

Merkblatt Firewall

Liebe Kundin, lieber Kunde

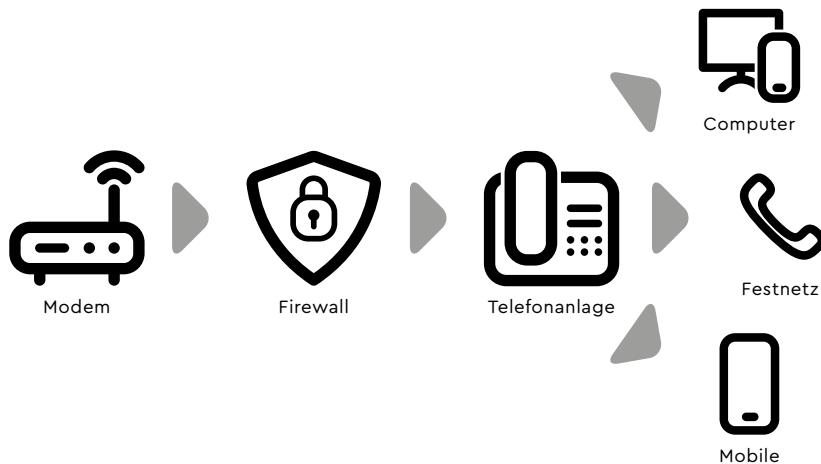
Herzlichen Glückwunsch! Sie haben sich für die Business Telefonie von Blizz entschieden.

Damit die Business Telefonie von Blizz reibungslos funktioniert, sind gewisse Punkte bezüglich Ihrem Firmennetzwerk zu beachten. Mit dem vorliegenden Dokument möchten wir Ihnen gerne die wichtigsten Infos im Zusammenhang mit Ihren neuen Produkten mit auf den Weg geben.

Das Allerwichtigste vorweg: Für den sicheren Betrieb Ihrer Blizz Business Telefonie empfehlen wir Ihnen in jedem Fall den Einsatz einer Firewall. Diese muss zwingend VoIP-fähig sein und eine DHCP-Funktion enthalten.

1. Netzwerkarchitektur und Firewall Regeln

1.1. Blizz Business Voice Channel (SIP Trunk und MS Teams)



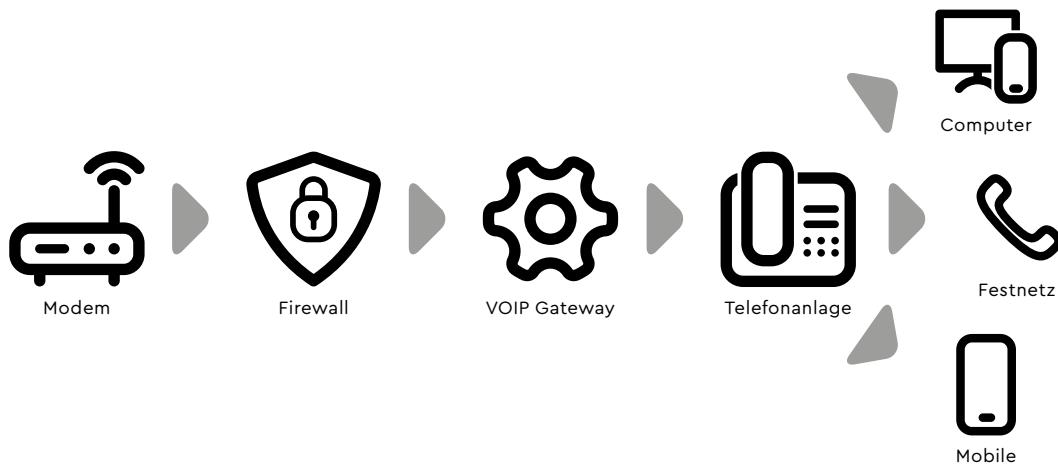
Folgende Einstellungen sind auf Ihrer Firewall notwendig:

PROTOKOLL	PORT	IP
SIP	UDP: 5060	185.185.32.60
RTP	UDP: 40'000–50'000	185.185.32.61 & 185.185.32.62

SIP-ALG: ausgeschalten

UDP-Session-Timeout: > = 300 Sekunden

1.2. Blizz Business Voice Channel (SIP to ISDN)



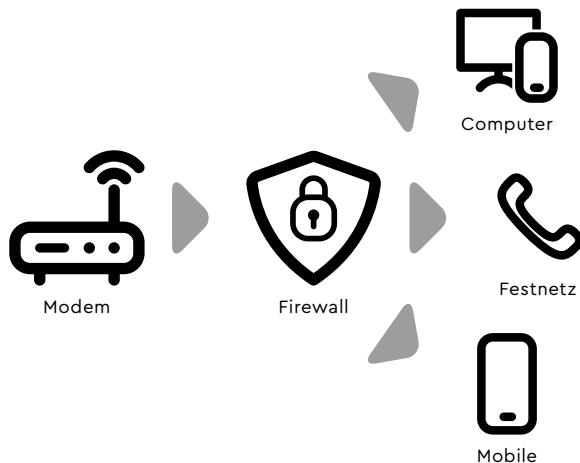
Folgende Einstellungen sind auf Ihrer Firewall notwendig:

PROTOKOLL	PORT	IP
SIP	UDP: 5060	185.185.32.60
RTP	UDP: 40'000–50'000	185.185.32.61 & 185.185.32.62

SIP-ALG: ausgeschalten

UDP-Session-Timeout: > = 300 Sekunden

1.3. Blizz Business Voice Hosted Pro (HPBX)



Jede Blizz Business Voice Hosted Pro Anlage erhält eine eigene IP Adresse. Diese IP Adresse muss auf der Firewall zugelassen werden.

Bei der häufigsten Firewall/Router Nutzung werden alle Pakete vom LAN Richtung WAN durchgelassen. Dann müssen nur diese Einstellungen beachtet werden:

- Keine ALG oder SIP-ALG einschalten (ist oft als Standard eingeschaltet)
- Die UDP-Session-Timeout muss mindestens auf 90 Sekunden eingestellt werden

Bei ausgehenden Rulesets müssen folgende Ports nach aussen zugelassen werden:

Ports in Richtung Internet bzw. WAN → wwphone

Im Modus; CTI, Softphone, Flex Client und Flex Core:

- TCP 443, 3333 und 5050 → wwcommunicator

Zusätzlich im Modus; Softphone und FLEX Core:

- UDP 5060 → wwcommunicator (SIP ohne TLS)
- TCP 5061 → wwcommunicator (SIP mit TLS)
- UDP 10000–20000 → wwcommunicator (RTP wird dynamisch ausgehandelt)

SIP-Endgeräte

- UDP 5060 → wwcommunicator
- UDP 10000–20000 → wwcommunicator
- LDAP 389 → wwcommunicator
- LDAP-SSL 636 → wwcommunicator

Provisioning

- TCP 8099 (Cisco-ATA) → wwcommunicator
- TCP 443 → wwcommunicator

Druckertreiber

- TCP 5050 und 3333 → wwcommunicator

TAPI-Treiber

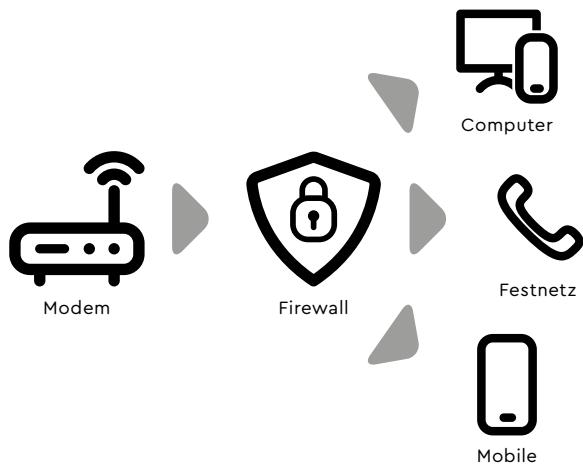
- TCP 5050 → wwcommunicator

Eingehende Ports

Call Recording

Hierzu wird eine ssh Verbindung über einen beliebigen Port, auf dem wwcommunicator konfiguriert. Über diesen Port werden die aufgenommenen Files auf einen externen Speicher kopiert, welche Kundenseitig eingehend freigegeben werden muss.

1.4. Blizz Business Voice Hosted Basic (Nexcloud)



Folgende Einstellungen sind auf Ihrer Firewall **notwendig**:

- Die IP von Blizz Business Voice Cloud Basic ist 185.185.33.10, dort registrieren sich die Endgeräte
- Keine ALG oder SIP-ALG einschalten (ist oft als Standard eingeschaltet)
- Die UDP-Session-Timeout muss mindestens auf 90 Sekunden eingestellt werden