Leitfaden zum Absichern der VoIP-Funktionalität von LANCOM Routern gegen Angriffe aus dem WAN

Beschreibung:

Netzwerk-Komponenten wie z.B. Router, welche direkt über das Internet (WAN) erreicht werden können, sind täglich das Ziel von Angriffen. Auch LANCOM Router bilden diesbezüglich keine Ausnahme.

Neben Versuchen, Zugriff auf die Konfiguration des Gerätes zur erlangen oder die Kommunikation des Gerätes selber sowie nachgelagerter Geräte zu überwachen oder zu manipulieren, kommt es zu Angriffen auf die VoIP-Funktionalität von Routern.

Angreifer aus dem Internet versuchen Telefonate zu initiieren. Hierbei handelt es sich häufig um Auslandsverbindungen und Sonderdienste, welche zu finanziellen Schäden beim Betreiber des Routers führen können.

Wird die Telefonie auf einem LANCOM Router über den Setup-Assistenten eingerichtet, werden automatisch die erforderlichen Einstellungen gesetzt, damit dieser gegen solche Angriffe abgesichert ist.

Wird die Telefonie manuell eingerichtet, sollte das in Kapitel 1 beschriebene Feature von Hand aktiviert werden.

Die in Kapitel 2 erwähnten Features sollten zusätzlich angepasst werden, um die Sicherheit weiter zu erhöhen. Diese werden aber nicht von jedem SIP-Provider sowie in jedem Tarif unterstützt bzw. können nicht in jedem Szenario verwendet werden. LANCOM Systems empfiehlt daher im Vorfeld Kontakt zu dem verwendeten SIP-Provider aufzunehmen.

Dieser Artikel beschreibt welche Einstellungen erforderlich sind, um die VoIP-Funktionalität eines LANCOM Routers gegen Angriffe aus dem Internet abzusichern.

Voraussetzungen:

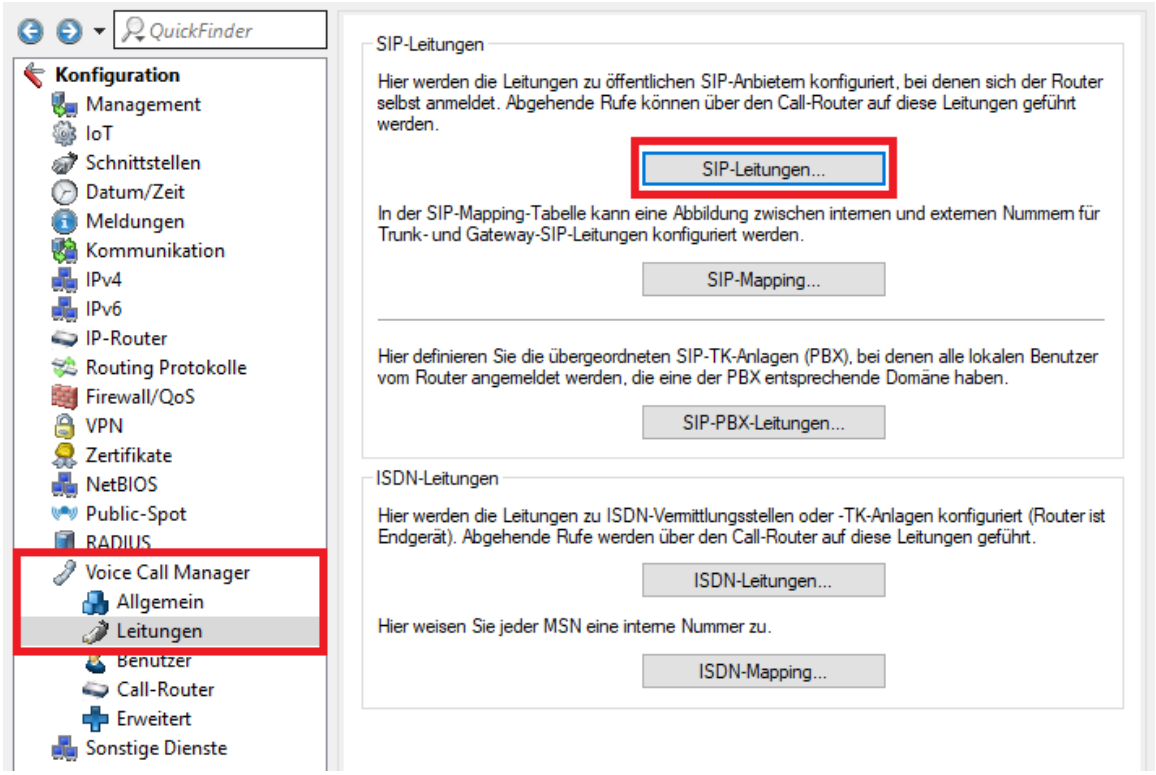
- LCOS ab Version 10.00 (download aktuelle Version)
- LANconfig ab Version 10.00 (download aktuelle Version)
- LANCOM VoIP-Router und LANCOM Router mit aktiver All-IP Option

Info:
Bei Routern mit einer LCOS-Version bis einschließlich 9.0 kann lediglich die Anmeldung von SIP-Benutzern aus dem Internet (WAN) unterbunden werden.

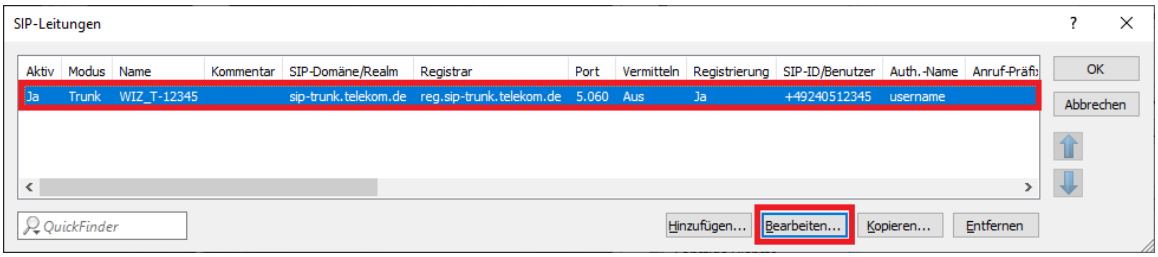
Vorgehensweise:

1. Zwingende Sicherheits-Einstellung bei manueller Konfiguration einer SIP-Leitung:

1.1 Öffnen Sie die Konfiguration des Routers in LANconfig und wechseln in das Menü **Voice Call Manager -> Leitungen -> SIP-Leitungen**.



1.2 Bearbeiten Sie die SIP-Leitung und wechseln in den Reiter **Sicherheit**.

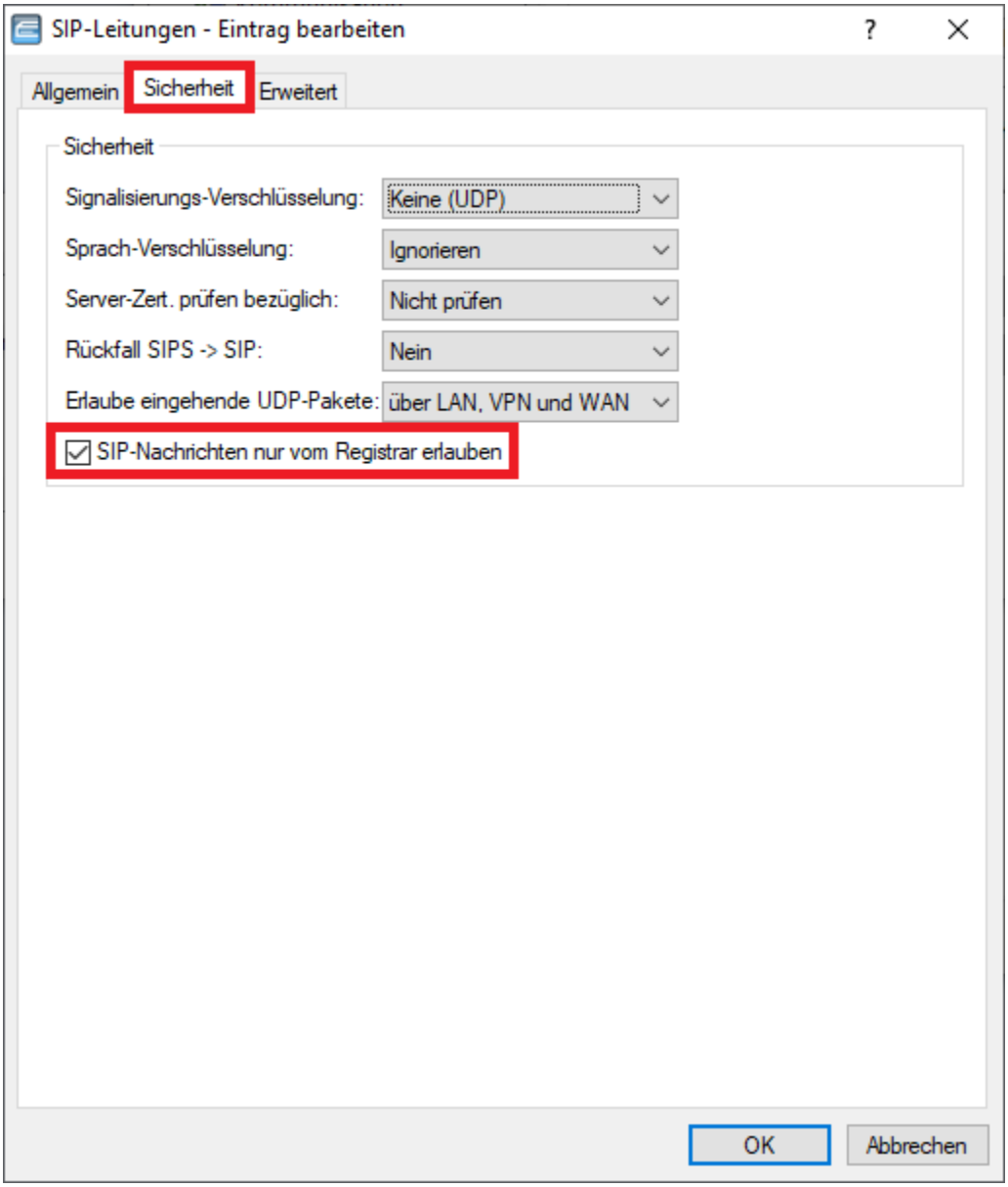


1.3 Stellen Sie sicher, dass der Haken bei **SIP-Nachrichten nur vom Registrar erlauben** gesetzt ist.

Ist diese Funktion aktiviert, werden eingehende Pakete nur vom Registrar erlaubt (in der Regel der SIP-Provider). Pakete aus anderen Quellen werden verworfen.

LANCOM Systems empfiehlt diese Funktion aus Sicherheitsgründen immer zu aktivieren.

Bei Ausführung des Setup-Assistenten für die Telefonie wird diese Funktion automatisch aktiviert.



2. Zusätzliche Einstellungen zur Erhöhung des Sicherheitsgrades:

Diese Einstellungen erhöhen die Sicherheit zusätzlich, werden aber nicht von jedem SIP-Provider oder in jedem Tarif unterstützt bzw. können nicht in jedem Szenario verwendet werden. Wenden Sie sich dazu gegebenenfalls an Ihren SIP-Provider.

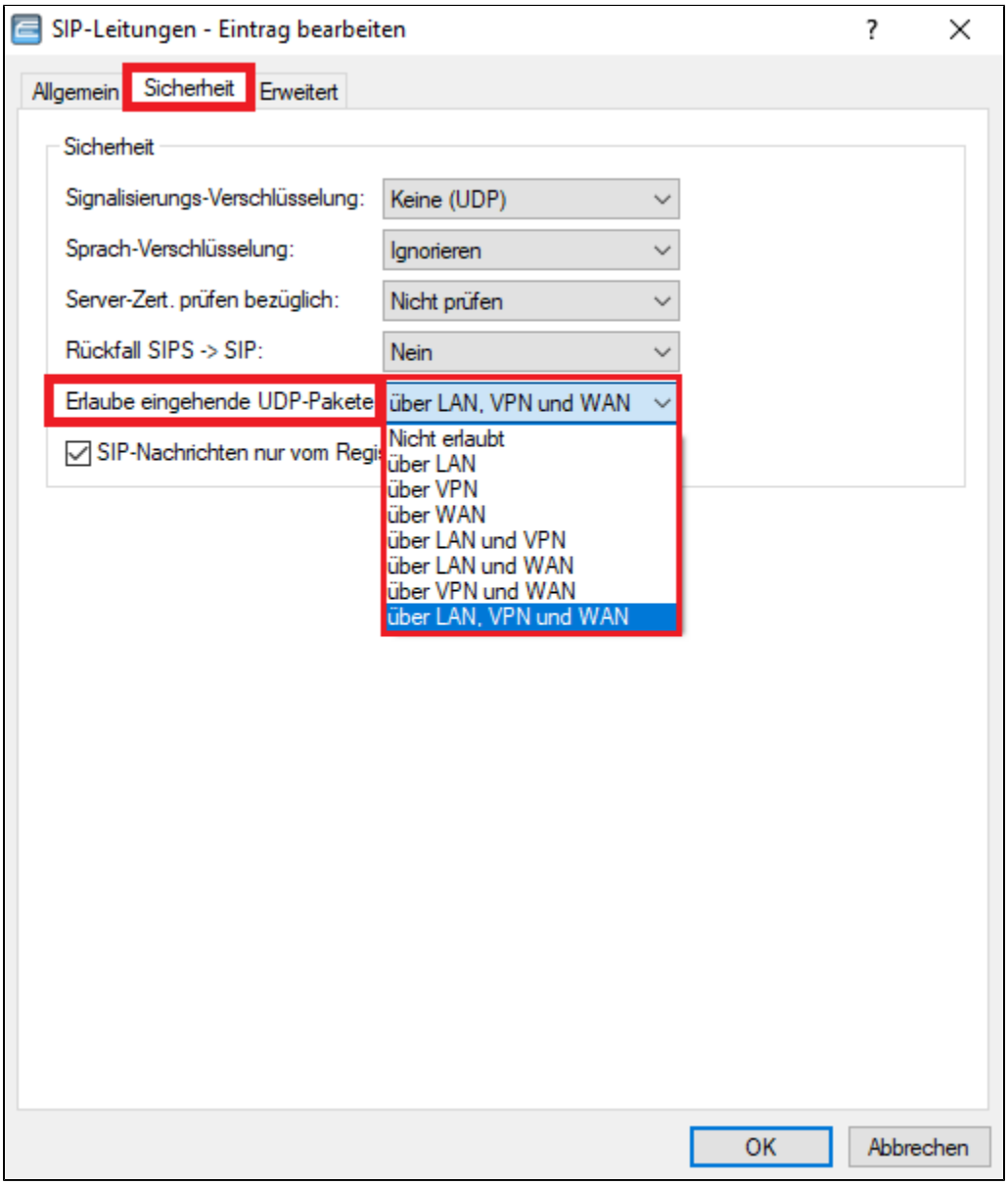
2.1 Erlaube eingehende UDP-Pakete:

Diese Funktion steuert, von welchen Schnittstellen eingehende UDP-Pakete angenommen werden.

Besteht eine **SIP-Leitung zu einem SIP-Provider im Internet**, müssen **UDP-Pakete aus dem WAN erlaubt** sein.

Besteht eine **SIP-Leitung zu einer SIP-TK-Anlage im lokalen Netzwerk des VoIP-Routers**, ist es empfehlenswert diese Funktion auf **über LAN** oder **über LAN und VPN** einzuschränken und somit **aus dem WAN zu verbieten**.

> **Wichtig:**
> Wird die **Signalisierungs-Verschlüsselung** (siehe **Schritt 2.2**) auf **Keine (TCP)** oder **TLS 1.x** gestellt, hat diese Funktion keine Auswirkung.

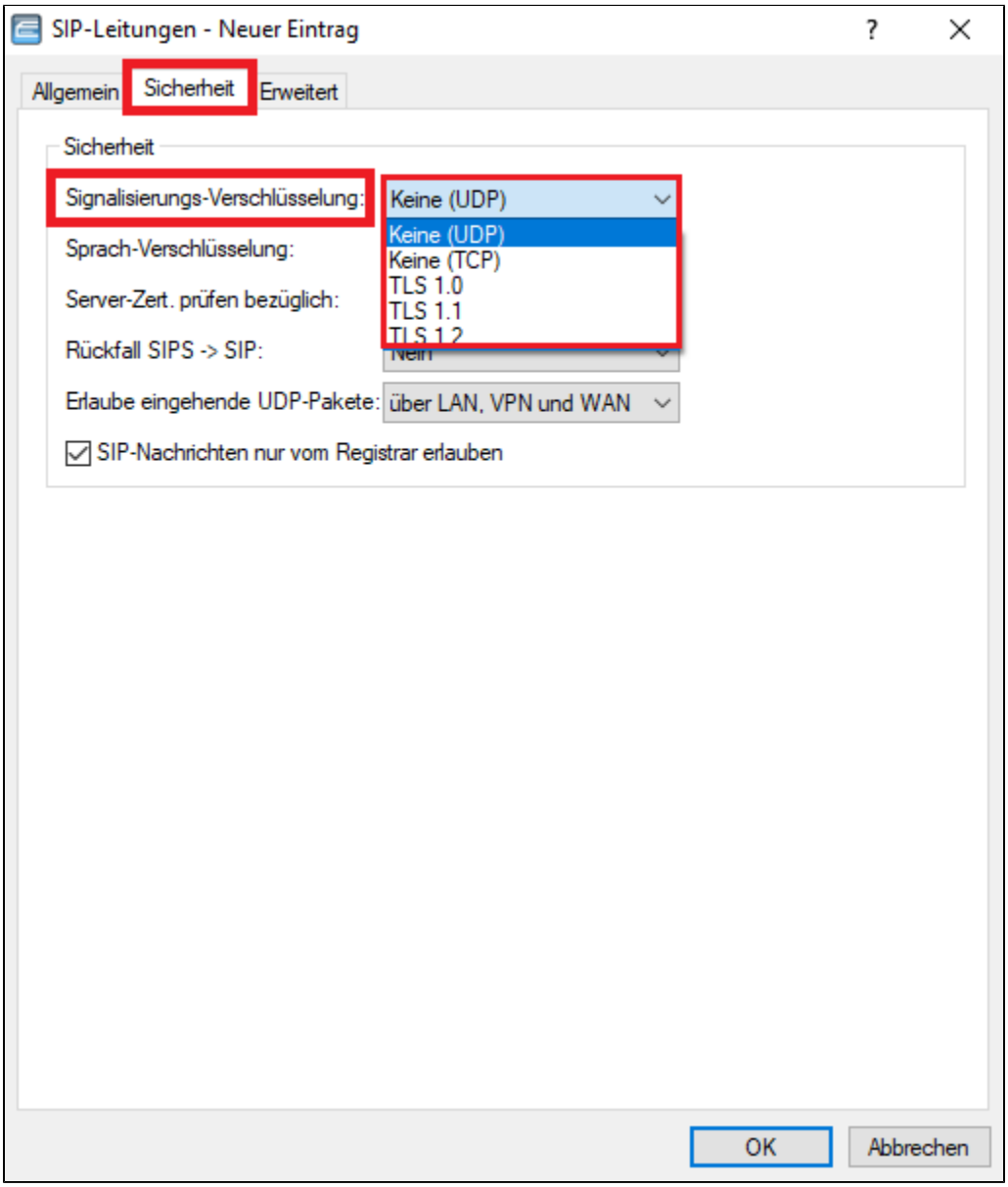


2.2 Signalisierungs-Verschlüsselung:

Bei Setzen der Funktion auf **Keine (UDP)** erfolgt die Ruf-Signalisierung über das **verbindungslose** Protokoll **UDP**. Eine Signalisierung kann dadurch von einer beliebigen Quelle erfolgen. Dies muss daher anderweitig verhindert werden (siehe **Schritt 1.3** und gegebenenfalls **2.1**).

Bei Setzen der Funktion auf **Keine (TCP)** erfolgt die Ruf-Signalisierung über das **verbindungsorientierte** Protokoll **TCP**. Es wird bei der Registrierung eine **TCP-Verbindung** zum SIP-Provider aufgebaut, welche für die Dauer der Registrierung aufrecht erhalten bleibt. Dadurch kann die Signalisierung nur vom SIP-Provider erfolgen (außer durch Man-in-the-Middle Attacken) und bietet daher gegenüber der **Signalisierung per UDP** einen **weiteren Sicherheitszugewinn**. In der Regel wird eine **TCP-Verbindung** nur bei einem **SIP-Trunk** unterstützt.

Bei Setzen der Funktion auf **TLS 1.x** wird ebenfalls eine **TCP-Verbindung** zum SIP-Provider aufgebaut. Zusätzlich wird die **Kommunikation zum SIP-Provider verschlüsselt**. Die Signalisierung kann nur durch den SIP-Provider erfolgen, außer durch Man-in-the-Middle Attacken, bei denen der Angreifer zusätzlich ein gefälschtes Zertifikat bei dem Angriffsziel einschleust. Diese Option bietet gegenüber der **Signalisierung per TCP** einen **weiteren Sicherheitszugewinn**.



2.3 Server-Zert. prüfen bezüglich:

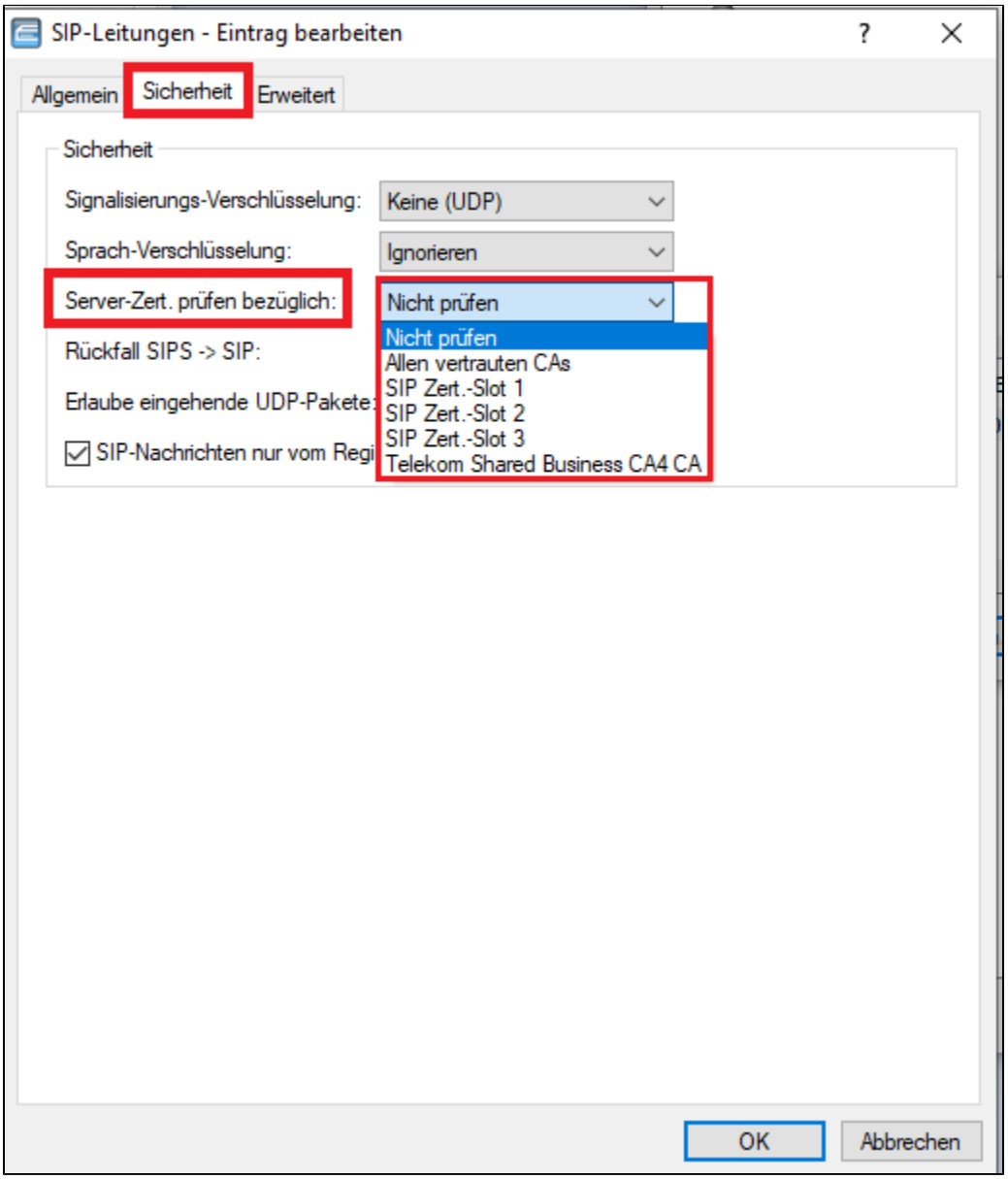
Mit dieser Einstellung wird gesteuert, ob Server-Zertifikate vom Voice Call Manager überprüft werden und mit welchem Zertifikat dies gegebenenfalls erfolgt. Nach Möglichkeit sollte das Server-Zertifikat gegengeprüft werden.

Mit der Einstellung **Nicht prüfen** wird das Server-Zertifikat nicht überprüft und somit beliebige Zertifikate zugelassen.

Bei **Allen vertrauten CAs** werden alle im Gerät hinterlegten Zertifikate verwendet, um das Server-Zertifikat gegenzuprüfen.

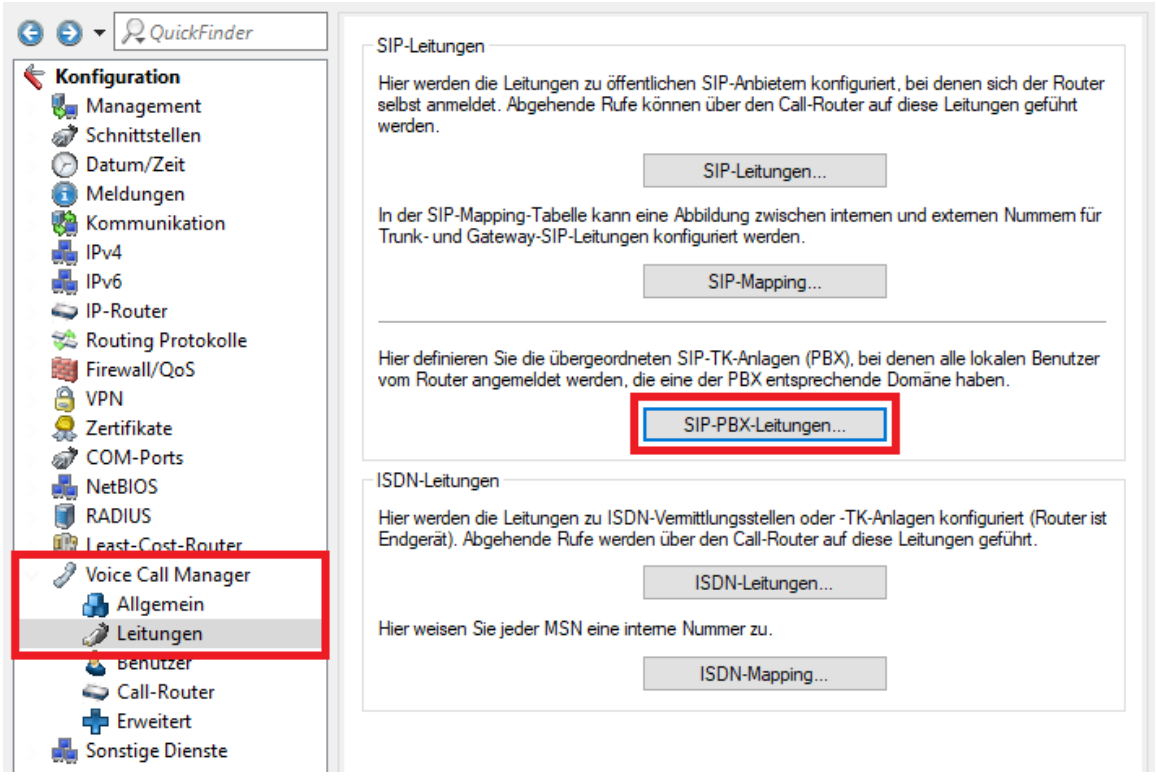
In die **SIP Zert.-Slots 1 -3** können vom SIP-Provider bezogene Zertifikate hochgeladen werden, welche zur Prüfung des Server-Zertifikates verwendet werden.

Bei Verwendung des **Telekom-Shared-Business-CA4** werden Server-Zertifikate akzeptiert, welche von der **Telekom Shared Business CA4 Certificate Authority (CA)** unterzeichnet wurden. Dieser Eintrag muss bei einem Telekom SIP-Trunk verwendet werden.



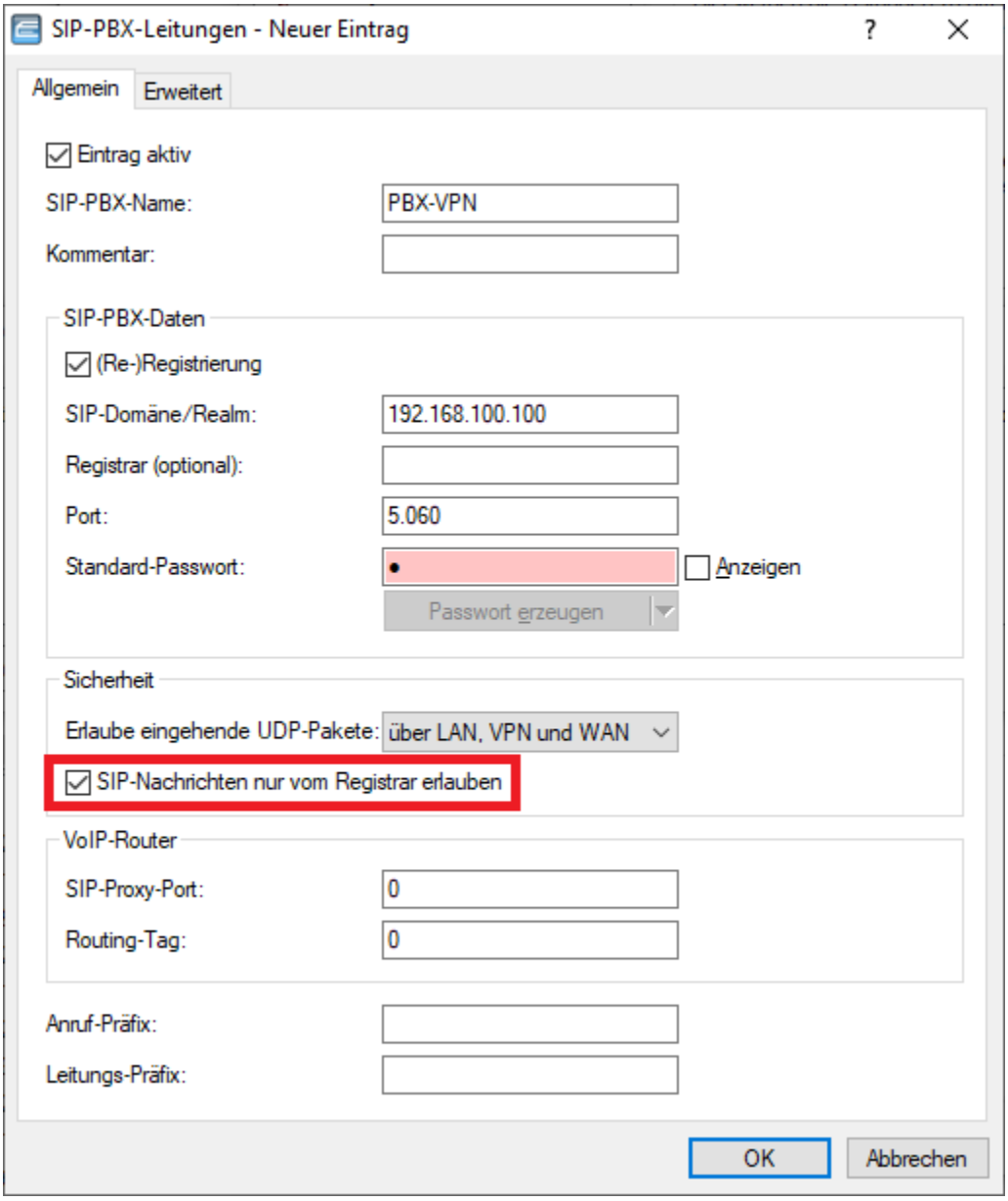
3. Möglichkeiten zur Absicherung bei Verwendung einer SIP-PBX-Leitung:

3.1 Wechseln Sie in das Menü **Voice Call Manager -> Leitungen -> SIP-PBX-Leitungen**.



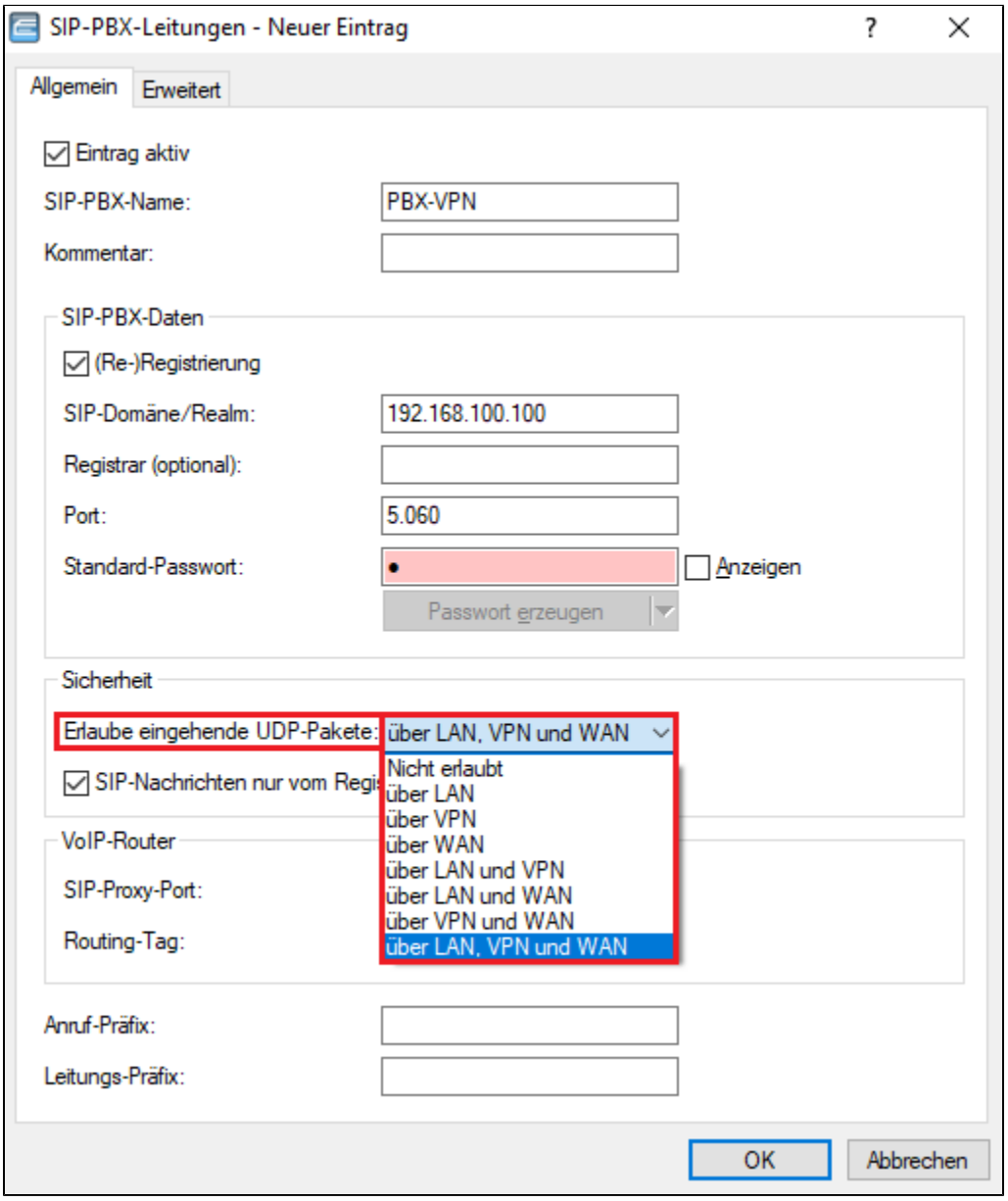
3.2 Stellen Sie sicher, dass der Haken bei **SIP-Nachrichten nur vom Registrar erlauben** gesetzt ist.

Die Funktionsweise ist die gleiche wie bei einer SIP-Leitung (siehe **Schritt 1.3**).



3.3 Schränken Sie die Funktion **Erlaube eingehende UDP-Pakete** auf das tatsächlich verwendete Interface ein.

In der Regel wird die angebundene SIP-TK-Anlage per LAN oder per VPN erreichbar sein und nicht per WAN. Eine direkte Anbindung per WAN ist aus Sicherheitsgründen zudem nicht empfehlenswert.


SIP-PBX-Leitungen - Neuer Eintrag
Allgemein
Erweitert
Eintrag aktiv
SIP-PBX-Name:
PBX-VPN
Kommentar:
SIP-PBX-Daten
(Re-)Registrierung
SIP-Domäne/Realm:
192.168.100.100
Registrar (optional):
Port:
5.060
Standard-Passwort:
Anzeigen
Passwort erzeugen
Sicherheit
Erlaube eingehende UDP-Pakete:
über LAN, VPN und WAN
SIP-Nachrichten nur vom Regi
Nicht erlaubt
über LAN
über VPN
über WAN
über LAN und VPN
über LAN und WAN
über VPN und WAN
über LAN, VPN und WAN
VoIP-Router
SIP-Proxy-Port:
Routing-Tag:
Anruf-Präfix:
Leitungs-Präfix:
OK
Abbrechen