Ersetzen eines S2M/S0 Anschlusses durch einen verschlüsselten VoIP Trunk mit einem innovaphone Gateway

77. DFN Betriebstagung | 19.10.2022

S. Crump, DFN Nutzer

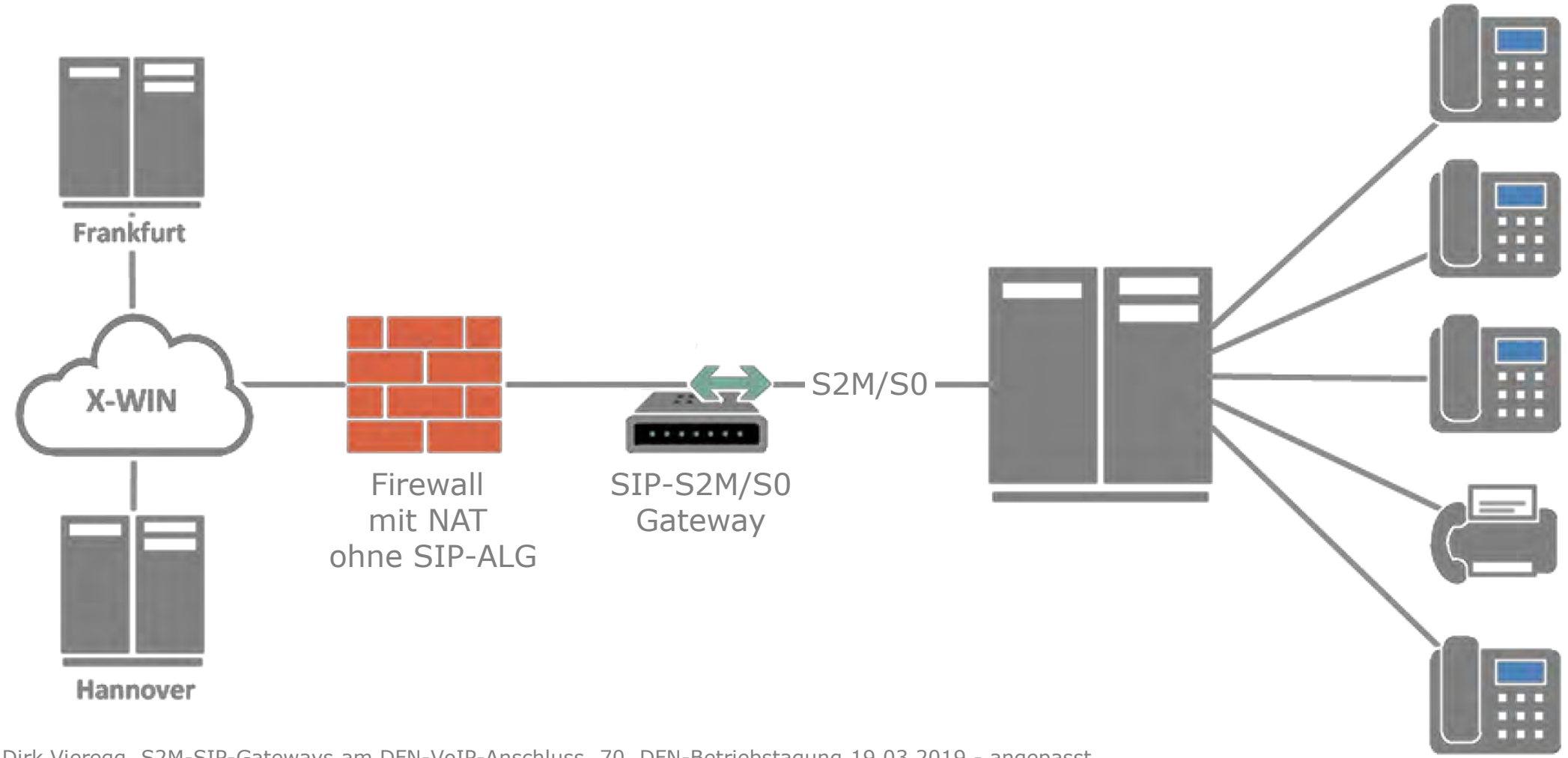
Warum ein SIP-S2M/S0 Gateway?

- **Vorhandene OpenScape 2-Draht TK Anlage** robust und ausreichend
- Weitestgehende **Trennung von TK und IT erwünscht**
- **Kostengünstiger und nachhaltiger** gegenüber einem Ersatz der vorhandenen Infrastruktur durch eine neue originäre VoIP Infrastruktur

Interne Basisanforderungen

- **Firewall mit NAT vor SIP-S2M/S0 Gateway**
- Aktuelle **Verschlüsselung mit TLS/sRTP**
- Fax, Frankit und Wählgeräte (D-/B-Kanal, DTMF) müssen weiter funktionieren

Aufbau



Quelle: Dirk Vieregg, S2M-SIP-Gateways am DFN-VoIP-Anschluss, 70. DFN-Betriebstagung 19.03.2019 - angepasst

Ablauf der VoIP Umstellung

- **15.02.2021: Anbieter kündigt die vorhandenen ISDN Anschlüsse**
- 29.03.2021: Auftrag für **ersten verschlüsselten SIP-Trunk**
- 12.04.2021: Bereitstellung Testnummern erster Trunk
- 01.06.2021: Beginn der Inbetriebnahme des IP811 Gateways
- 18.07.2021: erfolgreicher Abnahmetest erster Trunk
- 14.09.2021: Rufnummernportierung **erster Trunk**
- 05.08.2021: Auftrag für **zweiten verschlüsselten SIP-Trunk**
- 03.09.2021: Bereitstellung Testnummern zweiter Trunk
- 14.09.2021: Beginn der Inbetriebnahme des IP3011 Gateways
- 06.10.2021: erfolgreicher Abnahmetest zweiter Trunk
- **24.11.2021: Rufnummernportierung zweiter Trunk**

fast 6 Monate

weniger als 4 Monate

3 Wochen

innovaphone IP811 / IP3011 Gateways

- **https://www.innovaphone.com** (Sindelfingen) mit vielen technischen Details unter https://wiki.innovaphone.com/
- verschiedene Gateways verfügbar (bis 5x S0, bis 2x S2M), beliebig kaskadierbar
- IP811 / IP3011, Firmware ≥13r2
  - 5x BRI (S0) / 1x PRI (S2M)
  - 2x LAN
  - PBX uvm. integriert, hier aber nicht genutzt,
    theoretisch sanfte Migration einzelner Teilnehmer von TK Anlage auf VoIP möglich via PBX
- Lizenzerwerb für BRI / PRI, pro Kanal usw. notwendig
- Georedundanz
- **responsiver Support** über viele Fachhändler, z.B. hier eine Firmwareanpassung innerhalb 5 Tagen
- TLS 1.2 wie benötigt unterstützt (und auch schon TLS 1.3)
- **gutes Tracing** z.B. der verschlüsselten Kommunikation über Wireshark rpcap://nnn.nnn.nnn.nnn/trace
- **Les- & editierbare Konfigurationsdateien**, bislang nie Probleme bei Firmwareupdate, „Reboot When Idle" möglich
- GWs unterstützen Silent Suppression, Trunk aber nicht (wird nicht genutzt, aber könnte per /rem-silence-sup abgeschaltet werden)
- erfüllen alle Anforderungen des DFN-Fernsprechen T-Systems Corporate SIP Germany

Von der Beauftragung zum Abnahmetest (1/2)

- Nach Beauftragung (entgeltpflichtig verschlüsselt, Audio-Codec ausschließlich G.711a, kein T.38 o.a.!) wird in 2-4 Wochen ein Trunk mit 10 Testrufnummern eingerichtet
- dfn_PRE-Test-*_Checkliste.docx
  ist nach interner Einrichtung abzuarbeiten und an T-Systems zu retournieren
- Terminvereinbarung für Abnahmetest benötigt ca. 1-2 Wochen Vorlaufzeit
- *«Der Acceptance Tests beinhaltet die Durchführung einer Reihe von einzelnen Testcases entsprechend des beigefügten Protokoll Templates.»*
- *«Die Dauer dieses Acceptance Tests beträgt im besten Fall 3-4 Stunden. Wenn Probleme auftreten verlängert sich die Dauer entsprechend der Dauer der Problemlösung. Wir planen deshalb in der Regel die Zeit von 9–16 Uhr für die Testdurchführung.»*

Von der Beauftragung zum Abnahmetest (2/2)

- empfohlene Hardware
  - zwei Telefone (intern)
  - zwei Handys
  - zwei Faxgeräte (intern / extern)
- Bedienung von Telefon und Handy sollte klar sein
  - Halten
  - 3er-Konferenz
  - Rufumleitung
  - Rufnummernunterdrückung
- Verbindung zu den einzelnen SIP Trunk Peers muss kurzfristig trennbar sein im Gateway oder in der Firewall, um die Georedundanz checken zu können

Nach dem Abnahmetest

- Abnahmetestdokumentation 1-3 Tagen nach Test erhalten
- Rufnummernportierung dann nach frühestens 34 Werktagen möglich
- Rufnummernportierung kann schiefgehen:

  Einmal hat der alte Anbieter das neue Routing zunächst nicht veröffentlicht

  ⇒ wir waren nur innerhalb des Telekom-Netzes erreichbar

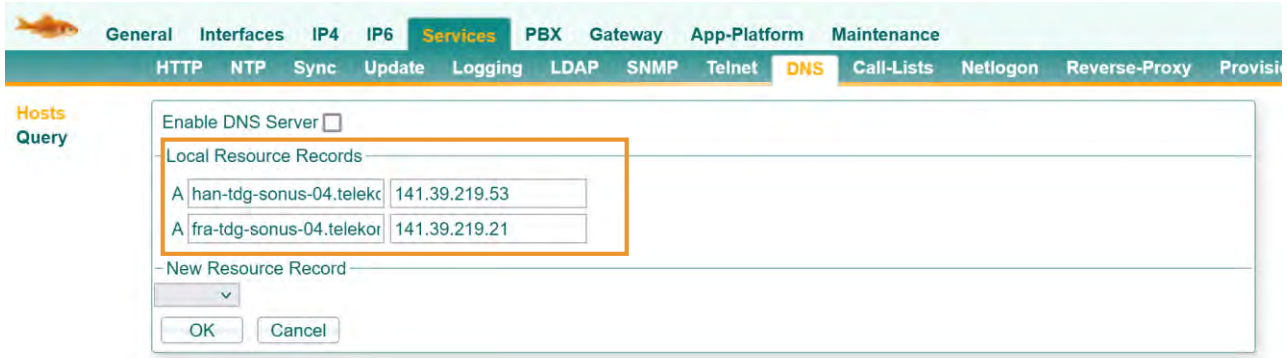
  ⇒ Telekom musste dem alten Anbieter eine **Portierungsstörung** melden

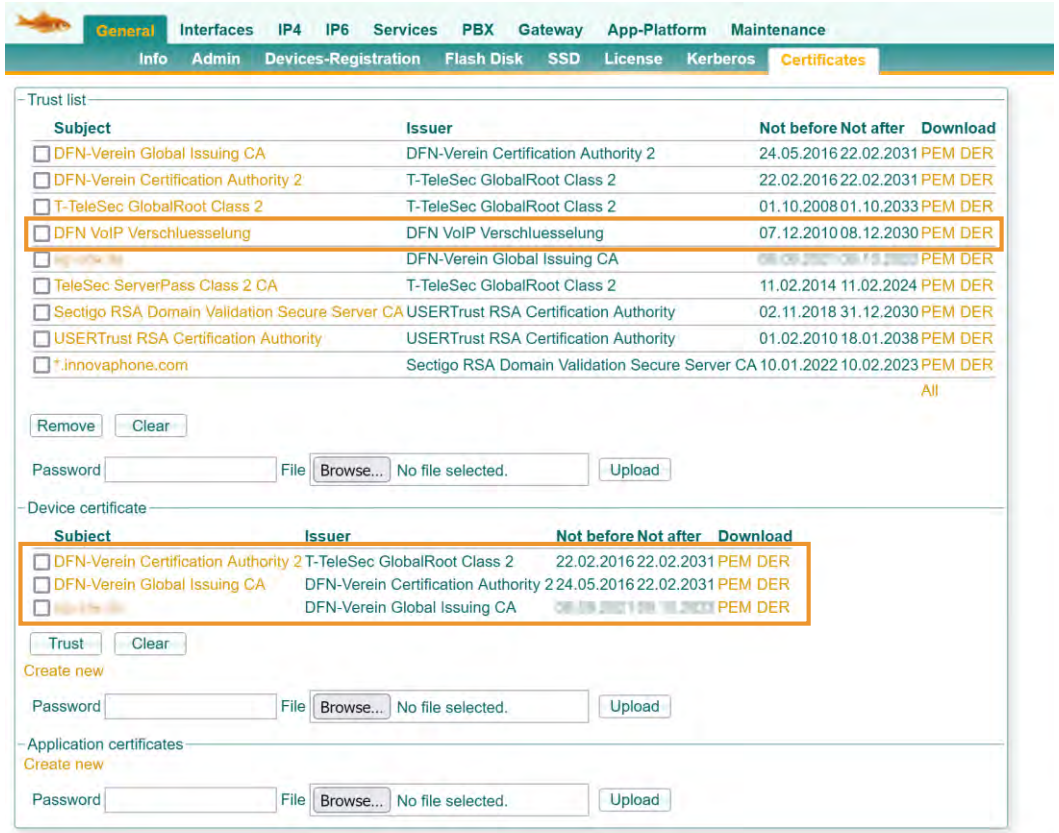
  ⇒ 2 Tage nur eingeschränkt erreichbar

Konfig: Zertifikate

- Serverzertifikate sind ausgestellt auf „han-tdg-sonus-04.telekom.de“ bzw. „fra-tdg-sonus-04.telekom.de“, haben aber keine öffentliche DNS Einträge

⇒ lokaler DNS / hosts Eintrag notwendig
ansonsten akzeptiert das Gateway die Verbindung nicht

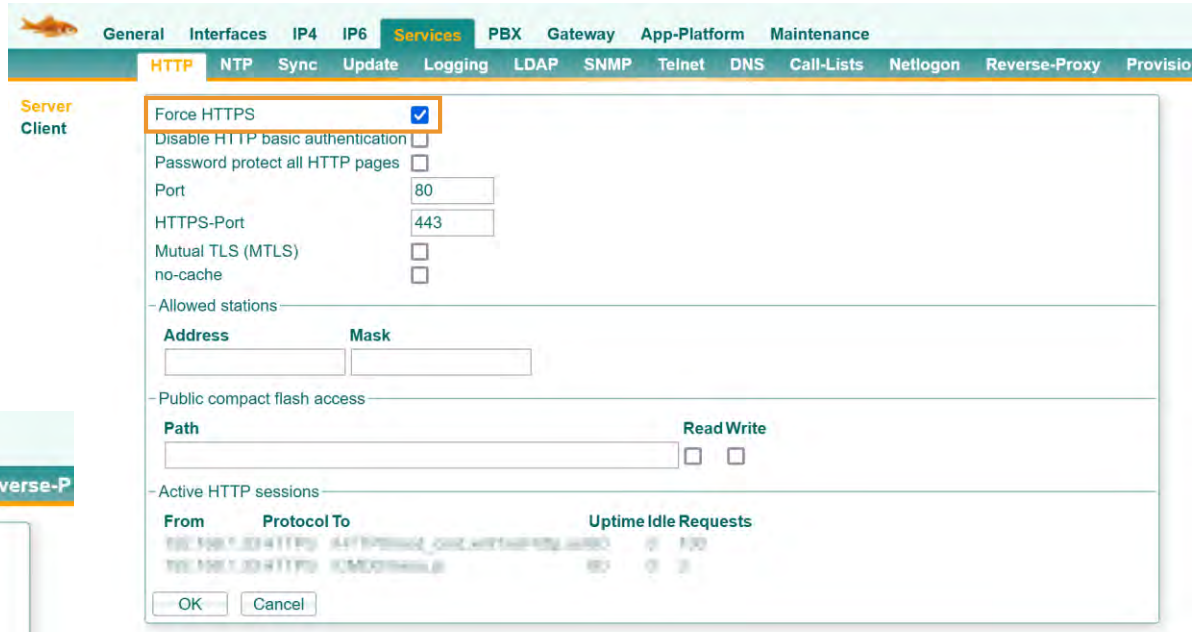


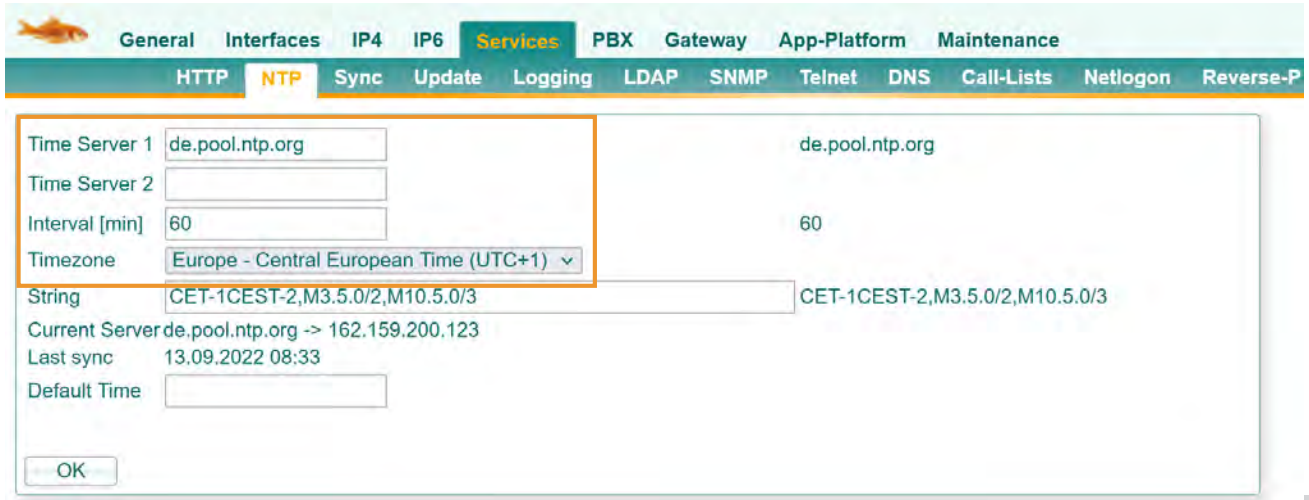


- Dem Wurzelzertifikat des Trunks unter „DFN VoIP“ https://doku.tid.dfn.de/de:dfnpki:dfnpki_root_certs muss vertraut werden
- Ein eigenes Server-Zertifikat der DFN-PKI mit dem Zertifikatsprofil „VoIP-Server“ muss beantragt, eingerichtet (komplette Kette) und vertraut werden

Konfig: Ein paar Basiseinstellungen

- Admin Zugang absichern / anlegen unter General > Admin
- HTTPS für Zugang erzwingen
- NTP einrichten



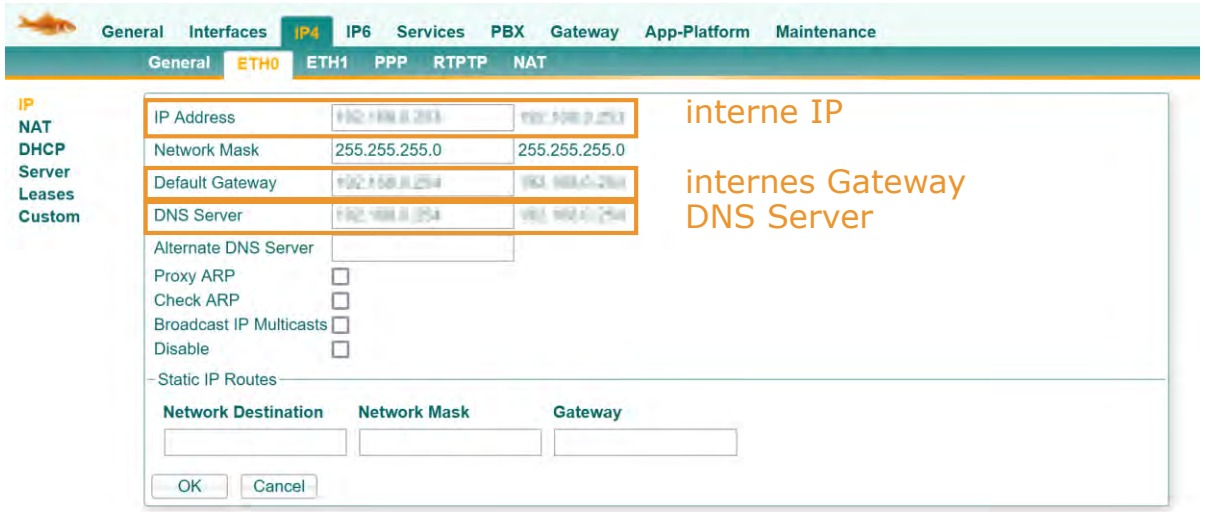


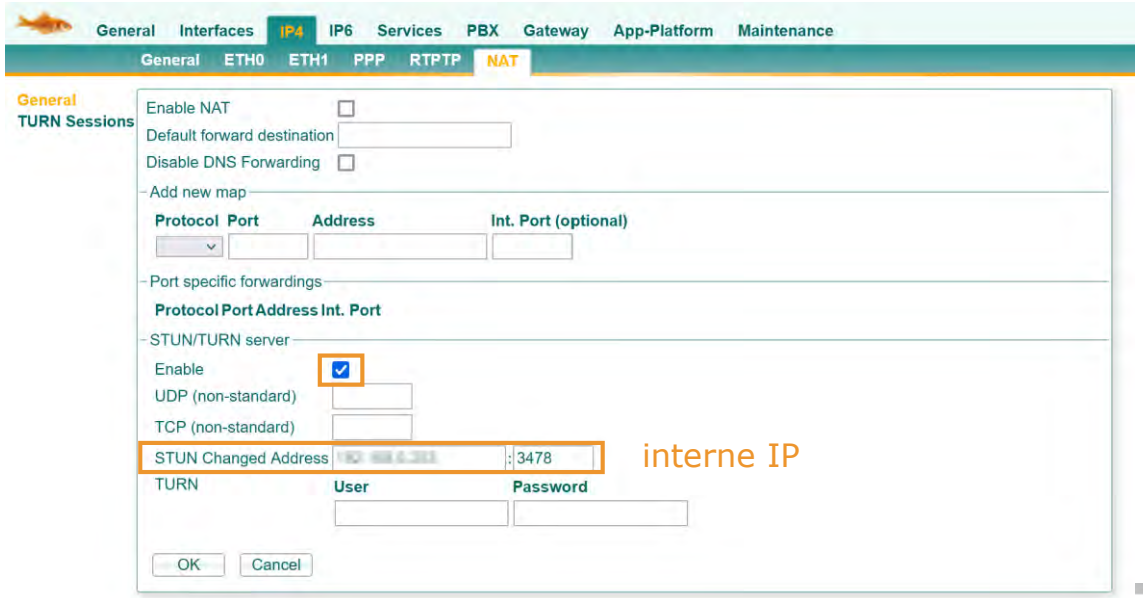
Konfig: Betrieb hinter Firewall mit STUN Server & NAT

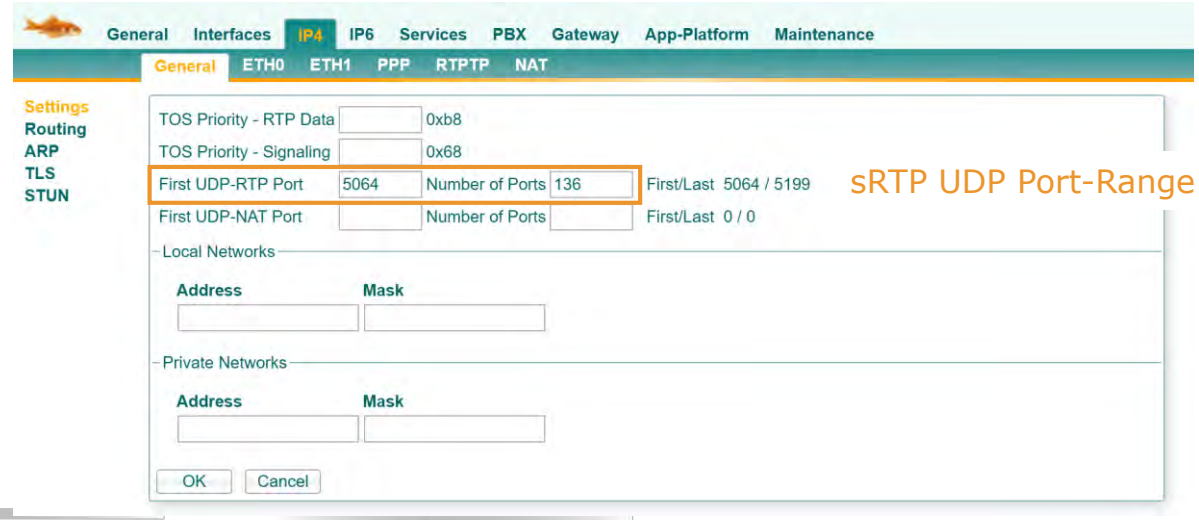
Firewall Konfiguration:

- 1:1 NAT öffentliche SIP IP > interne IP
- SIP-ALG ausschalten!
- Firewall blockiert von außen alles außer:
  - TLS Signaling TCP/UDP von 1024-65535 an 5061
  - STUN Abfrage TCP/UDP von 1024-65535 an 3478

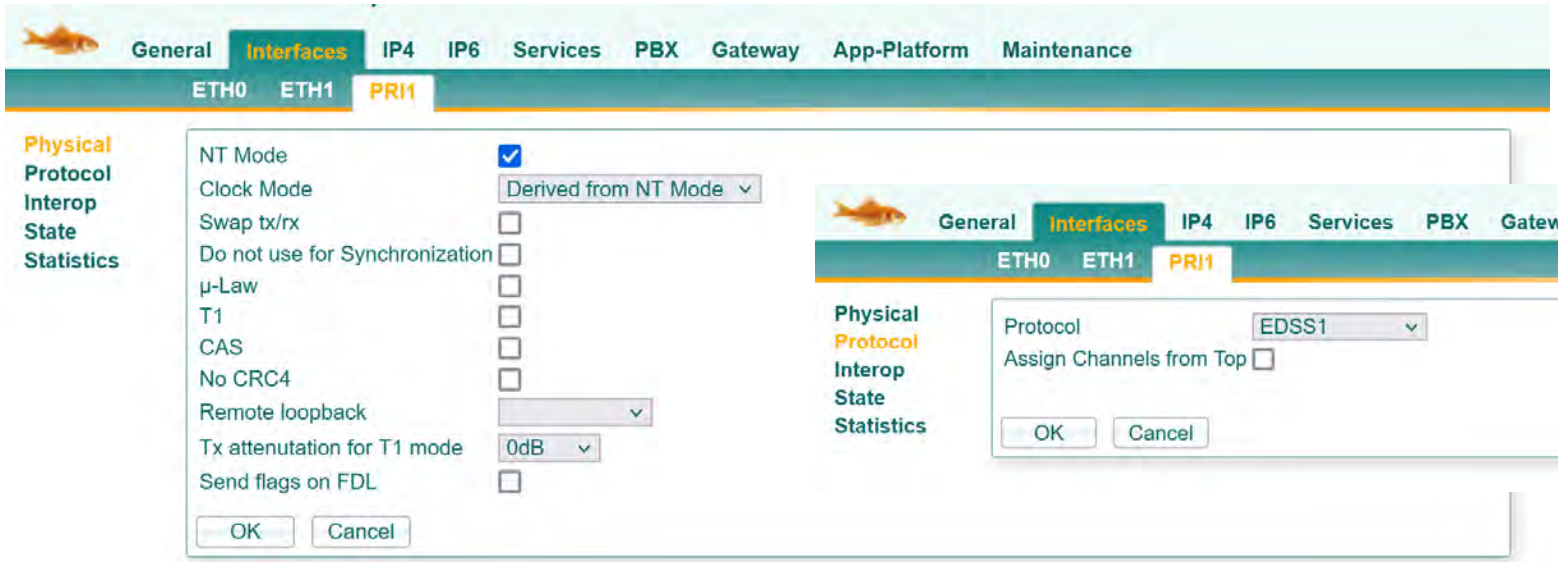
vom T-Systems Trunk, also
141.39.219.53 (Han) und 141.39.219.21 (Fra)

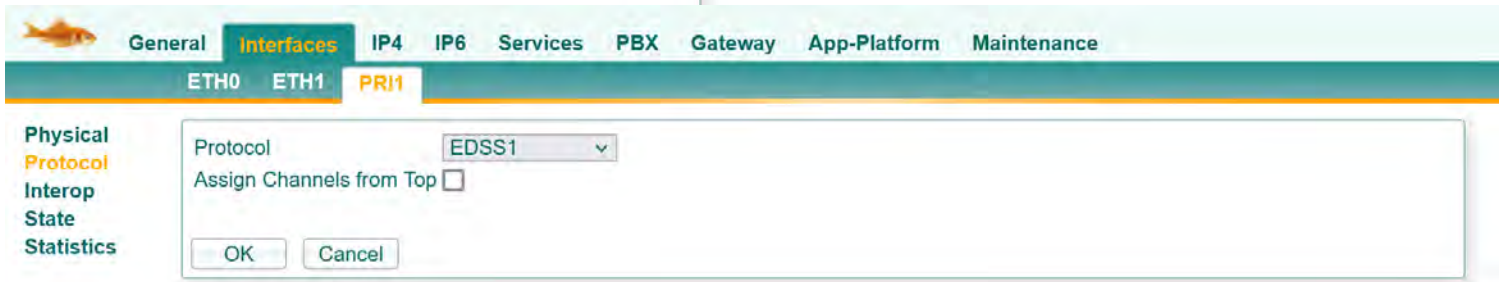


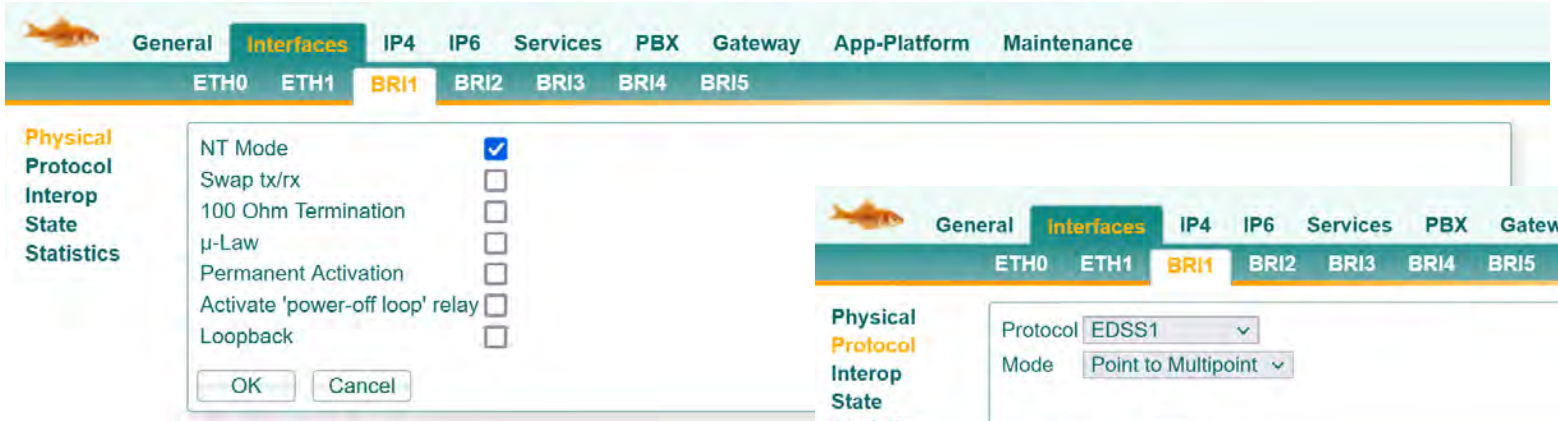


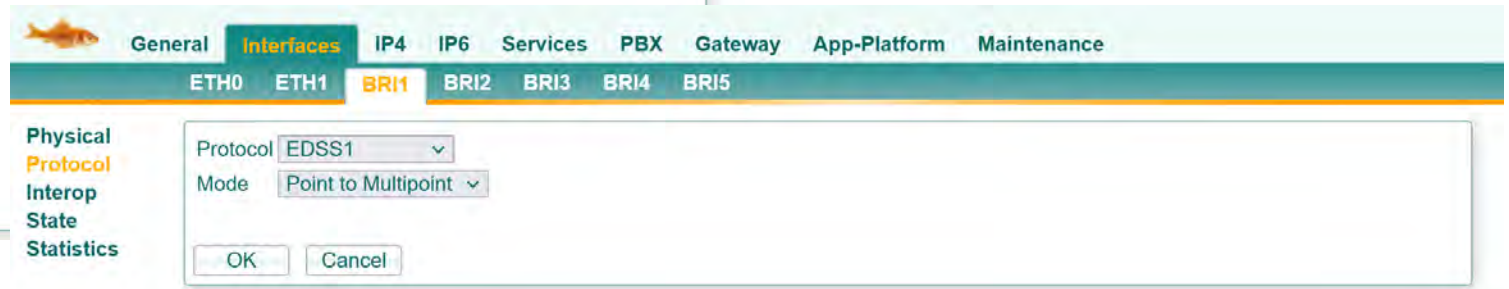


Konfig: Interfaces PRI (S2M) / BRI (S0)

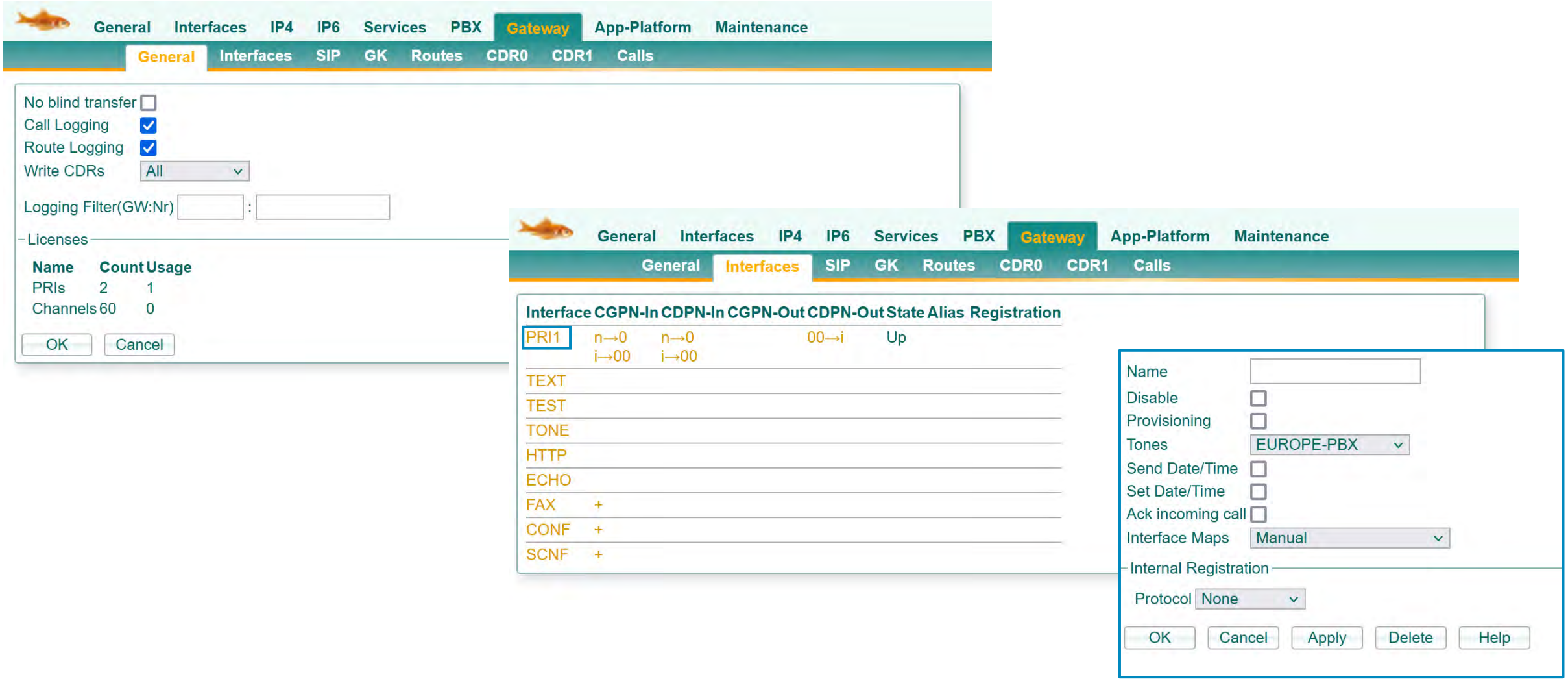




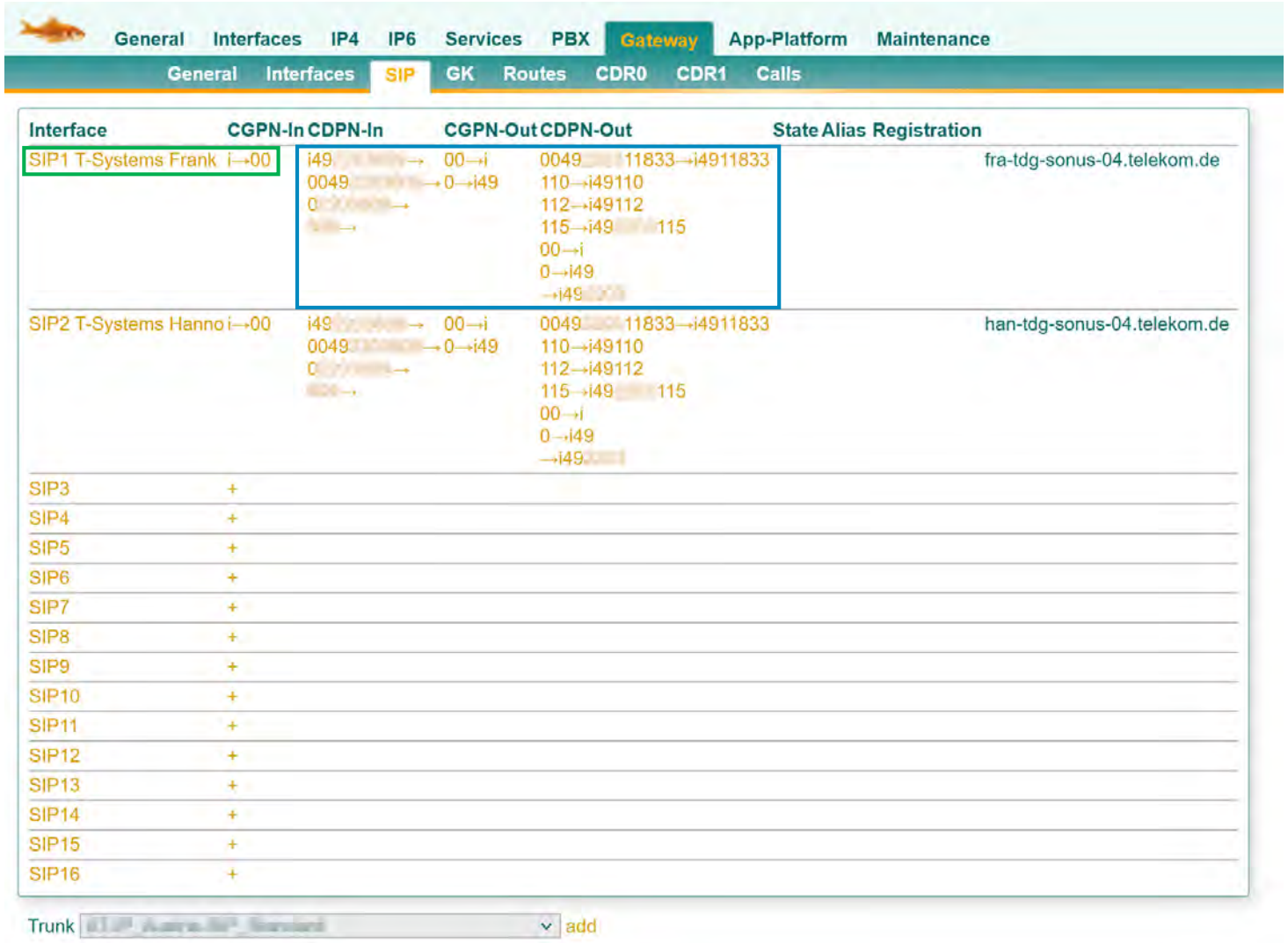


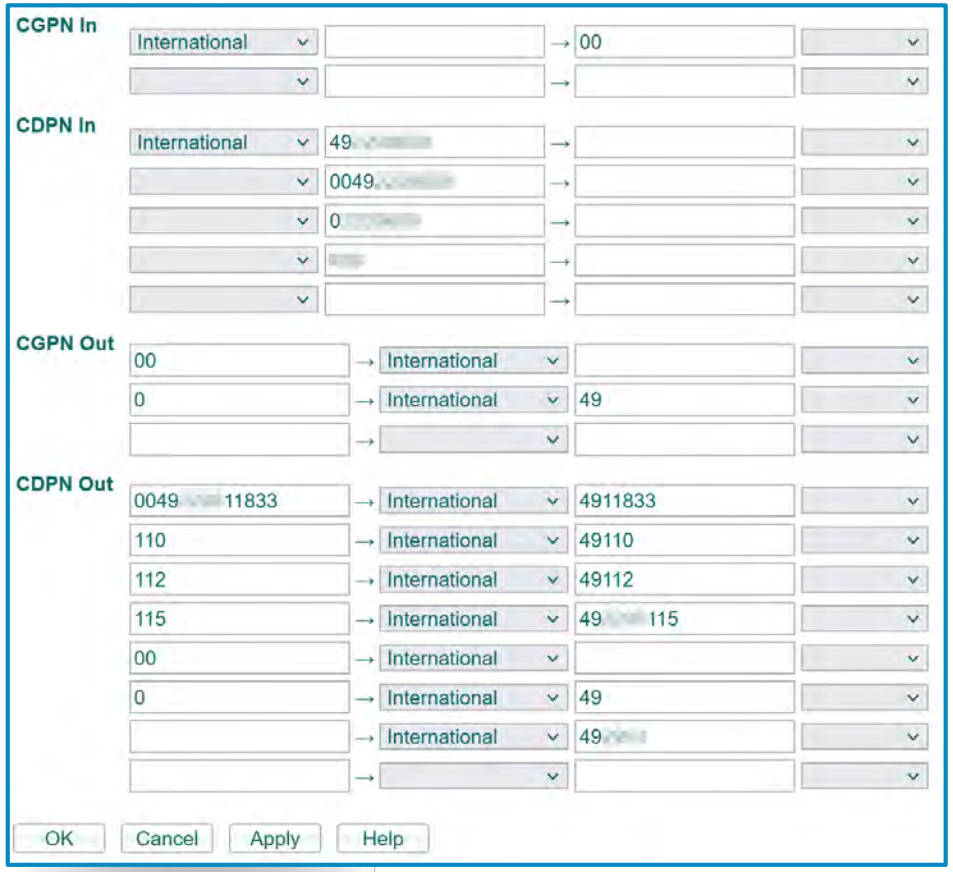


Konfig: Gateway > General / Interfaces

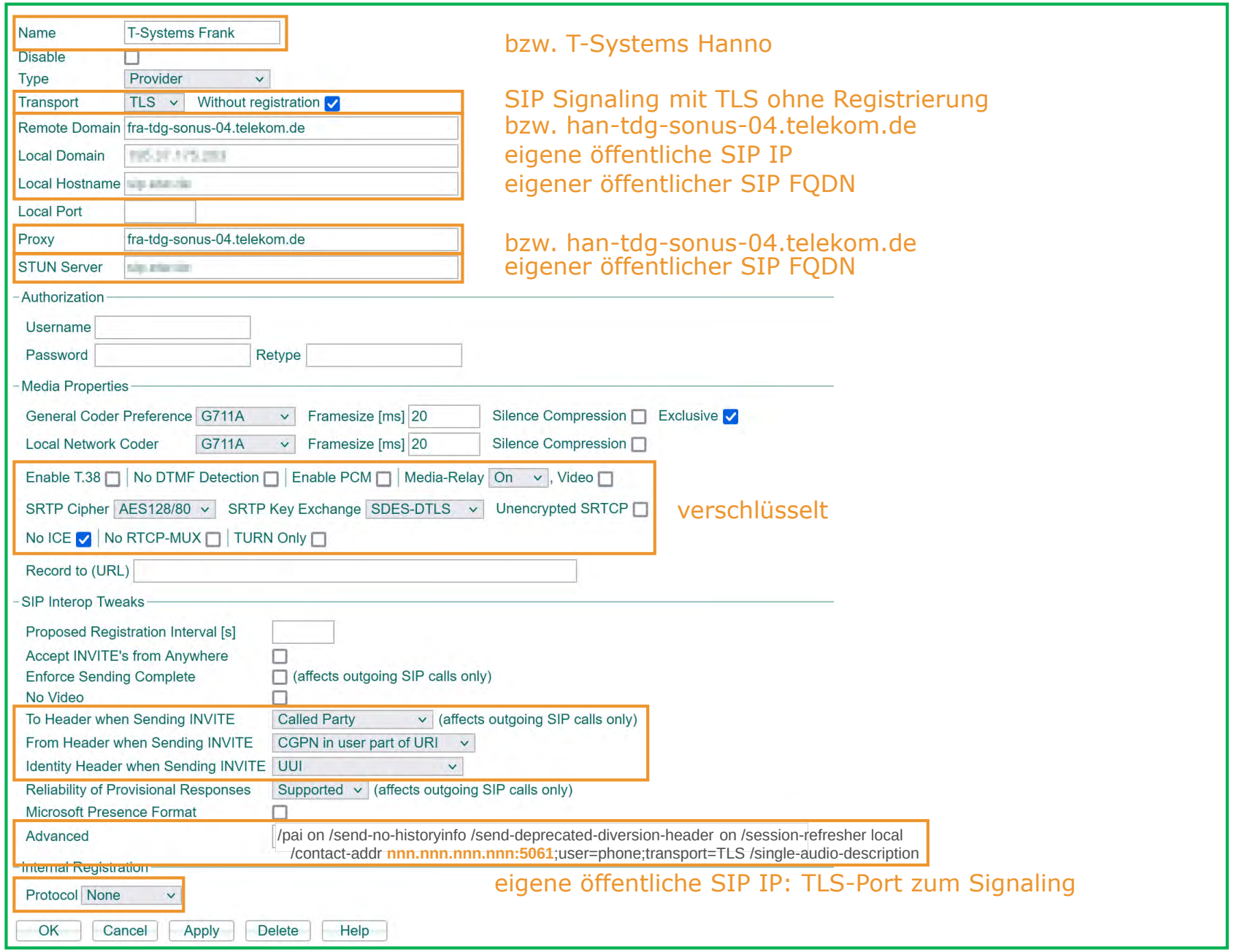


Konfig: Gateway > SIP

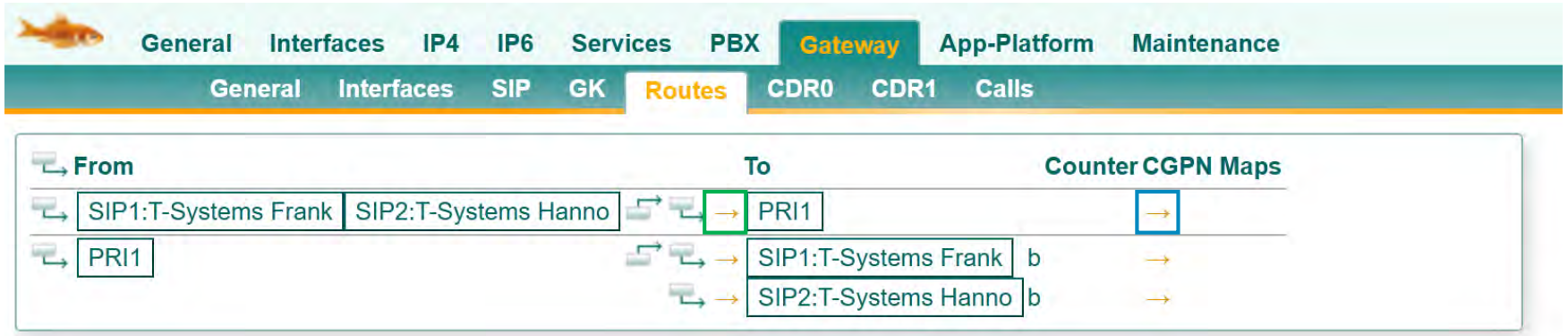


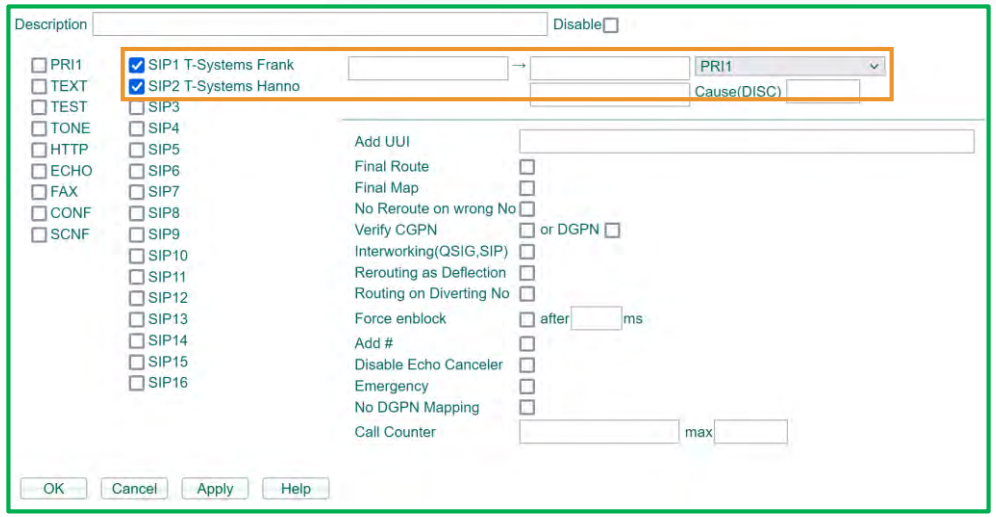


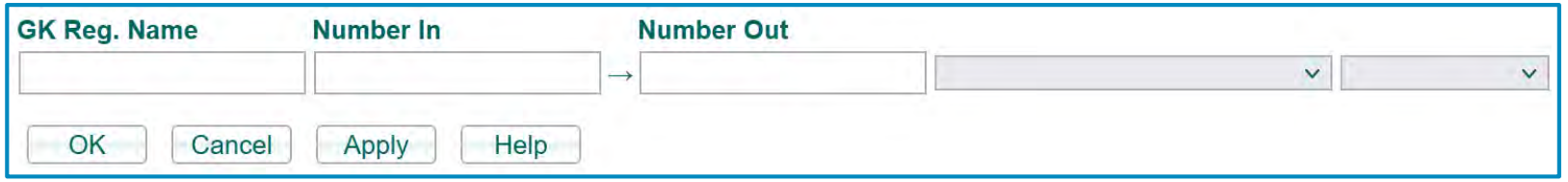
Konfig: Gateway > SIP > Interface



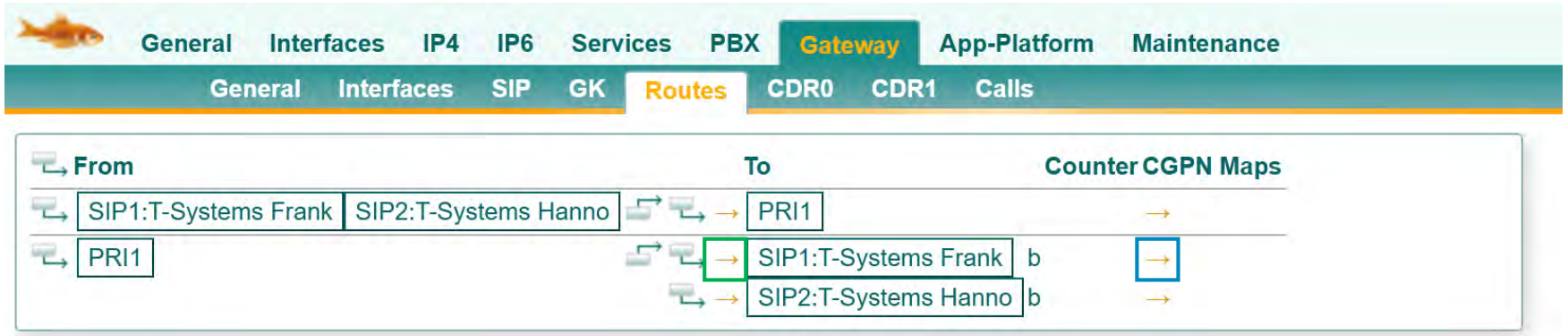
Konfig: Gateway > Routes

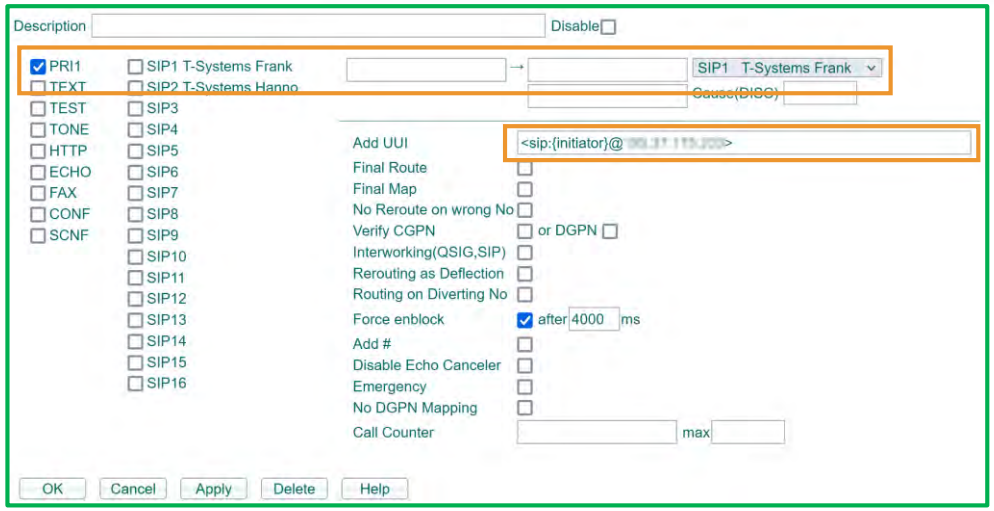






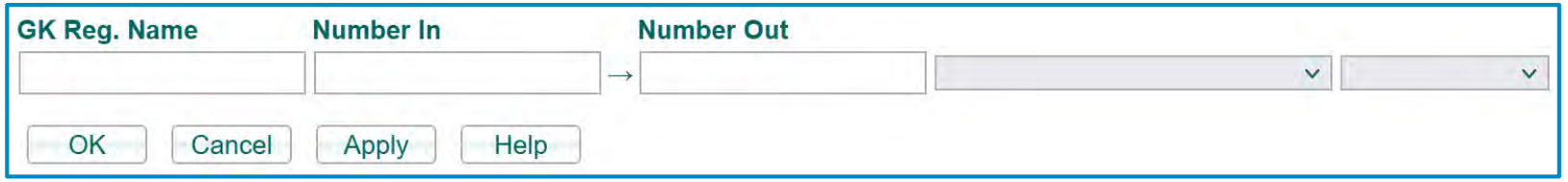
Konfig: Gateway > Routes





bzw. T-Systems Hanno

eigene öffentliche SIP IP



Zusammenfassung

IP811 / IP3011 überzeugen als verlässliche SIP-S0/S2M Gateways mit gutem Support:

- Bisher stets problemlose Aktualisierung auf neue Firmware
- Telefon, Fax und Frankit funktionierten ad hoc
- Wählgeräte mit D-Kanal Euro-ISDN (DSS1) X.31 und B-Kanal HDLC X.75 SLP transparent funktionierte ebenfalls ad hoc, aber Protokolle gehören *«nicht zum versprochenen Produkt(-umfang) DFN-C.SIP.G. (…) keinen Support (…) Es ist möglich, dass die Protokolle bei einem Update seitens der Deutsche Telekom-Plattform C.SIP.G. nicht mehr funktionieren.»*
- Wählgeräte mit DTMF funktionieren seit einem Firmware Update des Wählgeräteherstellers, durch das die Steuergeräte nun auf Rückantworten etwas länger wartet
- Bereits eingebaute Unified Communications Funktionen wie PBX, myApps bieten Skalierbarkeit

Einen großen Dank an die tolle Unterstützung von DFNFernsprechen, innovaphone, Telekom & T-Systems – man steht nicht einsam vor Hürden, auch wenn man mitdenken muss …

Wunsch an DFN & innovaphone: «Automatic Certificate Management Environment (ACME)»

Nützliche Abkürzungen

STUN	Session Traversal Utilities for NAT
TLS	Transport Layer Security
sSIP	secure Session Initiation Protocol
sRTP	secure Real-Time Transport Protocol
SIP-ALG	SIP Application Layer Gateway
DTMF	Dual Tone Multi-Frequency, Mehrfrequenzwahlverfahren (MFV)
PBX	Private Branche Exchange, Telefonanlage