

Technische Anforderungen 3CX

Nachdem die Produkte der 3CX über Ihr Netzwerk/Internetleitung abgeführt werden, ist es wesentlich, dass ausreichend Bandbreite für ein Gespräch garantiert zur Verfügung gestellt wird. Je Gespräch wird ~ 100 Kbit Up & Down benötigt (Codec ISDN/711a).

Wird eine gemeinsame Internet-Leitung für Daten & 3CX verwendet ist ausdrücklich auf Ihrer Firewall eine Quality of Service (QoS) einzurichten, womit VoIP-Pakete höher als Daten-Pakete priorisiert werden. Entweder direkt auf dem Port Ihrer Firewall wo unser VPN-Router eingebunden wird oder ein QoS auf das IP-Netz der IP-Telefone (10.XXX.XX.XX). Sollte QoS nicht möglich sein, wird eine dedizierte Internet-Leitung ausschließlich als Voice-Leitung empfohlen. Das Netzwerk muss über eine strukturierte LAN-Verkabelung verfügen und jedes Telefon über einen Netzwerk-Anschluss.

Damit Gespräche im lokalen Netz intern abgehandelt und die Telefone an unsere Cloud Anlage bestens angebunden werden können, setzen wir einen VPN-Router ein.

Die bevorzugteste Lösung (Standard) wäre die Telefone direkt oder ab 4 Telefone über einen Unmanaged-Switch am VPN-Router (Port 1-3 für Tischtelefone bzw. Unmanaged-Switch, Port 4 Uplink WAN) anzuschließen.

Sollte dies aufgrund der Verkabelung nicht möglich sein, dann wird der VPN-Router im Netzwerk angeschlossen (Port 1 & Port 4 an LAN) und verteilt statische IP-Adressen an die MAC-Adressen der Tischtelefone. Bitte um Kontaktaufnahme sollte diese Variante von Ihnen priorisiert werden.

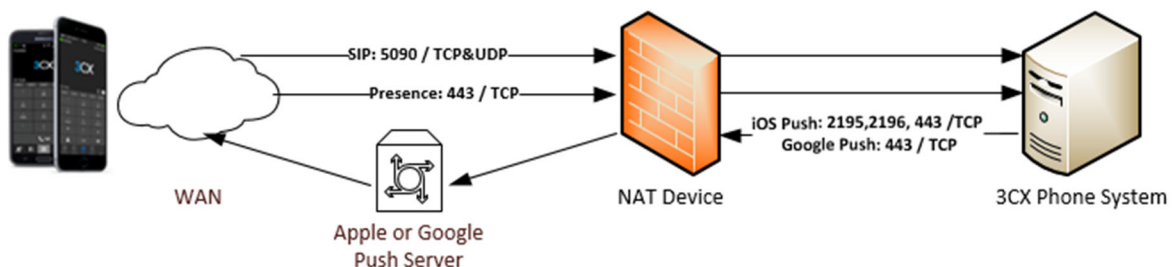
Weiteres könnten die Tischtelefone auf Wunsch auch über VLAN konfiguriert werden, sofern Ihr VLAN-Switch alle Pakete der Tischtelefone ungefiltert UDP/TCP/Multicast an den VPN-Router durchlässt. Bitte um Kontaktaufnahme sollte diese Variante von Ihnen priorisiert werden.

Zulassen von VPN Verbindungen

Im Regelfall lassen Standard-Konfigurationen VPN-Verbindungen ohne gesonderter Freischaltung zu. Unser VPN-Router arbeitet mit Open VPN. Verbindungen für Open VPN über TCP müssen in Ihrer Firewall freigeschaltet sein.

Konfigurieren Ihrer Firewall von Ports für externe 3CX-Applikationen

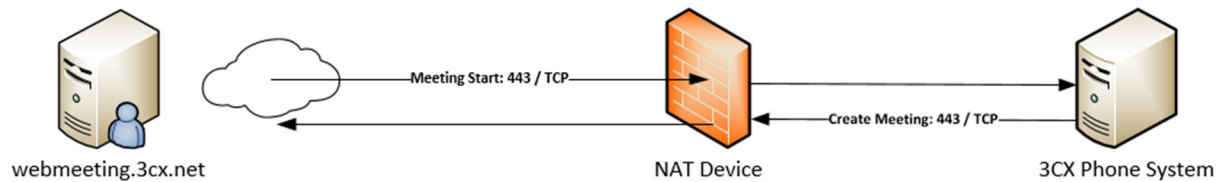
Öffnen Sie die folgenden Ports, damit Benutzer die 3CX-Applikationen für Android, iOS, Mac, Microsoft Windows oder Web-Client (Chrome/Firefox) nutzen können:



- Port 5090 (eingehend, UDP und TCP) für den 3CX-Tunnel
- Port 5060 (eingehend, UDP) zur Übertragung von SIP-Daten
- 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
- Port 9000 bis 10999 (eingehend, UDP) zur RTP-Kommunikation (Audio/eigentlicher Anruf)

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 3CX WebMeeting



tellen und an Konferenzen teilnehmen können, muss 3CX WebMeeting als gehosteter Cloud-Service an die 3CX-Telefonanlage angebunden werden. Zur beidseitigen Kommunikation zwischen Anlage und Dienst müssen folgende Ports weitergeleitet und ausgehender Datenverkehr zugelassen werden:

- Port 443 (ausgehend, TCP) an Ihren FQDN (XXXX.3cx-hostprofis.at:XXXX).
- Port 443 oder 5001 (eingehend, TCP); alternativ der von Ihnen vorgegebene HTTPS-Port. Dient der Benachrichtigung von Benutzern über eingehende Online-Meeting-Verbindungen.

Deaktivieren des SIP ALG

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