Technische Anforderungen
der ITM Informationstransport und -management GmbH
für die Verwendung des Produkt „Vpbx“

Inhaltsverzeichnis

Allgemein

Mit der Vpbx Cloud stellt die ITM Gmbh dem Kunden die Dienste einer virtuellen Kundennebenstellenanlage über das IP-Protokoll zur Verfügung. Diese stellt die Verbindung mit dem öffentlichen Telefonnetz (PSTN) her und bietet weitere Funktionen zur internen und externen Zusammenarbeit.
Die Steuerung und der Transport der Daten zwischen der zentralen Vpbx Instanz und dem Kundenstandort erfolgt verschlüsselt über das Internet. Zur Nutzung der angebotenen Dienste ist daher ein entsprechend dimensionierter Internet-Anschluss erforderlich.
Wir empfiehlen ein SDSL (Symmetric Digital Subscriber Line) Access Produkt, da sich hiermit die Daten mit der gleichen Geschwindigkeit in beide Richtungen übertragen lassen, welche durch den Kunden bereitgestellt werden muss.
Die benötigte Bandbreite ist abhängig von der Art und Anzahl der verwendeten Dienste.

Für die Dimensionierung gelten die nachfolgenden Mindestbandbreiten (Up- und Download):

- Bruttobandbreite (IP) je externer Sprachkanal: 100 kbit/s
- Bruttobandbreite (IP) je Faxübertragung gemäß T.38 (G3): 14,4 kbit/s
- Bruttobandbreite (IP) je Videokanal / Desktop Sharing: variable Bitrate bis zu 500 kbit/s

Direkte interne Sprachverbindungen zwischen IP-Endgeräten werden innerhalb des lokalen Netzwerks hergestellt.

Netzwerkanforderungen

Voice over IP ist nur dann in einem Netzwerk nutzbar, wenn die wichtigen Kennwerte, wie Bandbreite, Laufzeit und Jitter bei einem voll ausgelasteten Netzwerk einschließlich der Netzübergänge ausreichend sind.

Die Sicherstellung einer ausreichenden Qualität der Vpbx Dienste erfordert folgende Umgebungs-anforderungen im LAN:

- LAN ab 100 MBit/sec
- mind. CAT.5 Netzwerkverkabelung
- Netzauslastung < 40 %
- Eigener Port am Switch oder Router für jedes IP-Endgerät
- Latenzzeit (round-trip delay time): < 150ms
- Paket Jitter (packet delay variation): < 20ms
- Paketverlust (packet loss): < 3%

Die Vpbx Endgeräte verwenden folgende Codecs:

- G711 A-law / µ-law: IP-Telefone, Softphone, IP analog Adapter
- G.722: IP-Telefone, Softphone, myApps (Android, iOS), IP analog Adapter
- Opus: Softphone, myApps (Android, iOS),
- H.264: myPBX/myApps Video/Applikation Sharing
- VP8/VP9: myApps Video/Applikation Sharing

Benötigte Netzwerkports für die Vpbx / Firewall

Von innen nach außen muss folgender Zugriff möglich sein. Werte in Klammern sind nur informativ und können sich ändern. Die rot dargestellten Werte sind neu ab 09.2023:

TCP/UDP	Port/s	Protokoll	IP / Subnetz IPv6	FQDN	Zweck
TCP	80	HTTP	(46.232.228.11)	config.innovaphone.com	Config-Redirect-Server
TCP	443	HTTPS / WebSocket	217.19.181.160/28 80.228.239.192/27 2a00:1f08:4012::/48 2a02:8204:d807::/48	(prov.vpbx.myadmin.cloud, store1.vpbx.myadmin.cloud)	Config- und Software-Download myApps
TCP	1300	H.323/TLS		(z.B. itmgmbh.vpbx.myadmin.cloud)	Signalisierungsprotokoll, FQDN ist kundenspezifisch
TCP	636	LDAP/S		(z.B. app01.vpbx.myadmin.cloud, kbcgmbh.vpbx.myadmin.cloud)	Telefonbuch und Namensauflösung
UDP	dynamisch	STUN / TURN	217.19.181.160/28 80.228.239.192/27	(stun1.vpbx.myadmin.cloud, stun2.vpbx.myadmin.cloud)	NAT-Traversal für RTP, initial wird Port 3478 verwendet, danach wird ein dynamischer Port ausgehandelt
UDP	123	NTP		de.pool.ntp.org	Zeit-Server, wird der NTP-Server per DHCP

TCP/UDP	Port/s	Protokoll	IP / Subnetz IPv6	FQDN	Zweck
					zugewiesen, dann greift zuerst der per DHCP zugewiesene
UDP	dynamisch	RTP	93.95.133.25/29 80.228.239.192/27 2a00:1f08:4012::/48 2a02:8204:d807::/48	-	Direktes Routing für Sprache, Video, App-Sharing
UDP	dynamisch	RTP	Internet	-	Direktes Routing für Sprache, Video, App-Sharing zu mobilen Clients (iOS/Android) oder Home-Office, für Clients hinter NAT ist der Port-Range nicht definiert, falls dies nicht freigeschaltet wird Umweg über TURN benutzt

DHCP und DNS

Die Telefone benötigen eine per DHCP vergebene IP-Adresse und einen DNS-Server. Optional kann auch ein eigener NTP-Server per DHCP vergeben werden.

Für DECT-Master Gateways muss eine feste IP-Adresse im Kundennetz vergeben werden. Diese wird dann projektspezifisch erfragt und vergeben.

E-Mail-Empfang und Firewall (z.B. Microsoft Safe Links, Advanced Threat Protection, Defender)

Seitens der Vpbx-Plattform werden E-Mails, z.B. für den Passwort-Reset versendet. Diese E-Mails enthalten HTTLS-Links (URLs).

Manche Applikations-Firewalls bzw. Sicherheitslösungen untersuchen URLs in E-Mails auf das Bedrohungspotential. Je nach Lösung, werden die URLs aus einer Sandbox heraus sogar mit einem HTTP-GET-Request ausgeführt. Dies führt zu Störungen bei der Passwort-Reset-Funktion. Deshalb sollte hier eine Ausnahme konfiguriert werden.

Definiert werden sollte die Aunahme für folgende URLs:

https://app01.vpbx.myadmin.cloud/*

https://app02.vpbx.myadmin.cloud/*

https://app03.vpbx.myadmin.cloud/*

https://app04.vpbx.myadmin.cloud/*

Für Microsoft Safe Links ist die Konfiguration von Ausnahmen hier im Kapitel „Do not rewrite the following URLs“ beschrieben:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links?view=o365-worldwide#do-not-rewrite-the-following-urls-lists-in-safe-links-policies

Anforderungen Endgeräte und APP

Die Provisionierung der durch den Reseller bereitgestellten IP-Endgeräte erfolgt automatisch. Eine manuelle Konfiguration der Endgeräte (STUN/TURN Zugangsdaten etc.) ist somit nicht erforderlich. Die Zuteilung der userbezogenen Konfigurationsdaten erfolgt auf Basis der MAC Adresse des Endgeräts.

Folgende Voraussetzungen müssen erfüllt sein:

- LAN Port RJ45 (Modular Jack 8P8C)
- Patchkabel RJ45 (Modular Jack 8P8C)
- Anschlusskabel RJ-11 (modular Jack 6P2C) für analoge Endgeräte
- Stromversorgung über „Power over Ethernet“ nach IEEE 802.3af
- Alternativ: Stromversorgung über Steckernetzteil (Primär: 110-240 V, 50 Hz, 45 mA)
- Zuteilung einer internen IP Adresse (über DHCP Server oder feste IP)
- Internetzugang (HTTPS über TCP-443)

Voraussetzungen für den Einsatz von Applikationen

Das Vpbx User Portal stellt folgende Funktionen zur Verfügung

- Download von Software und Dokumentationen
- Userbezogene Zugangsdaten
- Konfiguration von IP-Telefonen
- Faxversand
- Konfiguration der Voicemail-Ansagen

Folgende Voraussetzungen müssen erfüllt sein:

- Persönliche E-Mail-Adresse für die Zustellung initialer Kennwörter
- Internetzugang (HTTPS)
- Aktueller Internet Browser

Web Version für UCC-Client

- Chrome
- Firefox
- Safari
- Edge
- Benötigte Browser-Features:
  - JavaScript

- HTML5 Local Storage

myApps for Windows

- Windows 10 oder höher
- Windows Server 2016 oder höher
- 32 & 64 bit Windows

myApps for macOS

- OS X 10.10 oder höher

myApps for iOS

- iOS 12 oder höher

myApps for Android

- Android 6.0 oder höher

Standard Systemgrenzen

Folgende Systemgrenzen sind für eine Standard/Default Cloud PBX definiert:

Pro eingerichtetem Kunde eine Kunden-PBX (IPVA)*

- Eine PBX bekommt einen oder mehrere gesonderte Amtsanschlüsse per SIP-Trunk maximal 16 pro PBX
- Maximale Anzahl von User pro Kunden-PBX – 100 User
- Maximale Anzahl von User pro Kunden-PBX bei Vollauslastung aller Services*** pro User – 70 User
- Gleichzeitig unterstütze Sprachkanäle – 100 Kanäle
- Maximale Anzahl von Konferenzkanälen pro Kunden-PBX – 60 Kanäle
- Maximale Anzahl von Teilnehmern pro Konferenzraum pro Kunden-PBX – 60 Teilnehmer
- Maximale Anzahl von Konferenzräumen pro Kunden-PBX – 4 Konferenzräume
- Maximale Anzahl gleichzeitig nutzbarer Fax-Server-Kanäle – 15 Kanäle**

Die Systemgrenzen können projektbezogen vom Standard aus angepasst bzw. erweitert werden.

*Wenn ein Kunde mehrere Kunden-PBXen (IPVA) benötigt, kann der Kunde mehrmals eingerichtet werden.
**Bei gleichzeitiger Nutzung der VoIP Dieste in Kombination mit UC-Funktionalitäten.
***Eine erfolgreiche Faxübertragung ist abhängig von den unterschiedlichen Verbindungsqualitäten der Providernetze und kann nicht zu 100% garantiert werden.

Anhang

Nr.	Version	Status	Datum	Bearbeiter	Änderungsgrund
1	0.1	Entwurf	03.04.2020	Georg Dachgruber	Erstellung
2	1.0	Freigabe	01.10.2020	Georg Dachgruber	Freigabe
3	2.0	Anpassung	01.12.2020	Georg Dachgruber	Freigabe
4	3.0	Anpassung	14.07.2021	Georg Dachgruber	Freigabe
4	3.1	Freigabe	29.07.2021	Georg Dachgruber	Freigabe
6	4.0	Anpassung	05.01.2021	Uwe Teichert	Erweiterung IP-Ports, Microsoft Safe Links / Defender
7	5.0	Entwurf	09.03.2023		IPv6
8	6.0	Freigabe	17.07.2023	Uwe Teichert	Erweiterung IP-Adressbereiche für Kunden-Firewall

Tabelle 2 Änderungsübersicht Dokument

Hinweis zu Status, Versionierung und Datenklassifizierung.

Status:	
Entwurf	Das Dokument ist in Arbeit
Freigegeben	Das Dokument wurde geprüft und ist freigegeben, es kann nur geändert werden, wenn die Versionsnummer hochgezogen wird.
Ungültig	Das Dokument ist nicht mehr gültig.
Versionierung:	
0.1 – 0.99	Nicht freigegebene Versionen im Entwurf
1.0	**Erste freigegebene Version mit Status “Freigegeben“**
1.1 – 1.99	Versionen im Entwurf, welche die Version A ergänzen oder ändern
2.0	**Zweite freigegeben Version mit Status “Freigegeben”**
Datenklassifizierung	
Öffentlich	Keine Einschränkung

Intern	Nur für interne und externe Kapsch-Mitarbeiter
Vertraulich	**Eingeschränkt auf ausgewählte Active Directory und/ oder Sharepoint-Gruppen (Standard)**
Geheim	Eingeschränkt auf ausgewählte Mitarbeiter, Server-Verschlüsselung erforderlich

- ENDE DES DOKUMENTS -