VPN TUNNEL

VPN connection between a TC ROUTER and an mGuard

Application note
107965_en_00

© PHOENIX CONTACT 2018-03-14

1 Description

This application note describes how you can establish a VPN connection between a mobile router and an mGuard. This requires the use of certificates.

Make sure that the latest firmware is installed on the devices.

You need the following:

Description	Order No.	Designation	Link to item
LTE 4G router, client	2702528	TC ROUTER 3002T-4G	phoenixcontact.net/product/2702528
Alternative:			
3G router, client	2702529	TC ROUTER 3002T-3G	phoenixcontact.net/product/2702529
Security appliance, server	2200515	FL MGUARD RS4000 TX/TX VPN	phoenixcontact.net/product/2200515

WARNING:
This application note does **not** replace the device-specific documents.
Please observe the safety notes in the associated packing slips and user manuals.

Make sure you always use the latest documentation. It can be downloaded using above links.

Table of contents

2 Certificates

Learn how to create certificates in the “Quick Reference Guide for creating certificates” at phoenixcontact.com/product/2702528.

Required certificates

Four certificates are required for a VPN tunnel between the TC ROUTER and the mGuard.

For upload to the TC ROUTER:

– Client1.p12# (private)
– mGuard.crt (public)

For upload to the mGuard:

– mGuard.p12# (private)
– Client1.crt (public)

3 Network plan

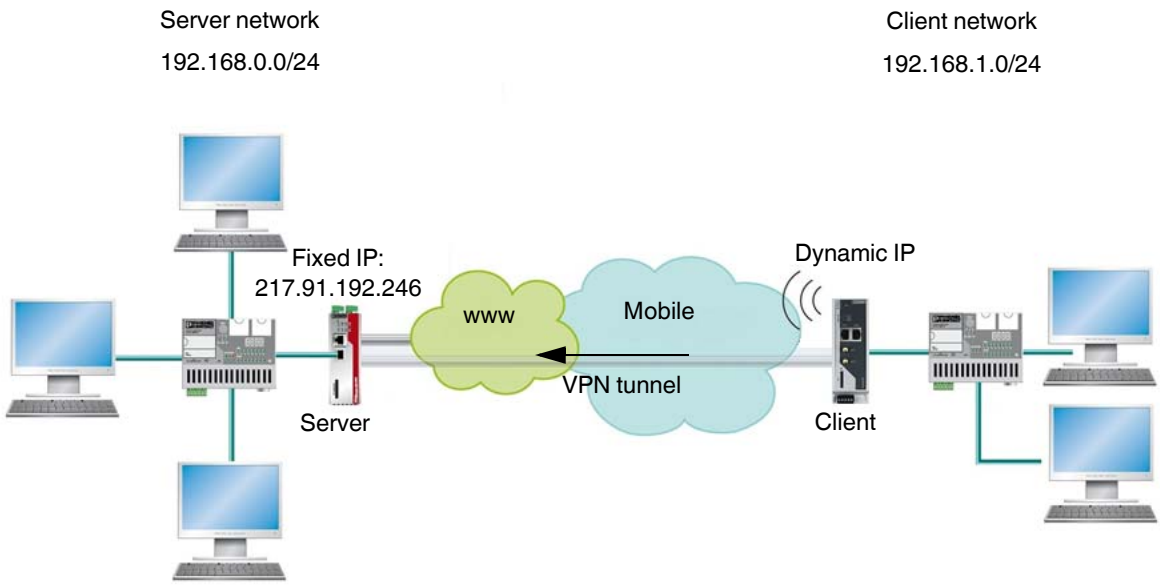

Figure 1 Network plan

4 Configuring the mobile router

Ensure that access to the mobile network is possible.

For additional information on mobile communication, refer to the mobile communication guide at phoenixcontact.com/product/2702528.

- Connect the mobile router to the public Internet access.
- The settings for establishing the Internet access can be found in the user manual for the router.
- Open the web-based management of the router.
- Log in with your user name and password.

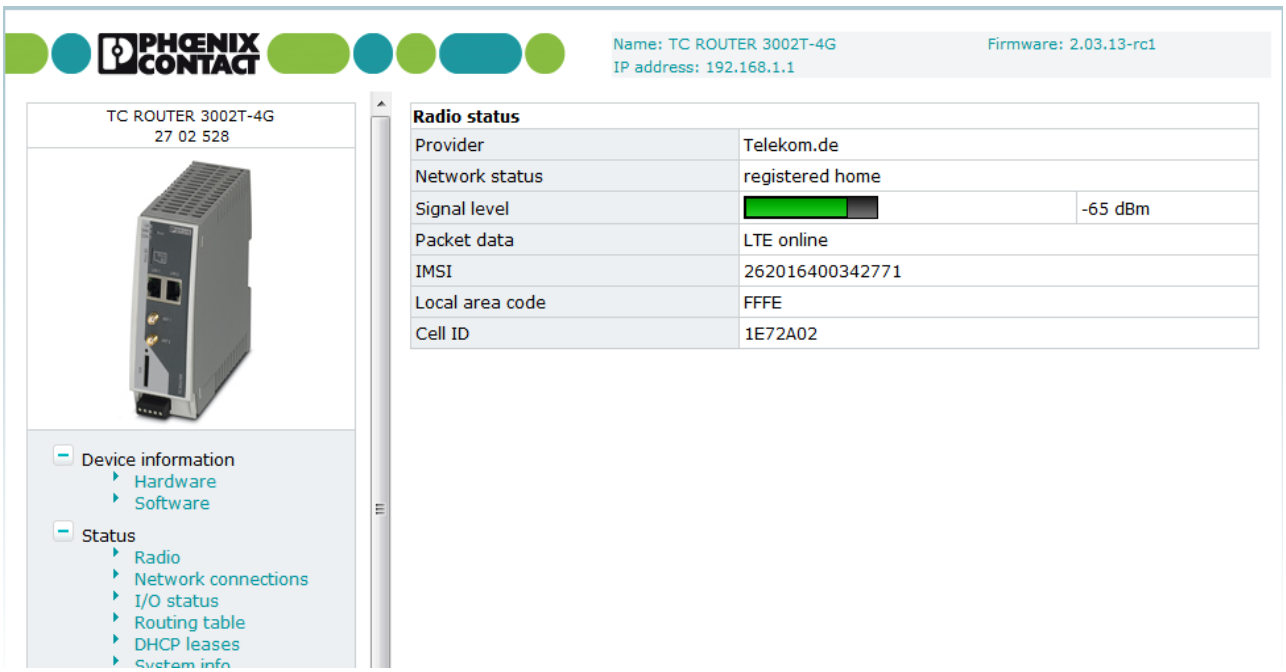

Figure 2 Active Internet connection

- Switch to the “VPN, IPsec, Certificates” subfolder.

Figure 3 Selecting certificates

- Load the previously created certificates to the mobile router.
- Confirm with “Apply”.

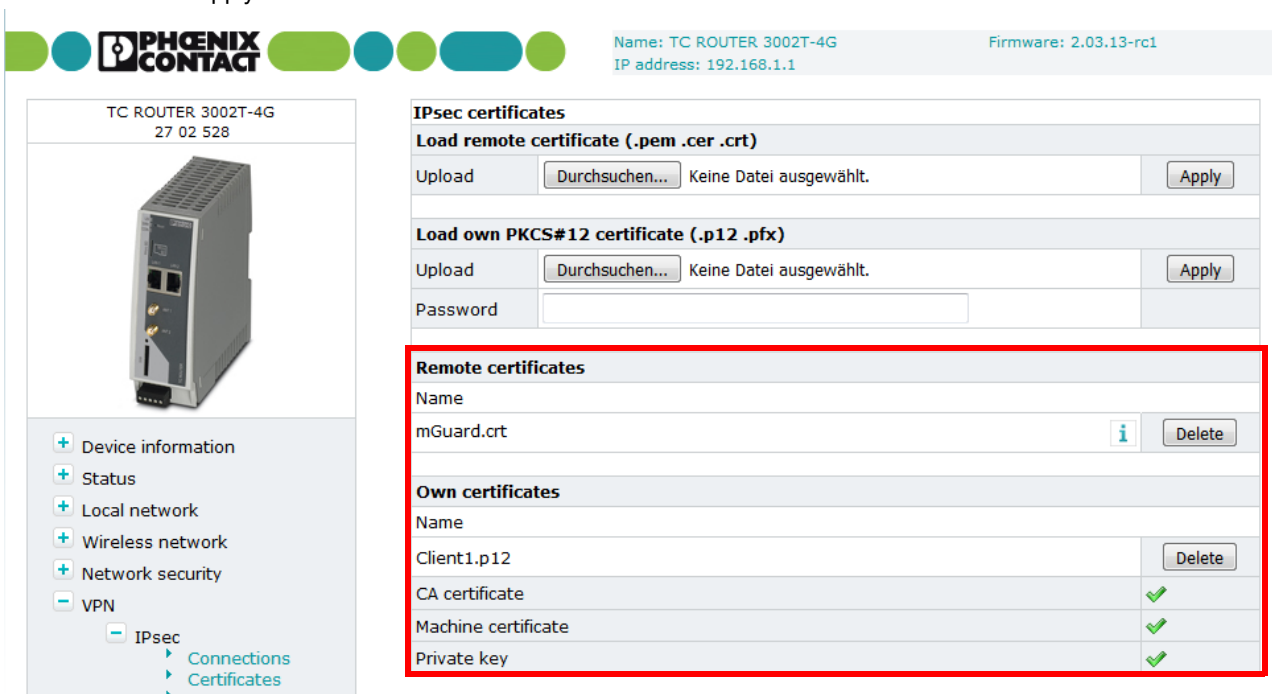

Figure 4 Certificates loaded

The certificates are now uploaded. You can use the certificates for the VPN settings.

- Switch to the “VPN, IPsec, Connections” subfolder.
- In the section for one of the three VPN tunnels, click on "Settings, Edit".

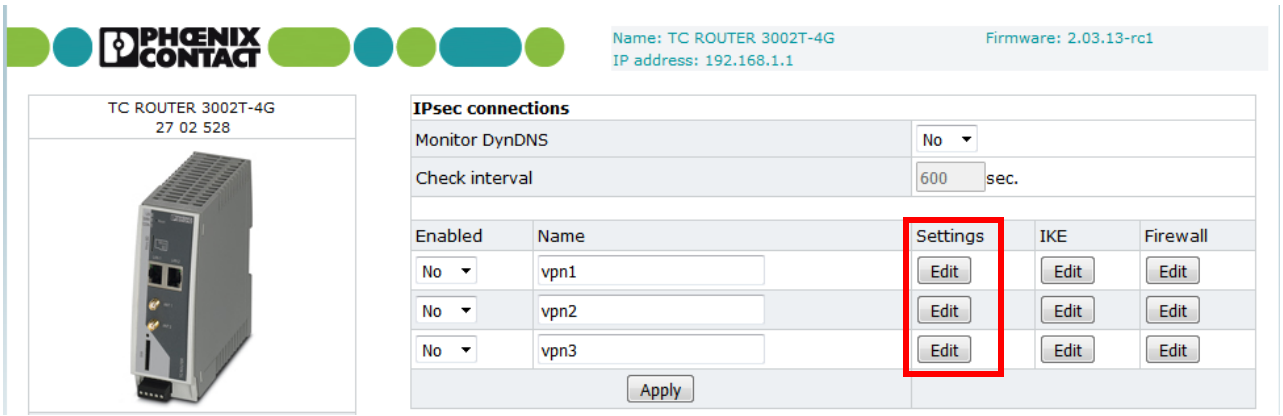

Figure 5 Configuring the VPN tunnel

The settings in the following screenshot are selected as displayed in the network plan (see Page 3).

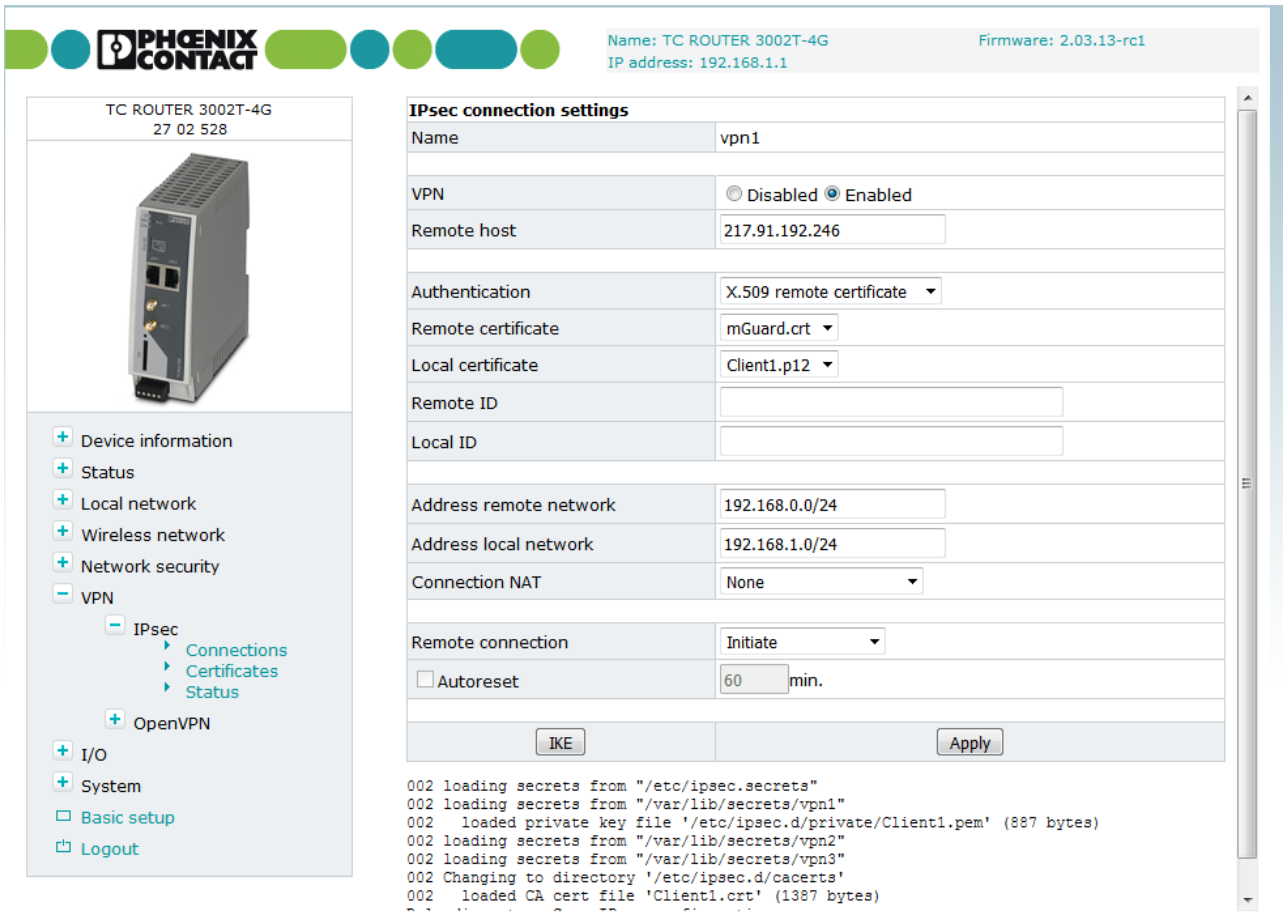

Figure 6 VPN tunnel settings

Remote host	Public IP address of the peer
Remote certificate	Public certificate of the peer (mGuard.crt)
Local certificate	Private certificate of the mobile router (Client1.p12)
Address remote network	Network area of the VPN server
Address local network	Network area of the VPN client
Remote connection	Information if mobile router is client or server

- Configure the VPN tunnel.
- Confirm with “Apply”.

- Switch to the IKE settings. Here, the encryption of the VPN tunnel is determined.
- Take the settings from the figure below.

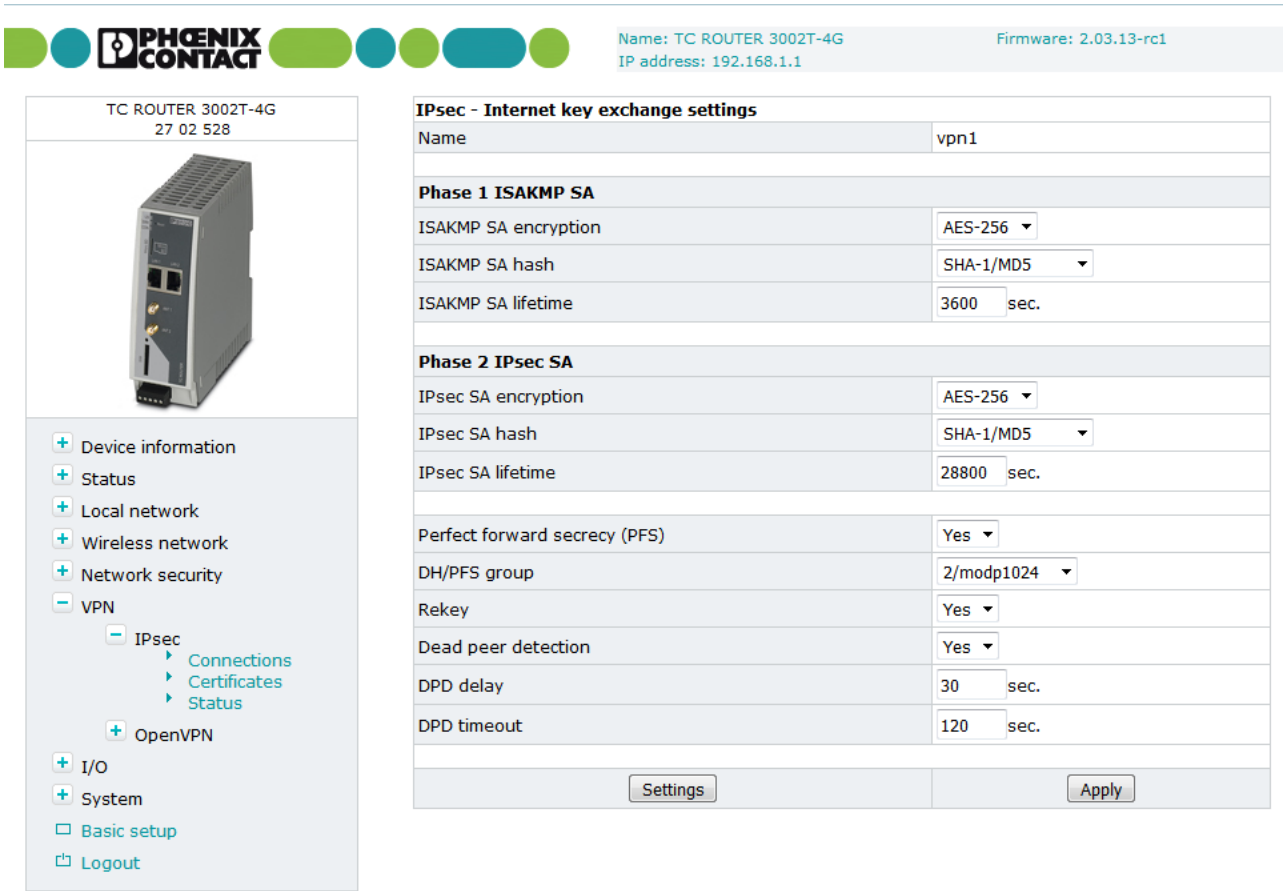

Figure 7 IKE settings TC ROUTER

5 Configuring the mGuard

Make sure the mGuard can be connected to the Internet. For the required settings, refer to the user manual at phoenixcontact.net/product/2200515.

- Connect the mGuard to the public Internet access.
- Log in to the mGuard.
- Set the matching IP address. The IP address must be located in the network you are using for the VPN tunnel. In our example on Page 3, we have selected the following network: 192.168.0.0/24
- The mGuard contains an IP address from this network. The settings can be found at "Network, Interfaces, Internal".

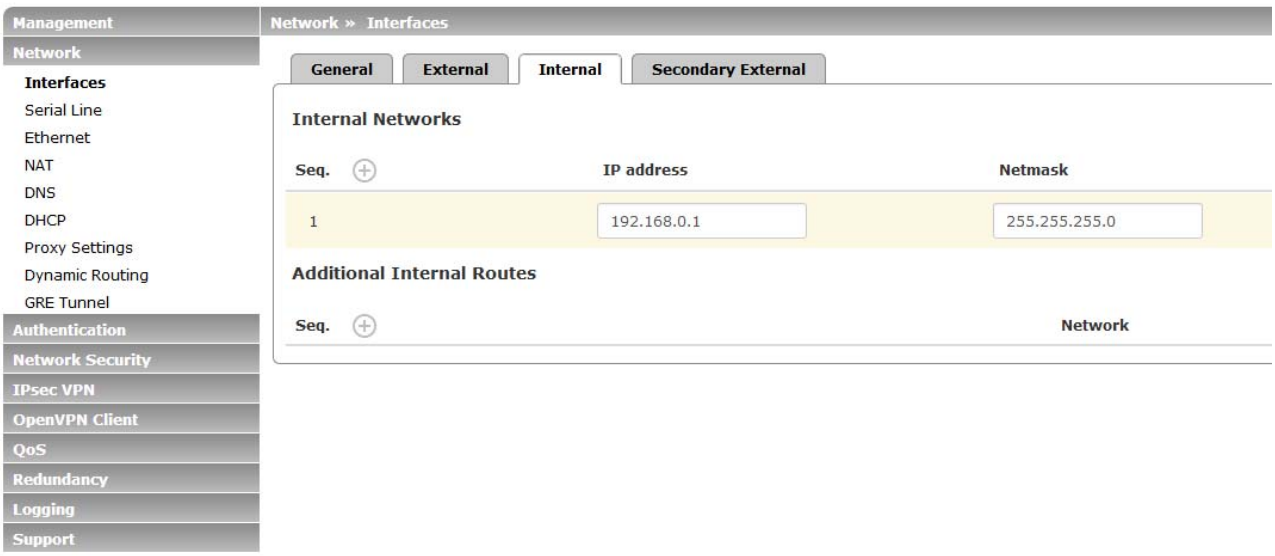

Figure 8 IP address of the mGuard

- Switch to the tab "Authentication, Certificates, Machine Certificates".
- Select the private certificate mguard.p12#.
- Upload the certificate.
- Save the settings.

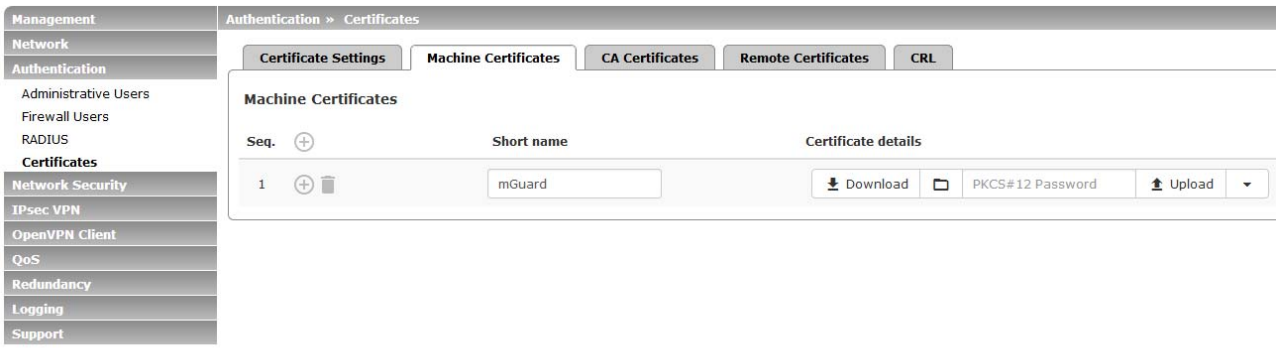

Figure 9 Uploading a private certificate

- Switch to the tab "IPsec VPN, Connections".
- To create a new VPN tunnel, click on "+".
- Enter a name for the VPN tunnel.

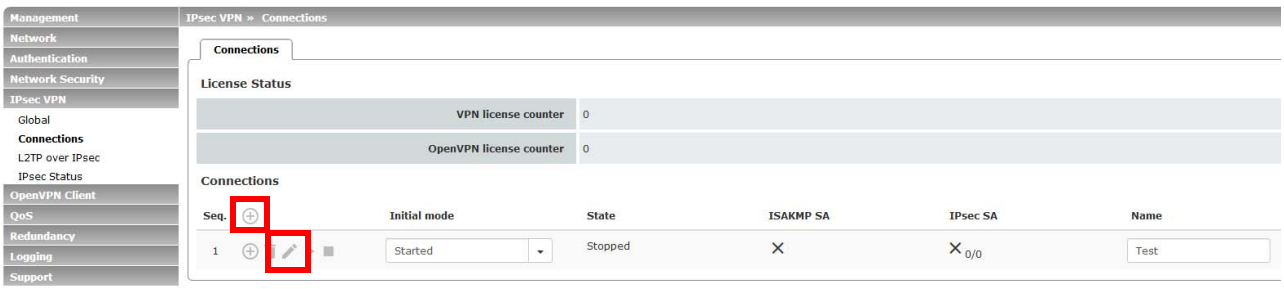

Figure 10 Creating and configuring the VPN tunnel

- To change the settings, click on the "pen" symbol.

- You only have to adapt the network parameters. In the example on Page 3, the following network addresses were used:
  - 192.168.0.0/24 (server)
  - 192.168.1.0/24 (client)

  Enter these addresses under "General, Transport and Tunnel Settings".

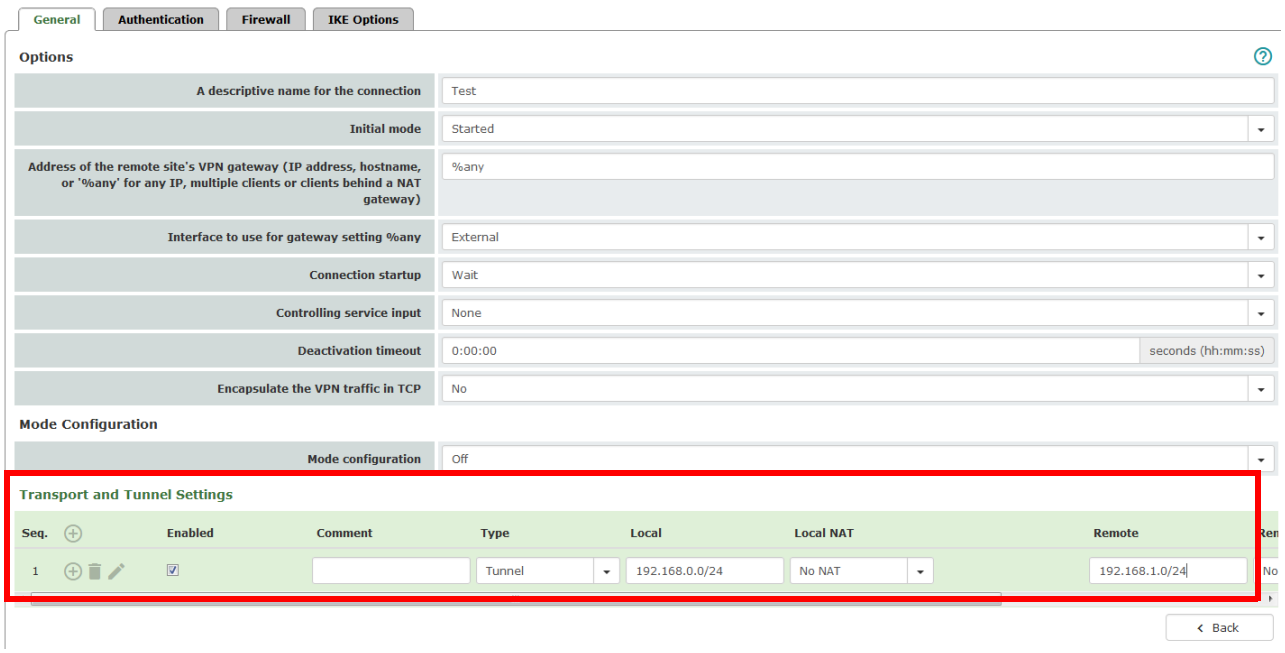

Figure 11 Entering network addresses

- Switch to the tab "Authentication".
- Under "Local X.509 certificate", select the certificate mGuard.p12#.
- Under "Remote certificate", upload the public certificate Client1.crt.

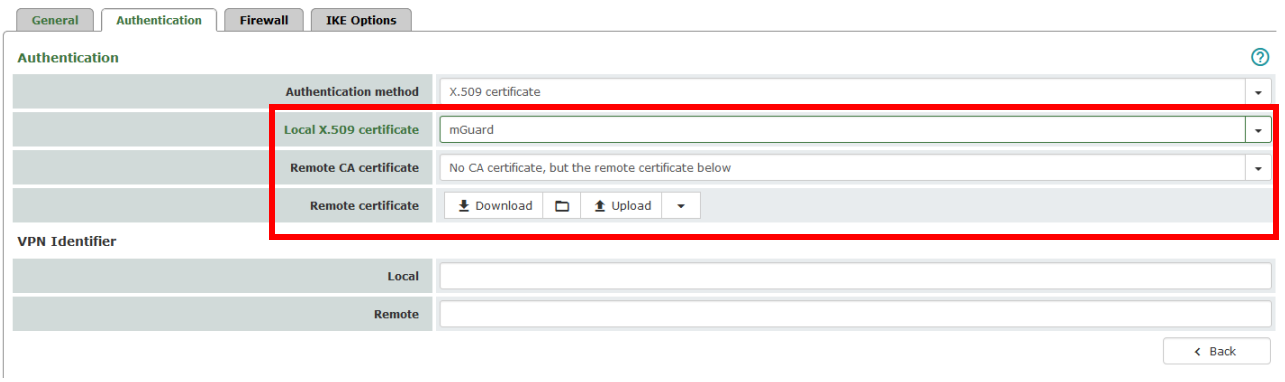

Figure 12 Selecting certificates

- Switch to the tab "IKE Options".
- Here, enter the same settings as for the mobile router (see Page 8).
- Save the settings.

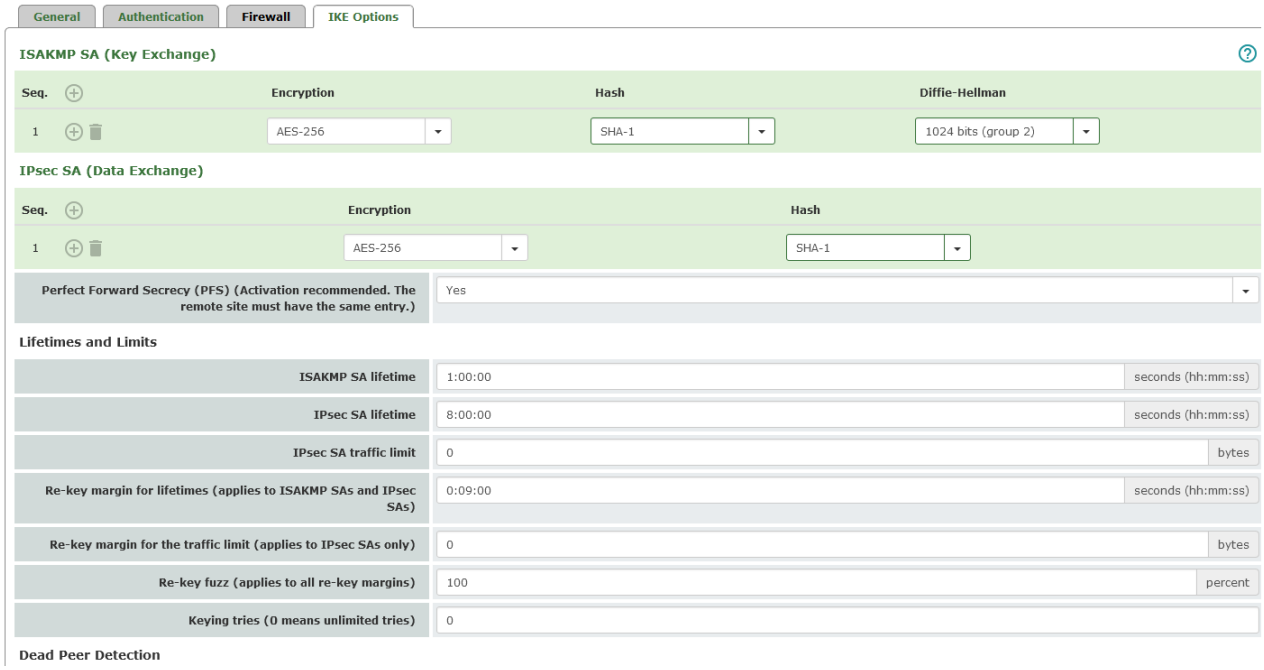

Figure 13 IKE settings mGuard

The VPN configuration is now complete. The mGuard is listening for incoming VPN connections.

In many applications, another router establishes the connection to the Internet in front of the mGuard.

Port forwarding is required so that the mGuard still can receive incoming VPN packages.

- Activate port forwarding to the WAN-IP address of the mGuard using the ports 4500 UDP and 500 UDP.

6 VPN status

mGuard

The connection overview of the mGuard on the first page at "IPsec VPN" shows if the VPN tunnel is established.

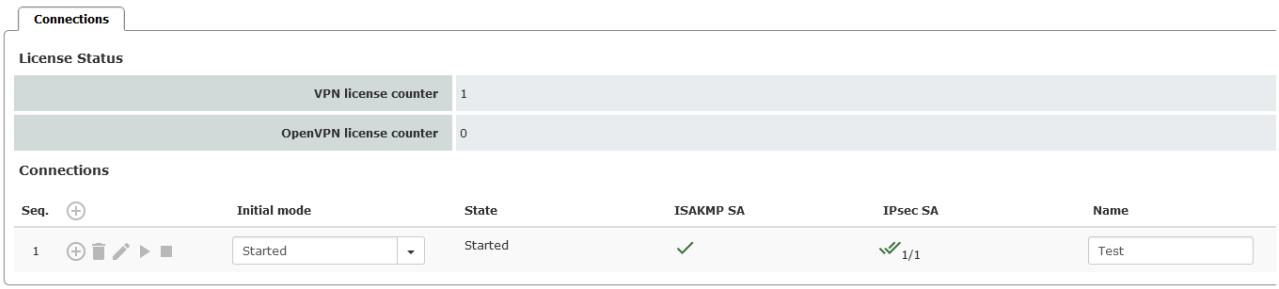

Figure 14 VPN status mGuard

TC ROUTER

The VPN status can be found on the TC ROUTER at "VPN, IPsec, Status".

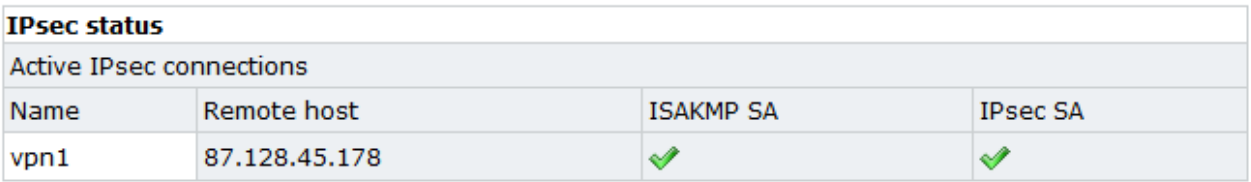

Figure 15 VPN status TC ROUTER

6.1 Troubleshooting

Display		Possible error cause
ISAKMP SA	**IPsec SA**	
Red	Red	– Faulty target IP address in the client – Another router in front of the server. You have not set port forwarding to the server on this router. – Faulty certificates – The IKE settings for the ISAKMP-SA phase do not correspond.
Green	Red	– The IKE settings for the IPsec SA phase do not correspond. – Different network areas are set – The PFS is set for one device, but not for the other.
Green	Green	– See next page

If both ticks are green, but communication is not working:

In most cases a default gateway is missing.

- Check communication via the VPN tunnel using a simple ping command.

The figure shows a ping command from the PC connected to the mGuard. This way you can check if the VPN tunnel is working correctly.

Figure 16 Ping command from the mGuard towards the TC ROUTER