

# Service SBC pour Trunk SIP, Mitel Dialer OTT et Unify Phone

08/2025

AMT/PTD/PBX/0138/3/2/FR

MANUEL DE MISE EN ŒUVRE



# Avertissement

Bien que les informations contenues dans ce document soient considérées comme pertinentes, Mitel Networks Corporation (MITEL ®) ne peut en garantir l'exactitude.

Les informations sont susceptibles d'être modifiées sans préavis et ne doivent pas être interprétées de quelque façon que ce soit comme un engagement de Mitel, de ses entreprises affiliées ou de ses filiales.

Mitel, ses entreprises affiliées et ses filiales ne sauraient être tenus responsables des erreurs ou omissions que pourrait comporter ce document. Celui-ci peut être revu ou réédité à tout moment afin d'y apporter des modifications.

Aucune partie de ce document ne peut être reproduite ou transmise sous une forme quelconque ou par n'importe quel moyen - électronique ou mécanique – quel qu'en soit le but, sans l'accord écrit de Mitel Networks Corporation.

© Copyright 2025, Mitel Networks Corporation. Tous droits réservés.

Mitel ® est une marque déposée de Mitel Networks Corporation.

Toute référence à des marques tierces est fournie à titre indicatif et Mitel n'en garantit pas la propriété.

# SOMMAIRE

<b>1</b>	<b>À PROPOS DE CE DOCUMENT</b>	<b>4</b>
1.1	OBJET DE CE DOCUMENT	4
1.2	ABRÉVIATIONS	4
1.3	DOCUMENTS DE RÉFÉRENCE	5
1.4	RAPPEL DE LA LOI INFORMATIQUE	5
<b>2</b>	<b>GÉNÉRALITÉS</b>	<b>6</b>
2.1	INTRODUCTION	6
2.2	RAPPEL DE LA PROBLÉMATIQUE DE LA NAT	6
2.3	ARCHITECTURE DU SBC	7
2.3.1	SBC STANDARD ET PBX COLOCALISÉS	7
2.3.2	SBC STANDARD ET PBX COLOCALISÉS ET SÉPARATION LAN/DMZ	8
2.3.3	SBC STANDARD ET PBX SÉPARÉS	9
2.3.4	SBC DAISY CHAIN AVEC PBX COLOCALISÉ	10
2.3.5	SBC DAISY CHAIN AVEC PBX SÉPARÉ	11
2.4	DÉMARRAGE DU SERVICE SBC	13
2.5	LICENCE	13
2.6	NIVEAU DE SÉCURITÉ	13
2.6.1	PRINCIPE	13
2.6.2	CHOIX DU NIVEAU DE SÉCURITÉ	14
2.6.3	GESTION DE LA ALLOW-LIST	16
2.6.4	GESTION DE LA DENY-LIST DOS	16
2.6.5	ÉTAT DU NIVEAU DE SÉCURITÉ LORS D'UNE PREMIÈRE INSTALLATION	17
<b>3</b>	<b>CONFIGURATION DU TRUNK SBC</b>	<b>18</b>
3.1	PARAMÈTRES GÉNÉRAUX DU SERVICE SBC	18
<b>4</b>	<b>CONFIGURATION DES ABONNEMENTS EN MODE OTT</b>	<b>21</b>
4.1	MITEL DIALER OTT	21
4.1.1	PRÉSENTATION DU MITEL DIALER OTT	21
4.1.2	PRÉREQUIS	22
4.1.3	CONFIGURER LE SBC DU MIVOICE 5000	22
4.1.4	CONFIGURER LE MIVOICE 5000 CALL SERVER	27
4.1.5	ACTIVER LE SSO OPENID CONNECT	28
4.1.6	DÉPLOYER LE MITEL DIALER	28
4.1.7	ACCÈS AU USER PORTAL EN MODE OTT	28
4.2	UNIFY PHONE	29
4.2.1	PRÉSENTATION D'UNIFY PHONE	29
4.2.2	PRÉREQUIS	29
4.2.3	CONFIGURER LE SBC DU MIVOICE 5000	30
4.2.4	CONFIGURER CLOUDLINK ET LA CLOUDLINK GATEWAY	33
4.2.5	CONFIGURER LE MIVOICE 5000 CALL SERVER	35

# 1 À PROPOS DE CE DOCUMENT

## 1.1 OBJET DE CE DOCUMENT

Ce document décrit la mise en œuvre du service SBC en environnement MiVoice 5000. Ce document est applicable aux systèmes Mitel suivants :

- MiVoice 5000 Server,
- Mitel 5000 Compact,
- Mitel EX Controller.

## 1.2 ABRÉVIATIONS

<b>Mitel 5000 Gateways</b>	Ce terme regroupe l'ensemble des systèmes, XS, XL et XD
<b>MiVoice 5000 Server</b>	Système de commutation téléphonique hébergé sur un PC Linux
<b>XS, XL, XD</b>	Gateways physiques de la gamme MiVoice 5000.
<b>XS</b>	Ce terme regroupe les systèmes XS, XS12 et XS6
<b>MiVoice 5000 Manager</b>	Centre de gestion d'un parc
<b>CAC</b>	Call Admission Control
<b>DoS</b>	Denial of Service
<b>DDoS</b>	Distributed Denial of Service
<b>DMZ</b>	Zone Démilitarisée
<b>FTP</b>	File Transfer Protocol.
<b>IP</b>	Internet Protocol
<b>ITF</b>	Interface
<b>LAN</b>	Local Area Network
<b>NAT</b>	Network Address Translation
<b>iPBX</b>	IP Private Branch eXchange
<b>PBX</b>	Private Branch eXchange
<b>PKI</b>	Public Key Infrastructure
<b>RHM</b>	Relation Homme Machine, commandes d'un iPBX
<b>RTP</b>	Real Time Protocol
<b>SBC</b>	Session Border Controller
<b>SIP</b>	Session Internet Protocol
<b>VPN</b>	Virtual Private Network
<b>WAN</b>	Wide Area Network

## 1.3 DOCUMENTS DE RÉFÉRENCE

Pour mieux comprendre ce document, se référer aux documents :

- MiVoice 5000 Server - Mise en Service
- MiVoice 5000 Server - Manuel Exploitation
- MiVoice 5000 Manager - Installation et Configuration
- MiVoice 5000 Manager - Guide Utilisateur
- CloudLink – Guide de Déploiement avec MiVoice 5000
- Mitel EX Controller Mitel GX Gateway Mitel AG4100 et TA7100 - Installation et Configuration
- Mitel 5000 Compact – Guide Installation Rapide

Ces documents sont accessibles dans le Document Center de Mitel :  
<https://www.mitel.com/document-center/business-phone-systems/mivoice-5000/technical-documentation>

## 1.4 RAPPEL DE LA LOI INFORMATIQUE

***Il est rappelé à l'utilisateur que la mise en œuvre des autocommutateurs sur les lieux de travail doit satisfaire aux recommandations de la Commission Nationale de l'Informatique et des Libertés en date du 18 septembre 1984.***

***L'attention de l'utilisateur est également attirée sur les dispositions de la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications.***

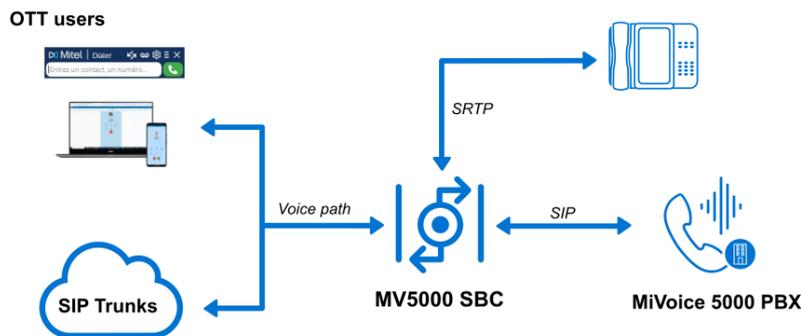
## 2 GÉNÉRALITÉS

### 2.1 INTRODUCTION

Le service SBC est intégré au MiVoice 5000 server, au système Mitel 5000 Compact et au système Mitel EX Controller.

Le service SBC est utilisé dans deux cas de figure, applicables seuls ou en simultanément :

- Pour les trunks SBC, par exemple un trunk SIP nécessitant une gestion de NAT,
- Pour supporter des abonnements en mode OTT, via Unify Phone et/ou le Mitel Dialer OTT.



La mise en œuvre du service est réalisable à partir de la Web Admin et consiste à configurer les différentes adresses IP côté public et privé pour les translations d'adresses dans l'architecture considérée.

Dans le cas d'un EX Controller ou d'un Mitel 5000 Compact avec deux adresses IP :

- Si les adresses IP sont sur la même carte réseau, les adresses IP peuvent être sur le même sous-réseau.
- Si les adresses IP sont sur des cartes réseau différentes, les adresses IP doivent être sur des sous-réseaux différents.

Le service SBC comporte également des évolutions relatives à la sécurité en utilisant des filtres sur des listes d'adresses IP pour se protéger de certaines attaques de type DDoS et DoS.

Le service SBC prend aussi en compte les sessions vocales et/ou vidéo.

### 2.2 RAPPEL DE LA PROBLÉMATIQUE DE LA NAT

Les équipements réseaux NAT (routeurs, pare-feu, etc.) réalisent une traduction d'adresses, pour des raisons de sécurité et/ou de manque d'adresses publiques IPv4 ou IPv6. La traduction d'adresse est exécutée dans l'en-tête d'IP, mais pas toujours sur des adresses IP encapsulées (dans des en-têtes d'application).

Le protocole SIP transporte des adresses IP/ports privés de négociation RTP. Le flux audio (RTP) peut être bloqué par les équipements réseaux NAT du client en raison d'adresses inconnues (non traduites).

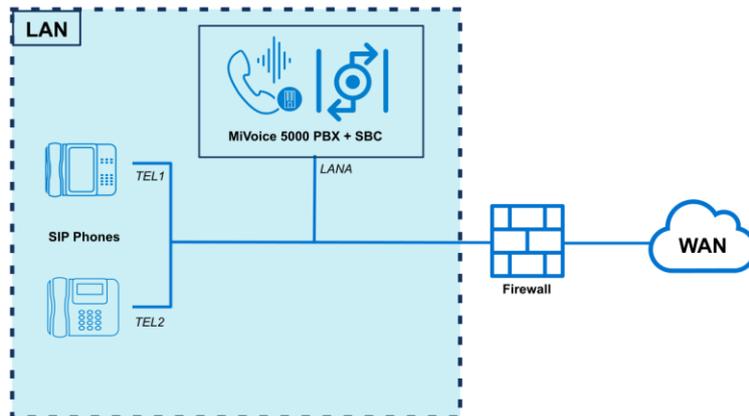
La solution proposée via le service SBC permet d'offrir des services téléphoniques vers un opérateur SIP en transitant par les équipements réseaux du client gérant la NAT et de compenser le cas échéant la NAT pour les équipements réseaux ne gérant pas complètement celle-ci pour les adresses IP encapsulées.

## 2.3 ARCHITECTURE DU SBC

Différents cas d'architecture sont à considérer. Ce paragraphe se concentre sur les cas les plus fréquents en environnement MiVoice 5000.

### 2.3.1 SBC STANDARD ET PBX COLOCALISÉS

L'architecture avec un SBC et un PBX colocalisés est souvent utilisée pour des petites installations.



En fonction de la configuration (utilisation du NAT ou du mode OTT), le menu **RESEAU ET LIAISONS>SBC Trunk** – Onglet **Paramètres généraux** est à remplir de la manière suivante :

Configuration Passerelle internet

Service téléphonie>Réseau et liaisons>Passerelle internet (4.6)

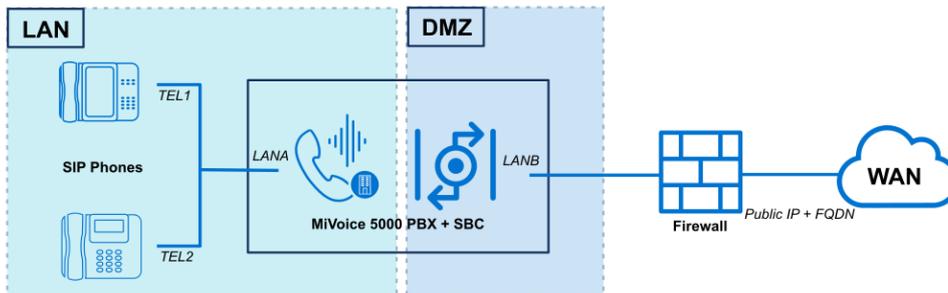
Paramètres généraux	WebRTC	Paramètres de sécurité	Allow-List
Service PASSERELLE INTERNET		ARRETE	
Mode	Standard		
Interface sécurisée	<input checked="" type="checkbox"/>		
Mode de fonctionnement	TRUNK SBC		
Support terminaux OTT	<input checked="" type="checkbox"/>		
- FQDN public SBC	<input type="text"/>		
			<b>FQDN public du SBC (en fonction de la configuration)</b>
Protocoles publics	TLS		
NAT sur l'interface publique	<input checked="" type="checkbox"/>		
- adresse publique	<input type="text"/>		
- port sécurisé (TLS)	5063		
- interface publique	<input type="text"/>		
- port sécurisé (TLS)	5063		
			<b>@IP public du SBC</b>
			<b>@IP LANA</b>
Protocoles privés	TLS		
interface privée	<input type="text"/>		
- port sécurisé (TLS)	5064		
			<b>@IP LANA</b>
NAT sur l'interface privée	<input type="checkbox"/>		
- Adresse ou FQDN de l'iPbx	<input type="text"/>		
- port sécurisé (TLS)	5061		
			<b>@IP LANA</b>

### 2.3.2 SBC STANDARD ET PBX COLOCALISÉS ET SÉPARATION LAN/DMZ

L'architecture avec un SBC et PBX colocalisés et les réseaux LAN et DMZ séparés est privilégiée lorsqu'il y a un besoin d'une adresse IP supplémentaire pour le SBC trunk.



**Rappel :** En cas d'utilisation d'un EX Controller ou d'un Mitel 5000 Compact avec deux cartes réseau, les cartes réseaux doivent être sur deux sous-réseaux différents.



En fonction de la configuration (utilisation du NAT ou du mode OTT), le menu **RESEAU ET LIAISONS>SBC Trunk** – Onglet **Paramètres généraux** est à remplir de la manière suivante :

Configuration Passerelle internet

Service téléphonie>Réseau et liaisons>Passerelle internet (4.6)

**Paramètres généraux** WebRTC Paramètres de sécurité Allow-List

Service PASSERELLE INTERNET

ARRETE

Mode Standard

Interface sécurisée

Mode de fonctionnement TRUNK SBC

Support terminaux OTT

- FQDN public SBC  **FQDN public du SBC (en fonction de la configuration)**

Protocoles publics TLS

NAT sur l'interface publique   
- adresse publique  **@IP public du SBC**

- port sécurisé (TLS) 5063

- interface publique  **@IP LANB**

- port sécurisé (TLS) 5063

Protocoles privés TLS  
interface privée  **@IP LANA**

- port sécurisé (TLS) 5064

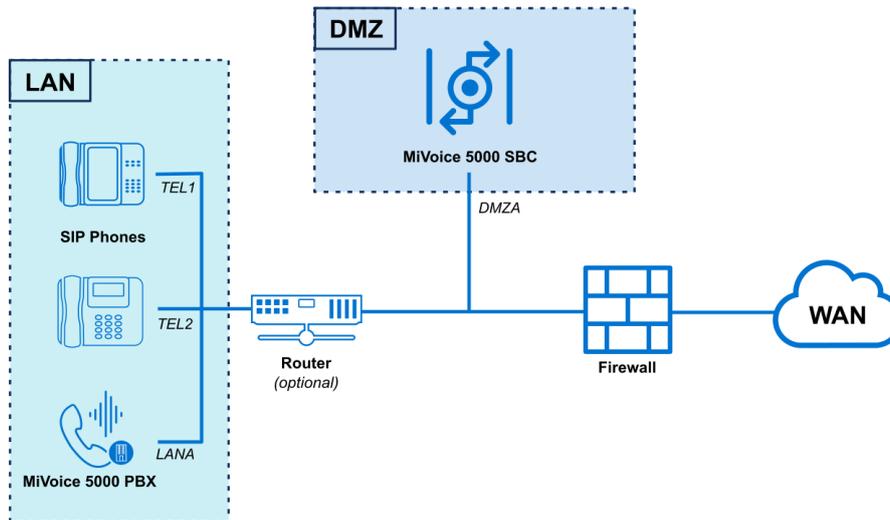
NAT sur l'interface privée

- Adresse ou FQDN de l'iPbx  **@IP LANA**

- port sécurisé (TLS) 5061

### 2.3.3 SBC STANDARD ET PBX SÉPARÉS

L'architecture avec un SBC et un PBX séparés reprend ici un cas d'installation sécurisée avec le SBC en DMZ et PBX en LAN.



**Note :** Si un firewall se trouve entre la DMZ et le LAN, les plages RTP et sous-réseaux des postes doivent avoir accès à la DMZ.

En fonction de la configuration (utilisation du NAT ou du mode OTT), le menu **RESEAU ET LIAISONS>SBC Trunk** – Onglet **Paramètres généraux** du MiVoice 5000 en DMZ est à remplir de la manière suivante :

Configuration Passerelle internet

Service téléphonie>Réseau et liaisons>Passerelle internet (4.6)

**Paramètres généraux** WebRTC Paramètres de sécurité Allow-List

Service PASSERELLE INTERNET

ARRETE

Mode Standard

Interface sécurisée

Mode de fonctionnement TRUNK SBC

Support terminaux OTT

- FQDN public SBC [redacted] **FQDN public du SBC (en fonction de la configuration)**

Protocoles publics TLS

NAT sur l'interface publique   
- adresse publique [redacted] **@IP public du SBC**

- port sécurisé (TLS) 5063

- interface publique [redacted] **@IP DMZA**

- port sécurisé (TLS) 5063

Protocoles privés TLS  
interface privée [redacted] **@IP DMZA**

- port sécurisé (TLS) 5064

NAT sur l'interface privée

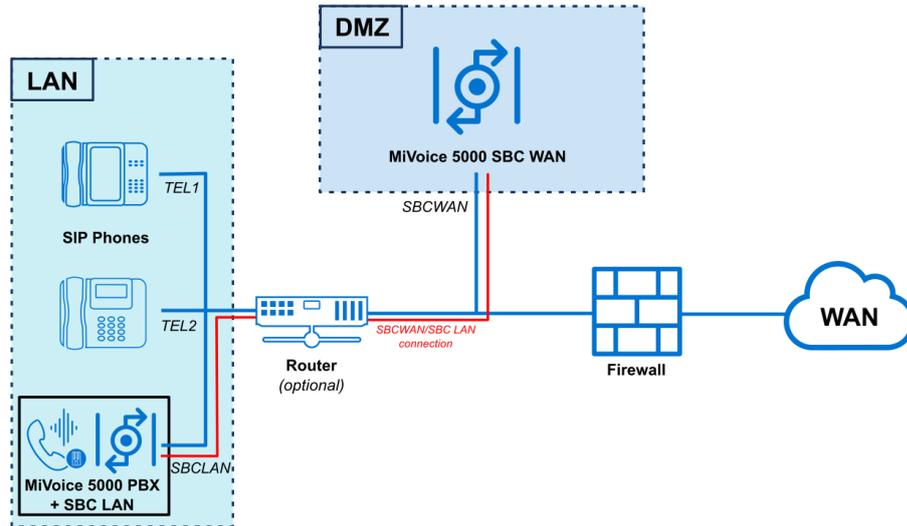
- Adresse ou FQDN de l'iPbx [redacted] **@IP LANA**

- port sécurisé (TLS) 5061

### 2.3.4 SBC DAISY CHAIN AVEC PBX COLOCALISÉ

Dans une configuration Daisy Chain, l'architecture intègre deux SBC distincts :

- Le premier SBC MiVoice 5000 se trouve en DMZ. C'est par ce SBC que vont passer les connexions (SIP TLS, voix, etc.) dans les configurations demandant un SBC. Le SBC en DMZ communique uniquement avec le SBC en LAN, dans ce cas de figure.
- Le second SBC MiVoice 5000 se trouve en LAN. Dans cette configuration précise, le MiVoice 5000 et le SBC en LAN se trouvent sur le même système.



**Note :** Si un firewall se trouve entre la DMZ et le LAN, les ranges RTP doivent avoir accès à la DMZ.

En fonction de la configuration (utilisation du NAT ou du mode OTT), le menu **RESEAU ET LIAISONS>SBC Trunk** – Onglet **Paramètres généraux** est à remplir de la manière suivante :

- Sur le SBC du MiVoice 5000 en DMZ (SBC WAN sur le schéma)

Configuration Passerelle internet  
Service téléphonie>Réseau et liaisons>Passerelle internet (4.6)

**Paramètres généraux** | WebRTC | Paramètres de sécurité | Allow-List

Service PASSERELLE INTERNET ARRETE

Mode	Chainé - élément WAN	
Interface sécurisée	<input checked="" type="checkbox"/>	
Mode de fonctionnement	TRUNK SBC	
Support terminaux OTT	<input checked="" type="checkbox"/>	
- FQDN public SBC		<b>FQDN public du SBC</b> (en fonction de la configuration)
Protocoles publics	TLS	
NAT sur l'interface publique	<input checked="" type="checkbox"/>	
- adresse publique		<b>@IP public du SBC WAN</b>
- port sécurisé (TLS)	5063	
- interface publique		<b>@IP SBC WAN</b>
- port sécurisé (TLS)	5063	
Protocoles privés	TLS	
interface privée		<b>@IP SBCWAN</b>
- port sécurisé (TLS)	5064	
- Adresse ou FQDN de l'élément LAN		<b>@IP SBCLAN</b>
- port sécurisé (TLS)	5063	

- Sur le SBC du MiVoice 5000 en LAN (SBC LAN sur le schéma)

Configuration Passerelle internet

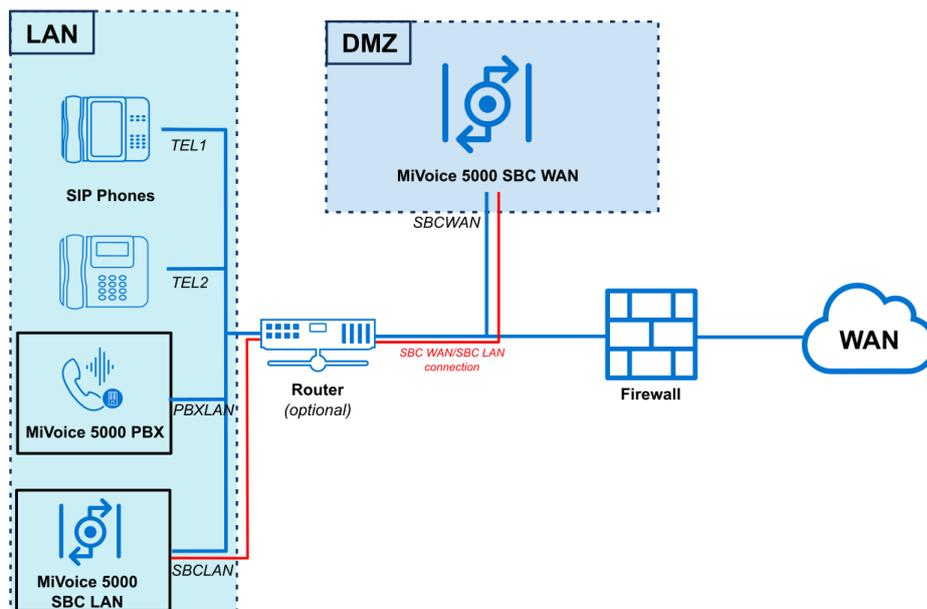
Service téléphonie>Réseau et liaisons>Passerelle internet (4.6)

Paramètres généraux	WebRTC	Paramètres de sécurité	Allow-List
Service PASSERELLE INTERNET		ARRÊTÉ	
Mode	Chainé - élément LAN		
Interface sécurisée	<input checked="" type="checkbox"/>		
Mode de fonctionnement	TRUNK SBC		
Protocoles publics	TLS		
- Adresse ou FQDN de l'élément WAN	[Redacted]		@IP SBC WAN
- port sécurisé (TLS)	5064		
- interface publique	[Redacted]		@IP SBC WAN
- port sécurisé (TLS)	5063		
Protocoles privés	TLS		
interface privée	[Redacted]		@IP SBC WAN
- port sécurisé (TLS)	5064		
NAT sur l'interface privée	<input type="checkbox"/>		
- Adresse ou FQDN de l'iPbx	[Redacted]		@IP PBX LAN
- port sécurisé (TLS)	5061		

### 2.3.5 SBC DAISY CHAIN AVEC PBX SÉPARÉ

Cette architecture est une variante de celle mentionnée dans le chapitre précédent. Ici, le PBX et le SBC en LAN sont sur des systèmes différents.

Contrairement à l'architecture Daisy Chain avec PBX colocalisé, le SBC en DMZ échange avec le SBC en LAN et le PBX.



**Note :** Si un firewall se trouve entre la DMZ et le LAN, les ranges RTP doivent avoir accès à la DMZ.

En fonction de la configuration (utilisation du NAT ou du mode OTT), le menu **RESEAU ET LIAISONS>SBC Trunk** – Onglet **Paramètres généraux** est à remplir de la manière suivante :

- Sur le SBC du MiVoice 5000 en DMZ (SBC WAN sur le schéma)

Configuration Passerelle internet  
Service téléphonie>Réseau et liaisons>Passerelle internet (4.6)

**Paramètres généraux** WebRTC Paramètres de sécurité Allow-List

Service PASSERELLE INTERNET ARRETE

Mode Chaîné - élément WAN

Interface sécurisée

Mode de fonctionnement TRUNK SBC

Support terminaux OTT

- FQDN public SBC  **FQDN public du SBC (en fonction de la configuration)**

Protocoles publics TLS

NAT sur l'interface publique

- adresse publique  **@IP public du SBC WAN**

- port sécurisé (TLS) 5063

- interface publique  **@IP SBC WAN**

- port sécurisé (TLS) 5063

Protocoles privés TLS

interface privée  **@IP SBCWAN**

- port sécurisé (TLS) 5064

- Adresse ou FQDN de l'élément LAN  **@IP SBCLAN**

- port sécurisé (TLS) 5063

- Sur le SBC séparé du MiVoice 5000 en LAN (SBC LAN sur le schéma)

Configuration Passerelle internet  
Service téléphonie>Réseau et liaisons>Passerelle internet (4.6)

**Paramètres généraux** WebRTC Paramètres de sécurité Allow-List

Service PASSERELLE INTERNET ARRETE

Mode Chaîné - élément LAN

Interface sécurisée

Mode de fonctionnement TRUNK SBC

Protocoles publics TLS

- Adresse ou FQDN de l'élément WAN  **@IP SBC WAN**

- port sécurisé (TLS) 5064

- interface publique  **@IP SBC LAN**

- port sécurisé (TLS) 5063

Protocoles privés TLS

interface privée  **@IP SBC LAN**

- port sécurisé (TLS) 5064

NAT sur l'interface privée

- Adresse ou FQDN de l'iPbx  **@IP PBX LAN**

- port sécurisé (TLS) 5061

## 2.4 CONFIGURATION DES INTERFACES RÉSEAU

En fonction de l'équipement MiVoice 5000 utilisé, la configuration des interfaces réseau pour le SBC peut varier.

Pour plus d'informations, se référer aux documents :

- **MiVoice 5000 Server - Mise en Service** pour les MiVoice 5000 Server non virtualisés ou virtualisés,
- **Mitel EX Controller Mitel GX Gateway Mitel AG4100 et TA7100 - Installation et Configuration** pour les Mitel EX Controller,
- **Mitel 5000 Compact - Guide Installation Rapide** pour les Mitel Compact.

## 2.5 DÉMARRAGE DU SERVICE SBC

Le Menu **Service téléphonie>Système>Configuration>Services (2.3.1)** permet de Démarrer, Arrêter ou Redémarrer le service SBC.

## 2.6 LICENCE

Pour utiliser des trunk SBC, le service SBC demande une licence de chiffrement uniquement dans le cas d'un trunk TLS avec SRTP. Sinon, le service SBC ne demande aucune licence.

## 2.7 NIVEAU DE SÉCURITÉ

### 2.7.1 PRINCIPE

Sur le MiVoice 5000 Server et pour les appels trunk uniquement, le SBC fournit les services suivants :

- NAT signalisation/média
- Transport audio/vidéo
- Défense contre les attaques SIP DoS (flooding ou Malicious call) et SIP DDoS
- Qualité de Service (QoS)
- Masquage de la topologie du réseau privé et Centralisation des flux

Le service de sécurité peut être activé pour se protéger d'attaques DoS de type Flooding ou DDoS.

- **DoS**, au moyen d'une liste blanche (adresses IP de confiance) et d'une liste noire
- **DDoS**, au moyen d'un filtre.

Indépendamment de l'activation de la sécurité, le SBC est protégé d'une attaque DoS de type Malicious Call.

La liste blanche (Onglet **Allow-List**) est composée d'adresses IP de confiance déclarées par l'installateur. Ces adresses IP restent néanmoins soumises au contrôle des attaques Malicious Call.

La liste noire (Onglet **Deny-List DoS**) n'est pas configurable et est remplie dynamiquement par les adresses IP considérées comme attaquantes.

Ces adresses IP ont contrevenu aux critères de sécurité définis contre les attaques SIP DoS (flooding ou Malicious call).

Les adresses IP sont renseignées pour une période configurable (indéfinie par défaut). La liste peut également être nettoyée par l'installateur (voir paragraphes suivants).

## 2.7.2 CHOIX DU NIVEAU DE SÉCURITÉ

Menu **RESEAU ET LIAISONS>Passerelle Internet** – Onglet **Paramètres de sécurité**

Le premier paramètre permet de configurer le niveau de sécurité mise en œuvre.

Les choix proposés par la liste de déroulante sont les suivants :

- **Aucun**
- **auto protection**
- **Allow-List seule**

Description des différents choix :

- **Aucun**

L'onglet **Allow-List** n'est pas accessible

Même si la sécurité est désactivée, le contrôle Malicious Call est systématiquement effectué, l'onglet **Deny-List DoS** est proposé.

- **Auto-protection**

Pour le niveau « auto-protection » les onglets **Allow-List** et **Deny-List DoS** servent de filtre.

L'onglet **Allow-List** comporte la liste des adresses IP saisies par l'opérateur.

L'onglet **Deny-List DoS** comporte la liste des adresses IP identifiées par le SBC comme provenant d'équipements considérées comme attaquantes.

Ces adresses IP ont contrevenu aux critères de sécurité définis contre les attaques SIP DoS (flooding ou Malicious call).

Ces adresses sont retirées automatiquement de la liste après une période configurable (une heure par défaut).

Le nombre d'adresses IP dans la **Deny-List** est configurable. Lorsque cette limite est atteinte, les entrées les plus anciennes sont supprimées.

Toute requête venant d'une adresse IP Blacklistée (non répondue).

Il permet de visualiser, à un instant T, les adresses IP n'étant pas dignes de confiance, précédées de la date et de l'heure de l'enregistrement.

- **Allow-List seule**

Dans ce cas, seul l'onglet **Allow-List** est proposé, comportant la liste des adresses IP saisies par l'opérateur.

Il permet de définir manuellement 100 adresses IP de confiance.

- Paramètres relatifs à la sécurité DoS

Les trois paramètres suivants sont relatifs à la sécurité DoS,

- **Seuil** : 10 à 5000 (Nombre de requêtes SIP autorisées par fenêtre avant le blocage des requêtes entrantes)
- **Fenêtre** (secondes) : 2 à 10 (période en secondes d'échantillonnage)
- **Période** : Période après laquelle est effectuée l'effacement du contenu de la Deny-List DoS, les valeurs possibles sont 30 secondes, 5 minutes, 30 minutes, 1 heure, 1 jour, 1 semaine, infinie.

- Paramètres relatifs à la sécurité DDoS

Les deux suivants sont relatifs au DDoS.

- **Seuil** : 10 à 5000 (Nombre de requêtes SIP autorisées par fenêtre avant le blocage des requêtes entrantes)

- **Fenêtre** (secondes) : 2 à 10 (période en secondes d'échantillonnage)
- o Effacement de la Deny-List DoS  
Après confirmation de l'action, ce choix efface toutes les entrées de la Deny-List DoS.

## 2.7.3 GESTION DE LA ALLOW-LIST

### Menu **RÉSEAU ET LIAISONS**> **Passerelle internet** – Onglet **Allow-List**

Configuration Passerelle internet  
Service téléphonie>Réseau et liaisons>Passerelle internet (4.6)

Paramètres généraux WebRTC Paramètres de sécurité **Allow-List** Deny-List DoS Deny-List Force Brute

Adresse IP 1	<input type="text"/>
Adresse IP 2	<input type="text"/>
Adresse IP 3	<input type="text"/>
Adresse IP 4	<input type="text"/>
Adresse IP 5	<input type="text"/>
Adresse IP 6	<input type="text"/>
Adresse IP 7	<input type="text"/>
Adresse IP 8	<input type="text"/>
Adresse IP 9	<input type="text"/>
Adresse IP 10	<input type="text"/>
Adresse IP 11	<input type="text"/>
Adresse IP 12	<input type="text"/>

Dans cet onglet chaque ligne permet la saisie d'une adresse IP.

100 adresses IP de confiance peuvent être saisies.

Un message d'erreur est affiché lors de la validation du champ.

## 2.7.4 GESTION DE LA DENY-LIST DOS

### Menu **RESEAU ET LIAISONS**>**Passerelle internet** – Onglet **Deny-List DoS**

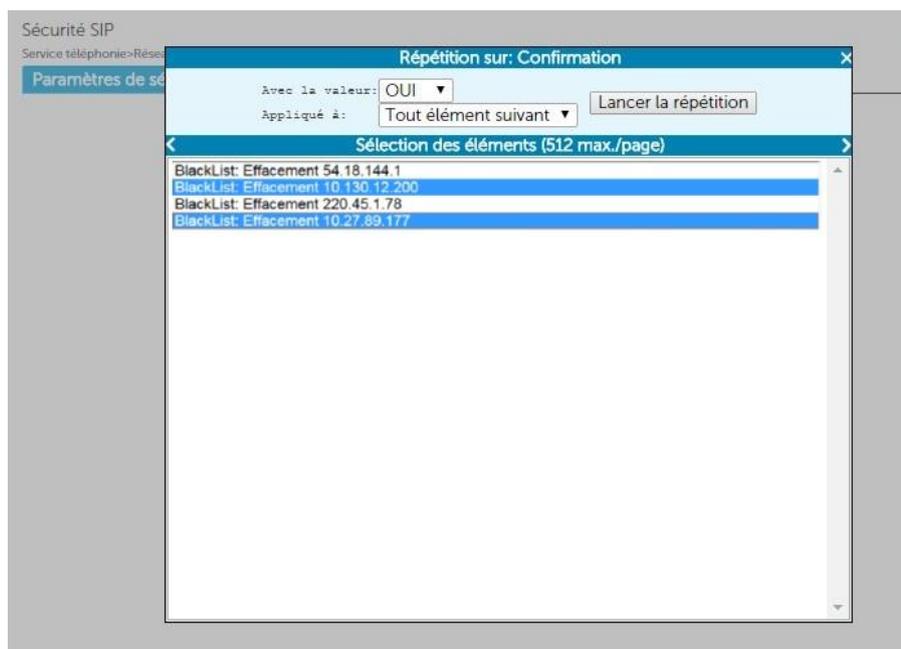
Chaque ligne du tableau présente une adresse blacklistée et permet de sélectionner l'adresse en vue de sa suppression.

Pour supprimer une adresse, cliquer sur le lien hypertexte en première colonne

L'écran suivant demande la suppression de l'adresse sélectionnée. Pour confirmer la procédure, cliquer sur le bouton **Confirmation**.

Après la suppression, le MiVoice 5000 revient automatiquement sur la Deny-List DoS.

Dans l'écran de suppression, la commande répétée est possible, ce qui permet d'effacer une série d'adresses sélectionnées dans la liste des adresses existantes à partir de celle sélectionnée.



## 2.7.5 ÉTAT DU NIVEAU DE SÉCURITÉ LORS D'UNE PREMIÈRE INSTALLATION

Lors d'une première installation, le niveau de sécurité est à **Autoprotection**.

### 3 CONFIGURATION DU TRUNK SBC

#### 3.1 PARAMÈTRES GÉNÉRAUX DU SERVICE SBC



**Rappel :** La configuration des interfaces réseau sont décrites dans les documents d'installation des équipements MiVoice 5000. Se référer aux documents :

- **MiVoice 5000 Server - Mise en Service pour les MiVoice 5000 Server non virtualisés ou virtualisés,**
- **Mitel EX Controller Mitel GX Gateway Mitel AG4100 et TA7100 - Installation et Configuration pour les Mitel EX Controller,**
- **Mitel 5000 Compact - Guide Installation Rapide pour les Mitel Compact.**

Selon l'architecture réseau choisie, le menu **RESEAU ET LIAISONS>Passerelle Internet** – Onglet **Paramètres généraux** permet de définir les différentes adresses et ports associés du service SBC :

Configuration Passerelle internet  
Service téléphonie>Réseau et liaisons>Passerelle internet (4.6)

Paramètres généraux	WebRTC	Paramètres de sécurité	Allow-List	Deny-List
Service <b>PASSERELLE INTERNET</b>		ARRETE		
Mode	Standard			
Interface sécurisée	<input checked="" type="checkbox"/>			
Mixte (MTLS)	<input checked="" type="checkbox"/>			
Mode de fonctionnement	TRUNK SBC			
Support terminaux OTT	<input type="checkbox"/>			
Protocoles publics	TLS			
NAT sur l'interface publique	<input checked="" type="checkbox"/>			
- adresse publique	[Redacted]			@IP1
- port sécurisé (TLS)	5063			
- interface publique	[Redacted]			@IP2
- port sécurisé (TLS)	5063			
Protocoles privés	TLS			
interface privée	[Redacted]			@IP3
- port sécurisé (TLS)	5064			
NAT sur l'interface privée	<input checked="" type="checkbox"/>			
- adresse ou FQDN de l'iPbx vu du SBC	[Redacted]			@IP4
- port sécurisé (TLS)	5061			
- Adresse ou FQDN de l'iPbx	[Redacted]			@IP5
- port sécurisé (TLS)	5061			
Plage de ports SBC :				
- port RTP minimum	20000			
- port RTP maximum	27999			
Changement du port RTP sur renégociation	<input checked="" type="checkbox"/>			
Support du RTP symétrique	NON			
Appliquer le masquage de topologie réseau	<input checked="" type="checkbox"/>			

- **IP1 :** Adresse IP public et le port dédié au service SBC (Utilisé par le client distant pour joindre le SBC)
- **IP2 :** Adresse IP privée et le port de l'interface SBC gérant le trafic public. Cette adresse est à choisir parmi les interfaces du système.

- **IP3** : Adresse IP privée et le port de l'interface SBC gérant le trafic privé. Cette adresse est à choisir parmi les interfaces du système.
- **IP4** : Adresse IP privée et port dédié au service SBC utilise pour joindre l'iPBX.
- **IP5** : Adresse IP de l'iPBX. Par défaut, l'adresse et le port sont ceux du service SIP de l'iPBX.



**Note :** La ligne **Service PASSERELLE INTERNET** indique l'état du service SBC. Pour le modifier, cliquer sur le lien hypertexte qui redirige vers le menu de configuration des services.

### Service PASSERELLE INTERNET

Champ non modifiable. Montre l'état de la passerelle internet.

L'hyperlien redirige vers le menu **Service téléphonie>Système>Configuration>Services (2.3.1)**.

### Mode

Liste déroulante. Permet de choisir le mode de la passerelle internet :

- **Standard** : Mode par défaut, à utiliser dans une configuration SBC
- **Chainé – Élément WAN** : Mode à utiliser dans une configuration Daisy Chain du SBC, sur le MiVoice 5000 en mode WAN.
- **Chainé – Élément LAN** : Mode à utiliser dans une configuration Daisy Chain du SBC, sur le MiVoice 5000 en mode LAN.

### Interface sécurisée

Case à cocher. Paramètre à activer en cas d'utilisation du chiffrement.

### Mode de Fonctionnement

Choix sur liste. Les choix disponibles sont :

- **TRUNK SBC** : Mode dédié au TRUNK SBC
- **Chainé – Element LAN** : Mode dédié au mode Daisy Chain, sur le MiVoice 5000 en mode LAN. Disponible en R8.2 SP2 et versions postérieures.
- **Chainé – Element WAN** : Mode dédié au mode Daisy Chain, sur le MiVoice 5000 en mode WAN. Disponible en R8.2 SP2 et versions postérieures.

### Protocoles publics

Choix sur liste. Visible uniquement si le paramètre **Interface sécurisée** est actif. Les choix disponibles sont :

- TLS
- TLS + UDP/TCP

### NAT sur l'interface publique

L'activation de la case est à réaliser lorsque la NAT est effectuée du côté du réseau public.

- Renseigner les adresses IP1 et IP2 (respectivement adresse et interface publiques SBC).



**Note :** Au niveau du routeur Firewall de l'entreprise, la NAT statique est à réaliser entre IP1 et IP2.

S'il n'y a pas de NAT côté Public (le SBC a une interface avec une adresse IP publique) :

- Renseigner **IP2** seulement.

**IP2** est alors renseigné automatiquement avec la même valeur qu'**IP2**.

### Protocoles privés

Choix sur liste. Visible uniquement si le paramètre **Interface sécurisée** est actif. Les choix disponibles sont :

- TLS
- TLS + UDP/TCP
- UDP/TCP

#### **NAT sur l'interface privée**

L'activation de la case est à réaliser lorsque la NAT est effectuée du côté du réseau privé.

- Renseigner les adresses **IP3** et **IP4** (respectivement interface et adresse privées).

S'il n'y a pas de NAT côté privée :

- Renseigner **IP3** seulement.

**IP5** est alors renseignée automatiquement avec la même valeur qu'**IP3**.

À noter qu'IP1 et IP4 peuvent recevoir toutes les adresses IP possibles. En revanche IP3 et IP4 sont restreintes aux seules adresses IP de la machine sur laquelle est exécutée la RHM.

La sixième adresse (IP5) est celle de l'iPBX avec son port (partie signalisation)

La configuration RTP comprend la plage de variation du port RTP (exemple de 20 000 à 28 000) et le choix de changement du port RTP sur une renégociation SIP (partie flux audio/vidéo). La NAT statique est à réaliser sur le routeur/Firewall si IP1 n'a pas une adresse IP publique.

La saisie erronée d'une adresse IP se traduit par un message « erreur syntaxe ». Les adresses IP 0.0.0.0 et 255.255.255.255 ne sont pas autorisées.

La saisie erronée d'un port RTP se traduit par un message « hors bornes » indiquant la plage de variation possible. Il faut au moins 4 ports pour une communication audio (1RTP public, 1 RTCP public, 1 RTP privé et 1 RTCP privé) et 8 en vidéo.

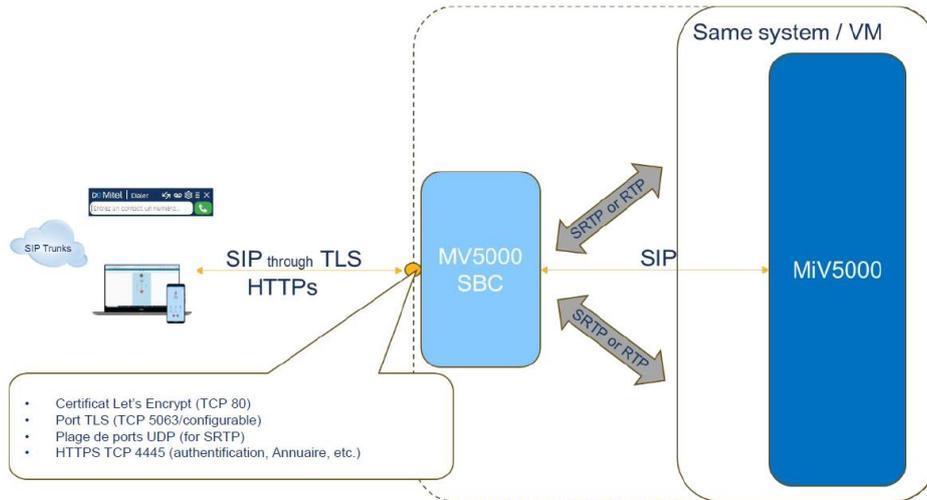
## 4 CONFIGURATION DES ABONNEMENTS EN MODE OTT

### 4.1 MITEL DIALER OTT

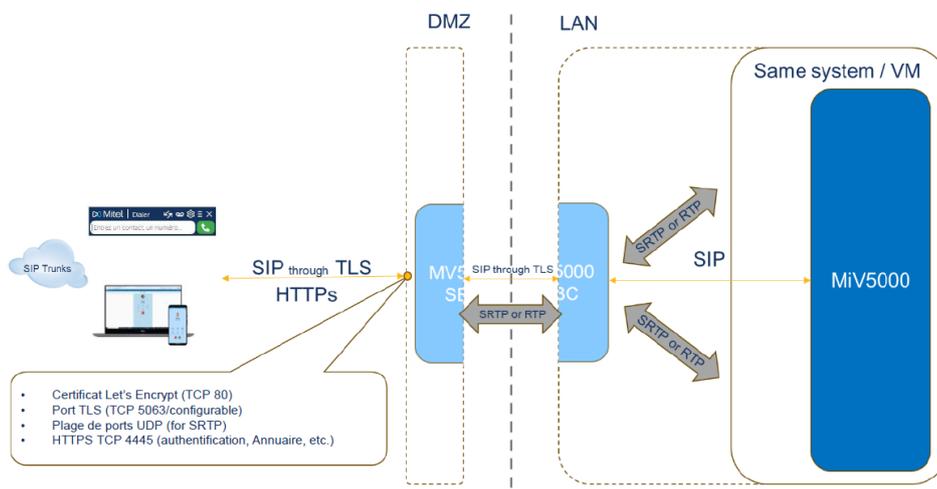
#### 4.1.1 PRÉSENTATION DU MITEL DIALER OTT

Il existe deux cas d'utilisation du Mitel Dialer OTT :

- Configuration SBC standard : Le Mitel Dialer fonctionne avec un MiVoice 5000 SBC de préférence en DMZ, colocalisé ou non avec le MiVoice 5000 Server.



- Configuration SBC Daisy Chain : Le Mitel Dialer fonctionne avec deux MiVoice 5000 SBC en Daisy Chain. Le premier est en DMZ, et le second est en LAN.



Pour plus d'informations sur les architectures possibles avec le SBC, se référer au paragraphe **2.3 – Architecture du SBC**.

La configuration se divise en 3 grandes étapes :

- La configuration du SBC du MiVoice 5000 (R8.2 SP2 minimum)
- La configuration du MiVoice 5000 Call Server (R8.2 SP2 minimum)
- Le déploiement du Mitel Dialer (R4.2 minimum).

## 4.1.2 PRÉREQUIS

Pour configurer le Mitel Dialer OTT, prévoir les éléments suivants :

- Une licence de chiffrement pour le SBC du MiVoice 5000,
- Une licence utilisateur avec l'option Dialer pour le MiVoice 5000,



**Note :** Les informations sur la licence sont disponibles dans le menu **Service téléphonie>Système>Info>Licences**.

- Un certificat importé (PKCS#12 ou PEM) ou Let's Encrypt à attribuer à la passerelle internet,
- 1 adresse IP en DMZ pour l'adresse locale du SBC du MiVoice 5000,
- 1 adresse IP publique pour le SBC du MiVoice 5000,
- 1 FQDN résolu en externe sur cette adresse IP publique,
  - Si utilisation du mode hybride, ce FQDN doit être résolu en interne sur le Call Server,
- Ouvrir des ports sur le firewall externe.

Se référer aux paragraphes :

- **4.1.3.2.1 – Configuration SBC standard pour le Mitel Dialer OTT** pour les ports à ouvrir dans le cas d'une configuration SBC standard
- **4.1.3.2.2 – Configuration SBC Daisy Chain pour le Mitel Dialer OTT** pour les ports à ouvrir dans le cas d'une configuration SBC Daisy Chain



**ATTENTION :** L'utilisation des trunks MTLs empêche l'utilisation du mode OTT. Pour utiliser le Mitel Dialer OTT, désactiver l'option MTLs.



**Rappel :** La configuration des interfaces réseau sont décrites dans les documents d'installation des équipements MiVoice 5000. Se référer aux documents :

- **MiVoice 5000 Server - Mise en Service pour les MiVoice 5000 Server non virtualisés ou virtualisés,**
- **Mitel EX Controller Mitel GX Gateway Mitel AG4100 et TA7100 - Installation et Configuration pour les Mitel EX Controller,**
- **Mitel 5000 Compact - Guide Installation Rapide pour les Mitel Compact.**

## 4.1.3 CONFIGURER LE SBC DU MIVOICE 5000

### 4.1.3.1 CONFIGURER LE CERTIFICAT POUR LA PASSERELLE INTERNET

L'utilisation du SBC demande l'attribution d'un certificat public à la passerelle internet. Il peut s'agir d'un certificat importé (PKCS#12 ou PEM), ou d'un certificat Let's Encrypt.

Menu **Service téléphonie>Système>Sécurité>Gestion des Certificats**, onglet **Affectation des certificats serveurs**

Usage	Nom	Valide depuis	Valide Jusqu'au
Lien Internet			
WebAdmin	SelfSignedSHA2	19/03/24 14 25	17/03/34 14 25
User Portal	SelfSignedSHA2	19/03/24 14 25	17/03/34 14 25
Passerelle Internet	SelfSignedSHA2	19/03/24 14 25	17/03/34 14 25
SIP	SelfSignedSHA2	19/03/24 14 25	17/03/34 14 25
Serveur LDAP	SelfSignedSHA2	19/03/24 14 25	17/03/34 14 25

- Dans la liste déroulante **Certificats présents**, sélectionner le certificat à attribuer à la passerelle internet.

Un tableau avec les informations sur le certificat et une liste de cases à cocher apparaissent.

- Cocher la case **Passerelle Internet**.
- Cliquer sur le bouton **Validation** pour enregistrer les modifications.

#### 4.1.3.2 CONFIGURER LA PASSERELLE INTERNET

##### 4.1.3.2.1 Configuration SBC standard pour le Mitel Dialer OTT

#### Ports à ouvrir sur le firewall

L'usage du Mitel Dialer OTT demande l'ouverture de certains ports sur le firewall externe. Les ports à ouvrir dans une configuration SBC sont les suivants :

- Ports Internet vers DMZ :
  - TCP 4445 pour les services Web nécessaires au Mitel Dialer OTT
  - TCP 5063 pour le SIP TLS et les protocoles publics (port configurable).
  - UDP 20000-27999 pour la voix (configurable).
  - TCP 80 (optionnel) pour l'utilisation d'un certificat Let's Encrypt,
- Port Call Server (LAN) vers SBC en DMZ
  - TCP 5065 pour la configuration du SIP TLS, le port pour les protocoles privés (configurable)
- Si le SBC et le MiVoice 5000 Call Server sont sur des serveurs différents, ouvrir les ports suivants de la DMZ à destination de l'adresse IP du Call Server seulement :
  - TCP 4445 pour les services Web
  - TCP 5061 pour la configuration du SIP TLS, le port pour accéder au Call Server (configurable)
  - UDP 40000-41000 pour la voix (configurable).
- Pour plus d'informations sur les ports, se référer au document **MiVoice 5000 Solution – List of TCP and UDP Ports**.

#### Sur le MiVoice 5000 SBC

Menu **Service téléphonie>Réseau et liaisons>Passerelle internet**

The screenshot displays the 'Configuration Passerelle Internet' page in the Mitel web interface. The 'Mode de fonctionnement' is set to 'TRUNK SBC'. Under 'Protocoles publics', 'NAT sur l'interface publique' is checked, and the 'port sécurisé (TLS)' is set to 5063. Under 'Protocoles privés', 'interface privée' is checked, and the 'port sécurisé (TLS)' is set to 5064. The 'Plage de ports SBC' section shows 'port RTP minimum' at 20000 and 'port RTP maximum' at 27999. The 'Changement du port RTP sur renégociation' checkbox is also checked.

- Sur la liste déroulante **Mode de fonctionnement**, Sélectionner **Standard**.

- Vérifier que la case **Interface sécurisée** est cochée.
- Cocher la case **Support Terminaux OTT**.  
Un nouveau champ apparait.
  - Dans le champ **FQDN public SBC**, entrer le FQDN résolu en externe sur l'adresse IP publique prévu pour le Mitel Dialer OTT.
- Si la case Mixte (MTLS) est visible, vérifier que la case **Mixte (MTLS)** est décochée.
- La configuration du Mitel Dialer OTT utilise le TLS. Pour le paramètre **Protocoles publics**, il est possible de sélectionner **TLS**, ou **TLS + UDP/TCP** pour supporter un trunk UDP en même temps.
- Sous la case **NAT sur l'interface publique** :
  - Sur le champ **interface publique**, entrer l'adresse IP publique prévue pour le Mitel Dialer OTT.



**Note :** Le champ **adresse publique** est visible uniquement si la case **NAT sur l'interface publique** est cochée.

- Vérifier que le champ **interface publique** est sur l'adresse IP publique du SBC, en fonction de la configuration prévue.
- Dans les champs **port sécurisé (TLS)**, entrer le port destiné au TLS (par défaut 5063)
- La configuration du Mitel Dialer OTT utilise le TLS. Pour le paramètre **Protocoles privés**, il est possible de sélectionner **TLS** ou **TLS + UDP/TCP** pour supporter un trunk UDP en même temps.
- Dans le champ **Adresse ou FQDN de l'ipbx**, entrer l'adresse du Call Server.
- Configurer les champs **port RTP minimum** (par défaut 20000) et **port RTP maximum** (par défaut 27999) en fonction de la configuration du système.

#### Menu **Service téléphonie>Système>Configuration>Services**

The screenshot shows the 'Gestion des services' page in the Mitel web interface. The page title is 'Service téléphonie - Système - Configuration - Services (2.1.1)'. On the left, there is a navigation menu with options like 'Accueil Web Admin', 'Abonnés', 'Système', 'Configuration', 'Services', 'Plan de numérotation', 'Réseau et liaisons', 'Accués', 'Messagerie et tonalités', and 'Liens rapides'. The main content area displays a list of services with their status. The 'Service PASSERELLE INTERNET' is highlighted with a red box and has a dropdown menu set to 'DEMARRE'. Other services listed include Service LDAP, Service WFB, Service SNMP, Service SNMP TRAP, Service XGNT/SNMP, Service SIP, Service FTP, Service TFTP, Service SSH, Service SYSLOG, Service POSTFS, Service MEDIA SERVER, Service VPN TTI, Service PROXY LDAP, Service CLD, and Service NTP.

Service	Statut
Service LDAP	DEMARRE
Service WFB	DEMARRE
Service SNMP	DEMARRE
Service SNMP TRAP	DEMARRE
Service XGNT/SNMP	DEMARRE
Service SIP	DEMARRE
Service FTP	DEMARRE
Service TFTP	DEMARRE
Service SSH	DEMARRE
Service SYSLOG	DEMARRE
Service POSTFS	DEMARRE
Service MEDIA SERVER	DEMARRE
<b>Service PASSERELLE INTERNET</b>	<b>DEMARRE</b>
Service VPN TTI	ARRÊTÉ
Service PROXY LDAP	DEMARRE
Service CLD	DEMARRE
Service NTP	DESACTIVÉ

- Vérifier que le paramètre **Service PASSERELLE INTERNET** est sur **DEMARRE**.

#### 4.1.3.2.2 Configuration SBC Daisy Chain pour le Mitel Dialer OTT

##### Ports à ouvrir sur le firewall

L'usage du Mitel Dialer OTT demande l'ouverture de certains ports sur le firewall externe. Les ports à ouvrir dans une configuration Daisy Chain sont les suivants :

- Ports Internet vers SBC en DMZ :
  - TCP 4445 pour les services Web nécessaires au Mitel Dialer OTT
  - TCP 5063 pour le SIP TLS, pour les protocoles publics (port configurable).
  - UDP 20000-27999 pour la voix (configurable).
  - TCP 80 (optionnel) pour l'utilisation d'un certificat Let's Encrypt,
- Port DMZ vers le LAN à destination de l'adresse IP de du SBC LAN uniquement
  - TCP 4445 pour les services Web
  - TCP 5063 pour le SIP TLS, pour accéder à l'iPbx (configurable)
  - UDP 20000-27999 pour la voix (configurable).
- Port SBC en LAN vers SBC en WAN
  - TCP 5065 pour le SIP TLS, pour les protocoles privés du SBC en WAN (port configurable).

Pour plus d'informations sur les ports, se référer au document **MiVoice 5000 Solution – List of TCP and UDP Ports**.

##### Sur le MiVoice 5000 SBC en mode WAN :

- Sur la liste déroulante **Mode de fonctionnement**, Sélectionner **Chainé – Élément WAN**.
- Vérifier que la case **Interface sécurisée** est cochée.
- Vérifier que la case **Mixte (MTLS)** est décochée.
- Cocher la case **Support Terminaux OTT**.  
Un nouveau champ apparaît.
  - Dans le champ **FQDN public SBC**, entrer le FQDN publique du SBC.
- Dans la liste déroulante **Protocoles publics**, sélectionner **TLS**.
- Vérifier que le champ **interface publique** est sur la bonne adresse IP, en fonction de la configuration prévue.
- Sous le paramètre **interface privée** :
  - Dans le champ **Adresse ou FQDN de l'élément LAN**, entrer l'adresse du SBC LAN.
  - Dans le champ **port sécurisé (TLS)**, entrer le port destiné au TLS (par défaut 5063)
- Configurer les champs **port RTP minimum** (par défaut 20000) et **port RTP maximum** (par défaut 27999) en fonction de la configuration du système.

**Sur le MiVoice 5000 SBC en mode LAN :**

- Sur la liste déroulante **Mode de fonctionnement**, Sélectionner **Chainé – Élément LAN**.
- Vérifier que la case **Interface sécurisée** est cochée.
- En fonction de la configuration voulue, il est possible de cocher la case MTLS.
- Dans la liste déroulante **Protocoles publics**, sélectionner **TLS**.
- Sous le paramètre **Protocoles publics** :
  - Sur le champ **adresse de l'élément WAN**, entrer l'adresse du SBC WAN.
  - Vérifier que le champ **interface publique** est sur la bonne adresse IP, en fonction de la configuration prévue.
  - Dans le deuxième champ **port sécurisé (TLS)**, entrer le port destiné au TLS (par défaut 5063)
- Sous le paramètre NAT sur l'interface privée
  - Dans le champ **Adresse ou FQDN de l'iPbx**, entrer l'adresse du Call Server.
  - Dans le champ **port sécurisé (TLS)**, entrer le port destiné au TLS (par défaut 5061)
- Configurer les champs **port RTP minimum** (par défaut 20000) et **port RTP maximum** (par défaut 27999) en fonction de la configuration du système.

## 4.1.4 CONFIGURER LE MIVOICE 5000 CALL SERVER

### 4.1.4.1 VÉRIFIER LE CHIFFREMENT DE LA VOIX ET GÉNÉRER LE HASH

Menu **Service téléphonie>Réseau et liaisons>Qualité de service>Chiffrement et paramètres IP**

- Vérifier que la case **chiffrement voix** est cochée.
- Vérifier si un hash existe déjà, via le champ **Chemin pour le téléchargement des fichiers**.

Si le MiVoice 5000 a déjà un hash, passer au chapitre **2.4.3 – Activer le SSO OpenId Connect**.



**ATTENTION :** Générer un nouveau hash dans ce cas de figure impactera tous les postes RemoteWorker déployés.

Si le MiVoice 5000 n'a aucun hash :

- Sur la liste déroulante **Génération du hash**, sélectionner **OUI**.
- Un Pop-up apparaît pour avertir du risque en cas de nouvelle génération du hash. Cliquer sur le bouton **OK** pour fermer le pop-up.
- Cliquer sur le nouveau bouton **Confirmation**.
- Un nouveau champ apparaît avec le hash généré.

### 4.1.4.2 VÉRIFIER LES DÉTAILS OTT DU MITEL DIALER

Menu **Service téléphonie>Abonnés>Terminaux et Applications>Dialer**

Ce menu affiche les informations spécifiques au Dialer OTT. Ces informations sont par défaut cachées.

- Cocher la case **Détails OTT** pour afficher les informations spécifiques au Mitel Dialer OTT.
- Vérifier que le port dans le champ **Port SIP/TLS** correspond au port dédié au SIP TLS au niveau du SBC du MiVoice 5000.



**ATTENTION :** Si le port SIP/TLS change après la procédure, modifier le port via le menu **Service téléphonie>Réseau et liaisons>Passerelle internet**. Le **MiVoice 5000 Server** récupère automatiquement le port pour l'assigner à ce champ.

- Le champ Hash chiffré affiche le hash dédié au Mitel Dialer OTT. Le champ dépend du hash dans le menu **Service téléphonie>Réseau et liaisons>Qualité de service>Chiffrement et paramètres IP**.

Si le champ ne s'affiche pas, vérifier que le hash du menu **Service téléphonie>Réseau et liaisons>Qualité de service>Chiffrement et paramètres IP** est bien généré. Se référer au paragraphe **4.1.4.2 – Vérifier le chiffrement et générer le hash**.

#### 4.1.5 ACTIVER LE SSO OPENID CONNECT

Le SSO OpenID Connect doit être actif pour les utilisateurs. C'est la méthode d'authentification qu'utilise le Mitel Dialer.

L'activation et configuration du SSO OpenID Connect se fait via le menu **Abonnés>Droits>Paramètres généraux**, onglet **SSO**.



**Note :** Si le SSO via Open ID Connect est déjà configuré sur le **MiVoice 5000 Server**, il faut :

Configurer un nouveau lien de redirection sur l'application existante Microsoft Azure au format [https://\[SBC FQDN\]:4445/sso-oidc](https://[SBC FQDN]:4445/sso-oidc)

Vérifier si chaque abonné utilisant le Mitel Dialer OTT a une adresse mail sur sa fiche abonné, pour qu'ils puissent se connecter.

Si l'installateur doit configurer le SSO OpenID Connect, se référer au document **MiVoice 5000 Server – Manuel Exploitation**, paragraphe **3.9.1.1 – Onglet SSO**.

#### 4.1.6 DÉPLOYER LE MITEL DIALER



**ATTENTION :** **Mitel Dialer OTT est compatible avec Mitel Dialer R4.2 ou version postérieure.**

Les méthodes de déploiement du Mitel Dialer sont disponibles dans le document **Mitel Dialer R4.2 - Guide Installation et Utilisateur**.

#### 4.1.7 ACCÈS AU USER PORTAL EN MODE OTT

Grâce à la configuration du mode OTT à travers le SBC du MiVoice 5000, le User Portal devient accessible en mode OTT.

L'accès peut se faire par le lien [https://\[SBC FQDN\]:4445/userportal/](https://[SBC FQDN]:4445/userportal/), où **SBC FQDN** représente le FQDN résolu sur l'adresse IP du SBC.

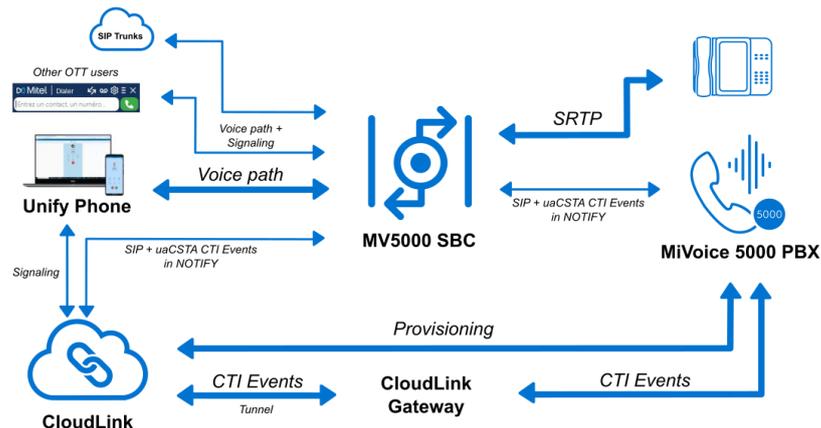
## 4.2 UNIFY PHONE

### 4.2.1 PRÉSENTATION D'UNIFY PHONE

Unify Phone est une application utilisable sur Android, IOS et PC via navigateur.

Pour son bon fonctionnement, Unify Phone utilise plusieurs services Mitel :

- CloudLink pour le provisioning
- La CloudLink Gateway pour les événements CTI,
- Le MiVoice 5000 et le SBC du MiVoice 5000 pour les voix.



Une architecture SBC standard est recommandée pour Unify Phone. L'architecture SBC Daisy Chain reste possible. Pour plus d'informations sur les architectures possibles avec le SBC, se référer au paragraphe **2.3 – Architecture du SBC**.

La configuration se divise en 3 grandes étapes :

- La configuration du SBC du MiVoice 5000 (R8.2 SP3 minimum),
- Le déploiement et la configuration de CloudLink, CloudLink Daemon et la CloudLink Gateway,
- La configuration du MiVoice 5000 Call Server (R8.2 SP3 minimum).

### 4.2.2 PRÉREQUIS

Pour configurer Unify Phone, prévoir les éléments suivants :

- Une licence de chiffrement pour le SBC du MiVoice 5000,
- Une licence utilisateur pour Unify Phone,



**Note :** Les informations sur la licence sont disponibles dans le menu **Service téléphonie>Système>Info>Licences**.

- 1 adresse IP publique fixe,
- Le déploiement de CloudLink et d'une CloudLink Gateway. Pour plus d'informations sur l'installation et la configuration de CloudLink et de CloudLink Gateway, se référer au document **CloudLink – Déploiement avec MiVoice 5000**.

- Ouvrir des ports sur le firewall externe :

Se référer aux paragraphes :

- **4.2.3.2.1 – Configuration SBC Standard pour Unify Phone** pour une configuration SBC standard

- **4.2.3.2.2 – Configuration Daisy Chain pour Unify Phone** pour une configuration SBC Daisy Chain

L'élément suivant est facultatif :

- 1 FQDN résolu en externe sur l'adresse IP publique. Le FQDN est obligatoirement associé à un certificat délivré par une autorité publique.



**ATTENTION :** L'utilisation des trunks MTLS empêche l'utilisation du mode OTT. Pour utiliser Unify Phone et le mode OTT, désactiver l'option MTLS. Si un utilisateur MiVoice 5000 est connecté à MiCollab et Unify Phone en même temps, la synchronisation de la présence Microsoft Teams ne fonctionnera pas pour MiCollab et Unify Phone.



**Rappel :** La configuration des interfaces réseau sont décrites dans les documents d'installation des équipements MiVoice 5000. Se référer aux documents :

- **MiVoice 5000 Server - Mise en Service pour les MiVoice 5000 Server non virtualisés ou virtualisés,**
- **Mitel EX Controller Mitel GX Gateway Mitel AG4100 et TA7100 - Installation et Configuration pour les Mitel EX Controller,**
- **Mitel 5000 Compact - Guide Installation Rapide pour les Mitel Compact.**

## 4.2.3 CONFIGURER LE SBC DU MIVOICE 5000

### 4.2.3.1 CONFIGURER LE CERTIFICAT POUR LA PASSERELLE INTERNET

L'utilisation du SBC demande l'attribution d'un certificat à la passerelle internet.

Pour Unify Phone, si la passerelle internet n'a aucun certificat affecté, le MiVoice 5000 Server lui attribue un certificat par défaut appelé defaultGW. L'installateur peut aussi remplacer le certificat par défaut par un certificat Trusted ou Let's Encrypt.

Le certificat affecté à la passerelle internet est visible via le Menu **Service téléphonie>Système>Sécurité>Gestion des Certificats**, onglet **Affectation des certificats serveurs**

Usage	Nom	Valide depuis	Valide Jusqu'au
Lien InterSite			
WebAdmin	SelfSignedSHA2	19/03/24 13 25	17/03/34 13 25
User Portal	SelfSignedSHA2	19/03/24 13 25	17/03/34 13 25
Passerelle Internet	defaultGW	24/02/25 10 33	25/02/26 10 33
SIP	SelfSignedSHA2	19/03/24 13 25	17/03/34 13 25
Serveur LDAP	SelfSignedSHA2	19/03/24 13 25	17/03/34 13 25
TLS			

### 4.2.3.2 CONFIGURER LA PASSERELLE INTERNET

#### 4.2.3.2.1 Configuration SBC standard pour Unify Phone

##### Ports à ouvrir sur le firewall

L'usage de Unify Phone demande l'ouverture de certains ports sur le firewall externe. Les ports à ouvrir dans une configuration SBC standard sont les suivants :

- Ports Internet vers WAN :
  - TCP 5063 pour le SIP TLS et les protocoles publics (port configurable).

- UDP 20000-27999 pour la voix (configurable).
- TCP 80 (optionnel) pour l'utilisation d'un certificat Let's Encrypt,
- Port Call Server (LAN) vers SBC en WAN
  - TCP 5065 pour la configuration du SIP TLS, le port pour les protocoles privés (configurable)
- Si le SBC et le MiVoice 5000 Call Server sont sur des serveurs différents, ouvrir les ports suivants du WAN à destination de l'adresse IP du Call Server seulement :
  - TCP 5061 pour la configuration du SIP TLS, le port pour accéder au Call Server (configurable)
  - UDP 40000-41000 pour la voix (configurable).
- Pour plus d'informations sur les ports, se référer au document **MiVoice 5000 Solution – List of TCP and UDP Ports**.

#### Menu **Service téléphonie>Réseau et liaisons>Passerelle internet**

- Sur la liste déroulante **Mode de fonctionnement**, Sélectionner **Standard**.
- Vérifier que la case **Interface sécurisée** est cochée.
- Si la case Mixte (MTLS) est visible, vérifier qu'elle est décochée.
- Cocher la case **Support Terminaux OTT**.  
Un nouveau champ apparaît.
  - Dans le champ **FQDN public SBC**, si la configuration comprend un certificat signé par une autorité publique, entrer le FQDN résolu en externe sur l'adresse IP publique.
- La configuration d'Unify Phone utilise le TLS. Pour le paramètre **Protocoles publics**, il est possible de sélectionner **TLS**, ou **TLS + UDP/TCP** pour supporter un trunk UDP en même temps.
- Sous la case **NAT sur l'interface publique** :
  - Sur le champ **interface publique**, entrer l'adresse IP publique prévue pour Unify Phone.
  - Vérifier que le champ **interface publique** est sur la bonne adresse IP, en fonction de la configuration prévue.
  - Dans les champs **port sécurisé (TLS)**, entrer le port destiné au TLS (par défaut 5063)
- La configuration d'Unify Phone utilise le TLS. Pour le paramètre **Protocoles privés**, il est possible de sélectionner **TLS** ou **TLS + UDP/TCP** pour supporter un trunk UDP en même temps.
- Dans le champ **Adresse ou FQDN de l'iPbx**, entrer l'adresse IP ou le FQDN du Call Server.
- Configurer les champs **port RTP minimum** (par défaut 20000) et **port RTP maximum** (par défaut 27999) en fonction de la configuration du système.

#### Menu **Service téléphonie>Système>Configuration>Services**

- Vérifier que le paramètre Service PASSERELLE INTERNET est sur DEMARRE.

#### 4.2.3.2.2 Configuration SBC Daisy Chain pour Unify Phone

##### **Ports à ouvrir sur le firewall**

L'usage de Unify Phone demande l'ouverture de certains ports sur le firewall externe. Les ports à ouvrir dans une configuration Daisy Chain sont les suivants :

- Ports Internet vers SBC en WAN :
  - TCP 5063 pour le SIP TLS, pour les protocoles publics (port configurable).
  - UDP 20000-27999 pour la voix (configurable).
  - TCP 80 (optionnel) pour l'utilisation d'un certificat Let's Encrypt,
- Port WAN vers le LAN à destination de l'adresse IP de du SBC LAN uniquement
  - TCP 5063 pour le SIP TLS, pour accéder à l'iPbx (configurable)
  - UDP 20000-27999 pour la voix (configurable).
  - TCP 4445 (optionnel) pour les services Web
- Port SBC en LAN vers SBC en WAN
  - TCP 5065 pour le SIP TLS, pour les protocoles privés du SBC en WAN (port configurable).

Pour plus d'informations sur les ports, se référer au document **MiVoice 5000 Solution – List of TCP and UDP Ports**.

#### Sur le MiVoice 5000 SBC en mode WAN :

- Sur la liste déroulante **Mode de fonctionnement**, Sélectionner **Chainé – Élément WAN**.
- Vérifier que la case **Interface sécurisée** est cochée.
- Vérifier que la case **Mixte (MTLS)** est décochée.
- Cocher la case **Support Terminaux OTT**.  
Un nouveau champ apparait.
  - Dans le champ **FQDN public SBC**, si la configuration comprend un certificat signé par une autorité public, entrer le FQDN résolu en externe sur l'adresse IP publique.
- Dans la liste déroulante **Protocoles publics**, sélectionner **TLS**.
- Vérifier que le champ **interface publique** est sur la bonne adresse IP, en fonction de la configuration prévue.
- Sous le paramètre **interface privée** :
  - Dans le champ **Adresse ou FQDN de l'élément LAN**, entrer l'adresse du SBC LAN.
  - Dans le champ **port sécurisé (TLS)**, entrer le port destiné au TLS (par défaut 5063)
- Configurer les champs **port RTP minimum** (par défaut 20000) et **port RTP maximum** (par défaut 27999) en fonction de la configuration du système.

#### Sur le MiVoice 5000 SBC en mode LAN :

- Sur la liste déroulante **Mode de fonctionnement**, Sélectionner **Chainé – Élément LAN**.
- Vérifier que la case **Interface sécurisée** est cochée.
- En fonction de la configuration voulue, il est possible de cocher la case **Mixte (MTLS)**.
- Dans la liste déroulante **Protocoles publics**, sélectionner **TLS**.
- Sous le paramètre **Protocoles publics** :

- Sur le champ **adresse de l'élément WAN**, entrer l'adresse du SBC WAN.
- Vérifier que le champ **interface publique** est sur la bonne adresse IP, en fonction de la configuration prévue.
- Dans le deuxième champ **port sécurisé (TLS)**, entrer le port destiné au TLS (par défaut 5063)
- Sous le paramètre NAT sur l'interface privée
  - Dans le champ **Adresse ou FQDN de l'iPbx**, entrer l'adresse du Call Server.
  - Dans le champ **port sécurisé (TLS)**, entrer le port destiné au TLS (par défaut 5061)
- Configurer les champs **port RTP minimum** (par défaut 20000) et **port RTP maximum** (par défaut 27999) en fonction de la configuration du système.

## 4.2.4 CONFIGURER CLOUDLINK ET LA CLOUDLINK GATEWAY

### 4.2.4.1 PRÉREQUIS

L'utilisation du Unify Phone nécessite une CloudLink Gateway.

Pour cela, l'installateur doit :

- Déployer CloudLink avec le MiVoice 5000
- Déployer une CloudLink Gateway
- Configurer CloudLink Daemon
- Configurer Unify Phone sur CloudLink.

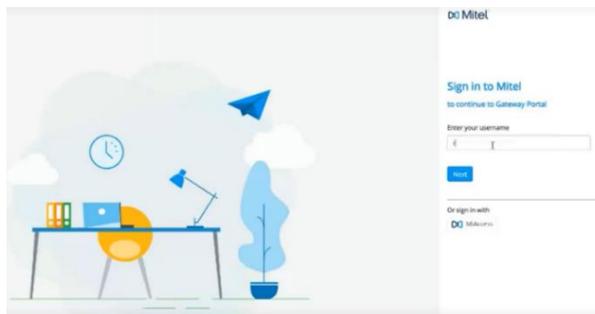
Ce paragraphe décrit la dernière étape, soit les configurations à faire sur CloudLink pour Unify Phone.

Pour plus d'informations sur le déploiement de CloudLink et la CloudLink Gateway, et la configuration de CloudLink Daemon, se référer au document **CloudLink – Guide de Déploiement avec MiVoice 5000**.

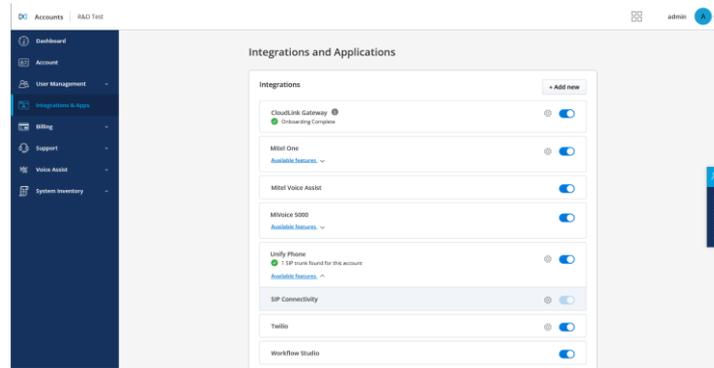
### 4.2.4.2 PROCÉDURE DE CONFIGURATION D'UNIFY PHONE SUR CLOUDLINK

Après avoir déployé la CloudLink Gateway :

- Se connecter en HTTP au portail CloudLink Gateway via l'adresse IP de la CloudLink Gateway définie au niveau du serveur DHCP.



- Cliquer sur le menu **Integrations & Apps**.



**Note :** Cette interface est aussi disponible dans le menu **Account**, section **Integrations**.

- Cliquer sur le bouton **+ Add new**.

Une fenêtre s'affiche avec la liste des intégrations disponibles.

- Dans l'onglet **Mitel**, chercher l'intégration **Unify Phone** et cliquer sur le bouton **Add** associé.
- Cliquer sur **Done** pour fermer la fenêtre.
- Cliquer sur le rouage de la ligne **Unify Phone** pour configurer Unify Phone.

Une nouvelle fenêtre s'affiche et demande un tenant pour Unify Phone.

- Renseigner les coordonnées d'une instance CloudLink pour Unify Phone :

#### Unify Phone Configuration

##### Tenant Details

Tenant Name	<input type="text"/>
First Name	<input type="text"/>
Last Name	<input type="text"/>
Email	<input type="text"/>
	<input type="text" value="+33"/>

Remove

Cancel

- Cliquer sur l'hyperlien **Available features** pour afficher le paramètre **SIP Connectivity**.
- Cliquer sur le rouage de la ligne **SIP Connectivity** pour configurer le point de connexion SIP externe.

Une nouvelle fenêtre s'affiche et demande un trunk SIP pour Unify Phone. CloudLink récupère automatiquement les trunks SIP utilisables pour Unify Phone.

- Sélectionner le trunk SIP à utiliser :

### SIP Connectivity Configuration

Please configure your primary SIP Proxy Mitel Border Gateway.

The configuration will create a SIP trunk between the identified Mitel Border Gateway and the Unify Phone Platform, and a SIP trunk between the PBX and the same Mitel Border Gateway.

PBX Type\*  
MiVoice 5000

Q Search

<input type="checkbox"/>	TRUNK NAME	TLS PORT	PBX	FQDN/IP ADDRESS
<input type="checkbox"/>	PrimarySipTrunk	5063		

[+ Add SIP Trunk](#) v

Done

## 4.2.5 CONFIGURER LE MIVOICE 5000 CALL SERVER



**ATTENTION :** Avant de configurer le MiVoice 5000 Call Server, lancer une resynchronisation entre le PBX et CloudLink via le menu CloudLink > Connexion, onglet Connexion.

La resynchronisation assure l'affichage des paramètres CloudLink et Unify Phone sur le MiVoice 5000.

### 4.2.5.1 VÉRIFIER LE CHIFFREMENT DE LA VOIX

Menu **Service téléphonie**>**Réseau et liaisons**>**Qualité de service**>**Chiffrement et paramètres IP**

Mitel | Service téléphonie

Chiffrement et paramètres IP (mode basique)

Chiffrement - QoS - QoS Externe

Chiffrement signalisation et voix

chiffrement voix

type de chiffrement AES 256

Chiffrement voix (7xx)

état fonction CLEF INEXISTANTE

allée à jour le ..... 4d .....

mode de fonctionnement ESCLAVE

chiffrement AUTORISE

Génération du hash NON

- Chemin pour le téléchargement des fichiers

Vérifier que la case **chiffrement voix** est cochée.

### 4.2.5.2 CONFIGURER LE COMPTE UTILISATEUR CG7450

Pour que Unify Phone puisse gérer la présence, il est nécessaire de configurer un compte utilisateur avec un profil interface XML. Par défaut, le MiVoice 5000 crée le compte cg7450 avec ce profil.

Menu **Service téléphonie**>**Système**>**Configuration**>**Utilisateurs**>**Définition des utilisateurs**

Mitel | Service téléphonie

Sélection d'un utilisateur

Service téléphonie>Système>Configuration>Utilisateurs>Définition des utilisateurs (2/3/3)

ID	Nom du compte	Nom du profil	Lang
0001	cg7450	INTERFACE XML	FRA
0002	admin	INSTALLATEUR	FRA
0003	adminen	INSTALLATEUR	ANG
0004	easyadmin	EASY ADMIN	FRA
0005	easyadminen	EASY ADMIN	FRA
0006	test	ANNUAIRE	FRA
0007			
0008			
0009			

Dans le tableau listant les comptes utilisateur, sélectionner l'abonné cg7450 (ou le compte utilisateur avec en nom de profil INTERFACE XML).

Vérifier si le champ Mot de passe est vide. Si le champ est vide, le compte cg7450 est inactif. Pour activer le compte :

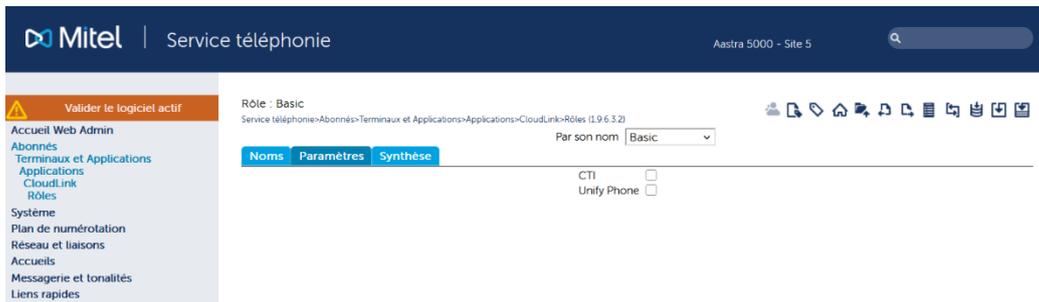
- Dans le champ Mot de passe, entrer un mot de passe pur l'utilisateur cg7450.

#### 4.2.5.3 ACCORDER LES DROITS UNIFY PHONE AUX RÔLES CLOUDLINK

L'attribution des fonctionnalités Unify Phone est à configurer via les rôles CloudLink. La gestion des rôles CloudLink se situe dans le menu Service **téléphonie** > **Abonnés** > **Terminaux et Applications** > **Applications** > **CloudLink** > **Rôles**.

Pour plus d'informations sur la configuration des utilisateurs CloudLink, se référer au document **CloudLink – Guide de Déploiement avec MiVoice 5000**.

Dans l'onglet **Paramètres** :



- Dans la liste déroulante **Par son nom**, sélectionner le rôle CloudLink à modifier
- Cocher la case **Unify Phone**. Cette option n'apparaît que si la configuration de la CloudLink Gateway est faite pour utiliser Unify Phone.

Menu **Service téléphonique** > **Abonnés** > **Abonnements** > **Caractéristiques**

Sélectionner la fiche abonnée considérée :

Dans l'onglet **Annuaire** :

- Dans le champ E-Mail, entrer une adresse mail unique pour l'abonnée considéré.

Dans l'onglet **Caractéristiques**

- Dans la liste déroulante **Rôle CloudLink**, sélectionner le rôle CloudLink créé ou modifié pour Unify Phone.
- Vérifier que la case **Droit ne pas déranger** est cochée.

Pour les nouveaux abonnements, la case est cochée par défaut.

Après attribution du rôle CloudLink, l'abonné considéré reçoit deux mails :

- Un mail de bienvenue CloudLink, avec un lien pour finir la configuration du compte utilisateur,
- Un mail donnant les liens de téléchargement de Unify Phone.

#### 4.2.6 DOCUMENTATION UTILISATEUR

Les utilisateurs Unify Phone peuvent consulter la documentation **Unify Phone pour MiVoice 5000**, pour avoir plus d'information sur la configuration de l'application.

Les documents sont disponibles sur Document Center : <https://www.mitel.com/document-center/applications/collaboration/unify-phone/unify-phone-for-mivoice-5000>



© Copyright 2025, Mitel Networks Corporation. All Rights Reserved. The Mitel word and logo are trademarks of Mitel Networks Corporation. Any reference to third party trademarks are for reference only and Mitel makes no representation of ownership of these marks.