

Bitte beachten Sie folgende Empfehlungen, um eine reibungslose Nutzung von VoIP zu gewährleisten.

1 VoIP Nutzung abklären

Informieren Sie Ihren EDV-Verantwortlichen über den geplanten Einsatz von VoIP und klären Sie im Vorfeld die notwendigen Konfigurationsmaßnahmen an Ihrem Router, Firewall oder Netzwerk ab.

2 Router Checklist

1. NAT-Session Timeout und Firewall Freigaben

Implementieren Sie die [Firewall Konfiguration](#) für SIP und RTP, damit der Server die Telefonanlage dauerhaft eingehend erreichen kann.

2. NAT Anforderungen

VoIP erfordert die Nutzung von sogenanntem Full Cone oder Static NAT, damit der Server die Telefonanlage zuverlässig über denselben Quell-Port erreichen kann. Source Port Randomization (zB.: pfSense) sollte für VoIP-Traffic deaktiviert werden.

3. Bandwidth Management (BWM) oder Quality of Service (QoS)

Falls Ihre Internet-Leitung neben IP-Telefonie auch anderweitig genutzt wird, empfehlen wir für SIP- und RTP-Traffic Bandbreite zu reservieren bzw. diesen Traffic zu priorisieren, damit es auch bei stark beanspruchter Internet-Leitung keine Probleme mit der Gesprächsqualität gibt. Pro gleichzeitigem Gespräch sollten **100 kbit/s Up und Download** einberechnet werden.

4. SIP ALG

Funktionen wie SIP Header Transformation werden nicht benötigt und können deaktiviert werden. Der Server behandelt NAT und lokale IP-Adressen in den SIP-Paketen automatisch korrekt. Falls Ihr Router SIP ALG auch für die Priorisierung von SIP-Traffic oder das Setzen eines NAT-Session Timeouts für SIP-Verbindungen (zB.: Zyxel) nutzt, können SIP ALG Funktionen sinnvoll sein. Bitte beachten Sie die empfohlenen SIP Einstellungen des Herstellers.

3 Firewall Konfiguration

Der Server muss die Telefonanlage jederzeit erreichen können, um Anrufe zustellen und den Online Status des SIP-Trunks überwachen zu können. Hierfür sind folgende Firewall Regeln zu konfigurieren:

Bezeichnung	Protokoll	Server Port	Server Subnets
SIP	UDP / TCP	5160	81.16.153.176/28 81.16.153.64/28
RTP	UDP	10000 - 32520	81.16.153.176/28 81.16.153.64/28

UDP NAT-Session Timeout

Konfigurieren Sie zusätzlich einen UDP-NAT Session Timeout von **600 Sekunden** für SIP-Traffic, damit die Verbindung zwischen Telefonanlage und Server dauerhaft offen gehalten wird.

Der Server sendet alle **60 Sekunden** ein OPTIONS-Paket, welches von der Telefonanlage beantwortet wird. Je nach Firewall muss die Telefonanlage allerdings aktiv ein neues Paket versenden, da die Antwort auf ein eingehendes Paket nicht ausreicht, um den NAT-Session Timeout der Verbindung zurückzusetzen.

In diesem Fall sollte bei der Telefonanlage SIP OPTIONS / Keepalive oder SIP Register Intervall von 500 Sekunden gewählt werden.

Ausgehende Firewall Freigaben

Falls Ihre Firewall auch ausgehende Verbindungen blockiert, müssen dieselben Freigaben für ausgehenden SIP- und RTP-Traffic eingerichtet werden.

4 Telefonanlagen Konfiguration

- ◆ Konfigurieren Sie einen SIP Register Intervall von **500 Sekunden**.
- ◆ Deaktivieren Sie Keep-Alive / SIP OPTIONS Pakete bei der Telefonanlage, sobald die Firewall Konfiguration durchgeführt wurde.

Falls SIP OPTIONS aktiviert bleibt, kann ein Register Intervall von bis zu 3600 Sekunden gewählt werden.

5 SIP Trunk Spezifikation

SIP Benutzer	Rufnummer im E.164 Format mit vorangestelltem u . (zB.: u+435352207207)
SIP Register Domain	<code>trunk.innofon.at:5160</code> oder <code>innotrunk.at:5160</code> Bitte beachten Sie die Angaben in dem Willkommensschreiben von Innosoft.
SIP Port	5160
SIP Transport	UDP und TCP. UDP wird empfohlen. TCP Transport muss vor der Nutzung von Innosoft aktiviert werden.
Signalisierung	Die Signalisierung von Rufnummer erfolgt im internationalen Format (<code>00435352207207</code> oder <code>+435352207207</code>) und ist abhängig von dem konfigurierten Profil: <ol style="list-style-type: none"> 1. Signalisierung per Display Name des SIP From Headers 2. Signalisierung per P-Preferred-Identity (PPI)-Header 3. Maßgeschneiderte Signalisierungen (Custom)
Codecs	Unterstützte Codecs mit folgender Priorisierung: <ul style="list-style-type: none"> ◆ G.711 (A-law und μ-law) ◆ G.726 (RFC3551) ◆ G.722
NAT Erkennung	Aktiviert. Das NAT-Handling für SIP Trunks sieht vor: <ul style="list-style-type: none"> ◆ SIP-Pakete werden an die IP-Adresse und Port des Absenders gesendet, sofern kein rport-Parameter vorhanden ist.

	◆ RTP-Pakete werden immer an die IP-Adresse und den Port des Absenders gesendet und die Port-Angaben im SDP werden ignoriert.
CLIR	Deaktiviert
CLIP no screening	Aktiviert
DTMF	RFC 2833
SIP OPTIONS	Aktiviert. Versand erfolgt alle 60 Sekunden. Der maximale Timeout der Antwort beträgt 2 Sekunden.
Blacklist	Deaktiviert. Es können Mehrwertnummern (9xx) oder Auslandsziele serverseitig gesperrt werden.
Bandbreite	<u>~100 kbit/s Up und Downstream</u> pro gleichzeitigem Gespräch bei der Verwendung von G.711.

Beispiele SIP-Header bei Signalisierung von Rufnummern

(1) Die zu signalisierende Rufnummer (05352207207-1) steht im Display Name des SIP-From Headers:

```
From: "+4353522072071" <sip:u+435352207207@trunk.innofon.at:5160>
```

(2) Die zu signalisierende Rufnummer (05352207207-1) steht im User Part des PPI-Headers:

```
From: <sip:u+435352207207@trunk.innofon.at:5160>
[...]
P-Preferred-Identity: <sip:+4353522072071@trunk.innofon.at:5160>
```