## 1. Aufgaben

### 1.1 Verwaltung eines eigenen ssh-Schlüssels

Es können ein oder mehrere ssh-Schlüssel persistent auf den Router abgelegt werden. Über diese kann sich per SSH eingeloggt werden, ein Einloggen mit Username und Password ist nicht mehr möglich.
Die o.g. ssh-Schlüssel sind auch nach dem Reset des Routers in die Werkseinstellung, sowie nach einem Firmwareupdate des Routers verfügbar.

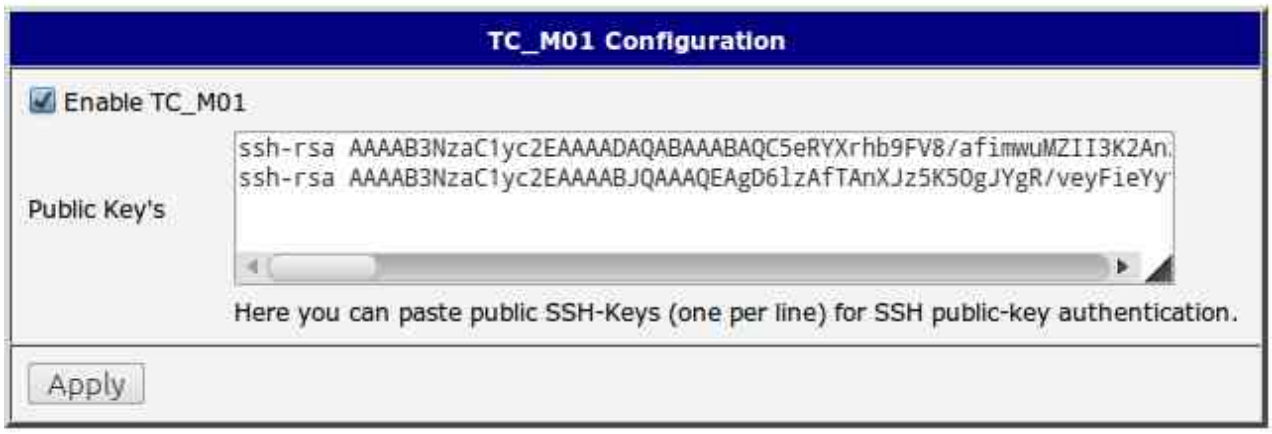
### 1.2 Verwaltung von IPSEC-Verbindungsdaten

Die IPSEC-Konfigurarion  wird auf dem Router persistent (s.o.) gespeichert.
Zertifikate und Schlüssel werden in einen flüchtigen Speicherbereich abgelegt, d.h. bei einem Neustart des Routers gehen diese Daten verloren.
Das Modul überwacht das Vorhandensein der IPSEC-Zertifikate und -Schlüssel und startet den konfigurierten IPSEC-Tunnel wenn diese vorhanden sind.
Werden die Zertifikate wieder vom Router entfernt, wird auch der IPSEC-Tunnel beendet.
Die Zertifikate und Schlüssel können per „sftp“ auf dem Router abgelegt werden. (z.B. mit WinSCP)

## 2. Installation

Das Softwaremodul „TC_M01“ wird über den Menüpunkt „User Modules“ installiert.

## 3. Konfiguration




**- Enable TC_M01**

über diese Checkbox wird das Usermodul aktiviert.
Das Usermodul ist in der Defaulteinstellung aktiviert.

**ACHTUNG :** Soll das Usermodul deinstalliert werden ist es vorher zu deaktivieren, da sonst nicht alle Teile des Moduls vom Router entfernt werden können.

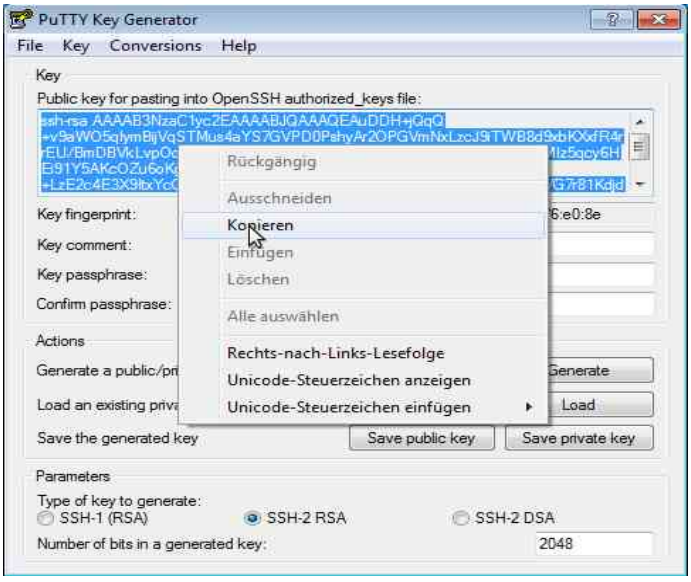
**- Public Key's**

Hier können ein oder mehrere öffentliche Schlüssel zur ssh-Authentifizierung abgelegt werden.
Die Schlüssel bleiben auch bei einem Werkseinstellungs-RESET ober beim Firmwareupdate des Routers erhalten.

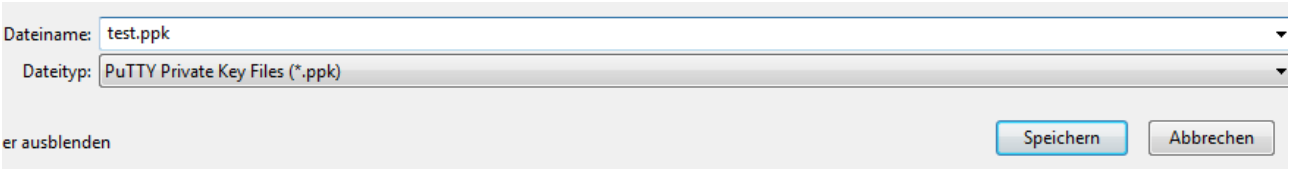
## 4. Erzeugung von ssh-Schlüsselpaaren mit „PuTTYgen“

- starten Sie „PuTTYgen“ und clicken Sie auf den Button „Generate“, folgen Sie dann den Anweisungen.


- Den erzeugten Public-Key können Sie über die Zwischenablage in das Usermodul kopieren. (siehe Punkt 3)



- Danach speichern Sie den „Private-Key“ z.B. zur Benutzung in „WinSCP“

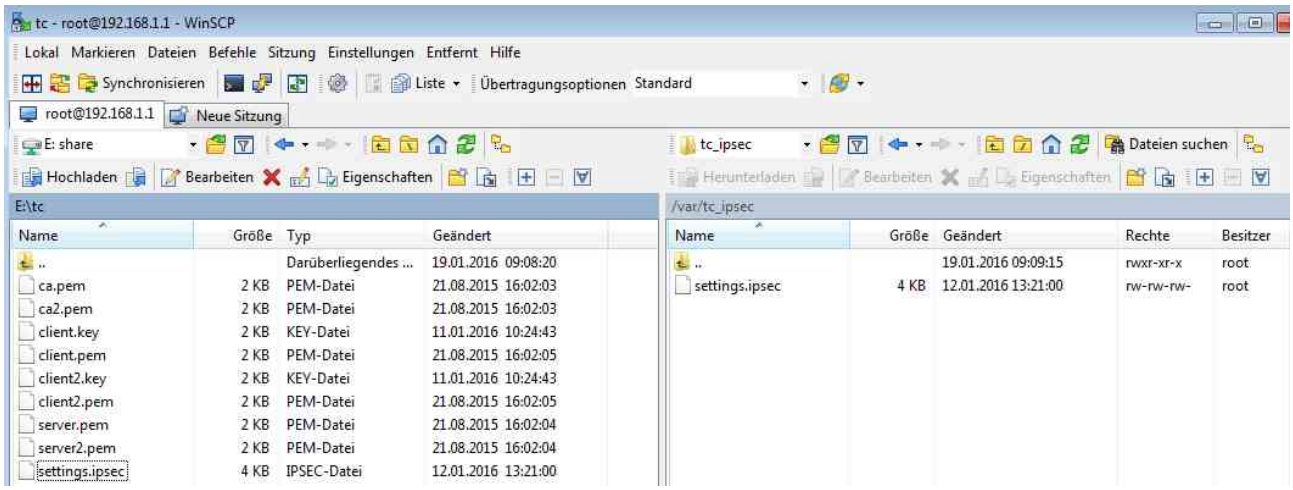



## 5. IPSEC

### 5.1 Konfiguration

Die Konfiguration der IPSEC-Tunnel erfolgt im Menüpunkt „Ipsec“ des Routers.
Es können alle 4 Tunnel benutzt werden. Zertifikate und Schlüssel werden nicht permanent gespeichert. Um eine Ipsec-Konfiguration abzuschließen kann man in die Felder für Zertifikate und Schlüssel Füllwörter oder -Zeichen einsetzten, (z.B. „-“) somit kann man die Konfiguration mit „Apply“ abschließen.

Weiterhin ist es möglich eine vorgefertigte Ipsec-Konfiguration per SFTP in den Router einzuspielen. Dazu muss diese als „ipsec.settings“ im Verzeichnis „/var/tc_ipsec/“ abgelegt werden.




### 5.2 Zertifikate und Schlüssel

Ohne die notwendigen Zertifikate und Schlüssel ist die jeweilige Ipsec-Verbindung deaktiviert. Nach Einspielen dieser wird der Ipsec-Tunnel automatisch aktiviert und gestartet. Die Zertifikate und Schlüssel müssen in das Verzeichnis „/var/tc_ipsec_certs“ abgelegt werden dabei sind folgende Nameskonventionen zu beachten.

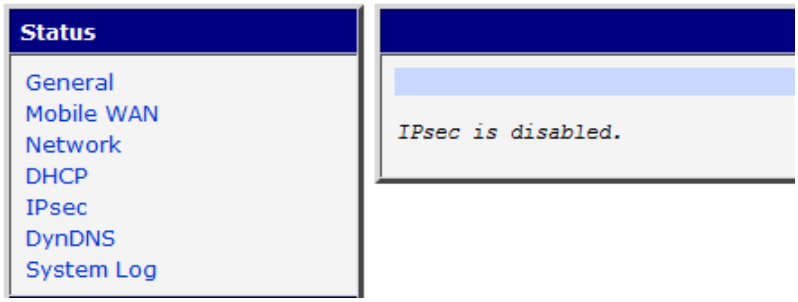
CA-Zertifikate
ca.pem, ca2.pem, ca3.pem, ca4.pem

Server-Zertifikate
server.pem, server2.pem, server3.pem, server4.pem

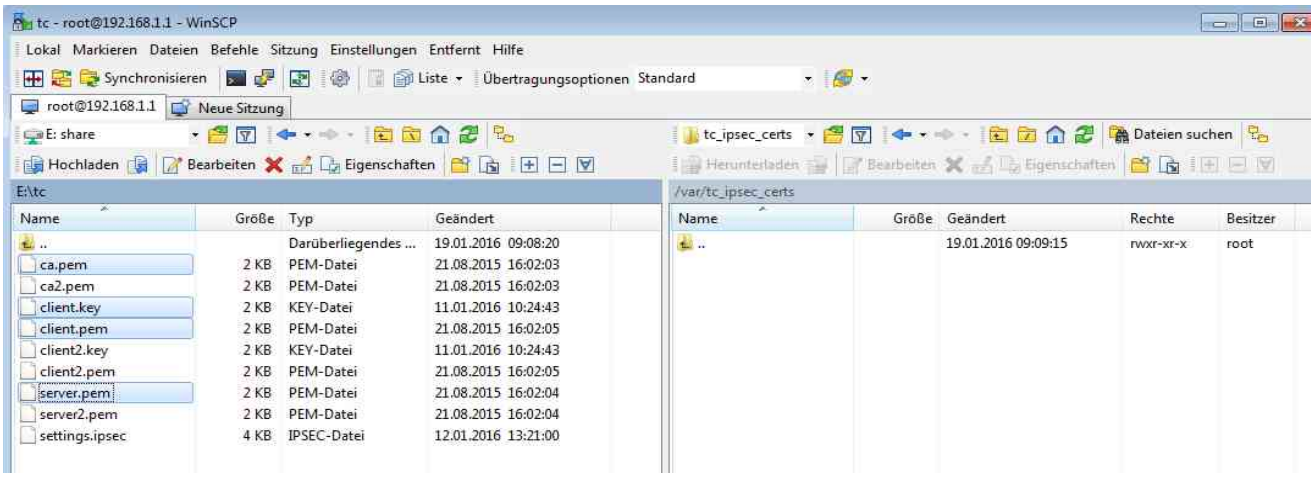
Client-Zertifikate
client.pem, client2.pem, client3.pem, client4.pem

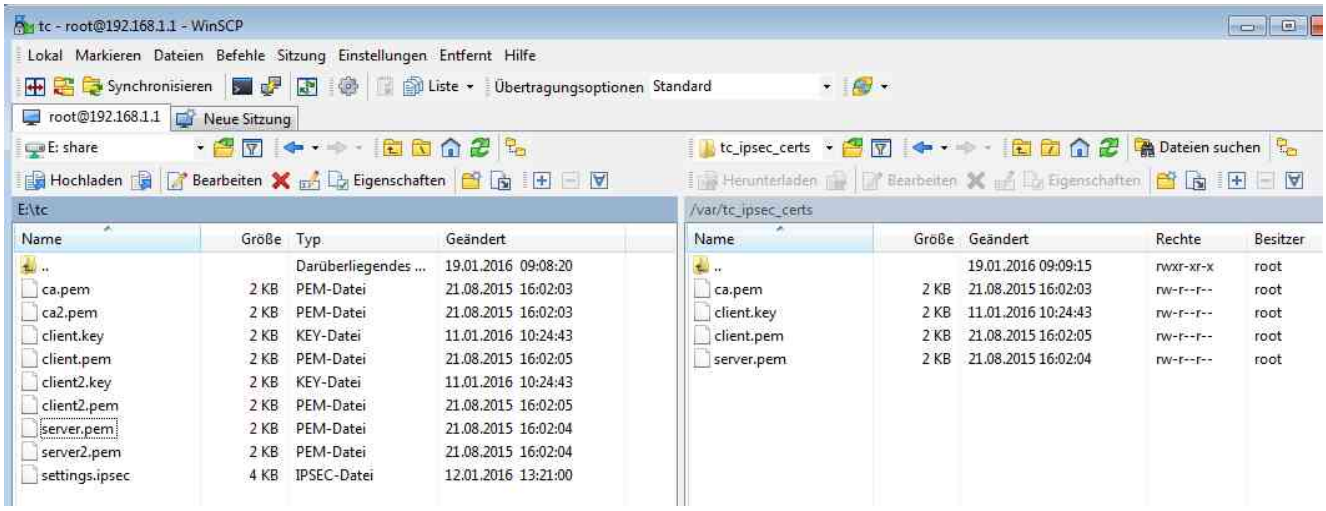
Die Dateinamen ohne Index beziehen sich auf den Ipsec-Tunel 1, die mit dem Index 2, 3 oder 4 jeweils auf den Ipsec-Tunnel 2, 3 oder 4.

Wenn keine Zertifikatsdaten eingespielt sind, ist kein Ipsec-Tunnel aktiv.

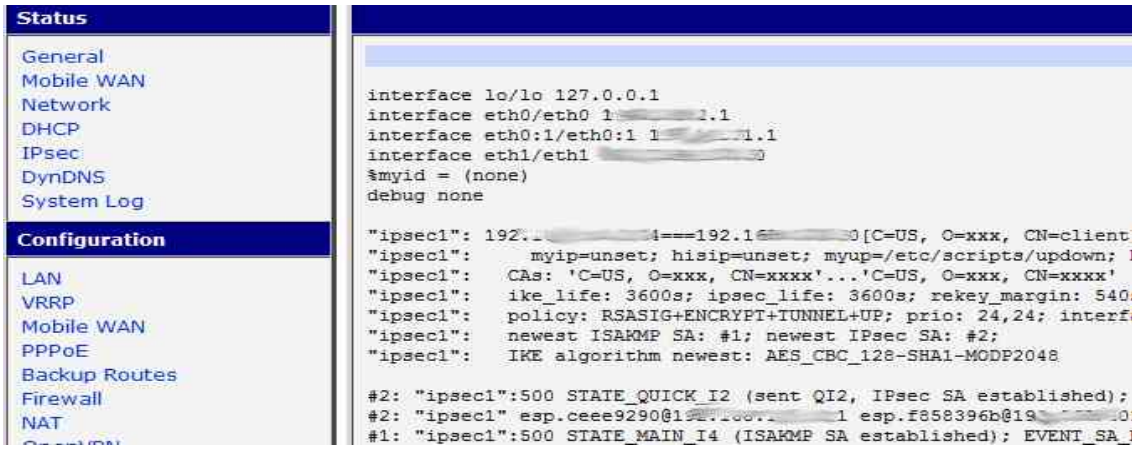



Einspielen der Daten

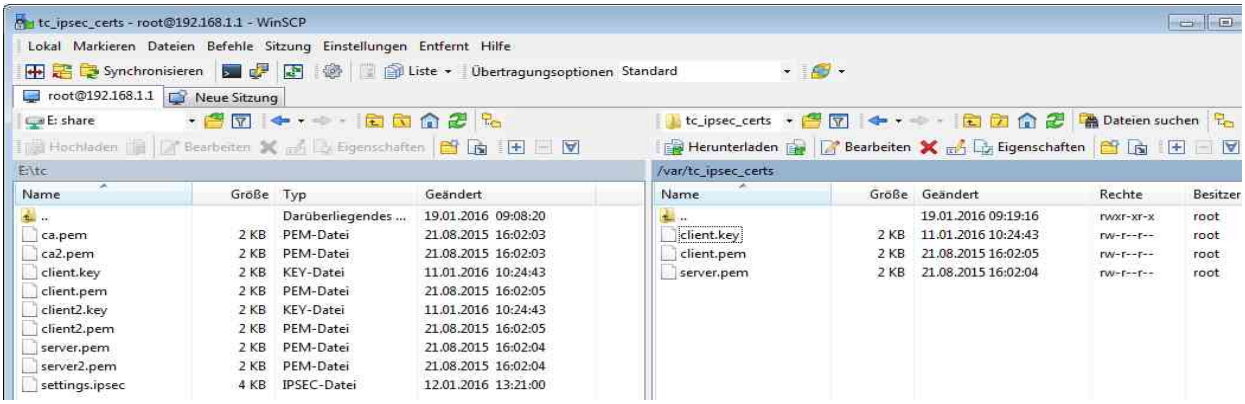


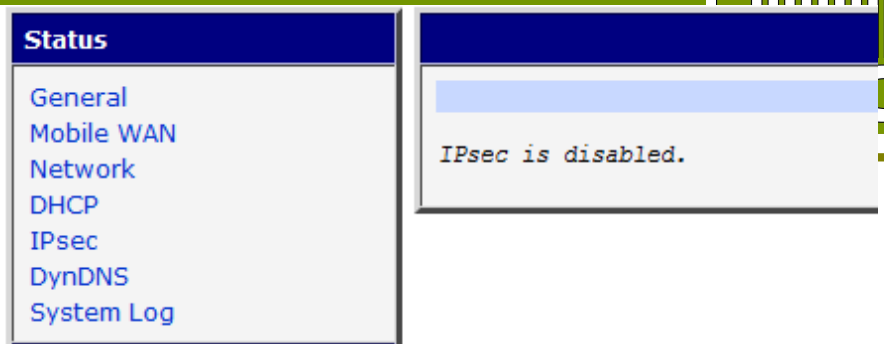



Nach dem Einspielen der Daten startet der Ipsec-Tunnel automatisch.




Wird nur ein Zertifikatsfile entfernt baut sich der Tunnel automatisch ab und wird deaktiviert.




Status
General
Mobile WAN
Network
DHCP
IPsec
DynDNS
System Log
IPsec is disabled.