

Richtlinien zur Netzwerkkonfiguration

1. Port

Folgende Ports sind für die VoIP Kommunikation wichtig:

5060 UDP: Auf diesem Port finden die Registrationen und Anrufsignalisationen statt.

RTP Portrange: In diesem Portrange werden die Sprachdaten übermittelt. Dieser Portrange kann auf der Telefonanlage konfiguriert werden. Die Einstellung heisst ist in der Regel Audio Portrange oder RTP Portrange. Falls nicht der standard Portrange verwendet werden möchte, kann dieser beliebig gesetzt werden. Dabei beachten sollten Sie, dass der Portrange höher als 10'000 gewählt wird, damit keine Ports von Services überschritten werden, und pro aktivem Gespräch mindestens 2 Ports verfügbar sind. Wenn zum Beispiel 10 Telefone vorhanden sind und man davon ausgeht, dass jedes Telefon eventuell eine 3er Konferenz macht, sollte der Portrange mindestens 60 Ports beinhalten.

2. Firewall

Auf der Firewall muss der Port 5060 UDP und der RTP Portrange freigegeben werden.

Beim Port 5060 empfehlen wir, falls möglich, eine Source Restriktion zu hinterlegen. Der Port 5060 muss für den IP Range 212.117.203.1 – 254 offen sein. Dieser IP Range ist von uns für die VoIP Server reserviert.

Beim RTP Portrange darf keine Restriktion definiert sein. Die Sprachdaten werden meist peer-to-peer übermittelt. Dieser Portrange ist nicht Sicherheitskritisch, da die Telefonanlage nur Sprachpakete auf diesen Ports entgegennimmt.

3. Router

Damit die Telefonanlage auch eingehend erreichbar ist, müssen eingehende Pakete auf dem Port 5060 vom Router zur Telefonanlage weitergeleitet werden.

Um dies zu erreichen gibt es 2 Möglichkeiten:

1. NAT Keep Alive auf der Telefonanlage aktivieren. Es werden dann alle 20 – 30 Sekunden ein Packet auf dem Port 5060 an den sipcall Server geschickt. Dadurch wird in der dynamischen NAT Tabelle der Eintrag gehalten.
2. Portforwarding für den Port 5060 auf die Telefonanlage einrichten. Dann werden alle Pakete die auf dem Port 5060 ankommen an die Telefonanlage weitergeleitet. Auch SIP Anfragen von anderen IPs als von den sipcall Servern. Daher sollte diese Variante nur in Kombination mit einer Source Restriktion auf der Firewall verwendet werden.

4. SIP-ALG

Es gibt viele Router auf denen SIP-ALG nicht SIP konform arbeitet. Wenn Sie Probleme mit der Sprachübertragung haben, also nichts zu hören ist, kann dies unter Umständen SIP-ALG verursachen. Um die Sprachqualität optimal zu halten, wird beim Anrufaufbau als Zieladresse für die Sprachdaten direkt die IP Adresse des Gateways, respektive des angerufenen VoIP Anschlusses, angegeben. Manche SIP-ALGs ersetzen diese IP Adresse einfach mit der SIP-Server Adresse, wodurch die Sprachdaten an die falsche IP geschickt werden und nicht ankommen. Bei solchen Problemen muss SIP-ALG auf dem Router deaktiviert werden. Diese Einstellung kann je nach Router als „SIP processing“, „SIP-ALG“ oder „SIP Application Layer Gateway“ benannt sein.