway	The default gateway of the network where the mGuard is located. **In Stealth mode "Autodetect" the following applies:** If a Management IP Address is assigned, the default gateway of the network in which the mGuard is located must be specified.

Network >> Interfaces >> Stealth (“Stealth” network mode) [...]

Networks to be routed over alternative gateways

Static routes

In Stealth modes "Autodetect" and "Static", the mGuard adopts the default gateway of the computer connected to its LAN port. This does not apply if a management IP address is configured with the default gateway.

Alternative routes can be specified for data packets destined for the WAN that have been created by the mGuard. These include for instance the packets from the following types of data traffic:

- Download of certificate revocation lists (CRLs)
- Download of a new configuration
- Communication with an NTP server (for time synchronization)
- Sending and receiving encrypted data packets from VPN connections
- Requests to DNS servers
- Log messages
- Download of firmware updates
- Download of configuration profiles from a central server (if configured)
- SNMP traps

If this option is used, make the relevant entries afterwards. If it is not used, the affected data packets are routed via the default gateway specified for the client.

Network: Specify the network in CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 26).

Gateway: The gateway via which this network can be accessed.

The routes specified here are mandatory routes for data packets created by the mGuard. This setting has priority over other settings (see also "Network example diagram" on page 27).

Settings for Stealth mode (static)

(Only when "static" stealth configuration is selected)

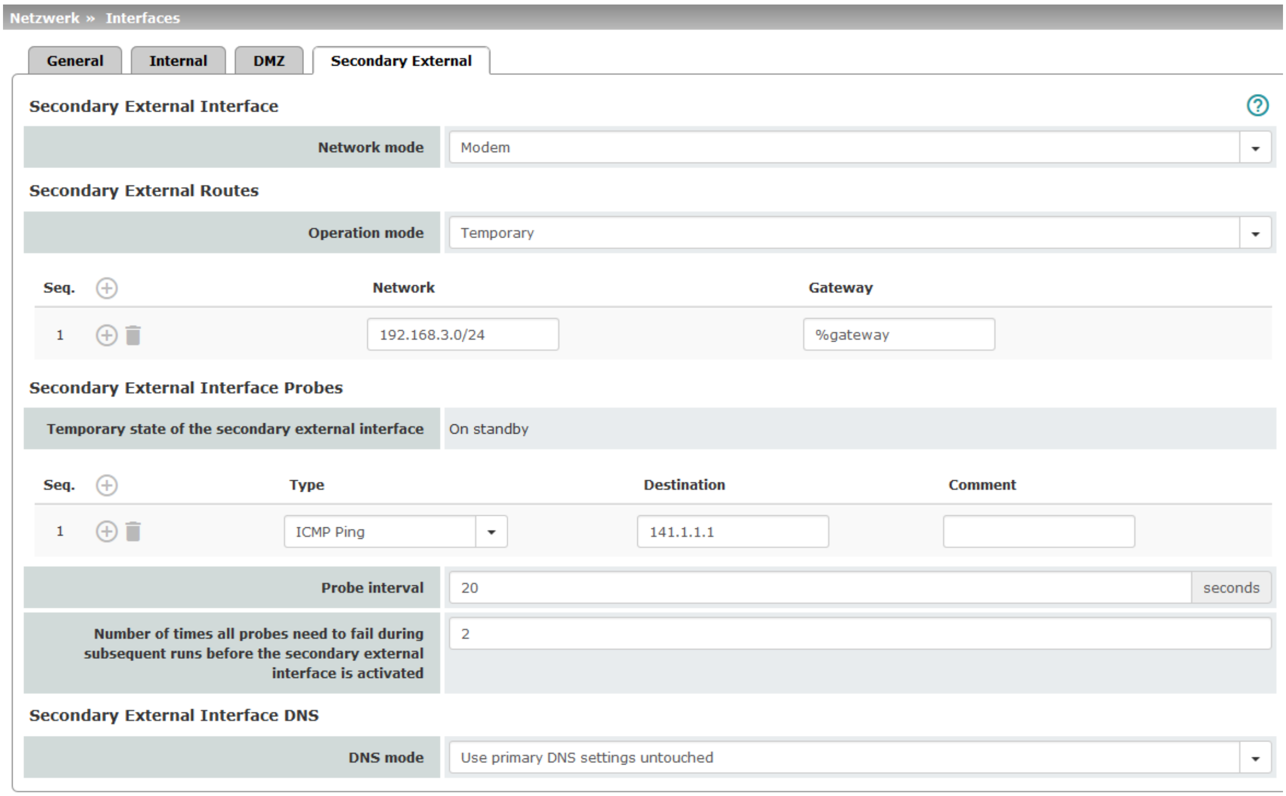
Client IP address: The IP address of the computer connected to the LAN port.

Client MAC address: The physical address of the network card of the local computer to which the mGuard is connected.

- The MAC address can be determined as follows:
  In DOS (Start, All Programs, Accessories, Command Prompt), enter the following command: ***ipconfig /all***

Network >> Interfaces >> Stealth (“Stealth” network mode) [...]		
		The MAC address does not necessarily have to be specified. The mGuard can automatically obtain the MAC address from the client. The MAC address 0:0:0:0:0:0 must be set in order to do this. Please note that the mGuard can only forward network packets to the client once the MAC address of the client has been determined. If no *Stealth Management IP Address* or *Client MAC address* is configured in static Stealth mode, then DAD ARP requests are sent via the internal interface (see RFC 2131, "Dynamic Host Configuration Protocol", Section 4.4.1).

6.1.10 Secondary External Interface



Network >> Interfaces >> Secondary External Interface	
Secondary External Interface (Not for TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000)	Only in *Router* network mode **with** *static/DHCP* router mode or *Stealth* network mode. Only for *FL MGUARD RS4000, FL MGUARD RS4004, mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD RS, FL MGUARD BLADE, mGuard delta (Innominate):* In these network modes, the serial interface of the mGuard can be configured as an additional **Secondary External Interface**. *TC MGUARD RS4000 3G* only: in "Router" network mode with "Static" or "DHCP" router mode, the built-in mobile network modem of the mGuard can be configured as an additional secondary external interface. The secondary external interface can be used to transfer data traffic *permanently* or *temporarily* to the external network (WAN). **If the secondary external interface is activated, the following applies:**

Network >> Interfaces >> Secondary External Interface [...]		
	In *Stealth* network mode Only the data traffic generated by the mGuard is subject to the routing specified for the secondary external interface, not the data traffic from a locally connected computer. Locally connected computers cannot be accessed remotely either; only the mGuard itself can be accessed remotely – if the configuration permits this. As in Router network mode, VPN data traffic can flow to and from the locally connected computers. Because this traffic is encrypted by the mGuard, it is seen as being generated by the mGuard. **In *Router* network mode** All data traffic, i.e., from and to locally connected computers, generated by the mGuard, can be routed to the external network (WAN) via the secondary external interface.	
	Network mode	**Off / Modem / Built-in mobile network modem** **Off** (Default). Select this setting if the operating environment of the mGuard does not require a secondary external interface. You can then use the serial interface (or the built-in modem, if present) for other purposes (see "Modem" on page 184). **Modem/Built-in modem** If you select one of these options, the secondary external interface will be used to route data traffic *permanently* or *temporarily* to the external network (WAN). The secondary external interface is created via the serial interface of the mGuard and an external modem connected to it. **Built-in mobile network modem** Firmware 5.2 or later supports an external or internal modem as a fallback for the external interface. From Version 8.0, this also includes the internal mobile network modem of the TC MGUARD RS4000 3G. The modem can be used *permanently* as the secondary external interface. In the event of a network error, it can also be used *temporarily* as a secondary external interface. It supports dedicated routes and DNS configuration.

Network >> Interfaces >> Secondary External Interface [...]

Secondary External Routes

(Not for TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000)

Notes on the Permanent / Temporary operation modes:

In both **Permanent** and **Temporary** mode, the modem must be available to the mGuard for the secondary external interface so that the mGuard can establish a connection to the WAN (Internet) via the telephone network connected to the modem.

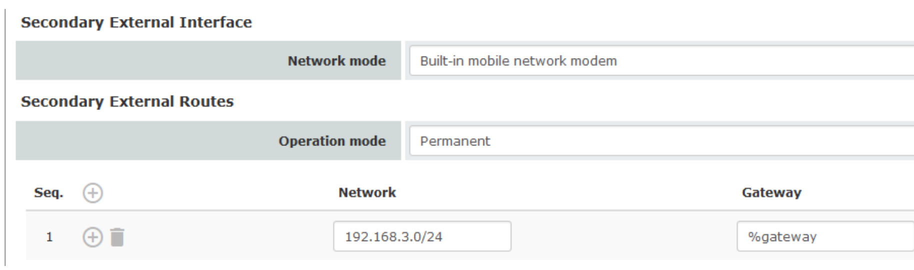
Which data packets are routed via the **primary external interface** (Ethernet interface) and which data packets are routed via the **secondary external interface** is determined by the routing settings that are applied for these two external interfaces. Therefore an interface can only take a data packet if the routing setting for that interface matches the destination of the data packet.

> **The following rules apply for routing entries:**
>
> If multiple routing entries for the destination of a data packet match, then the smallest network defined in the routing entries that matches the data packet destination determines which route this packet takes.

Operation Mode

Permanent / Temporary

After selecting *Modem*, *Built-in modem* or *Built-in mobile network modem* network mode for the secondary external interface, the operating mode of the secondary external interface must be specified (see "Example of use of routing entries:" on page 155).



Permanent

Data packets whose destination corresponds to the routing settings specified for the secondary external interface are always routed via this external interface. The secondary external interface is always activated.

Temporary

Data packets whose destination corresponds to the routing settings specified for the secondary external interface are only routed via this external interface when additional, separately defined conditions are met. Only then is the secondary external interface activated and the routing settings for the secondary external interface take effect (see "Secondary External Interface Probes" on page 153).

Network

Specify the routing to the external network here. Multiple routes can be specified. Data packets intended for these networks are then routed to the corresponding network via the secondary external interface – in *permanent* or *temporary* mode.

Network >> Interfaces >> Secondary External Interface [...]		
	Gateway	Specify the IP address (if known) of the gateway that is used for routing to the external network described above. When you dial into the Internet using the phone number of the Internet service provider, the address of the gateway is usually not known until you have dialed in. In this case, enter **%gateway** in the field as a placeholder.

Network >> Interfaces >> Secondary External Interface [...]

Secondary External Interface Probes

(Only **Temporary** operation mode)

If the operating mode of the secondary external interface is set to **Temporary**, the following is checked using periodic ping tests: can a specific destination or destinations be reached when data packets take the route based on all the routing settings specified for the mGuard – apart from those specified for the secondary external interface? Only if **none** of the ping tests are successful does the mGuard assume that it is currently not possible to reach the destination(s) via the primary external interface (Ethernet interface or WAN port of the mGuard). In this case, the secondary external interface is activated, which results in the data packets being routed via this interface (according to the routing setting for the secondary external interface).

The secondary external interface remains activated until the mGuard detects in subsequent ping tests that the destination(s) can be reached again. If this condition is met, the data packets are routed via the **primary** external interface again and the **secondary** external interface is deactivated.

Therefore, the purpose of the ongoing ping tests is to check whether specific destinations can be reached via the primary external interface. When they cannot be reached, the secondary external interface is activated until they can be reached again.

Successful ping test

A ping test is successful if the mGuard receives a positive response to the sent ping request packet within 4 seconds. If the response is positive, the peer can be reached.

> Please note the following when programming ping tests:
>
> It is useful to program multiple ping tests. This is because it is possible that an individual tested service is currently undergoing maintenance. This type of scenario should not result in the secondary external interface being activated and an expensive dial-up connection being established via the telephone network.
>
> Because the ping tests generate network traffic, the number of tests and their frequency should be kept within reasonable limits. You should also avoid activating the secondary external interface too early. The timeout time for the individual ping requests is 4 seconds. This means that after a ping test is started, the next ping test starts after 4 seconds if the previous one was unsuccessful.

Type	Specify the ping type of the ping request packet that the mGuard is to send to the device with the IP address specified under **Destination**. Multiple ping tests can be configured for different destinations.

Network >> Interfaces >> Secondary External Interface [...]		
		IKE ping Determines whether a VPN gateway can be reached at the IP address specified. **ICMP ping** Determines whether a device can be reached at the IP address specified. This is the most common ping test. However, the response to this ping test is disabled on some devices. This means that they do not respond even though they can be reached. **DNS ping** Determines whether an operational DNS server can be reached at the IP address specified. A generic request is sent to the DNS server with the specified IP address, and every DNS server that can be reached responds to this request.
	Destination	IP address or hostname of the probe target.
	Probe interval	The ping tests defined above under **Probes for activation...** are performed one after the other. When the ping tests defined are performed once in sequence, this is known as a *test run*. Test runs are continuously repeated at intervals. The interval entered in this field specifies how long the mGuard waits after starting a test run before it starts the next test run. The test runs are not necessarily completed: as soon as one ping test in a test run is successful, the subsequent ping tests in this test run are omitted. If a test run takes longer than the interval specified, then the subsequent test run is started directly after it.
	Number of times all probes need to fail during subsequent runs before the secondary external interface is activated	Specifies how many sequentially performed test runs must return a negative result before the mGuard activates the secondary external interface. The result of a test run is negative if **none** of the ping tests it contains were successful. The number specified here also indicates how many consecutive test runs must be successful after the secondary external interface has been activated before this interface is deactivated again.
DNS settings for the secondary external interface	**DNS Mode**	Only relevant if the secondary external interface is activated in **Temporary** mode: The DNS mode selected here specifies which DNS server the mGuard uses for temporary connections established via the secondary external interface.

Network >> Interfaces >> Secondary External Interface [...]	
	Use primary DNS settings untouched The DNS servers defined under Network >> DNS Server (see "Network >> DNS" on page 205) are used. **DNS root servers** Requests are sent to the root name servers on the Internet whose IP addresses are stored on the mGuard. These addresses rarely change. **Provider-defined (via PPP dial-out)** The domain name servers of the Internet service provider that provide access to the Internet are used. **User-defined (servers listed below)** If this setting is selected, the mGuard will connect to the domain name servers listed under *User-defined name servers*.
DNS server (Only **user-defined** for DNS mode)	The IP addresses of domain name servers can be entered in this list. The mGuard uses this list for communication via the secondary external interface if this is activated temporarily.

Example of use of routing entries:

– The external route of the **primary** external interface is specified as 10.0.0.0/8, while the external route of the **secondary** external interface is specified as 10.1.7.0/24. Data packets to network 10.1.7.0/24 are then routed via the secondary external interface, although the routing entry for the primary external interface also matches them. Explanation: the routing entry for the secondary external interface refers to a smaller network (10.1.7.0/24 < 10.0.0.0/8).
– This rule does not apply in *Stealth* network mode with regard to the stealth management IP address (see note under "Stealth Management" on page 145).
– If the routing entries for the primary and secondary external interfaces are identical, then the secondary external interface “wins”, i.e., the data packets with a matching destination address are routed via the secondary external interface.
– The routing settings for the secondary external interface only take effect when the secondary external interface is activated. Particular attention must be paid to this if the routing entries for the primary and secondary external interfaces overlap or are identical, whereby the priority of the secondary external interface has a filter effect, with the following result: data packets whose destination matches both the primary and secondary external interfaces are always routed via the secondary external interface, but only if this is activated.
– In **Temporary** mode, “activated” signifies the following: the secondary external interface is only activated when specific conditions are met, and it is only then that the routing settings of the secondary external interface take effect.

Network address 0.0.0.0/0 generally refers to the largest definable network, i.e., the Internet.

> In Router network mode, the local network connected to the mGuard can be accessed via the secondary external interface as long as the specified firewall settings allow this.

6.2 Network >> Mobile Network

> This menu is **only** available on the **TC MGUARD RS4000/RS2000 3G** and **TC MGUARD RS4000/RS2000 4G**.

Mobile network standard

TC MGUARD RS4000/RS2000 3G supports the establishment of a WAN via mobile network. The following mobile network standards are supported.

- GSM
- GSM with GPRS
- GSM with EGPRS
- 3G/UMTS
- 3G/UMTS with HSDPA
- 3G/UMTS with HSUPA
- 3G/UMTS with HSDPA and HSUPA
- 3G/UMTS with HSPA+
- CDMA 1xRTT (only 3G devices)
- CDMA EVDO (only 3G devices)

TC MGUARD RS4000/RS2000 4G supports the following mobile network standard in addition to those listed above:

- 4G (LTE)

TC MGUARD RS4000/RS2000 4G ATT only supports:

- 3G/UMTS
- 4G (LTE)

TC MGUARD RS4000/RS2000 4G VZW only supports:

- 4G (LTE)

Information on the used frequency ranges can be found on the website of the respective product in the Phoenix Contact E-Shop:phoenixcontact.net/product/<order number>

In addition, the GPS and GLONASS positioning systems for location and time synchronization are supported on the devices **TC MGUARD RS4000/RS2000 3G / 4G**. Note that the time synchronization and position data from the positioning systems can be manipulated by interference signals (GPS spoofing).

Establishing a mobile network connection

Antenna

To establish a mobile network connection, at least one matching **antenna** must be connected to the antenna connection (ANT) on the device (see user manual for the devices: UM EN MGUARD DEVICES at phoenixcontact.net/products). When using LTE, a second antenna should be connected to the device in order to improve the mobile network connection (diversity).

For information on recommended antennas, refer to the corresponding mGuard product pages at phoenixcontact.net/products).

SIM card

When GSM/UMTS/LTE is used, the TC MGUARD RS4000/RS2000 3G and TC MGUARD RS4000/RS2000 4G require at least one valid **mini SIM card** in 2FF/ID-000 format, via which the device assigns and authenticates itself to a mobile network.

The devices can be equipped with two SIM cards. The SIM card in slot SIM 1 is the primary SIM card which is normally used to establish the connection. If this connection fails, the device can turn to the second SIM card in slot SIM 2 (see "SIM Fallback" on page 165). You can set whether, and under which conditions, the connection to the primary SIM card is restored.

CDMA

For the CDMA mobile network standard, the connection to the mobile network provider is established without a SIM card. CDMA is used in the USA by US mobile network provider "Verizon" and requires separate registration.

LEDs

The state of the SIM cards is indicated via two LEDs on the front of the devices. The SIM1 and SIM2 LEDs light up green when the SIM card is active. If the SIM card is faulty or no PIN or the wrong PIN was entered, the LED continuously flashes green.

Quality of the mobile network connection

The signal strength of the mobile network connection is indicated by three LEDs on the front of the devices. The LEDs function as a bar graph.

Table 6-1 LED indication of signal strength

LED 1	**LED 2**	**LED 3**	**Signal strength**	
Lower LED	Middle LED	Upper LED		
Off	Off	Off	-113 dBm ... -111 dBm	Extremely poor to no network reception
Yellow	Off	Off	-109 dBm ... -89 dBm	Adequate network reception
Yellow	Green	Off	-87 dBm ... -67 dBm	Good network reception
Yellow	Green	Green	-65 dBm ... -51 dBm	Very good network reception

For stable data transmission, we recommend at least good network reception.

TC MGUARD RS2000 3G / TC MGUARD RS2000 4G

In the case of the **TC MGUARD RS2000 3G and TC MGUARD RS2000 4G**, the WAN is only available via the mobile network, as a WAN interface is not available. The mobile network function is preset. The devices can only be operated in router mode.

The status of the mobile network connection can be queried via SNMP. SNMP traps are sent in the following cases:

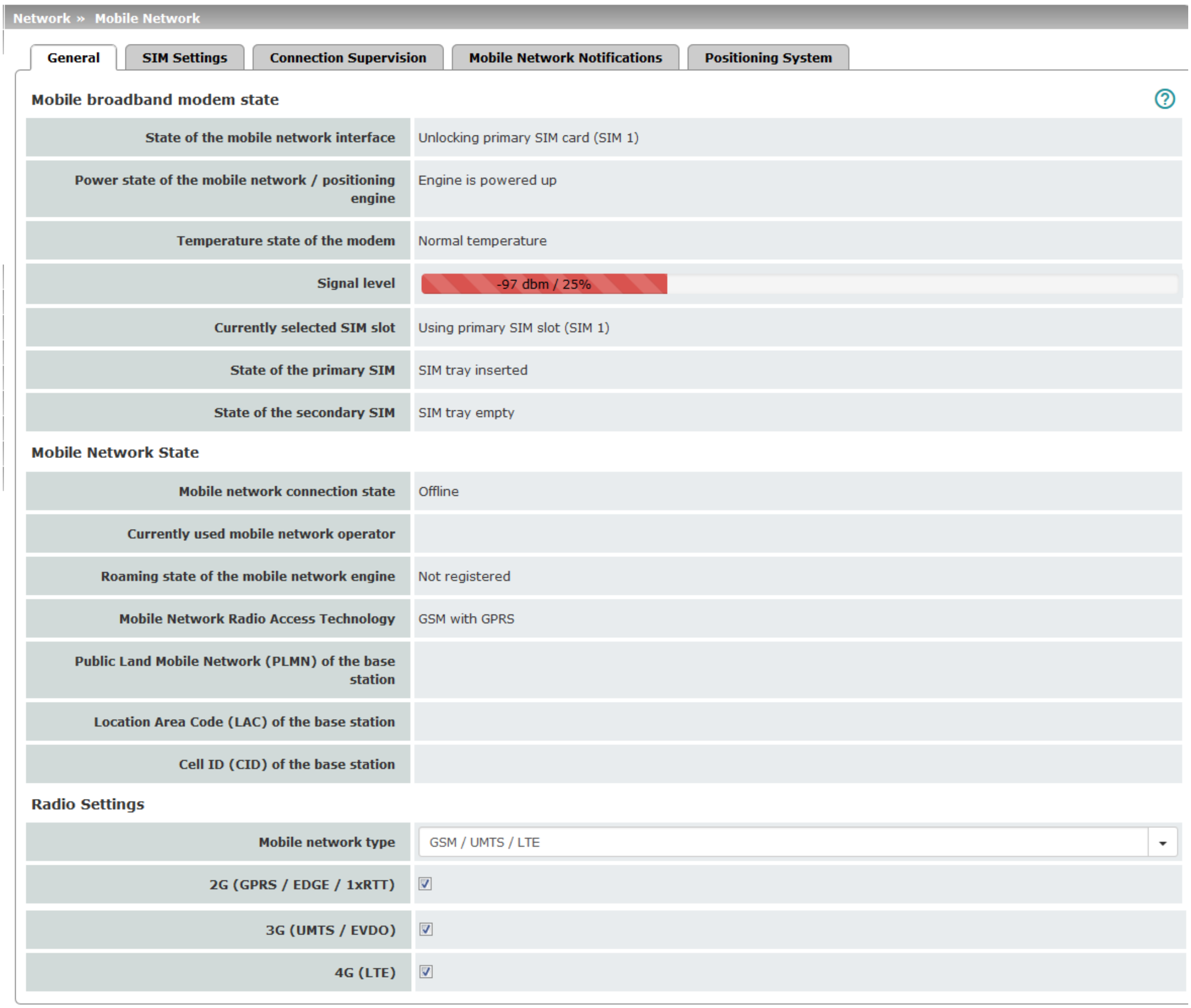
– Incoming text message (mGuardEDSGsmIncomingSMS)
– Incoming call (only up to mGuard firmware Version 8.3)
– Mobile network connection error (ping test) (mGuardEDSGsmNetworkProbe)

You can switch SNMP support on and off under **Management >> SNMP**.

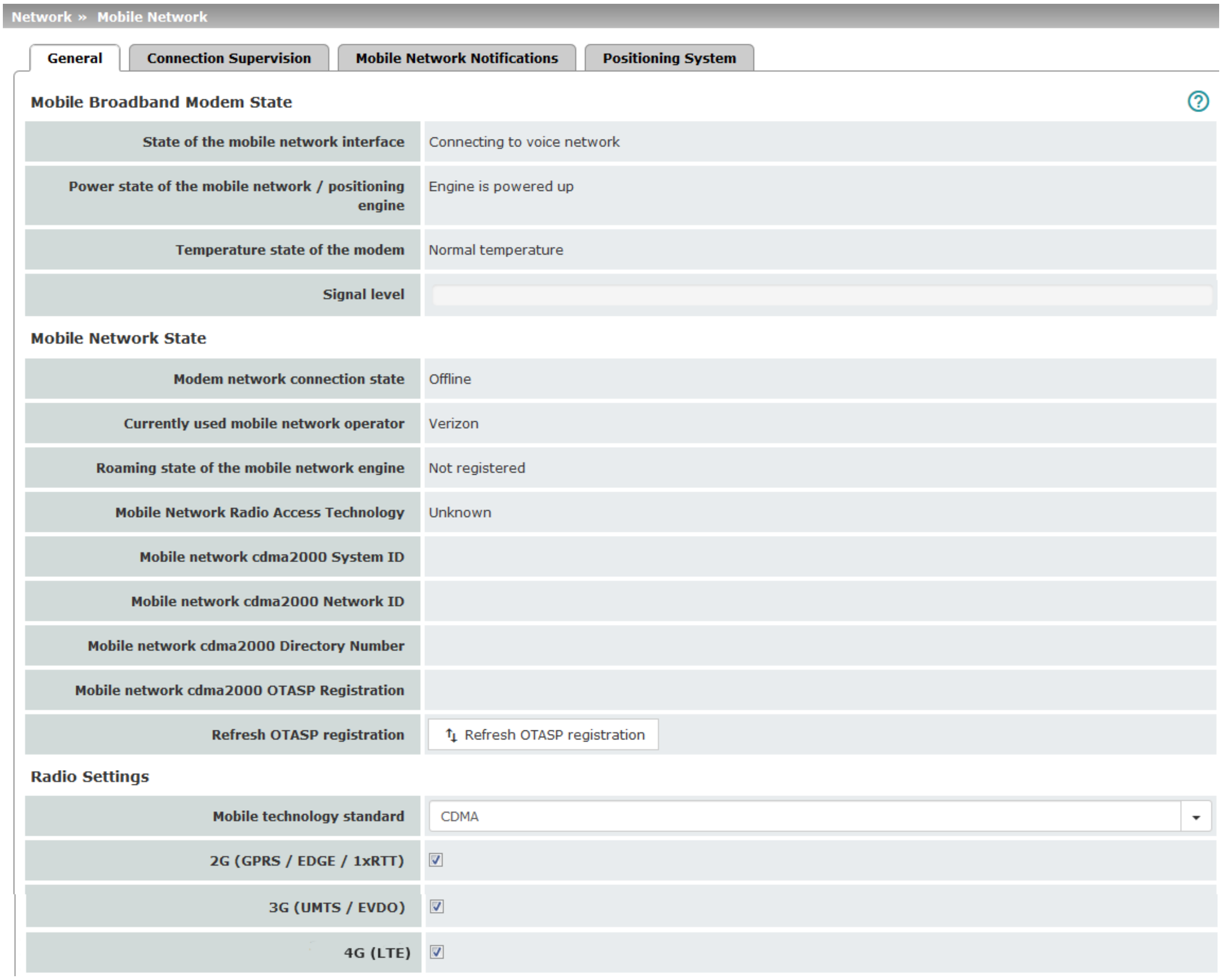
6.2.1 General

Different status messages are displayed depending on the mobile network standard used (GSM/UMTS/LTE or CDMA).

Display for GSM / UMTS / LTE selection (device-specific)



Display for CDMA selection



Network >> Mobile Network >> General		
Mobile Broadband Modem State	**State of the mobile network interface**	Indicates the state of the mobile network modem *state machine* (e.g., dialing into the data network or SIM card error).
	Power state of the mobile network / positioning engine	Operating state: Engine is powered up / Engine is powered down
	Temperature state of the modem	Temperature state of the mobile network modem In the event that the temperature exceeds or falls below a critical temperature, the mobile network modem switches off automatically.
	Signal strength	Strength of the mobile network signal, from 0% ... 100%, -113 dBm ... > -51 dBm The optimum received power is 100% signal strength and -51 dBm attenuation.

Network >> Mobile Network >> General [...]		
	Currently selected SIM slot	Indicates which SIM card slot is used (SIM 1 or SIM 2).
	State of the primary SIM	State of the SIM card or SIM tray in slot 1.
	State of the secondary SIM	State of the SIM card or SIM tray in slot 2.
Mobile Network State	**Modem network connection state**	Connection state to the mobile data network: Offline / Dialing in / Online
	Currently used mobile network operator	Name of the mobile network provider currently used by the mGuard.
	Roaming state of the mobile network engine	Possible states: – Registered to home network – Registered to foreign network – Not registered
	Mobile Network Radio Access Technology	Mobile network standard currently used
	Public Land Mobile Network (PLMN) of the base station (Only for "GSM/UMTS/LTE" network connection)	**PLMN**: unique identification number of the provider assigned to the base station The PLMN consists of the three-digit Mobile Country Code (**MCC)** and the two-digit Mobile Network Code (**MNC)** (MCC + MNC = PLMN).
	Location Area Code (LAC) of the base station (Only for "GSM/UMTS/LTE" network connection)	**LAC:** area code, location in the mobile network (in decimal format)
	Cell ID (CID) of the base station (Only for "GSM/UMTS/LTE" network connection)	**CID:** unique identification number of the mobile phone cell
	Mobile network cdma2000 System ID (Only for "CDMA" network connection)	**SID:** system identification number of the CDMA mobile phone cell
	Mobile network cdma2000 Network ID (Only for "CDMA" network connection)	**NID:** network identification number of the CDMA mobile phone cell
	Mobile network cdma2000 Directory Number (Only for "CDMA" network connection)	Phone number (**Mobile Directory Number – MDN**) assigned to the mGuard by the CDMA network provider (e.g., Verizon). Valid for the North American Numbering Plan (NANP). The number is only displayed once successfully registered with the CDMA network provider (e.g., Verizon OTASP) (see below).

Network >> Mobile Network >> General [...]		
	Mobile network cdma2000 OTASP Registration (Only for "CDMA" network connection)	In order that the mGuard can be operated in the mobile network of the CDMA provider (e.g., Verizon), the necessary configurations must be requested and downloaded from the CDMA network provider once. This is only possible if a mobile network connection has already been established to the CDMA mobile network. **mGuard firmware Version 8.3 or earlier:** the configuration is downloaded by clicking on the “Verizon registration” button (OTASP method). In order to do this, the mGuard must first be registered with and authorized by Verizon. **mGuard firmware Version 8.4 or later:** the configuration is downloaded automatically as soon as the mGuard **registered with and authorized by Verizon** connects to the Verizon network via CDMA for the first time. Following successful registration, the MDN is displayed under "**Mobile Directory Number (MDN) or the CDMA cell**".
	Refresh OTASP registration	If an already registered mGuard device is to be operated with a new mobile phone contract (e. g. *data plan* from Verizon) and a new mobile phone number, the registration must be repeated. Click on the "**Refresh OTASP registration**" button to download the new configuration. After successful registration, the new MDN will be displayed under "**Mobile network cdma2000 Directory Number**". This is only possible if a mobile network connection has already been established to the CDMA mobile network. To refresh the registration on the command line, enter the following command: *perform_action cdma/otasp_verizon* .

Network >> Mobile Network >> General [...]

Radio Settings

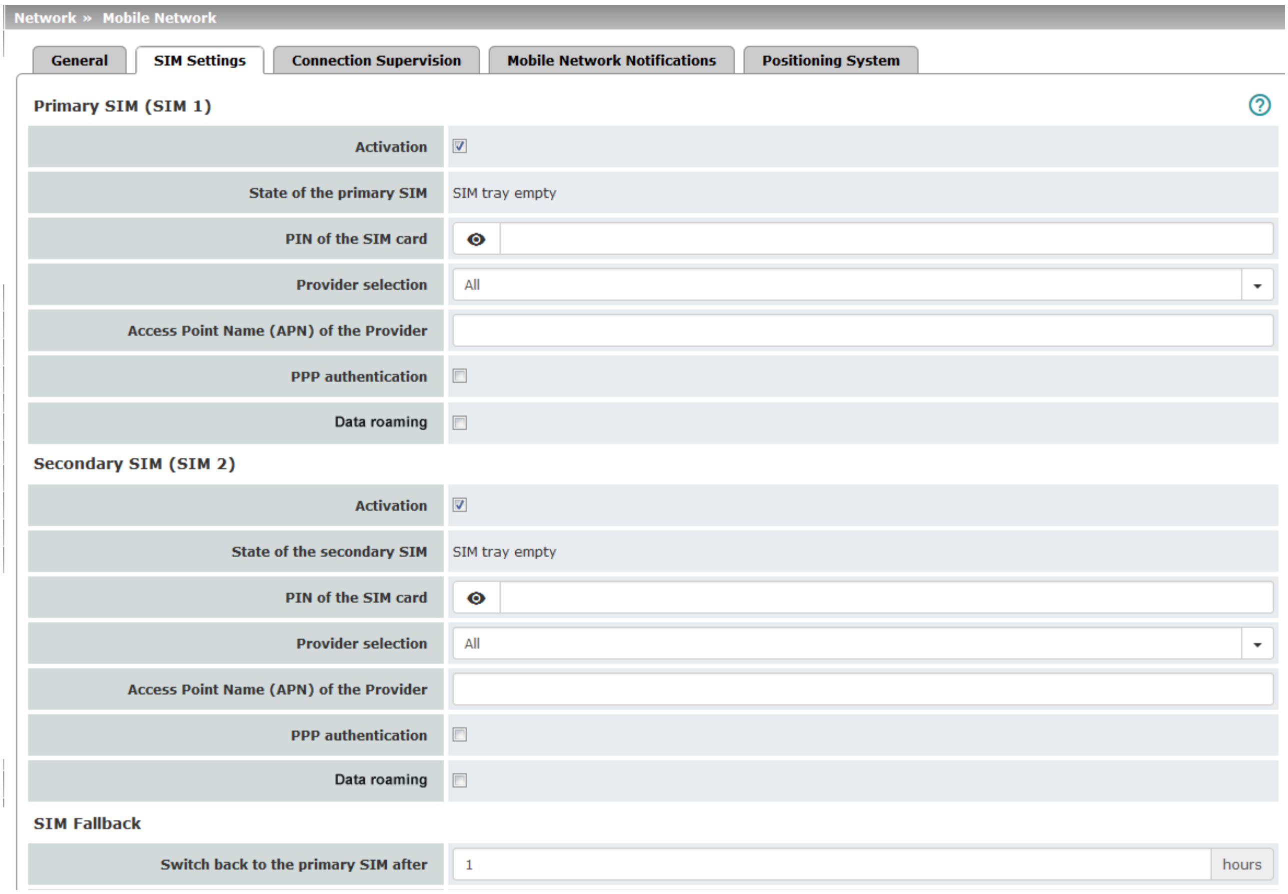
The explicit selection of mobile network frequencies is no longer necessary or possible from mGuard firmware Version 8.4. It is enough to simply select the mobile network standard.

> **As of mGuard firmware Version 8.4:** the selection of the mobile network standard can be restricted to one standard or entrusted to the modem. The following settings can be made:
>
> 1. If only one of the three available device-specific standards (2G, 3G, and 4G) is selected, only this standard will be used.
> 2. If more than one standard is selected, the modem will behave as follows:
>   - **2G and 4G**: this selection is not permitted.
>   - **2G and 3G**: the transmission method is automatically determined by the modem.
>   - **3G and 4G**: the transmission method is automatically determined by the modem.
>   - **2G, 3G, and 4G**: the transmission method is automatically determined by the modem.

Mobile network standard (Device-specific)	**No mobile network connection**: mobile network connection disabled **GSM / UMTS / LTE**: mobile network connection via the SIM card provider **CDMA**: mobile network connection using the CDMA method without SIM card The MEID code, which is printed on the housing of the device used, is used for registration and authorization with the CDMA provider (e.g., Verizon). The configuration is registered and downloaded automatically with mGuard firmware Version 8.4 or later (see above).
2G (GPRS / EDGE / 1xRTT) (Device-specific)	Depending on the selected mobile network standard, the data is transmitted using GPRS/EDGE (**GSM/UMTS/LTE**) or 1xRTT (**CDMA**).
3G (UMTS / EVDO) (Device-specific)	Depending on the selected mobile network standard, the data is transmitted using UMTS (**GSM/UMTS/LTE**) or EVDO (**CDMA**).
4G (LTE) (Device-specific)	The data is transmitted using LTE (**GSM/UMTS/LTE**).

6.2.2 SIM Settings

Not displayed when **"CDMA" used as mobile network standard**.



The TC MGUARD RS4000/RS2000 3G and TC MGUARD RS4000/RS2000 4G devices can be equipped with two SIM cards.

The TC MGUARD RS4000/RS2000 4G ATT and VZW devices can only be operated with *one* SIM card. SIM Fallback is not possible.

If two SIM cards are used, the following applies: The SIM card in slot SIM 1 is the **primary SIM card** which is normally used to establish the connection. If this connection fails, the device can turn to the **secondary SIM card** in slot SIM 2. To do this, both SIM cards must be activated and configured. It is also possible to only use the primary or just the secondary SIM card on its own.

The primary SIM card (SIM 1) in slot 1 takes over the mobile network connection in these cases:

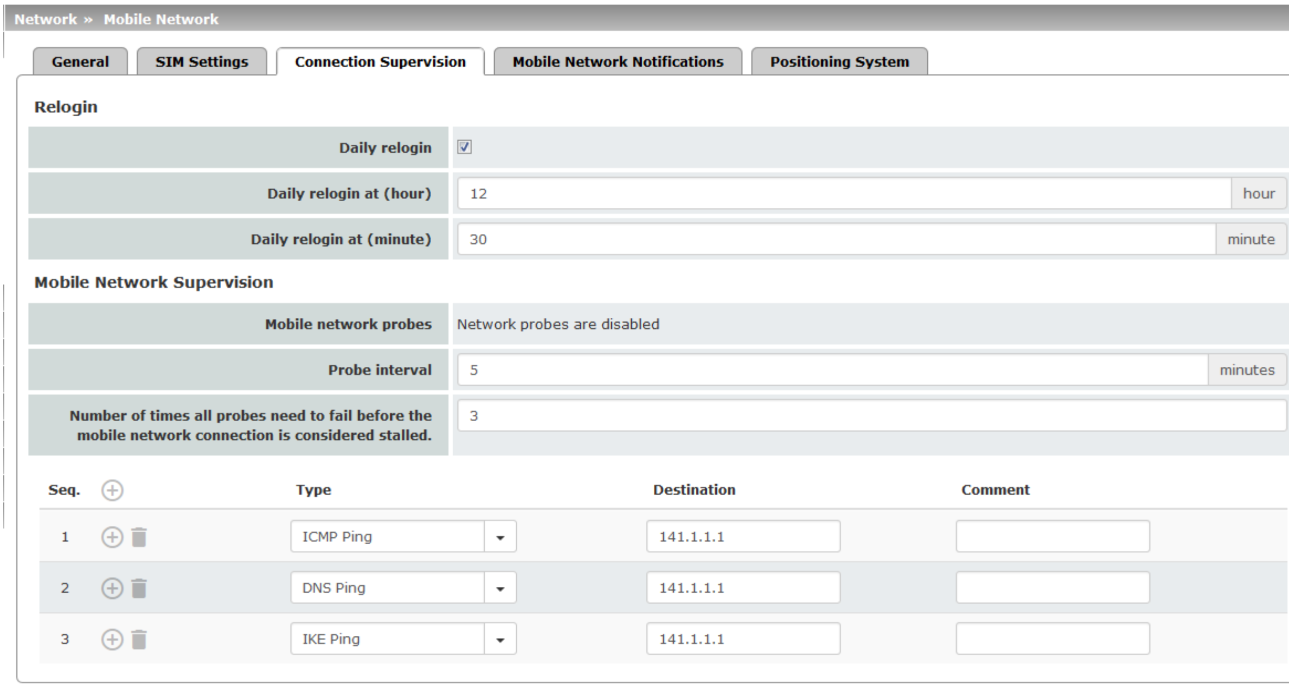
– If the mGuard is restarted
– When logging into the mobile network provider again
– In the event of an error in the mobile network connection of SIM 2 (see Connection Supervision)
– If there is a timeout, which is set under "Switch back to the primary SIM after" (see SIM Fallback)

The secondary SIM card (SIM 2) in slot 2 takes over the mobile network connection if the mobile network connection via the primary SIM card (SIM 1) fails. The secondary SIM card (SIM 2) maintains the mobile network connection until one of the aforementioned cases occurs.

Network >> Mobile Network >> SIM Settings		
		The settings for **Secondary SIM (SIM 2)** are the same as for **Primary SIM (SIM 1)** so are not described separately. The TC MGUARD RS4000/RS2000 4G ATT and VZW devices can only be operated with the **Primary SIM card**.
Primary SIM (SIM 1)	**Activation**	You can activate or deactivate the use of the SIM card.
	State of the primary SIM	The following statuses are displayed: – SIM tray inserted and empty (without SIM card) – No SIM tray (neither the SIM card nor tray are available) – PIN required – SIM card authorized (PIN) – Wrong PIN – PUK required (if the PIN is incorrectly entered too often) – SIM card error
	PIN of the SIM card	Numeric code provided by the mobile network provider. This field is left empty for SIM cards without a PIN.
	Provider selection	You can restrict the SIM card registration to **one provider** from the list or allow **all providers**. When **All** is selected, a suitable provider that is available is selected automatically.
	Manual APN selection (Only for TC MGUARD RS4000/RS2000 4G ATT and VZW)	**Default: deactivated** The Access Point Name (APN) on the TC MGUARD RS4000/RS2000 4G ATT and VZW devices is automatically transmitted by the provider and applied by the device. If errors occur during automatic transmission, the feature *Manual APN selection* must be activated and the APN must be entered in the field *Access Point Name (APN) of the provider* (see below).
	Access Point Name (APN) of the Provider	Enter the name of the access gateway for the packet transmission of your mobile network provider. The APN can be obtained from your mobile network provider.
	APN (Only for TC MGUARD RS4000/RS2000 4G ATT and VZW)	The APN automatically obtained from the provider or entered manually is displayed.
	Telephone number (Only for TC MGUARD RS4000/RS2000 4G VZW)	The telephone number assigned to the SIM card is displayed.

Network >> Mobile Network >> SIM Settings [...]		
	OTA registration status (Only for TC MGUARD RS4000/RS2000 4G VZW)	Status of the registration with the mobile network operator *Verizon*.
	PPP authentication	PPP authentication is required by some mobile network providers for the transmission of packet data. If you activate the function, you must also enter the corresponding access data (login and password).
	PPP login (only when “PPP authentication” function is activated)	Enter the PAP or CHAP user identifier (login) to log into the access gateway of the mobile network provider. This information can be obtained from your mobile network provider.
	PPP password (only when “PPP authentication” function is activated)	Enter the PAP or CHAP user password to log into the access gateway of the mobile network provider. This information can be obtained from your mobile network provider.
	Data roaming	Activating this function can support the establishment of a data connection. Only activate the function if there are problems establishing a data connection with the currently used SIM card of the mobile network provider.
SIM Fallback (Only if both SIM cards are activated) (Not available at TC MGUARD RS4000/RS2000 4G ATT and VZW)	**Switch back to the primary SIM after**	Specifies the time in hours (0 - 24) after which the secondary SIM card (SIM 2) switches back to the primary SIM card (SIM 1), provided the check of the targets was successful. In the event of an error, it immediately switches back to the primary SIM card. If “0” is specified as the value, it only switches back to the primary SIM card in the event of an error or after a restart.
	SIM initialization timeout	Maximum time period for SIM initialization. If this time is exceeded, switches to the other SIM if activated. Otherwise, the activated SIM is initialized again.
	Mobile network registration timeout	Maximum period of time between successful SIM initialization and connection with the voice network (text messages can be sent). If this time is exceeded, switches to the other SIM if activated. Otherwise, waits until the mobile network modem can reconnect to the voice network.

6.2.3 Connection Supervision

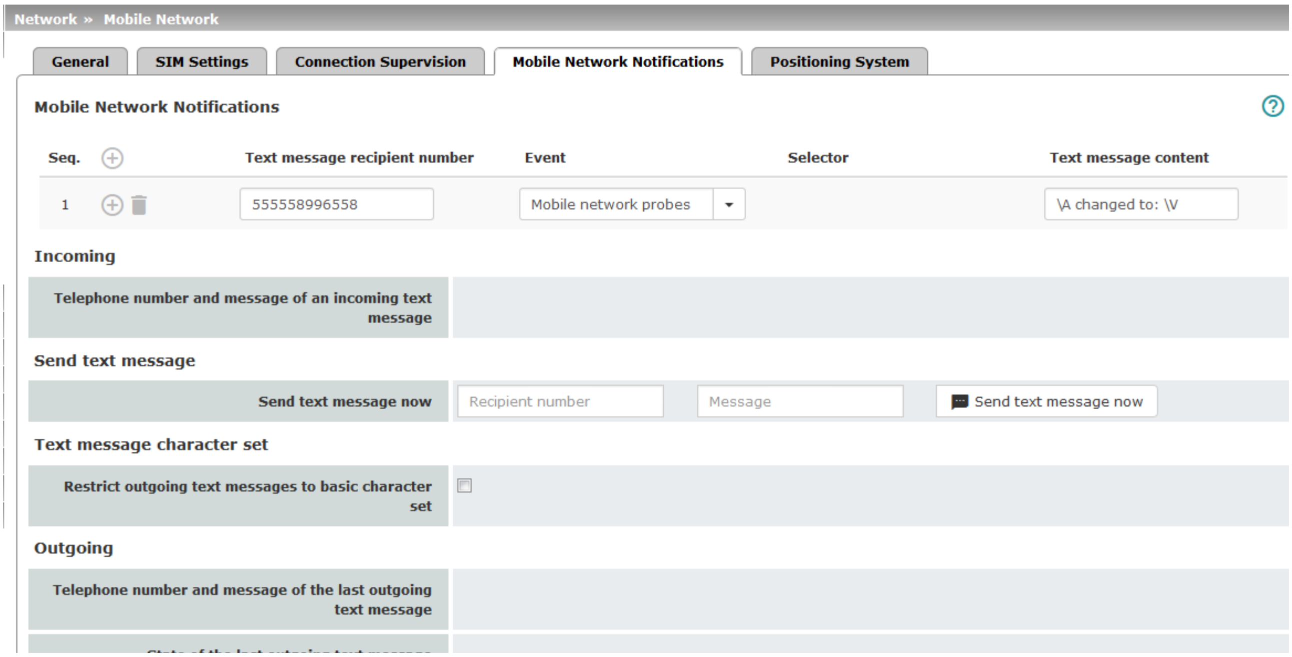


Network >> Mobile Network >> Connection Supervision		
Relogin	**Daily relogin**	The connection to the mobile network provider is disconnected and re-established daily at a fixed time in order to avoid forced disconnection by the provider.
	Daily relogin at (hour) (minute) (Only when “Daily relogin” function is activated)	Time at which the connection is renewed. Requirement: the time on the mGuard must be synchronized successfully (see "Time and Date" on page 46). **Default: 0 h : 0 m** Values: 0 - 23 hours and 0 - 59 minutes

Network >> Mobile Network >> Connection Supervision		
Mobile Network Supervision	In order to increase the availability of the mobile network connection, network tests should be activated if possible. This applies independent of the mobile network process (CDMA or GSM/ UMTS/LTE) or the number of SIM cards used. You can use the following probe targets to check whether data can actually be transmitted with an active mobile network connection with packet data transmission. To do so, probe targets (hosts) in the Internet are pinged and therefore tested at specific intervals to see whether at least one of the targets can be reached. If the defined targets cannot be reached after specified intervals, the mobile network connection is perceived to be faulty. If two SIM cards are configured, the mobile network connection is re-established with the SIM card that is currently not in use. In the case of only one activated SIM card or in the CDMA process, the mobile network modem is reset and then the mobile network connection is reestablished. Furthermore, state changes in mobile network supervision can be sent by e-mail, text message or SNMP trap.	
	Mobile network probes	Status of network supervision Supervision is only activated under the following conditions: – “Built-in mobile network modem” is selected as Network or Router mode – At least one probe target is configured
	Probe interval (minutes)	Time between two tests in minutes Value: 2 - 60 minutes (default: 5 minutes)
	Number of times all probes need to fail before the mobile network connection is considered stalled	Number of attempts before the mobile network connection is considered to be aborted. Value: 1 - 5 (default: 3)

Network >> Mobile Network >> Connection Supervision		
	Probe targets	**Type:** the ping type can be configured separately for each probe target: – **ICMP Ping** (ICMP echo request, ICMP echo reply): Determines whether a device can be reached at the IP address specified. This is the most common ping test. However, the response to this ping test is disabled on some devices. This means that they do not respond even though they can be reached. – **DNS Ping** (DNS query to UDP port 53): Determines whether an operational DNS server can be reached at the IP address specified. A generic request is sent to the DNS server with the specified IP address, and every DNS server that can be reached responds to this request. – **IKE Ping** (IPsec IKE query to UDP port 500): Determines whether a VPN gateway can be reached at the IP address specified. **Destination:** here you can enter the probe targets as host names or IP addresses. The probe targets are processed in the specified order. If a mobile network provider is unable to resolve a host name, they often redirect the request to their own Internet domain. The test probe therefore always appears to be reachable. In order to avoid this problem, IP addresses should be used as the destination instead of host names. **Comment:** freely selectable comment.

6.2.4 Mobile Network Notifications



The TC MGUARD RS4000/RS2000 3G and TC MGUARD RS4000/RS2000 4G devices can send and receive text messages.

Text messages can be sent via the following mechanisms:

- Web interface
- Command line

To do so, you must enter the recipient number followed by a space and then add the message:

/Packages/mguard-api_0/mbin/action gsm/sms “<recipient number> <message>”

Text messages can be sent to freely definable mobile network recipients for selectable events. A complete list of all events can be found under "Event table" on page 66.

Incoming text messages can be used to control VPN connections or firewall rule records, for example (see "Token for text message trigger" on page 270 and 330).

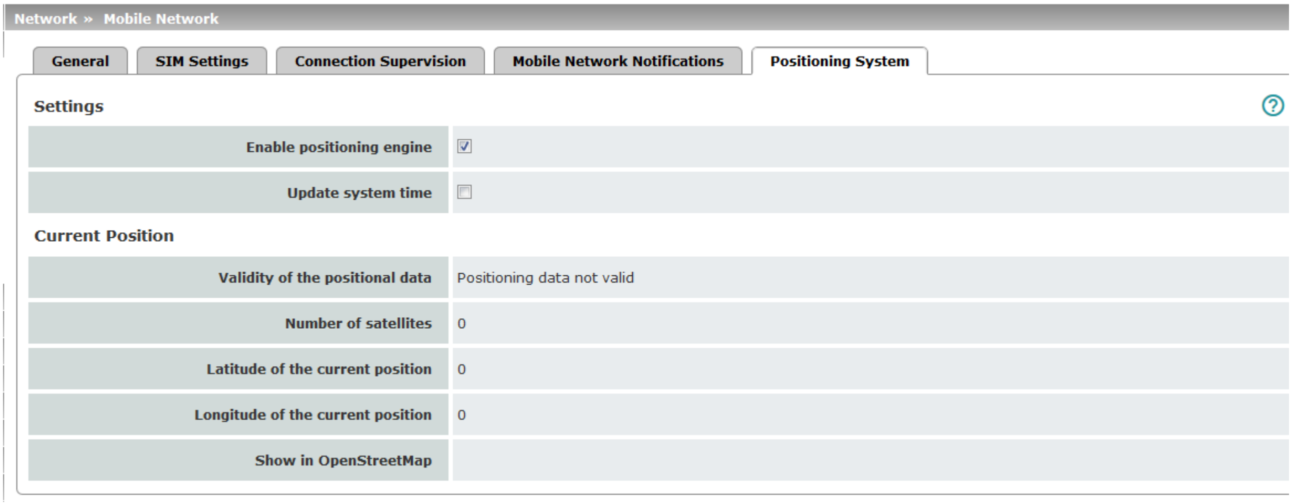
Network >> Mobile Network >> Mobile Network Notifications		
Text Message Notifications	Any text message recipient can be linked to predefined events and a freely definable message. The list is processed from top to bottom. **NOTE:** Depending on the configuration, a very high number of text messages may be sent. It is recommended that you select a mobile network tariff that has a flat rate for text messages sent.	
	Text message recipient number	Recipient number for the text message

Network >> Mobile Network >> Mobile Network Notifications [...]		
	Event	When the selected event occurs, the linked recipient number is selected and the event is sent to them as a text message. A text message can also be stored and sent. A complete list of all events can be found under "Event table" on page 66.
	Selector	Configured VPN connections (IPsec VPN / OpenVPN) or firewall rule records that are to be monitored by email can be selected here.
	Text message content	Here you can enter the text that is sent as a text message. Maximum of 160 characters from the GSM-based alphabet (see Text Message Character Set) or 70 Unicode symbols. The text is freely definable. You can use blocks from the event table which can be inserted as placeholders in plain text (\A and \V) or in machine-readable format (\a and v\). Time stamps in the form of a placeholder (\T or \t (machine readable)) can also be inserted (see "Event table" on page 66).
Incoming	Incoming text messages can be used to start or stop VPN connections. The text message must contain a configured token and the corresponding command for the relevant VPN connection.	
	Telephone number and content of the last incoming text message	Displays the sender number and message of the last incoming text message.
Send text message	**Send text message now**	**Recipient number** Enter the telephone number of the recipient of the text message (maximum 20 digits, and a '+' for international telephone numbers). **Message** Enter the text that is to be sent as a text message here. Maximum of 160 characters from the GSM-based alphabet (see Text Message Character Set) or 70 Unicode symbols. **Send text message now** Click on the “Send text message now” button to send the message.

Network >> Mobile Network >> Mobile Network Notifications [...]		
Text Message Character Set	In firmware versions prior to 8.3, the approach was to try and send a maximum number of characters in one text message. Since some telecommunications providers do not adhere to standards, some text messages were not sent accurately (word-for-word). This led to problems in automated applications. In order to ensure word-for-word transmission, the characters used needed to be restricted to the following basic character set: – (space) – 0-9 – a - z – A - Z – ! " # % & ( ) * + , - / : ; < = > ?	
	Restrict outgoing text messages to basic character set	In order to force the use of the basic character set, activate the function. Once activated, a text message sent by the mGuard is not translated into the language set for the web user interface; it is always sent in English. This does not affect e-mail notifications that are sent.
Outgoing	**Telephone number and content of the last outgoing text message**	Sender number and message of the last text message sent.
	State of the last outgoing text message	State of the last text message sent.

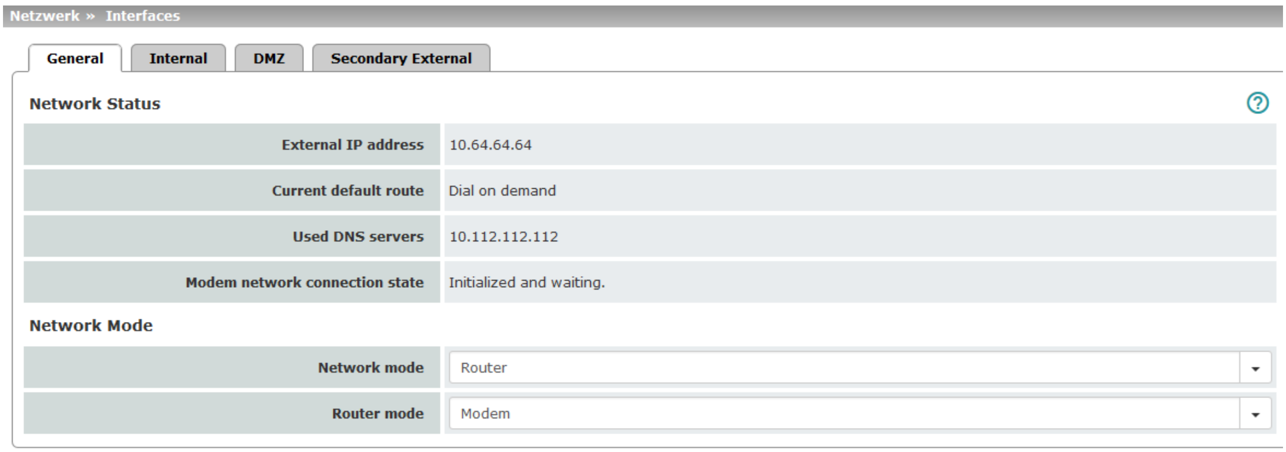
6.2.5 Positioning System

> Depending on the device, this menu is not available on all mobile devices.



Network >> Mobile Network >> Positioning System		
	The positioning system can only be used with a matching GPS antenna. For information on recommended antennas, refer to the corresponding mGuard product pages at phoenixcontact.net/products.	
Settings	**Enable positioning engine**	When you enable this function, the position of the mGuard is determined.
	Update system time	When the function is activated, the local system time is synchronized by means of the positioning system used. If time synchronization by means of NTP server is activated at the same time (see "Enable NTP time synchronization" on page 50), all sources are used to determine the time.
Current Position	**Validity of the positional data**	Indicates whether valid position data is available for the mGuard.
	Number of satellites	Displays the number of available GPS/GLONASS satellites for the mGuard which are available for position determination.
	Latitude of the current position	Displays the current latitude of the mGuard position.
	Longitude of the current position	Displays the current longitude of the mGuard position.
	Show in OpenStreetMap	A link to OpenStreetMap is generated from the mGuard position data, which can be used with a web browser to display a map view of the current position of the mGuard.

6.3 Serial interface



Modem network mode is available for: *FL MGUARD RS4000/RS2000, TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G,FL MGUARD RS4004/RS2005, mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD RS, FL MGUARD BLADE.*

Built-in modem network mode is also available for the *FL MGUARD RS*, if it has a built-in modem or a built-in ISDN terminal adapter (optional).

Built-in mobile network modem mode is also available for the *TC MGUARD RS4000/RS2000 3G* and *TC MGUARD RS4000/RS2000 4G*.

For all of the devices mentioned above, data traffic is routed via the serial interface and not via the mGuard WAN port when in *Modem* or *Built-in (mobile network) modem* network mode and from there it continues as follows.

– A – data traffic is routed via the externally accessible serial interface (serial port) to which an external modem must be connected.
– B – data traffic is routed via the built-in (mobile network) modem/built-in ISDN terminal adapter, if available.

In both cases, the connection to the ISP and therefore the Internet is established via the telephone network using a modem or ISDN terminal adapter.

In *Modem* network mode, the serial interface of the mGuard is not available for the PPP dial-in option or for configuration purposes (see page "Modem" on page 184).

After selecting **Modem**[1] as the network mode, specify the required parameters for the modem connection on the **Dial-out** and/or **Dial-in** tab page (see "Dial-out" on page 174 and "Dial-in" on page 181).

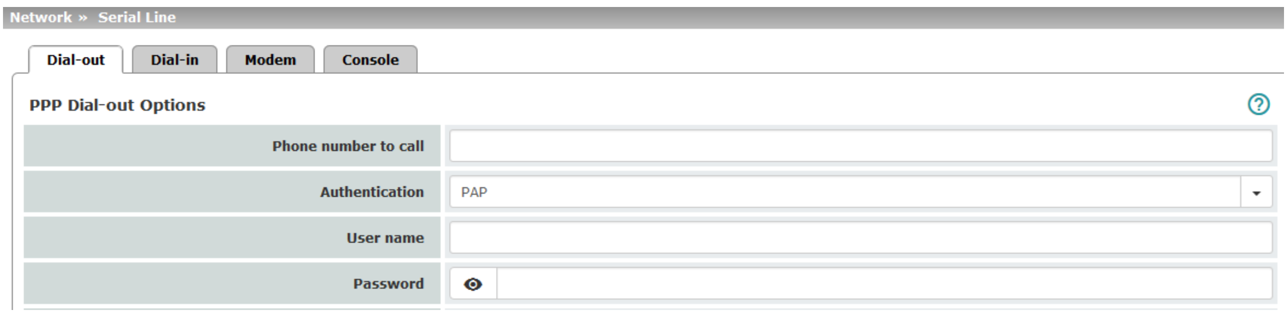
Enter the connection settings for an external modem on the ***Modem*** tab page (see "Modem" on page 184).

1 In the case of the FL MGUARD RS with built-in modem or ISDN terminal adapter, **Built-in modem** is available as an option and in the case of the TC MGUARD RS4000/RS2000 3G and TC MGUARD RS4000/RS2000 4G, **Built-in mobile network modem** is available as an option

This is a DTE interface in the case of the serial interface.

6.3.1 Dial-out

> Only for *TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4000, FL MGUARD RS4004*, *mGuard centerport (Innominate), FL MGUARD CENTERPORT*, *FL MGUARD RS, FL MGUARD BLADE, FL MGUARD DELTA, mGuard delta (Innominate)*



Network >> Serial interface >> Dial-out

PPP Dial-out Options

(Not for TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000)

> These settings are only necessary when the mGuard is to establish a data link to the WAN (Internet) via one of these interfaces.
> – Via the primary external interface (*Modem* or *Built-in (mobile network) modem* network mode)
> – Via the secondary external interface (also available in *Stealth* or *Router* network mode)

Phone number to call

Phone number of the Internet service provider. The connection to the Internet is established after establishing the telephone connection.

Command syntax: together with the previously set ATD modem command for dialing, the following dial sequence, for example, is created for the connected modem: ATD765432.

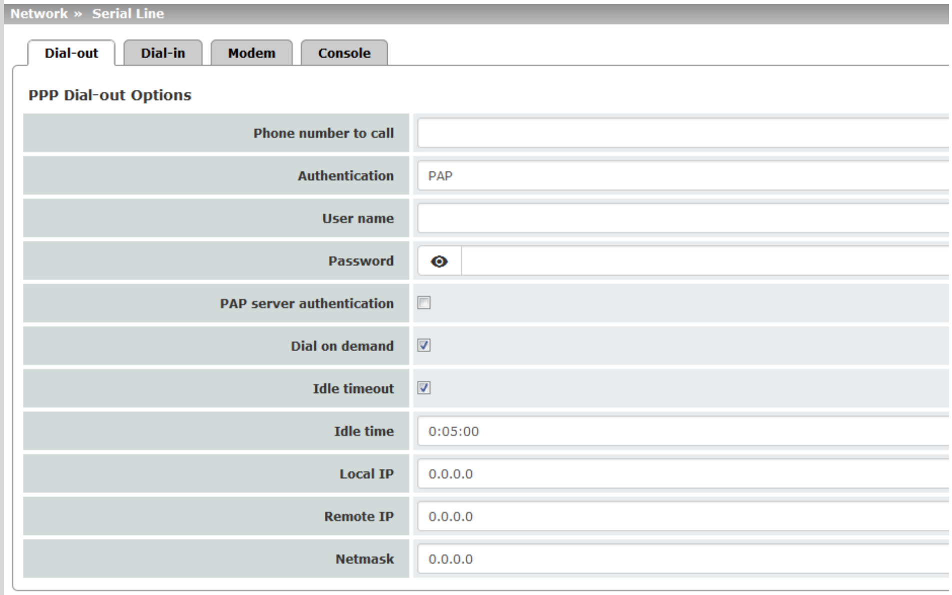
A compatible pulse dialing procedure that works in all scenarios is used as standard.

Special dial characters can be used in the dial sequence.

Network >> Serial interface >> Dial-out [...]		
		HAYES special dial characters – **W:** instructs the modem to insert a dialing pause at this point until the dial tone can be heard. Used when the modem is connected to a private branch exchange. An outside line must be obtained first for outgoing calls by dialing a specific number (e.g., 0) before the phone number of the relevant subscriber can be dialed. Example: ATD0W765432 – **T**: switch to tone dialing. Insert the special dial character T before the phone number if the faster tone dialing procedure is to be used (with tone-compatible telephone connections). Example: ATDT765432
	Authentication	**PAP / CHAP / None** – **PAP** = Password Authentication Protocol – **CHAP** = Challenge Handshake Authentication Protocol These terms describe procedures for the secure transmission of authentication data using the Point-to-Point Protocol. If the Internet service provider requires the user to log in using a user name and password, then PAP or CHAP is used as the authentication method. The user name, password, and any other data that must be specified by the user to establish a connection to the Internet are given to the user by the Internet service provider. The corresponding fields are displayed depending on whether **PAP**, **CHAP** or **None** is selected. Enter the corresponding data in these fields.

Network >> Serial interface >> Dial-out [...]

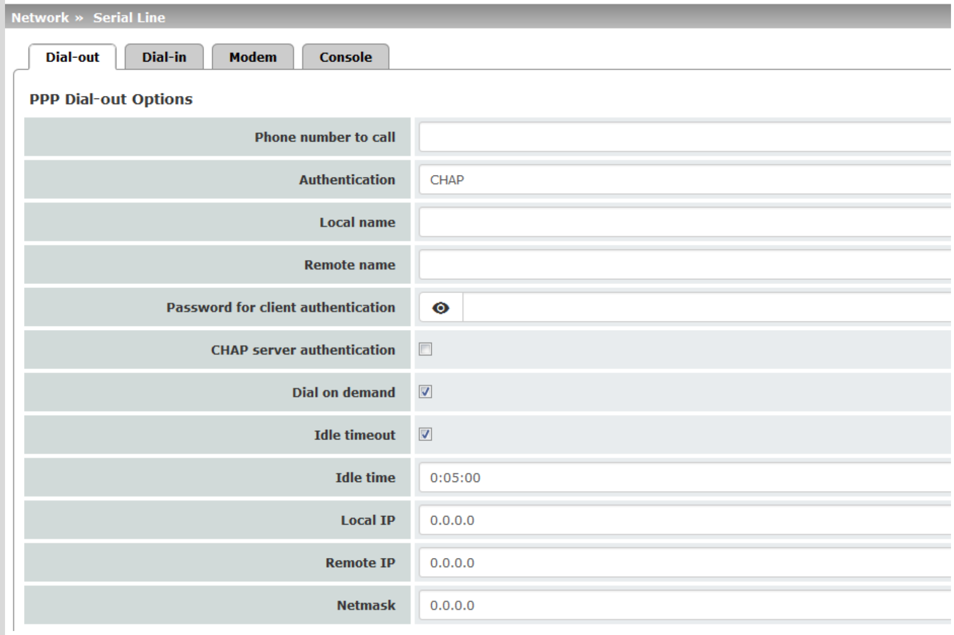
If authentication is via PAP:



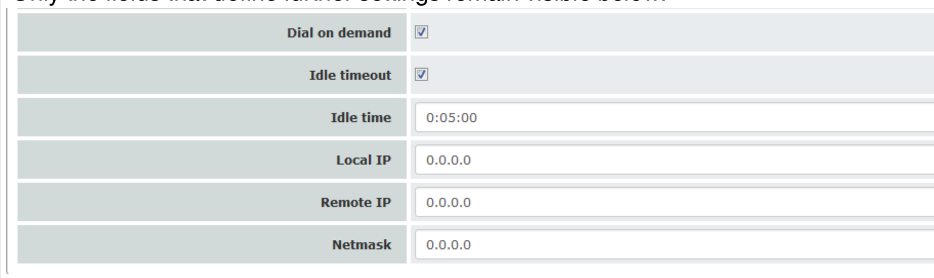
User name	User name specified during Internet service provider login to access the Internet.
Password	Password specified during Internet service provider login to access the Internet.
PAP server authentication	The following two input fields are shown when the function is activated:
User name of the server	User name and password that the mGuard requests from the server. The mGuard only allows the connection if the server returns the agreed user name/password combination.
Server password	
Subsequent fields	See under "If “None” is selected as the authentication method" on page 177.

Network >> Serial interface >> Dial-out [...]

If authentication is via CHAP:



Local name	A name for the mGuard that it uses to log into the Internet service provider. The service provider may have several customers and it uses this name to identify who is attempting to dial in. After the mGuard has logged into the Internet service provider with this name, the service provider also compares the password specified for client authentication (see below). The connection can only be established successfully if the name is known to the service provider and the password matches.
Remote name	A name given to the mGuard by the Internet service provider for identification purposes. The mGuard will not establish a connection to the service provider if the ISP does not give the correct name.
Password for client authentication	Password that must be specified during Internet service provider login to access the Internet.
CHAP server authentication	The following two input fields are shown when the function is activated:
Password for server authentication	Password that the mGuard requests from the server. The mGuard only allows the connection if the server returns the agreed password.
Subsequent fields	See "If “None” is selected as the authentication method" on page 177.
If “None” is selected as the authentication method	In this case, the fields that relate to the **PAP** or **CHAP** authentication methods are hidden.

Network >> Serial interface >> Dial-out [...]	
	Only the fields that define further settings remain visible below. 

Other common settings

Network >> Interfaces >> Dial-out		
PPP Dial-out Options	**Dial on demand**	
		Regardless of whether activated: the telephone connection is always established by the mGuard. If the function is activated (default): this setting is useful for telephone connections where costs are calculated according to the connection time. The mGuard only commands the modem to establish a telephone connection when network packets are actually to be transferred. It also instructs the modem to terminate the telephone connection as soon as no more network packets are to be transmitted for a specific time (see value in *Idle timeout* field). By doing this, however, the mGuard is not constantly available externally, i.e., for incoming data packets.

Network >> Interfaces >> Dial-out [...]

> The mGuard also often or sporadically establishes a connection via the modem, or keeps a connection longer, if the following conditions apply:

- Often: the mGuard is configured so that it synchronizes its system time (date and time) regularly with an external NTP server.
- Sporadically: the mGuard acts as a DNS server and must perform a DNS request for a client.
- After a restart: an active VPN connection is set to **Initiate**. If this is the case, the mGuard establishes a connection after every restart.
- After a restart: for an active VPN connection, the gateway of the peer is specified as the host name. After a restart, the mGuard must request the IP address that corresponds to the host name from a DNS server.
- Often: VPN connections are set up and DPD messages are sent regularly (see "Dead Peer Detection" on page 360).
- Often: the mGuard is configured to send its external IP address regularly to a DNS service, e.g., DynDNS, so that it can still be accessed via its host name.
- Often: the IP addresses of peer VPN gateways must be requested from the DynDNS service or they must be kept up to date by new queries.
- Sporadically: the mGuard is configured so that SNMP traps are sent to the remote server.
- Sporadically: the mGuard is configured to permit and accept remote access via HTTPS, SSH or SNMP. (The mGuard then sends reply packets to every IP address from which an access attempt is made (if the firewall rules permit this access)).
- Often: the mGuard is configured to connect to an HTTPS server at regular intervals in order to download any configuration profiles available there (see "Management >> Central Management" on page 110).

When the function is deactivated, the mGuard establishes a telephone connection using the connected modem as soon as possible after a restart or activation of *Modem* network mode. This remains permanently in place, regardless of whether or not data is transmitted. If the telephone connection is then interrupted, the mGuard attempts to restore it immediately. Thus a permanent connection is created, like a permanent line. By doing this, the mGuard is constantly available externally, i.e., for incoming data packets.

Idle timeout

Only considered when *Dial on demand* is activated.

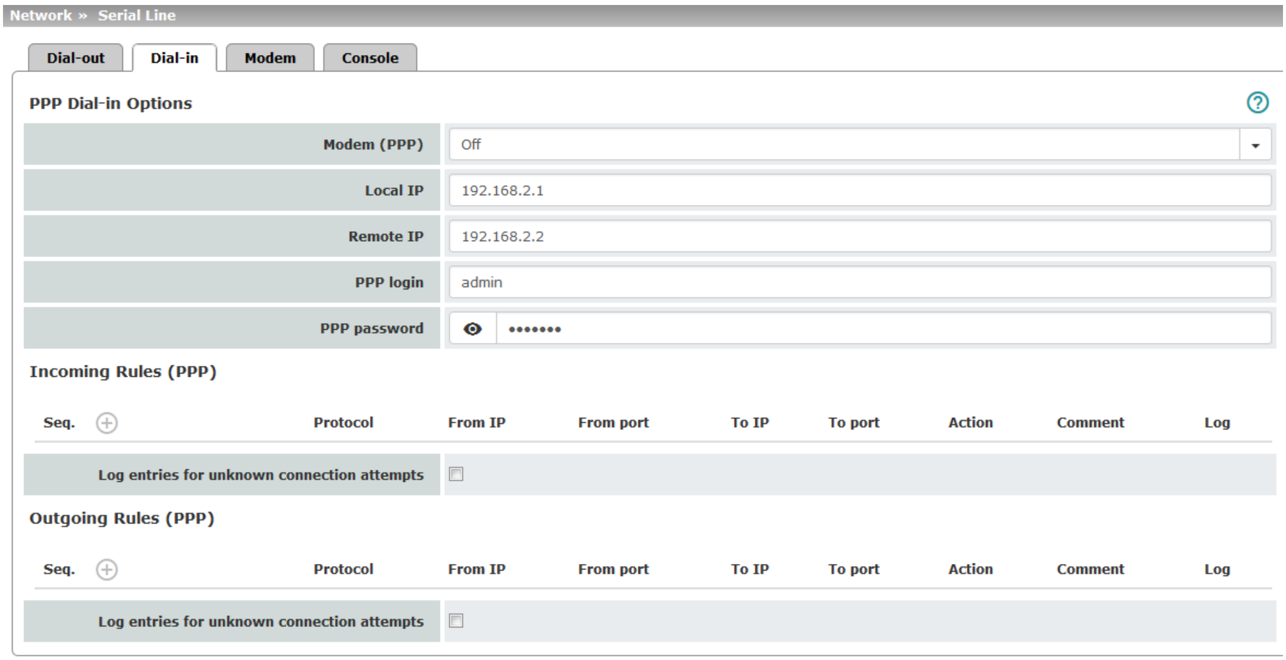
When the function is activated (default), the mGuard terminates the telephone connection as soon as no data traffic is transmitted over the time period specified under *Idle time*. The mGuard gives the connected modem the relevant command for terminating the telephone connection.

When the function is deactivated, the mGuard does not give the connected modem a command for terminating the telephone connection.

Network >> Interfaces >> Dial-out [...]		
	Idle time (seconds)	Default: 300 seconds (00:05:00) If there is still no data traffic after the time specified here has elapsed, the mGuard can terminate the telephone connection (see above under *Idle timeout*). The entry can be in seconds [ss], minutes and seconds [mm:ss] or hours, minutes, and seconds [hh:mm:ss].
	Local IP	IP address of the serial interface of the mGuard that now acts as the WAN interface. If this IP address is assigned dynamically by the Internet service provider, use the preset value: 0.0.0.0. Otherwise, e.g., for the assignment of a fixed IP address, enter this here.
	Remote IP	IP address of the peer. When connecting to the Internet, this is the IP address of the Internet service provider, which is used to provide access to the Internet. As the Point-to-Point Protocol (PPP) is used for the connection, the IP address does not usually have to be specified. This means you can use the preset value: 0.0.0.0.
	Netmask	The netmask specified here belongs to both the *Local IP* address and the *Remote IP* address. Normally all three values (*Local IP, IP address of peer, Netmask*) are either fixed or remain set to 0.0.0.0. Enter the connection settings for an external modem on the *Modem* tab page (see "Modem" on page 184).

6.3.2 Dial-in

Only for *TC MGUARD RS4000 3G, FL MGUARD RS4004, FL MGUARD RS4000, mGuard centerport (Innominate), FL MGUARD CENTERPORT*, *FL MGUARD RS*, *FL MGUARD BLADE, FL MGUARD DELTA, mGuard delta (Innominate)*



Network >> Interfaces >> Dial-in

PPP Dial-in Options

(Not for TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000)

Only for *TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004, FL MGUARD RS4000, mGuard centerport (Innominate), FL MGUARD CENTERPORT*, *FL MGUARD RS*, *FL MGUARD BLADE, FL MGUARD DELTA, mGuard delta (Innominate).*

Should only be configured if the mGuard is to permit PPP dial-in via one of the following:

– A modem connected to the serial interface
– A built-in modem (as option for the FL MGUARD RS)
– A built-in mobile network modem (for *TC MGUARD RS4000 3G,* TC MGUARD RS4000 4G).

PPP dial-in can be used to access the LAN (or the mGuard for configuration purposes) (see "Modem" on page 184).

If the modem is used for dialing out by acting as the primary external interface (*Modem* network mode) of the mGuard or as its secondary external interface (when activated in *Stealth* or *Router* network mode), it is not available for the PPP dial-in option.

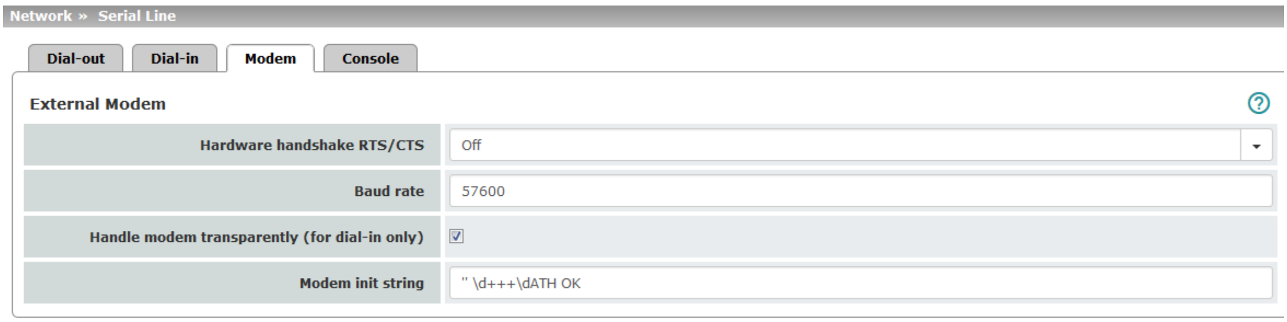
Network >> Interfaces >> Dial-in [...]		
	Modem (PPP) (Only for TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4000, FL MGUARD RS4004, FL MGUARD RS (without built-in modem/ISDN TA), FL MGUARD DELTA, mGuard delta (Innominate))	**Off / Internal Modem / External Modem** This option **must** be set to “Off” if no serial interface and no internal modem is to be used for the PPP dial-in option. If this option is set to **Internal/External Modem**, the PPP dial-in option is available. The connection settings for the connected external modem should be made on the *Modem* tab page.
	Modem (PPP) (Only for FL MGUARD RS (with built-in modem/ISDN TA))	**Off / Built-in modem / External Modem** This option **must** be set to **Off** if no serial interface should be used for the PPP dial-in option. If this option is set to **External Modem**, the PPP dial-in option is available. An external modem must then be connected to the serial interface. The connection settings for the connected external modem should be made on the *Modem* tab page. If this option is set to **Built-in modem**, the PPP dial-in option is available. In this case, the modem connection is not established via the *serial* socket on the front. Instead it is established via the terminal strip on the bottom where the built-in modem or built-in ISDN terminal adapter is connected to the telephone network. The connection settings for the built-in modem should be made on the *Modem* tab page. If the **Built-in modem** option is used, the serial interface can also be used. For the options for using the serial interface, see "Modem" on page 184.
	Local IP	IP address of the mGuard via which it can be accessed for a PPP connection.
	Remote IP	IP address of the peer of the PPP connection.
	PPP login	User identifier (login) that must be specified by the PPP peer in order to access the mGuard via a PPP connection.
	PPP password	The password that must be specified by the PPP peer in order to access the mGuard via a PPP connection.
Incoming Rules (PPP)	Firewall rules for incoming PPP connections to the LAN interface. If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored. The following options are available:	
Incoming firewall rules (serial interface)	**Protocol**	**All** means TCP, UDP, ICMP, GRE, and other IP protocols
	From IP / To IP	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 26).

Network >> Interfaces >> Dial-in [...]		
	From port / To port (Only for TCP and UDP protocols)	**any** refers to any port. **startport:endport** (e.g., 110:120) refers to a port range. Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110).
	Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back and the sender is informed of their rejection. **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts. **Name of rule records**, if defined. When a rule record is selected, the firewall rules configured under this rule record take effect (see "Rule Records" on page 268). For security reasons, rule records that contain IP groups with host names should not be used in firewall rules that execute “Drop” or “Reject” as the action. **Name of Modbus TCP rule records**, if defined. When a Modbus TCP rule record is selected, the firewall rules configured under this rule record take effect (see "Modbus TCP" on page 284).
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – activate *Log* function – Should not be logged – deactivate *Log* function (default)
	Log entries for unknown connection attempts	When the function is activated, all connection attempts that are not covered by the rules defined above are logged.
Outgoing Rules (PPP)	Firewall rules for outgoing PPP connections from the LAN interface. The parameters correspond to those under *Incoming Rules (PPP)*. These outgoing rules apply to data packets that are sent out via a data link initiated by PPP dial-in.	

6.3.3 Modem

> Only for *TC MGUARD RS4000 3G, TC MGUARD RS2000 3G (only console), FL MGUARD RS4004, FL MGUARD RS4000/RS2000, mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD RS, FL MGUARD SMART2*, *FL MGUARD DELTA* (**not** *FL MGUARD SMART 533/266, FL MGUARD PCI(E)4000, FL MGUARD BLADE, mGuard delta (Innominate).*

Some mGuard models have a serial interface that can be accessed externally, while the FL MGUARD RS is also available with a built-in modem as an option (see "Network >> Interfaces" on page 127).



Options for using the serial interface

The serial interface can be used alternatively as follows:

Primary external interface
(This menu item is not included in the scope of functions for the TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005 or FL MGUARD RS2000)

As a **primary external interface**, if the network mode is set to *Modem* under *Network >> Interfaces* on the *General* tab page (see "Network >> Interfaces" on page 127 and "General" on page 134).

In this case, data traffic is not processed via the WAN port (Ethernet interface), but via the serial interface.

Secondary external interface
(This menu item is not included in the scope of functions for the TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005 or FL MGUARD RS2000)

As a **secondary external interface**, if *Secondary External Interface* is activated and *Modem* is selected under *Network >> Interfaces* on the *General* tab page (see "Network >> Interfaces" on page 127 and "General" on page 134).

In this case, data traffic is processed (permanently or temporarily) via the serial interface.

For dialing in to the LAN or for configuration purposes (This menu item is not included in the scope of functions for the TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005 or FL MGUARD RS2000)

Used for **dialing in to the LAN or for configuration purposes** (see also "Dial-in" on page 181). The following options are available:

– A modem is connected to the serial interface of the mGuard. This modem is connected to the telephone network (fixed-line or GSM network).

  (The connection to the telephone network is established via the terminal strip on the bottom of the device for the FL MGUARD RS **with** built-in modem or ISDN terminal adapter.)

  This enables a remote PC that is also connected to the telephone network via a modem or ISDN adapter to establish a PPP (Point-to Point Protocol) dial-up connection to the mGuard.

This method is referred to as a PPP dial-in option. It can be used for access to the LAN, which is located behind the mGuard or for configuration of the mGuard. *Dial-in* is the interface designation used for this connection type in firewall selection lists.

In order to access the LAN with a Windows computer using the dial-up connection, a network connection must be set up on this computer in which the dial-up connection to the mGuard is defined. In addition, the IP address of the mGuard (or its host name) must be defined as the gateway for this connection so that the connections to the LAN can be routed via this address.

To access the web configuration interface of the mGuard, you must enter the IP address of the mGuard (or its host name) in the address line of the web browser.

– The serial interface of the mGuard is connected to the serial interface of a PC.

  On the PC, the connection to the mGuard is established using a terminal program and the configuration is implemented using the command line of the mGuard.

If an external modem is connected to the serial interface, you may have to enter corresponding settings below under *External Modem*, regardless of the use of the serial interface and the modem connected to it.

Network >> Serial interface >> Modem		
External Modem (Not for TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005, FL MGUARD RS2000)	**Hardware handshake RTS/CTS**	**Off / On** When set to **On**, flow is controlled by means of RTS and CTS signals for PPP connections.
	Baud rate	**Default: 57600 / (FL MGUARD GT/GT: 38400).** Transmission speed for communication between the mGuard and modem via the serial connecting cable between both devices. This value should be set to the highest value supported by the modem. If the value is set lower than the maximum possible speed that the modem can reach on the telephone line, the telephone line will not be used to its full potential.
	Handle modem transparently (for dial-in only)	If the external modem is used for dial-in (see Page 181), activation of the function means that the mGuard does not initialize the modem. The subsequently configured modem initialization sequence is not observed. Thus, either a modem is connected which can answer calls itself (default profile of the modem contains “auto answer”) or a null modem cable to a computer can be used instead of the modem, and the PPP protocol is used over this.
	Modem init string	Specifies the initialization sequence that the mGuard sends to the connected modem. Default: '' \d+++\dATH OK Consult the modem user manual for the initialization sequence for this modem. The initialization sequence is a sequence of character strings expected by the modem and commands that are then sent to the modem so that the modem can establish a connection.

The preset initialization sequence has the following meaning:

" (two simple quotation marks placed directly after one another)	The empty character string inside the quotation marks means that the mGuard does not initially expect any information from the connected modem, but instead sends the following text directly to the modem.
\d+++\dATH	The mGuard sends this character string to the modem in order to determine whether the modem is ready to accept commands.
OK	Specifies that the mGuard expects the ***OK*** character string from the modem as a response to ***\d+++\dATH***.

On many modem models it is possible to save modem default settings to the modem itself. However, this option should not be used.

Initialization sequences should be configured externally instead (i.e., on the mGuard). In the event of a modem fault, the modem can then be replaced quickly and smoothly without changing the modem default settings.

If the external modem is to be used for incoming calls without the modem default settings being entered accordingly, then you have to inform the modem that it should accept incoming calls after it rings.

If using the extended HAYES command set, append the character string " ***AT&S0=1 OK***" (a space followed by "***AT&S0=1***", followed by a space, followed by "***OK***") to the initialization sequence.

Depending on their default settings, some external modems require a physical connection to the DTR cable of the serial interface in order to operate correctly.

Because the mGuard models do not provide this cable at the external serial interface, the character string " ***AT&D0 OK***" (a space followed by "***AT&D0***", followed by a space, followed by "***OK***") must be appended to the above initialization sequence. According to the extended HAYES command set, this sequence means that the modem does not use the DTR cable.

If the external modem is to be used for outgoing calls, it is connected to a private branch exchange, and if this private branch exchange does not generate a dial tone after the connection is opened, then the modem must be instructed not to wait for a dial tone before dialing.

In this case, append the character string " ***ATX3 OK***" (a space followed by "***ATX3***", followed by a space, followed by "***OK***") to the initialization sequence.

In order to wait for the dial tone, the control character "***W***" should be inserted in the *Phone number to call* after the digit for dialing an outside line.

For the FL MGUARD RS with built-in modem/built-in ISDN modem (ISDN terminal adapter)

The FL MGUARD RS is available with a built-in analog modem/built-in ISDN terminal adapter as an option. The built-in modem or built-in ISDN terminal adapter can be used as follows:

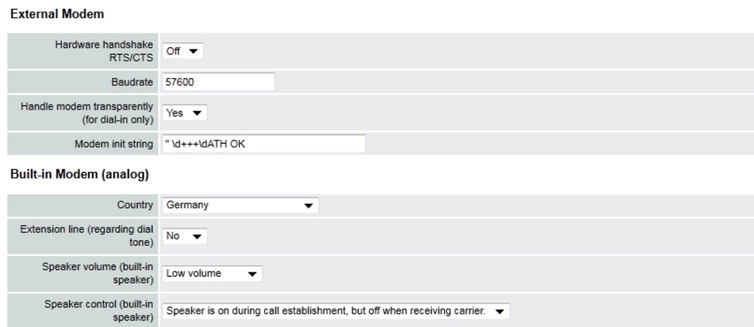
Primary External Interface

– As a **primary external interface**, if the network mode is set to *Built-in modem* under *Network >> Interfaces* on the *General* tab page (see "Network >> Interfaces" on page 127 and "General" on page 134). In this case, data traffic is not processed via the WAN port (Ethernet interface), but via this modem.

Secondary External Interface	– As a **secondary external interface**, if *Secondary External Interface* is activated and *Built-in modem* is selected under *Network >> Interfaces* on the *General* tab page (see "Network >> Interfaces" on page 127 and "General" on page 134). In this case, data traffic is also processed via the serial interface.
PPP Dial-in Options	– For the PPP dial-in option (see "Options for using the serial interface" on page 184).

Please note that the serial interface of the device also provides similar options for use (see above). Therefore on an FL MGUARD RS with a built-in modem, normal data traffic can be routed via a modem connection (*Modem* network mode) and a second modem connection can be used simultaneously for the PPP dial-in option, for example.

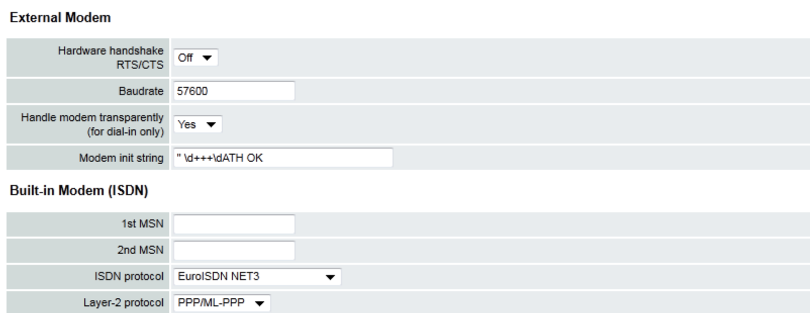
For the FL MGUARD RS with built-in modem



Additionally for the FL MGUARD RS with built-in modem (analog)

Network >> Interfaces >> Modem / Console (for the FL MGUARD RS with built-in modem)		
External Modem	**As for the TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004, FL MGUARD RS (without built-in modem), FL MGUARD DELTA, mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD BLADE, mGuard delta (Innominate):**	
	Configuration as above for **External Modem** (see "External Modem" on page 185).	
Built-in Modem (analog)	**Country**	The country where the mGuard with built-in modem is operated must be specified here. This ensures that the built-in modem operates according to the applicable remote access guidelines in the respective country and that it recognizes and uses dial tones correctly, for example.
	Extension line (regarding dial tone)	When set to **No**, the mGuard waits for the dial tone when the telephone network is accessed and the mGuard is calling the peer. When set to **Yes**, the mGuard does not wait for a dial tone. Instead it begins dialing the peer immediately. This procedure may be necessary if the built-in modem of the mGuard is connected to a private branch exchange that does not emit a dial tone when it is “picked up”. When a specific number must be dialed to access an outside line, e.g., “0”, this number should be added to the start of the desired peer phone number that is to be dialed.
	Speaker volume (built-in speaker)	
	Speaker control (built-in speaker)	These two settings specify which sounds should be emitted by the mGuard speaker and at what volume.

For the FL MGUARD RS with built-in ISDN terminal adapter

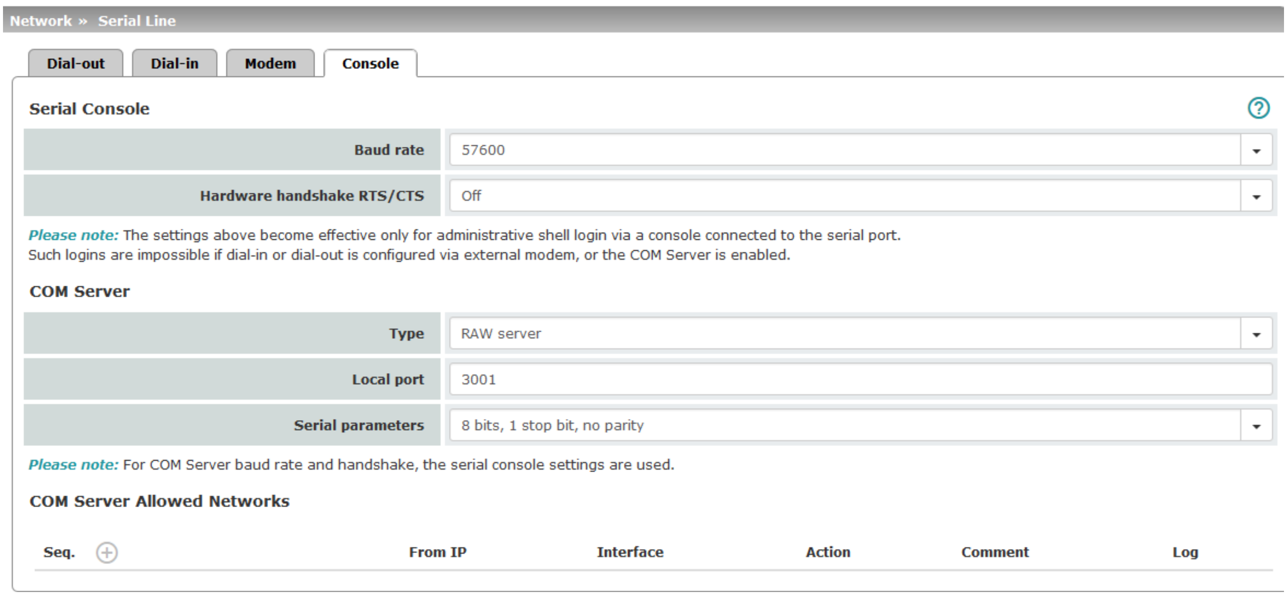


Additionally for the FL MGUARD RS with built-in modem (ISDN)

Network >> Interfaces >> Modem / Console (for the FL MGUARD RS with ISDN terminal adapter)		
External Modem	**As for the FL MGUARD RS4000, TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004, FL MGUARD RS (without built-in modem), mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD BLADE, mGuard delta (Innominate):**	
	Configuration as above for **External Modem** (see "External Modem" on page 185).	
Built-in Modem (ISDN)	**1st MSN**	For outgoing calls, the mGuard transmits the MSN (Multiple Subscriber Number) entered here to the called peer. In addition, the mGuard can receive incoming calls via this MSN (provided dial-in operation is enabled, see General tab page). Maximum of 25 alphanumeric characters; the following special characters can be used: *****, **#**, **:** (colon)
	2nd MSN	If the mGuard should also receive incoming calls via another number for dial-in operation (if enabled), enter the second MSN here.
	ISDN protocol	The EuroISDN protocol (also known as NET3) is used in Germany and many other European countries. Otherwise the ISDN protocol should be specified according to the country. If necessary, this must be requested from the relevant phone company.
	Layer-2 protocol	The set of rules used by the ISDN terminal adapter of the local mGuard to communicate with its ISDN peer. This generally is the ISDN modem of the Internet service provider used to establish the connection to the Internet. It must be requested from the Internet service provider. PPP/ML-PPP is often used.

6.3.4 Console

Only for *TC MGUARD RS4000 3G, TC MGUARD RS2000 3G (only console), FL MGUARD RS4004, FL MGUARD RS4000/RS2000, mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD RS, FL MGUARD SMART2*, *FL MGUARD DELTA* (**not** *FL MGUARD SMART 533/266, FL MGUARD PCI(E)4000, FL MGUARD BLADE, mGuard delta (Innominate).*



Network >> Serial interface >> Console

Serial Console

The following settings for the *Baud rate* and *Hardware handshake* are only valid for a configuration connection where a terminal or PC with terminal program is connected to the serial interface as described above.

The settings are not valid when an external modem is connected. Settings for this are made under "Modem" on page 184.

Baud rate — **9600 / 19200 / 38400 / 57600 (default) / 115200**

(**Default for FL MGUARD GT/GT: 38400**)

The transmission speed of the serial interface is specified via the selection list.

Hardware handshake RTS/CTS — **Off / On**

When set to **On**, flow is controlled by means of RTS and CTS signals.

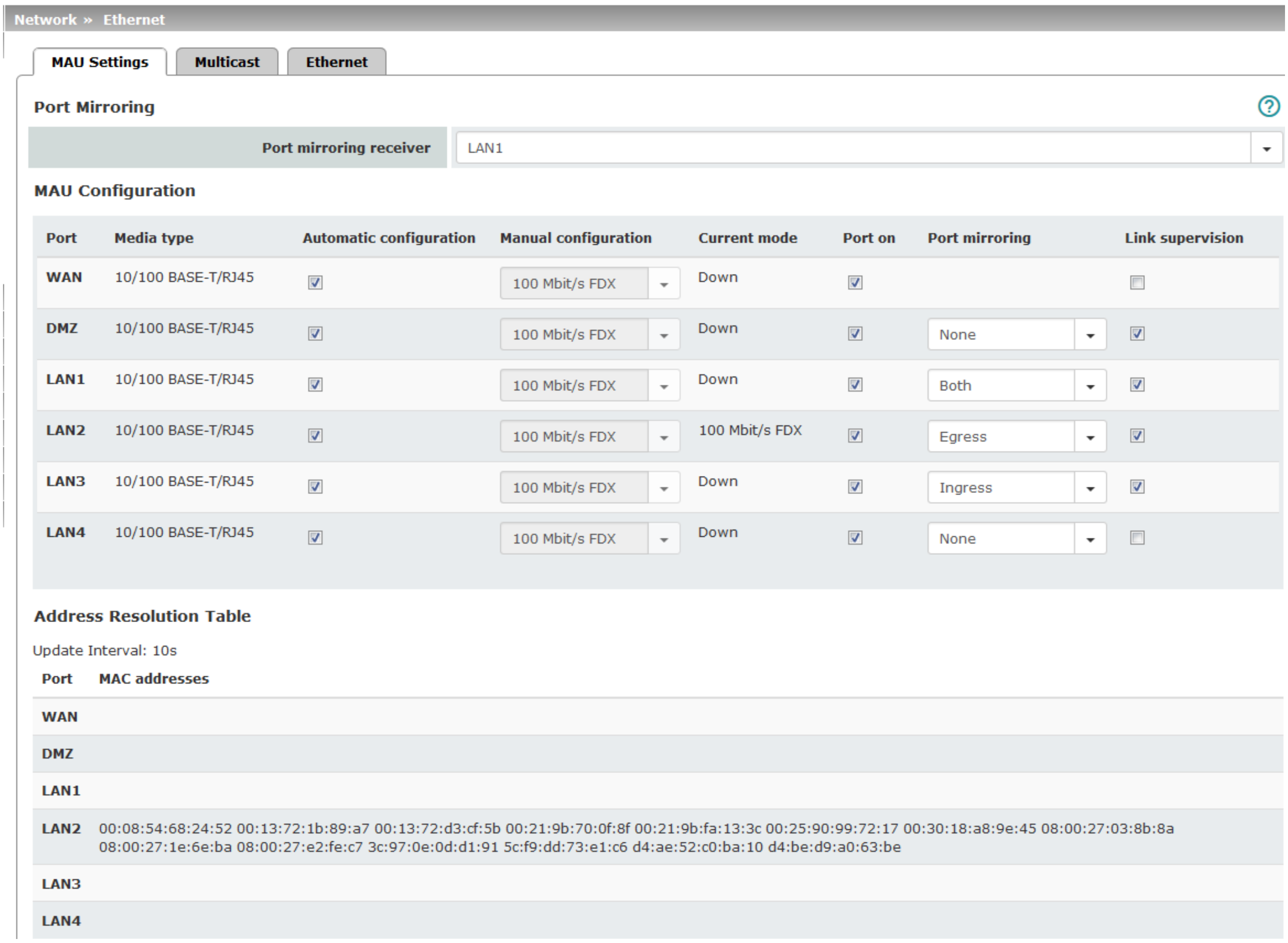
Network >> Serial interface >> Console [...]		
	Serial console via USB (Only FL MGUARD SMART2)	When the function is deactivated, the FL MGUARD SMART2 uses the USB connection solely as a power supply. When the function is activated, the FL MGUARD SMART2 provides an additional serial interface for the connected computer through the USB interface. The serial interface can be accessed on the computer using a terminal program. The FL MGUARD SMART2 provides a console through the serial interface, which can then be used in the terminal program. A special driver is required under Windows in order to use the serial console via USB. This can be downloaded directly from the mGuard.
	Serial USB driver (Windows) (Only FL MGUARD SMART2)	Click on the "Download Windows Driver from device" button to download the Windows driver.
COM Server (Only for mGuard platforms with serial interface)	The mGuard platforms with a serial interface have an integrated COM server as of firmware 8.0. This enables serial interface data exchange via an IP connection. Three options are available. – **RFC 2217** (Telnet server, complies with RFC 2217). In this mode, the serial interface can be configured via client software in the network. The Telnet server is available via the port which is defined under **"Local port"** . – **RAW client** In this mode, the mGuard initiates a connection to the address which is set under **"IP address of the peer"** . The connection is established via the port which is configured under **"Remote port"** . The interface can be configured here ("Serial parameters"). The settings of the serial console are used for the baud rate and the hardware handshake (see "External Modem" under "Network >> Serial interface >> Modem"). – **RAW server** Behaves in the same way as the RAW client. However, the RAW server responds to incoming connections via the port which is configured under **"Local port"** .	
	Type	Here you can select the way that the COM server should operate. Possible options are: RFC 2217, RAW client, RAW server.
	IP address of the peer (only for **RAW client** type)	**Default: 10.1.0.254** Defines the IP address of the peer.
	Local port (only for **RFC 2217** and **RAW server** type)	**Default: 3001** Defines the port that the COM server should respond to. Values: 1 - 65535.
	Remote port (only for **RAW client** type)	**Default: 3001** Defines the port to which the RAW client sends the data. Values: 1 - 65535.

Network >> Serial interface >> Console [...]		
	Via VPN (only for **RAW client** type)	The COM server's request is – **where possible** – carried out via a VPN tunnel (IPsec VPN or OpenVPN). **Prerequisite**: A suitable VPN tunnel is available. If no suitable VPN tunnel is available, traffic is always sent **unencrypted via the default gateway**. A suitable VPN tunnel is available if the remote peer belongs to the remote network of a configured VPN tunnel and the mGuard has an internal IP address that belongs to the local network of the same VPN tunnel. **Please note:** **For IPsec VPN connections**, the "Via VPN" function must be activated so that the traffic is routed through a suitable IPsec VPN tunnel. **For OpenVPN connections**, traffic is always routed via a suitable OpenVPN tunnel even if the function is deactivated.
	Serial parameters	Defines the parity and stop bits for the serial interface. Supported packet lengths of the serial interface: 8 Bit / 7 Bit. – 8 Bits (7 Bits), 1 stop bit, no parity (standard with 8 Bit) – 8 Bits (7 Bits), 1 stop bit, even parity – 8 Bits (7 Bits), 1 stop bit, odd parity – 8 Bits (7 Bits), 2 stop bits, no parity – 8 Bits (7 Bits), 2 stop bits, even parity – 8 Bits (7 Bits), 2 stop bits, odd parity
COM Server Allowed Networks	Access rules can be defined for the COM server to prevent unauthorized access to it. The default rule does not allow any access via the external interface.	
	From IP	0.0.0.0/0 means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 26).
	Interfaces	**Internal / External / External 2 / DMZ / VPN / GRE / Dial-in** Interface for which the rule should apply.
	Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back. The sender is informed of their rejection. **Drop** means that the data packets are not permitted to pass through. The sender is not informed of their whereabouts.
	Comment	Freely selectable comment for this rule.

Network >> Serial interface >> Console [...]		
	Log	For each firewall rule you can specify whether the event is to be logged if the rule is applied.

6.4 Network >> Ethernet

6.4.1 MAU Settings

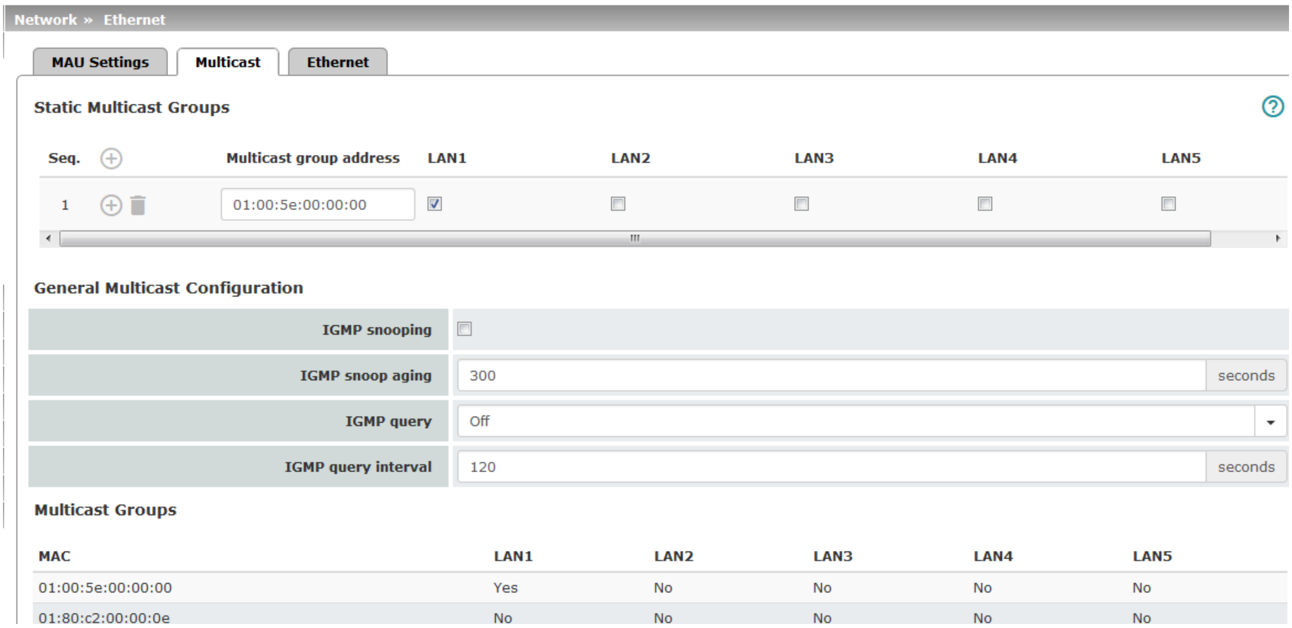


Network >> Ethernet >> MAU Settings		
Port Mirroring (Only for TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004)	**Port mirroring receiver**	The integrated switch controls port mirroring in order to monitor the network traffic. Here, you can decide which ports you want to monitor. The switch then sends copies of data packets from the monitored ports to a selected port. The port mirroring function enables any packets to be forwarded to a specific recipient. You can select the receiver port or the mirroring of the incoming and outgoing packets from each switch port.
MAU Configuration (Not for TC MGUARD RS2000 3G, TC MGUARD RS2000 4G)	Configuration and status indication of the Ethernet connections:	
	Port	Name of the Ethernet connection to which the row refers.
	Media type	Media type of the Ethernet connection.

Network >> Ethernet >> MAU Settings [...]		
	Automatic configuration	**Activated**: tries to determine the required operating mode automatically. **Deactivated**: uses the operating mode specified in the “Manual configuration” column.
	Manual configuration	The desired operating mode when ***Automatic configuration*** is **deactivated**.
	Current mode	The current operating mode of the network connection.
	Port on	Switches the Ethernet connection on or off. The **Port on** function is **not** supported by the mGuard centerport (Innominate) or FL MGUARD CENTERPORT. The **Port on** function is supported with restrictions on: **mGuard delta (Innominate)**: the internal side (switch ports) cannot be switched off. **FL MGUARD PCI 533/266**: in driver mode, the internal network interface cannot be switched off (however, this is possible in Power-over-PCI mode).
	Link supervision	Only visible when the "Management >> Service I/O >> Alarm output" menu item under Management >> Service I/O >> Alarm output is set to “Supervise”. If link supervision is active, the alarm output is opened if one link does not indicate connectivity.
	Port mirroring	The port mirroring function enables any packets to be forwarded to a specific recipient. You can select the receiver port or the mirroring of the incoming and outgoing packets from each switch port.
Address Resolution Table (Only for TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004)	**Port**	Name of the Ethernet connection to which the row refers.
	MAC addresses	Lists the MAC addresses of the connected Ethernet-capable devices. The switch can learn MAC addresses which belong to the ports of its connected Ethernet-capable devices. The contents of the list can be deleted by clicking on the “Purge” button.
Port Statistics (Only for TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004)	A statistic is displayed for each physically accessible port of the integrated Managed Switch. The counter can be reset via the web interface or the following command: ***/Packages/mguard-api_0/mbin/action switch/reset-phy-counters***	
	Port	Name of the Ethernet connection to which the row refers.
	TX collisions	Number of errors while sending the data
	TX octets	Data volume sent
	RX FCS errors	Number of received frames with invalid checksum
	RX good octets	Volume of the valid data received

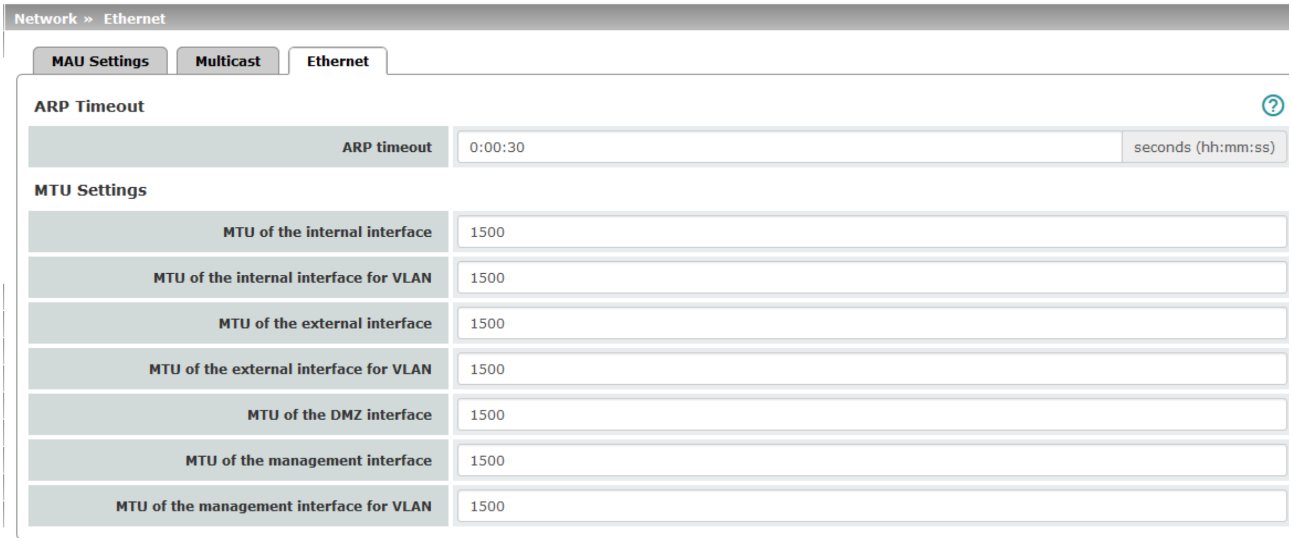
6.4.2 Multicast

Only available with the TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004.



Network >> Ethernet >> Multicast		
Static Multicast Groups	**Static Multicast Groups**	Multicast is a technology which enables data to be sent to a group of recipients, without the transmitter having to send it multiple times. The data replication takes place through the distributor within the network. You can create a list of **multicast group addresses**. The data is forwarded to the configured ports (LAN1 ... LAN5).
General Multicast Configuration	**IGMP snooping**	The switch uses IGMP snooping to guarantee that multicast data is only forwarded via ports which are intended for this use.
	IGMP snoop aging	Period, after which membership to the multicast group expires, in seconds.
	IGMP query	IGMP is used to join and leave a multicast group. Here, the IGMP version can be selected (Version v3 is not supported).
	IGMP query interval	Interval in which IGMP queries are generated in seconds
Multicast Groups	Displays the multicast groups. The display contains all static entries and the dynamic entries which are discovered by IGMP snooping.	

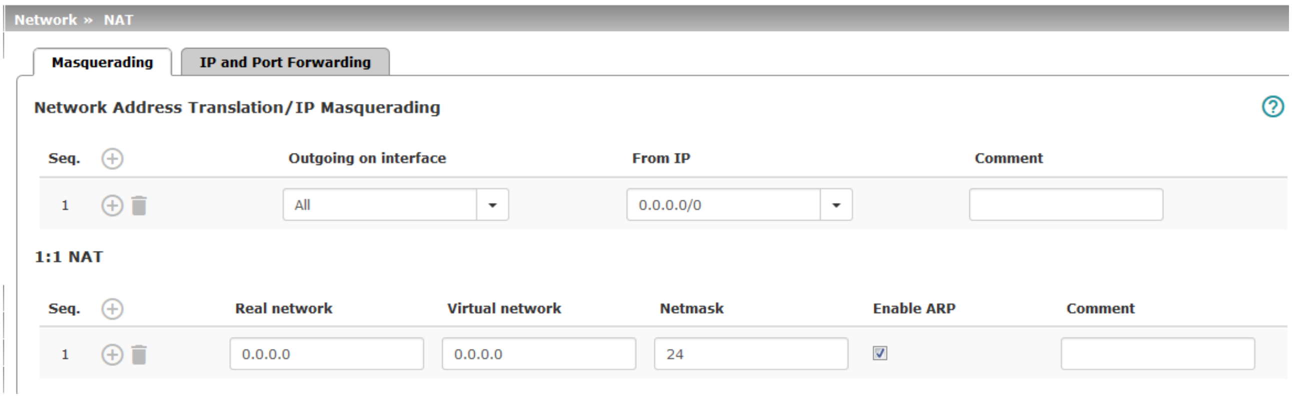
6.4.3 Ethernet



Network >> Ethernet >> Ethernet		
ARP Timeout	**ARP Timeout**	Service life of entries in the ARP table. The entry can be in seconds [ss], minutes and seconds [mm:ss] or hours, minutes, and seconds [hh:mm:ss]. MAC and IP addresses are assigned to each other in the ARP table.
The MTU settings	**MTU of the ... interface**	The maximum transfer unit (MTU) defines the maximum IP packet length that may be used for the relevant interface. The following applies for a VLAN interface: As VLAN packets contain 4 bytes more than those without VLAN, certain drivers may have problems processing these larger packets. Such problems can be solved by reducing the MTU to 1496.

6.5 Network >> NAT

6.5.1 Masquerading



Network >> NAT >> Masquerading

Network Address Translation/IP Masquerading

Lists the rules established for NAT (**N**etwork **A**ddress **T**ranslation).

For outgoing data packets, the device can rewrite the specified sender IP addresses from its internal network to its own external address, a technique referred to as NAT (Network Address Translation), see also NAT (Network Address Translation) in the glossary.

This method is used if the internal addresses cannot or should not be routed externally, e.g., because a private address area such as 192.168.x.x or the internal network structure should be hidden.

The method can also be used to hide external network structures from the internal devices. To do so, set the **Internal** option under **Outgoing on interface**. The **Internal** setting allows for communication between two separate IP networks where the IP devices have not configured a (useful) default route or differentiated routing settings (e.g., PLCs without the corresponding settings). The corresponding settings must be made under **1:1 NAT**.

This method is also referred to as *IP masquerading*.

Default setting: NAT is not active.

> If the mGuard is operated in *PPPoE/PPTP* mode, NAT must be activated in order to access the Internet. If NAT is not activated, only VPN connections can be used.

> If multiple static IP addresses are used for the WAN port, the first IP address in the list is always used for IP masquerading.

> These rules do not apply in Stealth mode.

Outgoing on interface

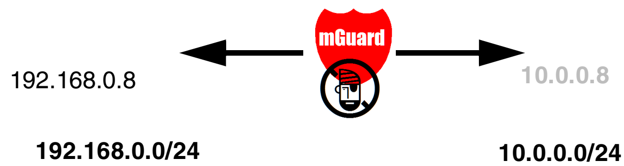
Internal / External / External 2 / DMZ / Any External[1]

Specifies via which interface the data packets are sent so that the rule applies to them. **Any External** refers to the **External** and **External 2** interfaces.

Network >> NAT >> Masquerading [...]		
		Masquerading is defined, which applies for network data flows in Router mode. These data flows are initiated so that they lead to a destination device which can be accessed over the selected network interface on the mGuard. To do this, the mGuard replaces the IP address of the initiator with a suitable IP address of the selected network interface in all associated data packets. The effect is the same as for the other values of the same variables. The IP address of the initiator is hidden from the destination of the data flow. In particular, the destination does not require any routes in order to respond in a data flow of this type (not even a default route (default gateway)).
		Set the firewall in order for the desired connections to be allowed. For incoming and outgoing rules, the source address must still correspond to the original sender if the firewall rules are used. Please observe the outgoing rules when using the “External / External 2 / Any External” settings (see "Outgoing Rules" on page 262). Please observe the incoming rules when using the “Internal” setting (see "Incoming Rules" on page 259).
	From IP	**0.0.0.0/0** means that all internal IP addresses are subject to the NAT procedure. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 26). **Name of IP groups**, if defined. When a name is specified for an IP group, the host names, IP addresses, IP areas or networks saved under this name are taken into consideration (see "IP/Port Groups" on page 275). If host names are used in IP groups, the mGuard must be configured so that the host name of a DNS server can be resolved in an IP address. If a host name from an IP group cannot be resolved, this host will not be taken into consideration for the rule. Further entries in the IP group are not affected by this and are taken into consideration.
	Comment	Can be filled with appropriate comments.
1:1 NAT	Lists the rules established for 1:1 NAT (Network Address Translation). With 1:1 NAT, the sender IP addresses are exchanged so that each individual address is exchanged with another specific address, and is not exchanged with the same address for all data packets, as in IP masquerading. This enables the mGuard to mirror addresses from the real network to the virtual network.	

Network >> NAT >> Masquerading [...]

Example: The mGuard is connected to network 192.168.0.0/24 via its LAN port and to network 10.0.0.0/24 via its WAN port. By using 1:1 NAT, the LAN computer with IP address 192.168.0.8 can be accessed via IP address 10.0.0.8 in the virtual network.



The mGuard claims the IP addresses entered for the “Virtual network” for the devices in its “Real network”. The mGuard returns ARP answers for all addresses from the specified “Virtual network” on behalf of the devices in the “Real network”. The IP addresses entered under “Virtual network” must not be used. They must not be assigned to other devices or used in any way, as an IP address conflict would otherwise occur in the virtual network. This even applies when no device exists in the “Real network” for one or more IP addresses from the specified “Virtual network”.

Default setting: 1:1 NAT is not active.

> 1:1 NAT cannot be applied to the *External 2* interface.

> 1:1 NAT is only used in *Router* network mode.

Real network

The real IP address of the client that should be reachable from another network via the virtual IP address (depending on the scenario at LAN, WAN, or DMZ port).

One or more clients can be reachable depending on the network mask.

From mGuard firmware 8.0.0, 1:1-NAT between all interfaces is possible (LAN <–> WAN, LAN <–> DMZ, DMZ <–> WAN).

Virtual network

The virtual IP address with which the clients are reachable from the other network (depending on the scenario at LAN, WAN, or DMZ port).

> The virtual IP-addresses must not be assigned and used by other clients.

From mGuard firmware 8.0.0, 1:1-NAT between all interfaces is possible (LAN <–> WAN, LAN <–> DMZ, DMZ <–> WAN).

Netmask

The netmask as a value between 1 and 32 for the local and external network address (see also "CIDR (Classless Inter-Domain Routing)" on page 26).

Enable ARP

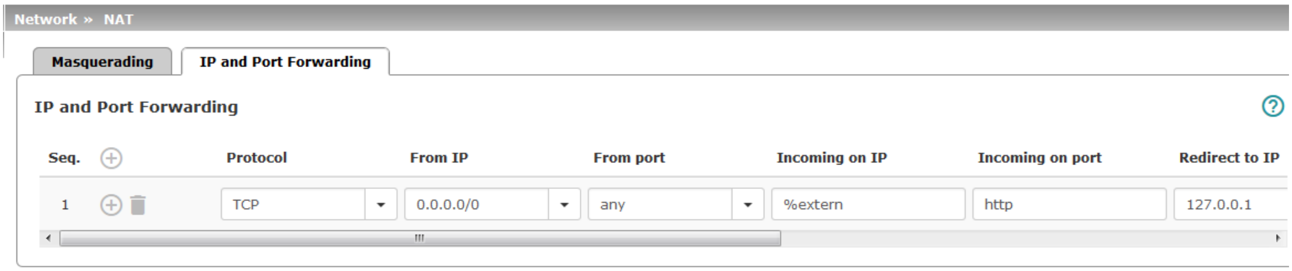
When the function is activated, ARP requests sent to the virtual network are answered on behalf of the mGuard. This means that hosts located in the real network can be accessed via their virtual address.

When the function is deactivated, ARP requests sent to the virtual network remain unanswered. This means that hosts in the real network cannot be accessed.

Network >> NAT >> Masquerading [...]		
	Comment	Can be filled with appropriate comments.

[1] *External 2* and *Any External* are only for devices with a serial interface: *TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4004/RS2005, FL MGUARD RS4000/RS2000, mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD RS, FL MGUARD BLADE, FL MGUARD DELTA, mGuard delta (Innominate)* (see "Secondary External Interface" on page 149).

6.5.2 IP and Port Forwarding



Network >> NAT >> IP and Port Forwarding

IP and Port Forwarding

Lists the rules defined for port forwarding (DNAT = Destination NAT).

IP and port forwarding performs the following: the headers of incoming data packets from the external network, which are addressed to the external IP address (or one of the external IP addresses) of the mGuard and to a specific port of the mGuard, are rewritten in order to forward them to a specific computer in the internal network and to a specific port on this computer. In other words, the IP address and port number in the header of incoming data packets are changed.

IP and port forwarding from the internal network behaves as described above.

> Port forwarding cannot be used for connections initiated via the *External 2*[1] interface.
>
> [1] *External 2* is only for devices with a serial interface.

> The rules defined here have priority over the settings made under Network Security >> Packet Filter >> Incoming Rules.

> IP and port forwarding cannot be used in *Stealth* network mode.

Protocol: TCP / UDP / GRE

Specify the protocol to which the rule should apply.

GRE

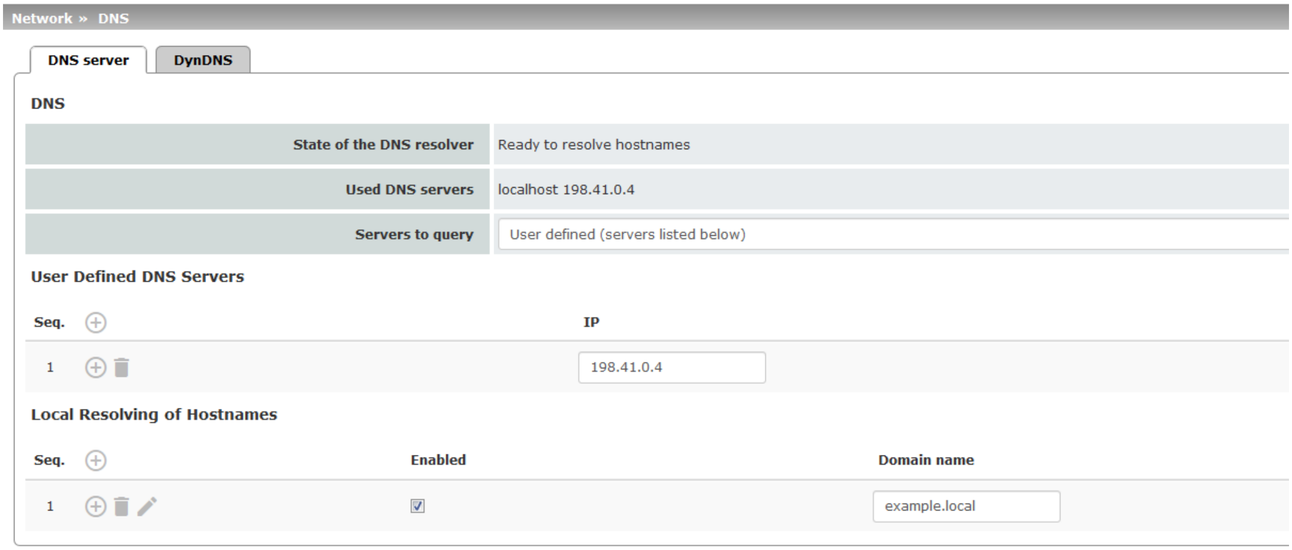
GRE protocol IP packets can be forwarded. However, only one GRE connection is supported at any given time. If more than one device sends GRE packets to the same external IP address, the mGuard may not be able to feed back reply packets correctly. We recommend only forwarding GRE packets from specific transmitters. These could be ones that have had a forwarding rule set up for their source address by entering the transmitter address in the “From IP” field, e.g., 193.194.195.196/32.

Network >> NAT >> IP and Port Forwarding [...]		
	From IP	The sender address for forwarding. **0.0.0.0/0** means all addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 26). **Name of IP groups**, if defined. When a name is specified for an IP group, the host names, IP addresses, IP areas or networks saved under this name are taken into consideration (see "IP/Port Groups" on page 275). If host names are used in IP groups, the mGuard must be configured so that the host name of a DNS server can be resolved in an IP address. If a host name from an IP group cannot be resolved, this host will not be taken into consideration for the rule. Further entries in the IP group are not affected by this and are taken into consideration.
	From port	The sender port for forwarding. **any** refers to any port. Either the port number or the corresponding service name can be specified here, e.g., *pop3* for port 110 or *http* for port 80. **Name of port groups**, if defined. When a name is specified for a port group, the ports or port ranges saved under this name are taken into consideration (see "IP/Port Groups" on page 275).
	Incoming on IP	– Specify the external IP address (or one of the external IP addresses) of the mGuard here, **or** – Specify the internal IP address (or one of the internal IP addresses) of the mGuard here, **or** – Use the variable **%extern** (if the external IP address of the mGuard is changed dynamically so that the external IP address cannot be specified). If multiple static IP addresses are used for the WAN port, the **%extern** variable always refers to the first IP address in the list.
	Incoming on port	The original destination port specified in the incoming data packets. Either the port number or the corresponding service name can be specified here, e.g., *pop3* for port 110 or *http* for port 80. This information is not relevant for the “GRE” protocol. It is ignored by the mGuard.
	Redirect to IP	The internal IP address to which the data packets should be forwarded and into which the original destination addresses are translated.

Network >> NAT >> IP and Port Forwarding [...]		
	Redirect to port	The port to which the data packets should be forwarded and into which the original port data is translated. Either the port number or the corresponding service name can be specified here, e.g., *pop3* for port 110 or *http* for port 80. This information is not relevant for the “GRE” protocol. It is ignored by the mGuard.
	Comment	Freely selectable comment for this rule.
	Log	For each individual port forwarding rule, you can specify whether the use of the rule: – Should be logged – activate *Log* function – Should not be logged – deactivate *Log* function (default)

6.6 Network >> DNS

6.6.1 DNS server



Network >> DNS >> DNS server		
DNS	If the mGuard is to initiate a connection to a peer on its own (e.g., to a VPN gateway or NTP server) and it is specified in the form of a host name (i.e., www.example.com), the mGuard must determine which IP address belongs to the host name. To do this, it connects to a domain name server (DNS) to query the corresponding IP address there. The IP address determined for the host name is stored in the cache so that it can be found directly (i.e., more quickly) for other host name resolutions. With the *Local resolving of hostnames* function, the mGuard can also be configured to respond to DNS requests for locally used host names itself by accessing an internal, previously configured directory. The locally connected clients can be configured (manually or via DHCP) so that the local address of the mGuard is used as the address of the DNS server to be used. If the mGuard is operated in *Stealth* mode, the management IP address of the mGuard (if this is configured) must be used for the clients, or the IP address 1.1.1.1 must be entered as the local address of the mGuard.	
	State of the DNS resolver	Status of the host name resolution
	Used DNS servers	DNS servers for which the associated IP address was queried.

Network >> DNS >> DNS server [...]

Servers to query

DNS root servers

Requests are sent to the root name servers on the Internet whose IP addresses are stored on the mGuard. These addresses rarely change.

Provider defined (i.e., via PPPoE or DHCP)

The DNS servers of the Internet service provider (ISP) that provide access to the Internet are used. Only select this setting if the mGuard operates in *PPPoE*, *PPTP*, *Modem* mode or in *Router* mode with DHCP.

From mGuard firmware version 8.6.0, the setting can also be used if the mGuard is located in ***Stealth* mode** (*automatic*). In this case, the DNS server that the client uses can be recognized and taken on.

User defined (servers listed below)

If this setting is selected, the mGuard will connect to the DNS servers listed under *User Defined DNS Servers*.

User Sefined DNS Servers

(Only when **User defined** is selected as root server)

The IP addresses of DNS servers can be entered in this list. If this should be used by the mGuard, select the "User defined (servers listed below)" option under **Servers to query**.

Local Resolving of Hostnames

You can configure multiple entries with assignment pairs of host names and IP addresses for various domain names.

You have the option to define, change (edit), and delete assignment pairs of host names and IP addresses. You can also activate or deactivate the resolution of host names for a domain. In addition, you can delete a domain with all its assignment pairs.

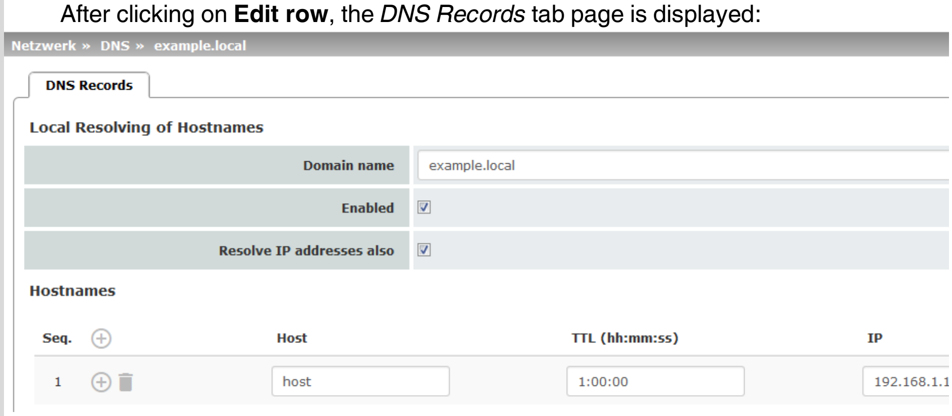
Creating a table with assignment pairs for a domain:

- Open a new row and click on the **Edit Row** icon in this row.

Changing or deleting assignment pairs belonging to a domain:

- Click on the **Edit Row** icon in the relevant table row.

  After clicking on **Edit row**, the *DNS Records* tab page is displayed:



Domain name

The name can be freely assigned, but it must adhere to the rules for assigning domain names. It is assigned to every host name.

Network >> DNS >> DNS server [...]		
	Enabled	Activates or deactivates the *Local Resolving of Hostnames* function for the domain specified in the “Domain name” field.
	Resolve IP addresses also	**Deactivated:** the mGuard only resolves host names, i.e., it supplies the assigned IP address for host names. **Activated**: as with “Deactivated”. It is also possible to determine the host names assigned to an IP address.
	Hostnames	The table can have any number of entries. A host name may be assigned to multiple IP addresses. Multiple host names may be assigned to one IP address.
	Host	Host name
	TTL (hh:mm:ss)	Abbreviation for **T**ime **T**o **L**ive. Default: 3600 seconds (1:00:00) Specifies how long called assignment pairs may be stored in the cache of the calling computer.
	IP	The IP address assigned to the host name in this table row.

Example: Local Resolving of Hostnames

The “Local Resolving of Hostnames” function is used in the following scenario, for example:

A plant operates a number of identically structured machines, each one as a cell. The local networks of cells A, B, and C are each connected to the plant network via the Internet using the mGuard. Each cell contains multiple control elements, which can be addressed via their IP addresses. Different address areas are used for each cell.

A service technician should be able to use her/his notebook on site to connect to the local network for machine A, B or C and to communicate with the individual controllers. So that the technician does not have to know and enter the IP address for every single controller in machine A, B or C, host names are assigned to the IP addresses of the controllers in accordance with a standardized diagram that the service technician uses. The host names used for machines A, B, and C are identical, i.e., the controller for the packing machine in all three machines has the host name “pack”, for example. However, each machine is assigned an individual domain name, e.g., cell-a.example.com.

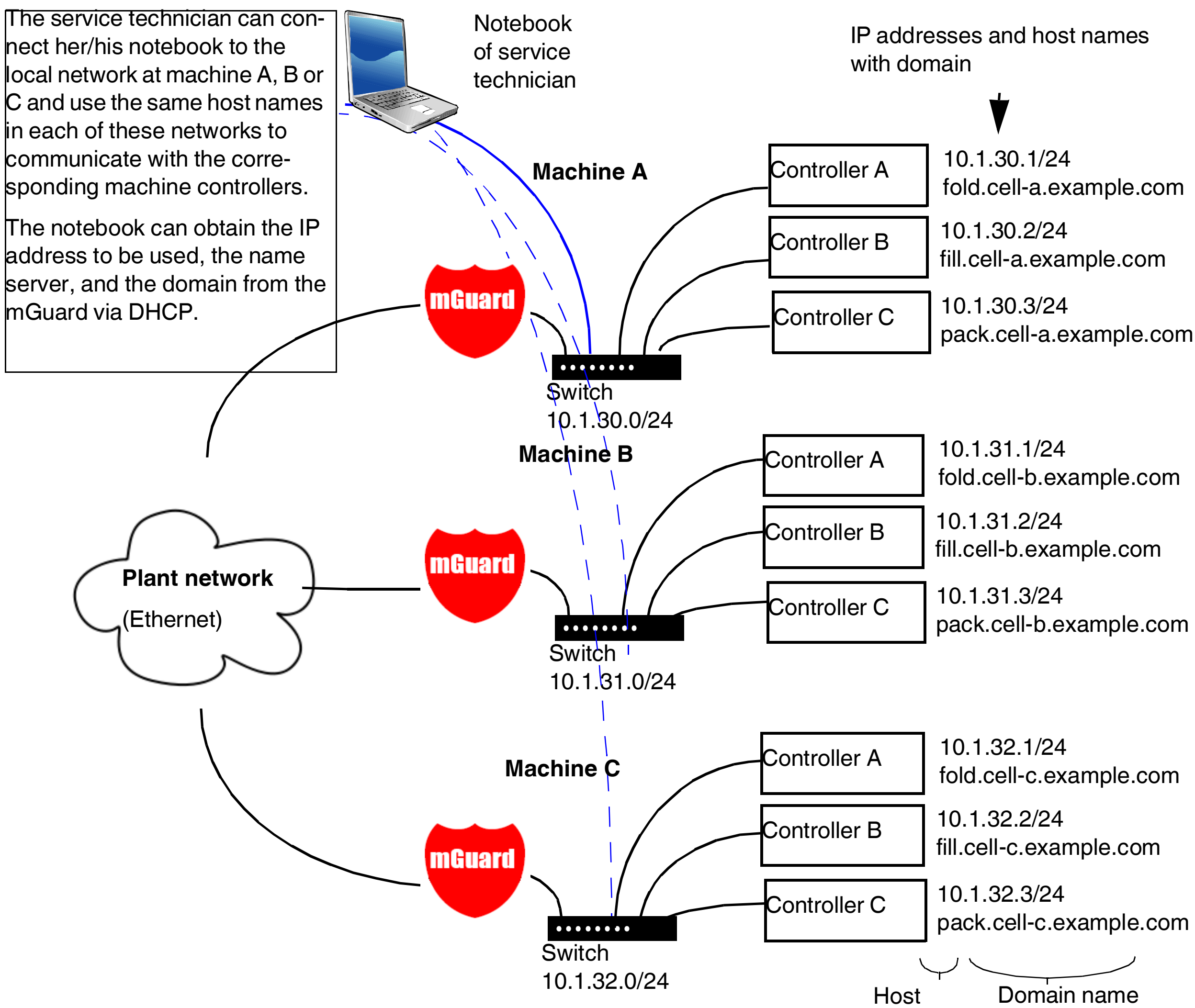
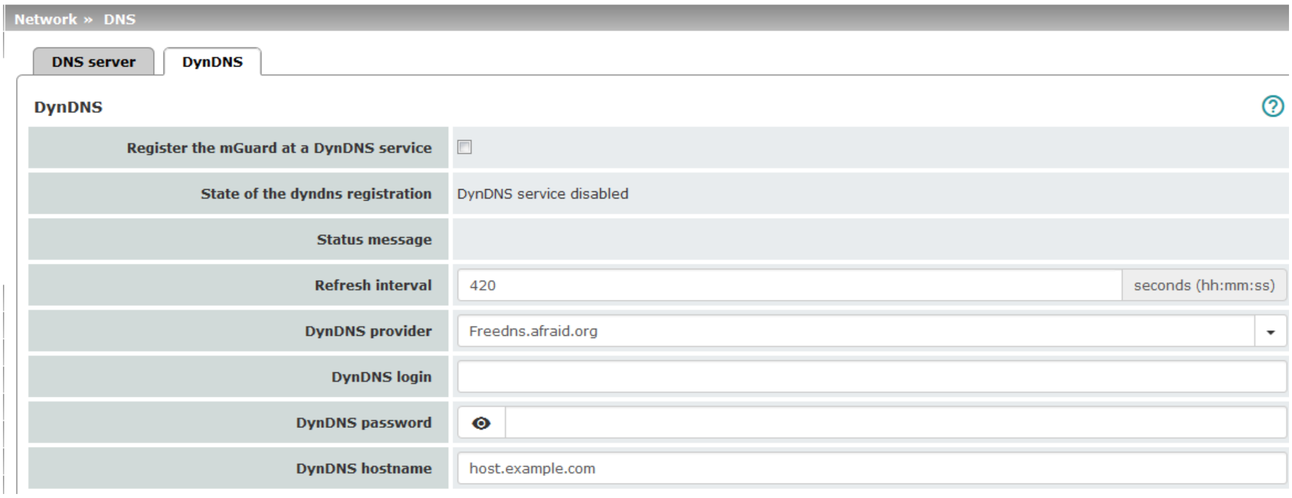


Figure 6-1 Local Resolving of Hostnames

6.6.2 DynDNS



Network >> DNS >> DynDNS		
DynDNS	In order for a VPN connection to be established, at least one partner IP address must be known so that the partners can contact each other. This condition is not met if both participants are assigned IP addresses dynamically by their respective Internet service providers. In this case, a DynDNS service such as DynDNS.org or DNS4BIZ.com can be of assistance. With a DynDNS service, the currently valid IP address is registered under a fixed name. If you have registered with one of the DynDNS services supported by the mGuard, you can enter the corresponding information in this dialog box. When using the TC MGUARD RS4000/RS2000 3G and TC MGUARD RS4000/RS2000 4G, be aware that DynDNS is not permitted by all mobile network providers.	
	Register the mGuard at a DynDNS service	Activate the function if you have registered with a DynDNS provider and if the mGuard is to use this service. The mGuard then reports its current IP address to the DynDNS service (i.e., the one assigned for its Internet connection by the Internet service provider).
	State of the DynDNS registration	State of the DynDNS registration
	Status message	Status message
	Refresh Interval	Default: 420 (seconds) The mGuard informs the DynDNS service of its new IP address whenever the IP address of its Internet connection is changed. In addition, the device can also report its IP address at the interval specified here. This setting has no effect for some DynDNS providers, such as DynDNS.org, as too many updates can cause the account to be closed.

Network >> DNS >> DynDNS [...]		
	DynDNS provider	The providers in this list support the same protocol as the mGuard. Select the name of the provider with whom you are registered, e.g., DynDNS.org, TinyDynDNS, DNS4BIZ. If your provider is not in the list, select **DynDNS-compatible** and enter the server and port for this provider.
	DynDNS server	Only visible when DynDNS provider is set to **DynDNS-compatible**. Name of the server for the DynDNS provider.
	DynDNS port	Only visible when DynDNS provider is set to **DynDNS-compatible**. Number of the port for the DynDNS provider.
	DynDNS login	Enter the user identifier assigned by the DynDNS provider here.
	DynDNS password	Enter the password assigned by the DynDNS provider here.
	DynDNS hostname	The host name selected for this mGuard at the DynDNS service, providing you use a DynDNS service and have entered the corresponding data above. The mGuard can then be accessed via this host name.

6.7 Network >> DHCP

The dynamic host configuration protocol (DHCP) can be used to automatically assign the network configuration set here to the computers connected directly to the mGuard. You can specify the DHCP settings for the internal interface (LAN port) under **Internal DHCP** and the DHCP settings for the external interface (WAN port) under **External DHCP**. DHCP settings for the DMZ interface (DMZ port) can be made under **DMZ DHCP**.

The **External DHCP** and **DMZ DHCP** menu items are not included in the scope of functions of FL MGUARD RS2000, TC MGUARD RS2000 3G, TC MGUARD RS2000 4G and FL MGUARD RS2005.

The DHCP server also operates in *Stealth* mode.

In multi-stealth mode, the external DHCP server of the mGuard cannot be used if a VLAN ID is assigned as the management IP.

IP configuration for Windows computers: when you start the DHCP server of the mGuard, you can configure the locally connected computers so that they obtain their IP addresses automatically from the mGuard via DHCP.

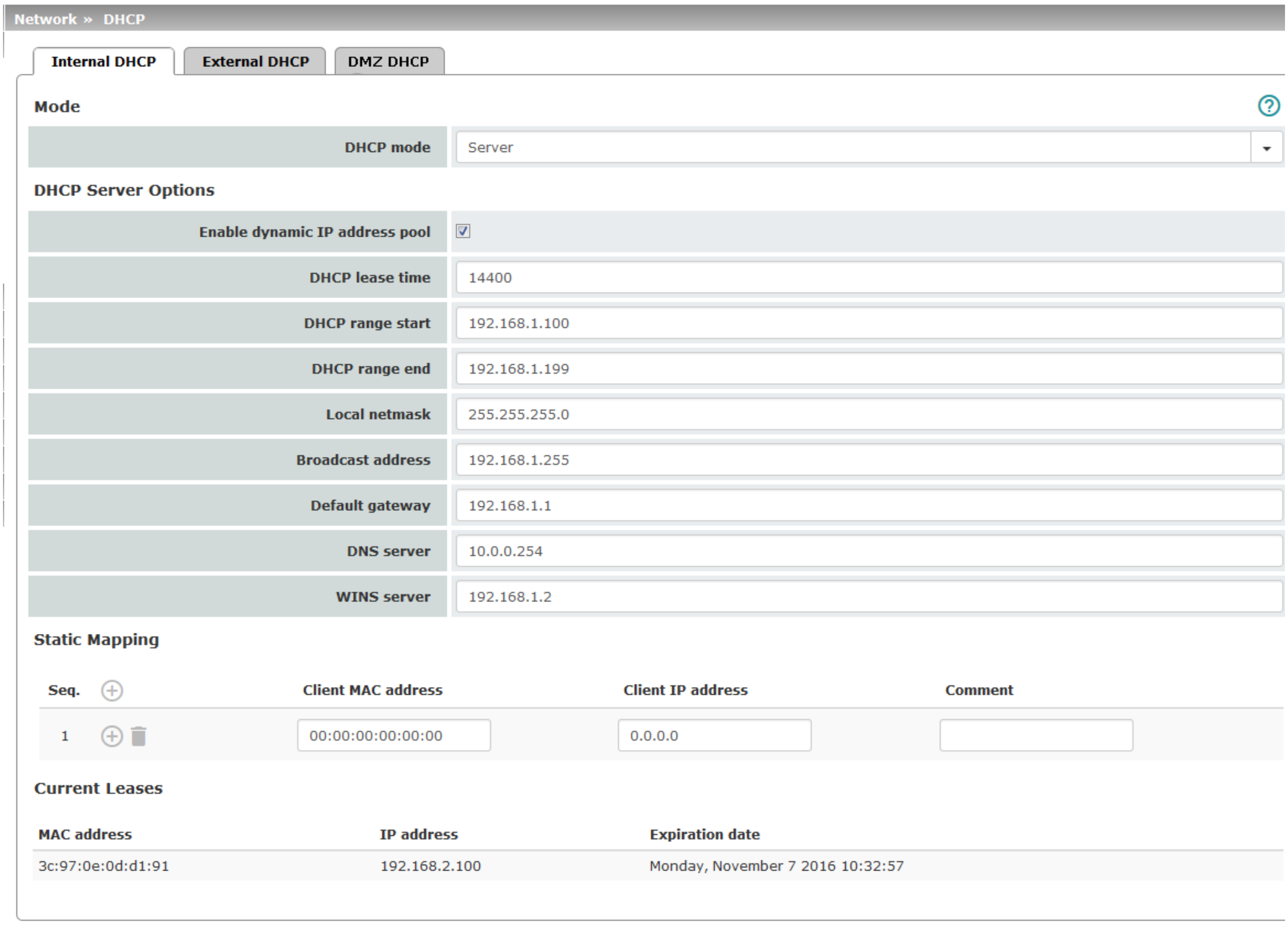
Under Windows XP

- In the Start menu, select “Control Panel, Network Connections”.
- Right-click on the LAN adapter icon and select “Properties” from the context menu.
- On the “General” tab, select “Internet Protocol (TCP/IP)” under “This connection uses the following items”, then click on the “Properties” button.
- Make the appropriate entries and settings in the “Internet Protocol Properties (TCP/IP)” dialog box.

Under Windows 7

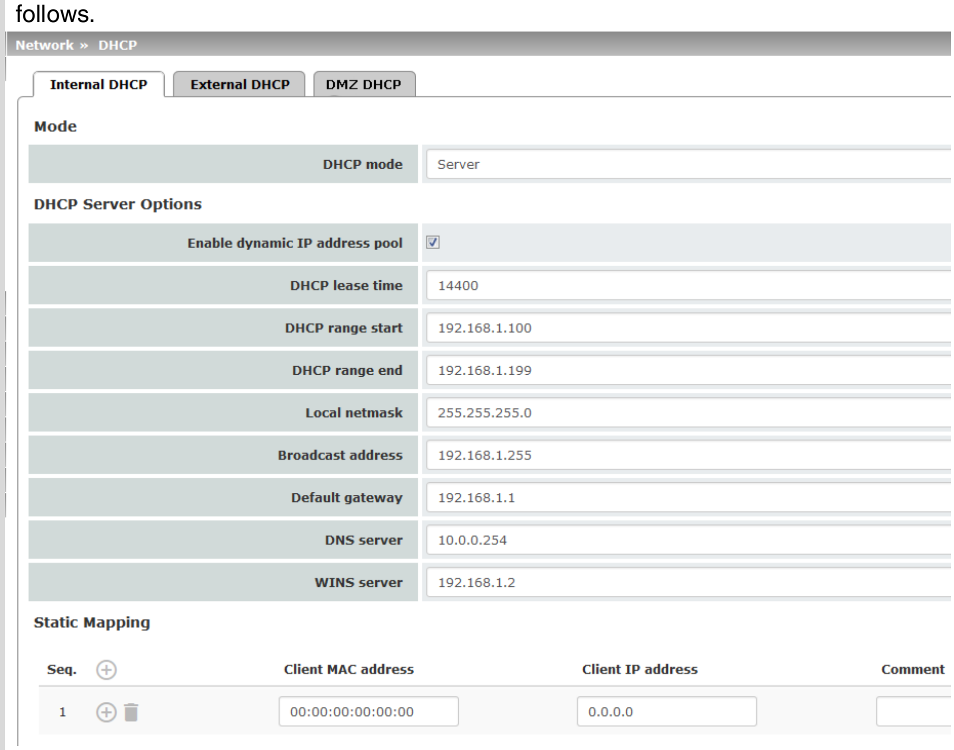
- In the Start menu, select: “Control Panel >> Network and Internet >> Network and Sharing Center”.
- Click on “Local Area Connection” under “Connections:”.
- Click on the “Properties” button in the “Local Area Connection Status” window (administrator rights required).
- In the “Local Area Connection Properties” window, select “Internet Protocol Version 4 (TCP/IPv4)” and click on the “Properties” button.
- Make the appropriate entries and settings in the “Internet Protocol Version 4 (TCP/IPv4) Properties” dialog box.

6.7.1 Internal/External DHCP



Network >> DHCP >> Internal DHCP	
	The settings for **Internal DHCP** and **External DHCP** are essentially identical and are not described separately in this section.

Network >> DHCP >> Internal DHCP[...]		
Mode	**DHCP mode**	**Disabled / Server / Relay**
		Set this option to **Server** if the mGuard is to operate as an independent DHCP server. The corresponding setting options are then displayed below on the tab page (see "DHCP mode: Server").
		Set this option to **Relay** if the mGuard is to forward DHCP requests to another DHCP server. The corresponding setting options are then displayed below on the tab page (see "DHCP mode: Relay").
		In mGuard *Stealth* mode, *Relay* DHCP mode is not supported. If the mGuard is in *Stealth* mode and *Relay* DHCP mode is selected, this setting will be ignored. However, DHCP requests from the computer and the corresponding responses are forwarded due to the nature of Stealth mode.
		If this option is set to **Disabled**, the mGuard does not answer any DHCP requests.
DHCP mode: Server		
	If DHCP mode is set to *Server*, the corresponding setting options are displayed below as follows.	



Network >> DHCP >> Internal DHCP[...]		
DHCP Server Options	**Enable dynamic IP address pool:**	When the function is activated, the IP address pool specified under *DHCP range start* and *DHCP range end* is used (see below). Deactivate the function if only static assignments should be made using the MAC addresses (see below).
	DHCP lease time	Time in seconds for which the network configuration assigned to the computer is valid. The client should renew its assigned configuration shortly before this time expires. Otherwise it may be assigned to other computers.
	DHCP range start (With enabled dynamic IP address pool)	The start of the address area from which the DHCP server of the mGuard should assign IP addresses to locally connected computers.
	DHCP range end (With enabled dynamic IP address pool)	The end of the address area from which the DHCP server of the mGuard should assign IP addresses to locally connected computers.
	Local netmask	Specifies the netmask of the computers. Default: 255.255.255.0
	Broadcast address	Specifies the broadcast address of the computers.
	Default gateway	Specifies which IP address should be used by the computer as the default gateway. Usually this is the internal IP address of the mGuard.
	DNS server	Address of the server used by the computer to resolve host names in IP addresses via the Domain Name Service (DNS). If the DNS service of the mGuard is to be used, enter the internal IP address of the mGuard here.
	WINS server	Address of the server used by the computer to resolve host names in addresses via the Windows Internet Naming Service (WINS).
Static Mapping	**Client MAC address**	To find out the **MAC address** of your computer, proceed as follows: **Windows 95/98/ME**: • Start **winipcfg** in a DOS box. **Windows NT/2000/XP/**: • Start **ipconfig /all** in a command prompt. The MAC address is displayed as the “Physical Address”. **Linux**: • Call **/sbin/ifconfig** or **ip link show** in a shell. The following options are available: – Client/computer MAC address (without spaces or hyphens) – Client IP address

Network >> DHCP >> Internal DHCP[...]

Client IP address

The static IP address of the computer to be assigned to the MAC address.

> Static assignments take priority over the dynamic IP address pool.

> Static assignments must not overlap with the dynamic IP address pool.

> Do not use one IP address in multiple static assignments, otherwise this IP address will be assigned to multiple MAC addresses.

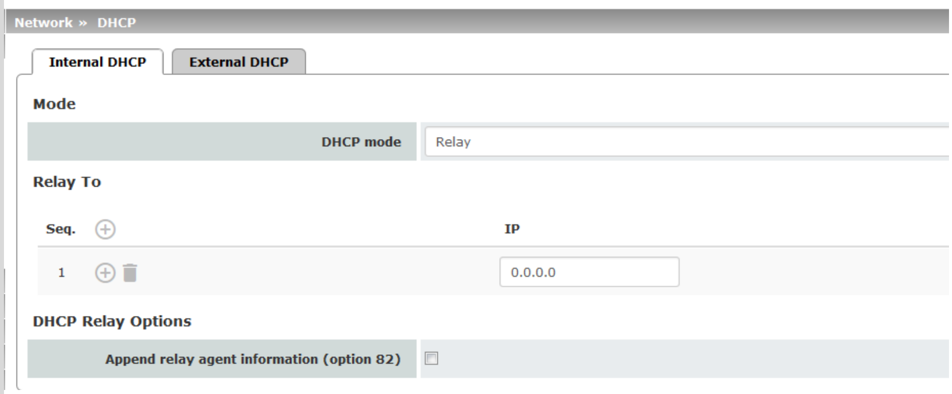
> Only one DHCP server should be used per subnetwork.

Current Leases

The current leases assigned by the DHCP server are displayed with MAC address, IP address, and expiration date (timeout).

DHCP mode: Relay

If DHCP mode is set to *Relay*, the corresponding setting options are displayed below as follows.



DHCP Relay Options

> In mGuard *Stealth* mode, *Relay* DHCP mode is not supported. If the mGuard is in *Stealth* mode and *Relay* DHCP mode is selected, this setting will be ignored. However, DHCP requests from the computer and the corresponding responses are forwarded due to the nature of *Stealth* mode.

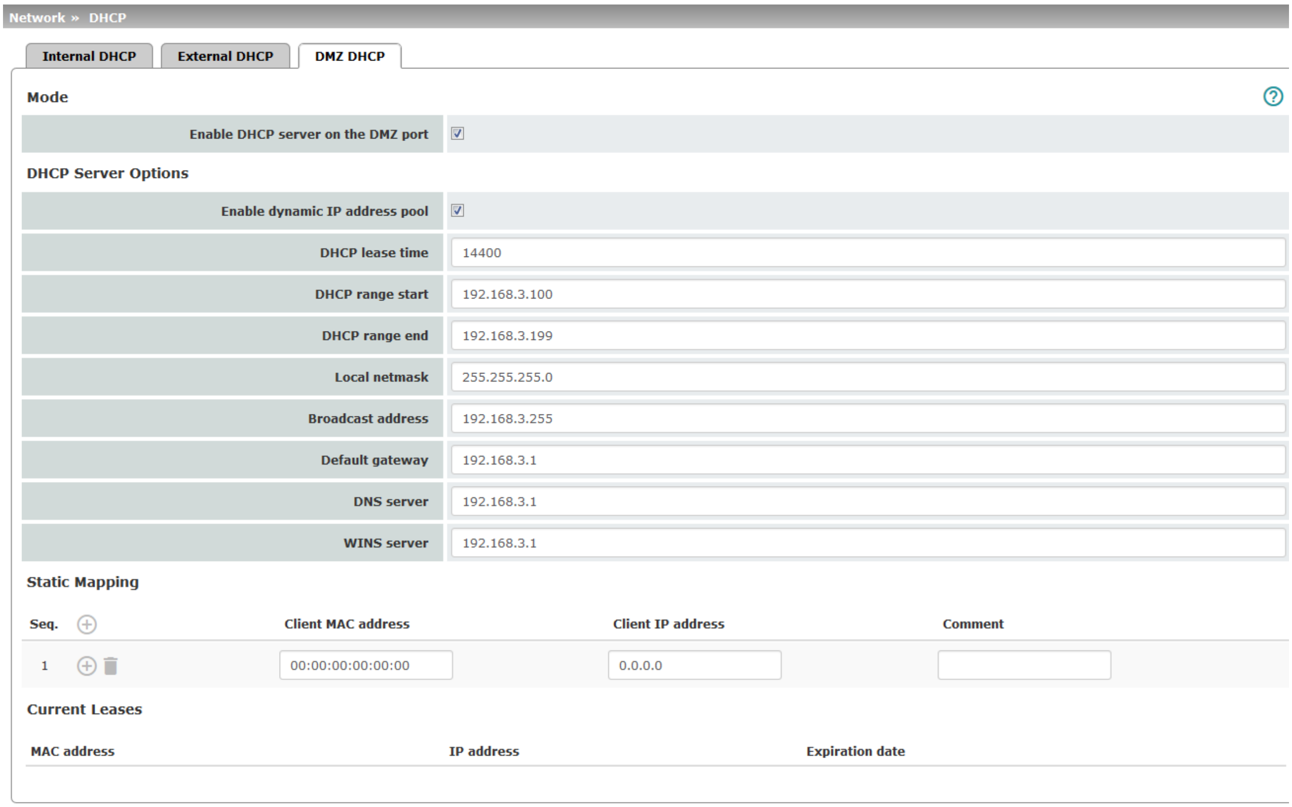
DHCP servers to relay to

A list of one or more DHCP servers to which DHCP requests should be forwarded.

Append relay agent information (option 82)

When forwarding, additional information for the DHCP servers to which information is being forwarded can be appended according to RFC 3046.

6.7.2 DMZ DHCP



From **mGuard firmware version 8.6.0**, the DHCP server functionality of the mGuard is expanded on its DMZ interface (DMZ port). The mGuard can automatically assign a network configuration to clients connected to the DMZ port via the DHCP protocol.

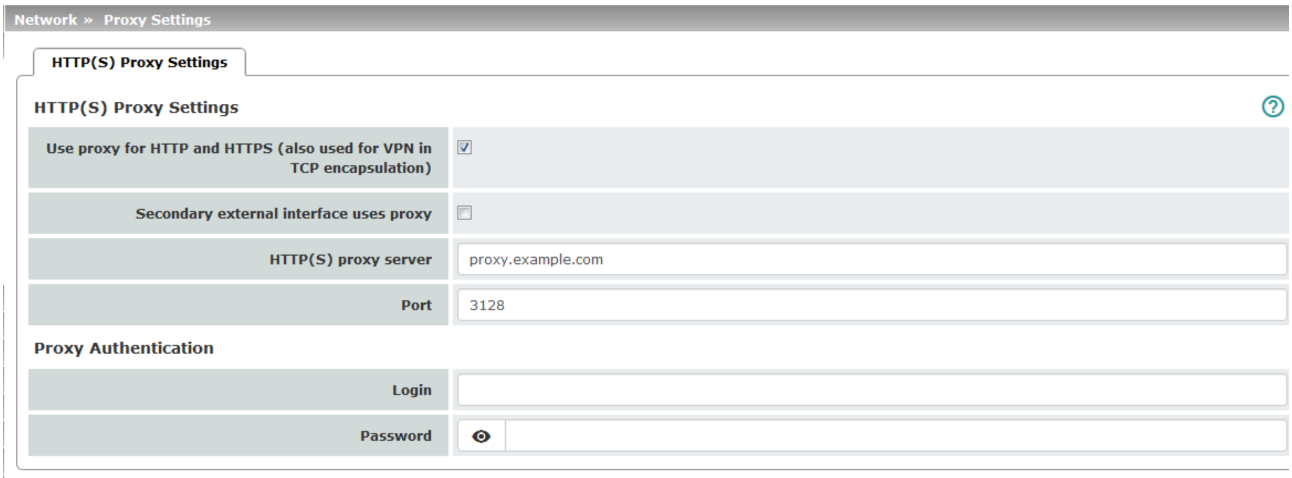
Network >> DHCP >> DMZ DHCP		
Mode	**Enable DHCP server on the DMZ port**	Enables the DHCP server on the DMZ interface. If the function is disabled, the mGuard does not answer any DHCP queries on the DMZ interface.
DHCP Server Options	**Enable dynamic IP address pool:**	When the function is activated, the IP address pool specified under *DHCP range start* and *DHCP range end* is used (see below). Deactivate the function if only static assignments should be made using the MAC addresses (see below).
	DHCP lease time	Time in seconds for which the network configuration assigned to the computer is valid. The client should renew its assigned configuration shortly before this time expires. Otherwise it may be assigned to other computers.
	DHCP range start (With enabled dynamic IP address pool)	The start of the address area from which the DHCP server of the mGuard should assign IP addresses to locally connected computers.

Network >> DHCP >> DMZ DHCP[...]		
	DHCP range end (With enabled dynamic IP address pool)	The end of the address area from which the DHCP server of the mGuard should assign IP addresses to locally connected computers.
	Local netmask	Specifies the netmask of the computers. Default: 255.255.255.0
	Broadcast address	Specifies the broadcast address of the computers.
	Default gateway	Specifies which IP address should be used by the computer as the default gateway. Usually this is the internal IP address of the mGuard.
	DNS server	Address of the server used by the computer to resolve host names in IP addresses via the Domain Name Service (DNS). If the DNS service of the mGuard is to be used, enter the internal IP address of the mGuard here.
	WINS server	Address of the server used by the computer to resolve host names in addresses via the Windows Internet Naming Service (WINS).
Static Mapping	**Client MAC address**	To find out the **MAC address** of your computer, proceed as follows: **Windows 95/98/ME**: • Start **winipcfg** in a DOS box. **Windows NT/2000/XP/**: • Start **ipconfig /all** in a command prompt. The MAC address is displayed as the “Physical Address”. **Linux**: • Call **/sbin/ifconfig** or **ip link show** in a shell. The following options are available: – Client/computer MAC address (without spaces or hyphens) – Client IP address
	Client IP address	The static IP address of the computer to be assigned to the MAC address. Static assignments take priority over the dynamic IP address pool. Static assignments must not overlap with the dynamic IP address pool. Do not use one IP address in multiple static assignments, otherwise this IP address will be assigned to multiple MAC addresses. Only one DHCP server should be used per subnetwork.

Network >> DHCP >> DMZ DHCP[...]	
Current Leases	The current leases assigned by the DHCP server are displayed with MAC address, IP address, and expiration date (timeout).

6.8 Network >> Proxy Settings

6.8.1 HTTP(S) Proxy Settings



A proxy server can be specified here for the following activities performed by the mGuard itself:

- CRL download
- Firmware update
- Regular configuration profile retrieval from a central location
- Restoring of licenses

Network >> Proxy Settings >> HTTP(S) Proxy Settings		
The http(s) proxy settings	**Use proxy for HTTP and HTTPS**	When the function is activated, connections that use the HTTP or HTTPS protocol are transmitted via a proxy server whose address and port should also be specified. Connections that are transmitted in encapsulated form using the **VPN in TCP encapsulation** function are also routed via the proxy server (see "TCP encapsulation" on page 317). If the proxy server uses the "Digest" authentication method, VPN connections initiated by the mGuard device that use TCP encapsulation or „Path Finder“ cannot be established. Use "Basic" authentication on the proxy server instead.
	Secondary external interface uses proxy	Only activate the function if the connection (HTTP or HTTPS) of the secondary external interface is also to be established via a proxy server (see "Secondary External Interface" on page 149).
	HTTP(S) proxy server	Host name or IP address of the proxy server.
	Port	Number of the port to be used, e.g., 3128.
Proxy Authentication	**Login**	User identifier (login) for proxy server login.
	Password	Password for proxy server login.

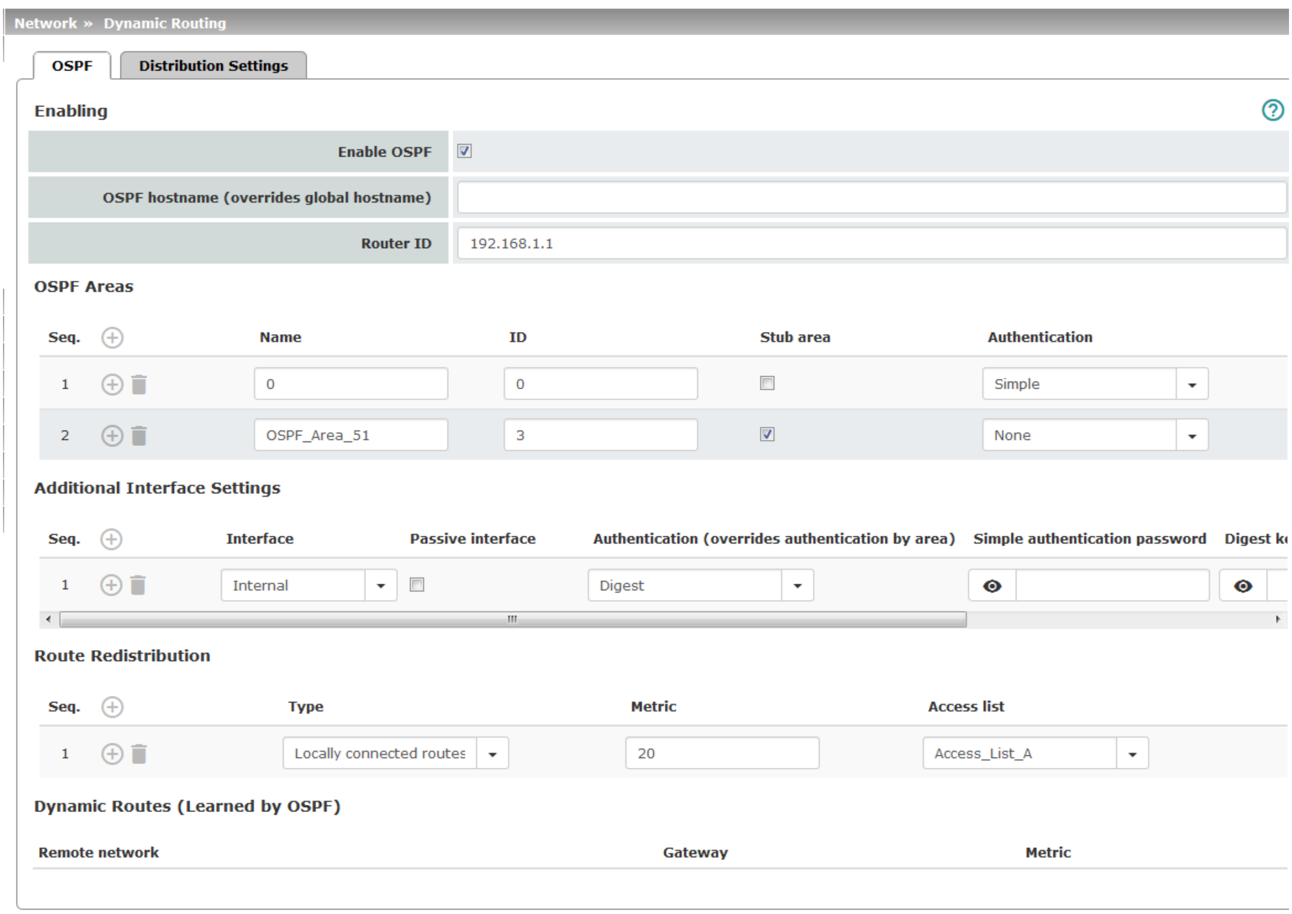
6.9 Network >> Dynamic Routing

In larger company networks, the use of dynamic routing protocols can make it easier for the network administrator to create and manage routes or even eliminate the need for this.

The **OSPF** (Open Shortest Path First) routing protocol allows participating routers to exchange and adapt the routes for transmitting IP packets in their autonomous network in real time (dynamically). The best route to each subnetwork is determined for all participating routers and entered in routing tables for the devices. Changes in the network topology are automatically sent to neighboring OSPF routers and eventually distributed by them to all participating OSPF routers.

> This menu is only available when the mGuard is in “Router” network mode. An OSPF area cannot be assigned to the WAN interface in **“DHCP” router mode**.

6.9.1 OSPF



OSPF can be configured for internal, external, and DMZ interfaces. If OSPF is to be used in IPsec connections, the OSPF packets (multicast) must be encapsulated in a GRE tunnel (unicast).

Multiple OSPF areas can be configured in order to distribute local routes and learn external routes. The status of all learned routes is displayed in a table.

Network >> Dynamic Routing >> OSPF		
Activation	**Enable OSPF**	When the function is deactivated (default): OSPF is disabled on the device. When the function is activated: dynamic routing using the OSPF protocol is enabled on the device. New routes are learned and distributed by neighboring OSPF routers. An OSPF area cannot be assigned to the WAN interface in **“DHCP” router mode**. New setting options under "Network >> Interfaces" , "IPsec VPN >> Connections" , and "Network >> GRE Tunnel" .
	OSPF hostname	If an **OSPF hostname** is assigned here, this is communicated to the participating OSPF routers instead of the global host name.
	Router ID	The **Router ID** in the form of an IP address must be unique within the autonomous system. It can otherwise be freely selected and typically corresponds to the IP address of the WAN or LAN interface of the mGuard.
OSPF Areas	The autonomous system is segmented using **OSPF Areas**. The routes between OSPF routers are exchanged within an area. The mGuard can belong to one or more OSPF areas. Distribution between neighboring areas is also possible using the “Transition Area” (see below).	
	Name	The **Name** can be freely selected (default: ID). An OSPF router is clearly identified by its ID.
	ID	In general, the **ID** can be freely selected. If an OSPF area is assigned the ID 0, it becomes the “**Transition Area**”. This area is used to exchange routing information between two neighboring areas and then distribute it.
	Stub area	If the OSPF area is a stub area, activate the function.
	Authentication	None / Simple / Digest Authentication of the mGuard within the OSPF area can be performed using the “Simple” or “Digest” method. The corresponding passwords and digest keys are assigned for the allocated interfaces (see "Additional Interface Settings").
Additional Interface Settings	**Interface**	Internal / External / DMZ Selects the interface for which the settings apply. If no settings are made here, the default settings apply (i.e., OSPF is enabled for the interface and the passwords are not assigned).
	Passive interface	Default: deactivated When the function is deactivated, OSPF routes are learned and distributed by the interface. When the function is activated, no routes are learned or distributed.

<table>
<tr><th colspan="3">Network >> Dynamic Routing >> OSPF</th></tr>
<tr><td></td><td>Authentication</td><td>None / Digest

If Digest is selected, “Digest” is always used for authentication at the selected interface – regardless of the authentication method already assigned to an OSPF area.

The authentication method (None / Simple / Digest) that has already been assigned to an OSPF area is therefore ignored and not used.</td></tr>
<tr><td></td><td>Simple authentication password</td><td>Password for authentication of the OSPF router (for “Simple” authentication method)</td></tr>
<tr><td></td><td>Digest key</td><td>Digest key for authentication of the OSPF router (for “Digest” authentication method)</td></tr>
<tr><td></td><td>Digest key ID</td><td>Digest key ID for authentication of the OSPF router (for “Digest” authentication method)

(1–255)</td></tr>
<tr><td>Route Redistribution</td><td colspan="2">Statically entered routes in the kernel routing table can also be distributed using OSPF. Rules can be created for locally connected networks and networks that are reachable via a gateway.

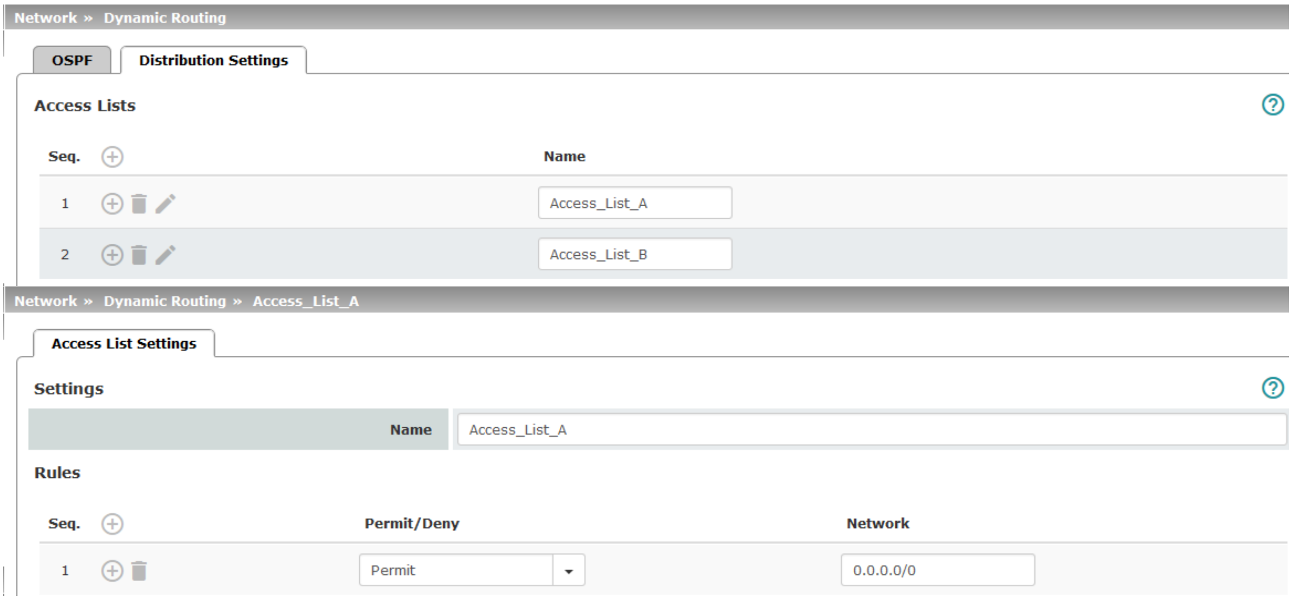
The networks whose routes are to be distributed using OSPF can be specified in “access lists” via the "Distribution Settings" .

By default, an access list is not selected for locally connected networks and networks reachable via a gateway. This means that all corresponding routes in the kernel routing table are distributed using OSPF if a rule and the OSPF function are enabled.</td></tr>
<tr><td></td><td>Type</td><td>Locally connected routes / Remotely connected routes

Locally connected routes: all local networks are distributed using OSPF, if OSPF is enabled. Distribution can be restricted by using access lists.

Remotely connected routes: all external networks are distributed using OSPF. External networks include, for example, static as well as IPsec, OpenVPN, and GRE remote networks. Distribution can be restricted by using access lists.</td></tr>
<tr><td></td><td>Metric</td><td>Metric used to distribute the routes. Unit representing the quality of a connection when a specific route is used (depends on the bandwidth, hop count, costs, and MTU).</td></tr>
<tr><td></td><td>Access list</td><td>Distributes the routes according to the selected access list (see "Distribution Settings"). If None is selected, all routes of the selected type are distributed.</td></tr>
<tr><td>Dynamic Routes (learned by OSPF)</td><td colspan="2">The status of all routes learned using OSPF is displayed.</td></tr>
<tr><td></td><td>Remote network</td><td>Dynamically learned remote network.</td></tr>
<tr><td></td><td>Gateway</td><td>Gateway to reach the remote network.</td></tr>
<tr><td></td><td>Metric</td><td>Metric for the learned route.</td></tr>
</table>

6.9.2 Distribution Settings



Dynamic routes are automatically distributed using the OSPF protocol. For statically entered routes in the kernel routing table, it must be specified whether they should also be distributed using OSPF.

> If a rule is selected for either the “Locally connected routes” or “Remotely connected routes” type, by default (Access List = None) all corresponding routes are distributed using OSPF if OSPF is enabled.

Rules can be created via Distribution Settings which determine the routes that are not learned dynamically that should be distributed using OSPF. These include:

– Locally configured networks (see "Network >> Interfaces" on page 127)
– Static routes entered as external, internal or DMZ networks (see "Network >> Interfaces" on page 127)
– Routes entered in the kernel routing table via OpenVPN (see "OpenVPN Client >> Connections" on page 365)
– Routes entered in the kernel routing table via the GRE tunnel configuration (see "Network >> GRE Tunnel" on page 225)

Network >> Dynamic Routing >> Distribution Settings >> Edit >> Access List Settings		
Settings	**Name**	The **Name** must be unique and must not be assigned more than once.
Rules	**Permit/Deny**	Lists the access list rules. These apply for routes that are not distributed dynamically using OSPF. **Permit** (standard)means that the route to the entered network is distributed using OSPF. **Deny** means that the route to the entered network is not distributed using OSPF.
	Network	**Network** whose distribution is permitted or denied by rules.

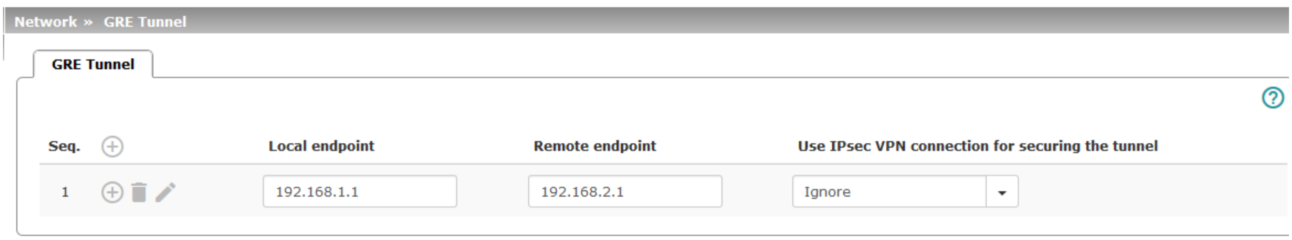
6.10 Network >> GRE Tunnel

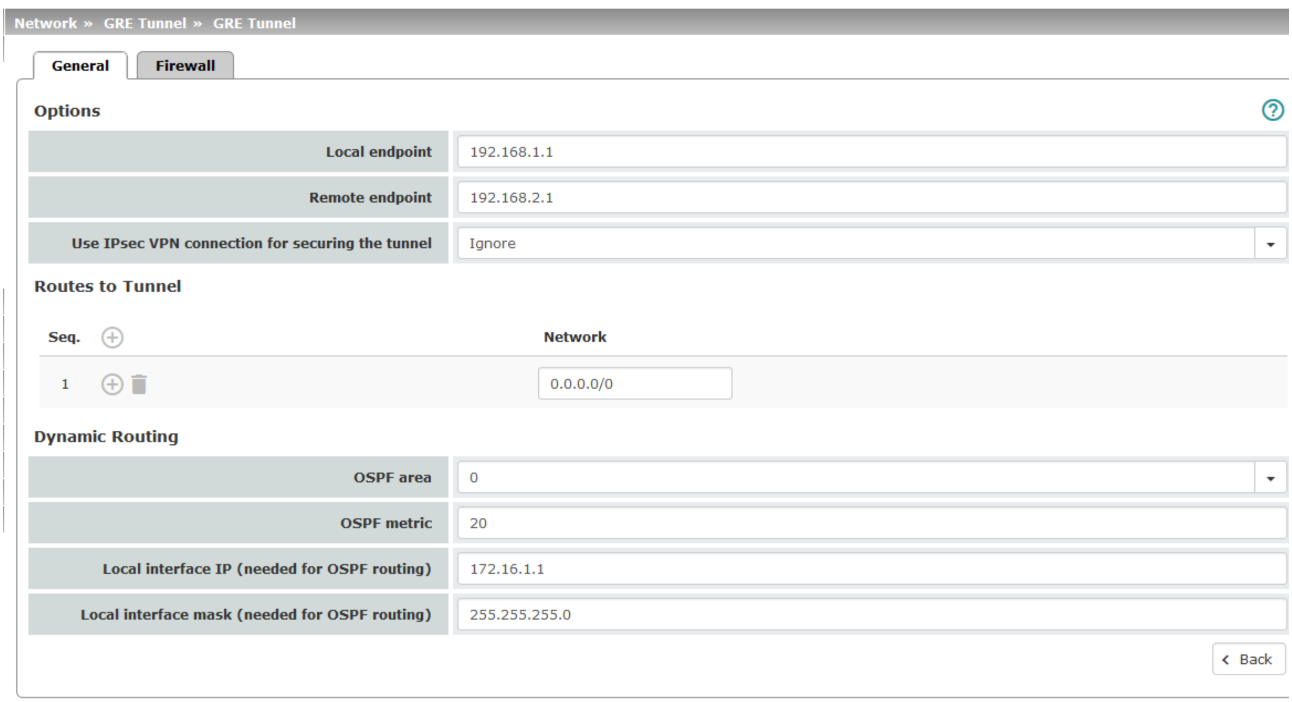
Generic Routing Encapsulation (GRE) is a network protocol that is used to encapsulate other protocols (including the OSPF routing protocol) and to transport them in a GRE tunnel via unicast IP connections. OSPF routes can also be learned and distributed via IPsec VPN connections.

To ensure that GRE packets are routed through a secure IPsec tunnel, a preconfigured IPsec connection can be selected for each GRE tunnel.

> The use of GRE tunnels via IPsec connections of the "**Transport**" connection type is not possible.

6.10.1 General

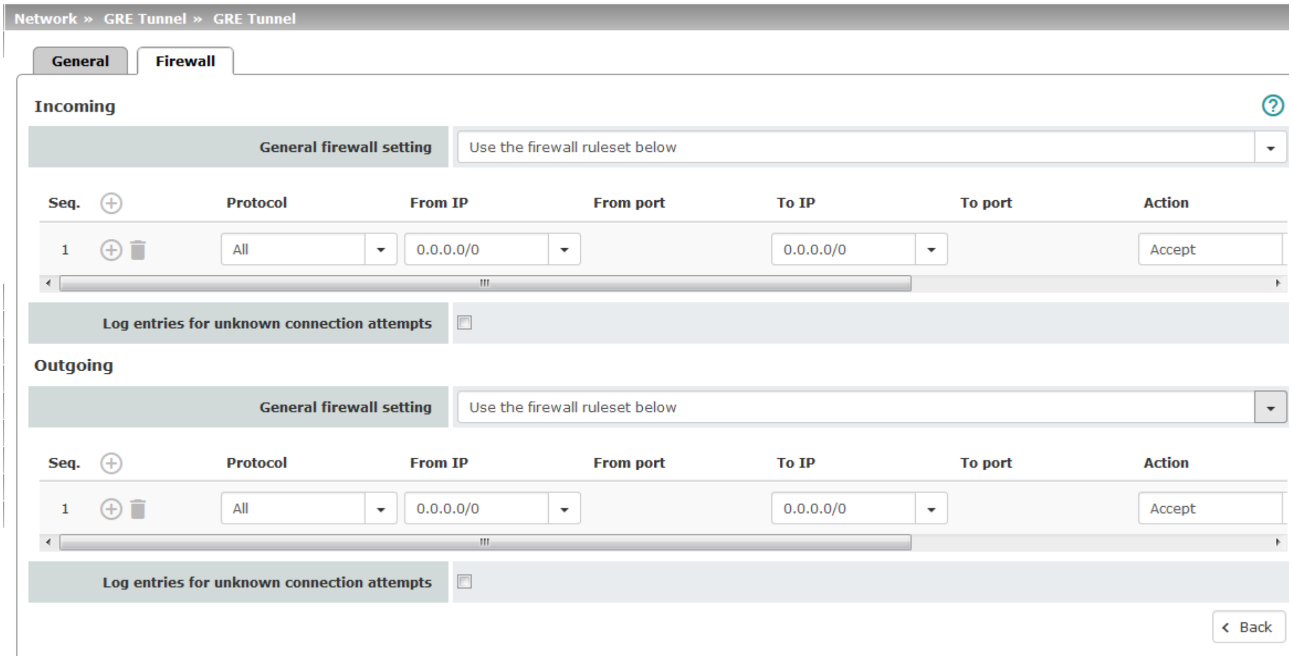




Network >> GRE Tunnel >> Edit >> General	
Options	**NOTE:** In order to route the GRE tunnel through an encrypted IPsec connection, its local and remote endpoints must be within the IPsec connection.

Network >> GRE Tunnel >> Edit >> General		
	Local endpoint	Local IP address from which the tunnel will be created. The IP address must already be configured under *"Network >> Interfaces"* for the mGuard itself.
	Remote endpoint	Remote IP address to which the tunnel will be created. The IP address must also be configured at the peer.
	Use IPsec VPN connection for securing the tunnel	For the selected IPsec connection, it is checked whether the GRE tunnel is routed through and therefore protected by this connection, i.e., whether both endpoints are in the IPsec networks (local and remote).
Routes to Tunnel	**Network**	All peer networks that are to be reached via the GRE tunnel in encapsulated form are entered here. Several routes can be configured for each GRE tunnel. **0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 26).
Dynamic Routing	**OSPF area**	Links the virtual GRE interface to an OSPF area (see "Network >> Dynamic Routing" on page 221).
	OSPF metric	Unit representing the quality of a connection through the GRE tunnel.
	Local interface IP	IP address of the virtual GRE interface (required in order to exchange routing information between OSPF routers). An IP address in the same network must be configured at the peer for the GRE interface.
	Local interface mask	Netmask of the virtual GRE interface.

6.10.2 Firewall



Incoming/Outgoing firewall

While the settings made in the Network Security menu only relate to non-VPN connections and non-GRE connections (see "Network Security menu" on page 257), the settings here only relate to the GRE connection defined on these tab pages.

If multiple GRE connections have been defined, you can restrict the outgoing or incoming access individually for each connection. Any attempts to bypass these restrictions can be logged.

> By default, the GRE firewall is set to allow all connections for the GRE connection.
>
> However, the extended firewall settings defined and explained above apply independently for each individual GRE connection (see "Network Security menu" on page 257, "Network Security >> Packet Filter" on page 257, and "Advanced" on page 278).

> If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored.

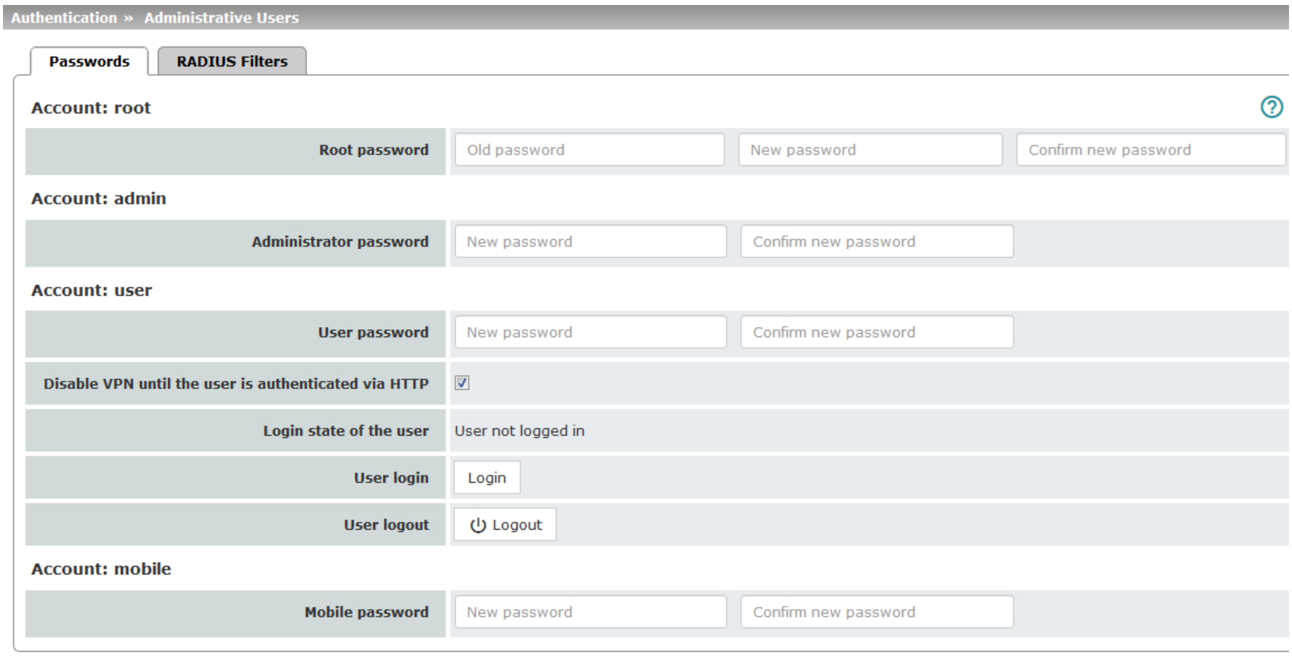
Network >> GRE Tunnel >> Edit >> Firewall		
Incoming	**General firewall setting**	**Accept all incoming connections**: the data packets of all incoming connections are allowed. **Drop all incoming connections**: the data packets of all incoming connections are discarded. **Accept Ping only:** the data packets of all incoming connections are discarded, except for ping packets (ICMP). **Use the firewall ruleset below**: displays further setting options.
	The following settings are only visible if “**Use the firewall ruleset below**” is set.	
	Protocol	**All** means TCP, UDP, ICMP, GRE, and other IP protocols.
	From IP / To IP	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 26). **Name of IP groups**, if defined. When a name is specified for an IP group, the host names, IP addresses, IP areas or networks saved under this name are taken into consideration (see "IP/Port Groups" on page 275). If host names are used in IP groups, the mGuard must be configured so that the host name of a DNS server can be resolved in an IP address. If a host name from an IP group cannot be resolved, this host will not be taken into consideration for the rule. Further entries in the IP group are not affected by this and are taken into consideration. The use of host names in IP groups is not possible on mGuard devices of the RS2000 series. **Incoming**: – From IP: IP address in the GRE tunnel – To IP: 1:1 NAT address or the actual address **Outgoing**: – From IP: 1:1 NAT address or the actual address – To IP: IP address in the GRE tunnel

Network >> GRE Tunnel >> Edit >> Firewall		
	From port / To port (Only for TCP and UDP protocols)	**any** refers to any port. **startport:endport** (e.g., 110:120) refers to a port range. Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110). **Name of port groups**, if defined. When a name is specified for a port group, the ports or port ranges saved under this name are taken into consideration (see "IP/Port Groups" on page 275).
	Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back and the sender is informed of their rejection. **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts. **Name of rule records**, if defined. When a name is specified for rule records, the firewall rules configured under this name take effect (see "Rule Records" on page 268). For security reasons, rule records that contain IP groups with host names should not be used in firewall rules which execute “Drop” or “Reject” as the action. The use of rule records is not possible on mGuard devices of the RS2000 series. **Name of Modbus TCP rule records**, if defined. When a Modbus TCP rule record is selected, the firewall rules configured under this rule record take effect (see "Modbus TCP" on page 284).
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – activate *Log* function – Should not be logged – deactivate *Log* function (default setting)
	Log entries for unknown connection attempts	When the function is activated, all connection attempts that are not covered by the rules defined above are logged.
Outgoing	The explanation provided under “Incoming” also applies to “Outgoing”.	

7 Authentication menu

7.1 Authentication >> Administrative Users

7.1.1 Passwords



Administrative Users refers to users who have the right (depending on their authorization level) to configure the mGuard (*root* and *administrator* authorization levels) or to use it (*user* authorization level).

Authentication >> Administrative Users >> Passwords		
	To log into the corresponding authorization level, the user must enter the password assigned to the relevant authorization level (*root*, *admin* or *user*). If you change passwords, you should then restart the mGuard to securely end existing sessions with passwords that are no longer valid.	
Account: root	**Root password**	Grants full rights to all parameters of the mGuard. Background: only this authorization level allows unlimited access to the mGuard file system. User name (cannot be modified): **root** Default root password: **root** • To change the root password, enter the old password in the *Old password* field, then the new password in the next two fields.

Authentication >> Administrative Users >> Passwords [...]		
Account: admin	**Administrator password**	Grants the rights required for the configuration options accessed via the web-based administrator interface. User name (cannot be modified): **admin** Default password: **mGuard**
Account: user	**User password**	There is no default user password. To set one, enter the desired password in both input fields.
	Disable VPN until the user is authenticated via HTTP	If a user password has been specified and activated, the user must always enter this password after an mGuard restart in order to **enable mGuard VPN connections** when attempting to access any HTTP URL. The function is deactivated by default. When the function is activated, VPN connections can only be used once a user has logged into the mGuard via HTTP. As long as authentication is required, all HTTP connections are redirected to the mGuard. Changes to this option only take effect after the next restart. To use this option, specify the user password in the corresponding input field.
	Login state of the user	Displays whether the user is logged on or off.
	User login	To log in the user, click on the **Login** button.
	User logout	To log out the user, click on the **Logout** button.
Account: mobile (Only TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G)	**Mobile password**	There is no default mobile password. To set one, enter the desired password in both input fields.

7.1.2 RADIUS Filters

Group names can be created here for administrative users whose password is checked using a RADIUS server when accessing the mGuard. Each of these groups can be assigned an administrative role.

> If you change passwords or make changes to the authentication process, you should then restart the mGuard to securely end existing sessions with certificates or passwords that are no longer valid.

Authentication >> Administrative Users >> RADIUS Filters

(This menu item is not included in the scope of functions for TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005 or FL MGUARD RS2000.)

The mGuard only checks passwords using RADIUS servers if you have activated RADIUS authentication:

– For shell access, see menu: *Management* >> *System Settings* >> *Shell Access*
– For web access, see menu: *Management* >> *Web Settings* >> *Access*

The RADIUS filters are searched consecutively. When the first match is found, access is granted with the corresponding role *(admin, netadmin, audit)*.

After a RADIUS server has checked and accepted a user's password, it sends the mGuard a list of filter IDs in its response.

These filter IDs are assigned to the user in a server database. They are used by the mGuard for assigning the group and therefore the authorization level as “admin”, “netadmin” or “audit”.

If authentication is successful, this is noted as part of the mGuard's logging process. Other user actions are logged here using the original name of the user. The log messages are forwarded to a remote server, provided a remote server has been approved by the mGuard.

The following actions are recorded:

– Login
– Logout
– Start of a firmware update
– Changes to the configuration
– Password changes for one of the predefined users *(root, admin, netadmin, audit, mobile, and user)*.

Authentication >> Administrative Users >> RADIUS Filters [...]		
RADIUS Filters for Administrative Access	**Group/Filter ID**	The group name may only be used once. Two lines must not have the same value. Responses from the RADIUS server with notification of successful authentication must have this group name in their filter ID attribute. Up to 50 characters are allowed (printable UTF-8 characters only) without spaces.
	Authorized for access as	Each group is assigned an administrative role. **admin:** administrator **netadmin**: administrator for the network **audit**: auditor/tester The *netadmin* and *audit* authorization levels relate to access rights with the mGuard device manager (FL MGUARD DM).

7.2 Authentication >> Firewall Users

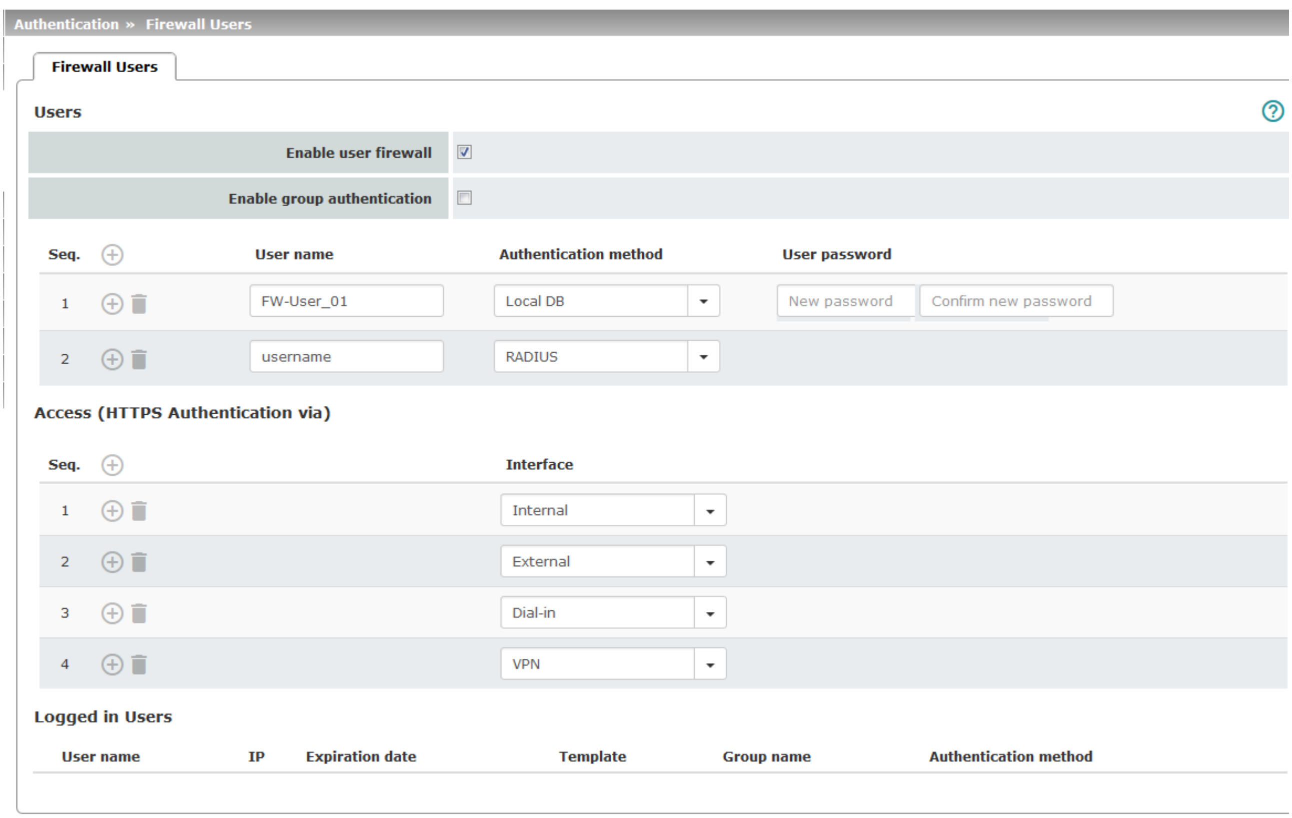
To prevent private surfing on the Internet, for example, every outgoing connection is blocked under *Network Security* >> *Packet Filter* >> *DMZ*. VPN is not affected by this.

Under *Network Security* >> *User Firewall*, different firewall rules can be defined for certain users, e.g., all outgoing connections are permitted. This user firewall rule takes effect as soon as the relevant firewall user(s) (to whom this user firewall rule applies) has (or have) logged in, see *"Network Security >> User Firewall" on page 291*.

7.2.1 Firewall Users

This menu is **not** available on the **FL MGUARD RS2000, TC MGUARD RS2000 3G, TC MGUARD RS2000 4G,** and **FL MGUARD RS2005**.

Concurrent administrative access via X.509 authentication and via login to the mGuard user firewall is not possible with the **“Safari” web browser**.



Authentication >> Firewall Users >> Firewall Users	
Users	Lists the firewall users by their assigned user identifier. Also specifies the authentication method.

Authentication >> Firewall Users >> Firewall Users [...]		
	Enable user firewall	Under the *Network Security* >> *User Firewall* menu item, firewall rules can be defined and assigned to specific firewall users. When the user firewall is activated, the firewall rules assigned to the listed users are applied as soon as the corresponding user logs in.
	Enable group authentication	When activated, the mGuard forwards login requests for unknown users to the RADIUS server. If successful, the response from the RADIUS server will contain a group name. The mGuard then enables user firewall templates containing this group name as the template user. The RADIUS server must be configured to deliver this group name in the “Access Accept” packet as a “Filter-ID=<group name>” attribute.
	User name	Name specified by the user during login.
	Authentication method	**Local DB**: when *Local DB* is selected, the password assigned to the user, and that the user must enter on login along with their *User name,* must be entered in the *User password* column. **RADIUS**: if *RADIUS* is selected, the user password can be stored on the RADIUS server. If you change passwords or make changes to authentication methods, you should then restart the mGuard to securely end existing sessions with certificate or passwords that are no longer valid.
	User password (Only if **Local DB** is selected as the authentication method.)	Assigned user password.

Authentication >> Firewall Users >> Firewall Users [...]		
Access (HTTPS Authentication via)	Specifies which mGuard interfaces can be used by firewall users to log into the mGuard. HTTPS remote access must also be enabled in the "*Management* >> *Web Settings*" menu, if access does not take place via the **Internal** interface. **NOTE: For authentication via an external interface, please consider the following**: If a firewall user can log in via an "unsecure" interface and the user leaves the session without logging out correctly, the login session may remain open and could be misused by another unauthorized person. An interface is "unsecure", for example, if a user logs in via the Internet from a location or a computer to which the IP address is assigned dynamically by the Internet service provider – this is usually the case for many Internet users. If such a connection is temporarily interrupted, e.g., because the user logged in is being assigned a different IP address, this user must log in again. However, the old login session under the old IP address remains open. This login session could then be used by an intruder, who uses this "old" IP address of the authorized user and accesses the mGuard using this sender address. The same thing could also occur if an (authorized) firewall user forgets to log out at the end of a session. This hazard of logging in via an "unsecure interface" is not completely eliminated, but the time is limited by setting the configured timeout for the user firewall template used. See "Timeout type" on page 293.	
	Interface	**Internal / External / External 2 / DMZ[1] / VPN / Dial-in[2]** Specifies which mGuard interfaces can be used by firewall users to log into the mGuard. For the interface selected, web access via HTTPS must be enabled: **"Management >> Web Settings" menu**, *Access* tab (see "Access" on page 71). In *Stealth* network mode, both the **Internal** and **External** interfaces must be enabled so that firewall users can log into the mGuard. (Two rows must be entered in the table for this.)
Logged in Users	When the user firewall is activated, the status of logged in firewall users is displayed here. Selected users can be logged off by clicking on the ⊖ icon.	

1 *DMZ* is only for devices with a DMZ interface.

2 *External 2* and *Dial-in* are only for devices with a serial interface (see "Network >> Interfaces" on page 127).

7.3 Authentication >> RADIUS

A RADIUS server is a central authentication server used by devices and services to check user passwords. The password is not known to these devices and services. Only one or a number of RADIUS servers know the password.

The RADIUS server also provides the device or service that a user wishes to access with further information about the user, e.g., the group to which the user belongs. In this way, all user settings can be managed centrally.

In order to activate RADIUS authentication, **Yes** must be set under *Authentication >> Firewall Users* (*Enable group authentication* sub-item) and *RADIUS* selected as the *Authentication method.*

A list of RADIUS servers used by the mGuard is generated under Authentication >> RADIUS Servers. This list is also used when RADIUS authentication is activated for administrative access (SSH/HTTPS).

When RADIUS authentication is active, the login attempt of a non-predefined user (not: *root, admin, netadmin, audit* or *user*) is forwarded to all the RADIUS servers listed here. The first response received by the mGuard from one of the RADIUS servers determines whether or not the authentication attempt is successful.

> If you change passwords or make changes to the authentication process, you should then restart the mGuard to securely end existing sessions with certificates or passwords that are no longer valid.

Authentication >> RADIUS		
RADIUS Servers (This menu item is not included in the scope of functions for TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005 or FL MGUARD RS2000.)	**RADIUS timeout**	Specifies the time (in seconds) the mGuard waits for a response from the RADIUS server. Default: 3 seconds.
	RADIUS retries	Specifies how many times requests to the RADIUS server are repeated after the RADIUS timeout time has elapsed. Default: 3.
	RADIUS NAS identifier	A NAS ID (NAS identifier) is sent with every RADIUS request, except when the field remains empty. All common characters on the keyboard can be used as the NAS ID. The NAS ID is a RADIUS attribute that can be used by the client to be identified by the RADIUS server. The NAS ID can be used instead of an IP address to identify the client. It must be unique within the range of the RADIUS server.

Authentication >> RADIUS [...]		
	Server	Name of the RADIUS server or its IP address. We recommend entering IP addresses as servers instead of names, where possible. Otherwise, the mGuard must first resolve the names before it can send authentication queries to the RADIUS server. This takes time when logging in. Also, it may not always be possible to perform authentication if name resolution fails, e.g., because the DNS is not available or the name was deleted from the DNS.
	Via VPN	The RADIUS server's request is – **where possible** – carried out via a VPN tunnel (IPsec VPN or OpenVPN). **Prerequisite**: A suitable VPN tunnel is available. If no suitable VPN tunnel is available, traffic is always sent **unencrypted via the default gateway**. A suitable VPN tunnel is available if the remote peer belongs to the remote network of a configured VPN tunnel and the mGuard has an internal IP address that belongs to the local network of the same VPN tunnel. **Please note:** **For IPsec VPN connections**, the "Via VPN" function must be activated so that the traffic is routed through a suitable IPsec VPN tunnel. **For OpenVPN connections**, traffic is always routed via a suitable OpenVPN tunnel even if the function is deactivated.
	When the **Via VPN** function is activated, the mGuard supports queries from a RADIUS server through its VPN connection. This happens automatically whenever the RADIUS server belongs to the remote network of a configured VPN tunnel and the mGuard has an internal IP address belonging to the local network of the same VPN tunnel. This makes the authentication query dependent on the availability of a VPN tunnel. During configuration, ensure that the failure of a single VPN tunnel does not prevent administrative access to the mGuard.	
	Port	The port number used by the RADIUS server.

Authentication >> RADIUS [...]		
	Secret	RADIUS server password (secret) This password must be the same as on the mGuard. The mGuard uses this password to exchange messages with the RADIUS server and to encrypt the user password. The RADIUS server password is not transmitted in the network. The password is important for security since the mGuard can be rendered vulnerable to attack at this point if passwords are too weak. We recommend a password with at least 32 characters and several special characters. It must be changed on a regular basis. If the RADIUS secret is discovered, an attacker can read the user password for the RADIUS authentication queries. An attacker can also falsify RADIUS responses and gain access to the mGuard if they know the user names. These user names are transmitted as plain text with the RADIUS request. The attacker can thus simulate RADIUS queries and thereby find out user names and the corresponding passwords. Administrative access to the mGuard should remain possible while the RADIUS server password is being changed. Proceed as follows to ensure this: • Set up the RADIUS server for the mGuard a second time with a new password. • Also set this new password on the RADIUS server. • On the mGuard, delete the line containing the old password.

7.4 Authentication >> Certificates

Authentication is a fundamental element of secure communication. The X.509 authentication method relies on certificates to ensure that the “correct” partners communicate with each other and that no “incorrect” partner is involved in communication. An “incorrect” communication partner is one who falsely identifies themselves as someone they are not (see glossary under "X.509 certificate" on page 455).

Certificate

A certificate is used as proof of the identity of the certificate owner. The relevant authorizing body in this case is the CA (certificate authority). The digital signature on the certificate is provided by the CA. By providing this signature, the CA confirms that the authorized certificate owner possesses a private key that corresponds to the public key in the certificate.

The name of the certificate issuer appears under **Issuer** on the certificate, while the name of the certificate owner appears under *Subject*.

Self-signed certificates

A self-signed certificate is one that is signed by the certificate owner and not by a CA. In self-signed certificates, the name of the certificate owner appears under both **Issuer** and *Subject*.

Self-signed certificates are used if communication partners want to or must use the X.509 authentication method without having or using an official certificate. This type of authentication should only be used between communication partners that know and trust each other. Otherwise, from a security point of view, such certificates are as worthless as, for example, a home-made passport without the official stamp.

Certificates are shown to all communication partners (users or machines) during the connection process, providing the X.509 authentication method is used. In terms of the mGuard, this could apply to the following applications:

– Authentication of communication partners when establishing VPN connections using IPsec (see "IPsec VPN >> Connections" on page 322, "Authentication" on page 344).
– Authentication of communication partners when establishing VPN connections using OpenVPN (see "OpenVPN Client >> Connections" on page 365, "Authentication" on page 372).
– Management of the mGuard via SSH (shell access) (see "Management >> System Settings >> Host" on page 43, "Shell Access" on page 53).
– Management of the mGuard via HTTPS (see "Management >> Web Settings" on page 70, "Access" on page 71).

Certificate, machine certificate

Certificates can be used to identify (authenticate) oneself to others. The certificate used by the mGuard to identify itself to others shall be referred to as the “machine certificate” here, in line with Microsoft Windows terminology.

A “certificate”, “certificate specific to an individual” or “user certificate showing a person” is one used by operators to authenticate themselves to peers (e.g., an operator attempting to access the mGuard via HTTPS and a web browser for the purpose of remote configuration). A certificate specific to an individual can also be saved on a chip card and then inserted by its owner in the card reader of their computer when prompted by a web browser during connection establishment, for example.

Remote certificate

A certificate is thus used by its owner (person or machine) as a form of ID in order to verify that they really are the individual they identify themselves as. As there are at least two communication partners, the process takes place alternately: partner A shows their certificate to their peer, partner B; partner B then shows their certificate to their peer, partner A.

Provision is made for the following so that A can accept the certificate shown by B, i.e., the certificate of their peer (thus allowing communication with B): A has previously received a copy of the certificate from B (e.g., by data carrier or e-mail) which B will use to identify itself to A. A can then verify that the certificate shown by B actually belongs to B by comparing it with this copy. With regard to the mGuard interface, the certificate copy given here by partner B to A is an example of a *remote certificate*.

For reciprocal authentication to take place, both partners must thus provide the other with a copy of their certificate in advance in order to identify themselves. A installs the copy of the certificate from B as its remote certificate. B then installs the copy of the certificate from A as its remote certificate.

Never provide the PKCS#12 file (file name extension: *.p12) as a copy of the certificate to the peer in order to use X.509 authentication for communication at a later time. The PKCS#12 file also contains the private key that must be kept secret and must not be given to a third party (see "Creation of certificates" on page 242).

To create a copy of a machine certificate imported in the mGuard, proceed as follows:

- On the “Machine Certificates” tab, click on the **Current Certificate File** button next to the *Download Certificate* row for the relevant machine certificate (see "Machine Certificates" on page 248).

CA certificates

The certificate shown by a peer can also be checked by the mGuard in a different way, i.e., not by consulting the locally installed remote certificate on the mGuard. To check the authenticity of possible peers in accordance with X.509, the method described below of consulting CA certificates can be used instead or as an additional measure, depending on the application.

CA certificates provide a way of checking whether the certificate shown by the peer is really signed by the CA specified in the peer's certificate.

A CA certificate is available as a file from the relevant CA (file name extension: *.cer, *.pem or *.crt). For example, this file may be available to download from the website of the relevant CA.

The mGuard can then check if the certificate shown by the peer is authentic using the CA certificates loaded on the mGuard. However, this requires all CA certificates to be made available to the mGuard in order to form a chain with the certificate shown by the peer. In addition to the CA certificate from the CA whose signature appears on the certificate shown by the peer to be checked, this also includes the CA certificate of the superordinate CA, and so forth, up to the root certificate (see glossary under "CA certificate" on page 449).

Authentication using CA certificates enables the number of possible peers to be extended without any increased management effort because it is not compulsory to install a remote certificate for each possible peer.

Creation of certificates

To create a certificate, a *private key* and the corresponding *public key* are required. Programs are available so that any user can create these keys. Similarly, a corresponding certificate with the corresponding *public key* can also be created, resulting in a self-signed certificate. (Additional information about self-creation can be downloaded from phoenixcontact.net/products. It is available in the download area in an application note entitled “How to obtain X.509 certificates”.)

A corresponding certificate signed by a CA must be requested from the CA.

In order for the private key to be imported into the mGuard with the corresponding certificate, these components must be packed into a PKCS#12 file (file name extension: *.p12).

Authentication methods

The mGuard uses two methods of X.509 authentication that are fundamentally different.

– The authentication of a peer is carried out based on the certificate and remote certificate. In this case, the remote certificate that is to be consulted must be specified for each individual connection, e.g., for VPN connections.
– The mGuard consults the CA certificates provided to check whether the certificate shown by the peer is authentic. This requires all CA certificates to be made available to the mGuard in order to form a chain with the certificate shown by the peer through to the root certificate.

“Available” means that the relevant CA certificates must be installed on the mGuard (see "CA Certificates" on page 250) and must also be referenced during the configuration of the relevant application (SSH, HTTPS, and VPN).

Whether both methods are used alternatively or in combination varies depending on the application (VPN, SSH, and HTTPS).

> If you change passwords or make changes to the authentication process, you should then restart the mGuard to securely end existing sessions with certificates or passwords that are no longer valid.

Restrictions using the “Safari” web browser

> Please note that during administrative access to the mGuard via an X.509 certificate using the **“Safari” web browser** all sub-CA certificates must be installed in the web browser's Trust Store.

Authentication for SSH

The peer shows the following:	Certificate (specific to individual), **signed by CA**	Certificate (specific to individual), **self-signed**
The mGuard authenticates the peer using:	⇕	⇕
	All CA certificates that form the chain to the root CA certificate together with the certificate shown by the peer PLUS (if required) Remote certificates, **if** used as a filter[1]	Remote certificate

[1] (See "Management >> System Settings" on page 43, "Shell Access" on page 53)

Authentication for HTTPS

The peer shows the following:	Certificate (specific to individual), **signed by CA**[1]	Certificate (specific to individual), **self-signed**
The mGuard authenticates the peer using:	⇕	⇕
	All CA certificates that form the chain to the root CA certificate together with the certificate shown by the peer PLUS (if required) Remote certificates, **if** used as a filter[2]	Remote certificate

[1] The peer can additionally provide sub-CA certificates. In this case, the mGuard can form the set union for creating the chain from the CA certificates provided and the self-configured CA certificates. The corresponding root CA certificate must always be available on the mGuard.

[2] (See "Management >> Web Settings" on page 70, "Access" on page 71)

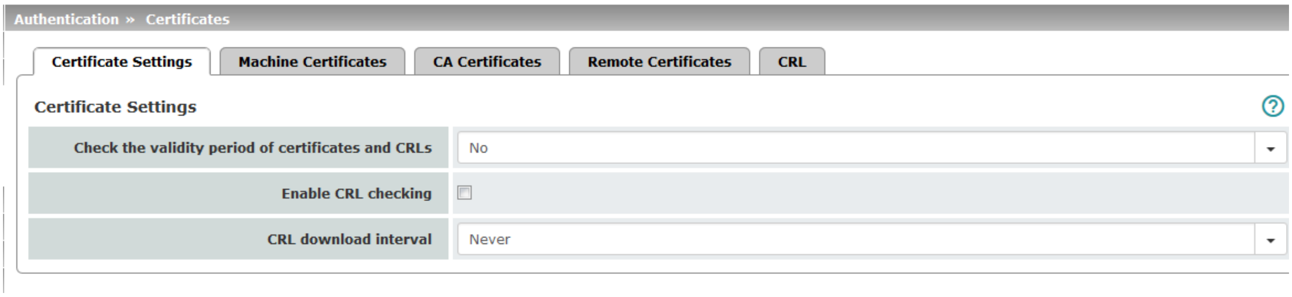
Authentication for VPN

The peer shows the following:	Machine certificate, **signed by CA**	Machine certificate, **self-signed**
The mGuard authenticates the peer using:	⇕	⇕
	Remote certificate Or all CA certificates that form the chain to the root CA certificate together with the certificate shown by the peer	Remote certificate

NOTE: It is not sufficient to simply install the certificates to be used on the mGuard under *Authentication* >> *Certificates*. In addition, the certificate from the pool of certificates imported into the mGuard that is to be used must be referenced in the relevant applications (VPN, SSH, HTTPS).

The remote certificate for authentication of a VPN connection (or the tunnels of a VPN connection) is installed in the *IPsec VPN* >> *Connections* menu.

7.4.1 Certificate Settings



Authentication >> Certificates >> Certificate Settings

Certificate Settings

The settings made here relate to all certificates and certificate chains that are to be checked by the mGuard.

This generally excludes the following:

– Self-signed certificates from peers
– All remote certificates for VPN

Check the validity period of certificates and CRLs

Always

The validity period is always observed.

No

The validity period specified in certificates and CRLs is ignored by the mGuard.

Wait for synchronization of the system time

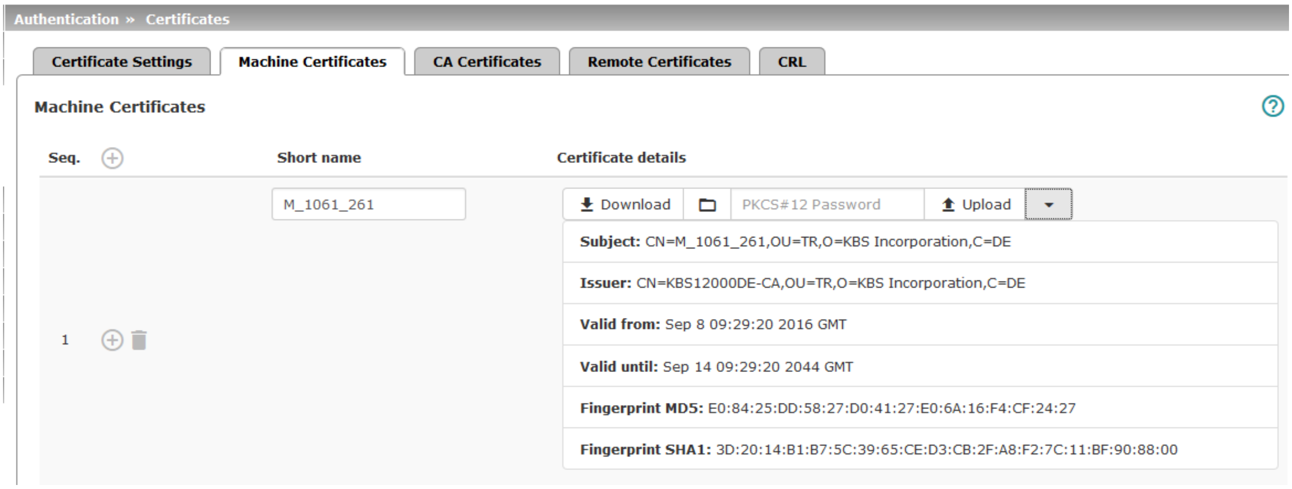
The validity period specified in certificates and CRLs is only observed by the mGuard if the current date and time are known to the mGuard:

– By means of the built-in clock (for *TC MGUARD RS4000/RS2000 3G*, TC MGUARD RS4000/RS2000 4G, *FL MGUARD RS2005, FL MGUARD RS4000/RS2000,* FL MGUARD GT/GT, *mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD RS*, *mGuard delta (Innominate)*, *FL MGUARD SMART2*) or
– By synchronizing the system clock (see "Time and Date" on page 46)

Until this point, all certificates to be checked are considered invalid for security reasons.

Authentication >> Certificates >> Certificate Settings [...]		
	Enable CRL checking	When **CRL checking is enabled**, the mGuard consults the CRL (certificate revocation list) and checks whether or not the certificates that are available to the mGuard are blocked. CRLs are issued by the CAs and contain the serial numbers of blocked certificates, e.g., certificates that have been reported stolen. On the **CRL** tab (see "CRL" on page 254), specify the origin of the revocation lists for the mGuard. When CRL checking is enabled, a CRL must be configured for each **issuer** of certificates on the mGuard. Missing CRLs result in certificates being considered invalid. Revocation lists are verified by the mGuard using an appropriate CA certificate. Therefore, all CA certificates that belong to a revocation list (all sub-CA certificates and the root certificate) must be imported on the mGuard. If the validity of a revocation list cannot be proven, it is ignored by the mGuard. If the use of revocation lists is activated together with the consideration of validity periods, revocation lists are ignored if (based on the system time) their validity has expired or has not yet started. After uploading a revocation list, up to 10 minutes can pass before VPN connections that use certificates for authentication are established.
	CRL download interval	If *CRL checking* is enabled (see above), select the time period in which the revocation lists should be downloaded and applied. On the **CRL** tab (see "CRL" on page 254), specify the origin of the revocation lists for the mGuard. If CRL checking is enabled, but CRL download is set to **Never**, the CRL must be manually loaded on the mGuard so that CRL checking can be performed.

7.4.2 Machine Certificates



The mGuard authenticates itself to the peer using a machine certificate loaded on the mGuard. The machine certificate acts as an ID card for the mGuard, which it shows to the relevant peer.

For a more detailed explanation, see "Authentication >> Certificates" on page 241.

By importing a PKCS#12 file, the mGuard is provided with a private key and the corresponding machine certificate. Multiple PKCS#12 files can be loaded on the mGuard, enabling the mGuard to show the desired self-signed or CA-signed machine certificate to the peer for various connections.

In order to use the machine certificate installed at this point, it must be referenced **additionally** during the configuration of applications (SSH, VPN) so that it can be used for the relevant connection or remote access type.

Example of imported machine certificates (see above).

Authentication >> Certificates >> Machine Certificates	
Machine Certificates	Shows the currently imported X.509 certificates that the mGuard uses to authenticate itself to peers, e.g., other VPN gateways.

To import a (new) certificate, proceed as follows:

Importing a new machine certificate

Requirement:

The PKCS#12 file (file name extension: *.p12 or *.pfx) is saved on the connected computer.

Proceed as follows:

- Click on the **No file selected** icon to select the file.
- In the ***Password*** field, enter the password used to protect the private key of the PKCS#12 file.
- Click on the **Upload** icon.
  Once imported, you can view the details of the certificate by clicking on the **Details** button.
- Save the imported certificate by clicking on the **Save** icon.

Short name

When importing a machine certificate, the CN attribute from the certificate subject field is suggested as the short name here (providing the *Short name* field is empty at this point). This name can be adopted or another name can be chosen.

- A name must be assigned, whether it is the suggested one or another. Names must be unique and must not be assigned more than once.

Using the short name

During the configuration of:

- SSH (*Management* >> *System Settings, Shell Access* menu)
- HTTPS (*Management* >> *Web Settings, Access* menu)
- VPN connections (*IPsec VPN* >> *Connections* menu)

the certificates imported on the mGuard are provided in a selection list.

The certificates are displayed under the short name specified for each individual certificate on this page.

For this reason, name assignment is mandatory.

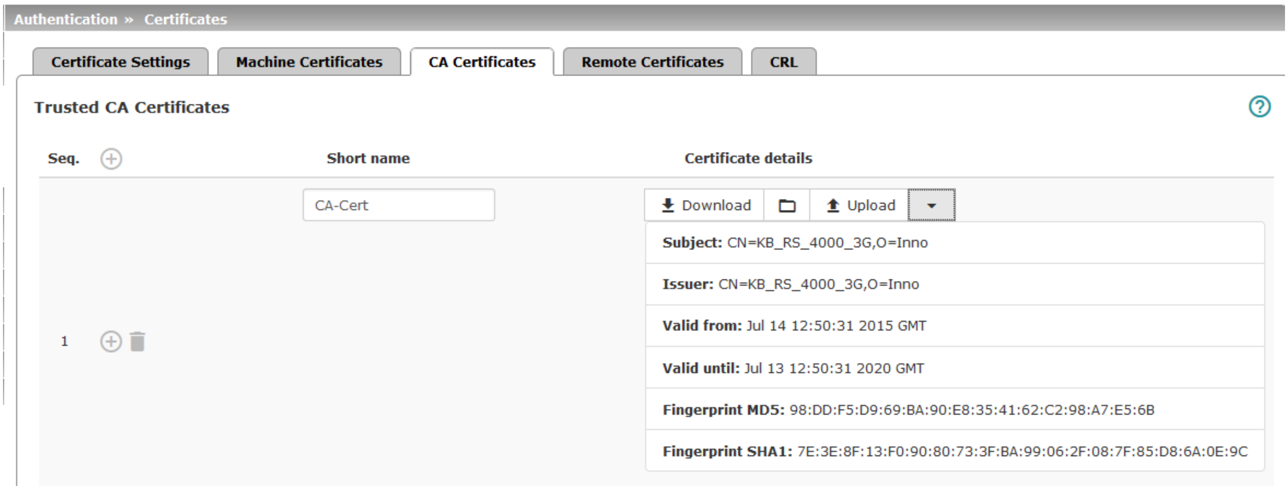
Creating and downloading a certificate copy

You can create and download a copy of the imported machine certificate (e.g., for the peer in order to authenticate the mGuard). This copy does not contain the private key and therefore does not pose a risk.

To do this, proceed as follows:

- Click on the **Download** icon in the row for the relevant machine certificate.
- Follow the instructions in the dialog boxes that are displayed.

7.4.3 CA Certificates



CA certificates are certificates issued by a certification authority (CA). CA certificates are used to check whether the certificates shown by peers are authentic.

The checking process is as follows: the certificate issuer (CA) is specified as the issuer in the certificate transmitted by the peer. These details can be verified using the local CA certificate from the same issuer. For a more detailed explanation, see "Authentication >> Certificates" on page 241.

Example of imported CA certificates (see above).

Authentication >> Certificates >> CA Certificates	
Trusted CA Certificates	**Displays the current imported CA certificates.**

To import a (new) certificate, proceed as follows:

Importing a CA certificate

The file (file name extension: *.cer, *.pem or *.crt) is saved on the connected computer.

Proceed as follows:

- Click on the **No file selected** icon to select the file.
- Click on the **Upload** icon.
  Once imported, you can view the details of the certificate by clicking on the **Details** button.
- Save the imported certificate by clicking on the **Save** icon.

Short name

When importing a CA certificate, the CN attribute from the certificate subject field is suggested as the short name here (providing the Short name field is empty at this point). This name can be adopted or another name can be chosen.

- You must assign a name. The name must be unique.

Using the short name

During the configuration of:

– SSH (*Management >> System Settings, Shell Access* menu)
– HTTPS (*Management >> Web Settings, Access* menu)
– VPN connections (*IPsec VPN >> Connections* menu)

the certificates imported on the mGuard are provided in a selection list. The certificates are displayed under the short name specified for each certificate in this selection list. Name assignment is mandatory.

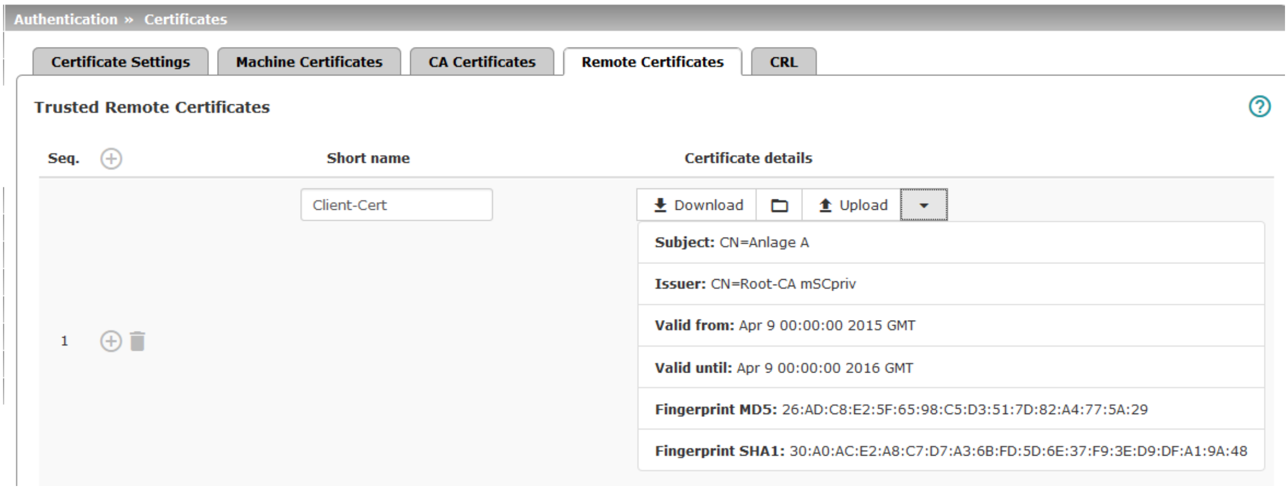
Creating and downloading a certificate copy

A copy can be created from the imported CA certificate and downloaded.

To do this, proceed as follows:

- Click on the **Download** icon in the row for the relevant CA certificate.
- Follow the instructions in the dialog boxes that are displayed.

7.4.4 Remote Certificates



A remote certificate is a copy of the certificate that is used by a peer to authenticate itself to the mGuard.

Remote certificates are files (file name extension: *.cer, *.pem or *.crt) received from the operators of possible peers by trustworthy means. You load these files on the mGuard so that reciprocal authentication can take place. The remote certificates of several possible peers can be loaded.

The remote certificate for authentication of a VPN connection (or the tunnels of a VPN connection) is installed in the *IPsec VPN* >> *Connections* menu.

For a more detailed explanation, see "Authentication >> Certificates" on page 241.

Example of imported remote certificates (see above)

Authentication >> Certificates >> Remote Certificates	
Trusted Remote Certificates	Displays the current imported remote certificates.

Importing a new certificate

Requirement:

The file (file name extension: *.cer, *.pem or *.crt) is saved on the connected computer.

Proceed as follows:

- Click on the **No file selected** icon to select the file.
- Click on the **Upload** icon.
  Once imported, you can view the details of the certificate by clicking on the **Details** button.
- Save the imported certificate by clicking on the **Save** icon.

Short name

When importing a remote certificate, the CN attribute from the certificate subject field is suggested as the short name here (providing the *Short name* field is empty at this point). This name can be adopted or another name can be chosen.

- A name must be assigned, whether it is the suggested one or another. Names must be unique and must not be assigned more than once.

Using the short name

During the configuration of:

– SSH (*Management* >> *System Settings, Shell Access* menu)
– HTTPS (*Management* >> *Web Settings, Access* menu)

the certificates imported on the mGuard are provided in a selection list. The certificates are displayed under the short name specified for each certificate in this selection list. Name assignment is mandatory.

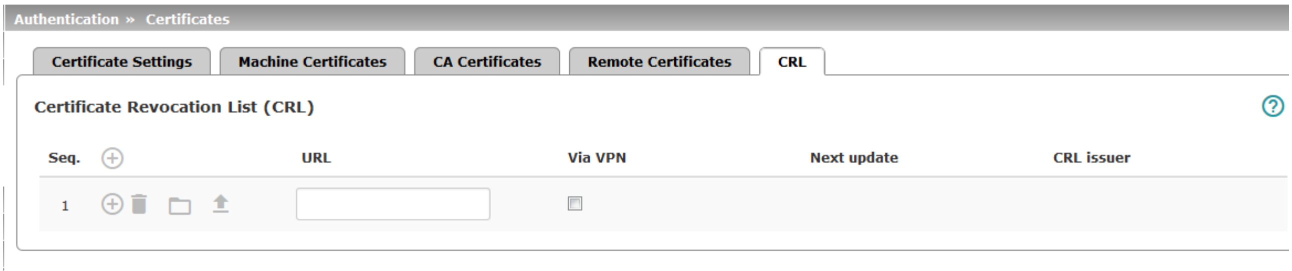
Creating and downloading a certificate copy

A copy can be created from the imported remote certificate and downloaded.

To do this, proceed as follows:

- Click on the **Download** icon in the row for the relevant remote certificate.
- Follow the instructions in the dialog boxes that are displayed.

7.4.5 CRL



Authentication >> Certificates >> CRL		
Certificate Revocation List (CRL)	CRL stands for certificate revocation list. The CRL is a list containing serial numbers of blocked certificates. This page is used for the configuration of sites from which the mGuard should download CRLs in order to use them. Certificates are only checked for revocations if the **Enable CRL checking** function has been activated (see "Certificate Settings" on page 246). A CRL with the same **issuer** name must be present for each **issuer** name specified in the certificates to be checked. If such a CRL is not present and CRL checking is enabled, the certificate is considered invalid. After uploading a revocation list, up to 10 minutes can pass before VPN connections that use certificates for authentication are established.	
	URL	Specify the URL of the CA where CRL downloads are obtained if the CRL should be downloaded on a regular basis, as defined under **CRL download interval** on the *Certificate Settings* tab (see "Certificate Settings" on page 246).

Authentication >> Certificates >> CRL		
	Via VPN	The CRL download server's (URL) request is – **where possible** – carried out via a VPN tunnel (IPsec VPN or OpenVPN). **Prerequisite**: A suitable VPN tunnel is available. If no suitable VPN tunnel is available, traffic is always sent **unencrypted via the default gateway**. A suitable VPN tunnel is available if the remote peer belongs to the remote network of a configured VPN tunnel and the mGuard has an internal IP address that belongs to the local network of the same VPN tunnel. **Please note:** **For IPsec VPN connections**, the "Via VPN" function must be activated so that the traffic is routed through a suitable IPsec VPN tunnel. **For OpenVPN connections**, traffic is always routed via a suitable OpenVPN tunnel even if the function is deactivated.
	Next update	Information read directly from the CRL by the mGuard: Time and date when the CA will next issue a new CRL. This information is not influenced or considered by the CRL download interval.
	CRL issuer	Information read directly from the CRL by the mGuard: Shows the issuer of the relevant CRL.

Authentication >> Certificates >> CRL		
	Action: upload CRL file	If the CRL is available as a file, it can also be imported on the mGuard manually. • Click on the **No file selected** icon and select the desired CRL file. Then click on the **Open** button. If the icon is not shown, then after inserting a new table row, you must first click on the **Save** icon. • Then click on the **Upload CRL file** icon to import the CRL file. • Click on the **Save** icon to apply the changes. An up-to-date CRL file must always be used. For this reason, it is not included in the mGuard configuration. When exporting an mGuard configuration and then importing it to another mGuard, the CRL file must be uploaded again. CRL files might be deleted during a firmware update. In this case, the mGuard downloads the CRL files from the specified URL again. Alternatively, they can also be uploaded manually.

8 Network Security menu

> This menu is **not** available on the **FL MGUARD BLADE controller**. A reduced version of the menu is available on the **FL MGUARD RS2000, TC MGUARD RS2000 3G**, **TC MGUARD RS2000 4G**, and **FL MGUARD RS2005**.

8.1 Network Security >> Packet Filter

The mGuard includes a *Stateful Packet Inspection Firewall*. The connection data of an active connection is recorded in a database (connection tracking). Rules therefore only have to be defined for one direction. This means that data from the other direction of the relevant connection, and only this data, is automatically allowed through.

A side effect is that existing connections are not aborted during reconfiguration, even if a corresponding new connection can no longer be established.

The firewall rules configured under **Network security >> Packet filter** are not used on IP packets which are directed to an mGuard IP address. They only apply to IP connections or IP traffic which passes through the mGuard.

Default firewall settings

– All incoming connections are discarded (excluding VPN).
– Data packets of all outgoing connections are allowed through.

The firewall rules here have an effect on the firewall that is permanently active, with the exception of:

– **VPN connections**. Individual firewall rules are defined for VPN connections (see "IPsec VPN >> Connections" on page 322, "Firewall" on page 352).
– **User firewall**. When a user logs in, for whom user firewall rules are defined, these rules take priority (see "Network Security >> User Firewall" on page 291), followed by the permanently active firewall rules.

> If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored.

Firewall settings for devices from the RS2000 series

> FL MGUARD RS2000, TC MGUARD RS2000 3G, TC MGUARD RS2000 4G and FL MGUARD RS2005 have a simple firewall functionality.
>
> The following functions are not supported:
>
> – **Firewall rule records** cannot be configured.
> – **MAC filters** cannot be configured.
> – A **user firewall** cannot be configured.
> – **Host names in IP-groups** cannot be used.
>
> Caution: configuration profiles which include the corresponding settings cannot be imported.

Use of host names in IP groups (firewall rules)

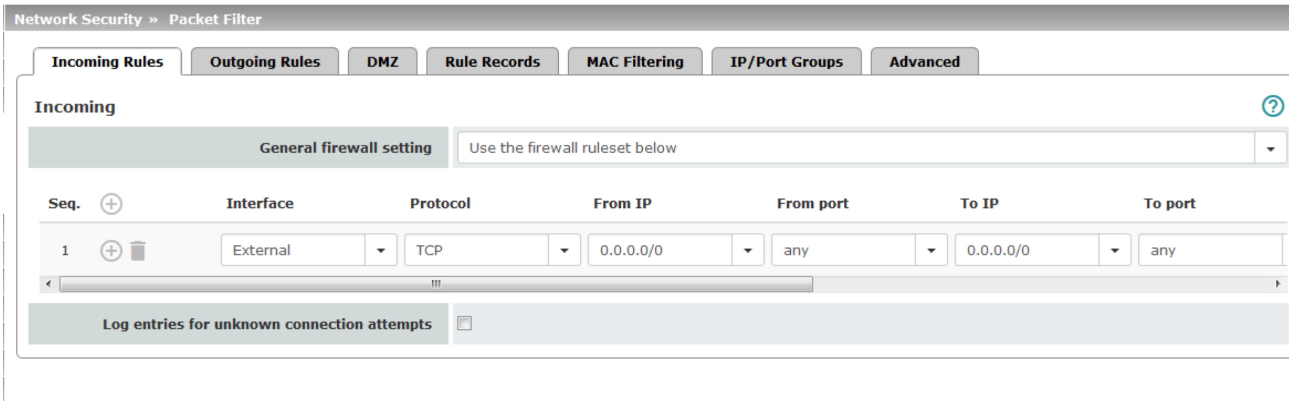
Host names can also be specified in IP groups in addition to IP addresses, IP areas, and networks (DNS-based firewall rules). IP address resolution of host names is performed according to the DNS settings of the mGuard. This allows host names to be used in firewall groups via IP groups (see "IP/Port Groups" on page 275).

NOTE: When using host names, there is always the risk of an attacker manipulating or blocking DNS requests (i.e. *DNS spoofing*). You should therefore only configure trustworthy and secure DNS servers from your internal company network on the mGuard, so as to avoid these types of attacks.

For security reasons, IP groups that contain host names should not be used in firewall rules which execute “Drop” or “Reject” as the action.

If a host name from an IP group cannot be resolved, e.g., because a DNS server has not been configured or cannot be reached, this host will not be taken into consideration for the rule. Further entries in the IP group are not affected by this and are taken into consideration.

8.1.1 Incoming Rules



Network Security >> Packet Filter >> Incoming Rules

Incoming

Lists the firewall rules that have been set up. They apply for incoming data links that have been initiated externally.

Special firewall settings apply for the mGuard devices from the RS2000 series (see "Firewall settings for devices from the RS2000 series" on page 257).

All incoming connections are discarded (excluding VPN) in the default setting.

If “*Use the firewall ruleset below*“ is selected as the **General firewall setting** and **no rule** has been set, the data packets of all incoming connections (excluding VPN) are dropped.

The DoS protection of the device is not available, if “*Accept all connections*“ is selected as the **General firewall setting** (see "Flood Protection" on page 289).

To provide DoS protection in this case, select the **General firewall setting** "*Use the firewall ruleset below*" and then create a firewall rule that accepts all connections.

General firewall setting

Accept all connections: the data packets of all incoming connections are allowed.

Drop all connections: the data packets of all incoming connections are discarded.

Accept Ping only: the data packets of all incoming connections are discarded, except for ping packets (ICMP). This setting allows all ping packets to pass through. The integrated protection against brute force attacks is not effective in this case.

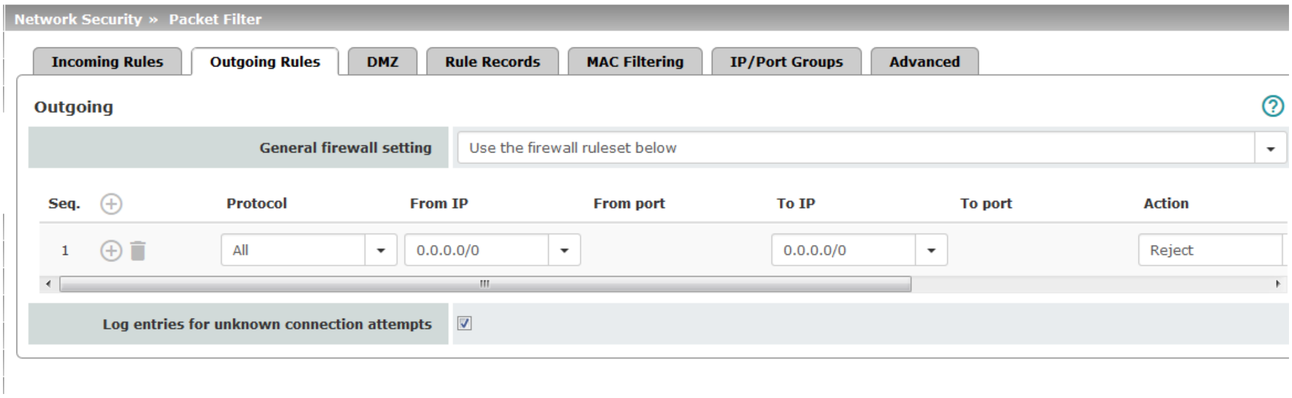
Use the firewall ruleset below: displays further setting options.

The following settings are only visible if “**Use the firewall ruleset below**” is set.

Network Security >> Packet Filter >> Incoming Rules [...]		
	Interface	External / External 2 / Any Specifies via which interface the data packets are received so that the rule applies to them. **Any** refers to the **External** and **External 2** interfaces. These interfaces are only available on mGuard models that have a serial interface with external access.
	Protocol	**All** means TCP, UDP, ICMP, GRE, and other IP protocols
	From IP / To IP	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 26). **Name of IP groups**, if defined. When a name is specified for an IP group, the host names, IP addresses, IP areas or networks saved under this name are taken into consideration (see IP/Port Groups tab page). If host names are used in IP groups, the mGuard must be configured so that the host name of a DNS server can be resolved in an IP address. If a host name from an IP group cannot be resolved, this host will not be taken into consideration for the rule. Further entries in the IP group are not affected by this and are taken into consideration. The use of host names in IP groups is not possible on mGuard devices of the RS2000 series.
	From port / To port (Only for TCP and UDP protocols)	**any** refers to any port. **startport:endport** (e.g., 110:120) refers to a port range. Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110). **Name of port groups**, if defined. When a name is specified for a port group, the ports or port ranges saved under this name are taken into consideration (see IP/Port Groups tab page).

Network Security >> Packet Filter >> Incoming Rules [...]		
	Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back and the sender is informed of their rejection. In Stealth mode, **Reject** has the same effect as **Drop**. **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts. **Name of rule records**, if defined. When a rule record is selected, the firewall rules configured under this rule record take effect (see "Rule Records" on page 268). For security reasons, rule records that contain IP groups with host names should not be used in firewall rules which execute “Drop” or “Reject” as the action. The use of rule records is not possible on mGuard devices of the RS2000 series. **Name of Modbus TCP rule records**, if defined. When a Modbus TCP rule record is selected, the firewall rules configured under this rule record take effect (see "Modbus TCP" on page 284).
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – activate *Log* function – Should not be logged – deactivate *Log* function (default)
	Log entries for unknown connection attempts	When the function is activated, all connection attempts that are not covered by the rules defined above are logged. (Default setting: **deactivated**)

8.1.2 Outgoing Rules

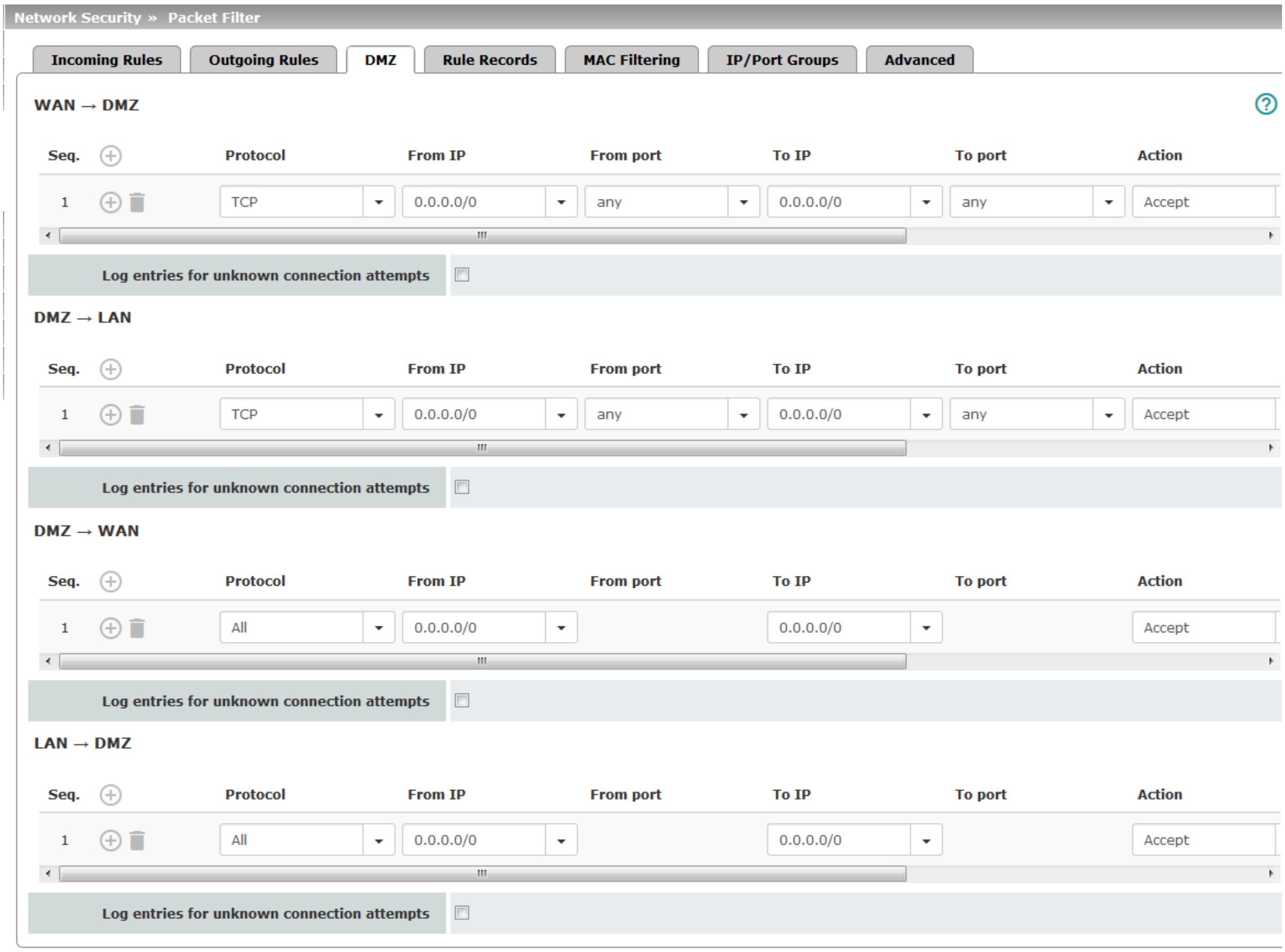


Network Security >> Packet Filter >> Outgoing Rules		
Outgoing	Lists the firewall rules that have been set up. They apply for outgoing data links that have been initiated internally in order to communicate with a remote peer. Special firewall settings apply for the mGuard devices from the RS2000 series (see "Firewall settings for devices from the RS2000 series" on page 257). A rule is defined by default that allows all outgoing connections. If "**Use the firewall ruleset below**" is selected and **no rule** has been set, the data packets of all outgoing connections (excluding VPN) are dropped.	
	General firewall setting	**Accept all connections**: the data packets of all outgoing connections are allowed. **Drop all connections**: the data packets of all outgoing connections are discarded. **Accept Ping only**: the data packets of all outgoing connections are discarded, except for ping packets (ICMP). **Use the firewall ruleset below**: displays further setting options.
	The following settings are only visible if "**Use the firewall ruleset below**" is set.	
	Protocol	**All** means TCP, UDP, ICMP, GRE, and other IP protocols

Network Security >> Packet Filter >> Outgoing Rules [...]		
	From IP / To IP	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 26). **Name of IP groups**, if defined. When a name is specified for an IP group, the host names, IP addresses, IP areas or networks saved under this name are taken into consideration (see IP/Port Groups tab page). If host names are used in IP groups, the mGuard must be configured so that the host name of a DNS server can be resolved in an IP address. If a host name from an IP group cannot be resolved, this host will not be taken into consideration for the rule. Further entries in the IP group are not affected by this and are taken into consideration. The use of host names in IP groups is not possible on mGuard devices of the RS2000 series.
	From port / To port (Only for TCP and UDP protocols)	**any** refers to any port. **startport:endport** (e.g., 110:120) refers to a port range. Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110). **Name of port groups**, if defined. When a name is specified for a port group, the ports or port ranges saved under this name are taken into consideration (see IP/Port Groups tab page).

Network Security >> Packet Filter >> Outgoing Rules [...]		
	Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back and the sender is informed of their rejection. . In Stealth mode, **Reject** has the same effect as **Drop**. **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts. **Name of rule records**, if defined. When a rule record is selected, the firewall rules configured under this rule record take effect (see "Rule Records" on page 268). For security reasons, rule records that contain IP groups with host names should not be used in firewall rules which execute “Drop” or “Reject” as the action. The use of rule records is not possible on mGuard devices of the RS2000 series. **Name of Modbus TCP rule records**, if defined. When a Modbus TCP rule record is selected, the firewall rules configured under this rule record take effect (see "Modbus TCP" on page 284).
	Comment	Freely selectable comment for this firewall rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – activate *Log* action – Should not be logged – deactivate *Log* action (default)
	Log entries for unknown connection attempts	When the function is activated, all connection attempts that are not covered by the rules defined above are logged. (Default setting: **deactivated**)

8.1.3 DMZ

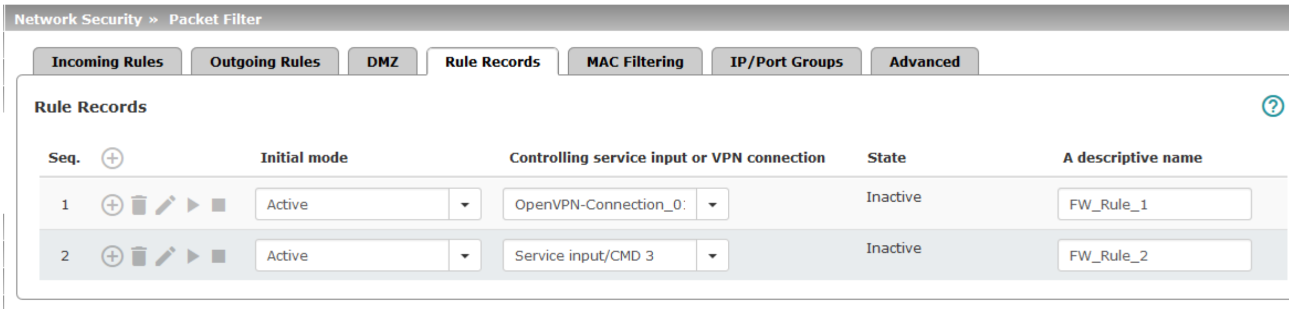


Network Security >> Packet Filter >> DMZ		
Firewall rules for the DMZ (Only for TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004, FL MGUARD CENTERPORT)	The DMZ can be protected against attacks from the internal network (LAN interface) and the external network (WAN interface) using a dedicated set of firewall rules. The settings are split into four possible directions of network traffic.	
WAN → DMZ		If no rule has been set, the data packets of all incoming connections (excluding VPN) are dropped (default setting).
DMZ → LAN		If no rule has been set, the data packets of all outgoing connections (excluding VPN) are dropped (default setting).
DMZ → WAN		A rule is defined by default that allows all outgoing connections.

Network Security >> Packet Filter >> DMZ [...]		
LAN → DMZ		A rule is defined by default that allows all incoming connections.
	Protocol	**All** means TCP, UDP, ICMP, GRE, and other IP protocols
	From IP / To IP	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 26). **Name of IP groups**, if defined. When a name is specified for an IP group, the host names, IP addresses, IP areas or networks saved under this name are taken into consideration (see IP/Port Groups tab page). If host names are used in IP groups, the mGuard must be configured so that the host name of a DNS server can be resolved in an IP address. If a host name from an IP group cannot be resolved, this host will not be taken into consideration for the rule. Further entries in the IP group are not affected by this and are taken into consideration.
	From port / To port (Only for TCP and UDP protocols)	**any** refers to any port. **startport:endport** (e.g., 110:120) refers to a port range. Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110). **Name of port groups**, if defined. When a name is specified for a port group, the ports or port ranges saved under this name are taken into consideration (see IP/Port Groups tab page).

Network Security >> Packet Filter >> DMZ [...]		
	Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back and the sender is informed of their rejection. . In Stealth mode, **Reject** has the same effect as **Drop**. **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts. **Name of rule records**, if defined. When a rule record is selected, the firewall rules configured under this rule record take effect (see "Rule Records" on page 268). For security reasons, rule records that contain IP groups with host names should not be used in firewall rules which execute “Drop” or “Reject” as the action. **Name of Modbus TCP rule records**, if defined. When a Modbus TCP rule record is selected, the firewall rules configured under this rule record take effect (see "Modbus TCP" on page 284).
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – activate *Log* action – Should not be logged – deactivate *Log* action (default)
	Log entries for unknown connection attempts	When the function is activated, all connection attempts that are not covered by the rules defined above are logged. (Default setting: **deactivated**)

8.1.4 Rule Records



Firewall rule records are used to combine firewall rules into one rule record. These can then be enabled or disabled together via the rule record.

A rule record – and thus all the firewall rules configured in it – could, for example, be controlled via an on/off switch or an established VPN connection (see "Management >> Service I/O" on page 115).

Notes on the use of rule records that are only temporarily activated

In firewall rule records that are only temporarily activated (e.g. controlled by a switch), so-called "**Allow rules**" (Action = Accept) should always be used:

– The rule record is activated to allow the configured connections.
– The rule record is deactivated to block the configured connections.

"**Deny rules**" (Action = Reject/Drop) should not be used in temporarily activated rule records, since corresponding already existing data connections would not be automatically terminated with the activation of the rule record.

If a connection associated with a firewall rule record has been established and is continuously creating data traffic, deactivation of the firewall rule record might not interrupt this connection as expected.

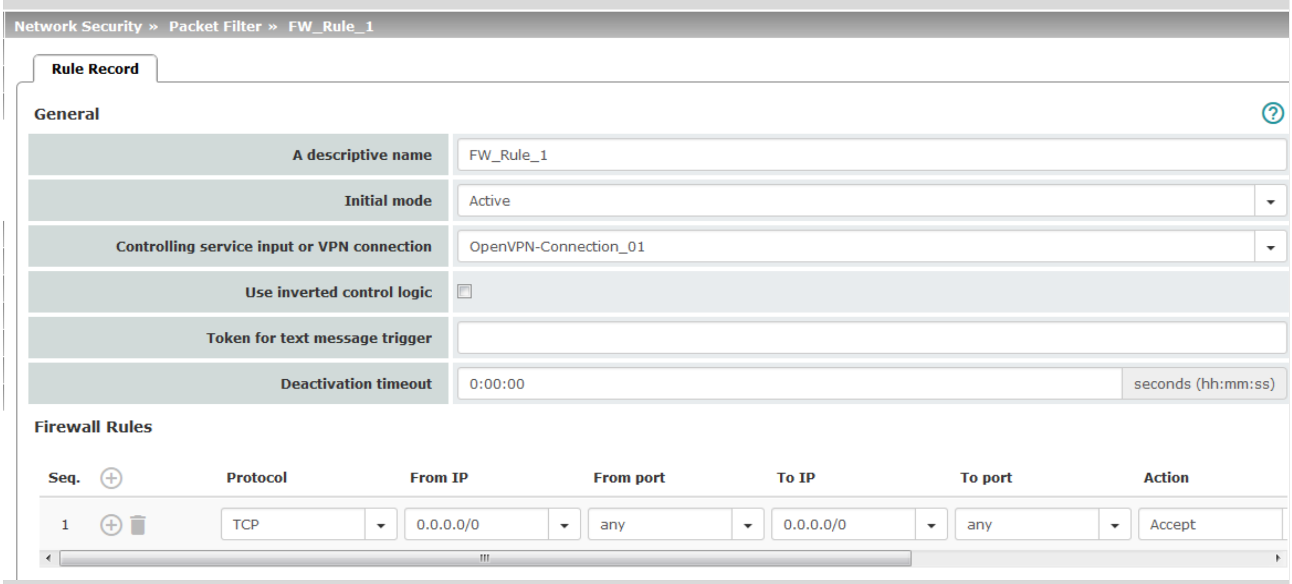
This happens because the (outgoing) response of a service on the LAN side creates an entry in the connection tracking table which enables a different (incoming) request from an external peer. This peer passes the firewall using the same parameters, however, it is not connected to the firewall rule record.

There are two ways to set up the mGuard so that it interrupts the associated connections when deactivating the firewall rule record.

– Activate the "Allow TCP connections upon SYN only" option under Network Security >> Packet Filter >> Advanced.
– In the firewall, block the outgoing connections that operate via the port that is the destination for the incoming connections.

If, for example, the firewall rule record enables incoming data traffic on port 22, an outgoing rule can be set up that deactivates any data traffic coming from port 22.

Network Security >> Packet Filter >> Rule Records		
Rule Records (This menu item is not included in the scope of functions for TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005 or FL MGUARD RS2000.)	**Initial mode**	**Disabled / Active / Inactive** Determines the output state of the firewall rule record following a reconfiguration or restart. The “Active/Inactive” setting is only applicable if a pushbutton is connected. If the firewall rule records are controlled via a switch or VPN connection, they have priority. If set to “Disabled”, the firewall rule record cannot be dynamically enabled. The firewall rule record is retained but has no influence.
	Controlling service input or VPN connection	**Service input CMD 1-3, VPN connection** The firewall rule record can be switched via a pushbutton/switch or a VPN connection. The pushbutton/switch must be connected to one of the service contacts (CMD 1-3).
	State	Indicates the current state.
	A descriptive name	The firewall rule record can be freely named/renamed.
	Activate / Inactivate rule record	**Activate / Inactivate** You can enable or disable the rule record by clicking on the ▶ **Activate** and ■ **Inactivate** icons.
Edit	The following tab page appears when you click on the ✎ **Edit Row** icon:	

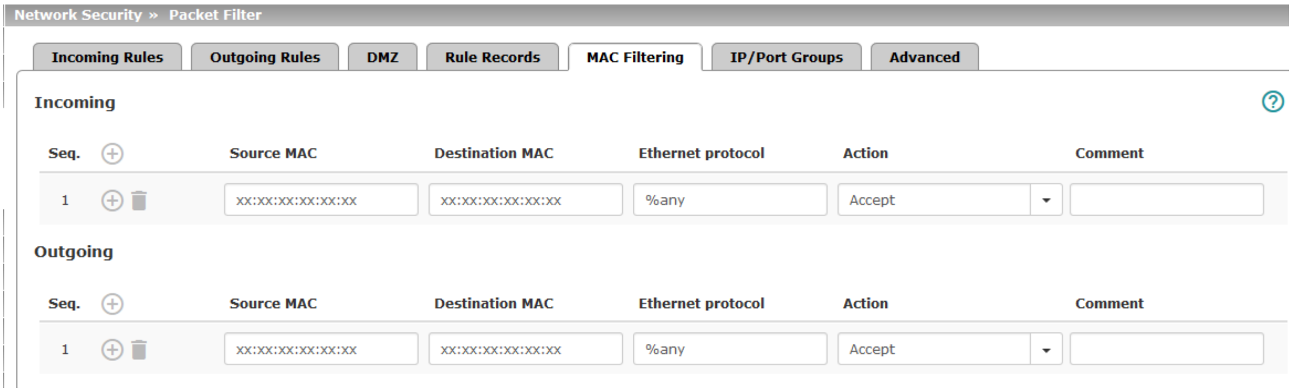


Network Security >> Packet Filter >> Rule Records [...]		
General	**A descriptive name**	The firewall rule record can be freely named/renamed.
	Initial mode	**Disabled / Active / Inactive** Determines the output state of the firewall rule record following a reconfiguration or restart. The “Active/Inactive” setting is only applicable if a pushbutton is connected. If the firewall rule records are controlled via a switch or VPN connection, they have priority. If set to “Disabled”, the firewall rule record cannot be dynamically enabled. It is retained but has no influence.
	Controlling service input or VPN connection	**Service input CMD 1-3, VPN connection** The firewall rule record can be switched via a pushbutton/switch or a VPN connection. The pushbutton/switch must be connected to one of the service contacts (CMD 1-3).
	Use inverted control logic	Inverts the behavior of the connected pushbutton/switch or the controlling VPN connection. If the controlling service input is configured as an on/off switch, it can activate one firewall rule record while simultaneously deactivating another, for example. The same is true for the controlling VPN connections.
	Token for text message trigger	Only available with the TC MGUARD RS4000 3G, TC MGUARD RS4000 4G. Incoming text messages can be used to activate or deactivate firewall rule records. The text message must contain the “fwrules/active” or “fwrules/inactive” command followed by the token.
	Deactivation timeout	Activated firewall rule records are deactivated after this time has elapsed. 0 means the setting is disabled. Time in hh:mm:ss (1 day maximum) The entry can be in seconds [ss], minutes and seconds [mm:ss] or hours, minutes, and seconds [hh:mm:ss].
Firewall Rules	**Protocol**	**All** means TCP, UDP, ICMP, GRE, and other IP protocols.

Network Security >> Packet Filter >> Rule Records [...]		
	From IP	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 26). **Name of IP groups**, if defined. When a name is specified for an IP group, the host names, IP addresses, IP areas or networks saved under this name are taken into consideration (see IP/Port Groups tab page). If host names are used in IP groups, the mGuard must be configured so that the host name of a DNS server can be resolved in an IP address. If a host name from an IP group cannot be resolved, this host will not be taken into consideration for the rule. Further entries in the IP group are not affected by this and are taken into consideration.
	From port / To port (Only for TCP and UDP protocols)	**any** refers to any port. **startport:endport** (e.g., 110:120) refers to a port range. Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110). **Name of port groups**, if defined. When a name is specified for a port group, the ports or port ranges saved under this name are taken into consideration (see IP/Port Groups tab page).
	Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back and the sender is informed of their rejection. In Stealth mode, **Reject** has the same effect as **Drop**. **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts. **Name of rule records**, if defined. When a rule record is selected, the firewall rules configured under this rule record take effect (see "Rule Records" on page 268). For security reasons, rule records that contain IP groups with host names should not be used in firewall rules which execute “Drop” or “Reject” as the action. **Name of Modbus TCP rule records**, if defined. When a Modbus TCP rule record is selected, the firewall rules configured under this rule record take effect (see "Modbus TCP" on page 284).

Network Security >> Packet Filter >> Rule Records [...]		
	Comment	Freely selectable comment for this rule.
	Log	For each firewall rule, you can specify whether the use of the rule: – Should be logged – activate *Log* function – Should not be logged – deactivate *Log* function (default)

8.1.5 MAC Filtering



The incoming and outgoing rules only apply to the Network mode *Stealth*.

The “Incoming” MAC filter is applied to frames that the mGuard receives at the WAN interface. The “Outgoing” MAC filter is applied to frames that the mGuard receives at the LAN interface. Data packets that are received or sent via a modem connection on models with a serial interface[1] are not picked up by the MAC filter because the Ethernet protocol is not used here.

In *Stealth* mode, in addition to the packet filter (Layer 3/4) that filters data traffic, e.g., according to ICMP messages or TCP/UDP connections, a MAC filter (Layer 2) can also be set. A MAC filter (Layer 2) filters according to MAC addresses and Ethernet protocols.

In contrast to the packet filter, the MAC filter is stateless. If rules are introduced, corresponding rules must also be created for the opposite direction.
If no rules are set, all ARP and IP packets are allowed to pass through.

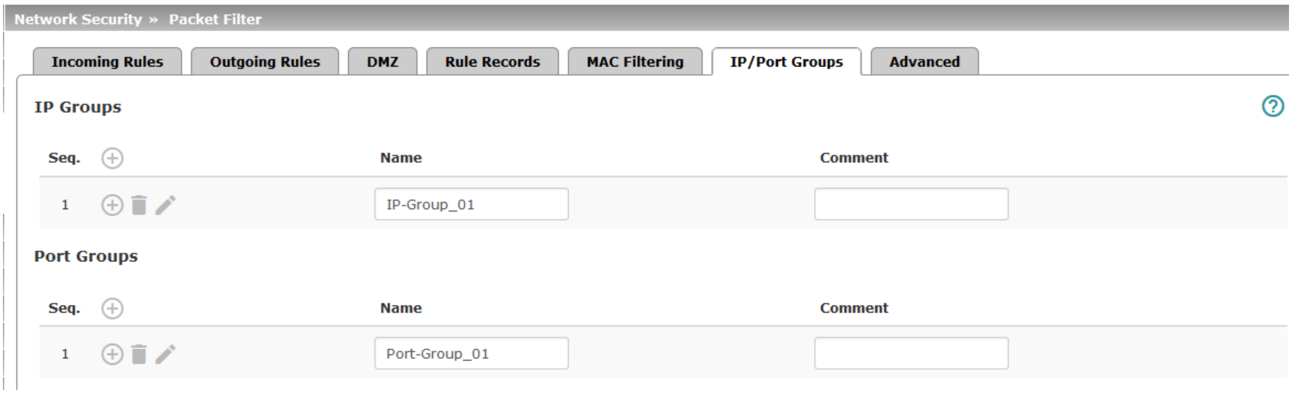
When setting MAC filter rules, please note the information displayed on the screen. The rules defined here have priority over packet filter rules. The MAC filter does not support logging.

Network Security >> Packet Filter >> MAC Filtering		
Incoming (This menu item is not included in the scope of functions for TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005 or FL MGUARD RS2000.)	**Source MAC**	xx:xx:xx:xx:xx:xx stands for all MAC addresses.
	Destination MAC	xx:xx:xx:xx:xx:xx stands for all MAC addresses. ff:ff:ff:ff:ff:ff stands for the broadcast MAC address to which all ARP requests are sent, for example.

[1] *TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4004/RS2005, FL MGUARD RS4000/RS2000, mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD RS, FL MGUARD BLADE, mGuard delta (Innominate)*

Network Security >> Packet Filter >> MAC Filtering [...]		
	Ethernet protocol	**%any** stands for all Ethernet protocols. Additional protocols can be specified in name or hexadecimal format, for example: – IPv4 or 0800 – ARP or 0806
	Action	**Accept** means that the data packets may pass through. **Drop** means that the data packets are not permitted to pass through (they are dropped).
	Comment	Freely selectable comment for this rule.
Outgoing	The explanation provided under “Incoming” also applies to “Outgoing”.	

8.1.6 IP/Port Groups



IP and port groups enable the easy creation and management of firewall and NAT rules in complex network structures.

Host names, IP addresses, IP areas, and networks can be grouped in IP groups and identified by a name. Likewise, ports or port ranges can be grouped in port groups.

If a firewall or NAT rule is created, instead of IP addresses/IP areas or ports/port ranges, the IP or port groups can be selected directly in the corresponding fields and assigned the rule.

NOTE: Ineffective firewall rules due to empty IP or port groups

Do not use empty IP or port groups, i.e. created groups in which no values are configured. Firewall rules that refer to empty IP or port groups have no effect.

NOTE: When using host names, there is always the risk of an attacker manipulating or blocking DNS requests (i.e. *DNS spoofing*). You should therefore only configure trustworthy and secure DNS servers from your internal company network on the mGuard, so as to avoid these types of attacks.

For security reasons, IP groups that contain host names should not be used in firewall rules which execute “Drop” or “Reject” as the action.

Use of hostnames

Address resolution of hostnames is performed according to the DNS settings of the mGuard (see "Network >> DNS" on page 205).

If a host name can be resolved in several IP addresses, all IP addresses returned by the DNS server are taken into consideration.

If a host name from an IP group cannot be resolved, e.g., because a DNS server has not been configured or cannot be reached, this host will not be taken into consideration for the rule. Further entries in the IP group are not affected by this and are taken into consideration.

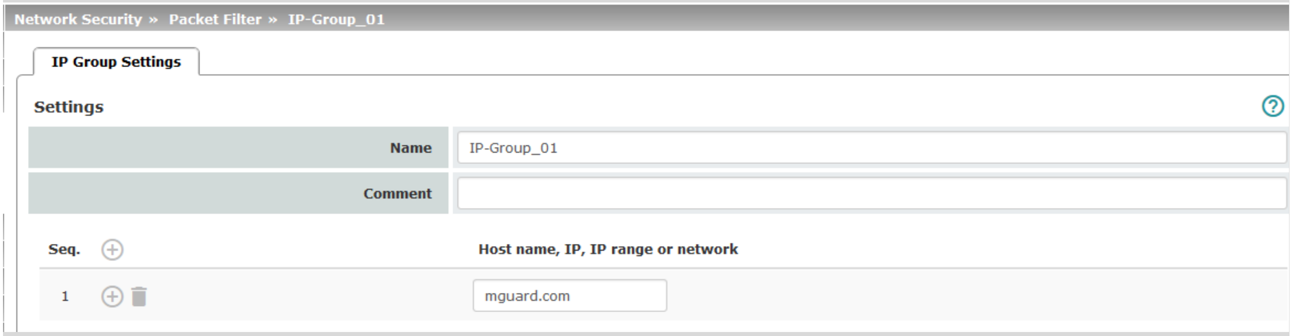
If a DNS server resolves a resolved host name with another IP address after the TTL has elapsed, an existing connection to the original IP address is **not aborted**.

mGuard devices of the RS2000 series

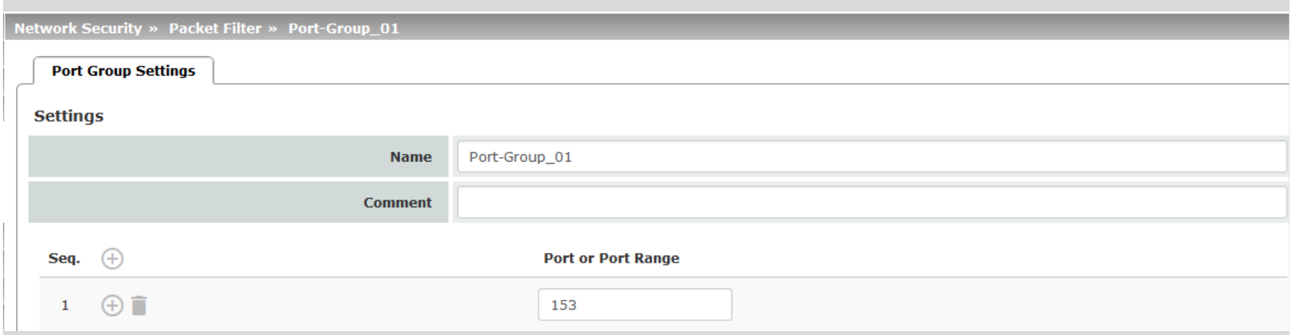
The use of host names in IP groups is not supported by mGuard devices of the RS2000 series.

Network Security >> Packet Filter >> IP/Port Groups		
IP Groups	**Name**	The IP group can be freely named/renamed.

Network Security >> Packet Filter >> IP/Port Groups [...]		
	Comment	Freely selectable comment for this group/rule.
Edit	The following tab page appears when you click on the **Edit Row** icon:	



IP Group Settings	**Name**	The IP group can be freely named/renamed.
	Comment	Freely selectable comment for this group/rule.
	Host name, IP, IP range or network	The entries can specify a host name (e.g., mguard.com), an IP address (e.g., 192.168.3.1), an IP address area (e.g., 192.168.3.1-192.168.3.10) or a network in CIDR format (e.g., 192.168.1.0/24). Using more than 200 host names in IP groups is not supported. When using host names, there is always the risk of an attacker manipulating or blocking DNS requests (i.e. *DNS spoofing*). You should therefore only configure trustworthy and secure DNS servers from your internal company network on the mGuard, so as to avoid these types of attacks.
Port groups	**Name**	The port group can be freely named/renamed.
	Comment	Freely selectable comment for this group/rule.
Edit	The following tab page appears when you click on the **Edit Row** icon:	

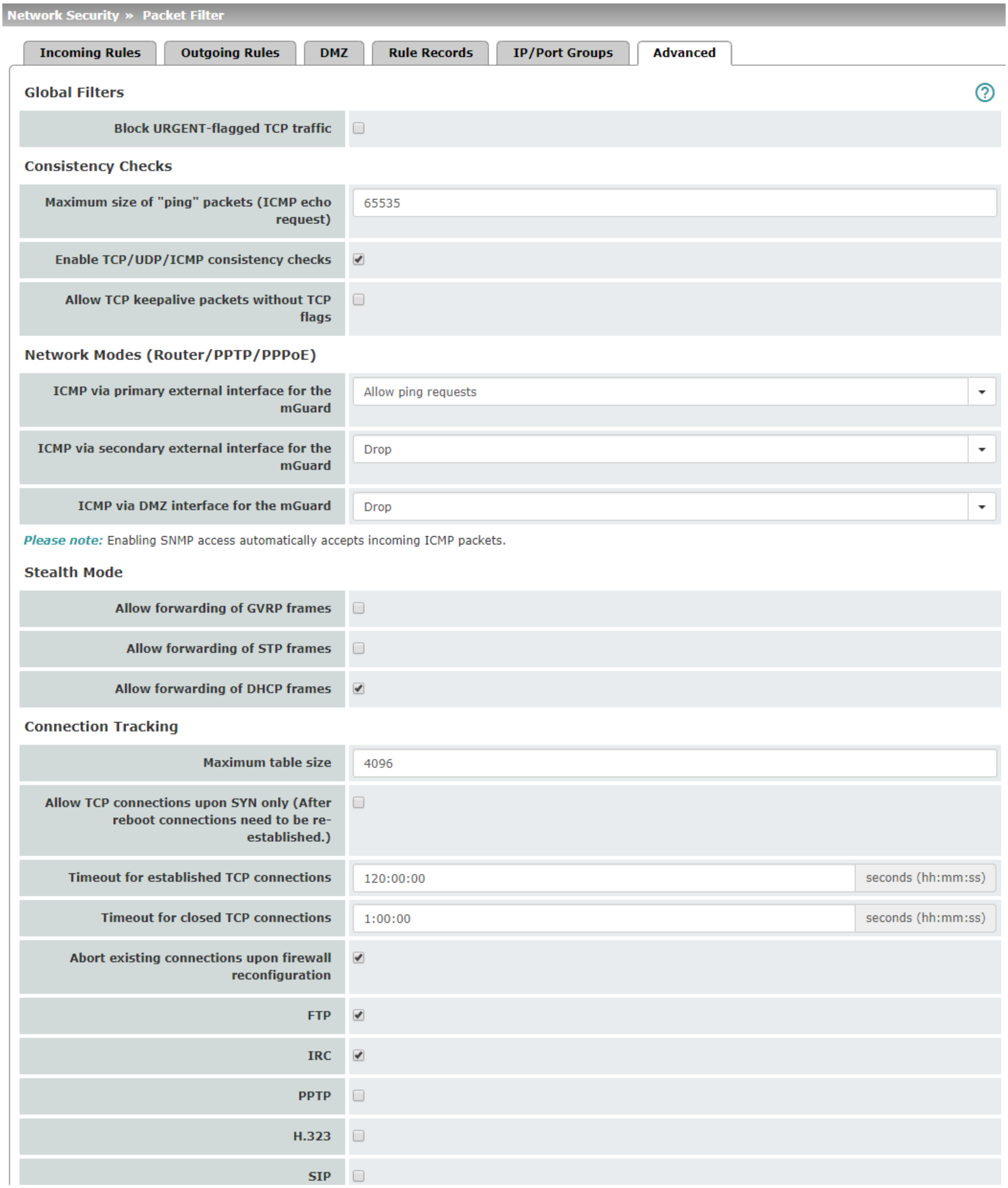


Port Group Settings	**Name**	The port group can be freely named/renamed.

Network Security >> Packet Filter >> IP/Port Groups [...]		
	Comment	Freely selectable comment for this group/rule.
	Port or Port Range	The entries can specify a port (e.g., pop3 or 110) or a port range (e.g., 110:120 or 110-120).

8.1.7 Advanced

The following settings affect the basic behavior of the firewall.



Network Security >> Packet Filter >> Advanced		
Global Filters (This menu item is not included in the scope of functions for TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005 or FL MGUARD RS2000.)	**Block URGENT-flagged TCP traffic**	When the function is activated, packets with the URGENT flag set in the TCP header are blocked: – In network mode "*Router*", the connections over which corresponding packets are sent are terminated. – In network mode "*Stealth*", the corresponding packets are dropped. TCP packets with the URGENT flag set that are routed through a VPN tunnel are also blocked.
Consistency Checks (This menu item is not included in the scope of functions for TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005 or FL MGUARD RS2000.)	**Maximum size of “ping” packets (ICMP echo request)**	Refers to the length of the entire packet including the header. The packet length is normally 64 bytes, but it can be larger. If oversized packets are to be blocked (to prevent bottlenecks), a maximum value can be specified. This value should be more than 64 bytes in order to not block normal ICMP echo requests.
	Enable TCP/UDP/ICMP consistency checks	When the function is activated, the mGuard performs a range of tests to check for incorrect checksums, packet sizes, etc. and drops packets that fail these tests. The function is deactivated by default.
	Allow TCP keepalive packets without TCP flags	TCP packets without flags set in their TCP header are normally rejected by firewalls. At least one type of Siemens controller with older firmware sends TCP keepalive packets without TCP flags set. These are therefore discarded as invalid by the mGuard. When the **function is activated**, forwarding of TCP packets where no TCP flags are set in the header is enabled. This only applies when TCP packets of this type are sent within an existing TCP connection established in the regular way. TCP packets without TCP flags do not result in a new entry in the connection table (see "Connection Tracking" on page 281). If the connection is already established when the mGuard is restarted, the corresponding packets are still rejected and connection problems can be observed as long as no packets with flags belonging to the connection are sent. These settings affect all the TCP packets without flags. **Activation** of this function therefore weakens the security functions provided by the mGuard.

Network Security >> Packet Filter >> Advanced [...]		
Network Modes (Router/PPTP/PPPoE)	**ICMP via primary external interface for the mGuard** **ICMP via secondary external interface for the mGuard** **ICMP via DMZ interface for the mGuard**	This option can be used to control the behavior of the mGuard when ICMP messages are received from the external network via the primary/secondary external interface. Regardless of the setting specified here, incoming ICMP packets are always accepted if SNMP access is activated. **Drop**: all ICMP messages to all IP addresses of the mGuard are dropped. **Allow ping requests**: only ping messages (ICMP type 8) to all IP addresses of the mGuard are accepted. **Allow all ICMPs**: all types of ICMP messages to all IP addresses of the mGuard are accepted.
Stealth Mode	**Allow forwarding of GVRP frames**	The GARP VLAN Registration Protocol (GVRP) is used by GVRP-capable switches to exchange configuration information. When the **function is activated**, GVRP packets are allowed to pass through the mGuard in *Stealth* mode.
	Allow forwarding of STP frames	The Spanning Tree Protocol (STP) (802.1d) is used by bridges and switches to detect and allow for loops in the cabling. When the **function is activated**, STP packets are allowed to pass through the mGuard in *Stealth* mode.
	Allow forwarding of DHCP frames	When the **function is activated**, the client is allowed to obtain an IP address via DHCP – regardless of the firewall rules for outgoing data traffic. The function is **activated** by default.

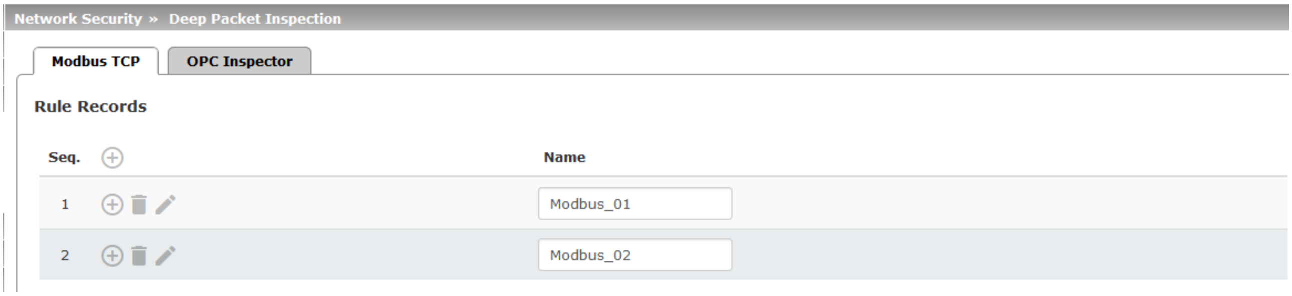
Network Security >> Packet Filter >> Advanced [...]		
Connection Tracking	**Maximum table size**	This entry specifies an upper limit. This is set to a value that can never be reached during normal practical operation. However, it can be easily reached in the event of attacks, thus providing additional protection. If there are special requirements in your operating environment, this value can be increased. Connections established from the mGuard are also counted. This value must therefore not be set too low, as this will otherwise cause malfunctions.
	Allow TCP connections upon SYN only	SYN is a special data packet used in TCP/IP connection establishment that marks the beginning of the connection establishment process. **Function deactivated** (**default**): the mGuard also allows connections where the beginning has not been registered. This means that the mGuard can perform a restart when a connection is present without interrupting the connection. **Function activated**: the mGuard must have registered the SYN packet of an existing connection. Otherwise, the connection is aborted. If the mGuard performs a restart while a connection is present, this connection is interrupted. Attacks on and the hijacking of existing connections are thus prevented.
	Timeout for established TCP connections	If a TCP connection is not used during the time period specified here, the connection data is deleted. A connection translated by NAT (not 1:1 NAT) must then be reestablished. If the "Allow TCP connections upon SYN only" function has been activated, all expired connections must be reestablished. Default setting: 120 hours (120:00:00) The entry can be in seconds [ss], minutes and seconds [mm:ss] or hours, minutes, and seconds [hh:mm:ss].
	Timeout for closed TCP connections	The timeout specifies how long the mGuard keeps a TCP-connection open when one side ends the connection with a "FIN packet", but the peer has not yet confirmed this. Default setting: 1 hour (1:00:00) The entry can be in seconds [ss], minutes and seconds [mm:ss] or hours, minutes, and seconds [hh:mm:ss].

Network Security >> Packet Filter >> Advanced [...]		
	Abort existing connections upon firewall reconfiguration	When the **function is activated (default)**, the existing connections are reset if the following applies: – If the "Allow TCP connections upon SYN only" function has been activated and – The firewall rules have been adjusted or – If the function is activated (even without changing the firewall rules) After changing the firewall rules, the mGuard behaves in the same way as after a restart. However, this only applies to the forwarded connections. Existing TCP connections are interrupted, even if they are allowed according to the new firewall rules. Connections to the device are not affected, even if the firewall rules have been changed for remote access. When the **function is not activated**, the connections remain, even if the firewall rules changed would not allow them or would abort them.
	FTP	If an outgoing connection is established to call data for the FTP protocol, two methods of data transmission can be used: With “active FTP”, the called server establishes an additional counter-connection to the caller in order to transmit data over this connection. With “passive FTP”, the client establishes this additional connection to the server for data transmission. FTP must be **activated** (default) so that additional connections can pass through the firewall.
	IRC	Similar to FTP: for IRC chat over the Internet to work properly, incoming connections must be allowed following active connection establishment. IRC must be **activated** (default) in order for these connections to pass through the firewall.
	PPTP	**Default: deactivated** Must be **activated** if VPN connections are to be established using PPTP from local computers to external computers without the aid of the mGuard. Must be **activated** if GRE packets are to be forwarded from the internal area to the external area.
	H.323	**Default: deactivated** Protocol used to establish communication sessions between two or more devices. Used for audio-visual transmission. This protocol is older than SIP.

Network Security >> Packet Filter >> Advanced [...]		
	SIP	**Default: deactivated** SIP (Session Initiation Protocol) is used to establish communication sessions between two or more devices. Often used in IP telephony. When the **function is activated**, it is possible for the mGuard to track the SIP and add any necessary firewall rules dynamically if further communication channels are established to the same session. When NAT is also activated, one or more locally connected computers can communicate with external computers by SIP via the mGuard.

8.2 Network Security >> Deep Packet Inspection

8.2.1 Modbus TCP



The Modbus protocol is often used to integrate automation devices in industrial applications. It enables process data to be exchanged between Modbus controllers regardless of the network structure. Modbus is a client/server protocol.

The TCP/IP version of the protocol is used to transmit data in industrial Ethernet: **Modbus TCP**. Access to specific device data is controlled via the Modbus TCP protocol using **function codes**.

Reserved TCP port 502 is usually used for transmission via the Modbus TCP protocol.

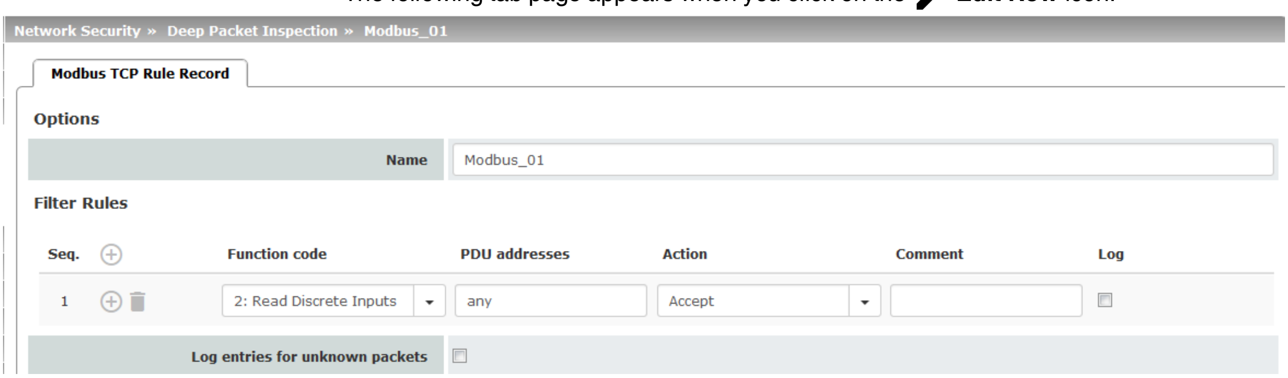
Deep Packet Inspection (DPI)

The mGuard can inspect packets of incoming and outgoing Modbus TCP connections (Deep Packet Inspection) and filter them if required. The user data of incoming packets is inspected. Responses to filtered requests are not subject to further DPI.

Packets which use specific function codes can be “dropped” or “accepted” via defined rules.

> If a TCP packet contains more than one *Protocol Data Unit* (PDU), the packet is always discarded.

The following tab page appears when you click on the **Edit Row** icon:

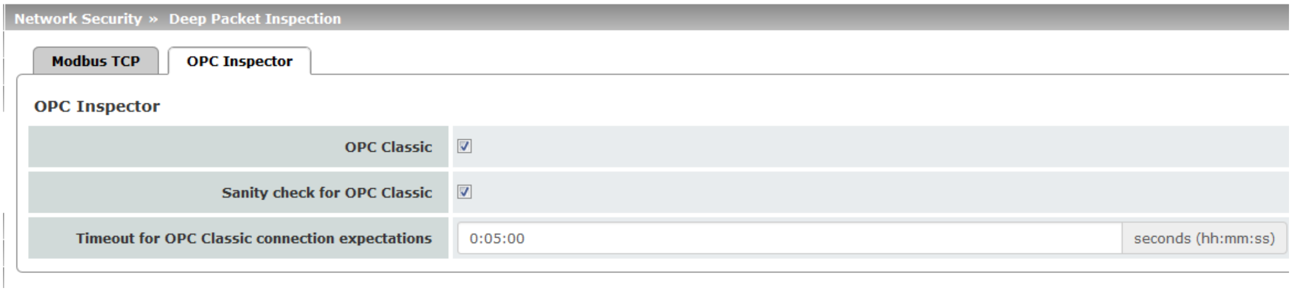


Network Security >> Deep Packet Inspection >> Modbus TCP >> Rule Records >> Edit		
Modbus TCP Rule Record	Modbus TCP rule records can only be used when a suitable license key is installed (*Modbus TCP Inspector*). The rules for filtering Modbus TCP packets are configured in rule records. These rule records can be used in the following firewall tables if "TCP" is selected as the protocol: general packet filter / DMZ / GRE / IPsec VPN / OpenVPN client / PPP. If a firewall rule uses a Modbus TCP rule record, data traffic is not possible via an affected connection which does not use the Modbus protocol. If the mGuard is unable to determine whether a Modbus packet is an incoming or outgoing packet, the packet is discarded. This is the case, for example, if the status of connection tracking has been deleted after connection establishment and the mGuard has therefore not registered the SYN packet of the existing connection.	
Options	**Name**	A descriptive name
Filter Rules	**Function code**	**1 - 255 / Name of the function code / any** Function codes in Modbus TCP connections indicate the purpose of data transmission, i.e., which operation is to be performed by the server (slave) based on the request from the client (master). You can select the function code from the drop-down list or enter it directly in the input field.

Network Security >> Deep Packet Inspection >> Modbus TCP >> Rule Records >> Edit		
	PDU addresses (Only displayed for certain function codes)	**0 - 65535 / any** Various addresses can be assigned to certain function codes (as PDU addresses based on 0). This setting can either be an individual PDU address (e.g., 47015) or an address area (e.g., 47010:47020). The PDU address area for incoming packets can either be **partially or fully** in the specified address area for the filter rule. The **action (Drop or Accept)** performed by the rule determines when the rule applies: 1. **Drop rule**: if “Drop” is selected as the action, the rule (i.e., that the packet will be discarded) applies if **at least one address** in the packet is in the specified address area. It also applies if the packet contains further addresses that are not in the specified address area. 2. **Accept rule**: if “Accept” is selected as the action, the rule (i.e., that the packet will be accepted) applies if **all addresses** in the packet are in the specified address area. An individual address is interpreted as an area in line with the behavior described above.
	Action	**Accept** means that the data packets may pass through. **Drop** means that the data packets are not permitted to pass through. They are discarded, rendering the TCP connection unusable. It therefore cannot be used for further data transmission. A new TCP connection must be established for subsequent Modbus requests. If multiple rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored. If no rule applies, the packet is discarded.
	Comment	Freely selectable comment for this rule.
	Log	For each individual Modbus TCP filter, you can specify whether the use of the rule: – Should be logged – activate *Log* action – Should not be logged – deactivate *Log* action (default)

Network Security >> Deep Packet Inspection >> Modbus TCP >> Rule Records >> Edit		
	Log entries for unknown packets	When the function is activated, the packets that are not covered by any of the created filter rules are logged.

8.2.2 OPC Inspector



Network Security >> Deep Packet Inspection >> OPC Inspector		
OPC Inspector	**OPC Classic**	This function can only be activated when a suitable license key (OPC Inspector) is installed. With OPC Classic, communication always starts via TCP port 135. The client and server then negotiate one or more additional connections on new ports. To enable these connections, in the past all ports of an interconnected firewall had to be open. If **OPC Classic** is activated, it is enough to only enable TCP port 135 for a client/server pair using the firewall rules. The mGuard inspects the user data of the packets (Deep Packet Inspection). It checks in the user data sent via this port whether a new connection has been negotiated, and opens the negotiated port. To do so, communication between the client and the server on port 135 must be enabled in both directions. The functionality of **OPC Classic** is also supported for the NAT methods *IP Masquerading* and *1:1 NAT*.
	Sanity check for OPC Classic	If **Sanity check for OPC Classic** is activated, only OPC packets may be transmitted via OPC Classic port 135 (TCP) and the newly negotiated ports.
	Timeout for OPC Classic connection expectations	Configures the timeout (in seconds) during which OPC traffic is expected. An existing OPC connection may negotiate another connection on a new port. If "Sanity check for OPC Classic" is activated, these connections must only be OPC connections. The mGuard creates a new dynamic firewall rule if it detects in OPC traffic that a new OPC connection should be established. The dynamic firewall rule immediately accepts new OPC connections with the negotiated parameters. If the timeout for the dynamic firewall expires, the rule is deleted. New connections with these parameters are then no longer accepted. Already established connections are not closed.

8.3 Network Security >> DoS Protection

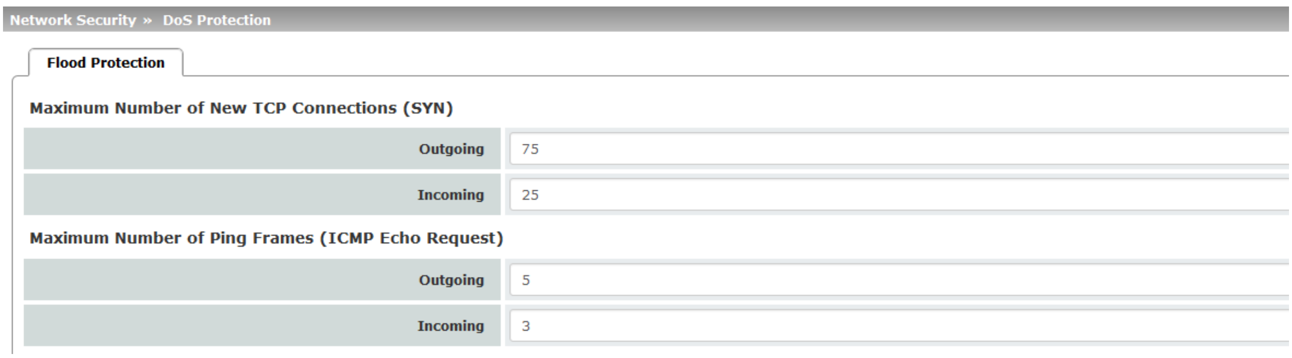
8.3.1 Flood Protection

This menu is **not** available on the **FL MGUARD RS2000, TC MGUARD RS2000 3G, TC MGUARD RS2000 4G,** and **FL MGUARD RS2005**.

NOTE: Firewall setting affects DoS protection

The DoS protection of the device is not available, if in the menu **Network Security >> Packet Filter >> Incoming Rules** "*Accept all connections*" is selected as the **General firewall setting** (see "Incoming Rules" on page 259).

To provide DoS protection in this case, select the **General firewall setting** "*Use the firewall ruleset below*" and then create a firewall rule that accepts all connections.



Network Security >> DoS Protection >> Flood Protection		
Maximum number of new TCP connections (SYN)	**Incoming/Outgoing**	Outgoing: default setting: 75 Incoming: default setting: 25 Maximum values for the number of incoming and outgoing TCP connections allowed per second. They are set to a value that can never be reached during normal practical operation. However, they can be easily reached in the event of attacks, thus providing additional protection. If there are special requirements in your operating environment, these values can be increased.
Maximum number of ping frames (ICMP echo request)	**Incoming/Outgoing**	Outgoing: default setting: 5 Incoming: default setting: 3 Maximum values for the number of incoming and outgoing “ping” packets allowed per second. They are set to a value that can never be reached during normal practical operation. However, they can be easily reached in the event of attacks, thus providing additional protection. If there are special requirements in your operating environment, these values can be increased. The value **0** means that no “ping” packets are allowed through or in.

Network Security >> DoS Protection >> Flood Protection [...]		
Maximum number of ARP requests or ARP replies each (Only in "Stealth" network mode)	**Incoming/Outgoing**	Default setting: 500 Maximum values for the number of incoming and outgoing ARP requests or replies allowed per second. They are set to a value that can never be reached during normal practical operation. However, they can be easily reached in the event of attacks, thus providing additional protection. If there are special requirements in your operating environment, these values can be increased.

8.4 Network Security >> User Firewall

> This menu is **not** available on the **FL MGUARD RS2000, TC MGUARD RS2000 3G, TC MGUARD RS2000 4G,** and **FL MGUARD RS2005**.

The user firewall is used exclusively by firewall users, i.e., users who are registered as firewall users (see "Authentication >> Firewall Users" on page 235).

Each firewall user can be assigned a set of firewall rules, also referred to as a template.

If a user firewall template or a firewall rule of a template is added, changed, deleted or disabled, this immediately affects all firewall users who are logged in.

Existing connections are interrupted. One exception is changing user firewall rules if the function *"Abort existing connections upon firewall reconfiguration"* is deactivated under **Network Security** >> **Packet Filter** >> **Advanced**. In this case, a network connection that exists due to a previously permitted rule is not interrupted.

> If a firewall rule record (template) is disabled, affected logged in firewall users still appear as *logged in*. However, the firewall rules from the **disabled** template no longer apply to them.
>
> If a firewall rule record (template) is **disabled** and then **enabled** again, affected logged in firewall users must first log out and then log in again to reactivate the firewall rules from the template for themselves.

8.4.1 User Firewall Templates

All defined user firewall templates are listed here. A template can consist of several firewall rules. A template can be assigned to several users.

Defining a new template:

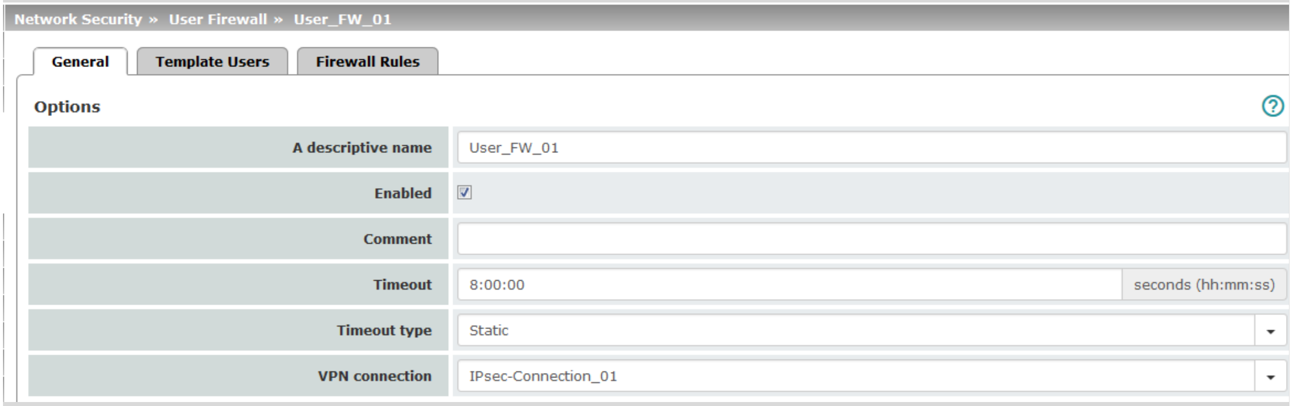
- In the template table, click on the **Insert Row** icon to add a new table row.
- Click on the **Edit Row** icon.

Editing a template:

- Click on the **Edit Row** icon in the relevant row.

Network Security >> User Firewall >> User Firewall Templates		
	Enabled	Activates/deactivates the relevant template.
	A descriptive name	The name of the template. The name is specified when the template is created.
General	The following tab page appears when you click on the **Edit Row** icon:	

Network Security >> User Firewall >> User Firewall Templates [...]



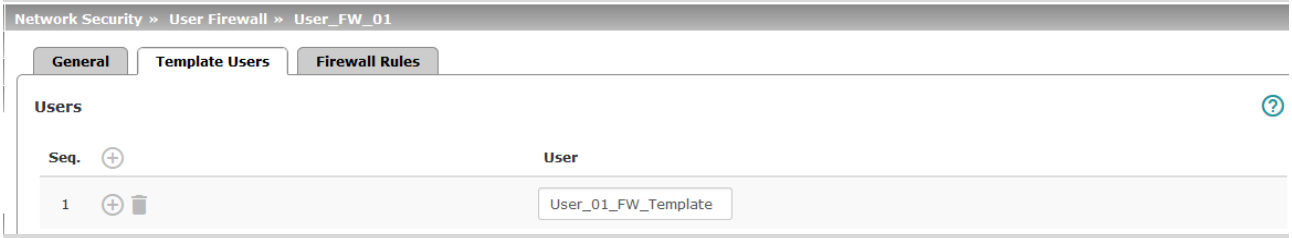
Options	**A descriptive name**	The user firewall template can be freely named/renamed.
	Enabled	When the function is activated, the user firewall template becomes active as soon as firewall users log into the mGuard who are listed on the *Template Users* tab page (see below) and who have been assigned this template. It does not matter from which computer and under what IP address the user logs in. The assignment of the firewall rules to a user is based on the authentication data that the user enters during login (user name, password).
	Comment	Optional explanatory text.
	Timeout	Default: 8 hours (8:00:00) Specifies the time at which point the firewall rules are deactivated. If the user session lasts longer than the timeout time specified here, the user has to log in again. The entry can be in seconds [ss], minutes and seconds [mm:ss] or hours, minutes, and seconds [hh:mm:ss].

Network Security >> User Firewall >> User Firewall Templates [...]		
	Timeout type	**Static / Dynamic** With a **static timeout**, users are logged out automatically as soon as the set timeout time has elapsed. With **dynamic timeout**, users are logged out automatically after all the connections have been closed by the user or have expired on the mGuard, and the set timeout time has **subsequently** elapsed. An mGuard connection is considered to have expired if no more data is sent for this connection over the following periods.
	Connection expiration period after non-usage: – TCP: 5 days (this value can be set, see "Timeout for established TCP connections" on page 281). 120 seconds are added after closing the connection. (These 120 seconds also apply to connections closed by the user.) – UDP: 30 seconds after data traffic in one direction; 180 seconds after data traffic in both directions – ICMP: 30 seconds – Others: 10 minutes	
	VPN connection	Specifies the VPN connection for which this user firewall rule is valid. This requires existing remote access through the VPN tunnel to the web interface.

Network Security >> User Firewall >> User Firewall Templates >> Edit > ...

Template Users

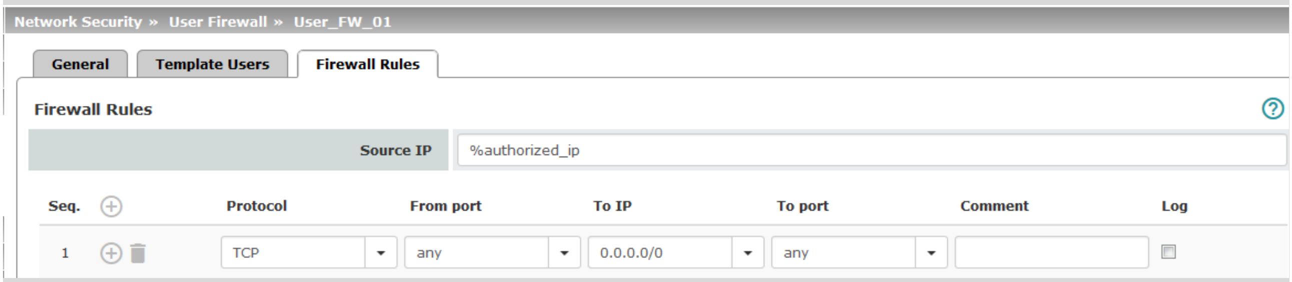
Specify the names of the users here. The names must correspond to those that have been defined under the Authentication >> Firewall Users menu (see Page 235).



Firewall Rules

Firewall rules for the user firewall templates.

When the template is configured with **dynamic timeout** approved UDPs and other network packets (excluding ICMP), reset the dynamic timeout to the initial value.



Source IP

IP address from which connections are allowed to be established. If this should be the address from which the user logged into the mGuard, the placeholder “%authorized_ip” should be used.

> If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored.

Protocol

All means TCP, UDP, ICMP, GRE, and other IP protocols.

From port / To port

(Only for TCP and UDP protocols)

any refers to any port.

startport:endport (e.g., 110:120) > port range.

Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110).

Name of port groups, if defined. When a name is specified for a port group, the ports or port ranges saved under this name are taken into consideration (see "IP/Port Groups" on page 275).

Network Security >> User Firewall >> User Firewall Templates >> Edit > ... [...]		
	To IP	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 26). **Name of IP groups**, if defined. When a name is specified for an IP group, the host names, IP addresses, IP areas or networks saved under this name are taken into consideration (see "IP/Port Groups" on page 275). If host names are used in IP groups, the mGuard must be configured so that the host name of a DNS server can be resolved in an IP address. If a host name from an IP group cannot be resolved, this host will not be taken into consideration for the rule. Further entries in the IP group are not affected by this and are taken into consideration.
	Comment	Freely selectable comment for this rule.
	Log	For each firewall rule, you can specify whether the use of the rule: – Should be logged – activate *Log* function – Should not be logged – deactivate *Log* function (default)

9 CIFS Integrity Monitoring menu

CIFS Integrity Monitoring is **not** available on the **FL MGUARD RS2000, TC MGUARD RS2000 3G, TC MGUARD RS2000 4G**, and **FL MGUARD RS2005**.

It must **not** be used on the **FL MGUARD BLADE controller**.

In Stealth network mode, CIFS integrity checking is not possible without a management IP address.

The **CIFS-Anti-Virus-Scan-Connector** function is no longer supported from mGuard firmware version 8.5.

CIFS Integrity Checking

When **CIFS Integrity Checking** is performed, the Windows network drives are checked to determine whether certain files (e.g., *.exe, *.dll) have been changed. Changes to these files indicate a possible virus or unauthorized intervention.

Setting options for CIFS Integrity Checking

- Which network drives are known to the mGuard (see "CIFS Integrity Monitoring >> Importable Shares" on page 298).
- What type of access is permitted (see "CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings" on page 301).
- At what intervals the drives should be checked (see "CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit >> Checked Share" on page 303).
- Which file types should be checked (see "CIFS Integrity Monitoring >> CIFS Integrity Checking >> Filename Patterns >> Edit" on page 310).

Warning method when a change is detected (e.g., via e-mail, see "CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings" on page 301 or via SNMP, see "CIFS Integrity Traps" on page 105).

9.1 CIFS Integrity Monitoring >> Importable Shares

Requirements

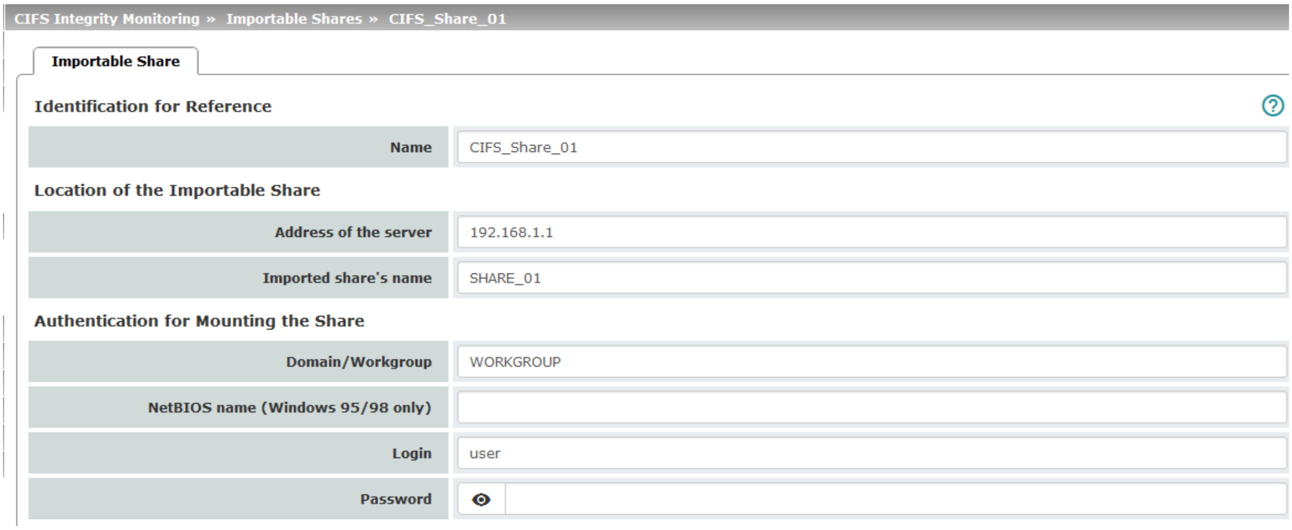
The network drives that the mGuard should check regularly can be specified here.

> In order for the network drives to be checked, you must also refer to these network drives in the CIFS Integrity Check.

You can set the reference to the network drive for the CIFS integrity check, see "Checked CIFS share" on page 302.

9.1.1 Importable Shares

CIFS Integrity Monitoring >> Importable Shares		
Importable CIFS Shares	**Name**	Name of the network drive to be checked (Internal name used in the configuration).
	Address of the server	IP address or DNS host name of the authorizing server.
	Name of the imported network drive	Share name of the network drive that is to be checked. Click on the **Edit Row** icon to specify the settings.



CIFS Integrity Monitoring >> Importable Shares >> Edit		
Identification for Reference	**Name**	Name of the network drive to be checked (Internal name used in the configuration).
Location of the Importable Share	**Address of the server**	IP address or DNS host name of the authorizing server.
	Imported share's name	Share name of the network drive that is to be checked.
Authentication for Mounting the Share	**Domain/Workgroup**	Name of the workgroup to which the network drive belongs.
	NetBIOS name (Windows 95/98 only)	NetBIOS name for Windows 95/98 computers.
	Login	Login (user identifier) for the server.
	Password	Password for login.

9.2 CIFS Integrity Monitoring >> CIFS Integrity Checking

When **CIFS Integrity Checking** is performed, the Windows network drives are checked to determine whether certain files (e.g., *.exe, *.dll) have been changed. Changes to these files indicate a possible virus or unauthorized intervention.

Integrity database

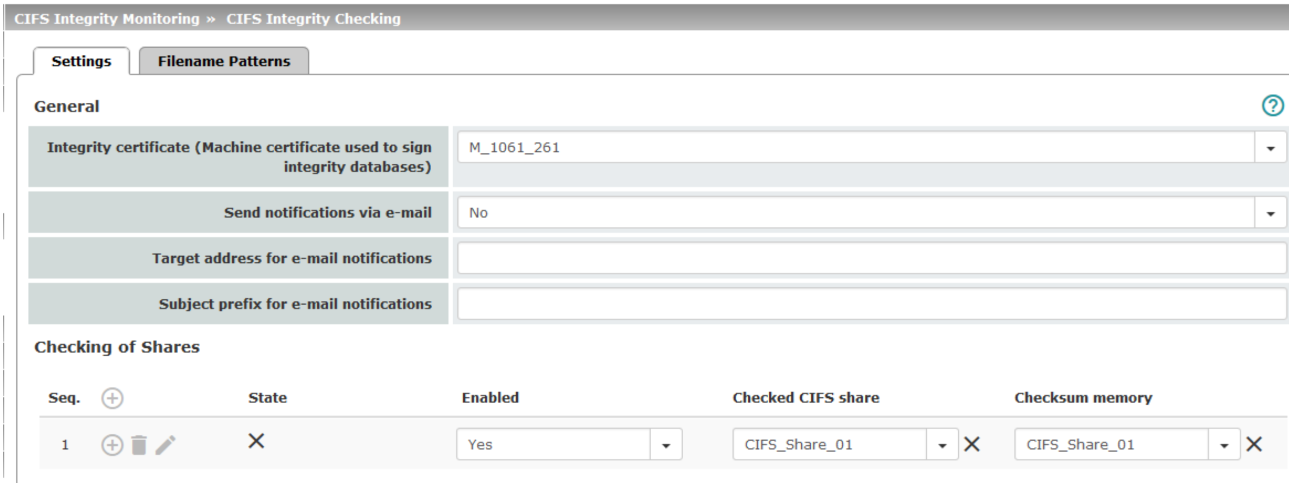
If a network drive that is to be checked is reconfigured, an integrity database must be created.

This integrity database is used as the basis for comparison when checking the network drive regularly. The checksums of all files to be monitored are recorded here. The integrity database is protected against manipulation.

The integrity database is either created explicitly due to a specific reason (see *CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit >> Management*, *Actions*) or on the first regular check of the drive.

> The integrity database must be created again following intentional manipulation of the relevant files of the network drive. Unauthorized manipulation of the relevant files cannot be detected if there is no (valid) integrity database.

9.2.1 Settings



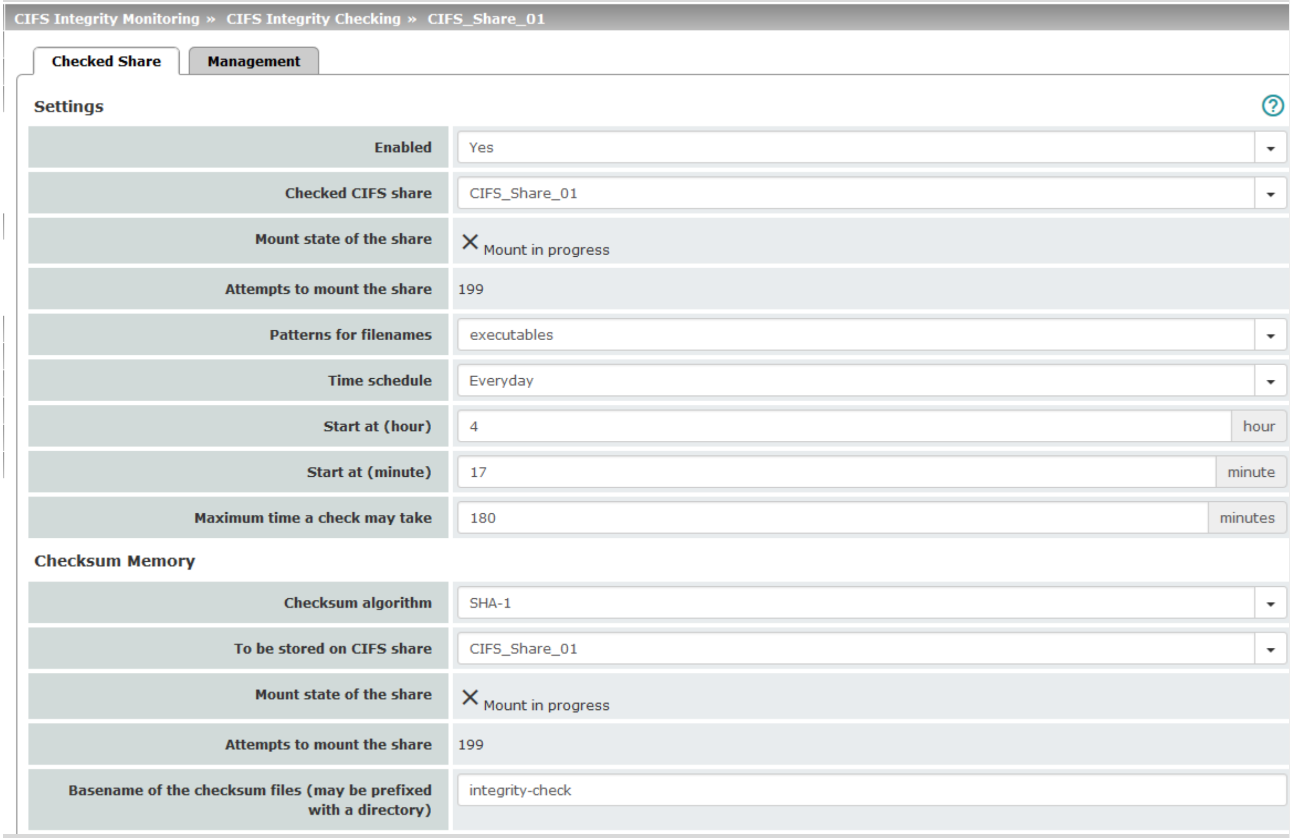
CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings		
General	**Integrity certificate (machine certificate used to sign integrity databases)**	Used to sign and check the integrity database so that it cannot be replaced or manipulated by an intruder without being detected. For information about certificates, please refer to "Machine Certificates" on page 248.
	Send notifications via e-mail	**After every check**: an e-mail is sent to the address specified below after every check. **No**: an e-mail is not sent to the address specified below. **Just in case of a failure or difference**: an e-mail is sent to the address specified below if a deviation is detected during CIFS Integrity Checking or if the check could not be carried out due to an access error.
	Target address for e-mail notifications	An e-mail is sent to this address either after every check or only if a deviation is detected during CIFS Integrity Checking or if the check could not be carried out due to an access error.
	Subject prefix for e-mail notifications	Text entered in the subject field of the e-mail.

CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings [...]		
Checking of Shares (If network drives are defined)	**State**	State of the network drive: – The network drive has not yet been checked. Probably no integrity database. – Last check finished successfully. – The process failed due to an unforeseen condition. Please consult the logs. – Last check was aborted due to timeout. – The integrity database is missing or incomplete. – The signature of the integrity database is invalid. – The integrity database was created with a different hash algorithm. – The integrity database is the wrong version. – The share which is to be checked is not available. – The share which is to be used as checksum memory is not available. – A file could not be read due to an I/O failure. Please consult the report. – The directory tree could not be traversed due to an I/O failure. Please consult the report. – All files in the share can be accessed successfully. An integrity check is possible.
	Enabled	**Yes**: a check is triggered regularly for this network drive. **No**: a check is not triggered for this network drive. The mGuard has not connected this drive. The status cannot be viewed. **Suspended**: the check has been suspended until further notice. The status can be viewed.
	Checked CIFS share	Name of the network drive to be checked (specified under *CIFS Integrity Monitoring* >> *Importable Shares* >> *Edit*).
	Checksum memory	In order to perform the check, the mGuard must be provided with a network drive for storing the files. The checksum memory can be accessed via the external network interface.
Action	Click on the ✎ **Edit Row** icon to make further settings for checking network drives.	

Settings >> Checking of Shares >> Edit >> Checked Share

(see below)

CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit >> Checked Share		



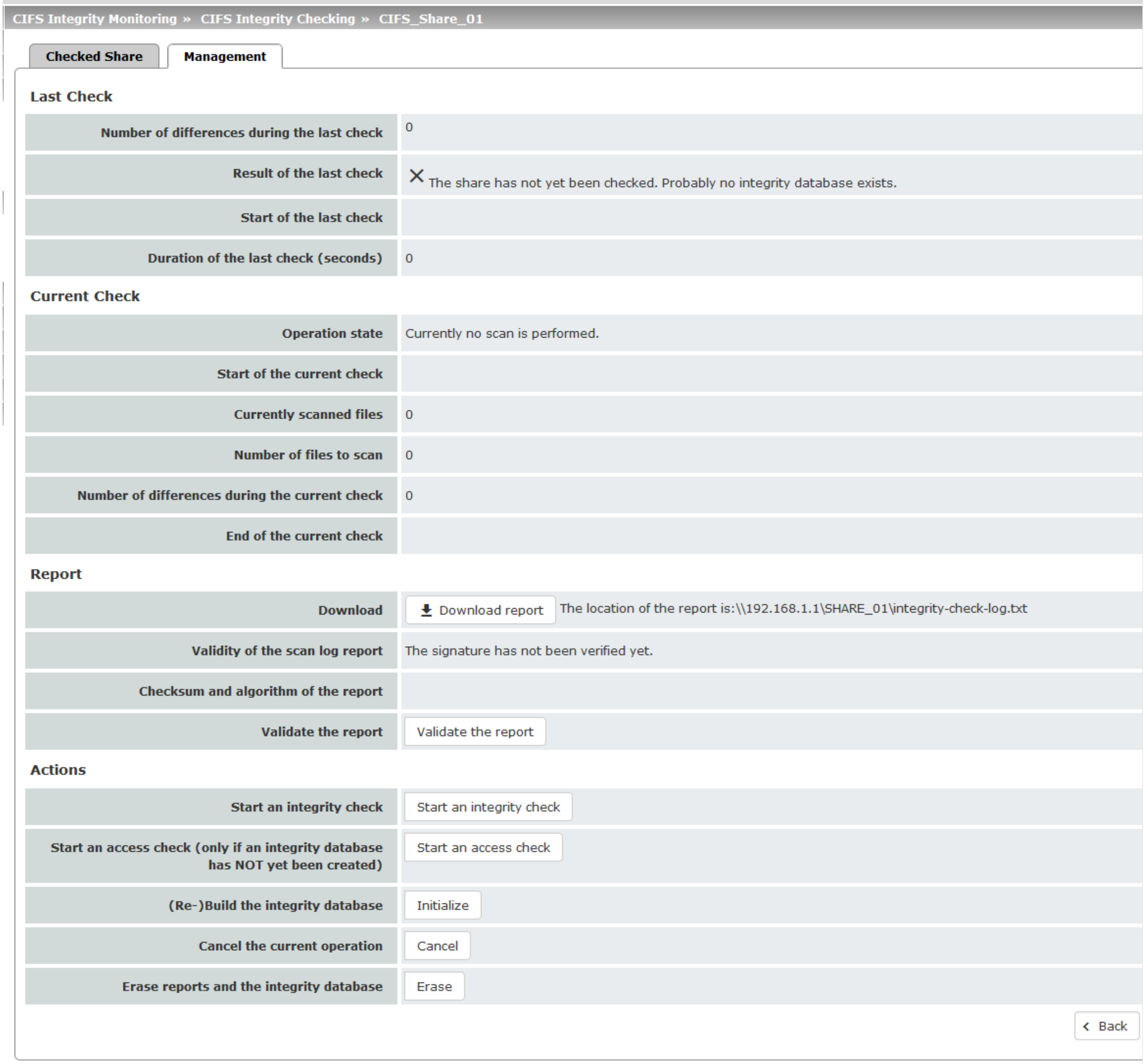
Settings	**Enabled**	**Yes**: a check is triggered regularly for this network drive. **No**: a check is not triggered for this network drive. The mGuard has not connected this drive. The status cannot be viewed. **Suspended**: the check has been suspended until further notice. The status can be viewed.
	Checked CIFS share	Name of the network drive to be checked (specified under *CIFS Integrity Monitoring >> Importable Shares >> Edit*).
	Mount state of the share	Shows the mount state of the network drive.
	Attempts to mount the share	Number of failed attempts to mount the network drive since its last reconfiguration or after restarting the mGuard.

CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit >> Checked Share [...]		
	Patterns for filenames	Specific file types are checked (e.g., only executable files such as *.exe and *.dll). The rules can be defined under *CIFS Integrity Monitoring >> CIFS Integrity Checking >> Filename Patterns >> Edit*. Do not check files that are changed in normal operation, as this could trigger false alarms. Do not check files that are simultaneously opened **exclusively** by other programs, as this can lead to access conflicts.
	Time schedule	Every Sunday, Every Monday, Every Tuesday, ... , Everyday, Several times a day, Continuous You can start the check every day, several times a day or on a specific weekday. The mGuard system time must be set for the time schedule to work properly. Integrity checks are not performed if the system time is not synchronized. This can be carried out manually or via NTP (see "Time and Date" on page 46). A check is only started if the mGuard is operating at the set time. If it is not operating at the time, a check is not performed later when the mGuard is started up again. If the previous check is still running at the time of the next start, the start of the next check will be postponed accordingly. If a check were set to start in less than one minute due to reconfiguration, it will not be restarted until the next interval. The check can also be started manually (see *CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit >> Management, Actions*).
	Start at (hour)	Time at which the check starts (hour). If “Several times a day” is selected, every 1 h, 2 h, 3 h, 4 h, 6 h, 8 h, 12 h
	Start at (minute)	Time at which the check starts (minute). If “Several times a day” is selected, every 1 h, 2 h, 3 h, 4 h, 6 h, 8 h, 12 h

CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit >> Checked Share [...]		
	Maximum time a check may take	Maximum duration of the check sequence in minutes. You can therefore ensure that the check is completed in good time (e.g., before a shift starts).
Checksum memory	**Checksum Algorithm**	**MD5, SHA-1, SHA-256** (Default) Checksum algorithms such as MD5, SHA-1 or SHA-256 are used to check whether a file has been changed. SHA-256 is more secure than SHA-1, but it takes longer to process. The use of MD5 and SHA-1 is no longer recommended for security reasons (see "Using secure encryption and hash algorithms" on page 19).
	To be stored on CIFS share	In order to perform the check, the mGuard must be provided with a network drive for storing the files. The checksum memory can be accessed via the external network interface. The same network drive can be used as the checksum memory for several different drives to be checked. The base name of the checksum files must then be clearly selected in this case. The mGuard recognizes which version the checksum files on the network drive must have. For example, if it is necessary to restore the contents of the network drive from a backup following a malfunction, old checksum files are provided in this case and the mGuard would detect the deviations. In this case, the integrity database must be recreated (see *CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit >> Management, Actions*).
	Mount state of the share	Shows the mount state of the network drive.
	Attempts to mount the share	Number of attempts to mount the network drive since its last reconfiguration or after restarting the mGuard.
	Basename of the checksum files (may be prefixed with a directory)	The checksum files are stored on the network drive specified above. They can also be stored in a separate directory. The directory name must not start with a backslash (\). Example: Checksumdirectory\integrity-checksum “Checksumdirectory” is the directory and contains the files beginning with “integrity-checksum”.

Settings >> Checking of Shares >> Edit >> Management

CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit >> Management



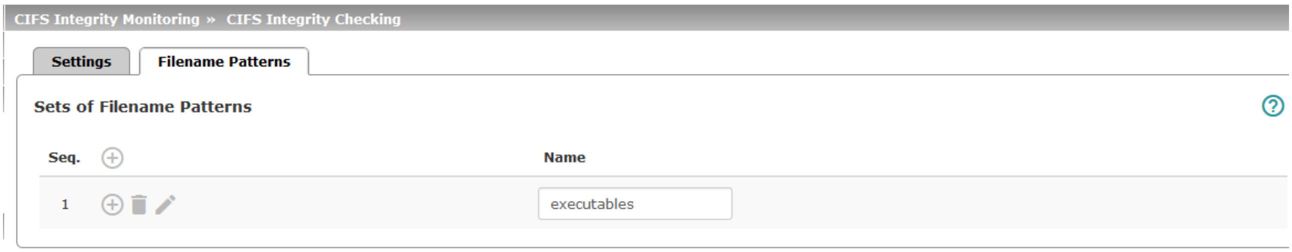
Last Check (Results are only displayed if a check has been carried out.)	**Number of differences during the last check**	Number of differences detected on the network drive.
	Result of the last check	The result of the last check (see "State" on page 302).

CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit >> Management [...]		
	Start of the last check	Weekday, month, day, HH:MM:SS (UTC). The local time may differ from this time. **Example**: the standard time in Germany is Central European Time (CET), which is UTC plus one hour. Central European Summer Time applies in summer, which is UTC plus two hours.
	Duration of the last check (seconds)	Duration of the check in seconds.
Current Check (Results are only displayed if a check has been carried out.)	**Operation state**	Current operating state during the check: – Currently no scan is performed. – Scanning of this share is suspended. – Currently the share is being checked. – Currently an integrity database is being created. – Currently access permissions are checked.
	Start of the current check	Starting point of the current integrity check.
	Currently scanned files	Number of files scanned during the current check.
	Number of files to scan	Total number of files to scan.
	Number of differences during the current check	Number of differences detected on the network drive.
	End of the current check	Estimated completion time for the check.
Report	**Download**	The report is displayed here. It can be downloaded by clicking on the “**Download report**” button. The report is stored on the checked network drive as a log file with the file name “integrity-check-log.txt”. On every check, the results of the new check are added to the log file. When the file size reaches 32 MB, the file is renamed “integrity-check-log.txt.1” (backup file). A new log file (“integrity-check-log.txt”) containing the results of the current check is created. When this file reaches 32 MB, it is likewise renamed “integrity-check-log.txt.1” and the existing “integrity-check-log.txt.1” file is irrevocably overwritten. The integrity of the log files is ensured by creating checksums. Click on the “**Validate the report**” button to check whether the report is unchanged from the definition in the mGuard (according to the signature and certificate).

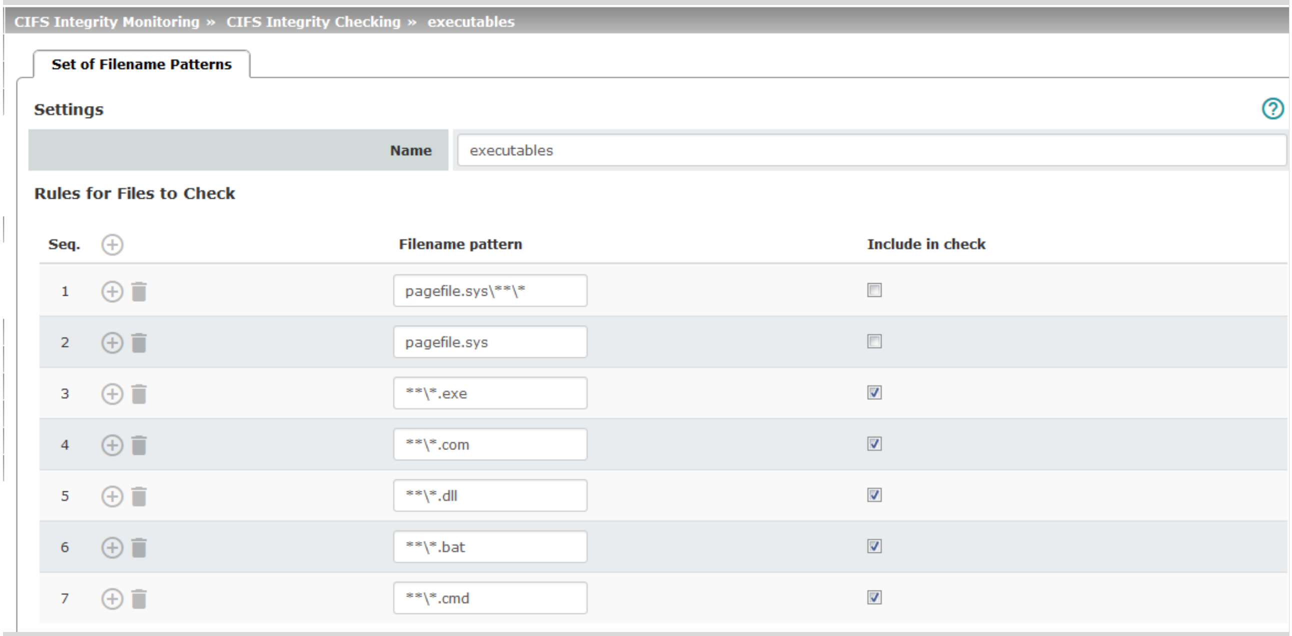
CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit >> Management [...]		
	Validity of the scan log report	Result of the signature check: – The signature has not been verified yet. – The signature is valid. – ERROR: The report is missing. – ERROR: The report does not belong to this device or is not up to date. – ERROR: The report was created with a different checksum algorithm. – ERROR: The report was tampered with. – ERROR: The test report is not available. Check whether the network drive is connected (mounted).
	Checksum and algorithm of the report	Checksum and algorithm
	Validate the report	The signature for the report is checked.
Actions	**Start an integrity check**	Click on the **Start an integrity check** button to start the integrity check. The result of the check can be viewed in the report by clicking on the **Download report** button. Before an **integrity check** is performed, an **integrity database** must be created first.
	Start an access check (only if an integrity database has NOT yet been created)	**NOTE: An existing integrity database will be deleted.** Only start the **access check** if an **integrity database** has not yet been created or a new one needs to be created. Click on the **Start an access check** button to check whether there are files present on the imported network drive that the mGuard cannot access. More comprehensive **creation of the integrity database** is therefore not aborted in the absence of the proper access permissions. After an **access check**, the **integrity database** must be created again by clicking on the **Initialize** button (see below). The result of the check can be viewed in the report by clicking on the **Download report** button.

CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit >> Management [...]		
	(Re-)Build the integrity database	Before creating an integrity database, an **access check** should be performed first. The absence of the proper access permissions can therefore be detected at an early stage. **An existing integrity database will be deleted by an access check.** The mGuard creates a database with checksums in order to check whether files have been changed. A change to executable files indicates a virus. However, if these files have been changed intentionally, a new database must be created by clicking on the **Initialize button** in order to prevent false alarms. The creation of an integrity database is also recommended if network drives have been newly set up. Otherwise, an integrity database is set up during the first scheduled check instead of a check being performed (if an **access check** was not performed first).
	Cancel the current procedure	Click on the **Cancel** button to stop the integrity check.
	Erase reports and the integrity database	Click on the **Erase** button to delete all existing reports/databases. A new integrity database must be created for any further integrity checks. This can be initiated by clicking on the **Initialize** button**.** Otherwise, a new integrity database is created automatically on the next scheduled check (if an **access check** was not performed first). This procedure cannot be seen.

9.2.2 Filename Patterns



CIFS Integrity Monitoring >> CIFS Integrity Checking >> Filename Patterns >> Edit



Sets of Filename Patterns	**Name**	Freely definable name for a set of rules for the files to be checked. This name must be selected under **CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Checking of Shares >> Edit** in order for the pattern to be activated. Click on the **Edit Row** icon to define a set of rules for the files to be checked and save this under the defined name.

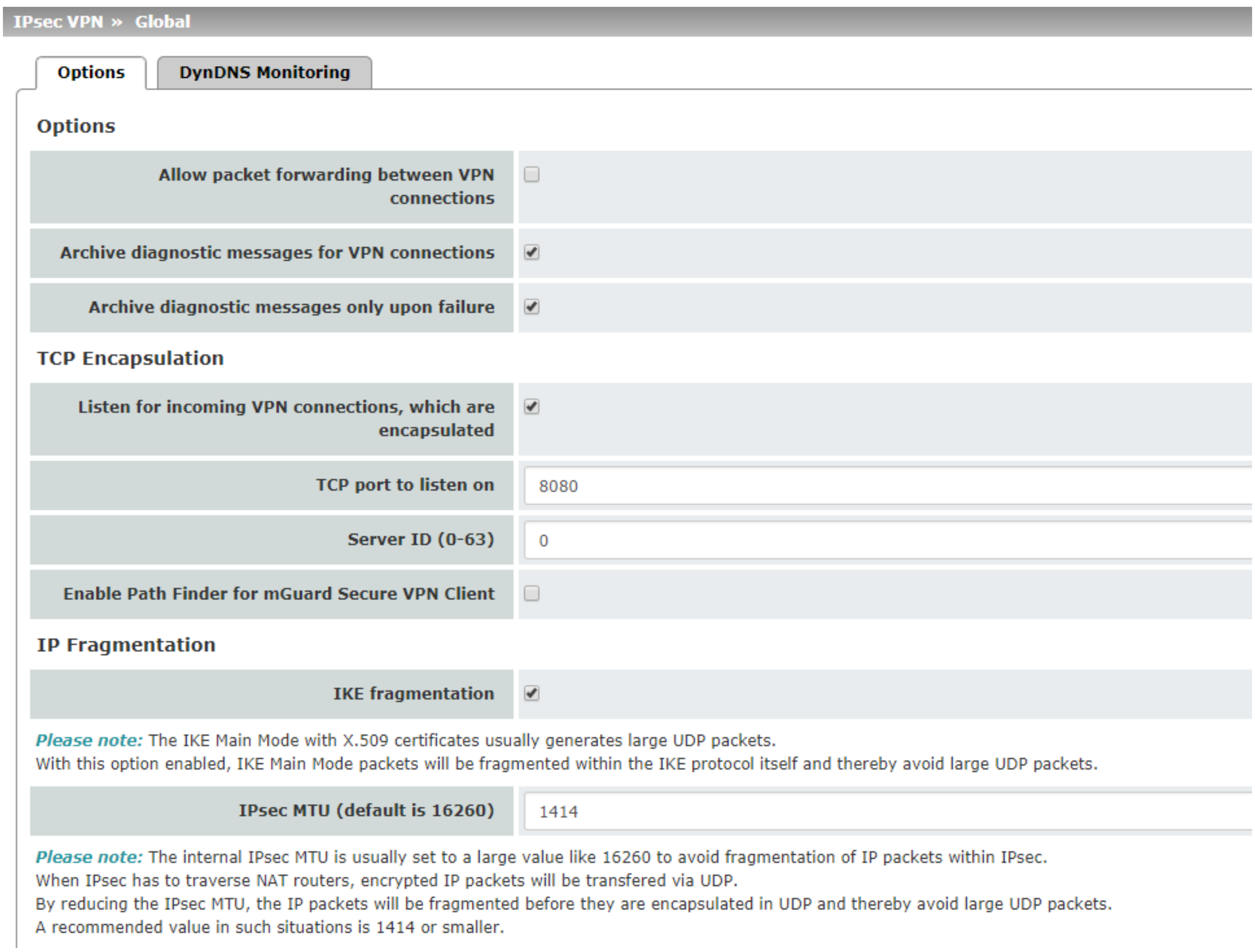
CIFS Integrity Monitoring >> CIFS Integrity Checking >> Set of Filename Patterns >> Edit		
Rules for Files to Check	**Filename pattern**	The following rules apply: ***.exe means that the files located in a specific directory and with file extension *.exe are checked (or excluded). Only one placeholder (*) is permitted per directory or file name. Placeholders represent characters, e.g., win**.exe returns files with the extension *.exe that are located in a directory that begins with *win*... ** at the start means that any directory is searched, even those at the top level (if this is empty). This cannot be combined with other characters (e.g., c** is not permitted). Example: Name***.exe refers to all files with the extension *.exe that are located in the “*Name*” directory and any subdirectories. Missing files trigger an alarm. Missing files are files that were present during initialization. An alarm is also triggered if additional files are present.
	Include in check	**Activate function (include)**: the files are included in the check. (Each file name is compared with the patterns in sequence. The first hit determines whether the file is to be included in the integrity check. The file is not included if no hits are found.) **Deactivate function (exclude**): the files are excluded from the check.

10 IPsec VPN menu

This menu is **not** available on the **FL MGUARD BLADE controller**.

10.1 IPsec VPN >> Global

10.1.1 Options



IPsec VPN >> Global >> Options		
Options	**Allow packet forwarding between VPN connections**	This function is only required on an mGuard communicating between two different VPN peers. To enable communication between two VPN peers, the local network of the communicating mGuard must be configured so that the remote networks containing the VPN peers are included. The opposite setup (local and remote network swapped round) must also be implemented for the VPN peers (see "Remote NAT for IPsec tunnel connections" on page 340). The function is not supported in *Stealth* network mode. When the **function is deactivated** (default): VPN connections exist separately. There is no packet forwarding between the configured VPN connections. When the **function is activated**: “hub and spoke” feature enabled: acting as a control center, the mGuard diverts VPN connections to several branches that can then also communicate with each other. The setting is also valid for OpenVPN and GRE connections. With a star VPN connection topology, mGuard peers can also exchange data with one another. In this case, it is recommended that the local mGuard consults CA certificates for the authentication of peers (see "Authentication" on page 344). In the case of “hub and spoke”, 1:1 NAT of the peer is not supported.

IPsec VPN >> Global >> Options [...]		
	Archive diagnostic messages for VPN connections	**Function deactivated (default)** If errors occur when establishing VPN connections, the mGuard logging function can be used to find the source of the error based on corresponding entries (see *Logging >> Browse Local Logs* menu item). This option for error diagnostics is used as standard. If it is sufficient, you can deactivate the function at this point. **Function activated** If the option of diagnosing VPN connection problems using the mGuard logging function is too impractical or insufficient, select this option. This may be the case if the following conditions apply: – In certain application environments, e.g., when the mGuard is “operated” by means of a machine controller via the CMD contact (*only for FL MGUARD RS4000/RS2000, TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4004/RS2005*, and *FL MGUARD RS, FL MGUARD GT/GT*), the option for a user to view the mGuard log file via the web-based user interface of the mGuard may not be available at all. – When used remotely, it is possible that a VPN connection error can only be diagnosed after the mGuard is temporarily disconnected from its power source – which causes all the log entries to be deleted. – The relevant log entries of the mGuard that could be useful may be deleted because the mGuard regularly deletes older log entries on account of its limited memory capacity. – If an mGuard is being used as the central VPN peer, e.g., in a remote maintenance center as the gateway for the VPN connections of numerous machines, the messages regarding activity on the various VPN connections are logged in the same data stream. The resulting logging volume makes it time-consuming to find the information relevant to one error.

IPsec VPN >> Global >> Options [...]		
		After archiving is enabled, relevant log entries about the operations involved in establishing VPN connections are archived in the non-volatile memory of the mGuard if the connections are established as follows: – Via the CMD contact – Via text message – Via the “Start” icon on the web interface – Via the CGI interface nph-vpn.cgi using the “synup” command (see application note: “How to use the CGI Interface”). (Application notes are available in the download area of phoenixcontact.net/products.) – Archived log entries are not affected by a restart. They can be downloaded as part of the support snapshot (*Hardware* menu item). A snapshot provides your supplier's support team with additional options for more efficient troubleshooting than would be possible without archiving.
	Archive diagnostic messages only upon failure (Only when **Archiving** is activated)	If only log entries generated for failed connection attempts are to be archived, activate the function. When the function is deactivated, all log entries will be archived.

TCP encapsulation

This function is used to encapsulate data packets to be transmitted via a VPN connection in TCP packets. Without this encapsulation, under certain circumstances it is possible for VPN connections that important data packets belonging to the VPN connection may not be correctly transmitted due to interconnected NAT routers, firewalls or proxy servers, for example.

Firewalls, for example, may be set up to prevent any data packets of the UDP protocol from passing through or (incorrectly implemented) NAT routers may not manage the port numbers correctly for UDP packets.

TCP encapsulation avoids these problems because the packets belonging to the relevant VPN connection are encapsulated in TCP packets, i.e., they are hidden so that only TCP packets appear for the network infrastructure.

The mGuard may receive VPN connections encapsulated in TCP, even when it is positioned behind a NAT gateway in the network and thus cannot be reached by the VPN peer under its primary external IP address. To do this, the NAT gateway must forward the corresponding TCP port to the mGuard (see "Listen for incoming VPN connections, which are encapsulated" on page 319).

> TCP encapsulation can only be used if an mGuard (Version 6.1 or later) is used at both ends of the VPN tunnel. The "Path Finder" function can be used from version 8.3 and also functions with the mGuard Secure VPN Client.

> TCP encapsulation should only be used if required, because connections are slowed down by the significant increase in the data packet overhead and by the correspondingly longer processing times.

> If the mGuard is configured to use a proxy for HTTP and HTTPS in the *Network >> Proxy Settings* menu item, then this proxy is also used for VPN connections that use TCP encapsulation.

> TCP encapsulation supports the *basic authentication* and *NTLM* authentication methods for the proxy.

> For the TCP encapsulation to work through an HTTP proxy, the proxy must be named explicitly in the proxy settings (*Network >> Proxy Settings* menu item) (i.e., it must not be a transparent proxy) and this proxy must also understand and permit the HTTP method CONNECT.

> To use the “Path Finder” function to establish a VPN connection to an mGuard Secure VPN Client, the function must be enabled on both sides of the connection (server and client).

> TCP encapsulation does not work in conjunction with authentication via pre-shared key (PSK).

> TCP encapsulation only works if one of the two ends is waiting for connections (**connection initiation: wait**) and is given as **address of the "%any" peer VPN gateway**.

TCP encapsulation with enabled “Path Finder” function

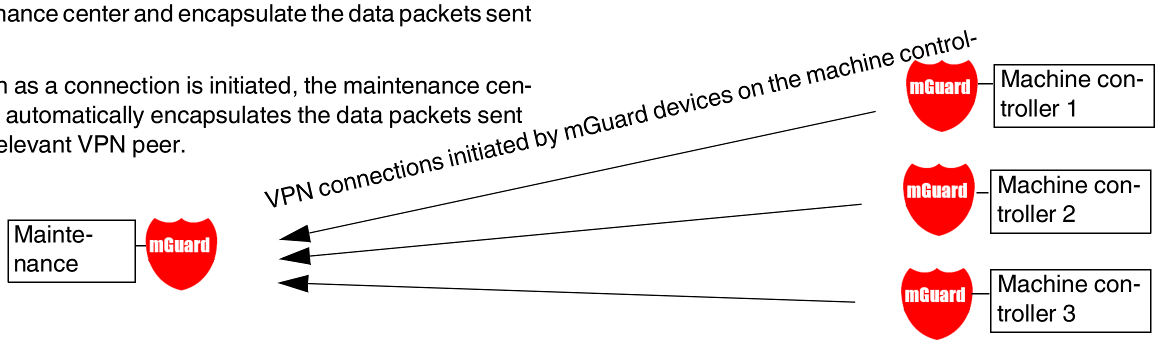
TCP encapsulation with enabled “Path Finder” function improves the behavior of the standard TCP encapsulation described above.

When the connection has been newly set up and no reverse compatibility is required, the Path Finder function should be used.

If a VPN connection is started by the mGuard Secure VPN Client, which is positioned behind a proxy server or a firewall, the “Path Finder” function must be enabled in the mGuard Secure VPN Client as well as in the mGuard (server). The data packets to be transmitted via the VPN connection are encapsulated in TCP packets (see "TCP encapsulation" on page 317).

As devices in the TCP encapsulation, the mGuard devices for the machine controllers initiate VPN data traffic to the maintenance center and encapsulate the data packets sent to it.

As soon as a connection is initiated, the maintenance center also automatically encapsulates the data packets sent to the relevant VPN peer.



Maintenance center mGuard

Required basic settings

- **IPsec VPN >> Global >> Options**:
  - Listen for incoming VPN connections, which are encapsulated: **activated**
- **IPsec VPN >> Connections >> General**:
  - Address of the remote site's VPN gateway: **%any**
  - Connection startup: **Wait**

mGuard devices on machine controllers

Required basic settings

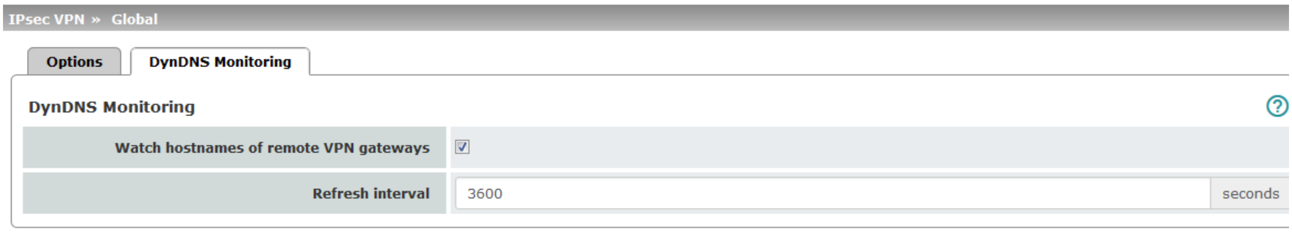
- **IPsec VPN >> Global >> Options**:
  - Listen for incoming VPN connections, which are encapsulated: **deactivated**
- **IPsec VPN >> Connections >> General**:
  - Address of the remote site's VPN gateway: **fixed IP address or host name**
  - Connection startup: **Initiate** or **Initiate on traffic**
  - Encapsulate the VPN traffic in TCP: **TCP encapsulation or Path Finder**

Figure 10-1 TCP encapsulation in an application scenario with a maintenance center and machines maintained remotely via VPN connections

IPsec VPN >> Global >> Options		
TCP encapsulation	**Listen for incoming VPN connections, which are encapsulated**	Default setting: **deactivated** Only activate this function if the TCP encapsulation function is used. Only then can the mGuard allow connection establishment with encapsulated packets. For technical reasons, the RAM requirements increase with each interface that is used to listen out for VPN connections encapsulated in TCP. If multiple interfaces need to be used for listening, then the device must have at least 64 Mbytes of RAM. The interfaces to be used for listening are determined by the mGuard according to the settings on the active VPN connections that have "%any" configured as the peer. The decisive setting is specified under "Interface to use for gateway setting %any".
	TCP port to listen on (For TCP encapsulation)	**Default: 8080** Number of the TCP port where the encapsulated data packets to be received arrive. The port number specified here must be the same as the one specified for the mGuard of the peer as the **TCP port of the server, which accepts the encapsulated connection** (*IPsec VPN* >> *Connections* menu item, Edit, *General* tab page). The following restriction applies: The port to be used for listening must not be identical to: – A port that is being used for remote access (SSH, HTTPS or SEC-Stick) – The port which is used for listening with enabled *Path Finder* function
	Server ID (0-63) (For TCP encapsulation)	The default value **0** does not usually have to be changed. The numbers are used to differentiate between different control centers. A different number is only to be used in the following scenario: an mGuard connected upstream of a machine must establish connections to two or more different maintenance centers and their mGuard devices with TCP encapsulation enabled.
	Enable Path Finder for mGuard Secure VPN Client	Default setting: **deactivated** Only activate this function if the mGuard should accept a VPN connection from an mGuard Secure VPN Client that is positioned behind a proxy server or a firewall. The "Path Finder" function must also be enabled in the mGuard Secure VPN Client.

IPsec VPN >> Global >> Options [...]		
	TCP port to listen on (For Path Finder)	**Default: 443** Number of the TCP port where the encapsulated data packets to be received arrive. The port number specified here must be the same as the one specified for the VPN client of the peer as the **TCP port of the server**, which accepts the encapsulated connection. The **mGuard Secure VPN Client** always uses port 443 as the destination port. It is when the port is overwritten by a firewall between the mGuard Secure VPN Client and the mGuard that the port in the mGuard has to be changed. **The following restriction applies:** The port to be used for listening must not be identical to: – A port that is being used for remote access (SSH, HTTPS or SEC-Stick) – The port which is used for listening with enabled *TCP encapsulation* function
IP Fragmentation	**IKE fragmentation**	UDP packets can be oversized if an IPsec connection is established between the participating devices via IKE and certificates are exchanged. Some routers are not capable of forwarding large UDP packets if they are fragmented over the transmission path (e.g., via DSL in 1500-byte segments). Some faulty devices forward the first fragment only, resulting in connection failure. If two mGuard devices communicate with each other, it is possible to ensure at the outset that only small UDP packets are to be transmitted. This prevents packets from being fragmented during transmission, which can result in incorrect routing by some routers. If you want to use this option, activate the function. When the function is activated, the setting only takes effect if the peer is an mGuard with firmware Version 5.1.0 or later installed. In all other cases, the setting has no effect, negative or otherwise.
	IPsec MTU (default is 16260)	The option for avoiding oversized IKE data packets, which cannot be routed correctly on the transmission path by faulty routers, can also be applied for IPsec data packets. In order to remain below the upper limit of 1500 bytes often set by DSL, it is recommended that a value of 1414 (bytes) be set. This also allows enough space for additional headers. If you want to use this option, specify a value lower than the default setting.

10.1.2 DynDNS Monitoring



For an explanation of DynDNS, see "DynDNS" on page 209.

IPsec VPN >> Global >> Options		
DynDNS Monitoring	**Watch hostnames of remote VPN gateways**	If the mGuard has the address of a VPN peer in the form of a host name (see "Defining a new VPN connection/VPN connection tunnel" on page 324) and this host name is registered with a DynDNS service, then the mGuard can check the relevant DynDNS at regular intervals to determine whether any changes have occurred. If so, the VPN connection will be established to the new IP address.
	Refresh interval	Default: 300 seconds

10.2 IPsec VPN >> Connections

Requirements for a VPN connection

A general requirement for a VPN connection is that the IP addresses of the VPN partners are known and can be accessed.

- mGuard devices provided in stealth network mode are preset to the “multiple clients” stealth configuration. In this mode, you need to configure a management IP address and default gateway if you want to use VPN connections (see "Default gateway" on page 146). Alternatively, you can select a different stealth configuration than the “multiple clients” configuration or use another network mode.
- In order to successfully establish an IPsec connection, the VPN peer must support IPsec with the following configuration:
  - Authentication via pre-shared key (PSK) or X.509 certificates
  - ESP
  - Diffie-Hellman group (2, 5 and 14 – 18)
  - DES, 3DES or AES encryption
  - MD5- and SHA hash algorithms
  - Tunnel or transport mode
  - XAuth and Mode Config
  - Quick mode
  - Main mode
  - SA lifetime (1 second to 24 hours)

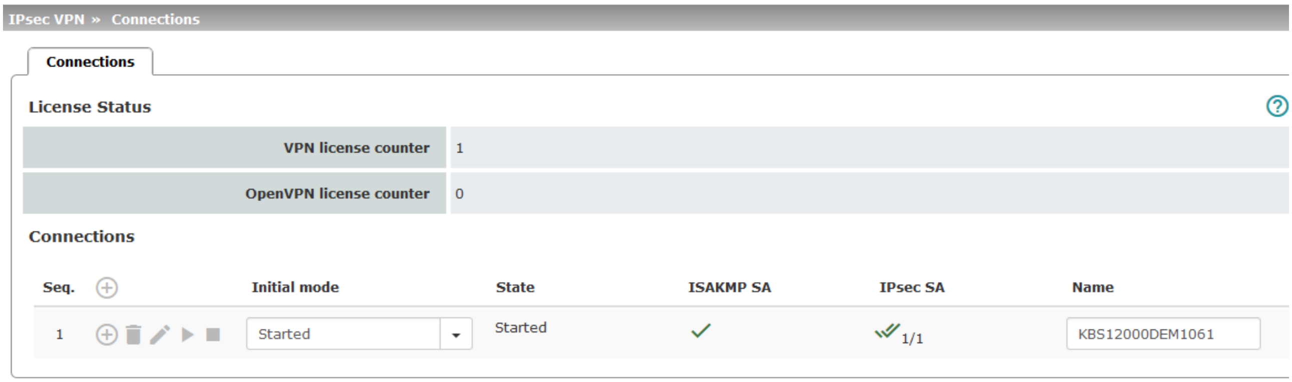
  If the peer is a computer running Windows 2000, the *Microsoft Windows 2000 High Encryption Pack* or at least *Service Pack 2* must be installed.
- If the peer is positioned downstream of a NAT router, the peer must support NAT traversal (NAT-T). Alternatively, the NAT router must know the IPsec protocol (IPsec/VPN passthrough). For technical reasons, only IPsec tunnel connections are supported in both cases.
- Authentication using “Pre-shared key” in Aggressive mode is not supported when using “XAuth”/“Mode Config”. If, e.g., a connection from the iOS or Android client to the mGuard server is created, the authentication must take place via certificate.

Encryption and hash algorithms

Some of the available algorithms are obsolete and are no longer considered secure. This is why they are not to be recommended. For reasons of reverse compatibility however they can still be selected and used in the mGuard.

NOTE: Use secure encryption and hash algorithms (see "Using secure encryption and hash algorithms" on page 19).

10.2.1 Connections



Lists all the VPN connections that have been defined.

Each connection name listed here can refer to an individual VPN connection or a group of VPN connection tunnels. You have the option of defining several tunnels under the transport and/or tunnel settings of the relevant entry.

You also have the option of defining new VPN connections, activating and deactivating VPN connections, changing (editing) the VPN connection or connection group properties, and deleting connections.

IPsec VPN >> Connections		
License Status	**VPN license counter**	Number of peers that currently have a VPN connection established using the IPsec protocol.
	OpenVPN license counter	Number of peers to which a VPN connection is currently established using the OpenVPN protocol.
Connections	**Initial mode**	**Disabled / Stopped / Started** The "**Disabled**" setting deactivates the VPN connection permanently; it cannot be started or stopped. The "**Started**" and "**Stopped**" settings determine the state of the VPN connection after restarting/booting the mGuard (e.g., after an interruption in the power supply). VPN connections that are not deactivated can be started or stopped via icons on the web interface, via text message, a switch, a pushbutton, data traffic or the script nph-vpn.cgi.
	State	Indicates the current activation state of the IPsec VPN connection.
	ISAKMP SA	Indicates whether or not the corresponding ISAKMP SA has been established.
	IPsec SA	Indicates how many of the configured tunnels are established. The number of established tunnels may be higher than the number of configured tunnels, if the "Tunnel Group" function is used.
	Name	Name of the VPN connection

Connections

Defining a new VPN connection/VPN connection tunnel

- In the connection table, click on the ⊕ **Insert Row** icon to add a new table row.
- Click on the **Edit Row** icon.

Editing a VPN connection/VPN connection tunnel

- Click on the **Edit Row** icon in the relevant row.

URL for starting, stopping, querying the status of a VPN connection

The following URL can be used to start and stop VPN connections that are in "**Started**" or "**Stopped**" initial mode or to query their connection status:

Example (only mGuard firmware Version < 8.4.0)

https://server/nph-vpn.cgi?name=verbindung&cmd=(up|down|status)
wget --no-check-certificate "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up"

> Using the command line tool *wget* only functions in combination with mGuard firmware versions < 8.4.0. From mGuard firmware Version 8.4.0, the command line tool *curl* can be used (parameters and options differ!).
>
> Example: *curl --insecure "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up"*

> The admin password and the name that an action relates to may only contain the following characters:
> - Letters: A - Z, a - z
> - Numbers: 0 - 9
> - Characters: - . _ ~
>
> Other characters, such as a space or question mark, must be encoded accordingly (see "Encoding of special characters (URL encoding)" on page 457).

The option ***--no-check-certificate*** (*wget*) or ***--insecure*** (*curl*) ensures that the HTTPS certificate on the mGuard does not undergo any further checking.

A command like this relates to all connection tunnels that are grouped together under the respective name (in this example, *Athen*). This is the name that is listed under *IPsec VPN >> Connections >> Edit >> General* as *"A descriptive name for the connection"* . In the event of ambiguity, the URL call only affects the first entry in the list of connections.

It is not possible to communicate with the individual tunnels of a VPN connection. If individual tunnels are deactivated, they are not started. Starting and stopping in this way therefore has no effect on the settings of the individual tunnels (see "Transport and Tunnel Settings" on page 334).

If the status of a VPN connection is queried using the URL specified above, then the following responses can be expected:

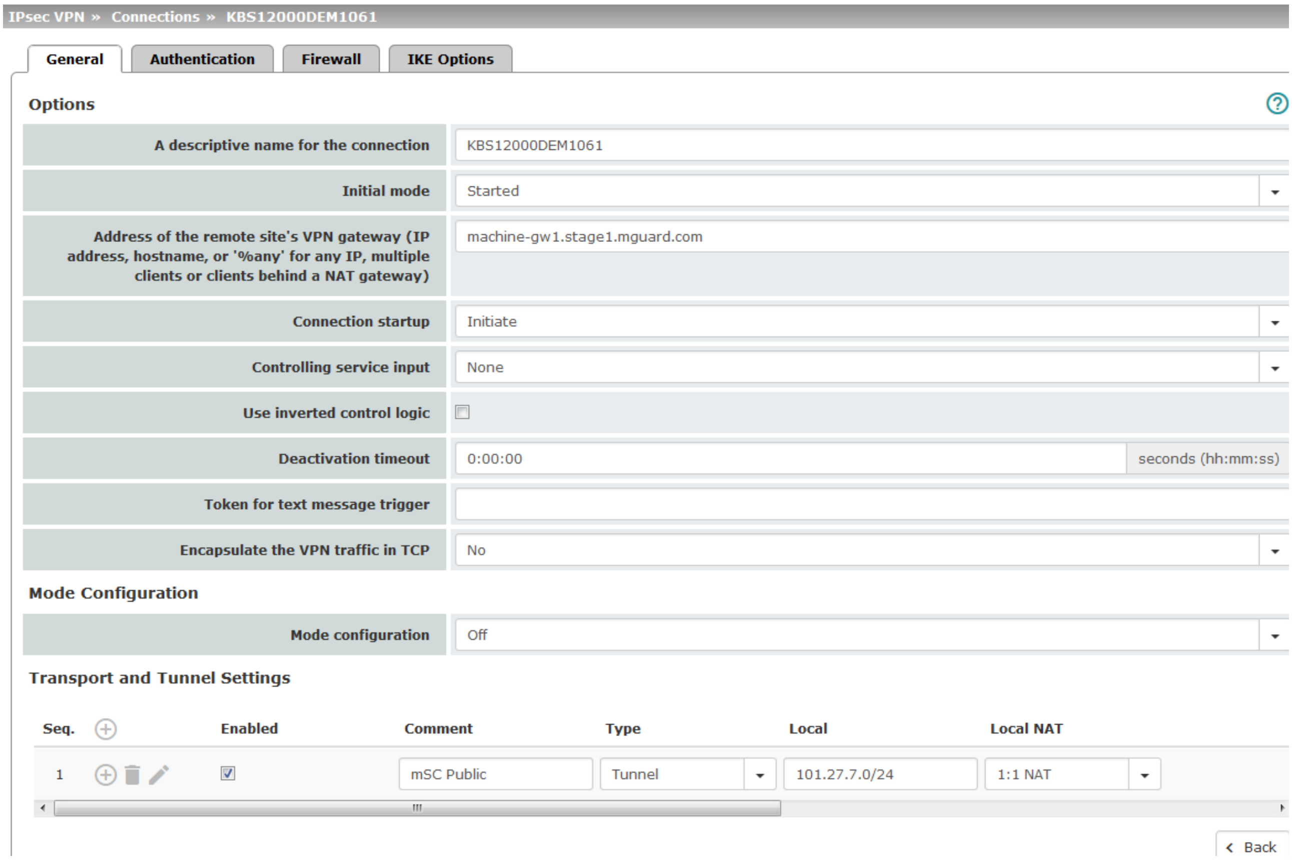
Table 10-1 Status of a VPN connection

Response	Indicates
unknown	A VPN connection with this name does not exist.
void	The connection is inactive due to an error, e.g., the external network is down or the host name of the peer could not be resolved in an IP address (DNS). The response “void” is also issued by the CGI interface, even if no error occurred. If, for example, the VPN connection is deactivated according to the configuration (**No** set in column) and has not been enabled temporarily using the CGI interface or CMD contact.
ready	The connection is ready to establish tunnels or allow incoming queries regarding tunnel setup.
active	At least one tunnel has already been established for the connection.

Defining a VPN connection/VPN connection tunnel

Depending on the network mode of the mGuard, the following page appears after clicking on the **Edit Row** icon.

10.2.2 General



IPsec VPN >> Connections >> Edit >> General		
Options	**A descriptive name for the connection**	The connection can be freely named/renamed. If several connection tunnels are defined under , then this name applies to the entire set of VPN connection tunnels grouped under this name. Similarities between VPN connection tunnels: – Same authentication method, as specified on the *Authentication* tab page (see "Authentication" on page 344) – Same firewall settings – Same IKE options set
	Initial mode	**Disabled / Stopped / Started** The “**Disabled**” setting deactivates the VPN connection permanently; it cannot be started or stopped. The “**Started**” and “**Stopped**” settings determine the status of the VPN connection after restarting/booting the mGuard (e.g., after an interruption in the power supply). VPN connections that are not deactivated can be started or stopped via icons on the web interface, via text message, a switch, a pushbutton, data traffic or the script nph-vpn.cgi.

IPsec VPN >> Connections >> Edit >> General[...]		
	Address of the remote site's VPN gateway	An IP address, host name or **%any** for several peers or peers downstream of a NAT router.

Address of the remote site's VPN gateway

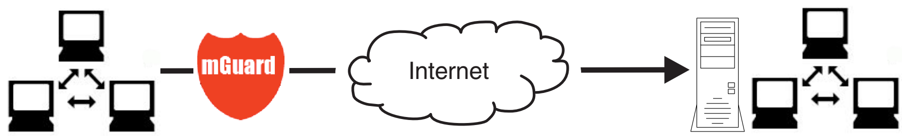


Figure 10-2 The address of the transition to the private network where the remote communication partner is located.

- If the mGuard should actively initiate and establish the connection to the remote peer, specify the IP address or host name of the peer here.
- If the VPN gateway of the peer does not have a fixed and known IP address, the DynDNS service (see glossary) can be used to simulate a fixed and known address.
- If the mGuard should be ready to allow a connection to the local mGuard that was actively initiated and established by a remote peer with any IP address, specify **%any**.

  This setting should also be selected for a VPN star configuration if the mGuard is connected to the control center.

  The mGuard can then be “called” by a remote peer if this peer has been dynamically assigned its IP address (by the Internet service provider), i.e., it has an IP address that changes. In this scenario, you may only specify an IP address if the remote “calling” peer also has a fixed and known IP address.

%any can only be used together with the authentication method using X.509 certificates.

If locally stored CA certificates are to be used to authenticate the peer, the address of the remote site's VPN gateway can be specified explicitly (by means of an IP address or host name) or by **%any**. If it is specified using an explicit address (and not by “%any”), then a VPN identifier (see "VPN Identifier" on page 347) must be specified.

%any must be selected if the peer is located downstream of a NAT gateway. Otherwise, the renegotiation of new connection keys will fail on initial contact.

If **TCP encapsulation** is used (see "TCP encapsulation" on page 317): a fixed IP address or a host name must be specified if this mGuard is to initiate the VPN connection and encapsulate the VPN data traffic.

If this mGuard is installed upstream of a maintenance center to which multiple remote mGuard devices establish VPN connections and transmit encapsulated data packets, **%any** must be specified for the VPN gateway of the peer.

IPsec VPN >> Connections >> Edit >> General		
Options	**Address of the remote site's VPN gateway**	IP address, host name or “%any” for any IP addresses, several peers or peers downstream of a NAT router.

IPsec VPN >> Connections >> Edit >> General [...]		
	Interface to use for gateway setting %any (If **%any** was specified for "**Address of the remote site's VPN gateway**")	**Internal, External, External 2, Dial-in, DMZ, Implicitly chosen by the IP address specified to the right** *External 2* and *Dial-in* are only for devices with a serial interface, see "Network >> Interfaces" on page 127. Selection of the **Internal** option is not permitted in Stealth mode. This interface setting is only considered when "%any" is entered as the address of the remote site's VPN gateway. In this case, the interface of the mGuard through which it answers and permits requests for the establishment of this VPN connection is set here. The VPN connection can be established through the LAN and WAN port in all Stealth modes when **External** is selected. The interface setting allows encrypted communication to take place over a specific interface for VPN peers without a known IP address. If an IP address or host name is entered for the peer, then this is used for the implicit assignment to an interface. The mGuard can be used as a "single-leg router" in Router mode when **Internal** is selected, as both encrypted and decrypted VPN traffic for this VPN connection is transferred over the internal interface. IKE and IPsec data traffic is only possible through the primary IP address of the individual assigned interface. This also applies to VPN connections with a specific peer. **DMZ** can only be selected in Router mode. Here, VPN connections can be established to hosts in the DMZ and IP packets can be routed from the DMZ in a VPN connection. **Implicitly chosen by the IP address below**: an IP address is used instead of a dedicated interface.
	IP address to use for gateway setting %any	IP address that is used for gateway setting **%any**.

IPsec VPN >> Connections >> Edit >> General [...]		
	Connection startup	**Initiate / Initiate on traffic / Wait** **Initiate** The mGuard initiates the connection to the peer. The fixed IP address of the peer or its name must be entered in the *Address of the remote site's VPN gateway* field (see above). **Initiate on traffic** The connection is initiated automatically when the mGuard sees that the connection should be used. (Can be selected for all operating modes of the mGuard (*Stealth, Router*, etc.)) If one peer is initiated on data traffic, **Wait** or **Initiate** must be selected for the other peer. **Wait** The mGuard is ready to allow the connection to the mGuard that a remote peer actively initiates and establishes. If **%any** is entered under *Address of the remote site's VPN gateway*, **Wait** must be selected.
	Controlling service input (Only available with the TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4000/RS2000, FL MGUARD GT/GT, FL MGUARD RS4004/RS2005 and FL MGUARD RS.)	**None / Service input CMD 1-3** The VPN connection can be switched via a connected pushbutton/switch. The pushbutton/switch must be connected to one of the service contacts (CMD 1-3). If starting and stopping the VPN connection via the CMD contact is enabled, only the CMD contact is authorized to do this. However, if a pushbutton is connected to the CMD contact (instead of a switch – see below), the connection can also be established and released using the CGI script command nph-vpn.cgi or via a text message, which has the same rights. If a VPN connection is controlled via a VPN switch, then VPN redundancy cannot be activated.
	Use inverted control logic	Inverts the behavior of the connected switch. If the switching service input is configured as an on/off switch, it can activate one VPN connection while simultaneously deactivating another which uses inverted logic, for example.

IPsec VPN >> Connections >> Edit >> General [...]		
	Deactivation timeout	Time, after which the VPN connection is stopped, if it has been started via a text message, switch, pushbutton, nph-vpn.cgi or the web interface. The timeout starts on transition to the “Started” state. After the timeout has elapsed, the connection remains in the “Stopped” state until it is restarted. **Exception: “Initiate on traffic”** A connection initiated (established) by data traffic is released after the timeout has elapsed, but remains in the “Started” state. The timeout only starts once there is no more data traffic. The VPN connection is established again when data traffic resumes. Time in hours, minutes and/or seconds (00:00:00 to 720:00:00, around 1 month). The entry can be in seconds [ss], minutes and seconds [mm:ss] or hours, minutes, and seconds [hh:mm:ss]. 0 means the setting is disabled.
	Token for text message trigger (Only available with the TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G.)	Incoming text messages can be used to start or stop VPN connections. The text message must contain the “vpn/start” or “vpn/stop” command followed by the token.

IPsec VPN >> Connections >> Edit >> General [...]		

	Encapsulate the VPN traffic in TCP	**No / TCP encapsulation / Path Finder (default: No)**
		
		If the **TCP encapsulation** function is used (see "TCP encapsulation" on page 317), only set this option to TCP encapsulation if the mGuard is to encapsulate its own outgoing data traffic for the VPN connection it initiated. In this case, the number of the port where the peer receives the encapsulated data packets must also be specified.
		
		TPC encapsulation can also be used with the "**Path Finder**" function (see "TCP encapsulation with enabled "Path Finder" function" on page 318). In this case, only set this option to **Path Finder** if the peer also supports the "Path Finder" function. The number of the port where the peer receives the encapsulated data packets must then also be specified.
		
		For TCP encapsulation / Path Finder the mGuard does not attempt to create the VPN connection via the standard IKE encryption (UDP-Port 500 and 4500), but always sends it via TCP protocol.
		
		Connection startup setting when using TCP encapsulation/Path Finder
		
		– If the mGuard is to establish a VPN connection to a maintenance center and encapsulate the data traffic there:
		    – "Initiate" or "Initiate on traffic" must be specified.
		– If the mGuard is installed at a maintenance center to which mGuard devices establish a VPN connection:
		    – "Wait" must be specified.

	TCP-Port of the server, which accepts the encapsulated connection (Only visible if "Encapsulate the VPN traffic in TCP" is set to **TCP encapsulation** or **Path Finder**.)	**Default: 8080** Number of the port where the encapsulated data packets are received by the peer. The port number specified here must be the same as the one specified for the mGuard of the peer under TCP port to listen on (IPsec VPN >> Global >> Options menu item).
Mode Configuration	The mGuard supports the "Extended Authentication" authentication method (XAuth) and the frequently required "Mode Config" protocol extension including "Split Tunneling" as the server and as the client (including iOS and Android-support). Network settings and DNS and WINS configurations are communicated to the IPsec client by the IPsec server.	

IPsec VPN >> Connections >> Edit >> General [...]

Mode configuration

Off / Server / Client (default: Off)

In order to communicate via an IPsec VPN connection as the server or client with peers that require “**XAuth**” and “**Mode Config**”, select “Server” or “Client”.

Off: do not use “Mode Config”.

Server: communicate the IPsec network configuration to the peer.

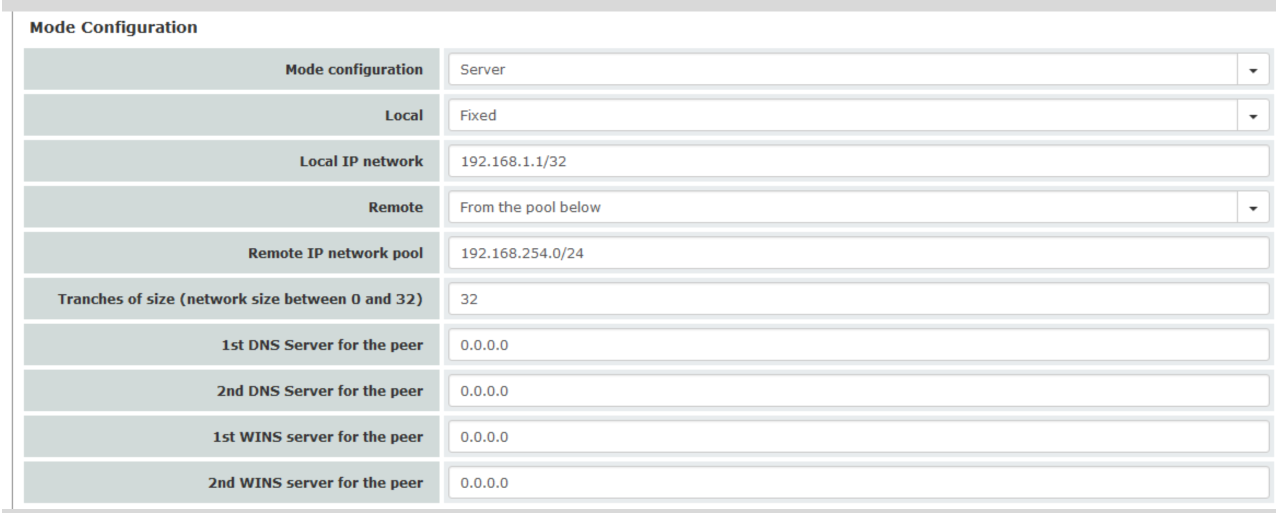
Client: accept and apply the IPsec network configuration communicated by the peer.

> “Mode Config” cannot be used in conjunction with “VPN redundancy” ("VPN redundancy" on page 437) or in “VPN Aggressive Mode” ("Aggressive Mode (insecure)" on page 351).

Settings as server

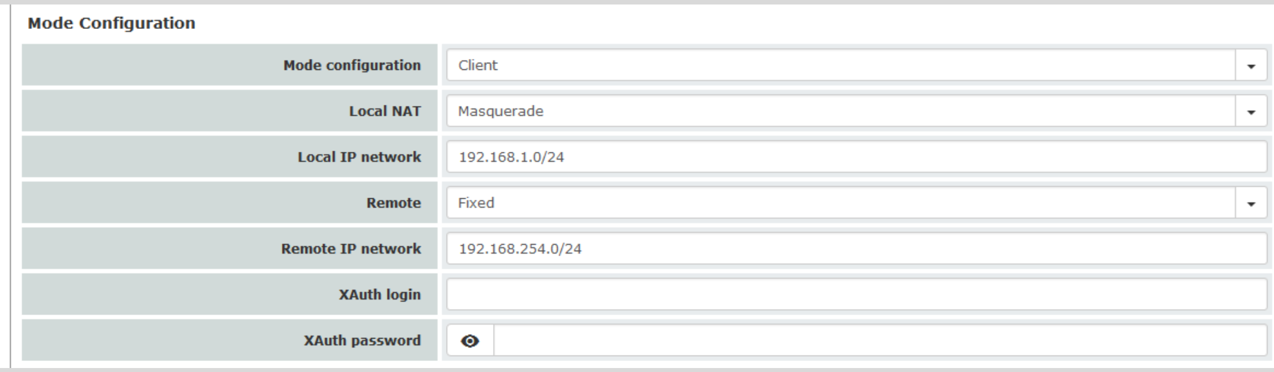
Allows clients that require “XAuth” and “Mode Config” (e.g., Apple iPad) to establish an IPsec VPN connection to the mGuard. The remote clients receive the necessary values for configuring the connection (local and remote network) from the mGuard.

> If a connection is to be established by the iOS client, a certificate must be used for authentication.
>
> The certificate name (CN) and the “Subject Alternative Name“ of the mGuard Machine Certificate must be identical to the IP address (or hostname/DNS name) that the iOS client uses to establish a VPN connection with the mGuard device (see "Authentication >> Certificates").



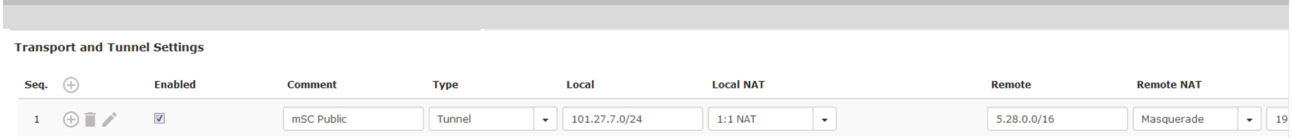
IPsec VPN >> Connections >> Edit >> General [...]		
	Local	**Fixed / From table below** **Fixed**: the local network on the server side is manually set and fixed and must also be set manually on the client side (on the remote client). **From table below**: the local network(s) on the server side is/are communicated to the remote client using the split tunneling extension. Entry in CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 26).
	Local IP network (If "Fixed" was selected)	Local network at the server end in CIDR format.
	Networks (If "From table below" was selected)	Local network at the server end in CIDR format.
	Remote	**From pool below / From table below** **From pool below** The server dynamically selects IP networks for the peer from the specified pool according to the selected tranche size. **From table below** (This function can only be used if an mGuard is used at the peer.) The IP networks of the peer are communicated to the remote client using the split tunneling extension.
	Remote IP network pool (If "From pool" was selected)	Network pool from which IP networks for the peer are selected, in CIDR format.
	Tranches of size (network size between 0 and 32) (If "From pool" was selected)	Section sizes which determine the size of the IP networks which can be taken from the network pool for the peer.
	Networks (If "From table below" was selected)	IP networks for the peer in CIDR format.
	1st and 2nd DNS server for the peer	Address of a DNS server which is communicated to the peer. The setting 0.0.0.0 means "no address".
	1st and 2nd WINS server for the peer	Address of a WINS server which is communicated to the peer. The setting 0.0.0.0 means "no address".
	Settings as client	
	Allows the mGuard to establish an IPsec VPN connection to servers that require "XAuth" and "Mode Config". As an option, the mGuard receives the necessary values (IP address/IP network) for configuring the connection (local and remote network) from the remote server of the peer.	

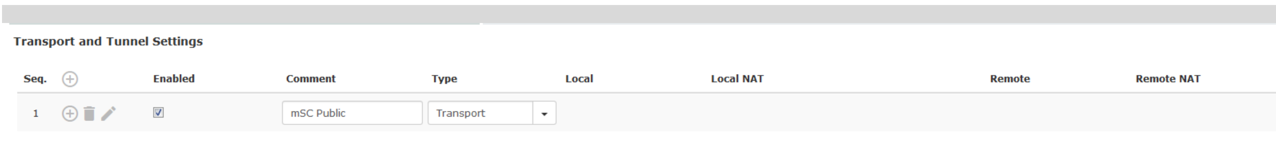
IPsec VPN >> Connections >> Edit >> General [...]



	Local NAT (Not active in Stealth modes "Autodetect" and "Static")	**No NAT / Masquerade** **No NAT** Local IP addresses selected by the server can use the tunnel. **Masquerade** The mGuard can masquerade its local network. To do this, the local network must be specified in CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 26).
	Local IP network	IP network at the local interface of the client that is masquer-aded.
	Remote	**Fixed / From Server** **Fixed**: the local network on the client side is manually set and fixed and must also be set manually on the server side (on the remote server). **From Server**: the remote network(s) on the server side is/are communicated to the local client using the split tunneling ex-tension. If the remote server does not use split tunneling, 0.0.0.0/0 is used.
	Remote IP network (If "Fixed" was selected)	The network of the remote server in CIDR format.
	XAuth login	Some remote servers require an XAuth user name (login) and an XAuth password in order to authenticate the client.
	XAuth password	Corresponding XAuth password
Transport and Tunnel Set-tings		

IPsec VPN >> Connections >> Edit >> General [...]





Enabled

Specify whether the connection tunnel should be active or not.

Comment

Freely selectable comment text. Can be left empty.

Type

The following can be selected:

– Tunnel (network ↔ network)
– Transport (host ↔ host)

Tunnel (network ↔ network)

This connection type is suitable in all cases and is also the most secure. In this mode, the IP datagrams to be transmitted are completely encrypted and are, with a new header, transmitted to the VPN gateway of the peer – the “tunnel end”. The transmitted datagrams are then decrypted and the original datagrams are restored. These are then forwarded to the destination computer.

> If the default route (0.0.0.0/0) is entered as the peer, the rules specified under “Network >> NAT >> IP and Port Forwarding” are given priority.
>
> This ensures that incoming connections to the WAN interface of the mGuard can continue using port forwarding. In this case, this data is not transmitted via VPN.

Transport (host ↔ host)

For this type of connection, only the data of the IP packets is encrypted. The IP header information remains unencrypted.

When you switch to *Transport*, the following fields (apart from Protocol) are hidden as these parameters are omitted.

Local

(For “Tunnel” connection type)

Define the network areas for both tunnel ends under **Local** and **Remote**.

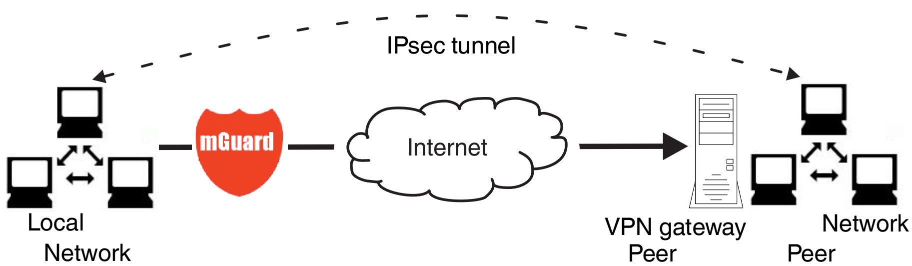
Local: here, specify the address of the network or computer which is connected locally to the mGuard.

Remote

(For “Tunnel” **(network ↔ network)** connection type)

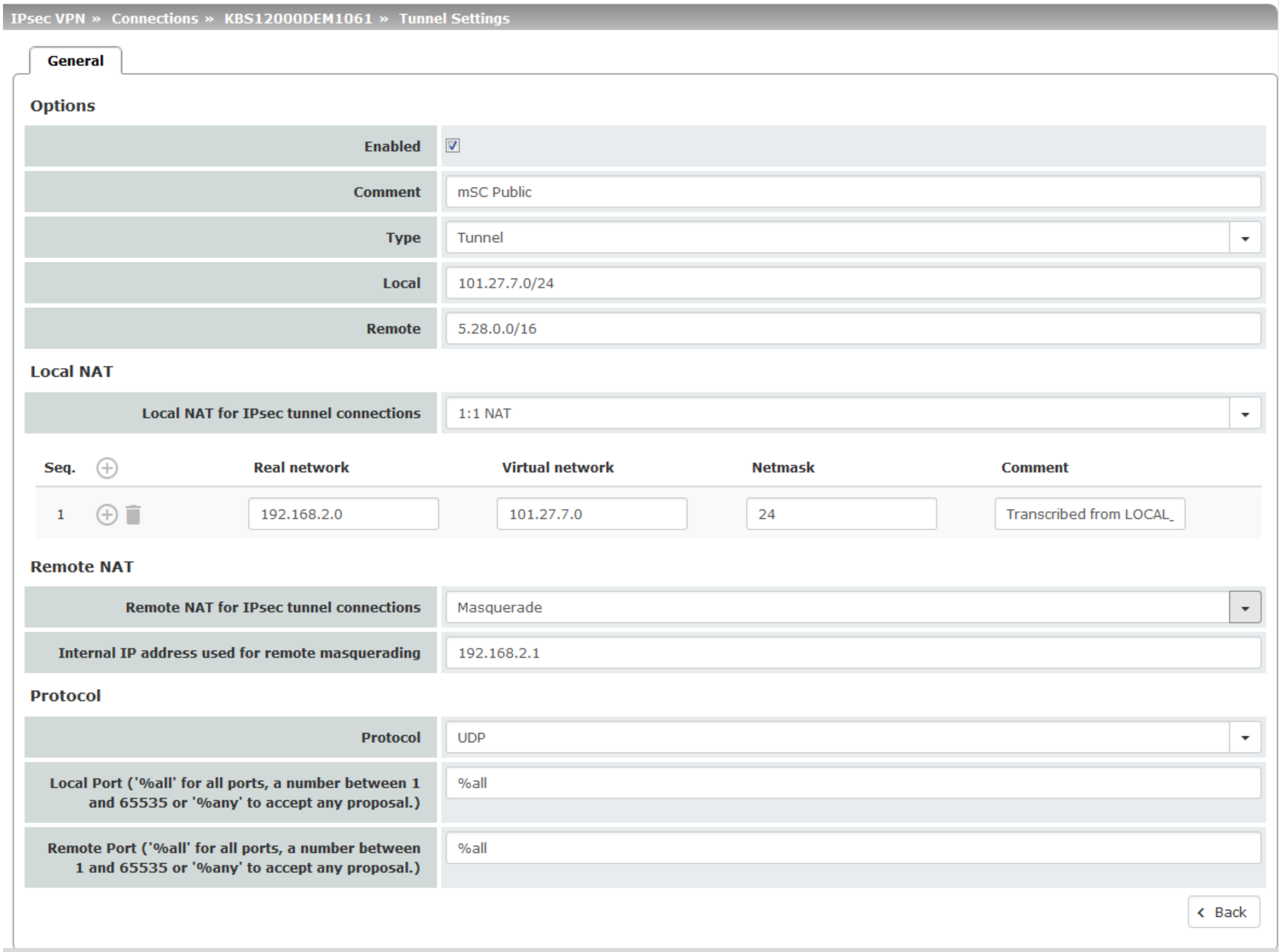
Remote: here, specify the address of the network or computer which is located downstream of the remote VPN gateway.

IPsec VPN >> Connections >> Edit >> General [...]		
	Local NAT (For “Tunnel” connection type)	**No NAT / 1:1 NAT / Masquerade** It is possible to translate the IP addresses of devices located at the respective end of the VPN tunnel. **No NAT**: NAT is not performed. With **1:1 NAT**, the IP addresses of devices at the local end of the tunnel are exchanged so that each individual address is translated into another specific address. You must click on the **Edit Row** icon in order to specify 1:1 NAT rules for local devices. With **Masquerade**, the IP addresses of devices at the local end of the tunnel are exchanged with an IP address that is identical for all devices.
	Remote NAT (For “Tunnel” connection type)	**No NAT / 1:1 NAT / Masquerade** **No NAT**: NAT is not performed. With **1:1 NAT**, the IP addresses of devices of the tunnel peer are exchanged so that each individual address is translated into another specific address. With **Masquerade**, the IP addresses of devices of the peer are exchanged with an IP address that is identical for all devices.



Click on the **Edit Row** icon to make further settings. The “IPsec VPN >> Connections >> Transport and Tunnel Settings >> General” window opens.

IPsec VPN >> Connections >> Edit >> General [...]



Options	**Transport and Tunnel Settings (Edit)**	
	Enabled	Specify whether the connection tunnel should be active or not.
	Comment	Freely selectable comment text. Can be left empty.

IPsec VPN >> Connections >> Edit >> General [...]		
	Type	The following can be selected: – Tunnel (network ↔ network) – Transport (host ↔ host) **Tunnel (network ↔ network)** This connection type is suitable in all cases and is also the most secure. In this mode, the IP datagrams to be transmitted are completely encrypted and are, with a new header, transmitted to the VPN gateway of the peer – the "tunnel end". The transmitted datagrams are then decrypted and the original datagrams are restored. These are then forwarded to the destination computer. If the default route (0.0.0.0/0) is entered as the peer, the rules specified under "Network >> NAT >> IP and Port Forwarding" are given priority. This ensures that incoming connections to the WAN interface of the mGuard can continue using port forwarding. In this case, this data is not transmitted via VPN. **Transport (host ↔ host)** For this type of connection, only the data of the IP packets is encrypted. The IP header information remains unencrypted. When you switch to *Transport*, the following fields (apart from Protocol) are hidden as these parameters are omitted.
	Local (For "Tunnel" connection type)	Define the network areas for both tunnel ends under **Local** and **Remote**. **Local:** here, specify the address of the network or computer which is connected locally to the mGuard.
	Remote (For "Tunnel" connection type)	**Remote:** here, specify the address of the network or computer which is located downstream of the remote VPN gateway.
Local NAT	**Local NAT for IPsec tunnel connections** (For "Tunnel" connection type)	**No NAT / 1:1 NAT / Masquerade** It is possible to translate the IP addresses of devices located at the respective end of the VPN tunnel. **No NAT**: NAT is not performed. With **1:1 NAT**, the IP addresses of devices at the local end of the tunnel are exchanged so that each individual address is translated into another specific address. With **Masquerade**, the IP addresses of devices at the local end of the tunnel are exchanged with an IP address that is identical for all devices.

IPsec VPN >> Connections >> Edit >> General [...]

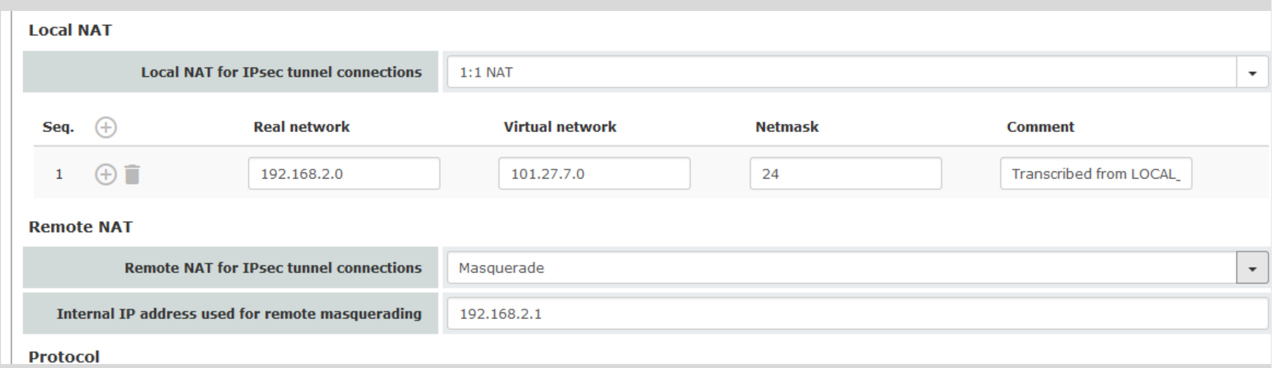
If local devices transmit data packets, only those data packets are considered which:

– Are actually encrypted by the mGuard (the mGuard only forwards packets via the VPN tunnel if they originate from a trustworthy source).
– Originate from a source address within the network which is defined here.
– Have their destination address in the *Remote* network if 1:1 NAT is not set there for the peer.

The data packets of local devices are assigned a source address according to the address set under *Local* and are transmitted via the VPN tunnel.

You can specify 1:1 NAT rules for each VPN tunnel for local devices. In this way, an IP area that is distributed over a wide network can be gathered and sent through a narrow tunnel.

Local 1:1 NAT networks must be specified in ascending order, beginning with the smallest network up to the largest network.



Real network — Configures the “From IP” address for 1:1 NAT.

Virtual network — Configures the translated IP address for 1:1 NAT.

Netmask — The netmask as a value between 1 and 32 for the real and virtual network address (see also "CIDR (Classless Inter-Domain Routing)" on page 26).

Comment — Can be filled with appropriate comments.

Internal network address for local masquerading

(When “Masquerade” is selected)

If local devices transmit data packets, only those data packets are considered which:

– Are actually encrypted by the mGuard (the mGuard only forwards packets via the VPN tunnel if they originate from a trustworthy source).
– Originate from a source address within the network which is defined here.
– Have their destination address in the *Remote* network if 1:1 NAT is not set for the *Remote* NAT.

IPsec VPN >> Connections >> Edit >> General [...]		
		Only one IP address (subnet mask /32) is permitted as the VPN network for this setting. The network to be masqueraded is translated to this IP address. The data packets are then transmitted via the VPN tunnel. Masquerading changes the source address (and source port). The original addresses are recorded in an entry in the Conntrack table. Where response packets are received via the VPN tunnel and there is a matching entry in the Conntrack table, these packets have their destination address (and destination port) written back to them.
Remote NAT	**Remote NAT for IPsec tunnel connections** (For “Tunnel” connection type)	**No NAT / 1:1 NAT / Masquerade** It is possible to translate the IP addresses of devices located at the respective end of the VPN tunnel. With **Remote 1:1 NAT**, the IP addresses of devices of the tunnel peer are exchanged so that each individual address is translated into another specific address. With **Masquerade** set for the peer network, the IP addresses of devices of the peer are exchanged with an IP address that is identical for all devices.
	Network address for 1:1 NAT (For selection "1:1-NAT")	If local devices transmit data packets, only those data packets are considered which: – Are actually encrypted by the mGuard (the mGuard only forwards packets via the VPN tunnel if they originate from a trustworthy source). – Have a source address within the network which is defined here under Local. The data packets are assigned a destination address from the network that is set under Remote. If necessary, the source address is also replaced (see Local). The data packets are then transmitted via the VPN tunnel.
	Internal IP address used for remote masquerading (When “Masquerade” is selected)	Only one IP address (subnet mask /32) is permitted as the VPN network for this setting. The network to be masqueraded is translated to this IP address. The data packets are then transmitted via the VPN tunnel. Masquerading changes the source address (and source port). The original addresses are recorded in an entry in the Conntrack table. Where response packets are received via the VPN tunnel and there is a matching entry in the Conntrack table, these packets have their destination address (and destination port) written back to them.

IPsec VPN >> Connections >> Edit >> General [...]		
Protocol	**Protocol**	**All** means TCP, UDP, ICMP, and other IP protocols **Local port (only for TCP/UDP)**: number of the port to be used. Select “%all” for all ports, a number between 1 and 65535 or “%any” to leave the decision to the client. **Remote port (only for TCP/UDP)**: number of the port to be used. Select “%all” for all ports, a number between 1 and 65535 or “%any” to leave the decision to the client.
Dynamic Routing	**Add kernel route to remote network to allow OSPF route redistribution** (Only if **OSPF** is activated)	When the function is activated, a kernel route to the remote network (peer) is added in order to enable distribution by means of OSPF.

Tunnel setting IPsec/L2TP

If clients should connect via the mGuard by IPsec/L2TP, activate the L2TP server and make the following entries in the fields specified below:

- **Type**: Transport
- **Protocol**: UDP
- **Local:** %all
- **Remote:** %all
- **PFS**: No ("Perfect Forward Secrecy (PFS)" on page 358)

Specifying a default route over the VPN

Address 0.0.0.0/0 specifies a *default route over the VPN*.

With this address, all data traffic where no other tunnel or route exists is routed through this VPN tunnel.

A default route over the VPN should only be specified for a single tunnel.

In *Stealth* mode, a *default route over the VPN* cannot be used.

Option of tunnel groups

The VPN license model (as of mGuard firmware Version 8.3) allows tunnel groups to be created with all VPN licenses.

The license no longer limits the number of tunnels established, but instead the number of connected peers (VPN peers). If several tunnels are established to a peer, only one peer is counted, which is an improvement over the old model.

If *Address of the remote site's VPN gateway* is specified as **%any**, there may be many mGuard devices or many networks on the remote side.

A very large address area is then specified in the **Remote** field for the local mGuard. A part of this address area is used on the remote mGuard devices for the network specified for each of them under **Local**.

This is illustrated as follows: the entries in the **Local** and **Remote** fields for the local and remote mGuard devices could be made as follows:

Local mGuard			Remote **mGuard A**	
Local	Remote		Local	Remote
10.0.0.0/8	10.0.0.0/8	>	10.1.7.0/24	10.0.0.0/8
			Remote **mGuard B**	
			Local	Remote
		>	10.3.9.0/24	10.0.0.0/8
			etc.	

In this way, by configuring a single tunnel, you can establish connections for a number of peers.

Masquerade

Can only be used for *Tunnel* VPN type.

Example

A control center has one VPN tunnel each for a large number of branches. One local network with numerous computers is installed in each of the branches, and these computers are connected to the control center via the relevant VPN tunnel. In this case, the address area could be too small to include all the computers at the various VPN tunnel ends.

Masquerading solves this problem:

The computers connected in the network of a branch appear under a single IP address by means of masquerading for the VPN gateway of the control center. In addition, this enables the local networks in the various branches to all use the same network address locally. Only the branch can establish VPN connections to the control center.

Network address for masquerading

Specify the IP address area for which masquerading is used.

The sender address in the data packets sent by a computer via the VPN connection is only replaced by the address specified in the **Local** field (see above) if this computer has an IP address from this address area.

The address specified in the **Local** field must have the netmask “/32” to ensure that only one IP address is signified.

Masquerade can be used in the following network modes: Router, PPPoE, PPTP, Modem, Built-in modem, Built-in mobile network modem, and Stealth (only “Multiple clients” in Stealth mode).

Modem / Built-in modem / Built-in mobile network modem: not available for all mGuard models (see "Network >> Interfaces" on page 127).

For IP connections via a VPN connection with active masquerading, the firewall rules for outgoing data in the VPN connection are used for the original source address of the connection.

1:1 NAT

> Can only be used for *Tunnel* VPN type.

With 1:1 NAT in VPN, it is still possible to enter the network addresses actually used to specify the tunnel beginning and end, independently of the tunnel parameters agreed with the peer:

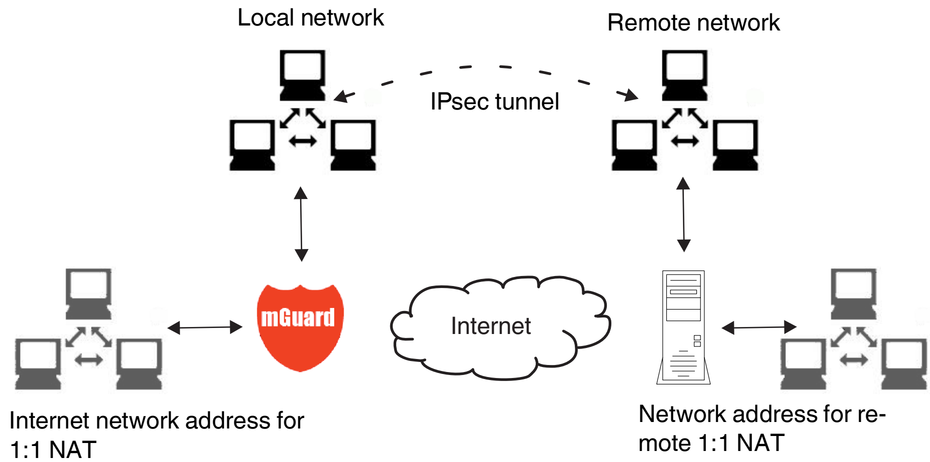
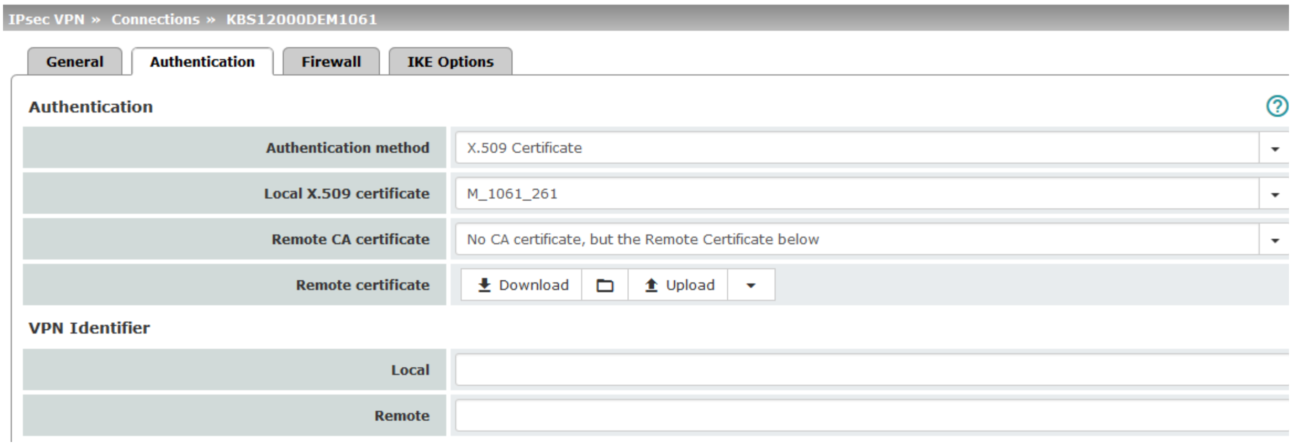


Figure 10-3 1:1 NAT

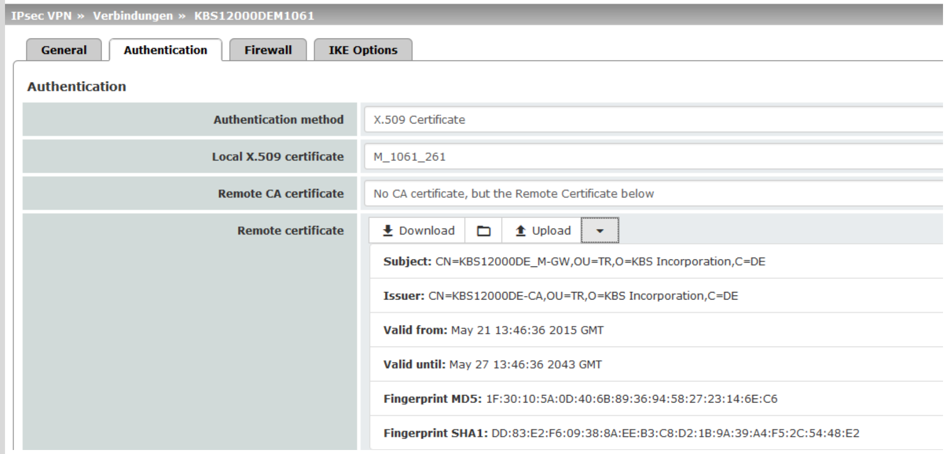
10.2.3 Authentication



IPsec VPN >> Connections >> Edit >> Authentication		
Authentication	**Authentication method**	There are two options: – X.509 Certificate (default setting) – Pre-shared key (PSK) **CAUTION: Insecure PSK authentication** Pre-shared key (PSK) authentication is considered insecure and should no longer be used. For security reasons, use X.509 certificates for authentication. The page contains different setting options depending on the method chosen. **Authentication method: X.509 Certificate** This method is supported by most modern IPsec implementations. With this option, each VPN device has a secret private key and a public key in the form of an X.509 certificate, which contains further information about the certificate's owner and the certification authority (CA). The following must be specified: – How the mGuard authenticates itself to the peer – How the mGuard authenticates the remote peer

IPsec VPN >> Connections >> Edit >> Authentication

How the mGuard authenticates itself to the peer



Local X.509 certificate

(Authentication method: “X.509 Certificate”)

Specifies which machine certificate the mGuard uses as authentication to the VPN peer.

Select one of the machine certificates from the selection list.

The selection list contains the machine certificates that have been loaded on the mGuard under the *Authentication >> Certificates* menu item.

> If *None* is displayed, a certificate must be installed first. *None* must not be left in place, as this results in no X.509 authentication.

How the mGuard authenticates the remote peer

The following definition relates to how the mGuard verifies the authenticity of the VPN remote peer.

The table below shows which certificates must be provided for the mGuard to authenticate the VPN peer if the VPN peer shows one of the following certificate types when a connection is established:

– A machine certificate signed by a CA
– A self-signed machine certificate

Remote CA certificate

The following selection options are available:

– Signed by any trusted CA
– No CA certificate, but the Remote Certificate below
– Name of a CA certificate if available

Remote certificate

(For authentication using remote certificate)

You can upload the remote certificate. The certificate is selected and stored in the list of remote certificates (see "Remote Certificates" on page 252).

For additional information about the table, see "Authentication >> Certificates" on page 241.

Authentication for VPN

The peer shows the following:	Machine certificate, **signed by CA**	Machine certificate, **self-signed**
The mGuard authenticates the peer using:		
	Remote certificate Or all CA certificates that form the chain to the root CA certificate together with the certificate shown by the peer	Remote certificate

According to this table, the certificates that must be provided are the ones the mGuard uses to authenticate the relevant VPN peer.

Requirements

The following instructions assume that the certificates have already been correctly installed on the mGuard (see *"Authentication >> Certificates" on page 241*, apart from the remote certificate).

If the use of revocation lists (CRL checking) is activated under the *Authentication >> Certificates, Certificate Settings* menu item, each certificate signed by a CA that is "shown" by the VPN peer is checked for revocations.

However, an existing VPN connection is not immediately terminated by a withdrawn certificate if the CRL update is being performed during the existing VPN connection. Nevertheless, it is no longer possible to exchange keys again (*rekeying*) or restart the VPN connection.

Remote CA certificate

Self-signed machine certificate

If the VPN peer authenticates itself with a **self-signed** machine certificate:

- Select the following entry from the selection list:
  "No CA certificate, but the Remote Certificate below"
- Install the remote certificate under *Remote certificate* (see "Installing the remote certificate" on page 347).

It is not possible to reference a remote certificate loaded under the *Authentication >> Certificates* menu item.

Machine certificate signed by the CA

If the VPN peer authenticates itself with a machine certificate **signed by a CA**:

It is possible to authenticate the machine certificate shown by the peer as follows:

– Using CA certificates
– Using the corresponding remote certificate

Authentication using a CA certificate:

Only the CA certificate from the CA that signed the certificate shown by the VPN peer should be referenced here (selection from list). The additional CA certificates that form the chain to the root CA certificate together with the certificate shown by the peer must be installed on the mGuard under the *Authentication >> Certificates* menu item.

The selection list contains all CA certificates that have been loaded on the mGuard under the *Authentication >> Certificates* menu item.

The other option is *“Signed by any trusted CA”.*

With this setting, all VPN peers are accepted, providing they log in with a signed CA certificate issued by a recognized certification authority (CA). The CA is recognized if the relevant CA certificate and all other CA certificates have been loaded on the mGuard. These then form the chain to the root certificate together with the certificates shown.

Authentication using the corresponding remote certificate:

- Select the following entry from the selection list:
  “*No CA certificate, but the Remote Certificate below*”
- Install the remote certificate under *Remote certificate* (see "Installing the remote certificate" on page 347).

> It is not possible to reference a remote certificate loaded under the *Authentication >> Certificates* menu item.

Installing the remote certificate

The remote certificate must be configured if the VPN peer is to be authenticated using a remote certificate.

To import a certificate, proceed as follows:

Requirement

The certificate file (file name extension: *.pem, *.cer or *.crt) is saved on the connected computer.

- **No file selected...** click to select the file
- Click on **Upload**.
  The contents of the certificate file are then displayed.

IPsec VPN >> Connections >> Edit >> Authentication	
VPN Identifier	**Authentication method: CA certificate** The following explanation applies if the VPN peer is authenticated using CA certificates. VPN gateways use the VPN identifier to detect which configurations belong to the same VPN connection. **If the mGuard consults CA certificates to authenticate a VPN peer, then it is possible to use the VPN identifier as a filter.** • Make a corresponding entry in the *Remote* field.

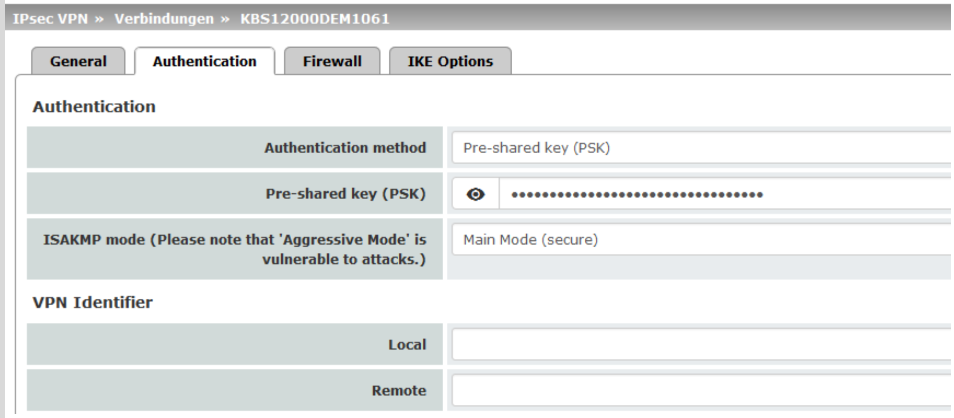
IPsec VPN >> Connections >> Edit >> Authentication [...]		
	Local	Default: empty field The local VPN identifier can be used to specify the name the mGuard uses to identify itself to the peer. It must match the data in the machine certificate of the mGuard. **Valid values:** – Empty, i.e., no entry (default). The “Subject” entry (previously *Distinguished Name*) in the machine certificate is then used. – The “Subject” entry in the machine certificate. – One of the *Subject Alternative Names*, if they are listed in the certificate. If the certificate contains *Subject Alternative Names*, these are specified under “Valid values:”. These can include IP addresses, host names with “@” prefix or e-mail addresses.
	Remote	Specifies what must be entered as a subject in the machine certificate of the VPN peer for the mGuard to accept this VPN peer as a communication partner. It is then possible to restrict or enable access by VPN peers, which the mGuard would accept in principle based on certificate checks, as follows: – Restricted access to certain *subjects* (i.e., machines) and/or to *subjects* that have certain attributes or – Access enabled for all *subjects* (See "Subject, certificate" on page 453.) “Distinguished Name” was previously used instead of “Subject”.

IPsec VPN >> Connections >> Edit >> Authentication [...]	
	Access enabled for all subjects: If the *Remote* field is left empty, then any subject entries are permitted in the machine certificate shown by the VPN peer. It is then no longer necessary to identify or define the subject in the certificate. **Restricted access to certain subjects:** In the certificate, the certificate owner is specified in the *Subject* field. The entry is comprised of several attributes. These attributes are either expressed as an object identifier (e.g., 132.3.7.32.1) or, more commonly, as an abbreviation with a corresponding value. Example: CN=VPN endpoint 01, O=Smith and Co., C=US If certain subject attributes have very specific values for the acceptance of the VPN peer by the mGuard, then these must be specified accordingly. The values of the other freely selectable attributes are entered using the ***** (asterisk) wildcard. Example: CN=*, O=Smith and Co., C=US (with or without spaces between attributes) In this example, the attributes “O=Smith and Co.” and “C=US” should be entered in the certificate that is shown under “Subject”. It is only then that the mGuard would accept the certificate owner (subject) as a communication partner. The other attributes in the certificates to be filtered can have any value. Please note the following when setting a subject filter: The number and the order of the attributes must correspond to that of the certificates for which the filter is used. Please note this is case-sensitive.

IPsec VPN >> Connections >> Edit >> Authentication [...]

Authentication

Authentication method: Pre-shared key (PSK)



This method is mainly supported by older IPsec implementations. In this case, both sides of the VPN authenticate themselves using the same PSK.

NOTE: Insecure PSK authentication

Pre-shared key (PSK) authentication is considered insecure and should no longer be used. For security reasons, use X.509 certificates for authentication.

To make the agreed key available to the mGuard, proceed as follows:

- Enter the agreed string in the **Pre-shared key (PSK)** input field.

To achieve security comparable to that of 3DES, the string should consist of around 30 randomly selected characters, and should include upper and lower case characters and digits.

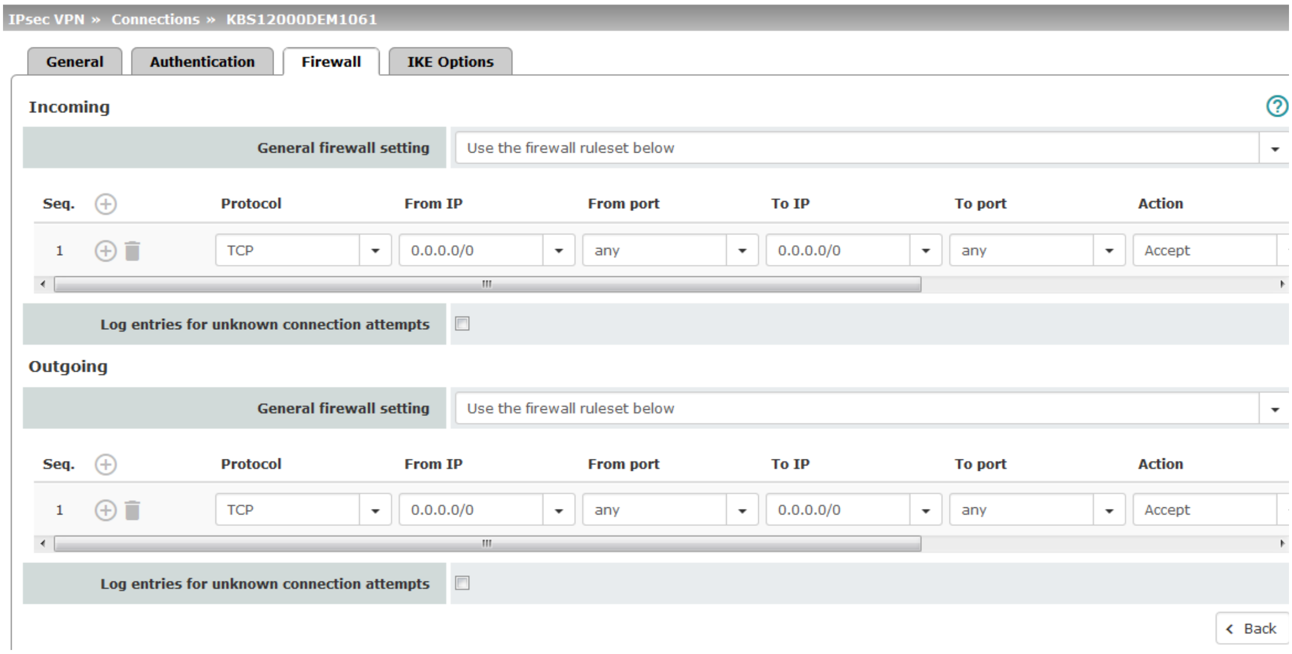
When PSK is used together with the "Aggressive Mode (insecure)" setting, a fixed Diffie-Hellman algorithm must be selected under IKE Options for the initiator of the connection.

When PSK is used together with the "Aggressive Mode (insecure)" setting, all Diffie-Hellman algorithms should be selected under IKE Options for the responder of the connection.

When using a fixed Diffie-Hellman algorithm, it must be the same for all connections using the "Aggressive Mode (insecure)" setting.

<table>
<tr><th colspan="3">IPsec VPN >> Connections >> Edit >> Authentication [...]</th></tr>
<tr><td></td><td>ISAKMP mode</td><td>Main Mode (secure)
In Main Mode, the party wishing to establish the connection (initiator) and the responder negotiate an ISAKMP SA.
We recommend using certificates in Main Mode.
Aggressive Mode (insecure)
Encryption for Aggressive Mode is not as secure as for Main Mode. The use of this mode can be justified if the responder does not know the initiator's address in advance, and both parties wish to use pre-shared keys for authentication. Another reason may be to achieve faster connection establishment when the responder's credentials are already known, e.g., an employee wishing to access the company network.
Requirement:
– Cannot be used together with the redundancy function.
– The same mode must be used between peers.
– Aggressive mode is not supported in conjunction with XAuth/Mode Config.
– If two VPN clients downstream of the same NAT gateway establish the same connection to a VPN gateway, they must use the same PSK.
VPN connections in Aggressive Mode and with PSK authentication, which are to be implemented by means of a NAT gateway, must use unique VPN identifiers on both the client and the gateway.</td></tr>
<tr><td>VPN Identifier</td><td colspan="2">VPN gateways use the VPN Identifier to detect which configurations belong to the same VPN connection.
The following entries are valid for PSK:
– Empty (IP address used by default)
– An IP address
– A host name with “@” prefix (e.g., “@vpn1138.example.com”)
– An e-mail address (e.g., “piepiorra@example.com”)</td></tr>
</table>

10.2.4 Firewall



Incoming/outgoing firewall

While the settings made under the *Network Security* menu item only relate to non-VPN connections (see above under "Network Security menu" on page 257), the settings here only relate to the VPN connection defined on these tab pages.

If multiple VPN connections have been defined, you can restrict the outgoing or incoming access individually for each connection. Any attempts to bypass these restrictions can be logged.

By default, the VPN firewall is set to allow all connections for this VPN connection.

However, the extended firewall settings defined and explained above apply independently for each individual VPN connection (see "Network Security menu" on page 257, "Network Security >> Packet Filter" on page 257, "Advanced" on page 278).

If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored.

In *Stealth* mode, the actual IP address used by the client should be used in the firewall rules, or it should be left at 0.0.0.0/0, as only one client can be addressed through the tunnel.

If the **Allow packet forwarding between VPN connections** function is **activated** on the **Global** tab page, the rules under **Incoming** are used for the incoming data packets to the mGuard, and the rules under **Outgoing** are applied to the outgoing data packets.

If the outgoing data packets are included in the same connection definition (for a defined VPN connection group), then the firewall rules for **Incoming** and **Outgoing** for the same connection definition are used.

If a different VPN connection definition applies to the outgoing data packets, the firewall rules for **Outgoing** for this other connection definition are used.

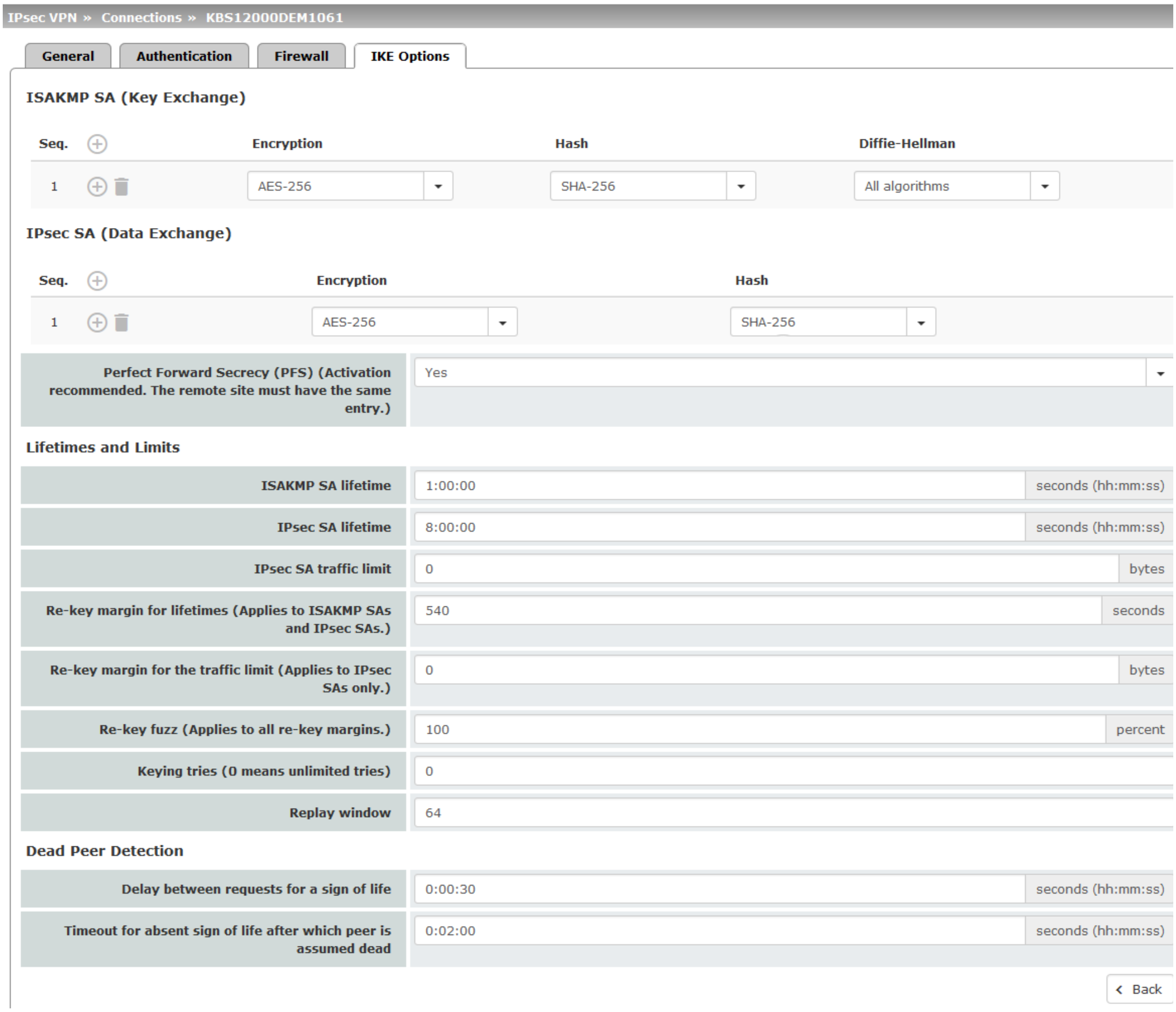
If the mGuard has been configured to forward SSH connection packets (e.g., by permitting a SEC-Stick hub & spoke connection), existing VPN firewall rules are not applied. This means, for example, that packets of an SSH connection are sent through a VPN tunnel despite the fact that this is prohibited by its firewall rules.

IPsec VPN >> Connections >> Edit >> Firewall		
Incoming	**General firewall setting**	**Accept all incoming connections**: the data packets of all incoming connections are allowed. **Drop all incoming connections**: the data packets of all incoming connections are discarded. **Accept Ping only:** the data packets of all incoming connections are discarded, except for ping packets (ICMP). **Use the firewall ruleset below**: displays further setting options.
	The following settings are only visible if "**Use the firewall ruleset below**" is set.	

IPsec VPN >> Connections >> Edit >> Firewall		
	Protocol	**All** means TCP, UDP, ICMP, GRE, and other IP protocols.
	From IP/To IP	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 26). **Name of IP groups,** if defined. When a name is specified for an IP group, the host names, IP addresses, IP areas or networks saved under this name are taken into consideration (see "IP/Port Groups" on page 275). If host names are used in IP groups, the mGuard must be configured so that the host name of a DNS server can be resolved in an IP address. If a host name from an IP group cannot be resolved, this host will not be taken into consideration for the rule. Further entries in the IP group are not affected by this and are taken into consideration. The use of host names in IP groups is not possible on mGuard devices of the RS2000 series. **Incoming**: – From IP: IP address in the VPN tunnel – To IP: 1:1 NAT address or the actual address **Outgoing**: – From IP: 1:1 NAT address or the actual address – To IP: IP address in the VPN tunnel
	From port / To port (Only for TCP and UDP protocols)	**any** refers to any port. **startport:endport** (e.g., 110:120) refers to a port range. Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110). **Name of port groups**, if defined. When a name is specified for a port group, the ports or port ranges saved under this name are taken into consideration (see "IP/Port Groups" on page 275).

IPsec VPN >> Connections >> Edit >> Firewall		
	Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back and the sender is informed of their rejection. (In *Stealth* mode, Reject has the same effect as Drop.) **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts. **Name of rule records**, if defined. When a name is specified for rule records, the firewall rules configured under this name take effect (see "Rule Records" on page 268 tab page). For security reasons, rule records that contain IP groups with host names should not be used in firewall rules which execute “Drop” or “Reject” as the action. The use of rule records is not possible on mGuard devices of the RS2000 series. **Name of Modbus TCP rule records**, if defined. When a Modbus TCP rule record is selected, the firewall rules configured under this rule record take effect (see "Modbus TCP" on page 284).
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – activate *Log* function – Should not be logged – deactivate *Log* function (default)
	Log entries for unknown connection attempts	When the function is activated, all connection attempts that are not covered by the rules defined above are logged.
Outgoing	The explanation provided under “Incoming” also applies to “Outgoing”.	

10.2.5 IKE Options



IPsec VPN >> Connections >> Edit >> IKE Options		
ISAKMP SA (Key Exchange)	**Algorithms** (This preference list starts with the most preferred pair of algorithms.) **Use secure algorithms** Some of the available algorithms are obsolete and are no longer considered secure. This is why they are not to be recommended. For reasons of reverse compatibility however they can still be selected and used in the mGuard See "Using secure encryption and hash algorithms" on page 19. Decide on which encryption method should be used with the administrator of the peer.	
	Encryption	**DES, 3DES, AES-128, AES-192, AES-256 (default)** Default pre-setting in mGuard firmware Version 8.5.0 changed in AES-256. **Use secure algorithms** Some of the available algorithms are obsolete and are no longer considered secure. This is why they are not to be recommended. Due to downwards compatibility, they can continue to be selected and used in mGuard. See "Using secure encryption and hash algorithms" on page 19. The following applies in principle: the longer the encryption length (in Bits) which uses an encryption algorithm (stated by the appended number), the more secure it is. The longer the key, the more time-consuming the encryption procedure. However, this does not affect the mGuard as it uses a hardware-based encryption technique. Nevertheless, this aspect may be of significance for the peer.

IPsec VPN >> Connections >> Edit >> IKE Options		
	Checksum	**MD5, SHA1, SHA-256 (default), SHA-512** Default pre-setting in mGuard firmware Version 8.6.0 changed in SHA-256. Leave this set to *All algorithms*. It is then of no consequence whether the peer works with MD5, SHA-1, SHA-256, SHA-384 or SHA-512. **Use secure algorithms** Some of the available algorithms are obsolete and are no longer considered secure. This is why they are not to be recommended. Due to downwards compatibility, they can continue to be selected and used in mGuard. See "Using secure encryption and hash algorithms" on page 19.
	Diffie-Hellman	The Diffie-Hellman key exchange method is not available for all the algorithms. The bit depth for the encryption can be set here.
IPsec SA (Data Exchange)	In contrast to *ISAKMP SA (Key Exchange)* (see above), the procedure for data exchange is defined here. It does not necessarily have to differ from the procedure defined for key exchange. The algorithm designated as “Null” does not contain encryption.	
	Algorithms	See above: ISAKMP SA (Key Exchange). Default pre-settings in mGuard firmware Version 8.6.0 changed. If the data exchange is to take place without encryption, the entry "Null" must be selected in the "Encryption" drop-down menu.
	Perfect Forward Secrecy (PFS)	Method for providing increased security during data transmission. With IPsec, the keys for data exchange are renewed at defined intervals. With PFS, new random numbers are negotiated with the peer instead of being derived from previously agreed random numbers. The peer must have the same entry. We recommend enabling this setting for security reasons. Select **Yes**, if the peer supports PFS. Set *Perfect Forward Secrecy (PFS)* to **No** if the peer is an IPsec/L2TP client.

IPsec VPN >> Connections >> Edit >> IKE Options		
Lifetimes and Limits	The keys of an IPsec connection are renewed at defined intervals in order to increase the difficulty of an attack on an IPsec connection.	
	ISAKMP SA lifetime	Lifetime in seconds (hh:mm:ss) of the keys agreed for ISAKMP SA. Default setting: 3600 seconds (1 hour). The maximum permitted lifetime is 86400 seconds (24 hours).
	IPsec SA lifetime	Lifetime in seconds (hh:mm:ss) of the keys agreed for IPsec SA. Default setting: 28800 seconds (8 hours). The maximum permitted lifetime is 86400 seconds (24 hours).
	IPsec SA traffic limit	0 to 2147483647 bytes The value 0 indicates that there is no traffic limit for the IPsec SAs on this VPN connection. All other values indicate the maximum number of bytes which are encrypted by the IPsec SA for this VPN connection (Hard Limit).
	Re-key margin for lifetimes	Applies to ISAKMP SAs and IPsec SAs. Minimum duration before the old key expires and during which a new key should be created. Default setting: 540 seconds (9 minutes).
	Re-key margin for the traffic limit	Only applies to IPsec SAs. The value 0 indicates that the traffic limit is not used. 0 must be set here when 0 is also set under *IPsec SA traffic limit*. If a value above 0 is entered, then a new limit is calculated from two values. The number of bytes entered here is subtracted from the value specified under *IPsec SA traffic limit* (i.e., the *Hard Limit*). The calculated value is then known as the *Soft Limit*. This specifies the number of bytes which must be encrypted for a new key to be negotiated for the IPsec SA. A further amount is subtracted when a re-key fuzz (see below) above 0 is entered. This is a percentage of the re-key margin. The percentage is entered under Re-key fuzz. The re-key margin value must be lower than the *Hard Limit*. It must be significantly lower when a *Re-key fuzz* is also added. If the *IPsec SA lifetime* is reached earlier, the *Soft Limit* is ignored.
	Re-key fuzz	Maximum percentage by which the *Re-key margin* should be randomly increased. This is used to delay key exchange on machines with multiple VPN connections. Default setting: 100 percent.
	Keying tries	Number of attempts to negotiate new keys with the peer. The value 0 results in unlimited attempts for connections initiated by the mGuard, otherwise it results in 5 attempts.

<table>
<tr><th colspan="3">IPsec VPN >> Connections >> Edit >> IKE Options</th></tr>
<tr><td rowspan="3">Dead Peer Detection</td><td colspan="2">If the peer supports the Dead Peer Detection (DPD) protocol, the relevant peers can detect whether or not the IPsec connection is still active and whether it needs to be established again.</td></tr>
<tr><td>Delay between requests for a sign of life</td><td>Duration in seconds after which DPD Keep Alive requests should be transmitted. These requests test whether the peer is still available.

Default setting: 30 seconds (00:00:30).</td></tr>
<tr><td>Timeout for absent sign of life after which peer is assumed dead</td><td>Duration in seconds after which the connection to the peer should be declared dead if there has been no response to the Keep Alive requests.

Default setting: 120 seconds (00:02:00).

If the mGuard finds that a connection is dead, it responds according to the setting under Connection startup (see definition of this VPN connection under Connection startup on the General tab page).</td></tr>
</table>

10.3 IPsec VPN >> L2TP via IPsec

These settings do not apply in Stealth mode. It is not possible to use the MD5 algorithm under Windows 7. The MD5 algorithm must be replaced by SHA-1.

Allows VPN connections to the mGuard to be established using the IPsec/L2TP protocol.

In doing so, the L2TP protocol is driven using an IPsec transport connection in order to establish a tunnel connection to a Point-to-Point Protocol (PPP). Clients are automatically assigned IP addresses by the PPP.

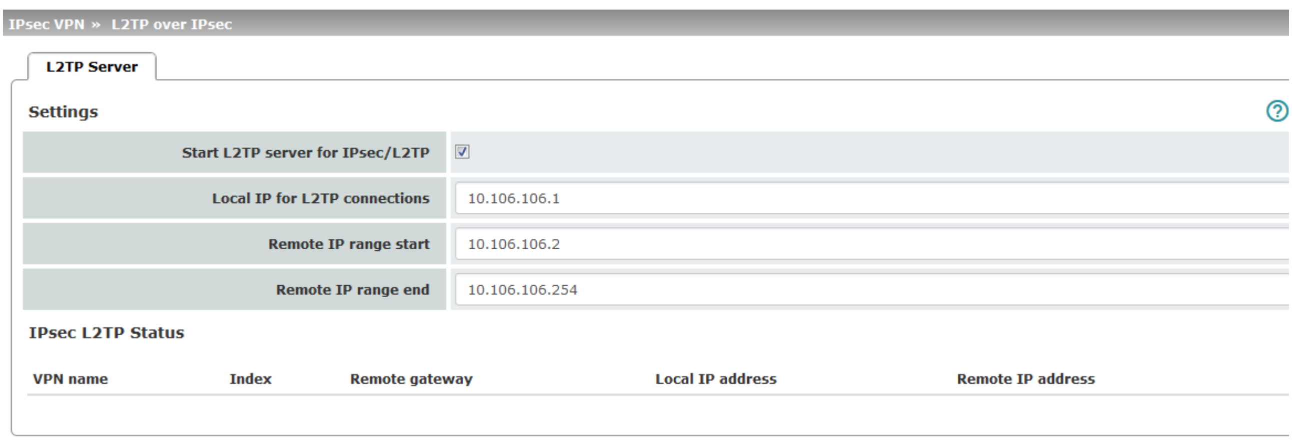
In order to use IPsec/L2TP, the L2TP server must be activated and one or more IPsec connections with the following properties must be defined:

- **Type**: Transport
- **Protocol**: UDP
- **Local:** %all
- **Remote:** %all
- **PFS**: No

See

- IPsec VPN >> Connections >> Edit >> General on Page 326
- IPsec VPN >> Connections >> Edit >> IKE Options, Perfect Forward Secrecy (PFS) on Page 358

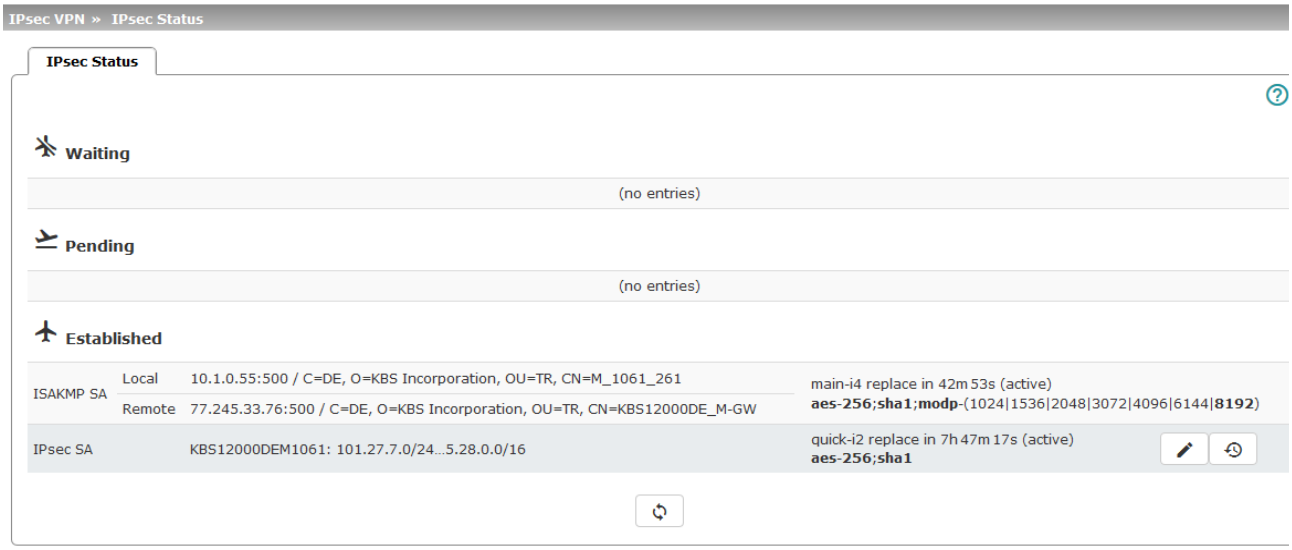
10.3.1 L2TP Server



IPsec VPN >> L2TP over IPsec >> L2TP Server		
Settings	**Start L2TP server for IPsec/L2TP**	If you want to enable IPsec/L2TP connections, activate the function. It is then possible to establish L2TP connections to the mGuard via IPsec, which dynamically assign IP addresses to the clients within the VPN.
	Local IP for L2TP connections	If set as shown in the screenshot above, the mGuard will inform the peer that its address is 10.106.106.1.

IPsec VPN >> L2TP over IPsec >> L2TP Server		
	Remote IP range start/end	If set as shown in the screenshot above, the mGuard will assign the peer an IP address between 10.106.106.2 and 10.106.106.254.
	Status	Displays information about the L2TP status if this connection type has been selected.

10.4 IPsec VPN >> IPsec Status



Displays information about the current status of the configured IPsec connections.

Waiting: displays all VPN connections that have not yet been established which will be started by means of initiation on data traffic or which are waiting for a connection to be established.

Pending: displays all VPN connections that are currently attempting to establish a connection.

The ISAKMP SA has been established and authentication of the connections was completed successfully. If the connection remains in “connection establishment” status the other parameters may not match: does the connection type (Tunnel, Transport) correspond? If “Tunnel” is selected, do the network areas match on both sides?

Established: displays all VPN connections that have successfully established a connection.

The VPN connection has been successfully established and can be used. However, if this is not possible, the VPN gateway of the peer is causing problems. In this case, deactivate and reactivate the connection to reestablish the connection.

Icons

Reload	To update the displayed data, click on the **Reload** icon.
Restart	Click on the **Restart** button if you want to disconnect a line and restart.
Edit	Click on the corresponding icon **Edit rows** to reconfigure a connection.

Connection, ISAKMP SA Status, IPsec SA Status

ISAKMP SA	**Local**	– Local IP address – Local port – ID = subject of an X.509 certificate	State, lifetime, and encryption algorithm for the connection (bold = active)
	Remote	– Remote IP address – Local port – ID = subject of an X.509 certificate	
IPsec SA		– Name of the connection – Local networks ... Remote networks	State, lifetime, and encryption algorithm for the connection (bold = active)

In the event of problems, it is recommended that you check the VPN logs of the peer to which the connection was established. This is because detailed error messages are not forwarded to the initiating computer for security reasons.

11 OpenVPN Client menu

> This menu is not available on the FL MGUARD BLADE controller.

11.1 OpenVPN Client >> Connections

> The OpenVPN client supports the following TLS versions: TLS 1.0, TLS 1.1, TLS 1.2

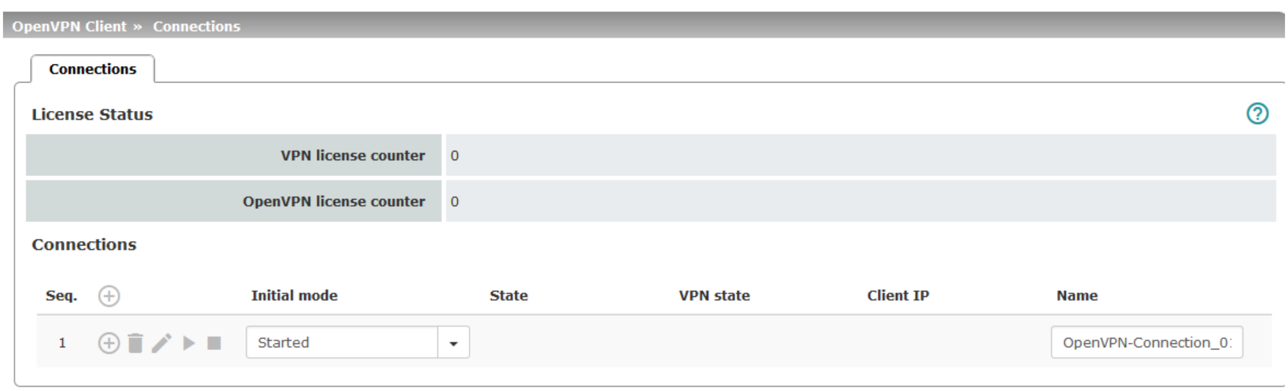
With OpenVPN, an encrypted VPN connection can be established between the mGuard as the OpenVPN client and a peer (OpenVPN server). The OpenSSL library is used for encryption and authentication. Data is transported using the TCP or UDP protocols.

Requirements for a VPN connection

A general requirement for a VPN connection is that the IP addresses of the VPN peers are known and can be accessed.

– mGuard devices provided in stealth network mode are preset to the “multiple clients” stealth configuration. In this mode, you need to configure a management IP address and default gateway if you want to use VPN connections (see “Default gateway” on page 146). Alternatively, you can select a different stealth configuration than the “multiple clients” configuration or use another network mode.
– In order to successfully establish an OpenVPN connection, the VPN peer must support the OpenVPN protocol as the OpenVPN server.

11.1.1 Connections



Lists all the VPN connections that have been defined.

Each connection name listed here can refer to an individual VPN connection. You also have the option of defining new VPN connections, activating and deactivating VPN connections, changing (editing) the VPN connection properties, and deleting connections.

OpenVPN Client >> Connections		
License Status	**VPN license counter**	Number of peers that currently have a VPN connection established using the IPsec protocol.

OpenVPN Client >> Connections[...]		
	OpenVPN license counter	Number of peers to which a VPN connection is currently established using the OpenVPN protocol.

OpenVPN Client >> Connections		
Connections	**Initial mode**	**Disabled / Stopped / Started** The "**Disabled**" setting deactivates the VPN connection permanently; it cannot be started or stopped. The "**Started**" and "**Stopped**" settings determine the status of the VPN connection after restarting/booting the mGuard (e.g., after an interruption in the power supply). VPN connections that are not disabled can be started or stopped via icons on the web interface, via text message, a switch or a pushbutton.
	State	Indicates the current activation state of the OpenVPN connection.
	VPN state	Indicates whether or not the corresponding OpenVPN connection has been established.
	Client IP	IP address of the OpenVPN interface.
	Name	Name of the VPN connection

Connections

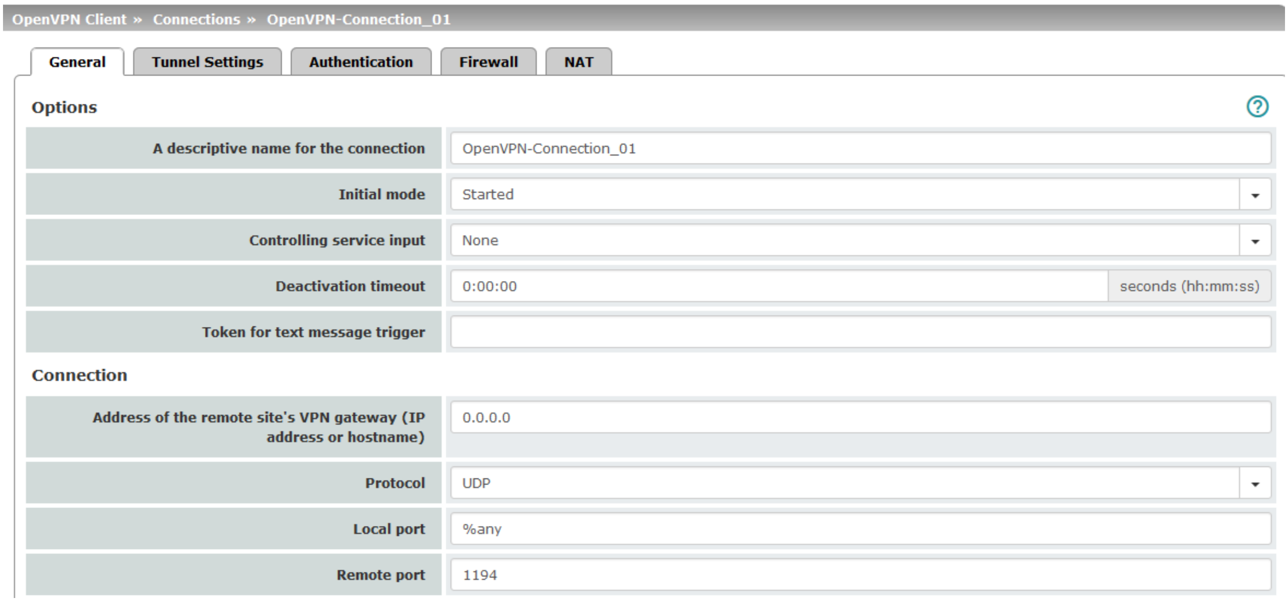
Defining a new VPN connection

- In the connection table, click on the ⊕ **Insert Row** icon to add a new table row.
- Click on the ✎ **Edit Row** icon.

Editing a VPN connection

Click on the ✎ **Edit Row** icon in the relevant row.

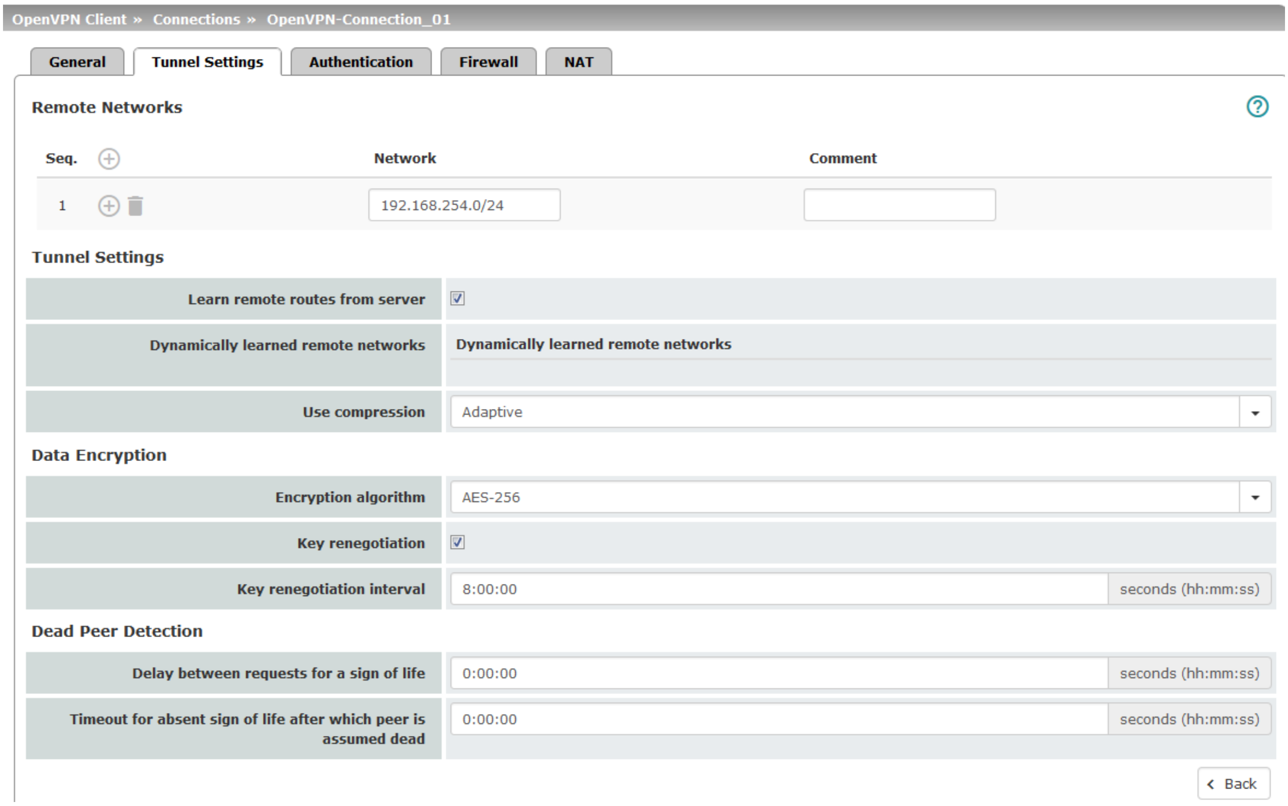
11.1.2 General



OpenVPN Client >> Connections >> Edit >> General		
Options	**A descriptive name for the connection**	The connection can be freely named/renamed.
	Initial mode	**Disabled / Stopped / Started** The “**Disabled**” setting deactivates the VPN connection permanently; it cannot be started or stopped. The “**Started**” and “**Stopped**” settings determine the status of the VPN connection after restarting/booting the mGuard (e.g., after an interruption in the power supply). VPN connections that are not disabled can be started or stopped via icons on the web interface, via text message, a switch or a pushbutton.
	Controlling service input (Only available with the TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4000/RS2000, FL MGUARD RS4004/RS2005, FL MGUARD RS, FL MGUARD GT/GT.)	**None / Service input CMD 1-3** The VPN connection can be switched via a connected pushbutton/switch. The pushbutton/switch must be connected to one of the service contacts (CMD 1-3). If starting and stopping the VPN connection via the CMD contact is enabled, only the CMD contact is authorized to do this. However, if a pushbutton is connected to the CMD contact (instead of a switch – see below), the connection can also be established and released concurrently via a text message, which has the same rights.

	Use inverted control logic	Inverts the behavior of the connected switch. If the switching service input is configured as an on/off switch, it can activate one VPN connection while simultaneously deactivating another which uses inverted logic, for example.
	Deactivation timeout	Time, after which the VPN connection is stopped, if it has been started via a text message, switch, pushbutton or the web interface. The timeout starts on transition to the “Started” state. After the timeout has elapsed, the connection remains in the “Stopped” state until it is restarted. Time in hours, minutes and/or seconds (00:00:00 to 720:00:00, around 1 month). The entry can be in seconds [ss], minutes and seconds [mm:ss] or hours, minutes, and seconds [hh:mm:ss]. 0 means the setting is disabled.
	Token for text message trigger (Only available with the TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G.)	Incoming text messages can be used to start or stop VPN connections. The text message must contain the “*openvpn/start*” or “*openvpn/stop*” command followed by the token.
Connection	**Address of the remote site's VPN gateway**	IP address or host name of the VPN gateway of the peer
	Protocol	**TCP / UDP** The network protocol used by the OpenVPN server must likewise be selected here in the mGuard.
	Local port	The port of the local OpenVPN client from which the connection to an OpenVPN server is initiated. Values: 1 - 65535; default: %any (selection left to the peer)
	Remote port	Port on the remote OpenVPN server that should respond to requests from the OpenVPN client. Values: 1 - 65535; default: 1194

11.1.3 Tunnel Settings

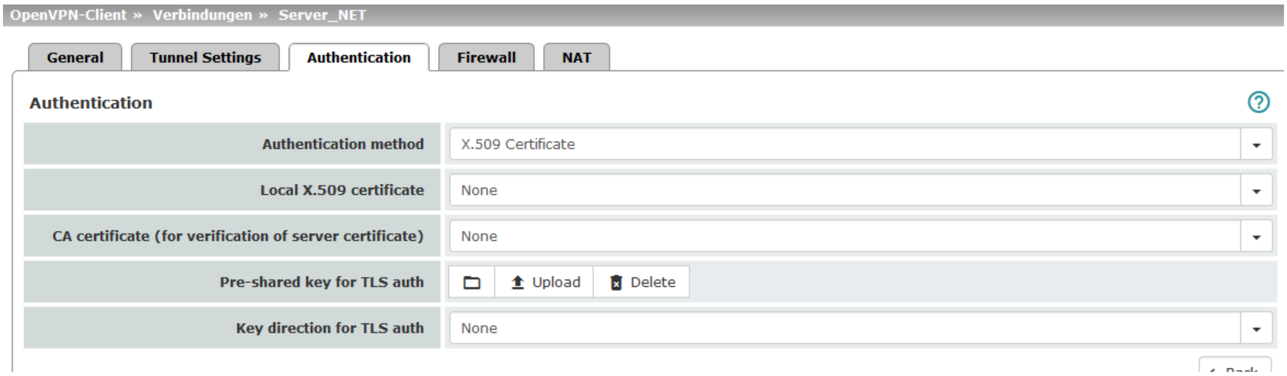


OpenVPN Client >> Connections >> Edit >> Tunnel Settings		
Remote Networks	**Network**	Addresses of networks that are located behind the OpenVPN server (VPN gateway of the peer) (CIDR format).
	Comment	Optional comment text.

Tunnel Settings	**Learn remote routes from server**	When the **function is activated** (default), remote networks are automatically learned from the server if the server is configured accordingly. The routes to remote networks are only known to the mGuard if the corresponding VPN connection is established. If this VPN connection is not in place, network traffic will not be blocked to the relevant IP addresses, instead it will be possible to send network traffic unencrypted via a different interface. In this case, the appropriate firewall rules must be set. Routes to remote networks behind the OpenVPN server can also be overwritten on other interfaces by higher priority routes, e.g., if there are routes with a smaller destination network. If, for example, 10.0.0.0/8 is a route via the OpenVPN interface and 10.1.0.0/16 is a route via the external interface, network traffic will be sent unencrypted to IP address 10.1.0.1 via the external interface. When the **function is deactivated**, the statically entered routes will be used.
	Dynamically learned remote networks	Dynamically learned remote networks are displayed.
	Use compression	**Yes** / **No** / **Adaptive / Disabled** You can select whether compression should always be applied, should never be applied or should be applied adaptively (adapted according to the type of traffic). The option **Disabled** disables compression completely by disabling the use of *liblzo* resp. *comp-lzo*. Note that the server and client must use the same compression settings. This applies in particular to the use of *iblzo* resp. *comp-lzo*.

Data Encryption	**Encryption algorithm**	**Blowfish** / **AES-128** / **AES-192** / **AES-256 (default)** Decide on which encryption algorithm should be used with the administrator of the peer. The Blowfish encryption algorithm is used by default as it is widely used with OpenVPN. **Changed factory default settings in mGuard firmware version 8.6.0** For security reasons, the default encryption algorithm has been changed from the frequently used encryption algorithm **Blowfish** to the more secure algorithm **AES-256**. **Use secure algorithms** If possible, the **AES** encryption algorithm should be used for security reasons (see “Using secure encryption and hash algorithms” on page 19). The following generally applies: the longer the key length (in bits) used by an encryption algorithm (specified by the appended number), the more secure it is. The longer the key, the more time-consuming the encryption procedure.
	Key renegotiation	When the **function is activated** (default), the mGuard will attempt to negotiate a new key when the old one expires.
	Key renegotiation interval	Duration after which the validity of the current key expires and a new key is negotiated between the server and client. Time in hh:mm:ss (default: 8 h)
Dead Peer Detection	If the peer supports Dead Peer Detection, the relevant partners can detect whether the OpenVPN connection is still active or whether it needs to be established again.	
	Delay between requests for a sign of life	Duration after which DPD Keep Alive requests should be transmitted. These requests test whether the peer is still available. Time in hh:mm:ss Default: 00:00:00 (DPD is disabled)
	Timeout for absent sign of life after which peer is assumed dead	Duration after which the connection to the peer should be declared dead if there has been no response to the Keep Alive requests. Time in hh:mm:ss If there is no response, the connection is initiated again by the mGuard. Default: 00:00:00 (DPD is disabled)

11.1.4 Authentication

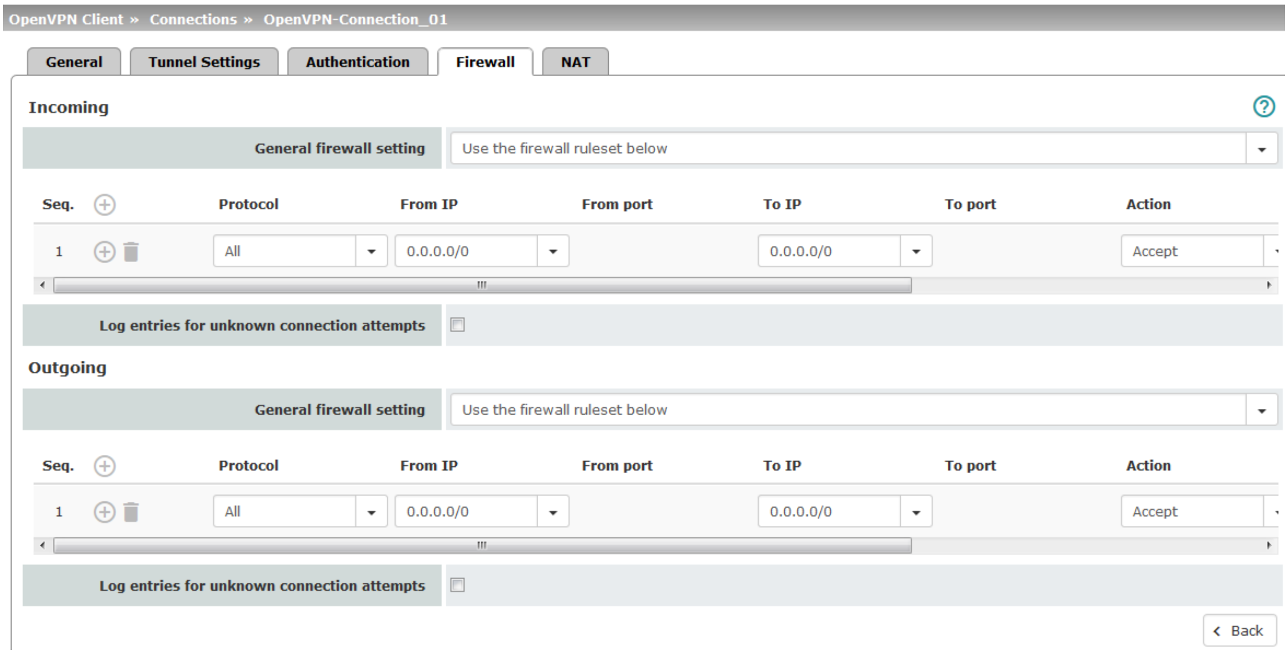


OpenVPN Client >> Connections >> Edit >> Authentication		
Authentication	**Authentication method**	There are three ways in which the mGuard can authenticate itself as an OpenVPN client to the OpenVPN server: – X.509 Certificate (default) – Login/password – X.509 Certificate + login/password The page contains different setting options depending on the method chosen.
	Login	**Authentication method: Login/Password** User identifier (login) that the mGuard uses to authenticate itself to the OpenVPN server.
	Password	Agreed password that is used together with a user identifier (login) for authentication. To achieve adequate security, the string should consist of around 30 randomly selected characters, and should include upper and lower case characters and digits. **Authentication method: X.509 Certificate** Each VPN device has a secret private key and a public key in the form of an X.509 certificate, which contains further information about the certificate's owner and the certification authority (CA). The following must be specified: – How the mGuard authenticates itself to the peer – How the mGuard authenticates the remote peer

OpenVPN Client >> Connections >> Edit >> Authentication		
	Local X.509 certificate	Specifies which machine certificate the mGuard uses as authentication to the VPN peer. Select one of the machine certificates from the selection list. The selection list contains the machine certificates that have been loaded on the mGuard under the *Authentication* >> *Certificates* menu item. If *None* is displayed, a certificate must be installed first. *None* must not be left in place, as this results in no X.509 authentication.
	CA certificate (for verification of server certificate)	Only the CA certificate from the certification authority (CA) that signed the certificate shown by the VPN peer (OpenVPN server) should be referenced here (selection from list). Verification with a CA certificate is also required if the “Login/Password” authentication method is selected. The additional CA certificates that form the chain to the root CA certificate together with the certificate shown by the peer must then be imported into the mGuard under the Authentication >> Certificates menu item. If *None* is displayed, a certificate must be imported first. *None* must not be left in place, as this results in no authentication of the VPN server. The selection list contains all CA certificates that have been imported into the mGuard under the Authentication >> Certificates menu item. With this setting, all VPN peers are accepted, providing they log in with a signed CA certificate issued by a recognized certification authority (CA). The CA is recognized if the relevant CA certificate and all other CA certificates have been loaded on the mGuard. These then form the chain to the root certificate together with the certificates shown.

OpenVPN Client >> Connections >> Edit >> Authentication		
	Pre-shared key for TLS auth	To increase security (e.g., prevent DoS attacks), authentication of the OpenVPN connection can also be protected via pre-shared keys (TLS-PSK). To do so, first a static PSK file (e.g., *ta.key*) must be created and installed and activated on both OpenVPN peers (server and client). The PSK file can: – be created by the OpenVPN server **or** – consist of any file (8 – 2048 bytes). If the file is generated by the server, the key direction can also be selected (see below). To activate TLS authentication, a PSK file must be selected using the icon and uploaded using the **Upload** button. To deactivate TLS authentication, the file must be deleted using the **Delete** button. The **Delete** button is always visible, i.e., even if no PSK file has been uploaded or an uploaded PSK file has been deleted.
	Key direction for TLS auth	**None / 0 / 1** **None** Must be selected if the PSK file was **not** generated by the OpenVPN server. **0 and 1** Can be selected if the PSK file was generated by the OpenVPN server. The selection on the client and server side must be complementary (0 <–>1 or 1 <–> 0) or identical (None <–> None). If the settings are incorrect, the connection will not be established and a log entry will be generated.

11.1.5 Firewall



Incoming/outgoing firewall

While the settings made under the *Network Security* menu item only relate to non-VPN connections (see above under “Network Security menu” on page 257), the settings here only relate to the VPN connection defined on these tabs.

If multiple VPN connections have been defined, you can restrict the outgoing or incoming access individually for each connection. Any attempts to bypass these restrictions can be logged.

By default, the VPN firewall is set to allow all connections for this VPN connection.

However, the extended firewall settings defined and explained above apply independently for each individual VPN connection (see “Network Security menu” on page 257, “Network Security >> Packet Filter” on page 257, “Advanced” on page 278).

If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored.

In *Single Stealth* mode, the actual IP address used by the client should be used in the firewall rules, or it should be left at 0.0.0.0/0, as only one client can be addressed through the tunnel.

> If the **Allow packet forwarding between VPN connections** function is activated on the *Options* tab under the *IPsec VPN* >> *Global* menu item, the rules under **Incoming** are used for the incoming data packets to the mGuard, and the rules under **Outgoing** are applied to the outgoing data packets. This applies for OpenVPN connections as well as for IPsec connections.
>
> If the outgoing data packets are included in the same connection definition, then the firewall rules for **Incoming** and **Outgoing** for the same connection definition are used.
>
> If a different VPN connection definition applies to the outgoing data packets, the firewall rules for **Outgoing** for this other connection definition are used.

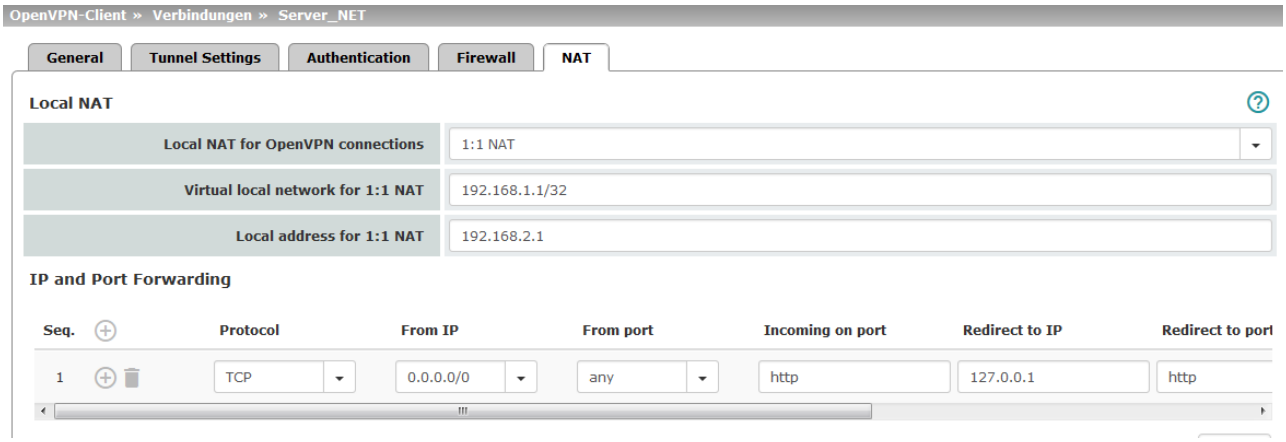
> If the mGuard has been configured to forward SSH connection packets (e.g., by permitting a SEC-Stick hub & spoke connection), existing VPN firewall rules are not applied. This means, for example, that packets of an SSH connection are sent through a VPN tunnel despite the fact that this is prohibited by its firewall rules.

OpenVPN Client >> Connections >> Edit >> Firewall		
Incoming	**General firewall setting**	**Accept all incoming connections**: the data packets of all incoming connections are allowed. **Drop all incoming connections**: the data packets of all incoming connections are discarded. **Accept Ping only:** the data packets of all incoming connections are discarded, except for ping packets (ICMP). **Use the firewall ruleset below**: displays further setting options.
	The following settings are only visible if “**Use the firewall ruleset below**” is set.	

OpenVPN Client >> Connections >> Edit >> Firewall		
	Protocol	**All** means TCP, UDP, ICMP, GRE, and other IP protocols.
	From IP/To IP	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 26). **Name of IP groups**, if defined. When a name is specified for an IP group, the host names, IP addresses, IP areas or networks saved under this name are taken into consideration (see “IP/Port Groups” on page 275). If host names are used in IP groups, the mGuard must be configured so that the host name of a DNS server can be resolved in an IP address. If a host name from an IP group cannot be resolved, this host will not be taken into consideration for the rule. Further entries in the IP group are not affected by this and are taken into consideration. On mGuard devices from the RS2000 series, it is not possible to use host names in IP groups. **Incoming**: – From IP: IP address in the VPN tunnel – To IP: 1:1 NAT address or the actual address **Outgoing**: – From IP: 1:1 NAT address or the actual address – To IP: IP address in the VPN tunnel
	From port / To port (Only for TCP and UDP protocols)	**any** refers to any port. **startport:endport** (e.g., 110:120) refers to a port range. Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110). **Name of port groups**, if defined. When a name is specified for a port group, the ports or port ranges saved under this name are taken into consideration (see “IP/Port Groups” on page 275).

OpenVPN Client >> Connections >> Edit >> Firewall		
	Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back and the sender is informed of their rejection. (In *Stealth* mode, Reject has the same effect as Drop.) **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts. **Name of rule records**, if defined. When a name is specified for rule records, the firewall rules configured under this name take effect (see Rule Records tab). For security reasons, rule records that contain IP groups with host names should not be used in firewall rules which execute “Drop” or “Reject” as the action. On mGuard devices from the RS2000 series, it is not possible to use rule records. **Name of Modbus TCP rule records**, if defined. When a Modbus TCP rule record is selected, the firewall rules configured under this rule record take effect (see “Modbus TCP” on page 284).
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – activate *Log* function – Should not be logged – deactivate *Log* function (default)
	Log entries for unknown connection attempts	When the function is activated, all connection attempts that are not covered by the rules defined above are logged.
Outgoing	The explanation provided under “Incoming” also applies to “Outgoing”.	

11.1.6 NAT



The IP address (OpenVPN client IP address) that the mGuard uses as the OpenVPN client is assigned to it by the OpenVPN server of the peer.

If NAT is not used, the local networks of the mGuard, from which the OpenVPN connection should be used, must be statically configured in the OpenVPN server. It is therefore recommended that you use NAT, i.e., that local routes (local IP addresses within the private address area) are rewritten to the OpenVPN client IP address so that devices in the local network can use the OpenVPN connection.

OpenVPN Client >> Connections >> Edit >> NAT		
Local NAT	For outgoing data packets, the device can rewrite the specified sender IP addresses from its internal network to its OpenVPN client IP address, a technique referred to as NAT (Network Address Translation). This method is used if the internal addresses cannot or should not be routed externally, e.g., because a private address area such as 192.168.x.x or the internal network structure should be hidden. In the **default setting (0.0.0.0/0)**, all networks positioned behind the mGuard are masqueraded and can use the OpenVPN connection.	
	Local NAT for OpenVPN connections	**No NAT / 1:1 NAT / Masquerade** It is possible to translate the IP addresses of devices located at the local end of the OpenVPN tunnel, (e.g., behind the mGuard). **No NAT**: NAT is not performed. With **1:1 NAT**, the IP addresses of devices at the local end of the tunnel are exchanged so that each individual address is translated into another specific address. With **Masquerade**, the IP addresses of devices at the local end of the tunnel are exchanged with an IP address that is identical for all devices.

OpenVPN Client >> Connections >> Edit >> NAT		
	Virtual local network for 1:1 NAT (When "1:1 NAT" was selected)	Configures the virtual IP address area to which the actual local IP addresses are translated when 1:1 NAT is used. The netmask specified in CIDR format also applies to the Local address for *1:1-NAT* (see below). If the function **Allow packet forwarding between VPN connections** was activated under *IPsec VPN >> Global >> Options*, use of the virtual local network addresses in other OpenVPN connections is not supported.
	Local address for 1:1-NAT (When "1:1 NAT" was selected)	Configures the local IP address area from which IP addresses are translated into the virtual IP addresses through the use of 1:1-NAT in the *Virtual local network for 1:1-NAT* defined above (see above). The netmask specified for the *Virtual local network for 1:1-NAT* applies (see above).
	Network (When "Masquerading" was selected)	Internal networks whose device IP addresses are translated into the OpenVPN client IP address. **0.0.0.0/0** means that all internal IP addresses are subject to the NAT procedure. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 26). The masquerading of remote networks can be configured under *Network >> NAT >> Masquerading* (see "Masquerading" on page 198). When the **Local NAT/Masquerading** function is used, IP and port forwarding must also be used (see below) in order to access devices in the local network of the mGuard from the remote network.
	Comment	Freely selectable comment for this rule.
IP and Port Forwarding	Lists the rules defined for IP and port forwarding (DNAT = Destination NAT). IP and port forwarding (**DNAT**) performs the following: the headers of incoming data packets from the OpenVPN tunnel, which are addressed to the OpenVPN client IP address of the mGuard and to a specific port of the mGuard, are rewritten in order to forward them to a specific computer in the internal network and to a specific port on this computer. In other words, the IP address and port number in the header of incoming data packets are changed. If port forwarding is used, the packets pass through the mGuard firewall without taking into consideration the rules configured under *Network Security >> Packet Filter >> Incoming Rules*.	

OpenVPN Client >> Connections >> Edit >> NAT		
	Protocol: TCP / UDP / GRE	Specify the protocol to which the rule should apply (**TCP** / **UDP** / **GRE**). **GRE protocol** IP packets can be forwarded. However, only one GRE connection is supported at any given time. If more than one device sends GRE packets to the same external IP address, the mGuard may not be able to feed back reply packets correctly. We recommend only forwarding GRE packets from specific transmitters. These could be ones that have had a forwarding rule set up for their source address by entering the transmitter address in the “From IP” field, e.g., 193.194.195.196/32.
	From IP	The sender address for forwarding. **0.0.0.0/0** means all addresses. To specify an address area, use CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 26). **Name of IP groups**, if defined. When a name is specified for an IP group, the host names, IP addresses, IP areas or networks saved under this name are taken into consideration (see “IP/Port Groups” on page 275). If host names are used in IP groups, the mGuard must be configured so that the host name of a DNS server can be resolved in an IP address. If a host name from an IP group cannot be resolved, this host will not be taken into consideration for the rule. Further entries in the IP group are not affected by this and are taken into consideration.
	From port	The sender port for forwarding. **any** refers to any port. Either the port number or the corresponding service name can be specified here, e.g., *pop3* for port 110 or *http* for port 80. **Name of port groups**, if defined. When a name is specified for a port group, the ports or port ranges saved under this name are taken into consideration (see “IP/Port Groups” on page 275).
	Incoming on port	The original destination port specified in the incoming data packets. Either the port number or the corresponding service name can be specified here, e.g., *pop3* for port 110 or *http* for port 80. This information is not relevant for the “GRE” protocol. It is ignored by the mGuard.

OpenVPN Client >> Connections >> Edit >> NAT		
	Redirect to IP	The internal IP address to which the data packets should be forwarded and into which the original destination addresses are translated.
	Redirect to port	Internal port to which the data packets should be forwarded and into which the original port is translated.
	Comment	Freely selectable comment for this rule.
	Log	For each individual port forwarding rule, you can specify whether the use of the rule: – Should be logged – activate *Log* function – Should not be logged – deactivate *Log* function (default)

12 SEC-Stick menu

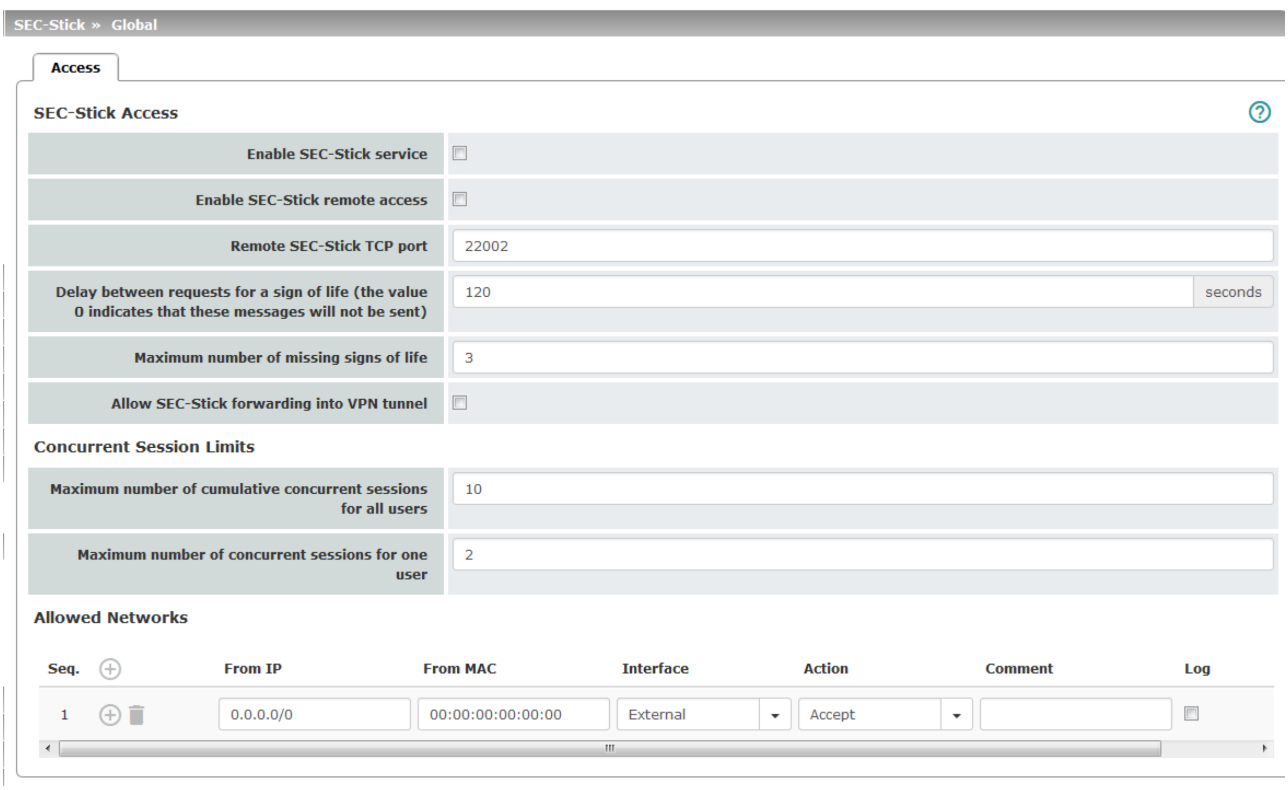
The mGuard supports the use of an SEC-Stick, which is an access protector for IT systems. The SEC-Stick is a product from team2work: www.team2work.de.

The SEC-Stick is essentially a key. The user inserts it into the USB port of a computer with an Internet connection, and can then set up an encrypted connection to the mGuard in order to securely access defined services in the office or home network. The Remote Desktop Protocol, for example, can be used within the encrypted and secure SEC-Stick connection to control a PC remotely in the office or at home, as if the user was sitting directly in front of it.

In order for this to work, access to the business PC is protected by the mGuard and the mGuard must be configured for the SEC-Stick to permit access. This is because the user of this remote computer, into which the SEC-Stick is inserted, authenticates himself/herself to the mGuard using the data and software stored on his/her SEC-Stick.

The SEC-Stick establishes an SSH connection to the mGuard. Additional tunnels can be embedded into this connection, e.g., TCP/IP connections.

12.1 Global



SEC-Stick >> Global >> Access		
SEC-Stick Access (This menu item is not included in the scope of functions for TC MGUARD RS2000 3G, TC MGUARD RS2000 4G, FL MGUARD RS2005 or FL MGUARD RS2000.)	Access via the SEC-Stick requires a license. It can only be used if the corresponding license has been purchased and installed.	
	Enable SEC-Stick service	When activated, the function specifies that the SEC-Stick being used at a remote location or its owner can log in. In this case, SEC-Stick remote access must also be enabled (next option).
	Enable SEC-Stick remote access	When the function is activated, SEC-Stick remote access is enabled.
	Remote SEC-Stick TCP port	Default: 22002 If this port number is changed, the new port number only applies for access via the *External, External 2, DMZ, GRE* or *VPN* interface. Port number 22002 still applies for internal access.
	Delay between requests for a sign of life	Default: 120 seconds Values from 0 to 3600 seconds can be set. Positive values indicate that the mGuard is sending a request to the peer within the encrypted SSH connection to find out whether it can still be accessed. This request is sent if no activity was detected from the peer for the specified number of seconds (e.g., due to network traffic within the encrypted connection). The value entered here relates to the functionality of the encrypted SSH connection. As long as it is working properly, the SSH connection is not terminated by the mGuard as a result of this setting, even when the user does not perform any actions during this time. As the number of simultaneously open sessions is limited (see *Maximum number of cumulative concurrent sessions for all users*), it is important to terminate sessions that have expired. Therefore, the request for a sign of life is preset to 120 seconds for Version 7.4.0 or later. If a maximum of three requests for a sign of life are issued, this causes an expired session to be detected and removed after six minutes. In previous versions, the preset was “0”. This means that no requests for a sign of life are sent. Please note that sign of life requests generate additional traffic.
	Maximum number of missing signs of life	Specifies the maximum number of times a sign of life request to the peer may remain unanswered. For example, if a sign of life request should be made every 15 seconds and this value is set to 3, the SEC-Stick client connection is deleted if a sign of life is not detected after approximately 45 seconds.

SEC-Stick >> Global >> Access [...]		
	Allow SEC-Stick forwarding into VPN tunnel	Allows SSH connections to be forwarded in a VPN tunnel (Hub & Spoke).
Concurrent Session Limits	The number of simultaneous sessions is limited for SEC-Stick connections. Approximately 0.5 MB of memory are required for each session to ensure the maximum level of security. The restriction does not affect existing sessions; it only affects newly established connections.	
	Maximum number of cumulative concurrent sessions for all users	0 to 2147483647 Specifies the number of connections that are permitted for all users simultaneously. When “0” is set, no session is permitted.
	Maximum number of concurrent sessions for one user	0 to 2147483647 Specifies the number of connections that are permitted for one user simultaneously. When “0” is set, no session is permitted.
Allowed Networks	**Lists the firewall rules that have been set up for SEC-Stick remote access** If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored. The rules specified here only take effect if the **Enable SSH remote access** function has been activated. Access via *Internal* is also possible if this function is deactivated. A firewall rule that would deny access via *Internal* does therefore not apply in this case. **Multiple rules can be specified.**	
	From IP	Enter the address of the computer/network from which access is permitted or forbidden in this field. IP address: **0.0.0.0/0** means all addresses. To specify an address area, use CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 26).
	Interface	**Internal / External / External 2 / DMZ / VPN / GRE / Dial-in**[1] Specifies to which interface the rule should apply. If no rules are set or if no rule applies, the following default settings apply: – SEC-Stick remote access is permitted via *Internal, DMZ, VPN*, and *Dial-in*. – Access via *External*, *External 2*, and *GRE* is denied. Specify the access options according to your requirements. If you want to deny access via *Internal, DMZ, VPN* or *Dial-in*, you must implement this explicitly by means of corresponding firewall rules, for example, by specifying *Drop* as the action.

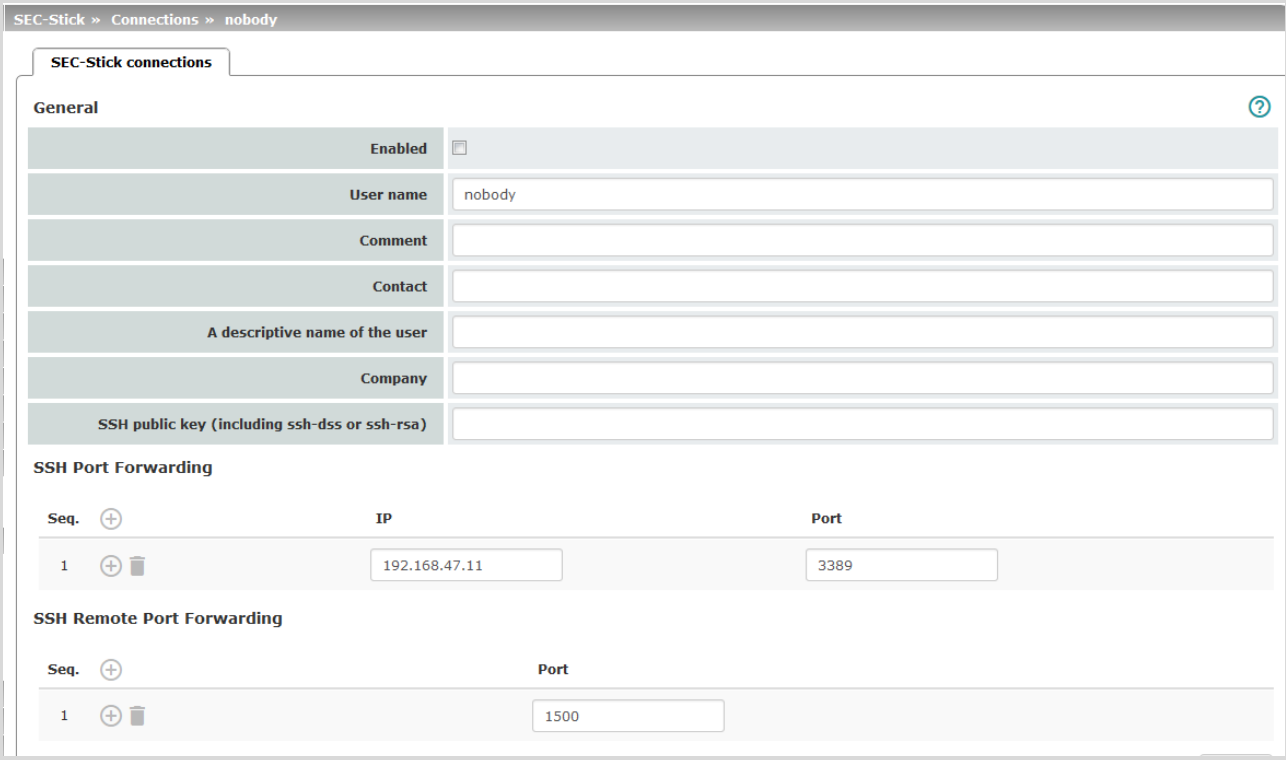
SEC-Stick >> Global >> Access [...]		
	Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back and the sender is informed of their rejection. (In *Stealth* mode, *Reject* has the same effect as *Drop*.) **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts. **Name of rule records**, if defined. When a name is specified for rule records, the firewall rules saved under this name take effect (see Rule Records tab page). For security reasons, rule records that contain IP groups with host names should not be used in firewall rules which execute “Drop” or “Reject” as the action.
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – set *Log* to **Yes** – Should not be logged – set *Log* to **No** (default setting)

1 *External 2* and *Dial-in* are only for devices with a serial interface (see “Network >> Interfaces” on page 127).

12.2 Connections

SEC-Stick >> Connections >> SEC-Stick Connections		
SEC-Stick Connections	List of defined SEC-Stick connections. Not all of the SEC-Stick functions can be configured via the web interface of the mGuard.	
	Enabled	To use a defined SEC-Stick connection, the **Enabled** option must be activated.
	User name	An SEC-Stick connection with a uniquely assigned user name must be defined for every owner of an SEC-Stick who has authorized access. This user name is used to uniquely identify the defined connections.
	A descriptive name of the user	Name of the person.
	Company	Name of the company.
	The following page appears when you click on the **Edit Row** icon:	

SEC-Stick >> Connections >> SEC-Stick Connections [...]



General	**Enabled**	As above
	User name	As above
	Comment	Optional comment text.
	Contact	Optional comment text.
	A descriptive name of the user	Optional: name of the person (repeated)
	Company	Optional: as above
	SSH public key (including ssh-dss or ssh-rsa)	Enter the SSH public key belonging to the SEC-Stick in ASCII format in this field. The secret equivalent is stored on the SEC-Stick.
SSH Port Forwarding	List of allowed access and SSH port forwarding relating to the SEC-Stick of the corresponding user.	
	IP	IP address of the computer to which access is enabled.
	Port	Port number to be used when accessing the computer.
SSH Remote Port Forwarding	**Port**	Port that is used for SSH remote port forwarding.

13 QoS menu

This menu is **not** available on the **FL MGUARD RS2000, TC MGUARD RS2000 3G, TC MGUARD RS2000 4G**, and **FL MGUARD RS2005**.

QoS (Quality of Service) refers to the quality of individual transmission channels in IP networks. This relates to the allocation of specific resources to specific services or communication types so that they work correctly. For example, the necessary bandwidth must be provided to transmit audio or video data in real time in order to reach a satisfactory communication level. At the same time, slower data transfer by FTP or e-mail does not threaten the overall success of the transmission process (file or e-mail transfer).

13.1 Ingress filters

An ingress filter prevents the processing of certain data packets by filtering and dropping them before they enter the mGuard processing mechanism. The mGuard can use an ingress filter to avoid processing data packets that are not needed in the network. This results in faster processing of the remaining, i.e., required data packets.

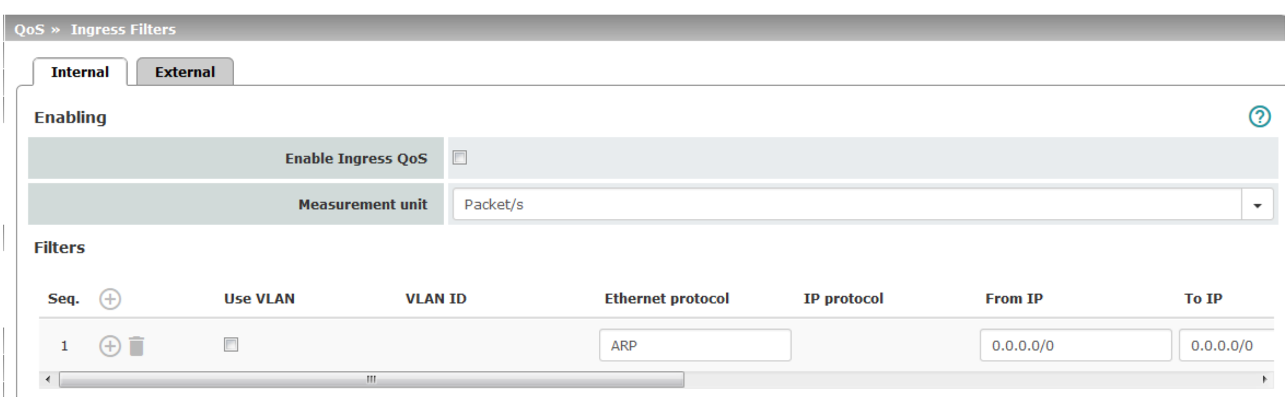
Using suitable filter rules, administrative access to the mGuard can be ensured with high probability, for example.

Packet processing on the mGuard is generally defined by the handling of individual data packets. This means that the processing performance depends on the number of packets to be processed and not on the bandwidth.

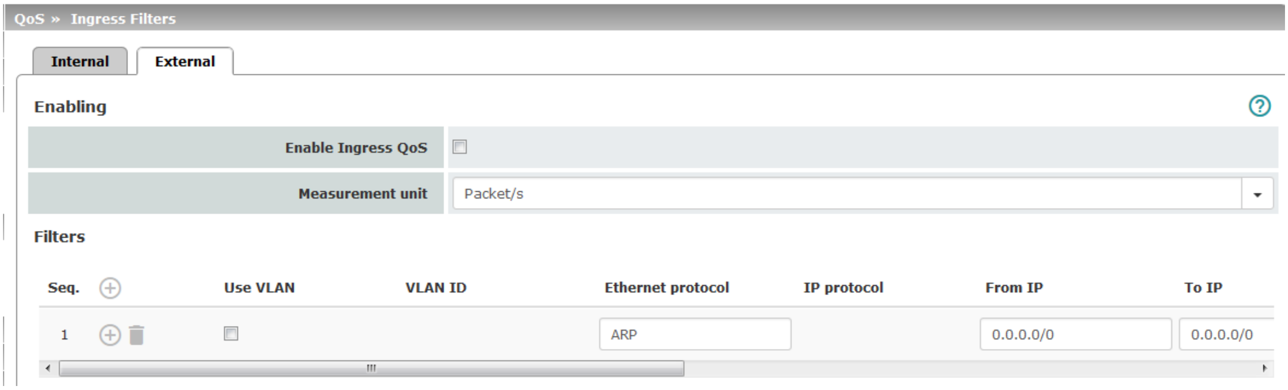
Filtering is performed exclusively according to features that are present or may be present in each data packet: the sender and receiver IP address specified in the header, the specified Ethernet protocol, the specified IP protocol, the specified TOS/DSCP value, and/or the VLAN ID (if VLANs have been set up). As a check must be carried out to see if the filter rules apply to each individual data packet, the list of filter rules should be kept as short as possible. Otherwise, the time spent on filtering could be longer than the time actually saved by setting the filter.

Please note that not all specified filter criteria should be combined. For example, it does not make sense to specify an additional IP protocol in the same rule set that contains the ARP Ethernet protocol. Nor does it make sense to specify a sender or receiver IP address if the IPX Ethernet protocol is specified (in hexadecimal format).

13.1.1 Internal/External



Internal: settings for ingress filters at the LAN interface



External: settings for ingress filters at the WAN interface

QoS >> Ingress Filters >> Internal/External		
Enabling	**Enable Ingress QoS**	**Deactivated** (default): this feature is disabled. If filter rules are defined, they are ignored. **Activated**: this feature is enabled. Data packets may only pass through and be forwarded to the mGuard for further evaluation and processing if they comply with the filter rules defined below. Filters can be set for the LAN port (**Internal** tab) and the WAN port (**External** tab).
	Measurement unit	**kbit/s / Packet/s** Specifies the unit of measurement for the numerical values entered further down under **Guaranteed** and **Upper limit**.
Filter	**Use VLAN**	If a VLAN is set up, the relevant VLAN ID can be specified to allow the relevant data packets to pass through. **Use VLAN** must not be activated if VLAN is already activated in the interface settings of the corresponding interface (internal or external).
	VLAN ID (When **Use VLAN** is activated)	Specifies that the VLAN data packets that have this VLAN ID may pass through.
	Ethernet protocol	Specifies that only data packets of the specified Ethernet protocol may pass through. Possible entries: **ARP**, **IPV4**, **%any**. Other entries must be in hexadecimal format (up to 4 digits). (The ID of the relevant protocol in the Ethernet header is entered here. It can be found in the publication of the relevant standard.)
	IP protocol	**All / TCP / UDP / ICMP / ESP** Specifies that only data packets of the selected IP protocol may pass through. When set to **All**, no filtering is applied according to the IP protocol.

QoS >> Ingress Filters >> Internal/External [...]		
	From IP	Specifies that only data packets from the specified IP address may pass through. **0.0.0.0/0** stands for all addresses, i.e., in this case no filtering is applied according to the IP address of the sender. To specify an address area, use CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 26).
	To IP	Specifies that only data packets that should be forwarded to the specified IP address may pass through. Entries correspond to *From IP*, as described above. **0.0.0.0/0** stands for all addresses, i.e., in this case no filtering is applied according to the IP address of the sender.
	Current TOS/DSCP	Each data packet contains a TOS or DSCP field. (TOS stands for Type of Service, DSCP stands for Differentiated Services Code Point.) The traffic type to which the data packet belongs is specified here. For example, an IP phone will write a different entry in this field for outgoing data packets compared to an FTP program. When a value is selected here, only data packets with this value in the TOS or DSCP field may pass through. When set to **All**, no filtering according to the TOS/DSCP value is applied.
	Guaranteed	The number entered specifies how many data packets per second or kbps can pass through at all times – according to the option set under **Measurement unit** (see above). This applies to the data stream that conforms to the rule set criteria specified on the left (i.e., that may pass through). The mGuard **may** drop the excess number of data packets in the event of capacity bottlenecks if this data stream delivers more data packets per second than specified.
	Upper limit	The number entered specifies the maximum number of data packets per second or kbps that can pass through – according to the option set under **Measurement unit** (see above). This applies to the data stream that conforms to the rule set criteria specified on the left (i.e., that may pass through). The mGuard drops the excess number of data packets if this data stream delivers more data packets per second than specified.
	Comment	Optional comment text.

13.2 Egress Queues

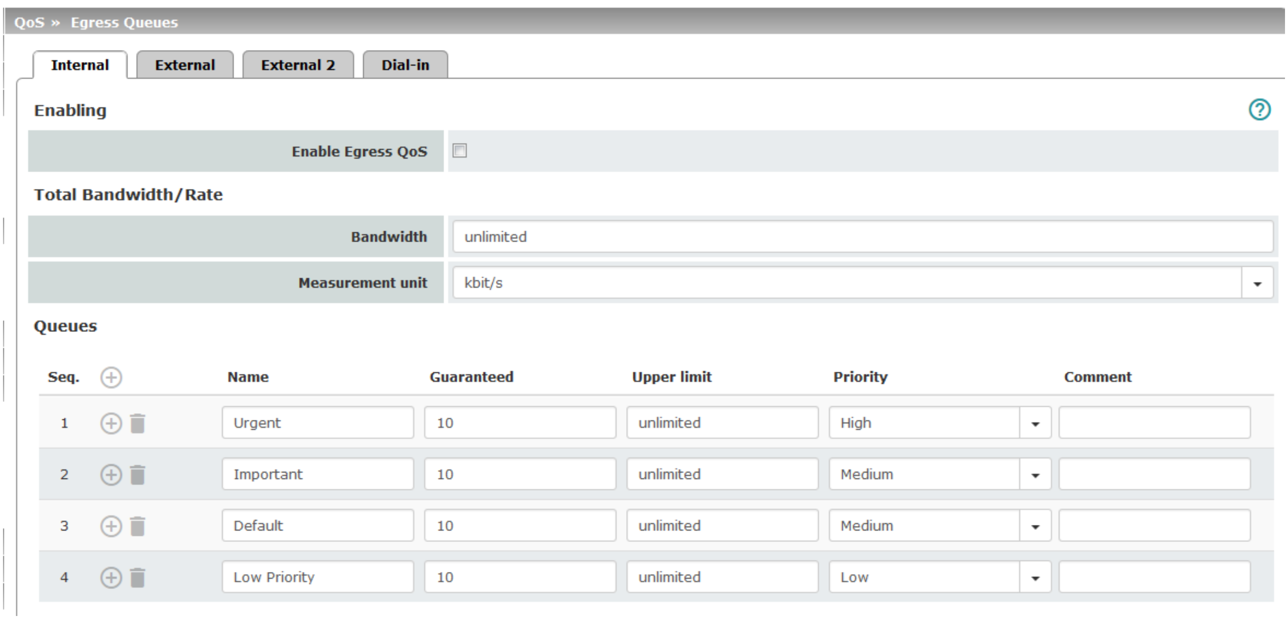
The services are assigned corresponding priority levels. In the event of connection bottlenecks, the outgoing data packets are placed in egress queues (i.e., queues for pending packets) according to the assigned priority level and are then processed according to their priority. Ideally, the assignment of priority levels and bandwidths should result in a sufficient bandwidth level always being available for the real-time transmission of data packets, while other packets, e.g., FTP downloads, are temporarily set to wait in critical cases.

The main application of egress QoS is the optimal utilization of the available bandwidth on a connection. In certain cases, it may be useful to limit the packet rate, e.g., to protect a slow computer from overloading in the protected network.

The *Egress Queues* function can be used for all interfaces. Up to mGuard firmware version 8.6.x, the function can also be used for VPN connections. In firmware version 8.7.0 the use of QoS in VPN connections is no longer possible.

13.2.1 Internal/External/External 2/Dial-in

Internal: settings for egress queues at the LAN interface



External/External 2/Dial-in:

The tabs for egress queues at the WAN interface (External), the secondary external interface (External 2), and for packets for PPP dial-up connection (Dial-in) feature the same setting options as the tabs for the LAN interface (Internal).

In all cases, the settings relate to the data that is sent externally into the network from the relevant mGuard interface.

QoS menu >> Egress Queues >> Internal/External/External 2/Dial-in		
Enabling	**Enable Egress QoS**	**Deactivated** (default): this feature is disabled. **Activated**: this feature is enabled. This option is recommended if the interface is connected to a network with low bandwidth. This enables bandwidth allocation to be influenced in favor of particularly important data.
Total Bandwidth/Rate	**Bandwidth**	Total maximum bandwidth that is physically available – specified in kbps or packets per second (see below: **Measurement unit**). In order to optimize prioritization, the total bandwidth specified here should be slightly lower than the actual amount. This prevents a buffer overrun on the transferring devices, which would result in adverse effects.
	Measurement unit	**kbit/s / Packet/s** Specifies the unit of measurement for the numerical values (see above: **Bandwidth**).
Queues	**Name**	The default name for the egress queue can be adopted or another can be assigned. The name does not specify the priority level.
	Guaranteed	Bandwidth that should be available at all times for the relevant queue. Based on the selection under **Measurement unit** (**kbit/s** or **Packet/s**), meaning that the unit of measurement does not have to be specified explicitly here. The total of all guaranteed bandwidths must be less than or equal to the total bandwidth.
	Upper limit	Maximum bandwidth available that may be set for the relevant queue by the system. Based on the selection under **Measurement unit** (**kbit/s** or **Packet/s**), meaning that the unit of measurement does not have to be specified explicitly here. The value must be greater than or equal to the guaranteed bandwidth. The value **unlimited** can also be specified, which means that there is no further restriction.
	Priority	**Low / Medium / High** Specifies with which priority the relevant queue, if available, should be processed, provided the total available bandwidth has not been exhausted.
	Comment	Optional comment text.

13.3 Egress Queues (VPN)

The *Egress Queues (VPN)* function is no longer available in mGuard firmware version **8.7.0**.

An update to mGuard firmware version 8.7.0 from an older firmware version with activated *Egress Queues (VPN)* function is not possible.

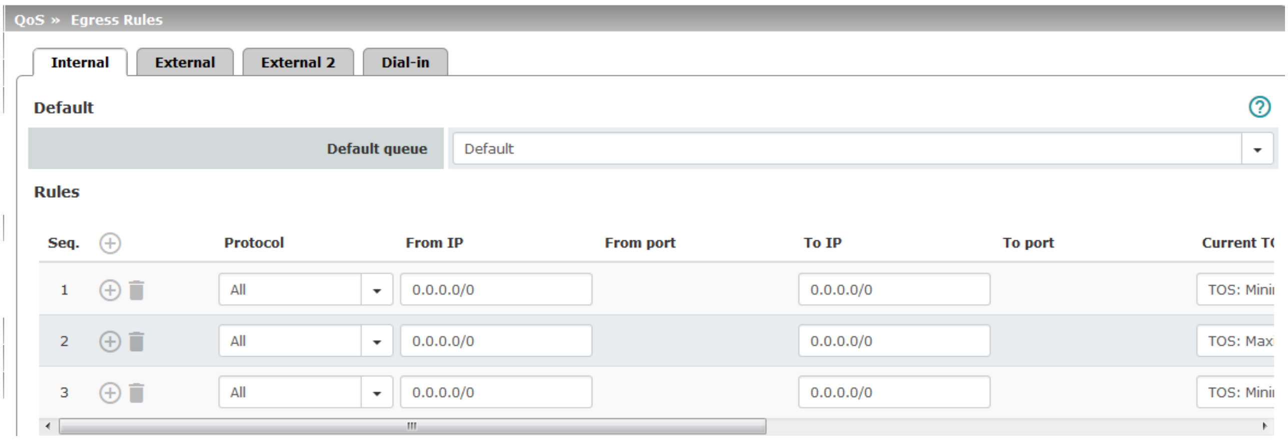
13.4 Egress Rules

This page defines the rules for the data that is assigned to the defined egress queues (see above) in order for the data to be transmitted with the priority assigned to the relevant queue.

Rules can be defined separately for all interfaces and for VPN connections.

13.4.1 Internal/External/External 2/Dial-in

Internal: settings for egress queue rules



External/External 2/Dial-in:

The tabs for egress queue rules at the WAN interface (External), the secondary external interface (External 2), and for packets for PPP dial-up connection (Dial-in) feature the same setting options as the tabs for the LAN interface (Internal).

In all cases, the settings relate to the data that is sent externally into the network from the relevant mGuard interface.

QoS >> Egress Rules >> Internal/External/External 2/Dial-in		
Default	**Default queue**	*Name of the egress queue* (user-defined). The names of the queues are displayed as listed or specified under *Egress Queues* on the *Internal/External/VPN via External* tabs. The following default names are defined: Default/Urgent/Important/Low Priority. Traffic that is **not** assigned to a specific egress queue under *Rules* remains in the *default queue*. You can specify which egress queue should be used as the *default queue* in this selection list.
Rules	The assignment of specific data traffic to an egress queue is based on a list of criteria. If the criteria in a row apply to a data packet, it is assigned to the egress queue specified in the row. **Example**: for audio data to be transmitted, you have defined a queue with guaranteed bandwidth and priority under Egress Queues (see page 392) under the name *Urgent*. You then define the rules here for how audio data is detected and specify that this data should belong to the *Urgent* queue.	

QoS >> Egress Rules >> Internal/External/External 2/Dial-in		
	Protocol	**All / TCP / UDP / ICMP / ESP** Protocol(s) relating to the rule.
	From IP	IP address of the network or device from which the data originates. **0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 26). Assign the traffic from this source to the queue selected under *Queue name* in this row.
	From port (Only for TCP and UDP protocols)	Port used at the source from which the data originates. **any** refers to any port. **startport:endport** (e.g., 110:120) refers to a port range. Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110).
	To IP	IP address of the network or device to which the data is sent. Entries correspond to *From IP*, as described above.
	To port (Only for TCP and UDP protocols)	Port used at the source where the data is sent. Entries correspond to *From port*, as described above.
	Current TOS/DSCP	Each data packet contains a TOS or DSCP field. (TOS stands for Type of Service, DSCP stands for Differentiated Services Code Point.) The traffic type to which the data packet belongs is specified here. For example, an IP phone will write a different entry in this field for outgoing data packets compared to an FTP program that uploads data packets to a server. When a value is selected here, only data packets that have this value in the TOS or DSCP field are chosen. These values are then set to a different value according to the entry in the **New TOS/DSCP** field.
	New TOS/DSCP	If you want to change the TOS/DSCP values of the data packets that are selected using the defined rules, enter the text that should be written in the TOS/DSCP field here. For a more detailed explanation of the **Current TOS/DSCP** and **New TOS/DSCP** options, please refer to the following RFC documents: – RFC 3260 “New Terminology and Clarifications for Diffserv” – RFC 3168 “The Addition of Explicit Congestion Notification (ECN) to IP” – RFC 2474 “Definition of the Differentiated Services Field (DS Field)” – RFC 1349 “Type of Service in the Internet Protocol Suite”
	Queue name	Name of the egress queue to which traffic should be assigned.

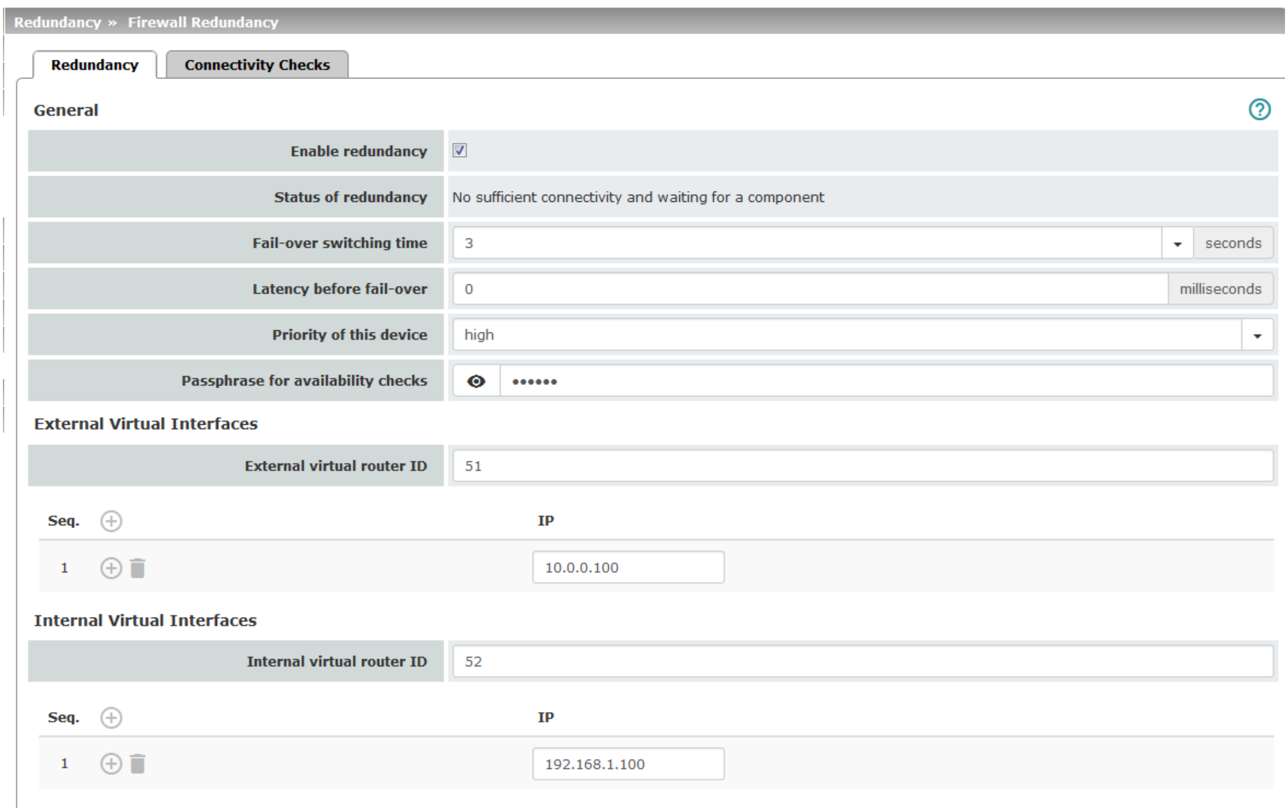
QoS >> Egress Rules >> Internal/External/External 2/Dial-in		
	Comment	Optional comment text.

13.5 Egress Rules (VPN)

> The *Egress Rules (VPN)* function is no longer available in mGuard firmware version **8.7.0**.
>
> An update to mGuard firmware version 8.7.0 from an older firmware version with activated *Egress Rules (VPN)* function is not possible.

14 Redundancy menu

i	Redundancy is described in detail in Section 17, “Redundancy”.
i	To use the redundancy function, both mGuards must have the same firmware.
i	When the redundancy function is activated, VLAN cannot be used in Stealth mode.



14.1 Redundancy >> Firewall Redundancy

> This menu is **not** available on the **FL MGUARD RS2000, FL MGUARD RS2005, TC MGUARD RS2000 3G,** and **TC MGUARD RS2000 4G**.

14.1.1 Redundancy

Redundancy >> Firewall Redundancy >> Redundancy		
General	**Enable redundancy**	**Deactivated** (default): firewall redundancy is disabled. **Activated**: firewall redundancy is enabled. This function can only be activated when a suitable license key is installed. Further conditions apply if VPN redundancy is to be enabled at the same time, see "VPN redundancy" on page 437.
	Status of redundancy	Shows the current status.
	Fail-over switching time	Maximum time that is allowed to elapse in the event of errors before switching to the other mGuard.
	Latency before fail-over	**0 ... 10,000 milliseconds, default: 0** Time the redundancy system ignores an error. The connectivity and availability checks ignore an error unless it is still present after the time set here has elapsed.
	Priority of this device	**high/low** Specifies the priority associated with the presence notifications (CARP). Set the priority to **high** on the mGuard that you want to be active. The mGuard on standby is set to **low**. Both mGuard devices in a redundancy pair may either be set to different priorities or to **high** priority. . Never set **both** mGuard devices in a redundancy pair to **low** priority.

Redundancy >> Firewall Redundancy >> Redundancy		
	Passphrase for availability checks	On an mGuard which is part of a redundancy pair, checks are constantly performed to determine whether an active mGuard is available and whether it should remain active. A variation of the CARP (Common Address Redundancy Protocol) is used here. CARP uses SHA-1 HMAC encryption together with a password. This password must be set so it is the same for both mGuard devices. It is used for encryption and is never transmitted in plain text. The password is important for security since the mGuard is vulnerable at this point. We recommend a password with at least 20 characters and several special characters (printable UTF-8 characters). It must be changed on a regular basis.

When changing the password, proceed as follows:

Set the new password on both mGuard devices. It does not matter which order you do this in but the same password must be used in both cases. If you inadvertently enter an incorrect password, follow the instructions under “How to proceed in the event of an incorrect password” on page 402.

As soon as a redundancy pair has been assigned a new password, it automatically negotiates when it can switch to the new password without interruption.

If an mGuard fails while the password is being changed, the following scenarios apply:

- Password replacement has been started on all mGuard devices and then interrupted because of a network error, for example. This scenario is rectified automatically.
- Password replacement has been started on all mGuard devices. However, one mGuard then fails and must be replaced.
- Password replacement has been started but not performed on all mGuard devices because they have failed. Password replacement must be started as soon as a faulty mGuard is back online. If an mGuard has been replaced, it must first be configured with the old password before it is connected.

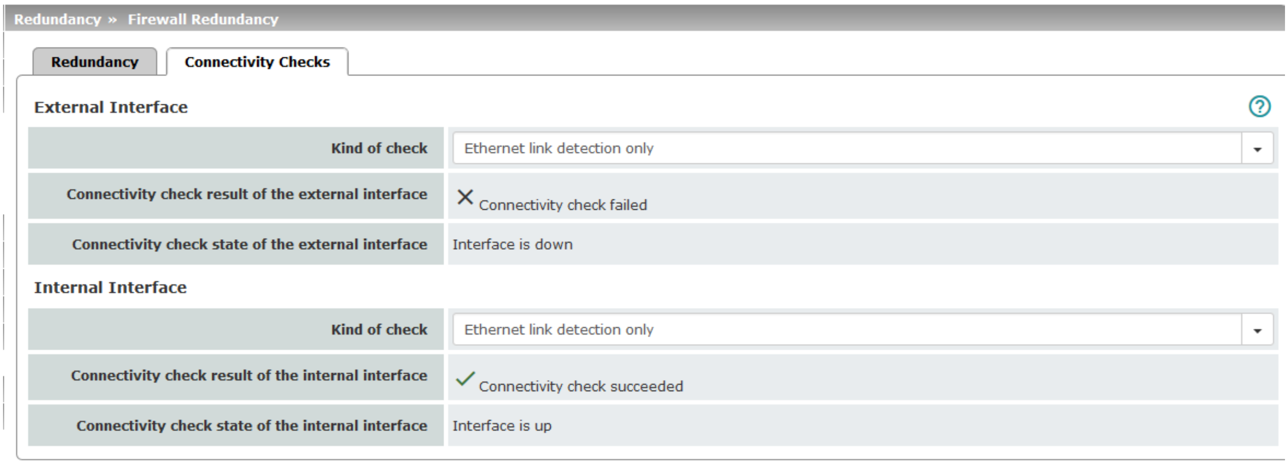
Redundancy >> Firewall Redundancy >> Redundancy		
	How to proceed in the event of an incorrect password If you have inadvertently entered an incorrect password on an mGuard, proceed as follows. **If you can still remember the old password, proceed as follows:** • Reconfigure the mGuard on which the incorrect password was entered so that it uses the old password. • Wait until the mGuard indicates that the old password is being used. • Then enter the correct password. **If you have forgotten the old password, proceed as follows:** • Check whether you can read the old password from the other mGuard. • If the other mGuard is disabled or missing, you can simply enter the correct new password on the active mGuard on which you inadvertently set the incorrect password. Make sure that the other mGuard is assigned the same password before operating it again. • If the other mGuard is already using the new password, you must make sure that the mGuard with the incorrect password is not active or able to be activated, e.g., by removing the cable at the LAN or WAN interface. In the case of remote access, you can enter a destination for the connectivity check that will not respond. Prior to provoking this type of error, check that there is no redundancy error on any of the mGuard devices. One mGuard must be active and the other must be on standby. If necessary, rectify any errors displayed and only then use this method. After that, follow these steps: – Replace the incorrect password with a different one. – Enter this password on the active mGuard too. – Restart the mGuard that is not active. You can do this, for example, by reconnecting the Ethernet cable or restoring the old settings for the connectivity check.	
External Virtual Interfaces	**External virtual router ID**	**1, 2, 3, ... 255 (default: 51)** Only in Router network mode. This ID is sent by the redundancy pair with each presence notification (CARP) via the external interface and is used to identify the redundancy pair. This ID must be the same for both mGuard devices. It is used to differentiate the redundancy pair from other redundancy pairs that are connected to the same Ethernet segment via their external interface. Please note that CARP uses the same protocol and port as VRRP (Virtual Router Redundancy Protocol). The ID set here must be different to the IDs on other devices which use VRRP or CARP and are located in the same Ethernet segment.

Redundancy >> Firewall Redundancy >> Redundancy		
	External virtual IP addresses	Default: 10.0.0.100 Only in Router network mode. These are IP addresses which are shared by both mGuard devices as virtual IP addresses of the external interface. These IP addresses must be the same for both mGuard devices. These addresses are used as a gateway for explicit static routes for devices located in the same Ethernet segment as the external network interface of the mGuard. The active mGuard can receive ICMP requests via this IP address. It responds to these ICMP requests according to the menu settings under *Network Security >> Packet Filter >> Advanced*. No network masks or VLAN IDs are set up for the virtual IP addresses as these attributes are defined by the real external IP address. For each virtual IP address, a real IP address must be configured whose IP network accommodates the virtual address. The mGuard transmits the network mask and VLAN setting from the real external IP address to the corresponding virtual IP address. The applied VLAN settings determine whether standard MTU settings or VLAN MTU settings are used for the virtual IP address. Firewall redundancy cannot function correctly if a real IP address and network mask are not available.
Internal Virtual Interfaces	**Internal virtual router ID**	**1, 2, 3, ... 255 (default: 52)** Only in Router network mode. This ID is sent by the redundancy pair with each presence notification (CARP) via the external and internal interface and is used to identify the redundancy pair. This ID must be set so it is the same for both mGuard devices. It is used to differentiate the redundancy pair from other Ethernet devices that are connected to the same Ethernet segment via their external/internal interface. Please note that CARP uses the same protocol and port as VRRP (Virtual Router Redundancy Protocol). The ID set here must be different to the IDs on other devices which use VRRP or CARP and are located in the same Ethernet segment.

Redundancy >> Firewall Redundancy >> Redundancy		
	Internal virtual IP addresses	As described under *External virtual IP addresses*, but with two exceptions. Under **Internal virtual IP addresses**, IP addresses are defined for devices which belong to the internal Ethernet segment. These devices must use the IP address as their default gateway. These addresses can be used as a DNS or NTP server when the mGuard is configured as a server for the protocols. For each virtual IP address, a real IP address must be configured whose IP network accommodates the virtual address. The response to ICMP requests with internal virtual IP addresses is independent from the settings made under *Network Security >> Packet Filter >> Advanced.*
Encrypted State Synchronization (No longer available)	**With mGuard firmware 8.8.0, the "Encrypted State Synchronization" is no longer available** An update to firmware version 8.8.0 is only possible if the function "Encrypted State Synchronization" has been deactivated before.	
Interface for State Synchronization (Only for mGuard centerport (Innominate), FL MGUARD CENTERPORT)	**Interface which is used for state synchronization**	**Internal Interface/Dedicated Interface** The *mGuard centerport (Innominate), FL MGUARD CENTERPORT* supports a **dedicated interface**. This is a reserved, direct Ethernet interface or a dedicated LAN segment, via which the state synchronization is sent. The redundancy pair can be connected via an additional dedicated Ethernet interface or an interconnected switch. When set to **Dedicated Interface**, presence notifications (CARP) are also listened for on the third Ethernet interface. Presence notifications (CARP) are also sent when the mGuard is active. However, no additional routing is supported for this interface. Frames received on this interface are not forwarded for security reasons. The connection status of the third Ethernet interface can be queried via SNMP.

Redundancy >> Firewall Redundancy >> Redundancy		
	IP of the dedicated interface (Only available when **Dedicated Interface** is selected.)	**IP** IP address used on the third network interface of the *mGuard centerport (Innominate), FL MGUARD CENTERPORT* for state synchronization with the other mGuard. Default: 192.168.68.29 **Netmask** Network mask used on the third network interface of the *mGuard centerport (Innominate), FL MGUARD CENTERPORT* for state synchronization with the other mGuard. Default: 255.255.255.0 **Use VLAN** When **Yes** is selected, a VLAN ID is used for the third network interface. **VLAN ID** 1, 2, 3, ... 4094 (default: 1) VLAN ID if this setting is activated.
	Disable the availability check at the external interface (Only available when **Dedicated Interface** is selected.)	When the **function is activated**, no presence notifications (CARP) are sent or received via the external interface. This is useful in some scenarios for protection against external attacks.

14.1.2 Connectivity Checks



Targets can be configured for the internal and external interface in the connectivity check. It is important that these targets are actually connected to the specified interface. An ICMP echo reply cannot be received by an external interface when the corresponding target is connected to the internal interface (and vice versa). When the static routes are changed, the targets may easily not be checked properly.

Redundancy >> Firewall Redundancy >> Connectivity Checks		
External Interface	**Kind of check**	Specifies whether a connectivity check is performed on the external interface, and if so, how. If **Ethernet link detection only** is selected, then only the state of the Ethernet connection is checked. If **at least one target must respond** is selected, it does not matter whether the ICMP echo request is answered by the primary or secondary target. The request is only sent to the secondary target if the primary target did not provide a suitable response. In this way, configurations can be supported where the devices are only provided with ICMP echo requests if required. If **all targets of one set must respond** is selected, then both targets must respond. If a secondary target is not specified, then only the primary target must respond.
	Connectivity check result of the external interface	Indicates whether the connectivity check was successful (green check mark).
	Connectivity check state of the external interface	Indicates the status of the connectivity check.

Redundancy >> Firewall Redundancy >> Connectivity Checks		
Primary External Targets (for ICMP echo requests) (Not available when **Ethernet link detection only** is selected.)	**IP**	This is an unsorted list of IP addresses used as targets for ICMP echo requests. We recommend using the IP addresses of routers, especially the IP addresses of default gateways or the real IP address of the other mGuard. Default: 10.0.0.30, 10.0.0.31 (for new addresses) Each set of targets for state synchronization can contain a maximum of ten targets.
Secondary External Targets (for ICMP echo requests) (Not available when **Ethernet link detection only** is selected.)	**IP**	(See above) Only used if the primary targets check has failed. Failure of a secondary target is not detected in normal operation. Default: 10.0.0.30, 10.0.0.31 (for new addresses) Each set of targets for state synchronization can contain a maximum of ten targets.
Internal Interface	**Kind of check**	Specifies whether a connectivity check is performed on the internal interface, and if so, how. If **Ethernet link detection only** is selected, then only the state of the Ethernet connection is checked. The Ethernet link cannot be checked on devices with an internal switch. This affects: TC MGUARD RS4000/RS2000 4G, TC MGUARD RS4000/RS2000 3G, and FL MGUARD RS4004/RS2005. If **at least one target must respond** is selected, it does not matter whether the ICMP echo request is answered by the primary or secondary target. The request is only sent to the secondary target if the primary target did not provide a suitable response. In this way, configurations can be supported where the devices are only provided with ICMP echo requests if required. If **all targets of one set must respond** is selected, then both targets must respond. If a secondary target is not specified, then only the primary target must respond.
	Connectivity check result of the internal interface	Indicates whether the connectivity check was successful (green check mark).
	Connectivity check state of the internal interface	Indicates the status of the connectivity check.
Primary Internal Targets (for ICMP echo requests) (Not available when **Ethernet link detection only** is selected.)		(See above) Default: 192.168.1.30, 192.168.1.31 (for new addresses)

Redundancy >> Firewall Redundancy >> Connectivity Checks	
Secondary Internal Targets (for ICMP echo requests) (Not available when **Ethernet link detection only** is selected.)	(See above) Default: 192.168.1.30, 192.168.1.31 (for new addresses)

14.2 Ring/Network Coupling

The ring/network coupling function is **not** supported by all mGuard devices.

14.2.1 Ring/Network Coupling

Redundancy >> Firewall Redundancy >> Ring/Network Coupling		
Settings	**Enable ring/network coupling/dual homing**	When activated, the status of the Ethernet connection is transmitted from one port to another in Stealth mode. This means that interruptions in the network can be traced easily.
	Redundancy port	**Internal / External** **Internal**: if the connection is lost/established on the LAN port, the WAN port is also disabled/enabled. **External**: if the connection is lost/established on the WAN port, the LAN port is also disabled/enabled.

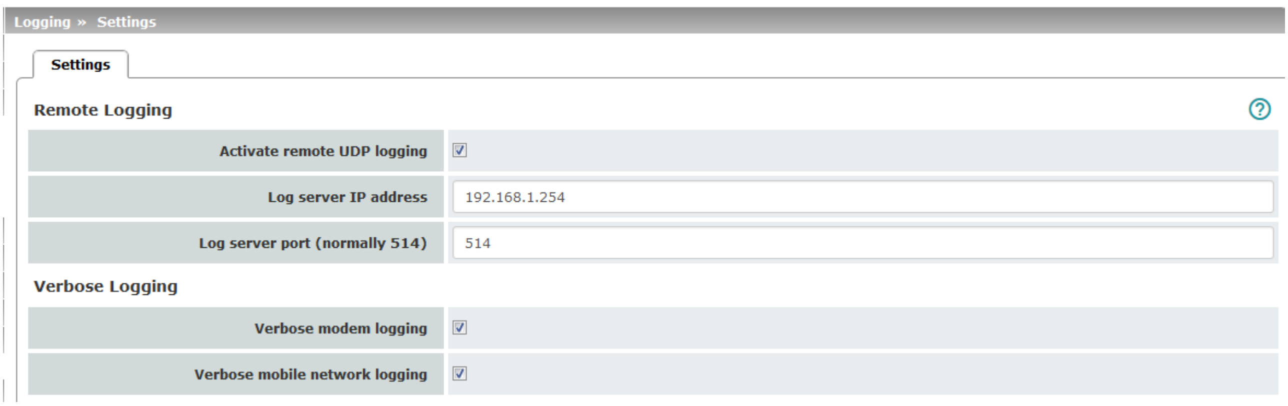
15 Logging menu

Logging refers to the recording of event messages, e.g., regarding settings that have been made, the application of firewall rules, errors, etc.

Log entries are recorded in various categories and can be sorted and displayed according to these categories (see “Logging >> Browse Local Logs” on page 413).

15.1 Logging >> Settings

15.1.1 Settings



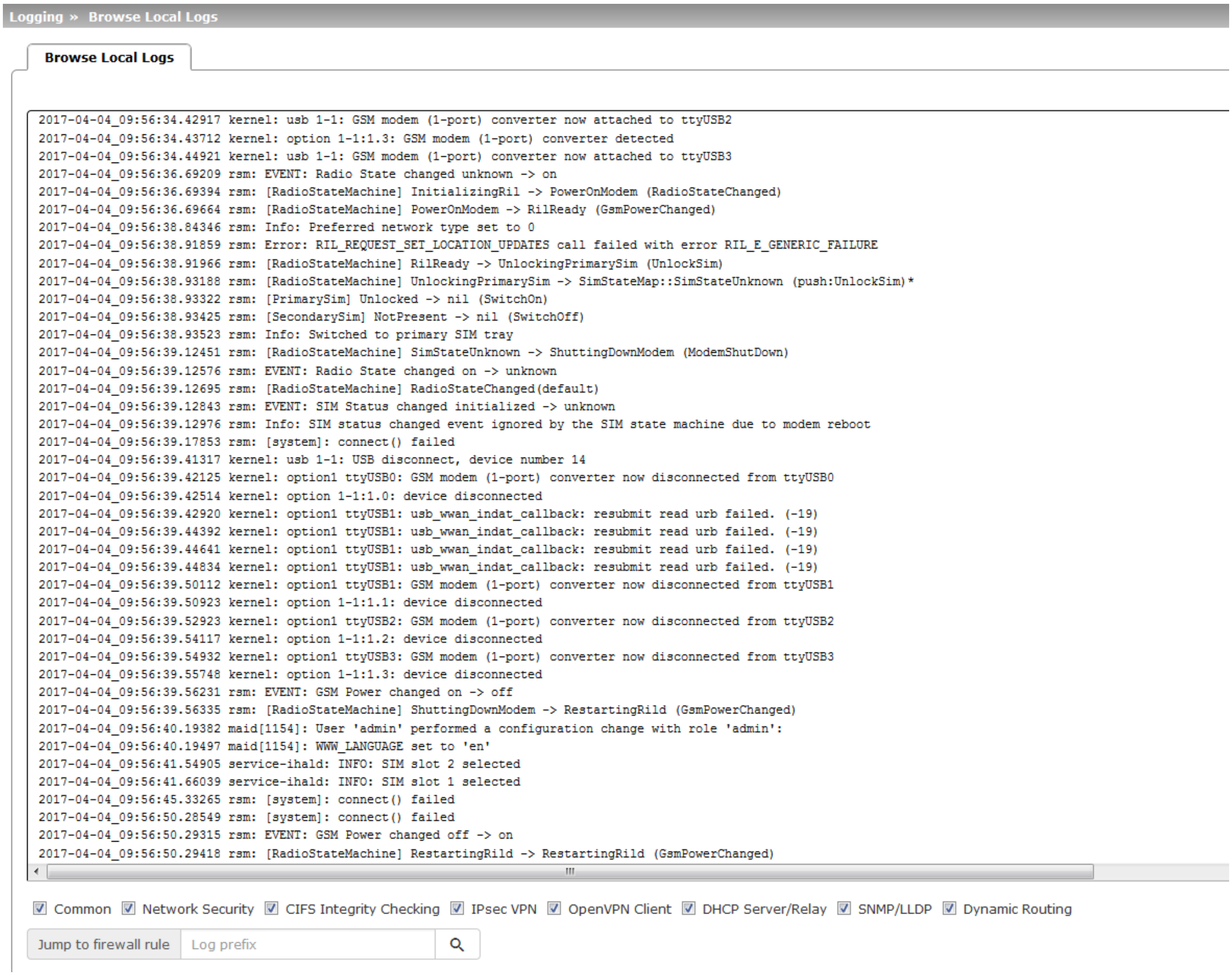
All log entries are recorded in the RAM of the mGuard by default. Once the maximum memory space for log entries has been used up, the oldest log entries are automatically overwritten by new entries. In addition, all log entries are deleted when the mGuard is switched off.

To prevent this, log entries can be transmitted to an external computer (remote server). This is particularly useful if you wish to manage the logs of multiple mGuard devices centrally.

Logging >> Settings		
Remote Logging	**Activate remote UDP logging**	If you want all log entries to be transmitted to the external log server (specified below), activate the function.
	Log server IP address	Specify the IP address of the log server to which the log entries should be transmitted via UDP. An IP address must be specified, not a host name. This function does not support name resolution because it might not be possible to make log entries if a DNS server fails.
	Log server port	Specify the port of the log server to which the log entries should be transmitted via UDP. Default: 514

Logging >> Settings [...]		
		If log messages should be transmitted to a remote server via a VPN tunnel, the IP address of the remote server must be located in the network that is specified as the **Remote** network in the definition of the VPN connection. The internal IP address must be located in the network that is specified as **Local** in the definition of the VPN connection (see IPsec VPN >> Connections >> Edit >> General).
		– If the IPsec VPN >> Connections >> Edit >> General, **Local** option is set to **1:1 NAT** (see page 338), the following applies: The internal IP address must be located in the specified local network. – If the IPsec VPN >> Connections >> Edit >> General, **Remote** option is set to **1:1 NAT** (see page 340), the following applies: The IP address of the remote log server must be located in the network that is specified as **Remote** in the definition of the VPN connection.
Verbose logging	**Verbose modem logging**	Only available if an internal or external modem is available and switched on. – Internal modem: TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS with internal analog modem or ISDN modem – External modem: FL MGUARD RS4000/RS2000, TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G, FL MGUARD RS4004/RS2005, mGuard centerport (Innominate), FL MGUARD CENTERPORT, FL MGUARD RS, FL MGUARD BLADE, mGuard delta (Innominate), FL MGUARD DELTA Verbose logging
	Verbose mobile network logging	Only available with the TC MGUARD RS4000/RS2000 3G, TC MGUARD RS4000/RS2000 4G Verbose logging

15.2 Logging >> Browse Local Logs



The corresponding check boxes for filtering entries according to their category are displayed below the log entries, depending on which mGuard functions were active.

To display one or more categories, enable the check boxes for the desired categories. The log entries are continuously updated according to the selection.

To pause or continue the continuous updating of the log entries, click on the **Pause** or **Continue** button.

Access to log entries

The log entries can be accessed in various ways.

Table 15-1 Viewing log entries

mGuard	UDP	Web interface (web UI)
/var/log/cifsscand	socklog	CIFS Integrity Checking
/var/log/dhclient	No	Common
/var/log/dhcp-ext	No	DHCP Server/Relay
/var/log/dhcp-int	No	DHCP Server/Relay
/var/log/dnscache	No	No
/var/log/dynrouting	socklog	Dynamic Routing
/var/log/firestarter	svlogd	IPsec VPN
/var/log/firewall	svlogd	Network Security
/var/log/fwrulesetd	socklog	Network Security
/var/log/gsm	No	Common
/var/log/https	No	No
/var/log/ipsec	socklog	IPsec VPN
/var/log/l2tp	No	IPsec VPN
/var/log/lldpd	No	SNMP/LLDP
/var/log/login	No	No
/var/log/maid	No	No
/var/log/main	socklog	Common
/var/log/maitrigger	No	No
/var/log/openvpn	socklog	OpenVPN Client
/var/log/pluto	svlogd	IPsec VPN
/var/log/psm-sanitize	No	Common
/var/log/pullconfig	socklog	Common
/var/log/redundancy	socklog	Common

Table 15-1 Viewing log entries

mGuard	UDP	Web interface (web UI)
/var/log/snmp	No	SNMP/LLDP
/var/log/tinydns	No	Common
/var/log/userfwd	socklog	Network Security

15.2.1 Log entry categories

Logging >> Browse Local Logs >> Categories	
General	Log entries that cannot be assigned to other categories.
Network Security	Logged events are shown here if the logging of events was selected when defining the firewall rules (Log = enabled). **Log ID and number for tracing errors** Log entries that relate to the firewall rules listed below have a log ID and number. This log ID and number can be used to trace the firewall rule to which the corresponding log entry relates and that led to the corresponding event. **Firewall rules and their log ID** – Packet filters: Network Security >> Packet Filter >> Incoming Rules menu Network Security >> Packet Filter >> Outgoing Rules menu Log ID: ***fw-incoming*** or ***fw-outgoing*** – Firewall rules for VPN connections: IPsec VPN >> Connections >> Edit >> Firewall menu, Incoming/Outgoing Log ID: ***fw-vpn-in*** or ***fw-vpn-out*** – Firewall rules for OpenVPN connections: OpenVPN Client >> Connections >> Edit >> Firewall menu, Incoming/Outgoing Log ID: ***fw-openvpn-in*** or ***fw-openvpn-out*** OpenVPN Client >> Connections >> Edit >> NAT menu Log ID: ***fw-openvpn-portfw*** – Firewall rules for web access to the mGuard via HTTPS: Management >> Web Settings >> Access menu Log ID: ***fw-https-access*** – Firewall rules for access to the mGuard via SNMP: Management >> SNMP >> Query menu Log ID: ***fw-snmp-access*** – Firewall rules for SSH remote access to the mGuard: Management >> System Settings >> Shell Access menu Log ID: ***fw-ssh-access*** – Firewall rules for access to the mGuard via NTP: Management >> System Settings >> Time and Date menu Log ID: ***fw-ntp-access*** – Firewall rules for the user firewall: Network Security >> User Firewall menu, Firewall Rules Log ID: ***ufw-*** – Rules for NAT, port forwarding: Network >> NAT >> IP and Port Forwarding menu Log ID: ***fw-portforwarding***

Logging >> Browse Local Logs >> Categories	
	– Firewall rules for the serial interface: Network >> Interfaces >> Dial-in menu Incoming rules: log ID: ***fw-serial-incoming*** Outgoing rules: log ID: ***fw-serial-outgoing***

Searching for firewall rules based on a network security log

As of mGuard firmware version 8.6.0, firewall log entries in the list are highlighted in blue and provided with a hyperlink. A click on the firewall log entry, e. g. *fw-https-access-1-1ec2c133-dca1-1231-bfa5-000cbe01010a* opens the configuration page (menu >> sub-menu >> tab) with the firewall rule that caused the log entry.

When using mGuard firmware versions < 8.6.0, proceed as follows:

If the **Network Security** check box is enabled so that the relevant log entries are displayed, the **Jump to firewall rule** search field is displayed below the *Reload logs* button.

Proceed as follows if you want to trace the firewall rule referenced by a log entry in the *Network Security* category and which resulted in the corresponding event:

Proceed as follows if you want to trace the firewall rule referenced by a log entry in the *Network Security* category and which resulted in the corresponding event:

1. Select the section that contains the log ID and number in the relevant log entry, for example: **fw-https-access-1-1ec2c133-dca1-1231-bfa5-000cbe01010a**

2. Copy this section to the **Jump to firewall rule** field.
3. Click on the **Lookup** button.

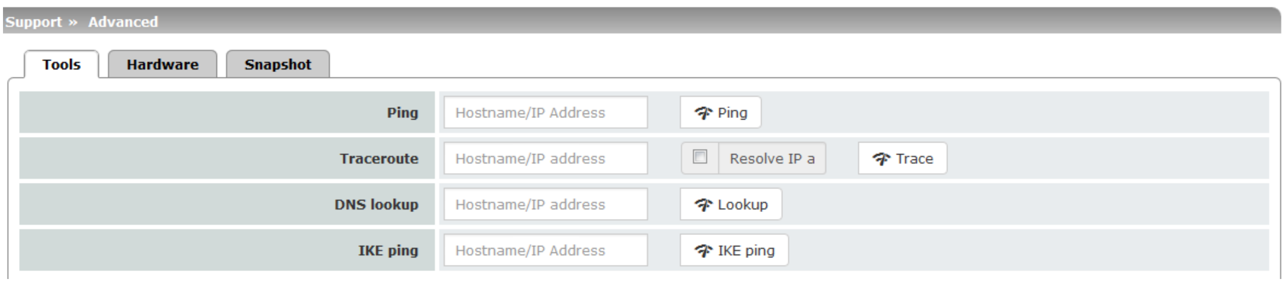
The configuration page containing the firewall rule that the log entry refers to is displayed.

Logging >> Browse Local Logs >> Categories	
FL MGUARD BLADE	In addition to error messages, the following messages are output on the FL MGUARD BLADE controller: (The areas enclosed by < and > are replaced by the relevant data in the log entries.) **General messages:** blade daemon "<version>" starting ... Blade[<bladenr>] online Blade[<bladenr>] is mute Blade[<bladenr>] not running Reading timestamp from blade[<bladenr>] **When activating a configuration profile on a blade:** Push configuration to blade[<bladenr>] reconfiguration of blade[<bladenr>] returned <returncode> blade[<bladenr>] # <text> **When retrieving a configuration profile from a blade:** Pull configuration from blade[<bladenr>] Pull configuration from blade[<bladenr>] returned <returncode>
CIFS Integrity Checking	Messages relating to the integrity check of network drives are displayed in this log. In addition, messages that occur when connecting the network drives and are required for the integrity check are also visible.
IPsec VPN	Lists all VPN events. The format corresponds to standard Linux format. There are special evaluation programs that present information from the logged data in a more easily readable format.
OpenVPN Client	Lists all OpenVPN events.
DHCP Server/Relay	Messages from the services that can be configured under Network >> DHCP.
SNMP/LLDP	Messages from the services that can be configured under Management >> SNMP.
Dynamic Routing	Lists all events that are generated by dynamic routing.

16 Support menu

16.1 Support >> Advanced

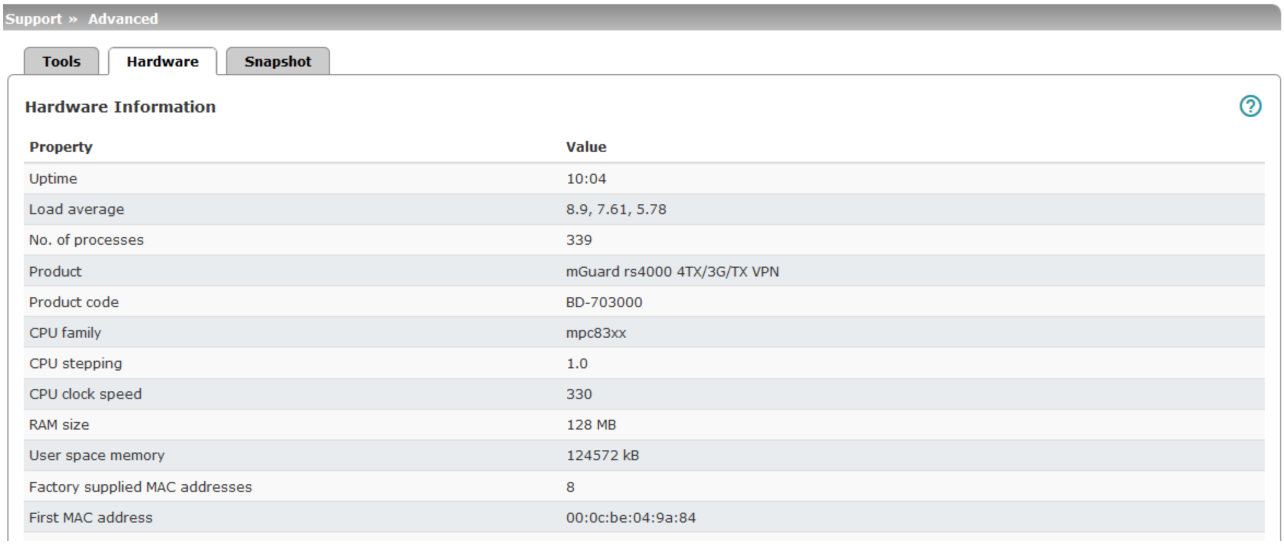
16.1.1 Tools



Support >> Advanced >> Tools	
Ping	**Aim**: to check whether a peer can be reached via a network. **Procedure**: • Enter the IP address or host name of the peer in the **Hostname/IP Address** field. Then click on the **Ping** button. A corresponding message is then displayed.
Traceroute	**Aim**: to determine which intermediate points or routers are located on the connection path to a peer. **Procedure**: • Enter the host name or IP address of the peer whose route is to be determined in the **Hostname/IP Address** field. • If the points on the route are to be output with IP addresses instead of host names (if applicable), activate the **Do not resolve IP addresses to hostnames** check box (check mark). • Then click on the **Trace** button. A corresponding message is then displayed.
DNS lookup	**Aim**: to determine which host name belongs to a specific IP address or which IP address belongs to a specific host name. **Procedure**: • Enter the IP address or host name in the **Hostname** field. • Click on the **Lookup** button. The response, which is determined by the mGuard according to the DNS configuration, is then returned.
IKE ping	**Aim**: to determine whether the VPN software for a VPN gateway is able to establish a VPN connection, or whether a firewall prevents this, for example. **Procedure**: • Enter the name or IP address of the VPN gateway in the **Hostname/IP Address** field. • Click on the **IKE ping** button. • A corresponding message is then displayed.

16.1.2 Hardware

This page lists various hardware properties of the mGuard.



Property	Value
Uptime	10:04
Load average	8.9, 7.61, 5.78
No. of processes	339
Product	mGuard rs4000 4TX/3G/TX VPN
Product code	BD-703000
CPU family	mpc83xx
CPU stepping	1.0
CPU clock speed	330
RAM size	128 MB
User space memory	124572 kB
Factory supplied MAC addresses	8
First MAC address	00:0c:be:04:9a:84

MAC addresses

The specified "First MAC address" is the MAC address of the WAN interface. The other MAC addresses (LAN/DMZ [optional]) can be calculated as follows:

- **WAN interface**: see type label.
- **LAN interface**: MAC address of the WAN interface incremented by 1 (**WAN + 1**).
  Devices with integrated switch: all switch ports use the same MAC address.
- **DMZ interface**: MAC address of the WAN interface incremented by 6 (**WAN + 6**).

Example:

- WAN: 00:a0:45:eb:28:9d (First MAC address)
- LAN: 00:a0:45:eb:28:9e
- DMZ: 00:a0:45:eb:28:a3

16.1.3 Snapshot

Support >> Advanced >> Snapshot		
Support Snapshot	**Support snapshot**	Creates a compressed file (in tar.gz format) containing all current configuration settings that could be relevant for error diagnostics. This file does not contain any private information such as private machine certificates or passwords. However, any pre-shared keys of VPN connections are contained in the snapshots. To create a **Support snapshot** or **Support snapshot with persistent logs**, proceed as follows: • Click on the **Download** button. • Save the file (under the name **snapshot-YYYY.MM.DD-hh.mm.ss.tar.gz** or **snapshot-all-YYYY.MM.DD-hh.mm.ss.tar.gz**). Provide the file to the support team of your supplier, if required.

17 Redundancy

The firewall and VPN redundancy functions are **not** available on the **FL MGUARD RS2000, FL MGUARD RS2005, TC MGUARD RS2000 3G**, and **TC MGUARD RS2000 4G.**

There are several different ways of compensating for errors using the mGuard so that an existing connection is not interrupted.

– **Firewall redundancy:** two identical mGuard devices can be combined to form a redundancy pair, meaning one takes over the functions of the other if an error occurs.
– **VPN redundancy**: an existing firewall redundancy forms the basis for VPN redundancy. In addition, the VPN connections are designed so that at least one mGuard in a redundancy pair operates the VPN connections.
– **Ring/network coupling**: in ring/network coupling, another method is used. Parts of a network are designed as redundant. In the event of errors, the alternative path is selected.

17.1 Firewall redundancy

Using firewall redundancy, it is possible to combine two identical mGuard devices into a redundancy pair pair (single virtual router). One mGuard takes over the functions of the other if an error occurs. Both mGuard devices run synchronously, meaning an existing connection is not interrupted when the device is switched.

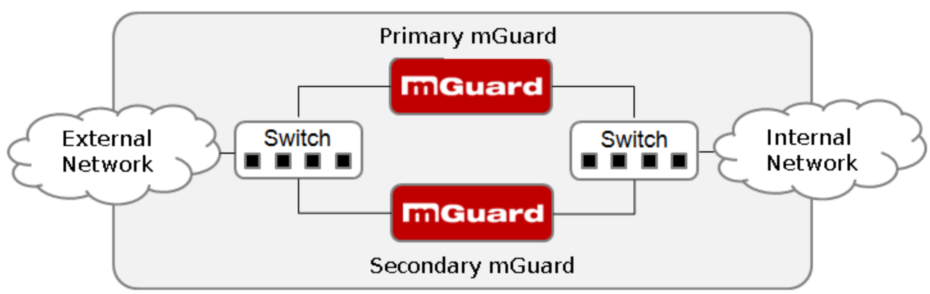


Figure 17-1 Firewall redundancy (example)

Basic requirements for firewall redundancy

A license is required for the firewall redundancy function. It can only be used if the corresponding license has been purchased and installed.

– Only identical mGuard devices can be used together in a redundancy pair.
– In Router network mode, firewall redundancy is only supported with “Static” Router mode.
– With mGuard firmware Version 7.5 or later, firewall redundancy is also supported in Stealth mode, but only when stealth configuration is set to “Multiple clients”.
– For further restrictions, see “Requirements for firewall redundancy” on page 426 and “Limits of firewall redundancy” on page 436.

17.1.1 Components in firewall redundancy

Firewall redundancy is comprised of several components:

- **Connectivity check**
  Checks whether the necessary network connections have been established.
- **Availability check**
  Checks whether an active mGuard is available and whether this should remain active.
- **State synchronization of the firewall**
  The mGuard on standby receives a copy of the current firewall database state.
- **Virtual network interface**
  Provides virtual IP addresses and MAC addresses that can be used by other devices as routes and default gateways.
- **State monitoring**
  Coordinates all components.
- **Status indicator**
  Shows the user the state of the mGuard.

Connectivity check

On each mGuard in a redundancy pair, checks are constantly made as to whether a connection is established via which the network packets can be forwarded.

Each mGuard checks its own internal and external network interfaces independently of each other. Both interfaces are tested for a continuous connection. This connection must be in place, otherwise the connectivity check will fail.

ICMP echo requests can also be sent (optional). The ICMP echo requests can be set via the *Redundancy >> Firewall Redundancy >> Connectivity Checks* menu.

Availability check

On each mGuard in a redundancy pair, checks are also constantly performed to determine whether an active mGuard is available and whether it should remain active. A variation of the CARP (Common Address Redundancy Protocol) is used here.

The active mGuard constantly sends presence notifications via its internal and external network interface while both mGuard devices listen. If a dedicated Ethernet link for state synchronization of the firewall is available, the presence notification is also sent via this link. In this case, the presence notification for the external network interface can also be suppressed.

The availability check fails if an mGuard does not receive any presence notifications within a certain time. The check also fails if an mGuard receives presence notifications with a lower priority than its own.

The data is always transmitted via the physical network interface and never via the virtual network interface.

State synchronization

The mGuard on standby receives a copy of the state of the mGuard that is currently active.

This includes a database containing the forwarded network connections. This database is filled and updated constantly by the forwarded network packets. The unencryptted data of the state is transmitted via the physical LAN interface and never via the virtual network interface.

> **NOTE: Unencrypted data transfer**
>
> The data from the connection tracking table of the firewall of the redundancy pair is transmitted unencrpyted over the LAN network.
>
> Use the redundancy function only in a secure network environment where the LAN network is fully under the control of the operator.

To keep internal data traffic to a minimum, a VLAN can be configured to store the synchronization data in a separate multicast and broadcast domain.

Virtual IP addresses

Each mGuard is configured with virtual IP addresses. The number of virtual IP addresses depends on the network mode used. Both mGuard devices in a redundancy pair must be assigned the same virtual IP addresses. The virtual IP addresses are required by the mGuard to establish virtual network interfaces.

Two virtual IP addresses are required in Router network mode, while others can be created. One virtual IP address is required for the external network interface and the other for the internal network interface.

These IP addresses are used as a gateway for routing devices located in the external or internal LAN. In this way, the devices can benefit from the high availability resulting from the use of both redundant mGuard devices.

The redundancy pair automatically defines MAC addresses for the virtual network interface. These MAC addresses are identical for the redundancy pair. In Router network mode, both mGuard devices share a MAC address for the virtual network interface connected to the external and internal Ethernet segment.

In Router network mode, the mGuard devices support forwarding of special UDP/TCP ports from a virtual IP address to other IP addresses, provided the other IP addresses can be reached by the mGuard. In addition, the mGuard also masks data with virtual IP addresses when masquerading rules are set up.

State monitoring

State monitoring is used to determine whether the mGuard is active, on standby or has an error. Each mGuard determines its own state independently, based on the information provided by other components. State monitoring ensures that two mGuard devices are not active at the same time.

Status indicator

The status indicator contains detailed information on the firewall redundancy state. A summary of the state can be called via the *Redundancy >> Firewall Redundancy >> Redundancy* or *Redundancy >> Firewall Redundancy >> Connectivity Checks* menu.

17.1.2 Interaction of the firewall redundancy components

During operation, the components work together as follows: both mGuard devices perform ongoing connectivity checks for both of their network interfaces (internal and external). In addition, an ongoing availability check is performed. Each mGuard listens continuously for presence notifications (CARP) and the active mGuard also sends them.

Based on the information from the connectivity and availability checks, the state monitoring function is made aware of the state of the mGuard devices. State monitoring ensures that the active mGuard mirrors its data to the other mGuard (state synchronization).

17.1.3 Firewall redundancy settings from previous versions

Existing configuration profiles for firmware Version 6.1.x (and earlier) can be imported with certain restrictions. For more information, please contact Phoenix Contact.

17.1.4 Requirements for firewall redundancy

- To use the redundancy function, both **mGuard** devices must have the same firmware.
- The firewall redundancy function can only be activated if a valid license key is installed.

  (under: *Redundancy >> Firewall Redundancy >> Redundancy >> Enable redundancy)*
- *Redundancy >> Firewall Redundancy >> Redundancy >> Interface which is used for state synchronization*

  The **Dedicated Interface** value is only accepted on **mGuard** devices which have more than two physical and separate Ethernet interfaces. This is currently the *mGuard centerport (Innominate), FL MGUARD CENTERPORT*.
- Each set of targets for the connectivity check cannot contain more than ten targets. (A fail-over time cannot be guaranteed without an upper limit.)

  Redundancy >> Firewall Redundancy >> Redundancy
  - *>> External Interface >> Primary External Targets (for ICMP echo requests)*
  - *>> External Interface >> Secondary External Targets (for ICMP echo requests)*
  - *>> Internal Interface >> Primary External Targets (for ICMP echo requests)*
  - *>> Internal Interface >> Secondary External Targets (for ICMP echo requests)*

  If “**at least one target must respond**” or “**all targets of one set must respond**” is selected under *External Interface >> Kind of check*, then *External Interface >> Primary External Targets (for ICMP echo requests)* must not be empty. This also applies to the internal interface.
- In **Router network mode**, at least one external and one internal virtual IP address must be set. A virtual IP address cannot be listed twice.

17.1.5 Fail-over switching time

The mGuard calculates the intervals for the connectivity check and availability check automatically according to the variables under **Fail-over switching time**.

Connectivity check

The factors which define the intervals for the connectivity check are specified in Table 17-1 on page 427.

64 byte ICMP echo requests are sent for the connectivity check. They are sent on Layer 3 of the Internet protocol. When VLAN is not used, 18 bytes for the MAC header and checksum are added to this with Ethernet on Layer 2. The ICMP echo reply is the same size.

The bandwidth is also shown in Table 17-1. This takes into account the values specified for a single target and adds up the bytes for the ICMP echo request and reply.

The timeout on the mGuard following transmission includes the following:
- The time required by the mGuard to transmit an ICMP echo reply. If other data traffic is expected, half duplex mode is not suitable here.
- The time required for the transmission of the ICMP echo request to a target. Consider the latency during periods of high capacity utilization. This applies especially when routers forward the request. The actual latency may be twice the value of the configured latency in unfavorable circumstances (connectivity check error).
- The time required on each target for processing the request and transmitting the reply to the Ethernet layer. Please note that full duplex mode is also used here.
- The time for transmission of the ICMP echo reply to the mGuard.

Table 17-1 Frequency of the ICMP echo requests

Fail-over switching time	ICMP echo requests per target	Timeout on the mGuard after transmission	Bandwidth per target
1 s	10 per second	100 ms	6560 bps
3 s	$3.\overline{3}$ per second	300 ms	2187 bps
10 s	1 per second	1 s	656 bps

If secondary targets are configured, then additional ICMP echo requests may occasionally be sent to these targets. This must be taken into account when calculating the ICMP echo request rate.

The timeout for a single ICMP echo request is displayed in Table 17-1. This does not indicate how many of the responses can be missed before the connectivity check fails. The check tolerates a negative result for one of two back-to-back intervals.

Availability check

Presence notifications (CARP) are up to 76 bytes in size on Layer 3 of the Internet protocol. When VLAN is not used, 18 bytes for the MAC header and checksum are added to this with Ethernet on Layer 2. The ICMP echo reply is the same size.

Table 17-2 shows the maximum frequency at which the presence notifications (CARP) are sent from the active mGuard. It also shows the bandwidth used in the process. The frequency depends on the mGuard priority and the *Fail-over switching time*.

Table 17-2 also shows the maximum latency tolerated by the mGuard for the network that is used to transmit the presence notifications (CARP). If this latency is exceeded, the redundancy pair can exhibit undefined behavior.

Table 17-2 Frequency of the presence notifications (CARP)

Fail-over switching time	Presence notifications (CARP) per second		Maximum latency	Bandwidth on Layer 2 for high priority
	High priority	Low priority		
1 s	50 per second	25 per second	20 ms	37600 bps
3 s	16.6 per second	8.3 per second	60 ms	12533 bps
10 s	5 per second	2.5 per second	200 ms	3760 bps

17.1.6 Error compensation through firewall redundancy

Firewall redundancy is used to compensate for hardware failures.

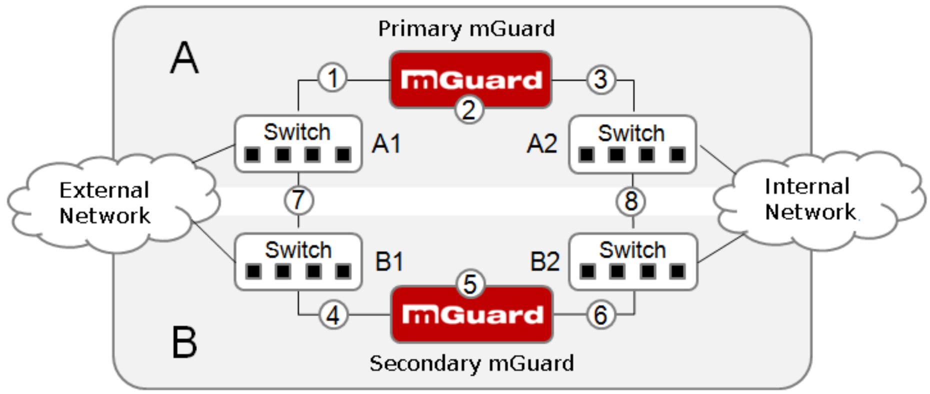


Figure 17-2 Possible error locations (1 ... 8)

Figure 17-2 shows a diagram containing various error locations (not related to the network mode).

Each of the mGuard devices in a redundancy pair is located in a different area (A and B). The mGuard in area A is connected to switch A1 through its external Ethernet interface and to switch A2 through its internal Ethernet interface. mGuard B is connected accordingly to switches B1 and B2. In this way, the switches and mGuard devices connect an external Ethernet network to an internal Ethernet network. The connection is established by forwarding network packets (in Router network mode).

Firewall redundancy compensates for errors shown in Figure 17-2 if only one occurs at any given time. If two errors occur simultaneously, they are only compensated if they occur in the same area (A or B).

For example, if one of the mGuard devices fails completely due to a power outage, then this is detected. A connection failure is compensated if the connection fails completely or partially. When the connectivity check is set correctly, a faulty connection caused by the loss of data packets or an excessive latency is detected and compensated. Without the connectivity check, the mGuard cannot determine which area caused the error.

A connection failure between switches on a network side (internal/external) is not compensated for (7 and 8 in Figure 17-2).

17.1.7 Handling firewall redundancy in extreme situations

The situations described here only occur rarely.

Restoration in the event of a network lobotomy

A network lobotomy occurs if a redundancy pair is separated into two mGuard devices operating independently of one another. In this case, each mGuard deals with its own tracking information as the two mGuard devices can no longer communicate via Layer 2. A network lobotomy can be triggered by a rare and unfortunate combination of network settings, network failures, and firewall redundancy settings.

Each mGuard is active during a network lobotomy. The following occurs after the network lobotomy has been rectified: if the mGuard devices have different priorities, the device with the higher priority becomes active and the other switches to standby mode. If both mGuard devices have the same priority, an identifier sent with the presence notifications (CARP) determines which mGuard becomes active.

Both mGuard devices manage their own firewall state during the network lobotomy. The active mGuard retains its state. Connections on the other mGuard, which were established during the lobotomy, are dropped.

Fail-over when establishing complex connections

Complex connections are network protocols which are based on different IP connections. One example of this is the FTP protocol. In the case of FTP, the client establishes a control channel for a TCP connection. The server is then expected to open another TCP connection over which the client can then transmit data. The data channel on port 20 of the server is set up while the control channel on port 21 of the server is being established.

If the relevant connection tracking function is activated on the mGuard (see "Advanced" on page 278), complex connections of this type are tracked. In this case, the administrator only needs to create a firewall rule on the mGuard which allows the client to establish a control channel to the FTP server. The mGuard enables the server to establish a data channel automatically, regardless of whether the firewall rules allow for this.

The tracking of complex connections is part of the firewall state synchronization process. However, to keep the latency short, the mGuard forwards the network packets independently of the firewall state synchronization update that has been triggered by the network packets themselves.

Therefore, it may be the case for a very brief period that a state change for the complex connection is not forwarded to the mGuard on standby if the active mGuard fails. In this case, tracking of the connection from the mGuard which is active after the fail-over is not continued correctly. This cannot be corrected by the mGuard. The data link is then reset or interrupted.

Fail-over when establishing semi-unidirectional connections

A semi-unidirectional connection refers to a single IP connection (such as UDP connections) where the data only travels in one direction after the connection is established with a bidirectional handshake.

The data flows from the responder to the initiator. The initiator only sends data packets at the very start.

The following applies only to certain protocols which are based on UDP. Data always flows in both directions on TCP connections.

If the firewall of the mGuard is set up to only accept data packets from the initiator, the firewall accepts all related responses per se. This happens regardless of whether or not a relevant firewall rule is available.

A scenario is conceivable in which the mGuard allows the initiating data packet to pass through and then fails before the relevant connection entry has been made in the other mGuard. The other mGuard may then reject the responses as soon as it becomes the active mGuard.

The mGuard cannot correct this situation due to the single-sided connection. As a countermeasure, the firewall can be configured so that the connection can be established in both directions. This is normally already handled via the protocol layer and no additional assignment is required.

Loss of data packets during state synchronization

If data packets are lost during state synchronization, this is detected automatically by the mGuard, which then requests the active mGuard to send the data again.

This request must be answered within a certain time, otherwise the mGuard on standby is assigned the “outdated” state and asks the active mGuard for a complete copy of all state information.

The response time is calculated automatically from the fail-over switching time. This is longer than the time for presence notifications (CARP), but shorter than the upper limit of the fail-over switching time.

Loss of presence notifications (CARP) during transmission

A one-off loss of presence notifications (CARP) is tolerated by the mGuard, but it does not tolerate the loss of subsequent presence notifications (CARP). This applies to the availability check on each individual network interface, even when these are checked simultaneously. It is therefore very unlikely that the availability check will fail as a result of a very brief network interruption.

Loss of ICMP echo requests/replies during transmission

ICMP echo requests or replies are important for the connectivity check. Losses are always observed, but are tolerated under certain circumstances.

The following measures can be used to increase the tolerance level for ICMP echo requests.

– Select **at least one target must respond** under **Kind of check** in the *Redundancy >> Firewall Redundancy >> Connectivity Checks* menu.
– Also define a secondary set of targets here. The tolerance level for the loss of ICMP echo requests can be further increased by entering the targets of unreliable connections under both sets (primary and secondary) or listing them several times within a set.

Restoring the primary mGuard following a failure

If a redundancy pair is defined with different priorities, the secondary mGuard becomes active if the connection fails. The primary mGuard becomes active again after the failure has been rectified. The secondary mGuard receives a presence notification (CARP) and returns to standby mode.

State synchronization

If the primary mGuard becomes active again after a failure of the internal network connection, it may contain an obsolete copy of the firewall database. This database must, therefore, be updated before the connection is reestablished. The primary mGuard ensures that it receives an up-to-date copy before becoming active.

17.1.8 Interaction with other devices

Virtual and real IP addresses

With firewall redundancy in Router network mode, the mGuard uses real IP addresses to communicate with other network devices.

Virtual IP addresses are used in the following two cases:

- Virtual IP addresses are used when establishing and operating VPN connections.
- If DNS and NTP services are used according to the configuration, they are offered to internal virtual IP addresses.

The use of real (management) IP addresses is especially important for the connectivity check and availability check. Therefore, the real (management) IP address must be configured so that the mGuard can establish the required connections.

The following are examples of how and why mGuard communication takes place:

- Communication with NTP servers to synchronize the time
- Communication with DNS servers to resolve host names (especially those from VPN partners)
- To register its IP address with a DynDNS service
- To send SNMP traps
- To forward log messages to a SysLog server
- To download a CRL from an HTTP(S) server
- To authenticate a user via a RADIUS server
- To download a configuration profile via an HTTPS server
- To download a firmware update from an HTTPS server

With firewall redundancy in Router network mode, devices connected to the same LAN segment as the redundancy pair must use their respective virtual IP addresses as gateways for their routes. If these devices were to use the actual IP address of either of the mGuard devices, this would work until that particular mGuard failed. However, the other mGuard would then not be able to take over.

Targets for the connectivity check

If a target is set for ICMP echo requests as part of the connectivity check, these requests must be answered within a certain time, even if the network is busy with other data. The network path between the redundancy pair and these targets must be set so that it is also able to forward the ICMP responses when under heavy load. Otherwise, the connectivity check for an mGuard could erroneously fail.

Targets can be configured for the internal and external interface in the connectivity check (see "Connectivity Checks" on page 406). It is important that these targets are actually connected to the specified interface. An ICMP echo reply cannot be received by an external interface when the target is connected to the internal interface (and vice versa). When the static routes are changed, it is easy to forget to adjust the configuration of the targets accordingly.

The targets for the connectivity check should be well thought out. Without a connectivity check, all it takes are two errors for a network lobotomy to occur.

A network lobotomy is prevented if the targets for both mGuard devices are identical and all targets have to answer the request. However, the disadvantage of this method is that the connectivity check fails more often if one of the targets does not offer high availability.

In **Router network mode**, we recommend defining a high-availability device as the target on the external interface. This can be the default gateway for the redundancy pair (e.g., a virtual router comprised of two independent devices). In this case, either no targets or a selection of targets should be defined on the internal interface.

Please also note the following information when using a virtual router consisting of two independent devices as the default gateway for a redundancy pair. If these devices use VRRP to synchronize their virtual IP, then a network lobotomy could split the virtual IP of this router into two identical copies. These routers could use a dynamic routing protocol and only one may be selected for the data flows of the network being monitored by the mGuard. Only this router should keep the virtual IP. Otherwise, you can define targets which are accessible via this route in the connectivity check. In this case, the virtual IP address of the router would not be a sensible target.

Redundancy group

Several redundancy pairs can be connected within a LAN segment (redundancy group). You define a value as an identifier (using the router ID) for each virtual instance of the redundancy pair. As long as these identifiers are different, the redundancy pairs do not come into conflict with each other.

Data traffic

In the event of a high **latency** in a network used for state synchronization updates or a serious data loss on this network, the mGuard on standby is assigned the "outdated" state. This does not occur, however, as long as no more than two back-to-back updates are lost. This is because the mGuard on standby automatically requests a repeat of the update. The latency requirements are the same as those detailed under "Fail-over switching time" on page 427.

Sufficient bandwidth

The data traffic generated as a result of the connectivity check, availability check, and state synchronization uses bandwidth in the network. The connectivity check also generates complicated calculations. There are several ways to limit this or stop it completely.

If the impact on other devices is unacceptable:

- The connectivity check must either be deactivated, or must only relate to the actual IP address of the other **mGuard**.
- The data traffic generated by the availability check and state synchronization must be moved to a separate VLAN.
- Switches must be used which allow separation of the VLANs.

Dedicated interface

The *mGuard centerport (Innominate)* / FL MGUARD CENTERPORT supports a **dedicated interface**. This is a reserved, direct Ethernet interface or a dedicated LAN segment, via which the state synchronization is sent. This separates the load physically from the internal LAN segment.

17.1.9 Transmission capacity with firewall redundancy

These values apply to Router network mode when the data traffic for state synchronization is transmitted without encryption. If the transmission capacity described here is exceeded, in the event of errors the switching time may be longer than that set.

Platform		Transmission capacity with firewall redundancy
mGuard centerport (Innominate), FL MGUARD CENTERPORT		1500 Mbps, bidirectional[1], not more than 400,000 frames/s
FL MGUARD RS FL MGUARD SMART 533/266 FL MGUARD BLADE mGuard delta (Innominate)	with 533 MHz	150 Mbps[1], bidirectional, not more than 12,750 frames/s
FL MGUARD RS FL MGUARD SMART 533/266 FL MGUARD BLADE mGuard delta (Innominate)	with 266 MHz	62 Mbps, bidirectional[1], not more than 5250 frames/s
FL MGUARD RS4000 TC MGUARD RS4000 3G, TC MGUARD RS4000 4G FL MGUARD RS4004 FL MGUARD SMART2 FL MGUARD CORE TX FL MGUARD PCI(E)4000 FL MGUARD DELTA		62 Mbps, bidirectional[1], not more than 5250 frames/s

1 Bidirectional includes traffic in both directions. For example, 1500 Mbps means that 750 Mbps is forwarded in each direction.

Fail-over switching time

The fail-over switching time can be set to 1, 3 or 10 seconds in the event of errors.

The upper limit of 1 second is currently only adhered to by the *mGuard centerport (Innominate),* FL MGUARD CENTERPORT, even under high load.

17.1.10 Limits of firewall redundancy

- In **Router network mode**, firewall redundancy is only supported with “Static” mode.
- Access to the mGuard via the HTTPS, SNMP, and SSH **management protocols** is only possible with a real IP address from each mGuard. Attempts to access virtual addresses are rejected.
- The following **features cannot be used** with firewall redundancy.
  - A secondary external Ethernet interface
  - A DHCP server
  - A DHCP relay
  - A SEC-Stick server
  - A user firewall
  - CIFS Integrity Monitoring
- The **redundancy pair must have the same configuration**. Take this into account when making the following settings:
  - NAT settings (masquerading, port forwarding, and 1:1 NAT)
  - Flood protection
  - Packet filter (firewall rules, MAC filter, advanced settings)
  - Queues and rules for QoS
- Some network connections may be interrupted following a **network lobotomy**. (See “Restoration in the event of a network lobotomy” on page 430.)
- After a fail-over, **semi-unidirectional or complex connections** that were established in the second before the fail-over may be interrupted. (See “Fail-over when establishing complex connections” on page 430 and “Fail-over when establishing semi-unidirectional connections” on page 430.)
- Firewall redundancy does not support the **FL MGUARD PCI 533/266 in Driver mode**.
- State synchronization does not replicate the connection tracking entries for **ICMP echo requests** forwarded by the mGuard. Therefore, ICMP echo replies can be dropped according to the firewall rules if they only reach the mGuard after the fail-over is completed. Please note that ICMP echo replies are not suitable for measuring the fail-over switching time.
- **Masquerading** involves hiding the transmitter behind the first virtual IP address or the first internal IP address. This is different to masquerading on the mGuard without firewall redundancy. When firewall redundancy is not activated, the external or internal IP address hiding the transmitter is specified in a routing table.

17.2 VPN redundancy

VPN redundancy can only be used together with firewall redundancy.

The concept is the same as for firewall redundancy. In order to detect an error in the system environment, the activity is transmitted from the active mGuard to the mGuard on standby.

At any given point in time, at least one mGuard in the redundancy pair is operating the VPN connection (except in the event of a network lobotomy).

Basic requirements for VPN redundancy

VPN redundancy does not have any of its own variables. It currently does not have its own menu in the user interface – it is activated together with firewall redundancy instead.

VPN redundancy can only be used if the corresponding license has been purchased and installed on the mGuard.

As VPN connections must be established for VPN redundancy, a corresponding VPN license is also necessary.

If you only have the license for firewall redundancy and VPN connections are installed, VPN redundancy cannot be activated. An error message is displayed as soon as an attempt is made to use firewall redundancy.

Only identical mGuard devices can be used together in a redundancy pair.

17.2.1 Components in VPN redundancy

The components used in VPN redundancy are the same as described under firewall redundancy. One additional component is available here – VPN state synchronization. A small number of components are slightly extended for VPN redundancy. However, the connectivity check, availability check, and firewall state synchronization are all performed in the same way as before.

VPN state synchronization

The mGuard supports the configuration of firewall rules for the VPN connection.

VPN state synchronization monitors the state of the different VPN connections on the active mGuard. It ensures that the mGuard on standby receives a valid, up-to-date copy of the VPN state database.

As with state synchronization of the firewall, VPN state synchronization sends updates from the active mGuard to the mGuard on standby. If requested to do so by the mGuard on standby, the active mGuard sends a complete record of all state information.

Dedicated interface (mGuard centerport (Innominate), FL MGUARD CENTERPORT)

In the case of the *mGuard centerport (Innominate), FL MGUARD CENTERPORT*, you can permanently assign the third Ethernet interface for VPN state synchronization.

As with the state synchronization of the firewall, the data traffic for VPN state synchronization for the dedicated interface is transmitted when a variable is set. Under *Redundancy >> Firewall Redundancy >> Redundancy* set the *Interface which is used for state synchronization* to **Dedicated Interface**.

Establishing VPN connections

In VPN redundancy, the virtual network interface is used for an additional purpose – to establish, accept, and operate VPN connections. The mGuard only listens for the first virtual IP address.

In Router network mode, it listens at the first external and internal virtual IP addresses.

State monitoring

State monitoring is used to monitor state synchronization on both the VPN and firewall.

Status indicator

The status indicator shows additional detailed information on the status of VPN state synchronization. This is located directly next to the information for firewall state synchronization.

As an ancillary effect, the status indicator of the VPN connection can also be seen on the mGuard on standby. You can therefore find the contents of the VPN state database replicated under the normal status indicator for the VPN connection (under *IPsec VPN >> IPsec Status)*.

Only the state of the synchronization process is shown in the status indicator for firewall redundancy *()*.

17.2.2 Interaction of the VPN redundancy components

The individual components interact in the same way as described for firewall redundancy. VPN state synchronization is also controlled by state monitoring. The state is recorded and updates are sent.

Certain conditions must be met for the states to occur. VPN state synchronization is taken into account here.

17.2.3 Error compensation through VPN redundancy

VPN redundancy compensates for the exact same errors as firewall redundancy (see “Error compensation through firewall redundancy” on page 429).

However, the VPN section can hinder the other VPN gateways in the event of a network lobotomy. The independent mGuard devices then have the same virtual IP address for communicating with the VPN partners. This can result in VPN connections being established and disconnected in quick succession.

17.2.4 Setting the variables for VPN redundancy

If the required license keys are installed, VPN redundancy is automatically activated at the same time as firewall redundancy. This occurs as soon as *Enable redundancy* is set to **Yes** in the *Redundancy >> Firewall Redundancy >> Redundancy* menu.

There is no separate menu for VPN redundancy. The existing firewall redundancy variables are extended.

Table 17-3 Extended functions with VPN redundancy activated

Redundancy >> Firewall Redundancy >> Redundancy		
General	**Enable redundancy**	Firewall redundancy and VPN redundancy are activated or deactivated.
Virtual interfaces	**External virtual IP addresses**	Only in Router network mode. The mGuard uses the first external virtual IP address as the address from which it sends and receives IKE messages. The external virtual IP address is used instead of the real primary IP address of the external network interface. The mGuard no longer uses the real IP address to send or answer IKE messages. ESP data traffic is handled similarly, but is also accepted and processed by the real IP address.
	Internal virtual IP addresses	As described under *External virtual IP addresses*, but for internal virtual IP addresses.

17.2.5 Requirements for VPN redundancy

– VPN redundancy can only be activated if a **license key** is installed for VPN redundancy and a VPN connection is activated.
– **Only for TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004, FL MGUARD RS4000, FL MGUARD GT/GT, and FL MGUARD RS**

  If a VPN connection is controlled via a **VPN switch**, then VPN redundancy cannot be activated.

  (under: *IPsec VPN* >> *Global* >> *Options* >> *VPN Switch*)

During VPN state synchronization, the state of the VPN connection is sent continuously from the active mGuard to the one on standby so that it always has an up-to-date copy in the event of errors. The only exception is the state of the IPsec replay window. Changes there are only transmitted sporadically.

The volume of the data traffic for state synchronization does not depend on the data traffic sent over the VPN tunnels. The data volumes for state synchronization are defined by a range of parameters that are assigned to the ISAKMP SAs and IPsec SAs.

17.2.6 Handling VPN redundancy in extreme situations

The conditions listed under “Handling firewall redundancy in extreme situations” on page 430 also apply to VPN redundancy. They also apply when the mGuard is used exclusively for forwarding VPN connections. The mGuard forwards the data flows via the VPN tunnels and rejects incorrect packets, regardless of whether firewall rules have been defined for the VPN connections or not.

An error interrupts the flow of data traffic

An error that interrupts the data traffic running via the VPN tunnels represents an extreme situation. In this case, the IPsec data traffic is briefly vulnerable to replay attacks. (A replay attack is the repetition of previously sent encrypted data packets using copies which have been saved by the attacker.) The data traffic is protected by sequential numbers. Independent sequential numbers are used for each direction in an IPsec tunnel. The mGuard drops ESP packets which have the same sequential number as a packet that has already been decrypted for a specific IPsec tunnel by the mGuard. This mechanism is known as the **IPsec replay window**.

The IPsec replay window is only replicated sporadically during state synchronization, as it is very resource-intensive. Therefore, the active mGuard may have an obsolete IPsec replay window following a fail-over. An attack is then possible until the real VPN partner has sent the next ESP packet for the corresponding IPsec SA, or until the IPsec SA has been renewed.

To avoid having an insufficient sequential number for the outgoing IPsec SA, VPN redundancy adds a constant value to the sequential number for each outgoing IPsec SA before the mGuard becomes active. This value is calculated so that it corresponds to the maximum number of data packets which can be sent through the VPN tunnel during the maximum fail-over switching time. At worst (1 Gigabit Ethernet and a switching time of 10 seconds), this is 0.5% of an IPsec sequence. At best, this is only one per thousand.

Adding a constant value to the sequential number prevents the accidental reuse of a sequential number already used by the other mGuard shortly before it failed. Another effect is that ESP packets sent from the previously active mGuard are dropped by the VPN partner if new ESP packets are received earlier from the mGuard that is currently active. To do this, the latency in the network must differ from the fail-over switching time.

An error interrupts the initial establishment of the ISAKMP SA or IPsec SA

If an error interrupts the initial establishment of the ISAKMP SA or IPsec SA, the mGuard on standby can continue the process seamlessly, as the state of the SA is replicated synchronously. The response to an IKE message is only sent from the active mGuard after the mGuard on standby has confirmed receipt of the corresponding VPN state synchronization update.

When an mGuard becomes active, it immediately repeats the last IKE message which should have been sent from the previously active mGuard. This compensates for cases where the previously active mGuard has sent the state synchronization but has failed before it could send the corresponding IKE message.

In this way, the establishment of the ISAKMP SA or IPsec SA is only delayed by the switching time during a fail-over.

An error interrupts the renewal of an ISAKMP SA

If an error interrupts the renewal of an ISAKMP SA, this is compensated in the same way as during the initial establishment of the SA. The old ISAKMP SA is also kept for Dead Peer Detection until the renewal of the ISAKMP SA is complete.

An error interrupts the renewal of an IPsec SA

If an error interrupts the renewal of an IPsec SA, this is compensated in the same way as during the initial establishment of the SA. Until renewal of the ISAKMP SA is complete, the old outgoing and incoming IPsec SAs are retained until the VPN partner notices the change.

VPN state synchronization ensures that the old IPsec SAs are retained throughout the entire time that the mGuard remains on standby. When the device becomes active, it can then continue with the encryption and decryption of the data traffic without the need for further action.

Loss of data packets during VPN state synchronization

State synchronization can cope with the loss of one of two back-to-back update packets. If more data packets are lost, this can result in a longer switching time in the event of errors.

The mGuard on standby has an obsolete machine certificate

X.509 certificates and private keys used by a redundancy pair to authenticate itself as a VPN partner may need to be changed. The combination of a private key and certificate is hereinafter referred to as a machine certificate.

Each mGuard in a redundancy pair must be reconfigured in order to switch the machine certificate. Both mGuard devices also require the same certificate so that their VPN partners view them as one and the same virtual VPN appliance.

As each mGuard has to be reconfigured individually, it may be the case that the mGuard on standby has an obsolete machine certificate for a brief period.

If the mGuard on standby becomes active at the exact moment when the ISAKMP SAs are being established, this procedure cannot be continued with an obsolete machine certificate.

As a countermeasure, VPN state synchronization replicates the machine certificate from the active mGuard to the mGuard on standby. In the event of a fail-over, the mGuard on standby will only use this to complete the process of establishing the ISAKMP SAs where this has already been started.

If the mGuard on standby establishes new ISAKMP SAs after a fail-over, it uses the machine certificate that has already been configured.

VPN state synchronization therefore ensures that the currently used machine certificates are replicated. However, it does not replicate the configuration itself.

The mGuard on standby has an obsolete pre-shared key (PSK)

Pre-shared keys (PSK) also need to be renewed on occasion in order to authenticate VPN partners. The redundant mGuard devices may then have a different PSK for a brief period. In this case, only one of the mGuard devices can establish a VPN connection as most VPN partners only accept one PSK. The mGuard does not offer any countermeasures for this.

> We therefore recommend using X.509 certificates instead of PSKs.

If VPN state synchronization replicates the PSKs being sent to the mGuard on standby for a prolonged period, an incorrect configuration remains concealed during this period, making it difficult to detect.

17.2.7 Interaction with other devices

Resolving host names

If host names are configured as VPN gateways, the mGuard devices in a redundancy pair must be able to resolve the host names for the same IP address. This applies especially when *DynDNS Monitoring* (see *page 321*) is activated.

If the host names are resolved from the mGuard on standby to another IP address, the VPN connection to this host is interrupted following a fail-over. The VPN connection is reestablished through another IP address. This takes place directly after the fail-over. However, a short delay may occur, depending (among other things) on what value is entered under *DynDNS Monitoring* for the *Refresh interval*.

Obsolete IPsec replay window

IPsec data traffic is protected against unauthorized access. To this end, each IPsec tunnel is assigned an independent sequential number. The mGuard drops ESP packets which have the same sequential number as a packet that has already been decrypted for a specific IPsec tunnel by the mGuard. This mechanism is known as the **IPsec replay window**. It prevents replay attacks, where an attacker sends previously recorded data to simulate someone else's identity.

The IPsec replay window is only replicated sporadically during state synchronization, as it is very resource-intensive. Therefore, the active mGuard may have an obsolete IPsec replay window following a fail-over. This means that a replay attack is possible for a brief period until the real VPN partner has sent the next ESP packet for the corresponding IPsec SA, or until the IPsec SA has been renewed. However, the traffic must be captured completely for this to occur.

Dead Peer Detection

Please note the following point for Dead Peer Detection.

> With Dead Peer Detection, set a higher timeout than the upper limit for the *Fail-over switching time* for the redundancy pair.
>
> (under: *IPsec VPN >> Connections >> Edit >> IKE Options, Delay between requests for a sign of life)*

Otherwise, the VPN partners may think that the redundancy pair is dead, even though it is only dealing with a fail-over.

Data traffic

In the event of a high latency in a network used for state synchronization updates, the mGuard on standby is assigned the “outdated” state. The same thing also happens in the event of serious data losses on this network.

This does not occur, however, as long as no more than two back-to-back updates are lost. This is because the mGuard on standby automatically requests a repeat of the update. The latency requirements are the same as those detailed under “Fail-over switching time” on page 427.

Real IP addresses

VPN partners may not send ESP traffic to the real IP address of the redundancy pair. VPN partners must always use the virtual IP address of the redundancy pair to send IKE messages or ESP traffic.

17.2.8 Transmission capacity with VPN redundancy

These values apply to Router network mode when the data traffic for state synchronization is transmitted without encryption. If the transmission capacity described here is exceeded, in the event of errors the switching time may be longer than that set.

Platform		Transmission capacity with firewall redundancy
mGuard centerport (Innominate), FL MGUARD CENTERPORT		220 Mbps, bidirectional[1], not more than 60,000 frames/s
FL MGUARD RS FL MGUARD SMART 533/266 mGuard core (Innominate) FL MGUARD PCI 533/266 FL MGUARD BLADE mGuard delta (Innominate)	with 533 MHz	50 Mbps, bidirectional[1], not more than 5550 frames/s
FL MGUARD RS FL MGUARD SMART 533/266 mGuard core (Innominate) FL MGUARD PCI 533/266 FL MGUARD BLADE mGuard delta (Innominate)	with 266 MHz	17 Mbps, bidirectional[1], not more than 2300 frames/s
FL MGUARD RS4000 TC MGUARD RS4000 3G TC MGUARD RS4000 4G FL MGUARD RS4004 FL MGUARD SMART2 FL MGUARD CORE TX FL MGUARD PCI(E)4000 FL MGUARD DELTA		17 Mbps, bidirectional[1], not more than 2300 frames/s

1 Bidirectional includes traffic in both directions. For example, 1500 Mbps means that 750 Mbps is forwarded in each direction.

Fail-over switching time

The fail-over switching time can be set to 1, 3 or 10 seconds in the event of errors.

The upper limit of 1 second is currently only adhered to by the mGuard centerport (Innominate), FL MGUARD CENTERPORT, even under high load.

17.2.9 Limits of VPN redundancy

The limits documented above for firewall redundancy also apply to VPN redundancy (see “Limits of firewall redundancy” on page 436). Further restrictions also apply.

- The redundancy pair must have the **same configuration** with respect to the following:
  - General VPN settings
  - Each individual VPN connection
- The mGuard only accepts VPN connections to the **first virtual IP address**.
  - In Router network mode, this means the first internal IP address and the first external IP address.
- The following **features cannot** be used with VPN redundancy:
  - Dynamic activation of the VPN connections using a VPN switch or the CGI script command nph-vpn.cgi (only on TC MGUARD RS4000 3G, TC MGUARD RS4000 4G, FL MGUARD RS4004, and FL MGUARD RS4000)
  - Archiving of diagnostic messages for VPN connections
- VPN connections are only supported in Tunnel mode. Transport mode does not take sufficient account of VPN connections.
- The upper limit of the **fail-over switching time** does not apply to connections which are **encapsulated with TCP**. Connections of this type are interrupted for a prolonged period during a fail-over. The encapsulated TCP connections must be reestablished by the initiating side after each fail-over. If the fail-over occurred on the initiating side, they can start immediately after the transfer. However, if the fail-over occurred on the answering side, the initiator must first detect the interruption and then reestablish the connection.
- VPN redundancy supports **masquerading** in the same way as without VPN redundancy. This applies when a redundancy pair is masked by a NAT gateway with a dynamic IP address.

  For example, a redundancy pair can be hidden behind a DSL router, which masks the redundancy pair with an official IP address. This DSL router forwards the IPsec data traffic (IKE and ESP, UDP ports 500 and 4500) to the virtual IP addresses. If the dynamic IP address changes, all active VPN connections which run via the NAT gateway are reestablished.

  The connections are reestablished by means of Dead Peer Detection (DPD) using the relevant configured time. This effect is beyond the influence of the mGuard.
- The redundancy function on the mGuard does not support **path redundancy**. Path redundancy can be achieved using other methods, e.g., by using a router pair. This router pair is seen on the virtual side of the mGuard devices. By contrast, on the other side, each of the routers has different connections.

  Path redundancy must not use NAT mechanisms such as masquerading to hide the virtual IP addresses of the mGuard devices. Otherwise, a migration from one path to another would change the IP addresses used to mask the redundancy pair. This would mean that all VPN connections (all ISAKMP SAs and all IPsec SAs) would have to be reestablished.

  The connections are reestablished by means of Dead Peer Detection (DPD) using the relevant configured time. This effect is beyond the influence of the mGuard.
- In the event of path redundancy caused by a network lobotomy, the VPN connections are no longer supported. A network lobotomy must be prevented whenever possible.

X.509 certificates for VPN authentication

The mGuard supports the use of X.509 certificates when establishing VPN connections. This is described in detail under “Authentication” on page 344.

However, there are some special points to note when X.509 certificates are used for authenticating VPN connections in conjunction with firewall redundancy and VPN redundancy.

Switching machine certificates

A redundancy pair can be configured so that it uses an X.509 certificate and the corresponding private key together to identify itself to a remote VPN partner as an individual virtual VPN instance.

These X.509 certificates must be renewed regularly. If the VPN partner is set to check the validity period of the certificates, these certificates must be renewed before their validity expires (see “Certificate Settings” on page 246).

If a machine certificate is replaced, all VPN connections which use it are restarted by the mGuard. While this is taking place, the mGuard cannot forward any data via the affected VPN connections for a certain period of time. This period depends on the number of VPN connections affected, the performance of the mGuard and VPN partners, and the latency of the mGuard devices in the network.

If this is not feasible for redundancy, the VPN partners of a redundancy pair must be configured so that they accept all certificates whose validity is confirmed by a set of specific CA certificates (see “CA Certificates” on page 250 and “Authentication” on page 344).

> To do this, select **Signed by any trusted CA** for *Remote CA certificate* under *IPsec VPN >> Connections >> Edit >> Authentication*.

If the new machine certificate is issued from a different sub-CA certificate, the VPN partner must be able to recognize this before the redundancy pair can use the new machine certificate.

The machine certificate must be replaced on both mGuard devices in a redundancy pair. However, this is not always possible if one cannot be reached. This might be the case in the event of a network failure, for example. The mGuard on standby may then have an obsolete machine certificate when it becomes active. This is another reason for setting the VPN partners so that they use both machine certificates.

The machine certificate is normally also replicated with the corresponding key during VPN state synchronization. In the event of a fail-over, the other mGuard can take over and even continue establishing incomplete ISAKMP SAs.

Switching the remote certificates for a VPN connection

The mGuard can be set to authenticate VPN partners directly using the X.509 certificates shown by these VPN partners. For this to happen, the relevant X.509 certificate must be set on the mGuard. This is known as the *Remote CA certificate*.

If a remote certificate is renewed, for a brief period, only one of the mGuard devices will have a new certificate. We therefore recommend authenticating the VPN partners using CA certificates instead of remote certificates in VPN redundancy.

Adding a new CA certificate to identify VPN partners

The mGuard can be set to authenticate VPN partners using CA certificates (see “CA Certificates” on page 250 and “Authentication” on page 344).

> To do this, select **Signed by any trusted CA** for *Remote CA certificate* under *IPsec VPN >> Connections >> Edit >> Authentication*.

With this setting, a new CA certificate can be added without affecting the established VPN connections. However, the new CA certificates are used immediately. The X.509 certificate used by the VPN partner to authenticate itself to the mGuard can then be replaced with minimal interruption. The only requirement is ensuring that the new CA certificate is available first.

The mGuard can be set to check the validity period of the certificates provided by the VPN partner (see “Certificate Settings” on page 246). In this case, new trusted CA certificates must be added to the mGuard configuration. These certificates should also have a validity period.

If CRL checking is activated (under *Authentication >> Certificates >> Certificate Settings),* one URL (where the corresponding CRL is available) must be maintained for each CA certificate. The URL and CRL must be published before the mGuard uses the CA certificates in order to confirm the validity of the certificates shown by the VPN partners.

Using X.509 certificates with limited validity periods and CRL checking

The use of X.509 certificates is described under “Certificate Settings” on page 246 (*“Authentication >> Certificates >> Certificate Settings”* menu).

If X.509 certificates are used and **Check the validity period of certificates and CRLs** is set, the system time has to be correct. We recommend synchronizing the system time using a trusted **NTP server**. Each mGuard in a redundancy pair can use the other as an additional NTP server, but not as the only NTP server.

18 Glossary

Asymmetrical encryption

In asymmetrical encryption, data is encrypted with one key and decrypted with a second key. Both keys are suitable for encryption and decryption. One of the keys is kept secret by its owner (private key), while the other is made available to the public (public key), i.e., to potential communication partners.

A message encrypted with the public key can only be decrypted and read by a recipient in possession of the associated private key. A message encrypted with the private key can be decrypted by any recipient in possession of the associated public key. Encryption using the private key shows that the message actually originated from the owner of the associated public key. Therefore, the expression “digital signature” is also often used.

However, asymmetrical encryption methods such as RSA are both slow and susceptible to certain types of attack. As a result, they are often combined with some form of symmetrical encryption (?“Symmetrical encryption” on page 456). On the other hand, concepts are available enabling the complex additional administration of symmetrical keys to be avoided.

DES/3DES

The encryption algorithms **DES** and **3DES** are no longer regarded as secure and should not be used where possible. The use of **AES** encryption algorithms is recommended as an alternative.

For reasons of backwards compatibility, the DES and 3DES encryption algorithms can continue to be used. For more information, see “Using secure encryption and hash algorithms” on page 19.

This symmetrical encryption algorithm (?“Symmetrical encryption” on page 456) was developed by IBM and checked by the NSA. DES was specified in 1977 by the American National Bureau of Standards (the predecessor of the National Institute of Standards and Technology (NIST)) as the standard for American governmental institutions. As this was the very first standardized encryption algorithm, it quickly won acceptance in industrial circles, both inside and outside America.

DES uses a 56-bit key length, which is no longer considered secure as the available processing power of computers has greatly increased since 1977.

3DES is a version of DES. It uses keys that are three times as long, i.e., 168 bits in length. Still considered to be secure today, 3DES is included in the IPsec standard, for example.

AES

AES (Advanced Encryption Standard) has been developed by NIST (National Institute of Standards and Technology) over the course of many years of cooperation with industry. This symmetrical encryption standard has been developed to replace the earlier DES standard. AES specifies three different key lengths (128, 192, and 256 bits).

In 1997, NIST started the AES initiative and published its conditions for the algorithm. From the many proposed encryption algorithms, NIST selected a total of five algorithms for closer examination – MARS, RC6, Rijndael, Serpent, and Twofish. In October 2000, the Rijndael algorithm was adopted as the encryption algorithm.

CA certificate

How trustworthy is a certificate and the issuing CA (certification authority)? (? “X.509 certificate” on page 455) A CA certificate can be consulted in order to check a certificate bearing this CA's signature. This check only makes sense if there is little doubt that the CA certificate originates from an authentic source (i.e., is authentic). In the event of doubt, the CA certificate itself can be checked. If (as is usually the case) the certificate is a sub-CA certificate (i.e., a CA certificate issued by a sub-certification authority), then the CA certificate of the superordinate CA can be used to check the CA certificate of the subordinate instance. If a superordinate CA certificate is in turn subordinate to another superordinate CA, then its CA certificate can be used to check the CA certificate of the subordinate instance, etc. This “chain of trust” continues down to the root instance (the root CA or certification authority). The root CA's CA file is necessarily self-signed, since this instance is the highest available and is ultimately the basis of trust. No-one else can certify that this instance is actually the instance in question. A root CA therefore is a state or a state-controlled organization.

The mGuard can use its imported CA certificates to check the authenticity of certificates shown by peers. In the case of VPN connections, for example, peers can only be authenticated using CA certificates. This requires all CA certificates to be installed on the mGuard in order to form a chain with the certificate shown by the peer. In addition to the CA certificate from the CA whose signature appears on the certificate shown by the VPN partner to be checked, this also includes the CA certificate of the superordinate CA, and so forth, up to the root certificate. The more meticulously this “chain of trust” is checked in order to authenticate a peer, the higher the level of security will be.

Client/server

In a client/server environment, a server is a program or computer which accepts and responds to queries from client programs or client computers.

In data communication, the computer establishing a connection to a server (or host) is also called a client. In other words, the client is the calling computer and the server (or host) is the computer called.

Datagram

In IP transmission protocols, data is sent in the form of data packets. These are known as IP datagrams. An IP datagram is structured as follows

IP header	TCP, UDP, ESP, etc. header	Data (payload)

The IP header contains:

– The IP address of the sender (source IP address)
– The IP address of the recipient (destination IP address)
– The protocol number of the protocol on the superordinate protocol layer (according to the OSI layer model)
– The IP header checksum used to check the integrity of the received header

The TCP/UDP header contains the following information:

– The port of the sender (source port)
– The port of the recipient (destination port)
– A checksum covering the TCP header and some information from the IP header (including source and destination IP address)

Default route

If a computer is connected to a network, the operating system creates a routing table internally. The table lists the IP addresses that the operating system has identified based on the connected computers and the routes available at that time. Accordingly, the routing table contains the possible routes (destinations) for sending IP packets. If IP packets are to be sent, the computer's operating system compares the IP addresses stated in the IP packets with the entries in the routing table in order to determine the correct route.

If a router is connected to the computer and its internal IP address (i.e., the IP address of the router's LAN port) has been relayed to the operating system as the default gateway (in the network card's TCP/IP configuration), then this IP address is used as the destination if all other IP addresses in the routing table are not suitable. In this case, the IP address of the router specifies the default route because all IP packets whose IP address has no counterpart in the routing table (i.e., cannot find a route) are directed to this gateway.

DynDNS provider

Also known as *Dynamic DNS provider*. Every computer connected to the Internet has an IP address (IP = Internet Protocol). If the computer accesses the Internet via a dial-up modem, ISDN or ADSL, its Internet service provider will assign it a dynamic IP address. In other words, the address changes for each online session. Even if a computer is online 24 hours a day without interruption (e.g., flat-rate), the IP address will change during the session.

If this computer needs to be accessible via the Internet, it must have an address that is known to the remote peer. This is the only way to establish a connection to the computer. However, if the address of the computer changes constantly, this will not be possible. This problem can be avoided if the operator of the computer has an account with a DynDNS provider (DNS = Domain Name Server).

In this case, the operator can set a host name with this provider via which the computer should be accessible, e.g., www.example.com. The DynDNS provider also provides a small program that must be installed and run on the computer concerned. Every time a new Internet session is launched on the local computer, this tool sends the IP address used by the computer to the DynDNS provider. The domain name server registers the current assignment of the host name to the IP address and also informs the other domain name servers on the Internet accordingly.

If a remote computer now wishes to establish a connection to a computer that is registered with the DynDNS provider, then the remote computer can use the host name of the computer as the address. This establishes a connection to the responsible DNS in order to look up the IP address that is currently registered for this host name. The corresponding IP address is sent back from the DNS to the remote computer, which can then use it as the destination address. This now leads directly to the desired computer.

In principle, all Internet addresses are based on this procedure: first, a connection to a DNS is established in order to determine the IP address assigned to the host name. Once this has been accomplished, the "looked up" IP address is used to set up a connection to the required peer, which could be any site on the Internet.

IP address

Every host or router on the Internet/Intranet has its own unique IP address (IP = Internet Protocol). An IP address is 32 bits (4 bytes) long and is written as four numbers (each between 0 and 255), which are separated by a dot.

An IP address consists of two parts: the network address and the host address.

Network address	Host address

All network hosts have the same network address, but different host addresses. The two parts of the address differ in length depending on the size of the respective network (networks are categorized as Class A, B or C).

	Byte 1	Byte 2	Byte 3	Byte 4
Class A	Network address	Host address		
Class B	Network address		Host address	
Class C	Network address			Host address

The first byte of the IP address determines whether the IP address of a network device belongs to Class A, B or C. The following is specified:

	Value of byte 1	Bytes for the network address	Bytes for the host address
Class A	1 - 126	1	3
Class B	128 - 191	2	2
Class C	192 - 223	3	1

Based on the above figures, the number of Class A networks worldwide is limited to 126. Each of these networks can have a maximum of 256 x 256 x 256 hosts (3 bytes of address area). There can be 64 x 256 Class B networks and each of these networks can have up to 65,536 hosts (2 bytes of address area: 256 x 256). There can be 32 x 256 x 256 Class C networks and each of these networks can have up to 256 hosts (1 byte of address area).

Subnet mask

Normally, a company network with access to the Internet is only officially assigned a single IP address, e.g., 128.111.10.21. The first byte of this example address indicates that this company network is a Class B network; in other words, the last two bytes are free to be used for host addressing. Accordingly, an address area for up to 65,536 possible hosts (256 x 256) can be computed.

Such a huge network is not practical and generates a need for subnetworks to be built. The subnet mask is used here. Like an IP address, the mask is 4 bytes long. The bytes representing the network address are each assigned the value 255. The primary purpose of doing this is to enable a portion of the host address area to be “borrowed” and used for addressing subnetworks. For example, if the subnet mask 255.255.255.0 is used on a Class B network (2 bytes for the network address, 2 bytes for the host address), the third byte, which was actually intended for host addressing, can now be used for subnetwork addressing. This computes to potential support for 256 subnetworks, each with 256 hosts.

IPsec

IP security (IPsec) is a standard that uses encryption to verify the authenticity of the sender and to ensure the confidentiality and integrity of the data in IP datagrams (? “Datagram” on page 450). The components of IPsec are the Authentication Header (AH), the Encapsulating Security Payload (ESP), the Security Association (SA), and the Internet Key Exchange (IKE).

At the start of the session, the systems involved in communication must determine which technique should be used and the implications of this choice, e.g., *Transport Mode* or *Tunnel Mode*.

In *Transport Mode*, an IPsec header is inserted between the IP header and the TCP or UDP header respectively in each IP datagram. Since the IP header remains unchanged, this mode is only suitable for host-to-host connections.

In *Tunnel mode*, an IPsec header and a new IP header are prefixed to the entire IP datagram. This means the original datagram is encrypted in its entirety and stored in the payload of the new datagram.

Tunnel Mode is used in VPN applications: the devices at the ends of the tunnel ensure that the datagrams are encrypted/decrypted along the tunnel; in other words, the actual datagrams are completely protected during transfer over a public network.

Subject, certificate

In a certificate, confirmation is provided by a certification authority (CA) that the certificate does actually belong to its owner. This is done by confirming specific owner properties. Furthermore, the certificate owner must possess the private key that matches the public key in the certificate. (→ “X.509 certificate” on page 455).

Example

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=XY, ST=Austria, L=Graz, O=TrustMe Ltd, OU=Certificate Authority, CN=CA/Email=ca@trustme.dom
    Validity
      Not Before: Oct 29 17:39:10 2000 GMT
→ Subject: CN=anywhere.com,E=doctrans.de,C=DE,ST=Hamburg,L=Hamburg,O=Phoenix Contact,OU=Security
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:c4:40:4c:6e:14:1b:61:36:84:24:b2:61:c0:b5:
          d7:e4:7a:a5:4b:94:ef:d9:5e:43:7f:c1:64:80:fd:
          9f:50:41:6b:70:73:80:48:90:f3:58:bf:f0:4c:b9:
          90:32:81:59:18:16:3f:19:f4:5f:11:68:36:85:f6:
          1c:a9:af:fa:a9:a8:7b:44:85:79:b5:f1:20:d3:25:
          7d:1c:de:68:15:0c:b6:bc:59:46:0a:d8:99:4e:07:
          50:0a:5d:83:61:d4:db:c9:7d:c3:2e:eb:0a:8f:62:
          8f:7e:00:e1:37:67:3f:36:d5:04:38:44:44:77:e9:
          f0:b4:95:f5:f9:34:9f:f8:43
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Subject Alternative Name:
        email:xyz@anywhere.com
      Netscape Comment:
        mod_ssl generated test server certificate
      Netscape Cert Type:
        SSL Server
  Signature Algorithm: md5WithRSAEncryption
    12:ed:f7:b3:5e:a0:93:3f:a0:1d:60:cb:47:19:7d:15:59:9b:
    3b:2c:a8:a3:6a:03:43:d0:85:d3:86:86:2f:e3:aa:79:39:e7:
    82:20:ed:f4:11:85:a3:41:5e:5c:8d:36:a2:71:b6:6a:08:f9:
    cc:1e:da:c4:78:05:75:8f:9b:10:f0:15:f0:9e:67:a0:4e:a1:
    4d:3f:16:4c:9b:19:56:6a:f2:af:89:54:52:4a:06:34:42:0d:
    d5:40:25:6b:b0:c0:a2:03:18:cd:d1:07:20:b6:e5:c5:1e:21:
    44:e7:c5:09:d2:d5:94:9d:6c:13:07:2f:3b:7c:4c:64:90:bf:
    ff:8e
```

The *subject distinguished name* (or *subject* for short) uniquely identifies the certificate owner. The entry consists of several components. These are called attributes (see the example certificate above). The following table contains a list of possible attributes. The sequence of attributes in an X.509 certificate can vary.

Table 18-1 X.509 certificate

Abbreviation	Name	Explanation
CN	Common name	Identifies the person or object to whom or which the certificate belongs. Example: CN=server1
E	E-mail address	Specifies the e-mail address of the certificate owner.
OU	Organizational unit	Specifies the department within an organization or company. Example: OU=Development
O	Organization	Indicates the organization or company. Example: O=Phoenix Contact

Table 18-1 X.509 certificate

Abbreviation	Name	Explanation
L	Locality	Indicates the location Example: L=Hamburg
ST	State	Specifies the state or county. Example: ST=Bavaria
C	Country	Two-letter code that specifies the country. (Germany=DE) Example: C=DE

A filter can be set for the subject (i.e., the certificate owner) during VPN connections and remote service access to the mGuard using SSH or HTTPS. This would ensure that only certificates from peers that have certain attributes in the subject line are accepted.

NAT (Network Address Translation)

Network Address Translation (NAT) (also known as *IP masquerading*) “hides” an entire network behind a single device, known as a NAT router. If you communicate externally via a NAT router, the internal computers in the local network and their IP addresses remain hidden. The remote communication partner will only see the NAT router with its IP address.

In order to allow internal computers to communicate directly with external computers (on the Internet), the NAT router must modify the IP datagrams that are sent from internal computers to remote partners and received by internal computers from remote partners.

If an IP datagram is sent from the internal network to a remote partner, the NAT router modifies the UDP and TCP headers of the datagram, replacing the source IP address and source port with its own official IP address and a previously unused port. For this purpose, the NAT router uses a table in which the original values are listed together with the corresponding new ones.

When a response datagram is received, the NAT router uses the specified destination port to recognize that the datagram is intended for an internal computer. Using the table, the NAT router replaces the destination IP address and port before forwarding the datagram via the internal network.

Port number

A port number is assigned to each device in UDP and TCP protocol-based communication. This number makes it possible to differentiate between multiple UDP or TCP connections between two computers and use them simultaneously.

Certain port numbers are reserved for specific purposes. For example, HTTP connections are usually assigned to TCP port 80 and POP3 connections to TCP port 110.

Proxy

A proxy is an intermediary service. A web proxy (e.g., Squid) is often connected upstream of a large network. For example, if 100 employees access a certain website frequently over a web proxy, then the proxy only loads the relevant web pages from the server once and then distributes them as needed among the employees. Remote web traffic is reduced, which saves money.

PPPoE

Acronym for **P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet. A protocol based on the PPP and Ethernet standards. PPPoE is a specification defining how to connect users to the Internet via Ethernet using a shared broadband medium such as DSL, wireless LAN or a cable modem.

PPTP

Acronym for **P**oint-to-**P**oint **T**unneling **P**rotocol. This protocol was developed by Microsoft and U.S. Robotics, among others, for secure data transfer between two VPN nodes (? VPN) via a public network.

Router

A router is a device that is connected to different IP networks and communicates between them. To do this, the router has an interface for each network connected to it. A router must find the correct path to the destination for incoming data and define the appropriate interface for forwarding it. To do this, it takes data from a local routing table listing assignments between available networks and router connections (or intermediate stations).

Trap

SNMP (Simple Network Management Protocol) is often used alongside other protocols, in particular on large networks. This UDP-based protocol is used for central administration of network devices. For example, the configuration of a device can be requested using the GET command and changed using the SET command; the requested network device must simply be SNMP-compatible.

An SNMP-compatible device can also send SNMP messages (e.g., should unexpected events occur). Messages of this type are known as SNMP traps.

X.509 certificate

A type of “seal” that certifies the authenticity of a public key (? asymmetrical encryption) and the associated data.

It is possible to use certification to enable the user of the public key (used to encrypt the data) to ensure that the received public key is indeed from its actual issuer (and thus from the instance that should later receive the data). A *certification authority* (CA) certifies the authenticity of the public key and the associated link between the identity of the issuer and its key. The certification authority verifies authenticity in accordance with its rules (for example, it may require the issuer of the public key to appear before it in person). After successful authentication, the CA adds its (digital) signature to the public key. This results in a certificate.

An X.509(v3) certificate thus consists of a public key, information about the key owner (the Distinguished Name (DN)), authorized use, etc., and the signature of the CA (? Subject, certificate).

The signature is created as follows: the CA creates an individual bitstring from the bitstring of the public key, owner information, and other data. This bitstring can be up to 160 bits in length and is known as the HASH value. The CA then encrypts this with its own private key and then adds it to the certificate. The encryption with the CA's private key proves the authenticity of the certificate (i.e., the encrypted HASH string is the CA's digital signature). If the certificate data is tampered with, then this HASH value will no longer be correct and the certificate will be rendered worthless.

The HASH value is also known as the fingerprint. Since it is encrypted with the CA's private key, anyone who has the corresponding public key can decrypt the bitstring and thus verify the authenticity of the fingerprint or signature.

The involvement of a certification authority means that it is not necessary for key owners to know each other. They only need to know the certification authority involved in the process. The additional key information also simplifies administration of the key.

X.509 certificates are used for e-mail encryption with S/MIME or IPsec, for example.

Protocol, transmission protocol

Devices that communicate with each other must follow the same rules. They have to “speak the same language”. Rules and standards of this kind are called protocols or transmission protocols. Some of the more frequently used protocols are IP, TCP, PPP, HTTP, and SMTP.

Service provider

Service providers are companies or institutions that enable users to access the Internet or online services.

Spoofing, anti-spoofing

In Internet terminology, spoofing means supplying a false address. Using this false Internet address, a user can create the illusion of being an authorized user.

Anti-spoofing is the term for mechanisms that detect or prevent spoofing.

Symmetrical encryption

In symmetrical encryption, the same key is used to encrypt and decrypt data. Two examples of symmetrical encryption algorithms are DES and AES. They are fast, but also increasingly difficult to administrate as the number of users increases.

TCP/IP (Transmission Control Protocol/Internet Protocol)

Network protocols used to connect two computers on the Internet.

IP is the base protocol.

UDP is based on IP and sends individual packets. The packets may reach the recipient in a different order than that in which they were sent or they may even be lost.

TCP is used for connection security and ensures, for example, that data packets are forwarded to the application in the correct order.

UDP and TCP add port numbers between 1 and 65535 to the IP addresses. These distinguish the various services offered by the protocols.

A number of additional protocols are based on UDP and TCP. These include HTTP (Hyper Text Transfer Protocol), HTTPS (Secure Hyper Text Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol, Version 3), and DNS (Domain Name Service).

ICMP is based on IP and contains control messages.

SMTP is an e-mail protocol based on TCP.

IKE is an IPsec protocol based on UDP.

ESP is an IPsec protocol based on IP.

On a Windows PC, the WINSOCK.DLL (or WSOCK32.DLL) handles the processing of both protocols.

(→ “Datagram” on page 450)

VLAN

A VLAN (Virtual Local Area Network) divides a physical network into several independent logical networks, which exist in parallel.

Devices on different VLANs can only access devices within their own VLAN. Accordingly, assignment to a VLAN is no longer defined by the network topology alone, but also by the configured VLAN ID.

VLAN settings can be used as optional settings for each IP. A VLAN is identified by its VLAN ID (1-4094). All devices with the same VLAN ID belong to the same VLAN and can communicate with one another.

The Ethernet packet for a VLAN (according to IEEE 802.1Q) is extended by 4 bytes, with 12 bits available for recording the VLAN ID. VLAN IDs “0” and “4095” are reserved and cannot be used for VLAN identification.

VPN (Virtual Private Network)

A **V**irtual **P**rivate **N**etwork (VPN) connects several separate private networks (subnetworks) via a public network (e.g., the Internet) to form a single common network. A cryptographic protocol is used to ensure confidentiality and authenticity. A VPN is therefore an inexpensive alternative to using permanent lines for building a nationwide company network.

19 Appendix

19.1 CGI interface

The additional HTTPS interfaces *nph-vpn.cgi*, *nph-diag.cgi, nph-status.cgi* and *nph-action.cgi* are implemented as CGI (**C**ommon **G**ateway **I**nterface) scripts.

For more information on using the CGI interfaces, see *mGuard Application Notes* (UM EN MGUARD APPNOTES), available at phoenixcontact.net/products or help.mguard.com.

When executing the CGI scrips *nph-vpn.cgi*, *nph-diag.cgi, nph-status.cgi* and *nph-action.cgi*, only the following characters may be used in user names, passwords, and other user-defined names (for example, the name of a VPN connection):

– Letters: A - Z, a - z
– Digits: 0 - 9
– Special characters: - . _ ~

If other special characters, such as "space" or the "question mark", are used, they must be encoded accordingly (URL encoding).

Using the command line tool ***wget*** only functions in combination with mGuard firmware versions < 8.4.0. From mGuard firmware Version 8.4.0, the command line tool ***curl*** can be used (parameters and options differ!).

Example:

wget --no-check-certificate "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up"

curl --insecure "https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up"

The option ***--no-check-certificate*** (*wget*) or ***--insecure*** (*curl*) ensures that the HTTPS certificate on the mGuard does not undergo any further checking.

Table 19-1 Encoding of special characters (URL encoding)

(Space)	!	"	#	$	%	&	'	(	)	*	+
%20	%21	%22	%23	%24	%25	%26	%27	%28	%29	%2A	%2B

,	/	:	;	=	?	@	[	\	]	{	|	}
%2C	%2F	%3A	%3B	%3D	%3F	%40	%5B	%5C	%5D	%7B	%7C	%7D

19.2 Command line tool „mg“

The following commands can be executed on the command line of the mGuard by the users **root** and **admin**.

Table 19-2 Command line tool “mg“

Command	Parameter	Description
mg update	*patches*	An automatic online update will be started. The required package set will be determined automatically by the mGuard (see“Automatic Update” on page 88). **Patch-Releases** resolve errors in previous versions and have a version number which only changes in the third digit position.
	minor	**Minor- und major releases** supplement the mGuard with new properties or contain changes that affect the behavior of the mGuard. Their version number changes in the first or second digit position.
	major	
mg status	*/network/dns-servers*	**Used DNS server** Names of the DNS servers used by the mGuard for name resolution.
	/network/if-state/ext1/gw	**Current default route** The IP address that the mGuard uses to try to reach unknown networks.
	/network/if-state/ext1/ip	**External IP address** The addresses via which the mGuard can be accessed by devices from the external network. In *Stealth* mode, the mGuard adopts the address of the locally connected computer as its external IP.
	/network/if-state/ext1/netmask	**Net mask of the external IP address.**

19.3 LED status indicator and blinking behavior

The described blinking behavior refers to devices of the FL MGUARD RS 200x / FL MGUARD RS 400x and TC MGUARD RS 200x / TC MGUARD RS 400x device family.

19.3.1 Description of LEDs

With the help of built-in LED diodes, mGuard devices indicate different system states. This can be status, alarm or error messages.

The states are indicated by permanent or temporary lighting or blinking of the LEDs. The displayed LED pattern can also represent a combination of different system states.

NOTE: Since several system states are indicated by the LEDs not clearly, only temporarily or in combination with other system states, the log files of the mGuard device must also be checked!

LED diodes of FL/TC MGUARD (RS200x/RS400x) devices:

P1	Stat	Mod	Info2 (Sig)
P2	**Err**	**Fault**	**Info1**

P1 / P2

LEDs *P1* and *P2* indicate which of the two power supplies is connected (devices of the FL/TC MGUARD RS2000 series: only *P1* is available).

Info 2 / Info 1 (the LED Sig is not in use)

Active VPN connections or (as of Version 8.1) active firewall rule records can be indicated via the LEDs *Info2* and *Info1*. The activation of the LEDs by a certain VPN connection or a certain firewall rule record is configured on the mGuard interface in the menu item **Management >> Service Contacts**.

The following states will be indicated:

ON	The VPN connection is established / the firewall rule record is set.
Blink	The VPN connection will be established or released or has been stopped/disabled by the remote peer.
OFF	The VPN connection is stopped/disabled on both peers.

Stat / Mod / Err / Fault

The LEDs *Stat*, *Mod*, *Err* and *Fault* indicate system states (status, alarm or error messages) (see Table 19-5).

In addition to the alarm messages, an illuminated **Fault LED** generally also indicates that the device is currently not in operation mode.

LAN / WAN

The LAN/WAN LEDs are located in the LAN/WAN sockets (10/100 and duplex LED).

The LEDs Indicate the ethernet status of the LAN or WAN port. As soon as the device is connected to the relevant network, a continuous light indicates that there is a connection to the network partner in the LAN or WAN. When data packets are transmitted, the LED goes out briefly.

If all LAN/WAN LEDs are illuminated, the system is booting.

Bar graph and SIM1/2 (Mobile)

Table 19-3 LEDs on TC MGUARD RS4000 3G and TC MGUARD RS2000 3G

LED	**State and Meaning**					
Bar graph	LED 3	Top	Off	Off	Off	Green
	LED 2	Middle	Off	Off	Green	Green
	LED 1	Bottom	Off	Yellow	Yellow	Yellow
	Signal strength (dBm)		–113 ... 111	–109 ... 89	–87 ... 67	–65 ... 51
	Network reception		Very poor to none	Sufficient	Good	Very good
SIM 1	Green	On Blinking	SIM card 1 active No PIN or incorrect one entered			
SIM 2	Green	On Blinking	SIM card 2 active No PIN or incorrect one entered			

19.3.2 LED lighting and blinking behavior

Table 19-4 Description of the lighting and blinking behavior of the LED diodes

Heartbeat	The blinking behavior is similar to a heartbeat, in which two strokes are performed in quick succession, followed by a short break.
Running light	Three lights form a continuously repeating running light from left to right and back again.
Blink 50/1500	Flashing with 1500 ms break (50 ms on, then 1500 ms off)
Blink 50/800	Flashing with 800 ms break (50 ms on, then 800 ms off)
Blink 50/100	Flashing with 100 ms break (50 ms on, then 100 ms off)
Blink 500/500	Constant blinking (500 ms on / 500 ms off)
Morse code (. . . – – – . . .)	The blinking behavior shows the *Morse code* '*SOS*', in which the blinking behavior "3x short, 3x long, 3x short" is repeated continuously.
ON	The diode lights up permanently.
ON (n sec)	The diode lights up permanently for the indicated time (in seconds n)

19.3.3 Representation of system states

The system states (status, alarm or error messages), which are displayed by the LED's lighting and blinking behavior, are shown in Table 19-5.

Table 19-5 System states represented by lighting and blinking behavior of the LEDs

STAT	MOD	Info 2 (Sig)	ERR	FAULT	Description of the system state
Heart-beat					The system status is OK.
			ON		A severe error has happened.
ON (12 sec)	ON (3 sec)		ON (12 sec)	ON (12 sec)	The system is booting.
Morse code					The license to operate this firmware is missing.
Morse code			**Morse code**		Bootloader replacement failed due to hardware error.
Heart-beat				ON	A power failure was detected.
Heart-beat				ON	No connectivity on WAN interface (link supervision configurable on device)
Heart-beat				ON	No connectivity on LAN interface (link supervision configurable on device)
Heart-beat				ON	No connectivity on LAN 1–4 interface (link supervision configurable on device)
Heart-beat				ON	No connectivity on DMZ interface (link supervision configurable on device)
Heart-beat				ON	Power supply 1 or 2 failed (alarm configurable on device)
Heart-beat				ON	Temperature too high / low (alarm configurable on device)
Heart-beat				ON	(Redundancy) Connectivity check failed (alarm configurable on device)
Heart-beat				ON	(Modem) Connectivity check failed (alarm configurable on the device)
Heart-beat			ON (3 sec)		ECS: The ECS is incompatible.
Heart-beat			ON (3 sec)		ECS: The capacity of the ECS is exhausted.
Heart-beat			ON (3 sec)		ECS: The root password from the ECS does not match.
Heart-beat			ON (3 sec)		ECS: Failed to load the configuration from the ECS.
Heart-beat			ON (3 sec)		ECS: Failed to save the configuration to the ECS.
Heart-beat	ON				PPPD: The internal modem got a connect (set by pppd).
Heart-beat	Blink 50/1500				PPPD: The internal modem is armed and expecting a dial in.
Heart-beat	Blink 500/500				PPPD: The internal modem is dialing.
			ON (2 sec)		RECOVERY: The recovery procedure failed.
ON (2 sec)					RECOVERY: The recovery procedure succeeded.
ON				ON	FLASH PROCEDURE: The flash procedure has been started. Please wait.
Running light	Running light	Running light		ON	FLASH PROCEDURE: The flash procedure is currently executed.
Blink 50/800	Blink 50/800	Blink 50/800		ON	FLASH PROCEDURE: The flash procedure succeeded.

Table 19-5 System states represented by lighting and blinking behavior of the LEDs

STAT	MOD	Info 2 (Sig)	ERR	FAULT	Description of the system state
ON			ON		FLASH PROCEDURE: The flash/production procedure failed.
			Blink 50/100 (5 sec)		FLASH PROCEDURE WARNING: Replacing the rescue system. Do not power off. When the blinking stops, the replacement of the rescue system is over.
			ON		FLASH PROCEDURE: The DHCP/BOOTP requests failed.
			ON		FLASH PROCEDURE: Mounting the data storage device failed.
			ON		FLASH PROCEDURE: The flash procedure failed.
			ON		FLASH PROCEDURE: Erasing the file system partition failed.
			ON		FLASH PROCEDURE: Failed to load the firmware image.
			ON		FLASH PROCEDURE: The signature of the firmware image is not valid.
			ON		FLASH PROCEDURE: Failed to load the install script.
			ON		FLASH PROCEDURE: The signature of the install script is not valid.
			ON		FLASH PROCEDURE: The rollout script failed.