

# DOKU - Hosted-PBX

## Technische Voraussetzungen für den Einsatz der Hosted-PBX

---

**Version:** 28

**Datum:** 03.09.2018 12:31

# 1 Voraussetzungen im Netzwerk

Bitte beachten Sie nachfolgende Punkte bezüglich der Anforderungen für Ihr Netzwerk, welche Voraussetzung für ein Plug&Play Rollout sind:

- IP-Adressvergabe per DHCP inkl. DNS, Gateway
- Option 66 deaktiviert oder nach Rücksprache
- Kein SIP ALG
- Keine aktivierten SIP-Helper-Funktionen
- Kein Spanning Tree

## 2 Firewall-Konfiguration

Für die Kommunikation mit der Hosted-PBX müssen die Endgeräte in der Lage sein zu folgenden Ports und Zielen ausgehend zu kommunizieren:

Protokoll	Zielport	Zweck	Ziele
UDP /TCP	alle Ports	SIP, RTP, TLS, T.38, ..	46.182.249.32/28
UDP /TCP	alle Ports	Applikationen- und Provisioning-Server	alt: 193.106.16.0/24 (gültig bis 31.12.2018) neu: 85.197.88.0/26

Protokoll	Zielpport	Zweck	Ziele
UDP	123	NTP-Server	Alle Netze
UDP	53	DNS-Server	Per DHCP mitgeteilte DNS-Server des Kunden
TCP	Abhängig vom Hersteller (meist 80 /443)	Redirection-Server der Endgerätehersteller	Abhängig von den verwendeten Endgeräten

Es sind im Regelfall keine eingehenden Port-Forwardings notwendig. Voraussetzung ist das eventuell vorhandenen Firewalls "Stateful" sind und Antworten in offenen Sessions, egal ob TCP oder UDP, akzeptiert werden.

Beim Einsatz von NAT ist ein Timeout von mehr als 60 Sekunden zwingend. Wir empfehlen einen Timeout von 90 Sekunden.

Sämtliche SIP ALG / SIP Helper Funktion im Router bzw. der Firewall sind zu deaktivieren.

## 2.1 Redirection-Server der Hersteller

[provisioning.snom.com](http://provisioning.snom.com)

[secure-provisioning.snom.com](http://secure-provisioning.snom.com)

[prov.aastra.com](http://prov.aastra.com)

[prov.gigaset.net](http://prov.gigaset.net)

[ztp.polycom.com](http://ztp.polycom.com)

[rcs.aastra.com](http://rcs.aastra.com)

[rps.yealink.com](http://rps.yealink.com)

(außerdem können abhängig von den verwendeten Endgeräten weitere Regeln für Provisioningserver nötig sein)

## 2.2 Hinweise:

- Alle angegebenen Hostname stehen unter dem Vorbehalt der Änderung der IP-Adressen. Diese können vom Hersteller oder vom Anbieter jederzeit geändert werden.

- Firewalls beim Endkunden sollen immer den gesamten Netzbereich mit sämtlichen Protokollen (nur auf IP-Adressen) Stateful Richtung Plattform freischalten.
- Eine Einschränkung auf einzelne IP-Adressen kann dazu führen, dass der Dienst nicht mehr funktioniert, wenn IP-Adressen geändert werden.
- Eine Freischaltung in Richtung der SIP-Endgeräte ist nur dann notwendig, wenn die Firewall keine "Stateful Rules" unterstützen.