

- 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-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.

	User Module	S
No user modules installed.		
New Module Durchsuche	en TC_M01.v2.tgz	Add or Update



3. Konfiguration

🗹 Enable TC_l	M01
Public Key's	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC5eRYXrhb9FV8/afimwuMZII3K2An ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAgD61zAfTAnXJz5K5OgJYgR/veyFieYy
	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 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.

	8 2
ile Key Conversions Help	
Key No key	
Actions Generate a public/private key pair	Generate
Actions Generate a public/private key pair Load an existing private key file	Generate Load
Actions Generate a public/private key pair Load an existing private key file Save the generated key Save	Generate Load Save private key
Actions Generate a public/private key pair Load an existing private key file Save the generated key Sava Parameters	Load Save private key
Actions Generate a public/private key pair Load an existing private key file Save the generated key Save Parameters Type of key to generate: © SSH-1 (RSA) © SSH-2 RSA	e public key Save private key

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

-				
r pasting into Op	oenSSH authorize	d_keys file:		
AB3NzaC1yc2E	AAAABJQAAAQE	AuDDH+jQqQ	Minute State	-
klepOc	PERSONAL PROPERTY OF A CONTRACT OF A CONTRACTACT OF A CONTRACT OF A CONTRACTACTACTACTACTACTACTACTACT	MARAGE GIVINI XILX5391	W B B B	Mz5qcy6H
DZu6aKe	Kuckgangig			CONTRACTOR OF STREET
Construction of the second sec	Ausschneiden			CHARGE COLORED
nt:	Konieren			6:e0:8e
t: ja	Einfügen			
ase:	Löschen			
phrase:				-
	Alle auswählen			
1	Rechts-nach-Lir	nks-Lesefolge		
ublic/pri	Unicode-Steuer	zeichen anzeigen		Senerate
ting privi	Unicode-Steuer	zeichen einfügen	×	Load
nerated key		Save public key	Sa	ve private key
o generate: SA)	SSH-2 RSA	SSI	1-2 DS	5A
nerated key to generate: SA) ts in a generated	SSH-2 RSA d key:	Save public key	Sa 1-2 DS	20



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

e Key Convers	ions Help	
Key		
Public key for pastin	g into Open SSH authorized_keys fi	le:
rEU/BmDBVkLvpO Ei91Y5AKcOZu6ok +LzE2c4E3X9lbxYc EBBEk1CEuxP/6B w5YSY8fW5iDaAat	om SVomOnji IEXQn P9town Eb ZxEw gxEni / Qikk+1 JLYO 00 p Sn 5Vo Gd+ QX D5t 1/n PS6m Gw4 Tufx 7zk 81e M ST 0484 Cpulkw K5Q58 Uc/S2 311 xL Gm Um Nb K13/jlw== rsa+key-201601	PBD/mBRQGZPtrik6Miz5qcy6H A 7N/W q4yOWOGZeX53GuVG7r81Kdjd e0g25Wam5kuvgV/XbcWYOw 18 ~
Key fingerprint:	ssh-rsa 2048 ff:ae:9d:0f:e7:90:6	54.fb:23:1b:c6:2d.f3:76:e0:8e
Key comment:	rsa-key-20160118	
Key passphrase:		
Confirm passphrase:		
Actions		
Generate a public/p	rivate key pair	Generate
Load an existing priv	ate key file	Load
Save the generated	key Save	public key Save private key
Parameters		14
Type of key to gene SSH-1 (RSA)	ate:	🔘 SSH-2 DSA
an a	Contracting and the second	22.40

Dateiname:	test.ppk		-
Dateityp: (PuTTY Private Key Files (*.ppk)		-
er ausblende	n	Speichern	Abbrechen



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.

💑 tc - root@192.168.1.1 -	WinSCP						Ē	
Lokal Markieren Date	ien Befehle S	itzung Einstellungen	Entfernt Hilfe					
🖶 🚝 👰 Synchronisi	eren 🔚 🧬	2 0 3 0	iste 👻 Übertragungsoptionen	Standard 👻 [9 -			
📮 root@192.168.1.1	👔 Neue Sitzuni	a .						
E: share	- 🖪 🔽 🗄	🖕 • 🔿 • 🔁 🕅	1 2 %	🔒 tc_ipsec 🔹 🗧	🛛 🔶 -		Dateien suc	hen 📴
🔒 Hochladen 👍 📝	Bearbeiten 💥	🕻 🛃 🕞 Eigenschafte	en 🚰 🚡 🛨 🖂 🗹	Herunterladen 🔐	Bearbeiten	🗶 🚮 🕞 Eigenschaft	en 🛗 🔓 19	E III 🛛
E:\tc				/var/tc_ipsec				
Name	Größe	Тур	Geändert	Name	Größe	Geändert	Rechte	Besitzer
<u>.</u>		Darüberliegendes	19.01,2016 09:08:20	<u>.</u>		19.01.2016 09:09:15	rwxr-xr-x	root
a.pem	2 KB	PEM-Datei	21.08.2015 16:02:03	settings.ipsec	4 KB	12.01.2016 13:21:00	rw-rw-rw-	root
a2.pem	2 KB	PEM-Datei	21.08.2015 16:02:03					
client.key	2 KB	KEY-Datei	11.01.2016 10:24:43					
Client.pem	2 KB	PEM-Datei	21.08.2015 16:02:05					
client2.key	2 KB	KEY-Datei	11.01.2016 10:24:43					
client2.pem	2 KB	PEM-Datei	21.08.2015 16:02:05					
server.pem	2 KB	PEM-Datei	21.08.2015 16:02:04					
server2.pem	2 KB	PEM-Datei	21.08.2015 16:02:04					
settings.ipsec	4 KB	IPSEC-Datei	12.01.2016 13:21:00					

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

눩 tc - root@192.168.1.1 -	WinSCP							
Lokal Markieren Date	ien Befehle S	itzung Einstellungen	Entfernt Hilfe					
🖶 🚝 📑 Synchronisi	eren 📰 🧬	2 0 0 0	iste 🕶 Übertragungsoption	en Standard -	- 🎯 -			
📮 root@192.168.1.1	Neue Sitzung							
💭 E: share	• 🖪 🗊 🕒	🖛 • 🔶 • 1 🔁 🕅	<u>↑ 2 %</u>	tc_ipsec_certs	• 🔗 🗑 া 🔶 •		Dateien suc	then 😤
🙀 Hochladen 🙀 📝	Bearbeiten 💥	🕻 🛃 🕞 Eigenschafte	n 🖆 🕞 🛨 🗆 💟	Herunterladen	🗐 📝 Bearbeiten	🗙 🛃 🗒 Eigenschaf	ten 📴 🔂 1	E E
E:\tc				/var/tc_ipsec_certs				
Name	Größe	Тур	Geändert	Name	Größe	Geändert	Rechte	Besitzer
a		Darüberliegendes	19.01.2016 09:08:20	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		19.01.2016 09:09:15	rwxr-xr-x	root
ca.pem	2 KB	PEM-Datei	21.08.2015 16:02:03					
ca2.pem	2 KB	PEM-Datei	21.08.2015 16:02:03					
client.key	2 KB	KEY-Datei	11.01.2016 10:24:43					
client.pem	2 KB	PEM-Datei	21.08.2015 16:02:05					
client2.key	2 KB	KEY-Datei	11.01.2016 10:24:43					
client2.pem	2 KB	PEM-Datei	21.08.2015 16:02:05					
server.pem	2 KB	PEM-Datei	21.08.2015 16:02:04					
server2.pem	2 KB	PEM-Datei	21.08.2015 16:02:04					
The second second	10.000	IDEEC Datai	12 01 2016 12:21:00					

tc - root@192.168.1.1	- WinSCP						1	- 0
Lokal Markieren Date	eien Befehle S	itzung Einstellungen	Entfernt Hilfe					
🖶 🚝 🚔 Synchronis	ieren 🛛 🗾 🧬	E @ 0 01	liste 👻 Übertragungsoptione	en Standard 🔹 🖌	<i>🚱</i> 👻			
📮 root@192.168.1.1	🗿 Neue Sitzun	9						
🕎 E: share	• 🚰 🔽 🗄	💠 • 👳 • 主 🔀	â 2 %	🔒 tc_ipsec_certs 👻 🍘	9 🔽 🔶 🕶	🔹 - 🔃 🖬 🏠 🧬	🙀 Dateien su	then 😪
Hochladen 📑 📄	Bearbeiten 🕻	🕻 🛃 🕞 Eigenschaft	en 📑 🔂 🕂 🖃 🕅	Herunterladen	2 Bearbeiten	🗙 🛒 🗟 Eigenschaf	ten 🚰 🔂 🛙	+ 🗸
E:\tc				/var/tc_ipsec_certs				
Name	Größe	Тур	Geändert	Name	Größe	Geändert	Rechte	Besitzer
₩		Darüberliegendes	19.01.2016 09:08:20	🛃		19.01.2016 09:09:15	rwxr-xr-x	root
a.pem	2 KB	PEM-Datei	21.08.2015 16:02:03	ca.pem	2 KB	21.08.2015 16:02:03	rw-rr	root
ca2.pem	2 KB	PEM-Datei	21.08.2015 16:02:03	client.key	2 KB	11.01.2016 10:24:43	rw-rr	root
Client.key	2 KB	KEY-Datei	11.01.2016 10:24:43	client.pem	2 KB	21.08.2015 16:02:05	rw-rr	root
client.pem	2 KB	PEM-Datei	21.08.2015 16:02:05	server.pem	2 KB	21.08.2015 16:02:04	rw-rr	root
client2.key	2 KB	KEY-Datei	11.01.2016 10:24:43	riste da				
client2.pem	2 KB	PEM-Datei	21.08.2015 16:02:05					
server.pem	2 KB	PEM-Datei	21.08.2015 16:02:04					
server2.pem	2 KB	PEM-Datei	21.08.2015 16:02:04					
settings.ipsec	4 KB	IPSEC-Datei	12.01.2016 13:21:00					



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



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

tc_ipsec_certs - root@	192.168.1.1 - Wi	nSCP)(0 0
Lokal Markieren Date	eien Befehle S	itzung Einstellungen	Entfernt Hilfe					
📑 🚰 🔁 Synchronisi	ieren 🛛 🗾 🧬	2 0 10	iste 🔹 🛛 Übertragungsoptioner	n Standard 👻	99 -			
💭 root@192.168.1.1	🗿 Neue Sitzun	3						
🖵 E: share	• 🥌 😨 🕛	🔶 • 🐟 • 🔀 🕅	â 2 %	🔒 tc_ipsec_certs 🔹 🐔	•	- 🖻 🖻 🏠 🌌	🕋 Dateien suo	chen 😤
Hochladen ()	Bearbeiten 🕽	👔 🚮 🔯 Eigenschafte	en 📑 🔓 🛨 🖂 🗹	Herunterladen 🙀	📝 Bearbeiten	🗙 🛃 🕞 Eigenschaft	ten 🖀 🕞 🛙	+
El\tc				/var/tc_ipsec_certs				
Name	Größe	Тур	Geändert	Name	Größe	Geändert	Rechte	Besitze
🛃		Darüberliegendes	19.01.2016 09:08:20	· · · ·		19.01.2016 09:19:16	rwxr-xr-x	root
ca.pem	2 KB	PEM-Datei	21.08.2015 16:02:03	client.key	2 KB	11.01.2016 10:24:43	rw-rr	root
ca2.pem	2 KB	PEM-Datei	21.08.2015 16:02:03	Client.pem	2 KB	21.08.2015 16:02:05	rw-rr	root
client.key	2 KB	KEY-Datei	11.01.2016 10:24:43	server.pem	2 KB	21.08.2015 16:02:04	rw-rr	root
client.pem	2 KB	PEM-Datei	21.08.2015 16:02:05					
client2.key	2 KB	KEY-Datei	11.01.2016 10:24:43					
client2.pem	2 KB	PEM-Datei	21.08.2015 16:02:05					
server.pem	2 KB	PEM-Datei	21.08.2015 16:02:04					
server2.pem	2 KB	PEM-Datei	21.08.2015 16:02:04					
settings.ipsec	4 KB	IPSEC-Datei	12.01.2016 13:21:00					

Status

- General Mobile WAN Network DHCP
- IPsec
- DynDNS
- System Log

IPsec is disabled.