

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 Alternative:	2702528	TC ROUTER 3002T-4G	phoenixcontact.net/product/2702528
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

1	Description.....	1
2	Certificates.....	3
3	Network plan.....	3
4	Configuring the mobile router.....	4
5	Configuring the mGuard.....	9
6	VPN status.....	13
6.1	Troubleshooting	13

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

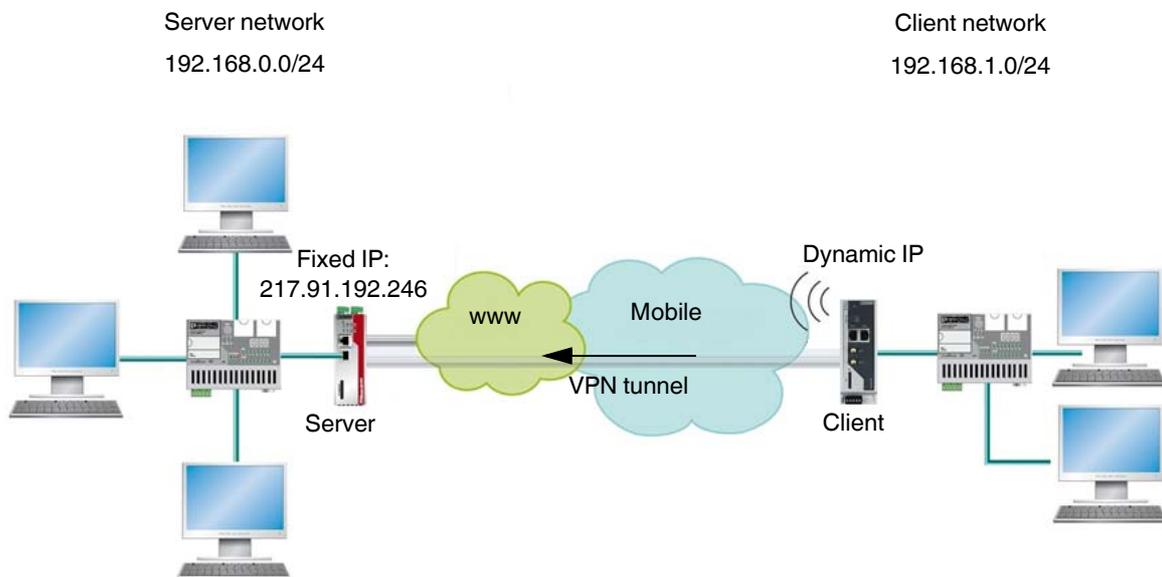


Figure 1 Network plan

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.

PHOENIX CONTACT

Name: TC ROUTER 3002T-4G
IP address: 192.168.1.1

Firmware: 2.03.13-rc1

TC ROUTER 3002T-4G
27 02 528

Radio status

Provider	Telekom.de
Network status	registered home
Signal level	<div style="width: 100%; height: 10px; background-color: green;"></div> -65 dBm
Packet data	LTE online
IMSI	262016400342771
Local area code	FFFE
Cell ID	1E72A02

Device information

- ▶ Hardware
- ▶ Software

Status

- ▶ Radio
- ▶ Network connections
- ▶ I/O status
- ▶ Routing table
- ▶ DHCP leases
- ▶ System info

Figure 2 Active Internet connection

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

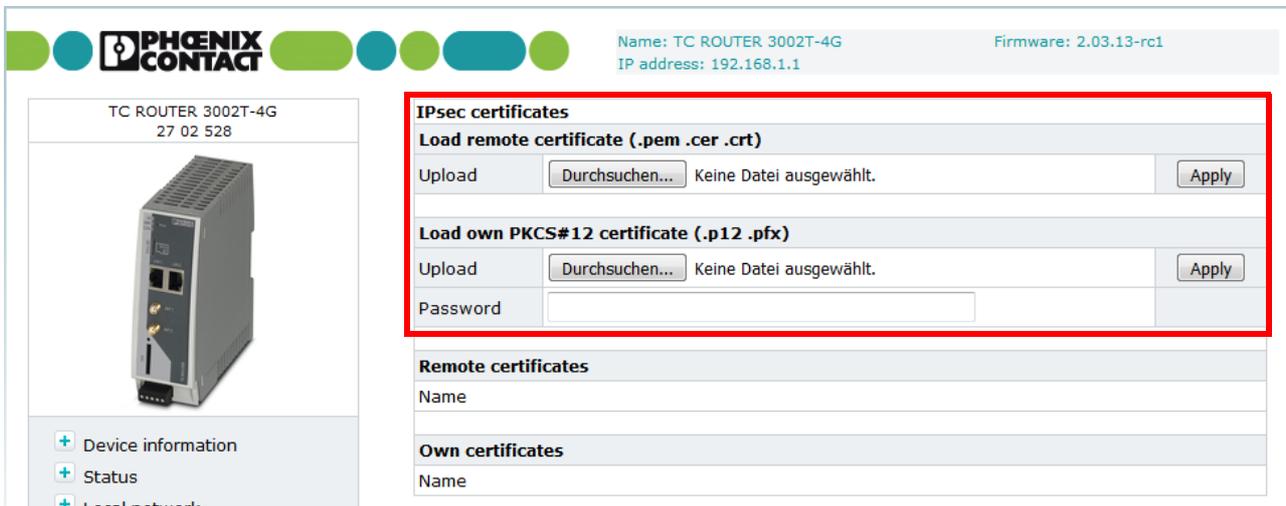


Figure 3 Selecting certificates

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

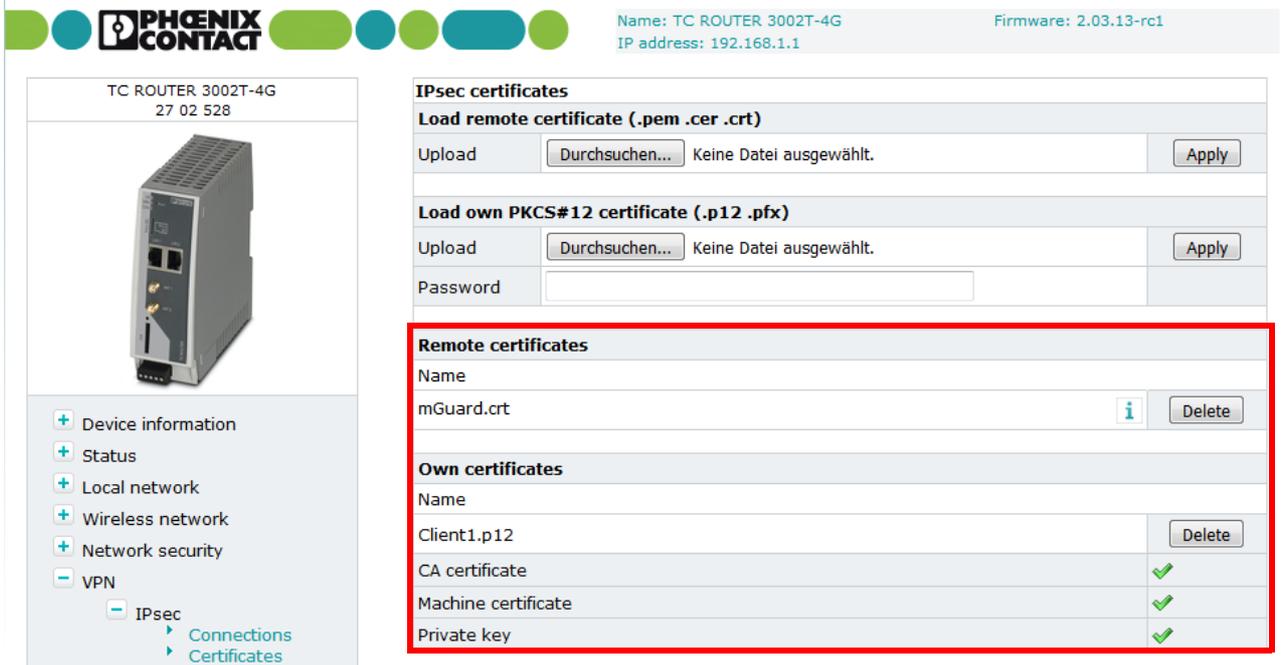
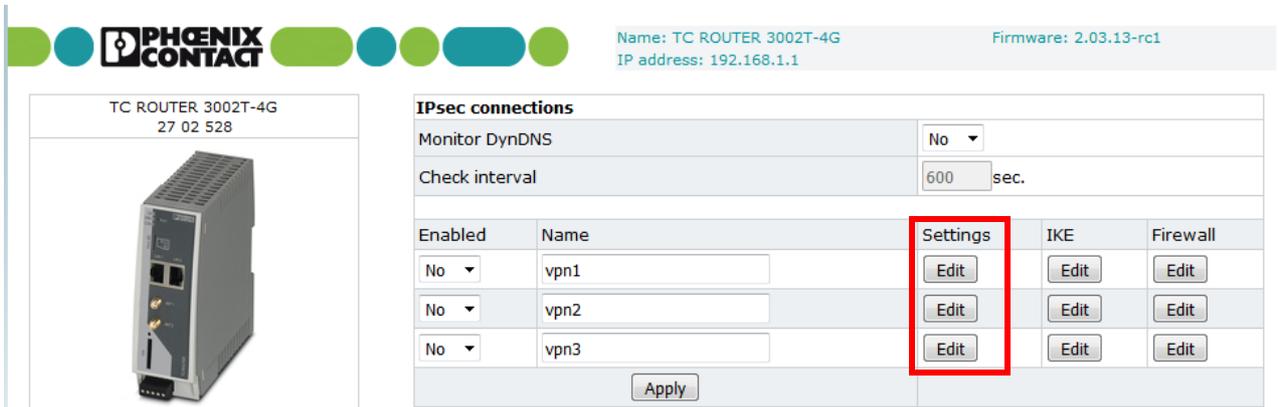


Figure 4 Certificates loaded

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".



PHOENIX CONTACT

Name: TC ROUTER 3002T-4G
IP address: 192.168.1.1

Firmware: 2.03.13-rc1

TC ROUTER 3002T-4G
27 02 528

IPsec connections

Monitor DynDNS: No

Check interval: 600 sec.

Enabled	Name	Settings	IKE	Firewall
No	vpn1	Edit	Edit	Edit
No	vpn2	Edit	Edit	Edit
No	vpn3	Edit	Edit	Edit

Apply

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.



Name: TC ROUTER 3002T-4G
IP address: 192.168.1.1

Firmware: 2.03.13-rc1

TC ROUTER 3002T-4G
27 02 528



- [+ Device information](#)
- [+ Status](#)
- [+ Local network](#)
- [+ Wireless network](#)
- [+ Network security](#)
- [- VPN](#)
 - [- IPsec](#)
 - [Connections](#)
 - [Certificates](#)
 - [Status](#)
 - [+ OpenVPN](#)
- [+ I/O](#)
- [+ System](#)
- [Basic setup](#)
- [Logout](#)

IPsec - Internet key exchange settings

Name	vpn1
Phase 1 ISAKMP SA	
ISAKMP SA encryption	AES-256
ISAKMP SA hash	SHA-1/MD5
ISAKMP SA lifetime	3600 sec.
Phase 2 IPsec SA	
IPsec SA encryption	AES-256
IPsec SA hash	SHA-1/MD5
IPsec SA lifetime	28800 sec.
Perfect forward secrecy (PFS)	Yes
DH/PFS group	2/modp1024
Rekey	Yes
Dead peer detection	Yes
DPD delay	30 sec.
DPD timeout	120 sec.

Settings
Apply

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".

Management	Network » Interfaces								
Network	<div style="display: flex; justify-content: space-around;"> General External Internal Secondary External </div>								
Interfaces	Internal Networks <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;">Seq.</th> <th style="width: 50%;">IP address</th> <th style="width: 40%;">Netmask</th> </tr> </thead> <tbody> <tr style="background-color: #ffffcc;"> <td style="text-align: center;">1</td> <td style="text-align: center;">192.168.0.1</td> <td style="text-align: center;">255.255.255.0</td> </tr> </tbody> </table>			Seq.	IP address	Netmask	1	192.168.0.1	255.255.255.0
Seq.	IP address	Netmask							
1	192.168.0.1	255.255.255.0							
Serial Line	Additional Internal Routes <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;">Seq.</th> <th style="width: 90%;">Network</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">+</td> <td></td> </tr> </tbody> </table>			Seq.	Network	+			
Seq.	Network								
+									
Ethernet									
NAT									
DNS									
DHCP									
Proxy Settings									
Dynamic Routing									
GRE Tunnel									
Authentication									
Network Security									
IPsec VPN									
OpenVPN Client									
QoS									
Redundancy									
Logging									
Support									

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.

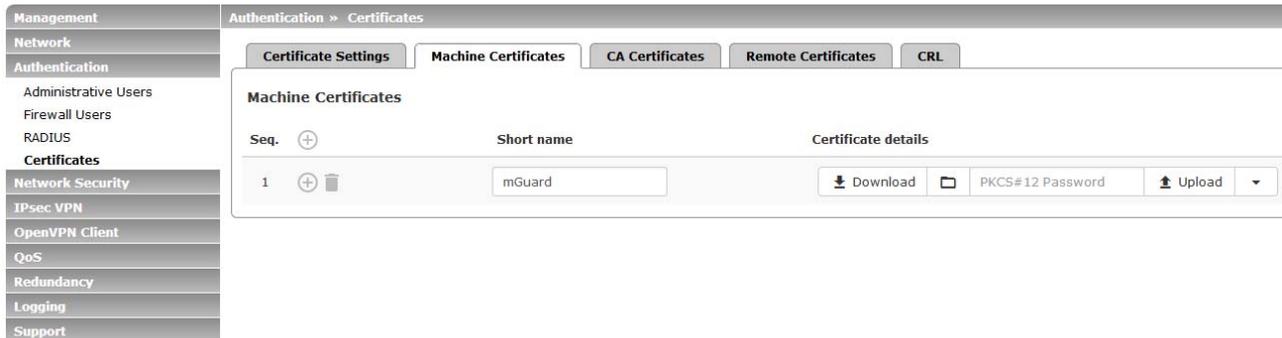


Figure 9 Uploading a private certificate

- 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".

The screenshot shows the 'VPN Tunnel' configuration page with tabs for 'General', 'Authentication', 'Firewall', and 'IKE Options'. The 'Options' section includes fields for connection name, initial mode, remote gateway address, interface, connection startup, controlling service input, deactivation timeout, and encapsulation. The 'Mode Configuration' section has a 'Mode configuration' dropdown set to 'Off'. The 'Transport and Tunnel Settings' section is highlighted with a red box and contains a table with the following data:

Seq.	Enabled	Comment	Type	Local	Local NAT	Remote
1	<input checked="" type="checkbox"/>		Tunnel	192.168.0.0/24	No NAT	192.168.1.0/24

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.

The screenshot shows the 'Authentication' tab selected. The 'Authentication method' is set to 'X.509 certificate'. The 'Local X.509 certificate' dropdown is set to 'mGuard'. The 'Remote CA certificate' dropdown is set to 'No CA certificate, but the remote certificate below'. The 'Remote certificate' field has 'Download' and 'Upload' buttons. The 'VPN Identifier' section has empty fields for 'Local' and 'Remote'. A red box highlights the 'Local X.509 certificate', 'Remote CA certificate', and 'Remote certificate' fields.

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.

General Authentication Firewall **IKE Options**

ISAKMP SA (Key Exchange)

Seq.	Encryption	Hash	Diffie-Hellman
1	AES-256	SHA-1	1024 bits (group 2)

IPsec SA (Data Exchange)

Seq.	Encryption	Hash
1	AES-256	SHA-1

Perfect Forward Secrecy (PFS) (Activation recommended. The remote site must have the same entry.) Yes

Lifetimes and Limits

ISAKMP SA lifetime	1:00:00	seconds (hh:mm:ss)
IPsec SA lifetime	8:00:00	seconds (hh:mm:ss)
IPsec SA traffic limit	0	bytes
Re-key margin for lifetimes (applies to ISAKMP SAs and IPsec SAs)	0:09:00	seconds (hh:mm:ss)
Re-key margin for the traffic limit (applies to IPsec SAs only)	0	bytes
Re-key fuzz (applies to all re-key margins)	100	percent
Keying tries (0 means unlimited tries)	0	

Dead Peer Detection

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.

Connections						
License Status						
VPN license counter		1				
OpenVPN license counter		0				
Connections						
Seq.	Initial mode	State	ISAKMP SA	IPsec SA	Name	
1	Started	Started	✓	✓ 1/1	Test	

Figure 14 VPN status mGuard

TC ROUTER

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

IPsec status			
Active IPsec connections			
Name	Remote host	ISAKMP SA	IPsec SA
vpn1	87.128.45.178	✓	✓

Figure 15 VPN status TC ROUTER

6.1 Troubleshooting

Display		Possible error cause
ISAKMP SA	IPsec SA	
Red	Red	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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.

```
C:\Users\User>ping 192.168.1.1

Ping wird ausgeführt für 192.168.1.1 mit 32 Bytes Daten:
Antwort von 192.168.1.1: Bytes=32 Zeit=122ms TTL=63
Antwort von 192.168.1.1: Bytes=32 Zeit=69ms TTL=63
Antwort von 192.168.1.1: Bytes=32 Zeit=334ms TTL=63
Antwort von 192.168.1.1: Bytes=32 Zeit=299ms TTL=63

Ping-Statistik für 192.168.1.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
    Minimum = 69ms, Maximum = 334ms, Mittelwert = 206ms
```

Figure 16 Ping command from the mGuard towards the TC ROUTER