Netzwerk Checklist für Cloud Telefonanlage

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

Je nachdem wie strikt Ihr Router oder Firewall konfiguriert ist, sind Anpassungen an dieser oder Ihrem SIP-Client (Hardware Telefon, Softphone) notwendig.

Online Status der Durchwahlen prüfen

Richten Sie Durchwahlen der Cloud-Telefonanlage bei Ihren Endgeräten ein und prüfen Sie nach einiger Zeit in dem MyInno Portal den Online Status der Durchwahlen.

Falls Ihre Durchwahlen dauerhaft als Online dargestellt werden, ist keine weitere Konfiguration notwendig. Falls Ihre Durchwahlen dauerhaft zwischen On- und Offline wechseln, ist einer der folgenden Schritte durchzuführen:

a) Erhöhen Sie den UDP NAT-Session Timeout Ihres Routers.
b) Implementieren Sie die Firewall Konfiguration für SIP und RTP oder richten Sie feste Port Weiterleitungen für alle Endgeräte ein.
c) Konfigurieren einen SIP-Keep-Alive Intervall bei den Endgeräten, damit diese die Verbindung zwischen Server und Endgerät dauerhaft offen halten.

Router Anforderungen und Informationen

1. **NAT Anforderungen**
   VoIP erfordert die Nutzung von sogenanntem Static NAT, damit der Server alle Endgeräte zuverlässig über denselben Quell-Port erreichen kann. Source Port Randomization (zB.: pfSense) sollte für VoIP-Traffic deaktiviert werden.

2. **Bandwidth Management (BWM) oder alternativ Quality of Serice (QoS)**
   Falls Ihre Internet-Leitung neben IP-Telefonie auch anderweitig genutzt wird und Sie Probleme mit der Gesprächsqualität feststellen, empfehlen wir für SIP- und RTP-Traffic Bandbreite zu reservieren bzw. diesen Traffic zu priorisieren. Pro Endgerät sollten `100 kbit/s Up und Download` reserviert werden.

3. **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 SIG ALG auch für die Priorisierung von SIP-Traffic oder das Setzen eines NAT-Session Timeouts für SIP-Verbindungen (zB.: Zyxel) nutzt, können SIG ALG Funktionen sinnvoll sein. Bitte beachten Sie die empfohlenen SIP Einstellungen des Herstellers.

4. **Dual WAN, Load Balancing oder Multihoming**
   Falls beim Router mehrere Internet-Provider/Leitungen angebunden sind und Traffic über diese verteilt wird, muss für alle SIP-Geräte eine statisches Routing über einen Anschluss konfiguriert werden, damit diese den Server immer über dieselbe Public IP-Adresse kontaktieren.

3 Router Konfiguration

Der Server muss die SIP-Telefone jederzeit eingehend erreichen können, um Anrufe zustellen und den Online Status der Durchwahl überwachen zu können.

3.1 UDP NAT-Session Timeout

Konfigurieren Sie einen UDP NAT-Session Timeout von `600 Sekunden` für SIP-Traffic, damit die Verbindung zwischen den Endgeräten und dem Server länger offen gehalten wird.

Der Server sendet alle `60 Sekunden` ein OPTIONS-Paket an jedes Endgerät, welches von diesen beantwortet wird. Diese Kommunikation sollte die NAT-Session dauerhaft offen halten.

Je nach Firewall müssen die Endgeräte allerdings aktiv ein neues, ausgehendes Paket versenden, da die Antwort auf ein eingehendes Paket nicht ausreicht, um den Timeout der NAT-Session zurückzusetzen.

In diesem Fall sind die Informationen unter 4 SIP-Client Konfiguration zu beachten.

3.2 Firewall Konfiguration

Konfigurieren Sie folgende Firewall Regeln:

Bezeichnung	Protokoll	Server Port	Server Subnets
SIP	UDP / TCP	5160	81.16.153.0/24 77.237.54.128/27
RTP	UDP	10000 - 32520	81.16.153.0/24 77.237.54.128/27

Zusätzlich zu den Firewall Regeln ist es auch notwendig, dass eine aktive Verbindung (NAT-Session) zwischen Server und Telefon besteht, damit der Router weiß, an welches Endgerät im lokalen Netzwerk die Pakete weitergeleitet werden sollen. Siehe auch 3.1 UDP NAT-Session Timeout.

Beachten Sie am besten die empfohlenen Einstellungen des Router Herstellers für VoIP.

Ausgehende Firewall Freigaben

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

Für SIP-Telefone, wie die vorkonfigurierten Mitel-Telefone von Innosoft, müssen zusätzlich ausgehend die Protokolle DNS (53), NTP (123) und HTTPS (443) freigegeben werden.

3.3 Port Weiterleitungen

Grundsätzlich ist es auch möglich Port-Weiterleitungen für jedes Endgerätes in Ihrem Netzwerk einzurichten. Hierfür müssen Sie jedem Ihrer Endgeräte einen eindeutigen, lokalen SIP-Port zuweisen.

Anschließend können Sie Port-Weiterleitungen von genannten Subnets und Port `5160` auf alle lokalen IP-Adressen und lokalen SIP-Ports der Endgeräte einrichten.

Für RTP-Traffic sind in der Regel keine Weiterleitungen notwendig, da während eines Gesprächs durchgehend Sprachpakete ausgetauscht werden und dadurch automatisch die NAT-Session offen gehalten wird.

3.4 SIP-Keep-Alive Intervall

Falls Sie weder Firewall Freigaben, Port Weiterleitungen noch den NAT-Session Timeout konfigurieren können, besteht die Möglichkeit einen SIP Keepalive Timout bei den Endgeräten zu konfigurieren. Dieser bewirkt, dass das Endgerät alle zB.: 30 Sekunden ein ausgehenden Paket an den Server sendet, wodurch der Router gezwungen ist die NAT-Session (Verbindung) zwischen Endgerät und Server offen zu halten.

Der optimale Intervall ist von dem NAT-Session Timout des Routers abhängig. Sie können mit 60 Sekunden beginnen und den Wert halbieren bis die Telefone unter Online Status dauerhaft online bleiben.

4 SIP-Client Konfiguration

- Aktivieren Sie die SIP Keep-Alive Funktion Ihres Endgerätes mit einem Intervall von zB.: `60 Sekunden`, damit dieses regelmäßig ausgehende Pakete sendet, um die Verbindung zum Server offen zu halten.

- Alternativ kann auch ein SIP Registrierungsintervall von `500 Sekunden` konfiguriert werden, damit sich das Endgerät öfter registriert. Ansonsten ist ein Register Intervall von `3600 Sekunden` ausreichend.

5 SIP Spezifikation

SIP Benutzer	Rufnummer der Durchwahl im E.164 Format mit vorangestelltem `u`. (zB.: `u+4353522072071`)
SIP Register Domain	Der SIP Servers kann in der MyInno Web-Anwendung unter PBX Durchwahlen über den Button Anmeldedaten angezeigt werden.
SIP Port	5160
SIP Transport	Standardmäßig immer UDP. TCP Transport muss vor der Nutzung von Innosoft aktiviert werden.
Signalisierung	Die Signalisierung der Rufnummer kann in der MyInno Web-Anwendung unter PBX und Durchwahlen für jede Durchwahl mit der Option `Signalisierung` konfiguriert werden. Möglich ist es nur die Hauptnummer zu signalisieren oder eine beliebige in der Anlage konfigurierte Durchwahl.

Codecs	Unterstützte Codecs mit folgender Priorisierung: ◆ G.711 (A-law und µ-law) ◆ G.726 (RFC3551) ◆ G.722
DTMF	RFC 2833
CLIR	Rufnummernunterdrückung kann für jede Durchwahl durch das Wählen der Tastencodes `*02#1` aktiviert und `*02#0` deaktiviert werden. Siehe das Dokument Tastenbefehle
SIP OPTIONS	Aktiviert. Versand erfolgt alle 60 Sekunden. Der maximale Timeout der Antwort beträgt 2 Sekunden.
NAT Erkennung	Aktiviert. Das NAT-Handling für SIP Accounts sieht vor: ◆ 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.
Bandbreite	~100 kbit/s Up und Downstream pro gleichzeitigem Gespräch bei der Nutzung von G.711 als Codec.