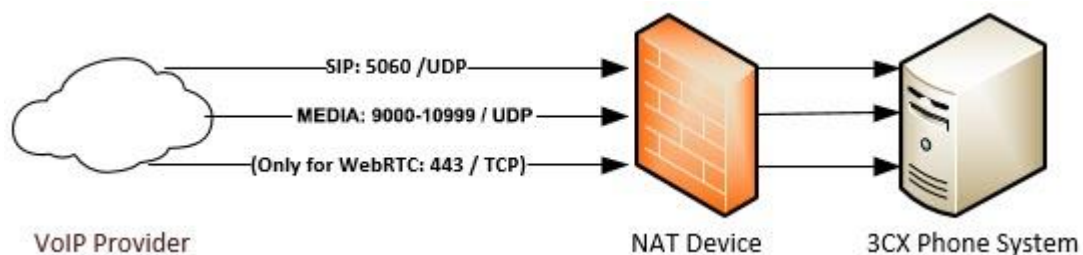


Einführung

Wenn Sie externe Nebenstellen oder einen VoIP-Provider nutzen möchten, müssen Sie Ihre Firewall für den SIP-Betrieb vorbereiten, damit sich SIP-Trunks und externe IP-Telefone problemlos an die 3CX-Telefonanlage anbinden lassen. Nachfolgend erhalten Sie einen grundlegenden Überblick über Ports, die in Ihrer Firewall geöffnet sein/statisch weitergeleitet werden müssen.

Konfigurieren von Ports für Ihren SIP-Trunk/VoIP-Provider



Öffnen Sie die folgenden Ports, damit die 3CX-Anlage mit Ihrem VoIP-Anbieter/SIP-Trunk und per WebRTC kommunizieren kann:

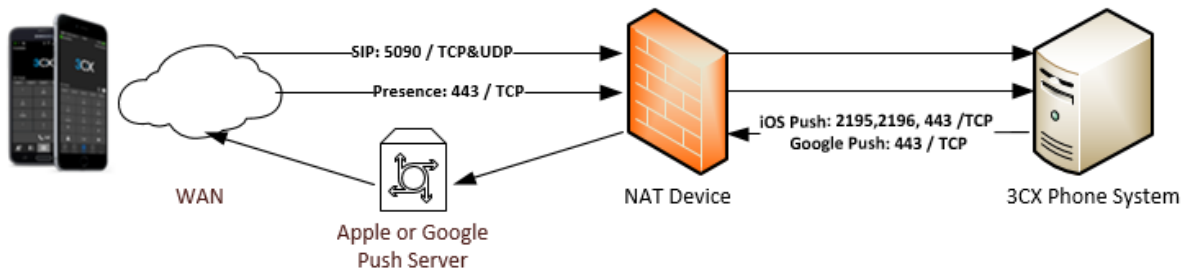
- Port 5060 (eingehend, UDP) zur Übertragung von SIP-Daten
- Port 9000 bis 10999 (eingehend, UDP) zur RTP-Kommunikation (Audio/eigentlicher Anruf). Für jeden Anruf sind zwei RTP-Ports erforderlich: ein Port zur Anrufsteuerung und ein weiterer zur Übertragung der Anrufdaten. Sollen mehrere Anrufe gleichzeitig erfolgen, muss somit stets die doppelte Anzahl an offenen Ports verfügbar sein.

💡 Tipp: Die oben angegebenen standardmäßigen Ports der 3CX-Anlage können über die 3CX-Verwaltungskonsole per **“Einstellungen” > “Netzwerk” > “Ports”** geändert werden.

Konfigurieren von Ports für externe 3CX-Applikationen

Öffnen Sie die folgenden Ports, damit Benutzer die 3CX-Applikationen für Android, iOS, Mac oder Microsoft Windows auch außerhalb des Unternehmensnetzwerks nutzen können:

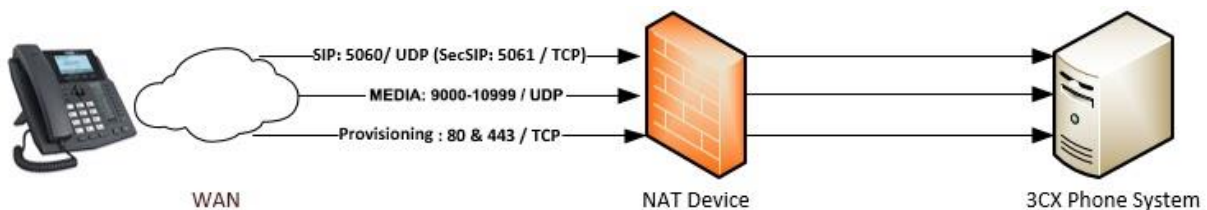
- Port 5090 (eingehend, UDP und TCP) für den 3CX-Tunnel
- Port 443 oder 5001 (eingehend, TCP, HTTPS) für Präsenzanzeige und Telefon-Provisionierung; alternativ der von Ihnen festgelegte HTTPS-Port
- Port 443 (ausgehend, TCP) für Push-Benachrichtigungen von Google Android
- Port 2195 und 2196 (ausgehend, TCP) für Push-Benachrichtigungen von Apple iOS



Die 3CX-Anlage schickt Push-Benachrichtigungen an Smartphones, die per 3CX-Applikation als mobile Nebenstellen fungieren und bei eingehenden Anrufen ggf. aus dem Ruhezustand geholt werden. Per Smartphone-Applikation genutzte mobile Nebenstellen werden somit bedeutend benutzerfreundlicher.

Konfigurieren von Ports für externe IP-Telefone/Bridges per direkte SIP-Verbindung

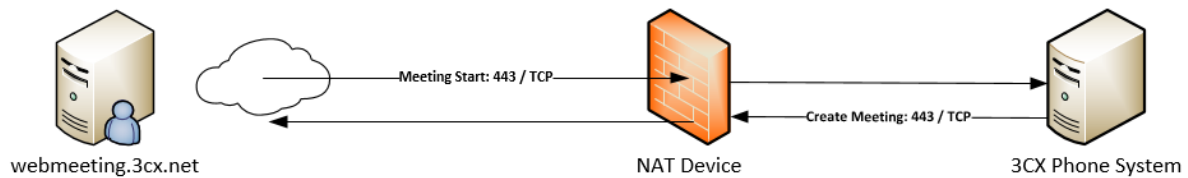
Die Anbindung von externen IP-Telefonen und Bridges kann per 3CX SBC (Session Border Controller für Tunnelverbindung) oder direkte SIP-Verbindung erfolgen. Der 3CX SBC bündelt als Dienst den gesamten VoIP-Traffic über einen einzelnen Port. Somit vereinfacht er die Firewall-Konfiguration und sorgt für höhere Zuverlässigkeit. Es ist keine weitere Konfiguration erforderlich, da der 3CX SBC dieselben Ports wie die 3CX-Applikationen nutzt. Nähere Informationen zum 3CX SBC erhalten Sie [hier](#).



Wenn Sie externe Nebenstellen hingegen per direkte SIP-Verbindung anbinden möchten, müssen Sie die nachfolgenden Ports öffnen:

- Port 5060 (eingehend, UDP und TCP), Port 5061 (eingehend, TCP, bei Verwendung von Secure SIP) – bei vorhandenen SIP-Trunks bereits geöffnet
- Port 9000 bis 10999 (eingehend, UDP) für RTP-Kommunikation – bei vorhandenen SIP-Trunks bereits geöffnet
- Port 443 oder 5001 (eingehend, TCP, HTTPS) zur Provisionierung von Telefonen (außer bei Nutzung benutzerdefinierter Ports).

Konfigurieren von Ports für 3CX WebMeeting und SMTP-Server



Damit Sie Online-Meetings erstellen und daran teilnehmen können, muss der von 3CX gehostete Cloud-Dienst an die 3CX-Telefonanlage angebunden werden. Zur Kommunikation zwischen Anlage und Dienst müssen Sie daher folgende Ports konfigurieren:

- Port 443 (ausgehend, TCP) für

webmeeting.3cx.net

. Da die IP-Adresse sich unter Umständen ändern kann, sollten Sie vorzugsweise Verbindungen mit dem FQDN zulassen, sofern möglich.

- Weiterleitung von Port 443 oder 5001 (eingehend, TCP) bzw. dem von Ihnen vorgegebenen HTTPS-Port. Dient der Benachrichtigung von Benutzern über eingehende Online-Meeting-Verbindungen.
- Um E-Mails über den 3CX SMTP-Server verschicken zu können, muss der 3CX-Server ausgehende Verbindungen auf TCP-Port 2528 erlauben.

Deaktivieren des SIP ALG

Setzen Sie einen Router/eine Firewall ohne SIP Helper und SIP ALG (Application Layer Gateway) ein. Alternativ können Sie ein Gerät verwenden, bei dem sich das SIP ALG deaktivieren lässt.