

1. Aufgaben

1.1 Verwaltung eines eigenen ssh-Schlüssels

1.2 Verwaltung von IPSEC-Verbindungsdaten

2. Installation

3. Konfiguration

4. Erzeugung von ssh-Schlüsselpaaren mit „PuTTYgen“

5. IPSEC

5.1 Konfiguration

5.2 Zertifikate und Schlüssel

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-Konfiguration 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.

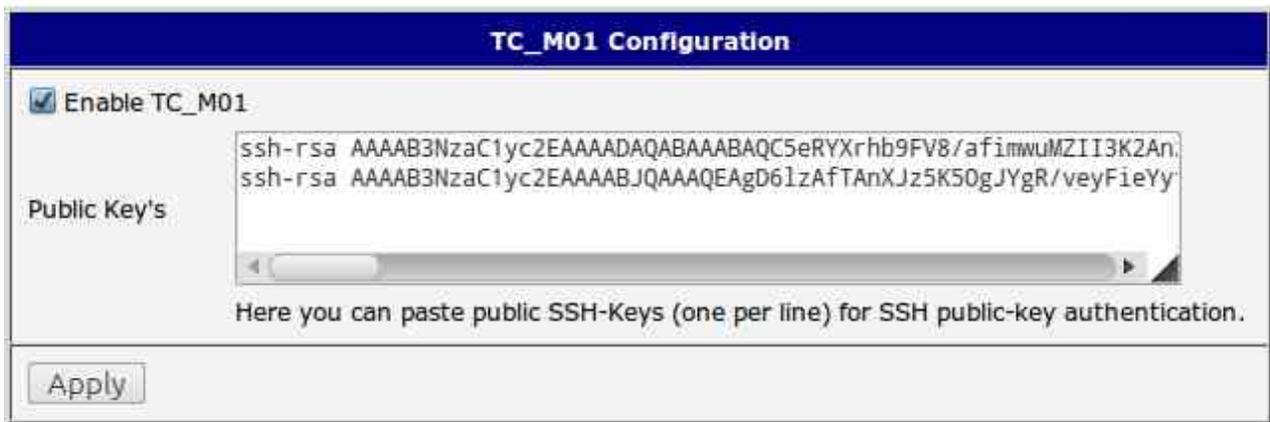
Werden die Zertifikate wieder vom Router entfernt, wird auch der IPSEC-Tunnel beendet. Die Zertifikate und Schlüssel können per „sftp“ auf dem Router abgelegt werden. (z.B. mit WinSCP)

2. Installation

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



3. Konfiguration

A screenshot of a web-based configuration interface titled "TC_M01 Configuration". At the top, there is a blue header bar with the title. Below the header, there is a checkbox labeled "Enable TC_M01" which is checked. Underneath, there is a text area labeled "Public Key's" containing two lines of SSH public keys: "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQ5eRYXrhb9FV8/afimwuMZII3K2An" and "ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAgD61zAfTAnXJz5K50gJYgR/veyFieYy". Below the text area is a horizontal scrollbar. At the bottom of the form, there is a button labeled "Apply". Below the form, there is a note: "Here you can paste public SSH-Keys (one per line) for SSH public-key authentication."

- 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.

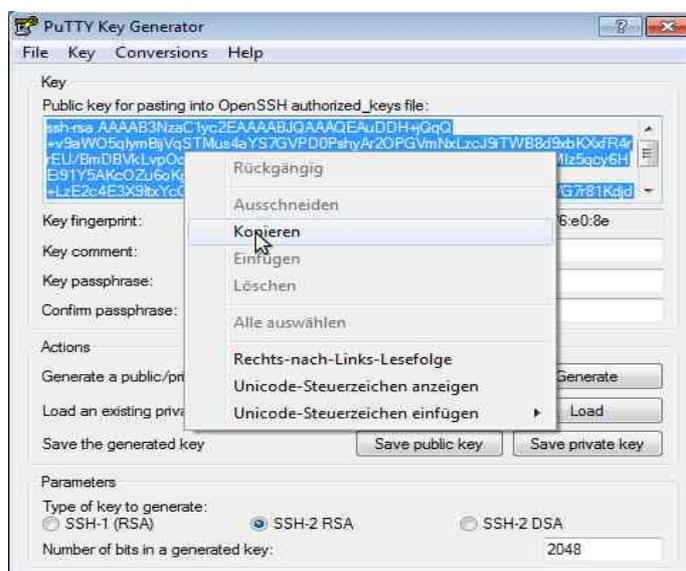
Die Schlüssel bleiben auch bei einem Werkseinstellungs-RESET oder beim Firmwareupdate des Routers erhalten.

4. Erzeugung von ssh-Schlüsselpaaren mit „PuTTYgen“

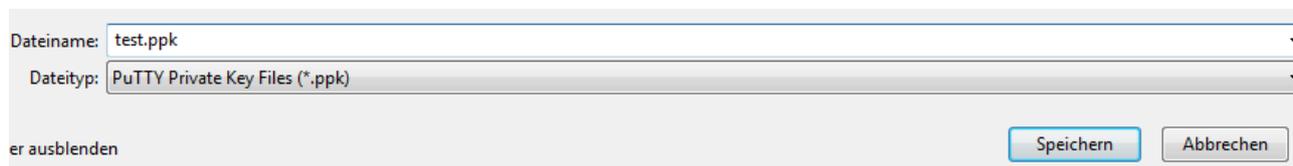
- starten Sie „PuTTYgen“ und klicken Sie auf den Button „Generate“, folgen Sie dann den Anweisungen.



- 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“

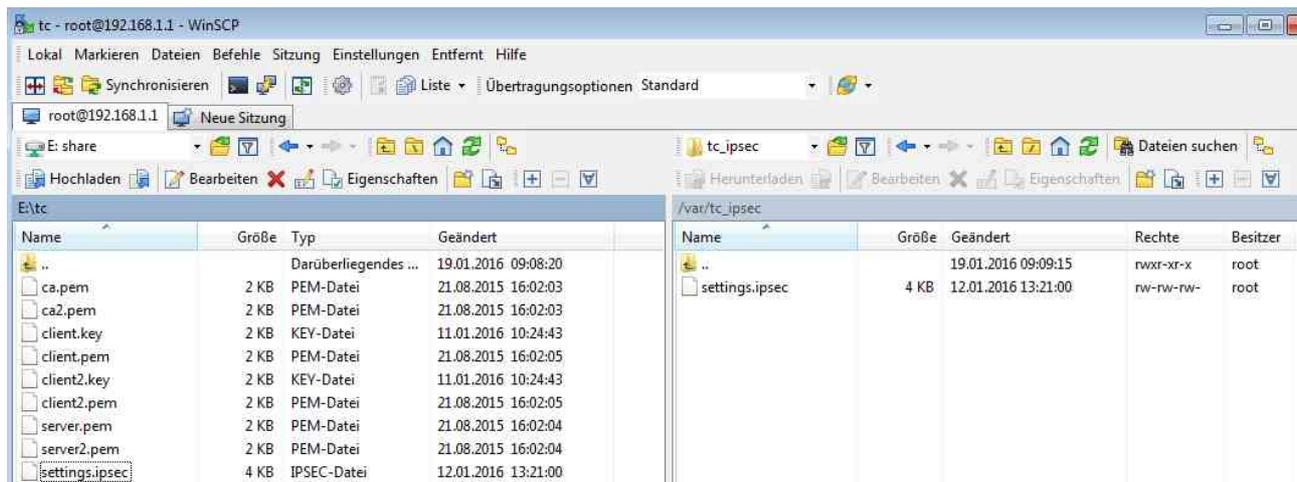


5. IPSEC

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 einsetzen, (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

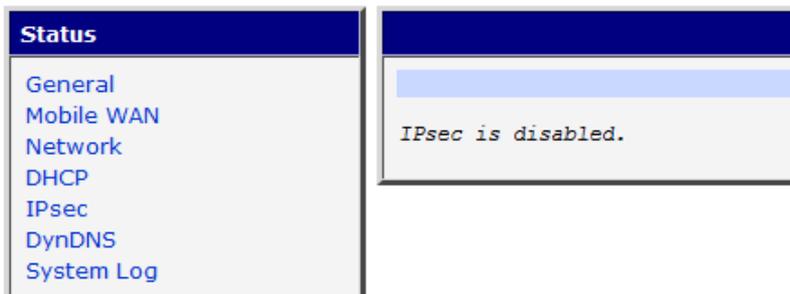
server.pem, server2.pem, server3.pem, server4.pem

Client-Zertifikate

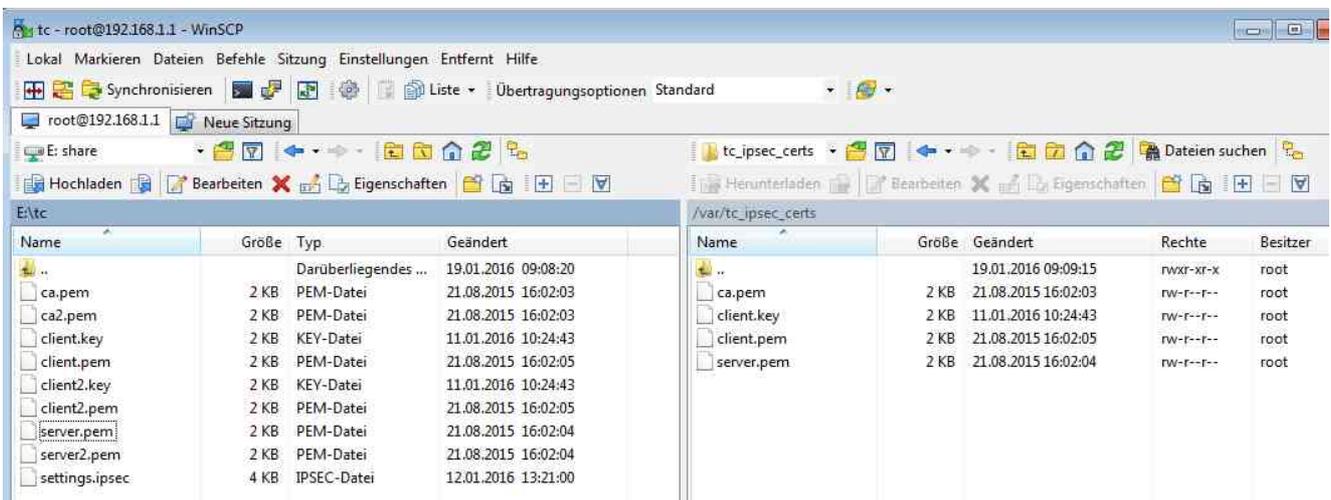
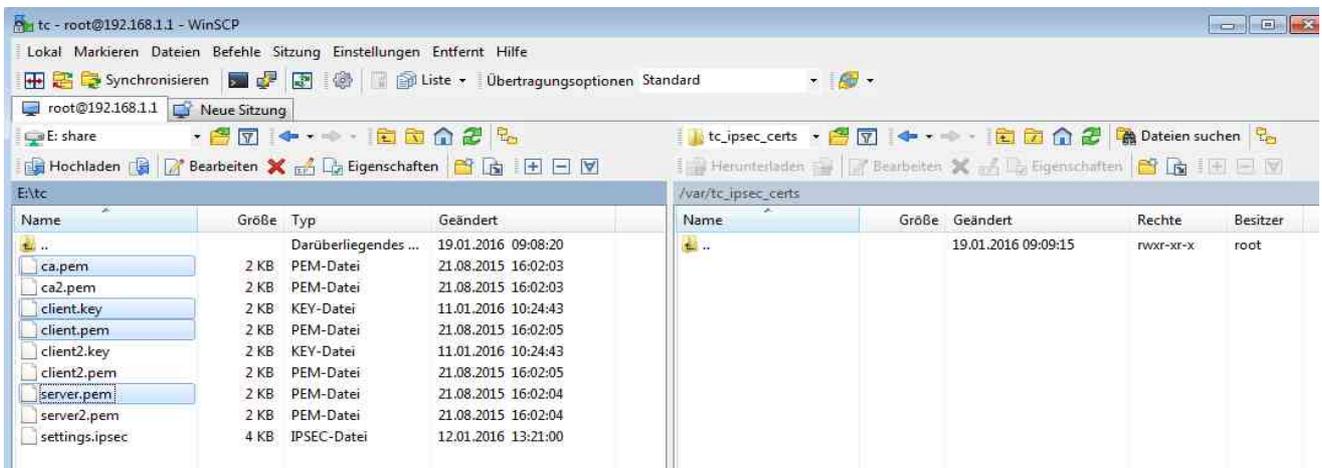
client.pem, client2.pem, client3.pem, client4.pem

Die Dateinamen ohne Index beziehen sich auf den Ipsec-Tunnel 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.



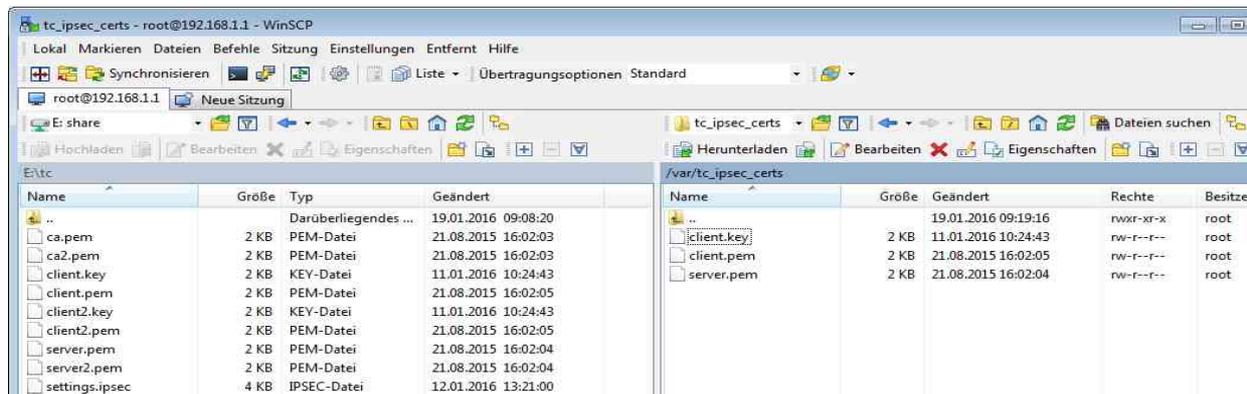
Einspielen der Daten



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

Status	Configuration
<ul style="list-style-type: none"> General Mobile WAN Network DHCP IPsec DynDNS System Log 	<pre> interface lo/lo 127.0.0.1 interface eth0/eth0 192.168.1.1 interface eth0:1/eth0:1 192.168.1.1 interface eth1/eth1 192.168.1.1 \$myid = (none) debug none "ipsec1": 192.168.1.1===192.168.1.1[C=US, O=xxx, CN=client] "ipsec1": myip=unset; hisip=unset; myup=/etc/scripts/updown; "ipsec1": CAs: 'C=US, O=xxx, CN=xxxx'...'C=US, O=xxx, CN=xxxx' "ipsec1": ike_life: 3600s; ipsec_life: 3600s; rekey_margin: 540 "ipsec1": policy: RSASIG+ENCRYPT+TUNNEL+UP; prio: 24,24; interf "ipsec1": newest ISAKMP SA: #1; newest IPsec SA: #2; "ipsec1": IKE algorithm newest: AES_CBC_128-SHA1-MODP2048 #2: "ipsec1":500 STATE_QUICK_I2 (sent QI2, IPsec SA established); #2: "ipsec1" esp.cee9290@192.168.1.1 esp.f858396b@192.168.1.1 #1: "ipsec1":500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_ </pre>

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.