Service SBC sur MiVoice 5000 Server, EX Controller et Mitel 5000 Compact

04/2025
AMT/PTD/PBX/0138/3/0/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.

SOMMAIRE

1 À PROPOS DE CE DOCUMENT

1.1 OBJET DE CE DOCUMENT

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

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

1.2 ABRÉVIATIONS

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

Ces documents sont retrouvables 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^{o} 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 :

- Pour les TRUNK SBC,
- Pour configurer les abonnements en mode 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, les cartes réseau de l'EX Controller 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.

Les sessions vidéo sont également prises en compte avec ce service.

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).

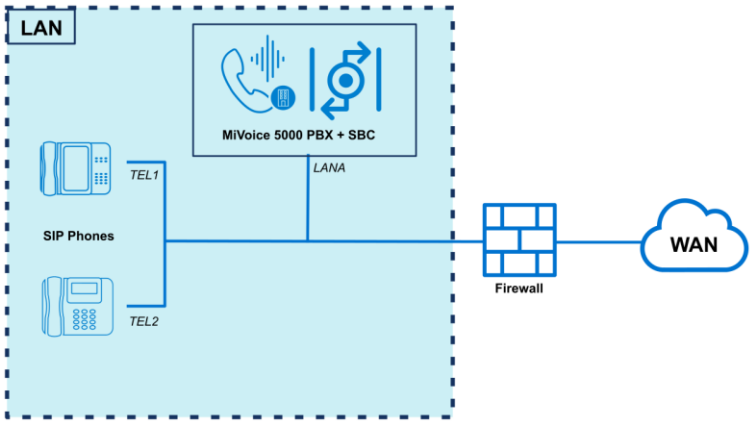
La solution proposée via le service SBC permet d'offrir des services téléphoniques vers un opérateur SIP en transitant par les équipements réseaux du client gérant la NAT et de compenser le cas échéant la NAT pour les équipements réseaux ne gérant pas complètement celle-ci pour les adresses IP encapsulées.

2.3 ARCHITECTURE DU SBC

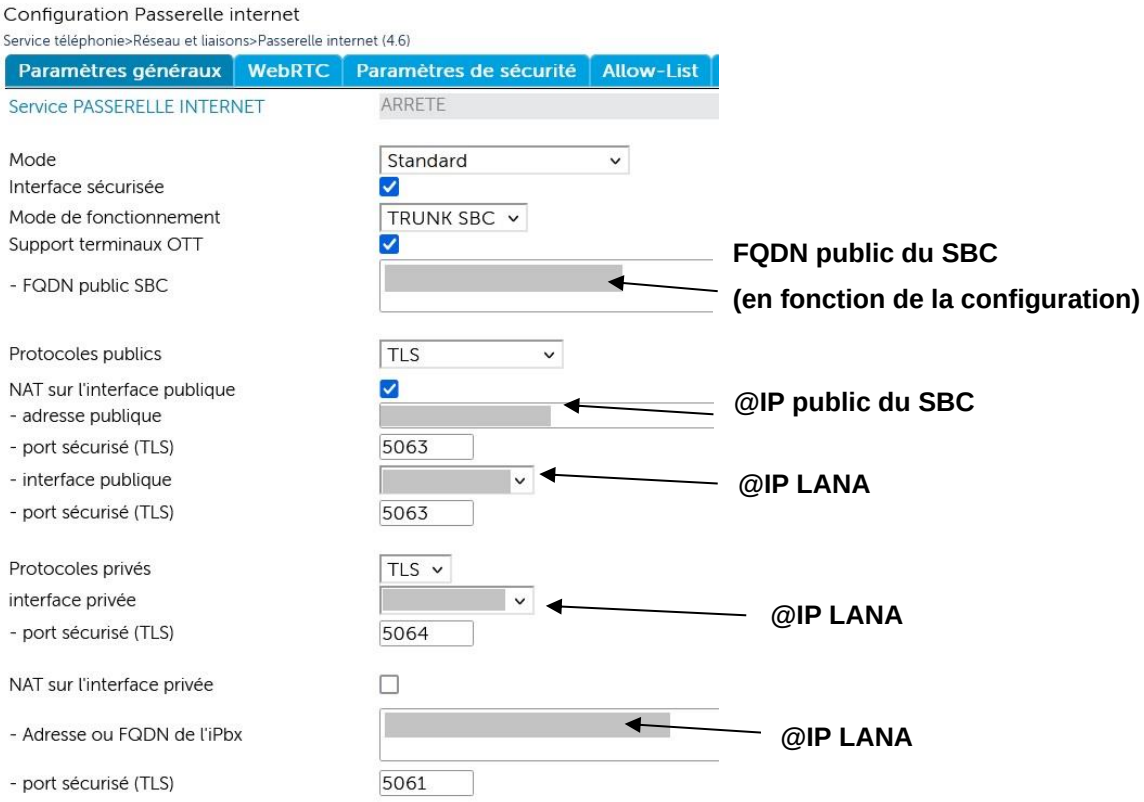
Différents cas d'architecture sont à considérer. Ce paragraphe se concentre sur les cas les plus fréquents.

2.3.1 SBC ET PBX COLOCALISÉS

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



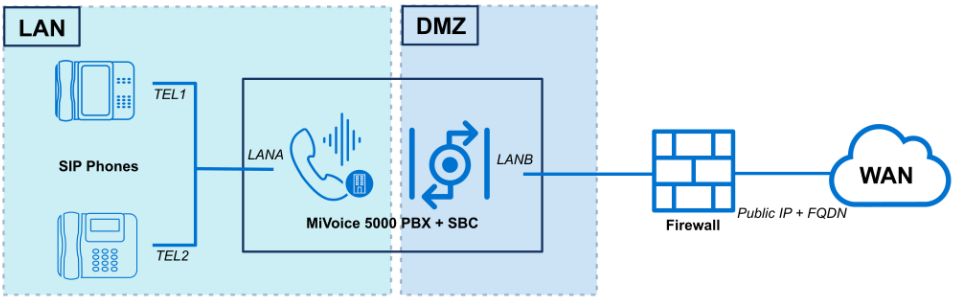
En fonction de la configuration sur le NAT, le menu **RESEAU ET LIAISONS>SBC Trunk** – Onglet **Paramètres généraux** est à remplir de la manière suivante :



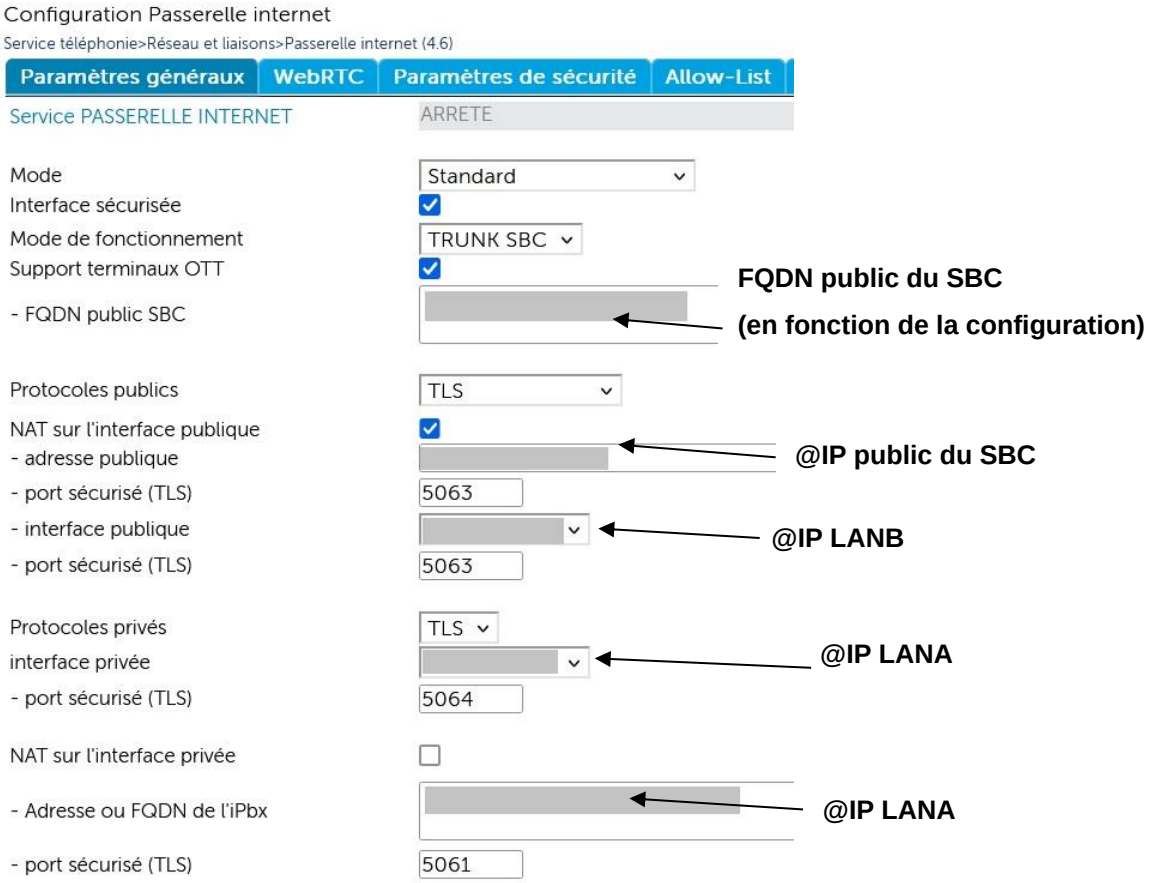
2.3.2 SBC ET PBX COLOCALISÉS ET SÉPARATION LAN/DMZ

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

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

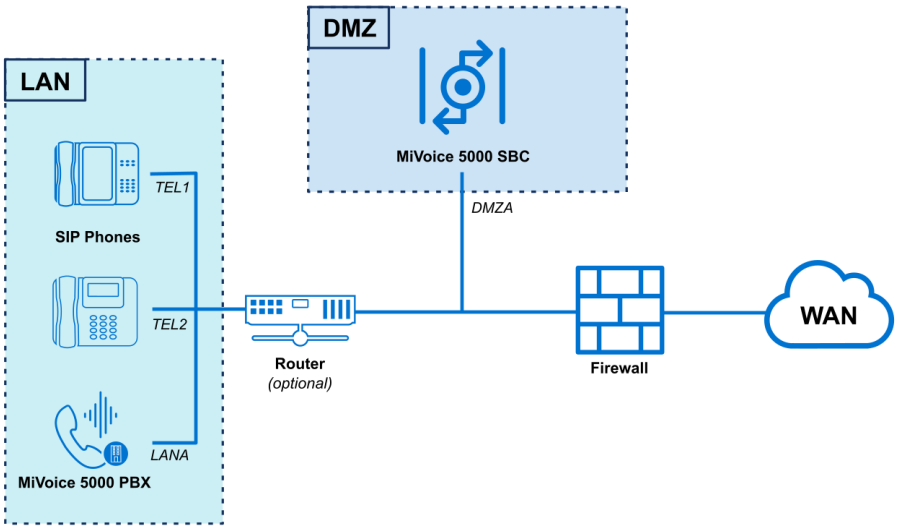


En fonction de la configuration du NAT, le menu **RESEAU ET LIAISONS>SBC Trunk** – Onglet **Paramètres généraux** est à remplir de la manière suivante :

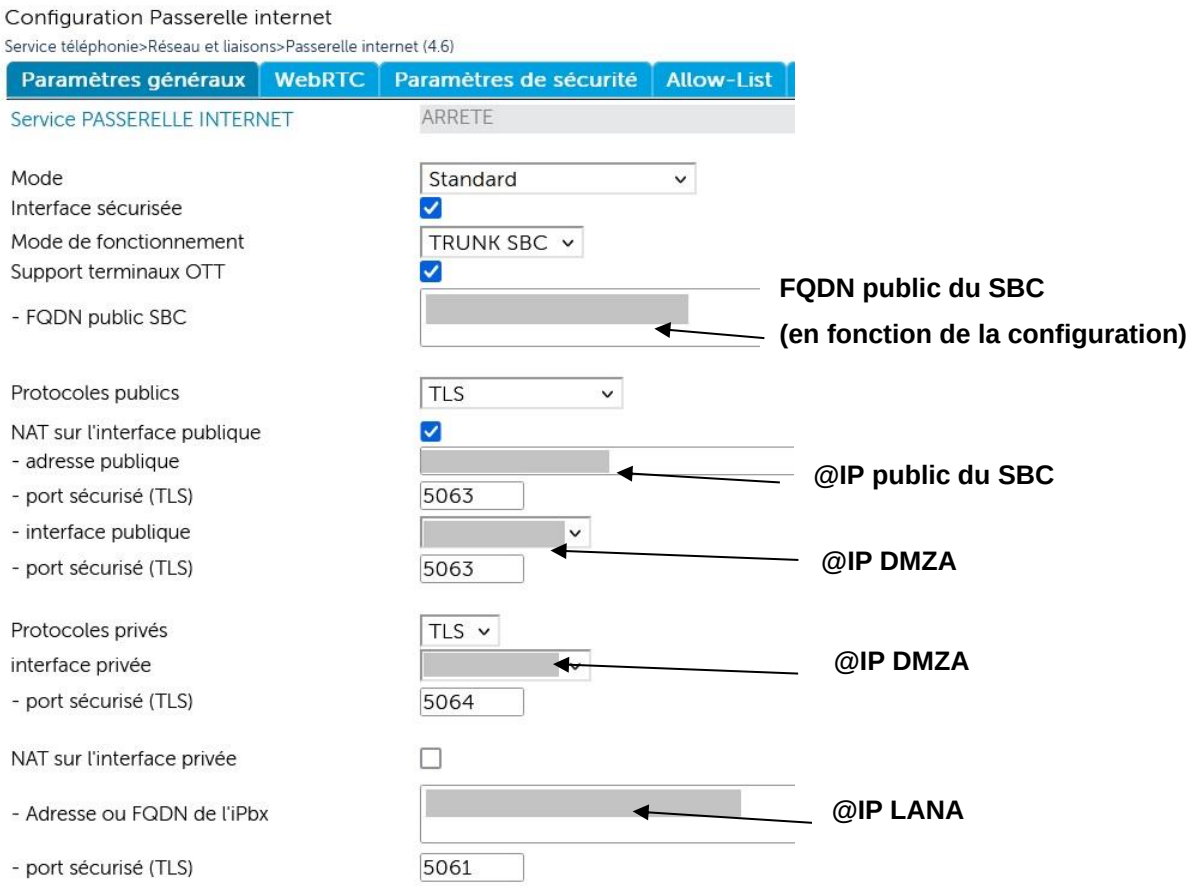


2.3.3 SBC ET PBX SÉPARÉS

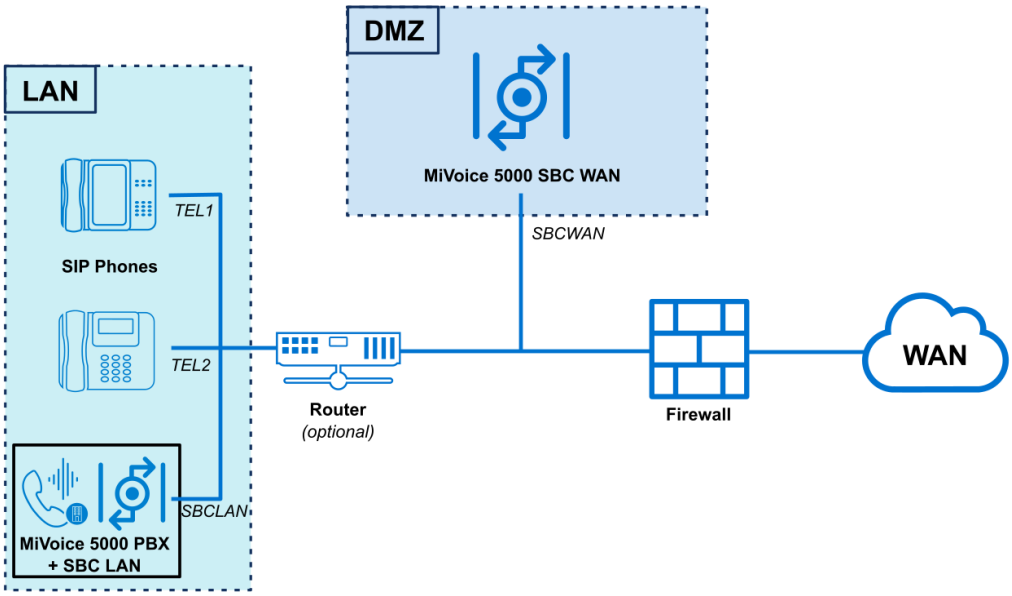
L'architecture avec un SBC et un PBX séparés reprend ici un cas d'installation sécurisée avec le SBC en DMZ et PBX en LAN.



En fonction de la configuration sur le NAT, le menu **RESEAU ET LIAISONS>SBC Trunk** – Onglet **Paramètres généraux** est à remplir de la manière suivante :

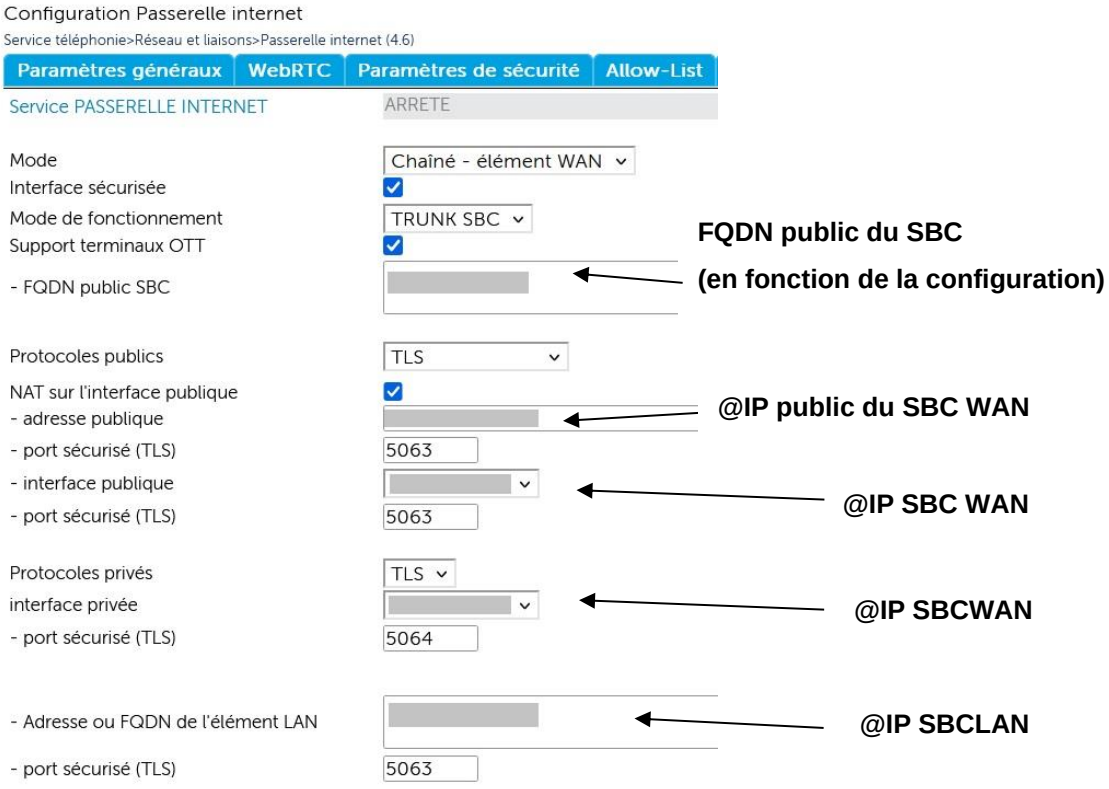


2.3.4 SBC DAISY CHAIN AVEC PBX COLOCALISÉ

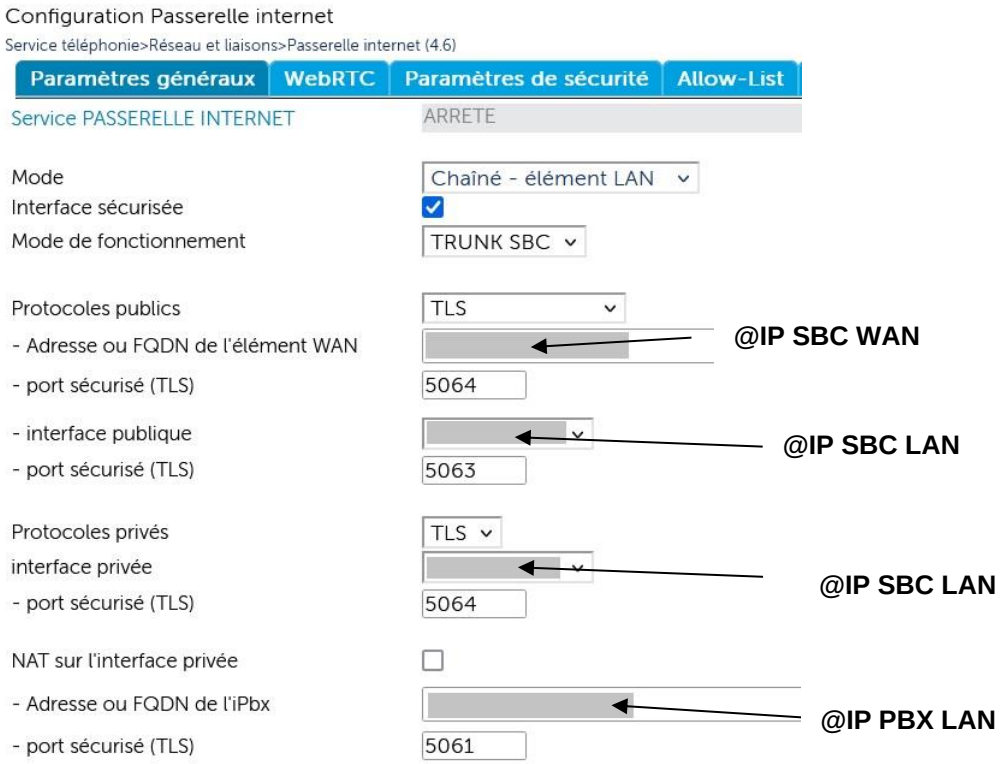


En fonction de la configuration sur le NAT, le menu **RESEAU ET LIAISONS>SBC Trunk** – Onglet **Paramètres généraux** est à remplir de la manière suivante :

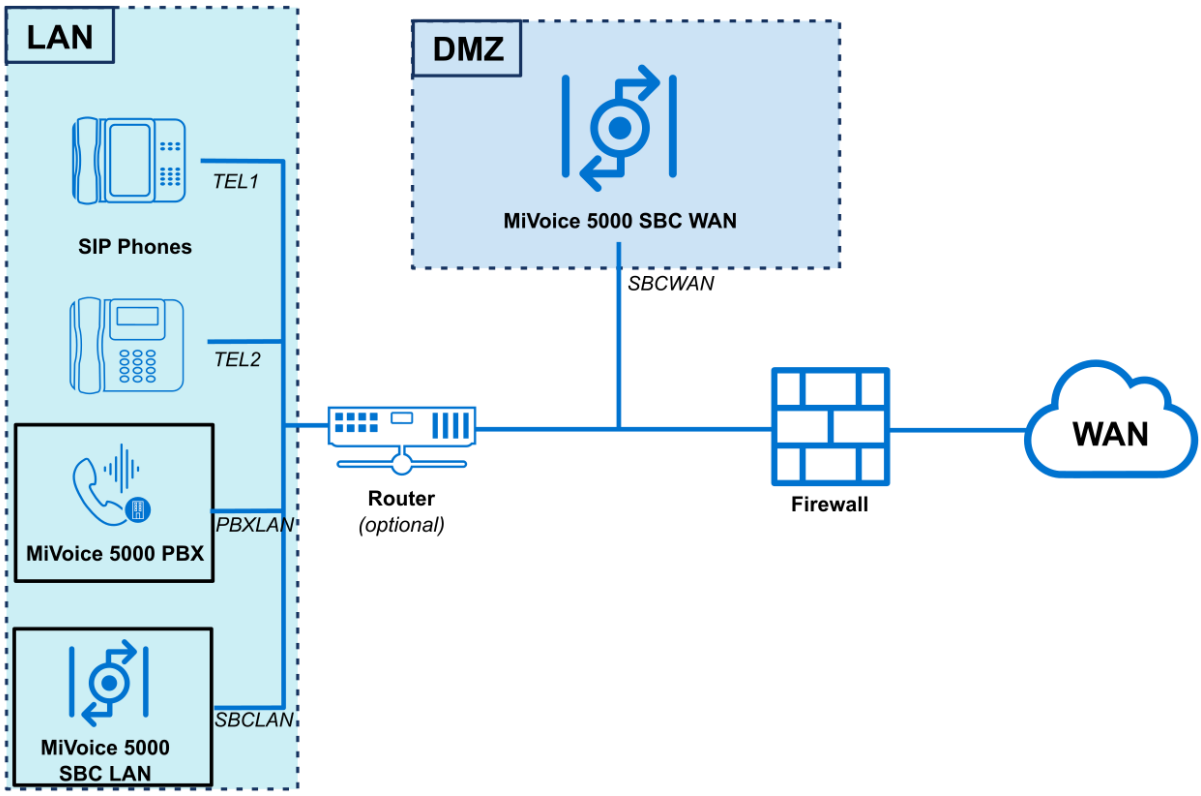
- Sur le SBC WAN



- Sur le SBC LAN

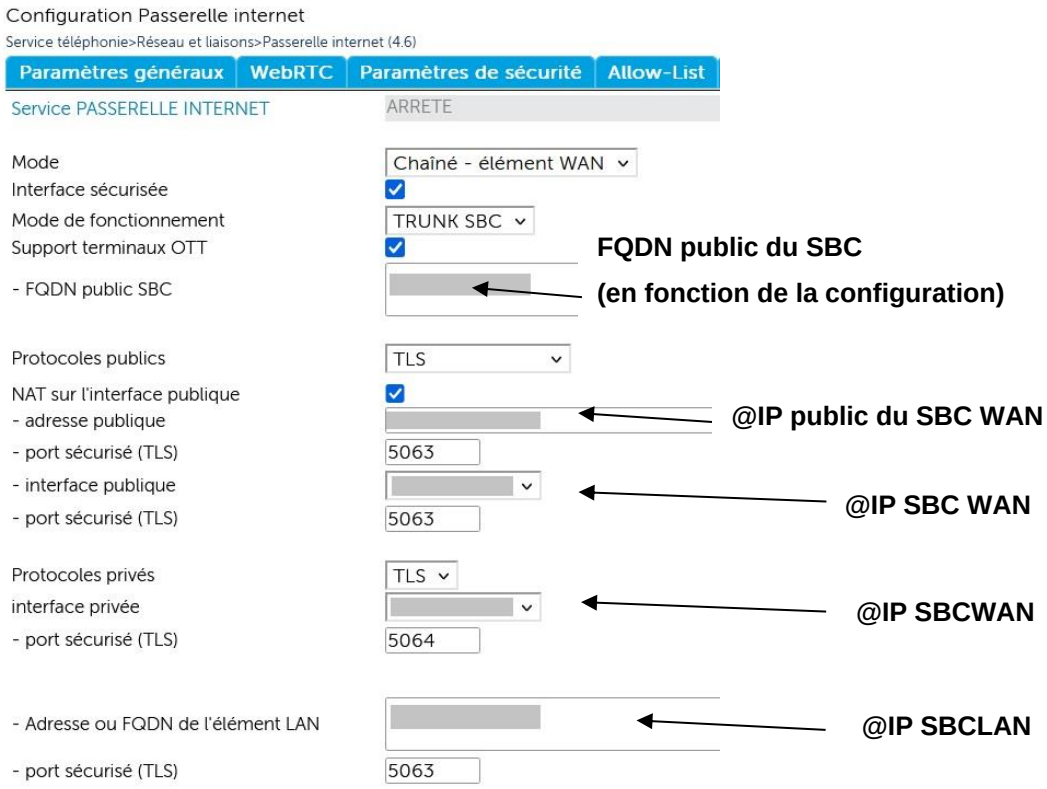


2.3.5 SBC DAISY CHAIN AVEC PBX SÉPARÉ

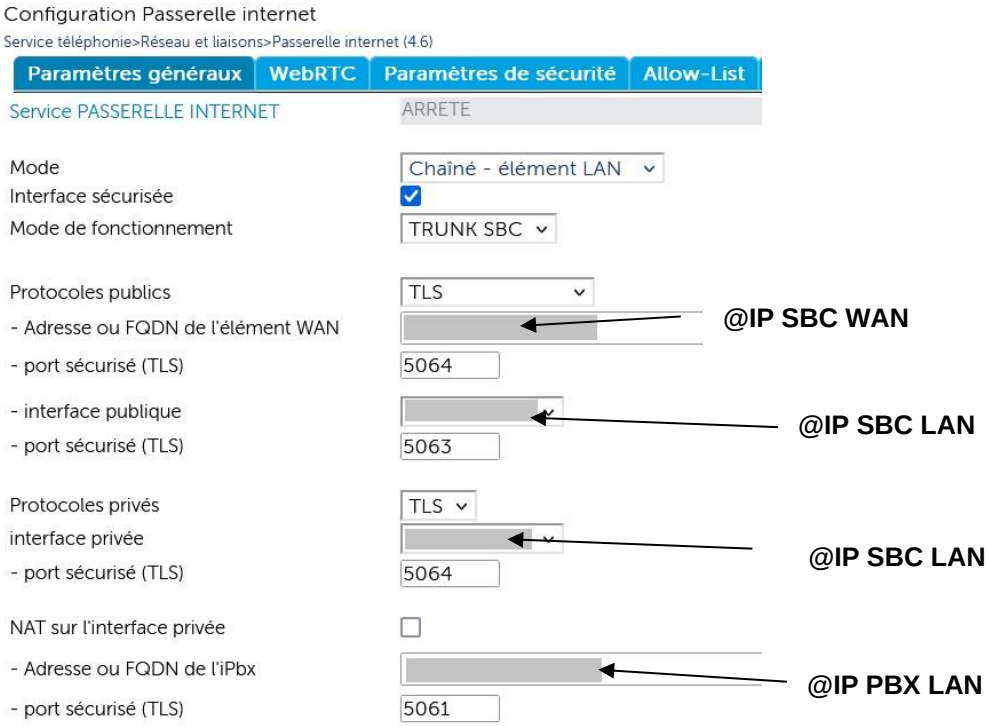


En fonction de la configuration sur le NAT, le menu **RESEAU ET LIAISONS>SBC Trunk** – Onglet **Paramètres généraux** est à remplir de la manière suivante :

- Sur le SBC WAN



- Sur le SBC LAN



2.4 DÉMARRAGE DU SERVICE SBC

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

Pour l'utilisation des trunk SBC, le service SBC ne nécessite aucune licence particulière.

2.5 NIVEAU DE SÉCURITÉ

2.5.1 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.

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.

Comme le service SBC est dédié au Trunk SIP, la protection contre les attaques de type **Force Brute** ne sont pas implémentées.

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 (1 heure par défaut). La liste peut également être nettoyée par l'installateur (voir paragraphes suivants).

2.5.2 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.

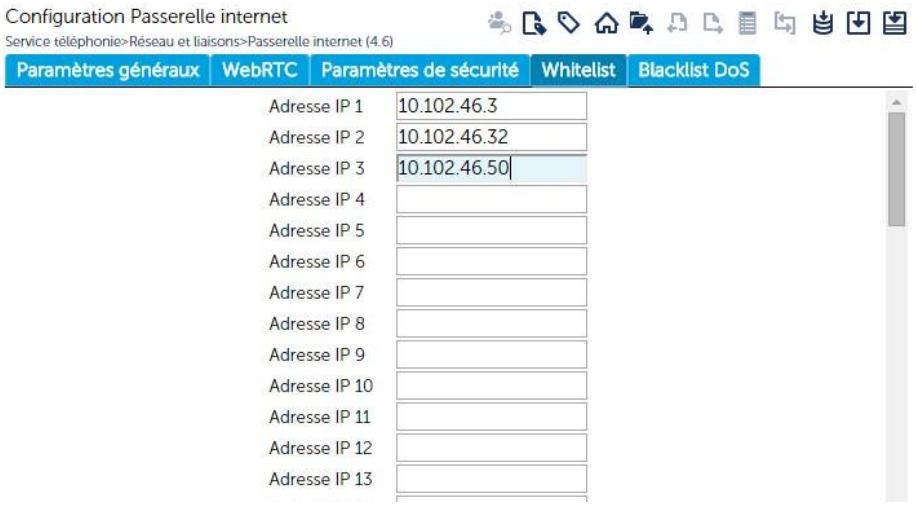
    - **Seuil** : 10 à 5000 (Nombre de requêtes SIP autorisées par fenêtre avant le blocage des requêtes entrantes)
    - **Fenêtre** (secondes) : 2 à 10 (période en secondes d'échantillonnage

  - **Effacement de la Deny-List DoS**

    Ce choix permet après confirmation de l'action d'effacer toutes les entrées de la black liste DoS.

2.5.3 GESTION DE LA ALLOW-LIST

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



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.

2.5.4 GESTION DE LA DENY-LIST DOS

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

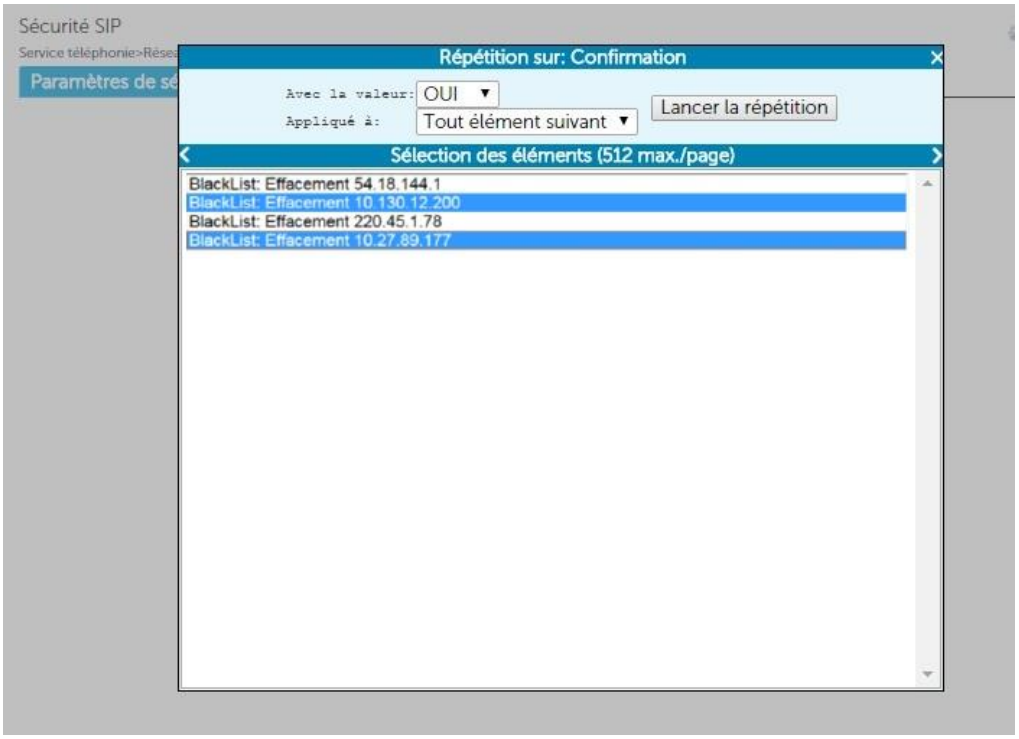
Chaque ligne du tableau présente une adresse blacklistée et permet de sélectionner l'adresse en vue de sa suppression.

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

Dans cet écran la suppression n'est effective que sur l'appui du bouton de 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.



2.5.5 ÉTAT DU NIVEAU DE SÉCURITÉ LORS D'UNE PREMIÈRE INSTALLATION

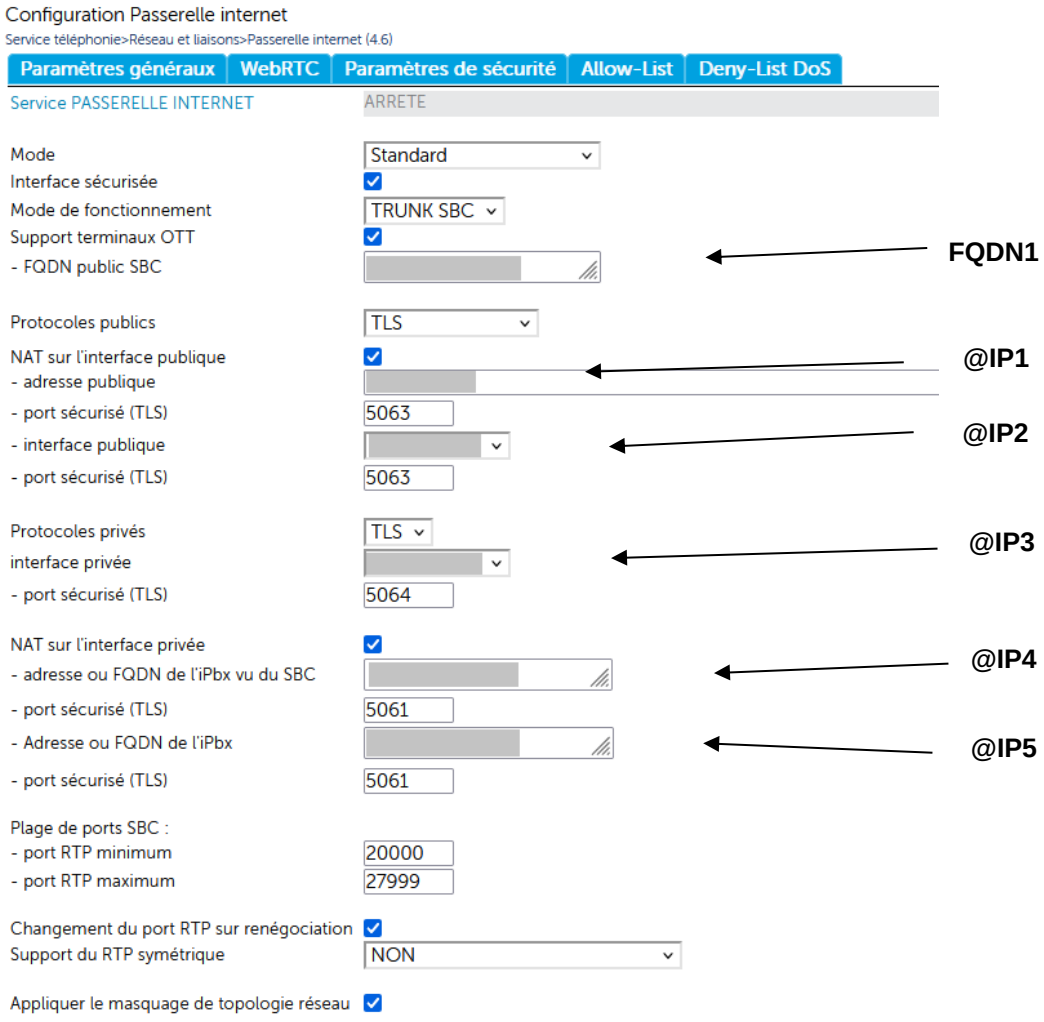
Lors d'une première installation, le niveau de sécurité est à **Autoprotection**.

3 CONFIGURATION DU TRUNK SBC

3.1 PARAMÈTRES GÉNÉRAUX DU SERVICE SBC

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

- **FQDN** : FQDN public du SBC, dédié au mode OTT. Champ actif uniquement en cas d'utilisation du paramètre Support Terminaux OTT.
- **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 de fonctionnement

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

- **Standard** : Mode par défaut, à utiliser dans une configuration standalone du 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.

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 adresse 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**.

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 adresse **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.

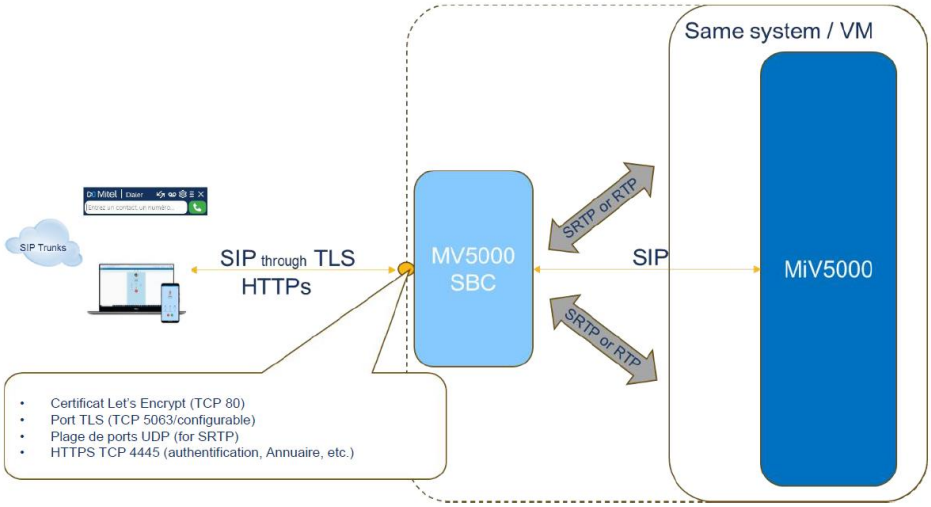
4 CONFIGURATION DES ABONNEMENTS EN MODE OTT

4.1 MITEL DIALER OTT

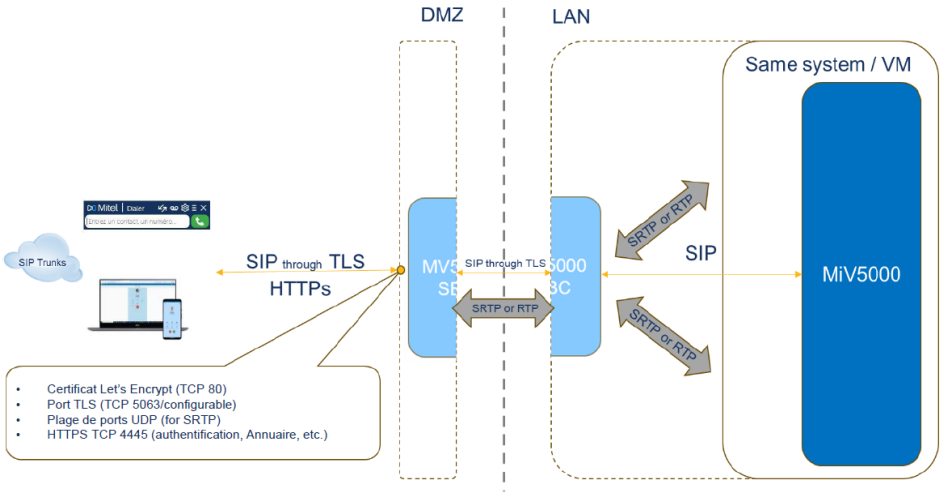
4.1.1 PRÉSENTATION DU MITEL DIALER OTT

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

- Configuration en Standalone : Le Mitel Dialer fonctionne avec un MiVoice 5000 SBC en DMZ.



- Configuration avec Daisy Chain : Le Mitel Dialer fonctionne avec deux MiVoice 5000 SBC. 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 SP1 minimum)
- La configuration du MiVoice 5000 Call Server
- 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, 1 FQDN résolu en interne sur le Call Server,
- Ouvrir des ports sur le firewall externe.

  Se référer aux paragraphes :

  - **4.1.3.2.1 – Configuration Standalone de la passerelle Internet pour le Mitel Dialer OTT** pour les ports à ouvrir dans le cas d'une configuration en Standalone
  - **4.1.3.2.2 – Configuration Daisy Chain de la passerelle Internet pour le Mitel Dialer OTT** pour les ports à ouvrir dans le cas d'une configuration avec Daisy Chain

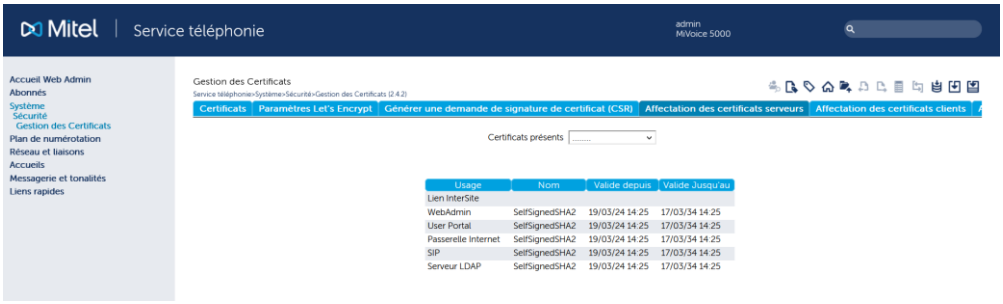
ATTENTION : L'utilisation des trunks MTLS empêche l'utilisation du mode OTT. Pour utiliser le Mitel Dialer OTT, il faut désactiver les options MTLS.

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 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**



- 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 Standalone de la passerelle internet pour le Mitel Dialer OTT*

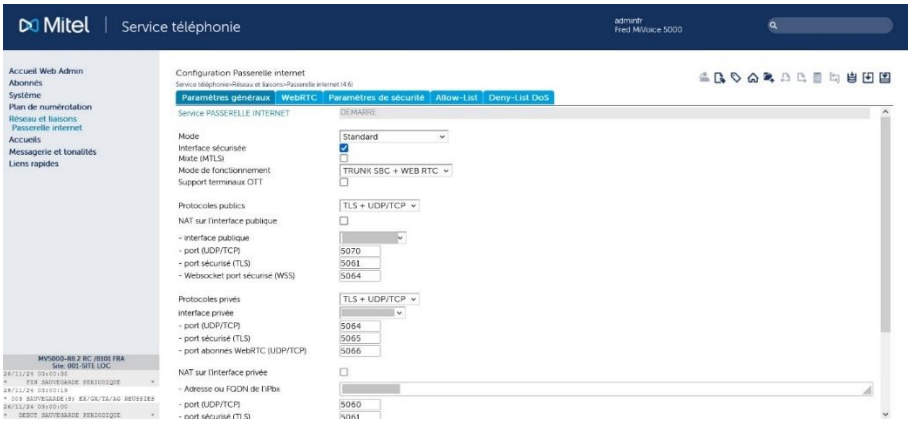
Ports à ouvrir sur le firewall

La configuration du Mitel Dialer OTT demande l'ouverture de plusieurs ports sur le firewall externe pour fonctionner. Les ports à ouvrir dans une configuration Standalone sont les suivants :

- Ports Internet vers DMZ :
  - TCP 80 s'il faut utiliser la génération de certificat Let's Encrypt,
  - TCP 4445 pour les services Web nécessaires au Mitel Dialer OTT
  - TCP 5063 pour le SIP TLS et les protocols publics (port configurable).
  - UDP 20000-27999 pour la voix (configurable).
- 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**



- Sur la liste déroulante **Mode de fonctionnement**, Sélectionner **Standard**.
- Vérifier que la case **Interface sécurisée** est cochée.
- En cas d'utilisation des options MTLS, vérifier que la case **Mixte (MTLS)** est décochée.
- 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.

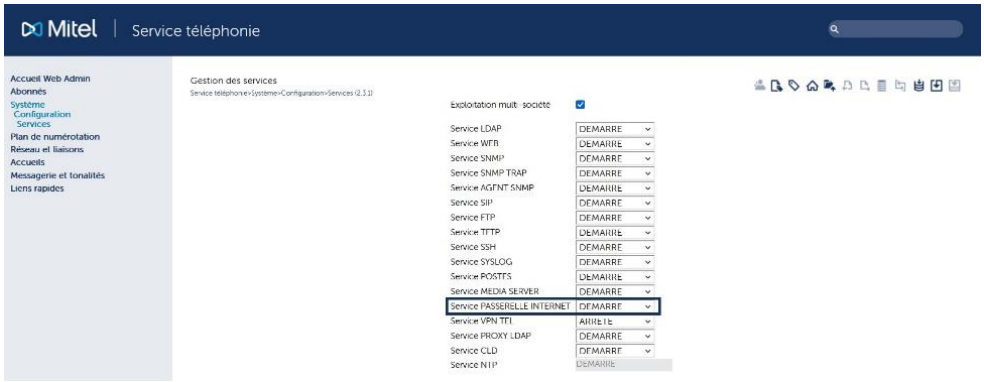
- La configuration du Mitel Dialer OTT utilise le TLS. Pour le paramètre **Protocoles publics**, il est possible de sélectionner **TLS** ou **TLS + UDP/TCP**.
- Sous la case **NAT sur l'interface publique** :
  - Sur le champ **interface publique**, entrer l'adresse IP publique prévue pour le Mitel Dialer OTT.

Note : Si la case NAT sur l'interface publique est cochée, le champ adresse publique est un champ à remplir.

Si la case NAT sur l'interface publique est décochée, le champ adresse publique est une liste déroulante.

  - 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 du Mitel Dialer OTT utilise le TLS. Pour le paramètre **Protocoles privées**, il est possible de sélectionner **TLS** ou **TLS + UDP/TCP**.
- 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**



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

4.1.3.2.2 *Configuration Daisy Chain de la passerelle internet pour le Mitel Dialer OTT*

Ports à ouvrir sur le firewall

La configuration du Mitel Dialer OTT demande l'ouverture de plusieurs ports sur le firewall externe pour fonctionner. Les ports à ouvrir dans une configuration avec Daisy Chain sont les suivants :

- Ports Internet vers SBC en DMZ :
  - TCP 80 s'il faut utiliser la génération de certificat Let's Encrypt,
  - 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).
- 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 apparait.
  - Dans le champ **FQDN public SBC**, entrer le FQDN publique du SBC.
- Dans la liste déroulante **Protocoles publics**, sélectionner **TLS.**

  En fonction de la configuration du MiVoice 5000, il est aussi possible de sélectionner **TLS + UDP/TCP**.
- 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 :

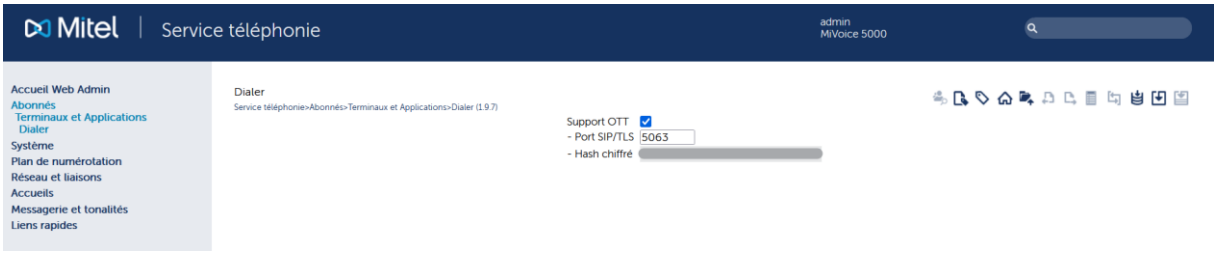
- Sur la liste déroulante **Mode de fonctionnement**, Sélectionner **Chainé – Élément LAN**.
- Vérifier que la case **Interface sécurisée** est cochée.
- En fonction de la configuration voulue, il est possible de cocher la case Mixte (MTLS).
- Dans la liste déroulante **Protocoles publics**, sélectionner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

  En fonction de la configuration du MiVoice 5000, il est aussi possible de sélectionner **TLS + UDP/TCP**.
- 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 ACTIVER LE MODE OTT DU MITEL DIALER

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



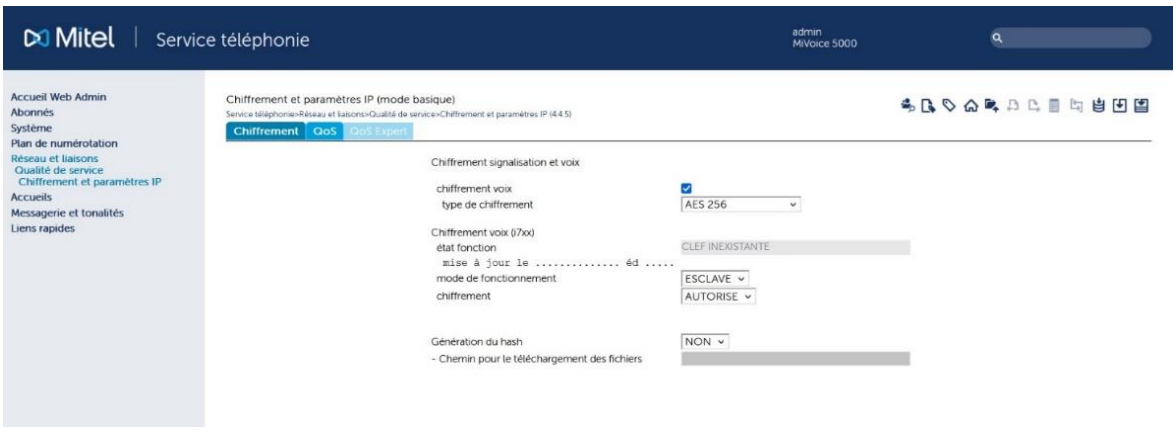
- Cocher la case **Support OTT**.

  Un nouveau champ apparait.

- Entrer dans le champ **Port SIP/TLS** le port dédié au SIP TLS.
- Le champ Hash chiffré affiche le hash, nécessaire pour l'utilisation du Mitel Dialer OTT. Si le champ ne s'affiche pas, le MiVoice 5000 demande de générer un hash. Se référer au paragraphe **4.1.4.2 – Vérifier le chiffrement et générer le hash**.

4.1.4.2 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 apparait 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 apparait avec le hash généré.

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**
- **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/**, où **SBC FQDN** représente le FQDN résolu sur l'adresse IP du SBC.

4.2 UNIFY PHONE

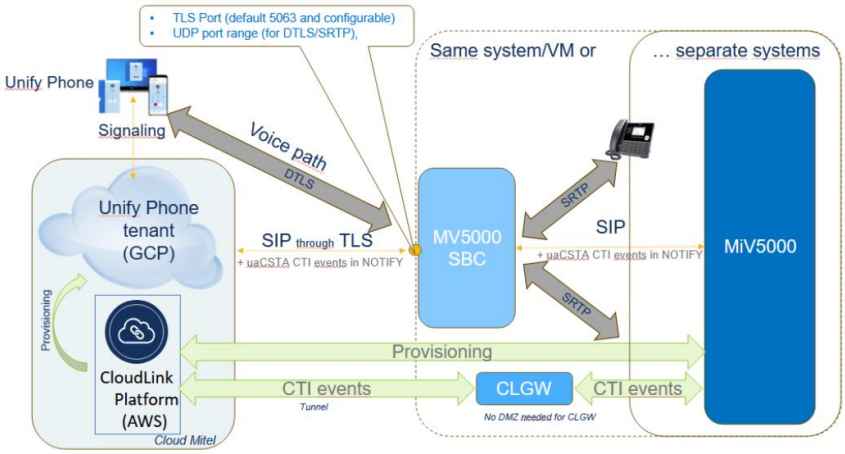
ASA : Nouveau paragraphe

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 évènements CTI,
- Le MiVoice 5000 pour les voix.



L'architecture standalone est recommandée pour Unify Phone. L'architecture en 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 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 Standalone de la passerelle internet pour Unify Phone** pour une configuration Standalone

- **4.2.3.2.2 – Configuration Daisy Chain de la passerelle internet pour Unify Phone** pour une configuration Daisy Chain

L'élément suivant est facultatif, mais recommandé :

- Si utilisation d'un certificat délivré par une autorité publique, 1 FQDN résolu en externe sur l'adresse IP publique.

ATTENTION : L'utilisation des trunks MTLS empêche l'utilisation du mode OTT. Pour utiliser Unify Phone et le mode OTT, il faut désactiver les options MTLS.

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 attribue un certificat par défaut à la passerelle internet 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**

4.2.3.2 CONFIGURER LA PASSERELLE INTERNET

4.2.3.2.1 *Configuration Standalone de la passerelle internet*

Ports à ouvrir sur le firewall

La configuration d'Unify Phone demande l'ouverture de plusieurs ports sur le firewall externe pour fonctionner. Les ports à ouvrir dans une configuration standalone sont les suivants :

- Ports Internet vers DMZ :
  - TCP 5063 pour le SIP TLS et les protocols publics (port configurable).
  - UDP 20000-27999 pour la voix (configurable).
- 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**.

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.
- En cas d'utilisation des options MTLS, 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 DNS signé par une autorité public, 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**.
- Sous la case **NAT sur l'interface publique** :
  - Sur le champ **interface publique**, entrer l'adresse IP publique prévue pour Unify Phone.

Note : Si la case NAT sur l'interface publique est cochée, le champ adresse publique est un champ à remplir, avec pré-remplissage de l'adresse IP.

Si la case NAT sur l'interface publique est décochée, le champ adresse publique est une liste déroulante.

  - 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 privées**, il est possible de sélectionner **TLS** ou **TLS + UDP/TCP**.
- 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**

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

4.2.3.2.2 *Configuration Daisy Chain de la passerelle internet*

Ports à ouvrir sur le firewall

La configuration d'Unify Phone demande l'ouverture de plusieurs ports sur le firewall externe pour fonctionner. Les ports à ouvrir dans une configuration avec Daisy Chain sont les suivants :

- Ports Internet vers SBC en DMZ :
  - TCP 5063 pour le SIP TLS, pour les protocoles publics (port configurable).
  - UDP 20000-27999 pour la voix (configurable).

- 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 apparait.
  - Dans le champ **FQDN public SBC**, si la configuration comprend un DNS signé par une autorité public, entrer le FQDN résolu en externe sur l'adresse IP publique.
- Dans la liste déroulante **Protocoles publics**, sélectionner **TLS.**

  En fonction de la configuration du MiVoice 5000, il est aussi possible de sélectionner **TLS + UDP/TCP**.
- 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.**

  En fonction de la configuration du MiVoice 5000, il est aussi possible de sélectionner **TLS + UDP/TCP**.
- 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 :

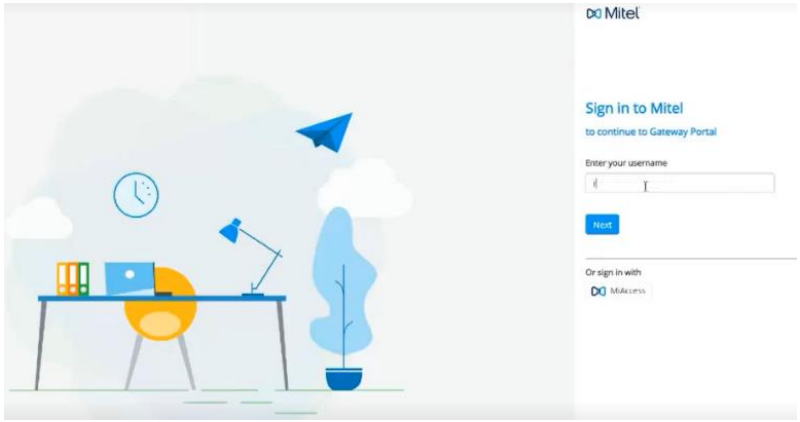
- Déployer CloudLink avec le MiVoice 5000
- Déployer une CloudLink Gateway
- Configurer Unify Phone sur CloudLink.

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, se référer au document **CloudLink – Déploiement avec MiVoice 5000.**

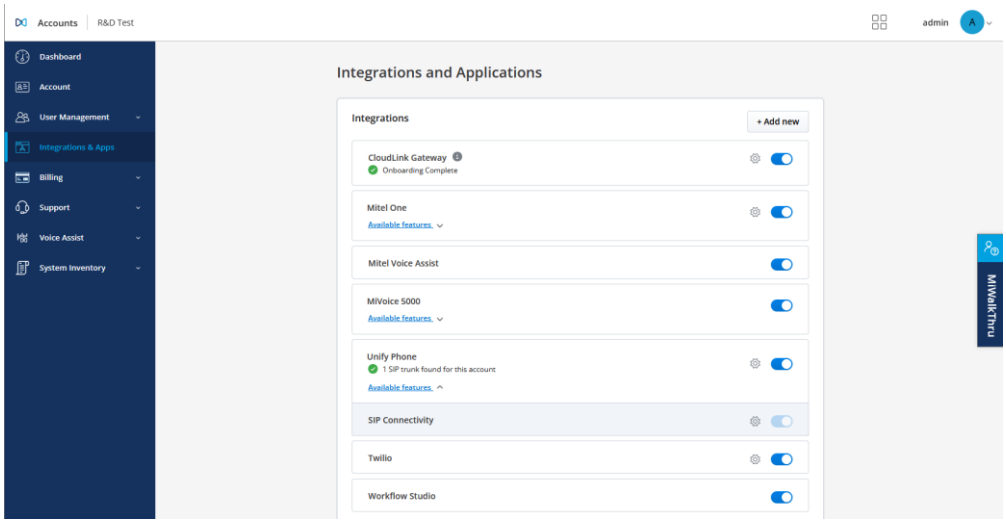
4.2.4.2 PROCÉDURE DE CONFIGURATION D'UNIFY PHONE SUR CLOUDLINK

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**.



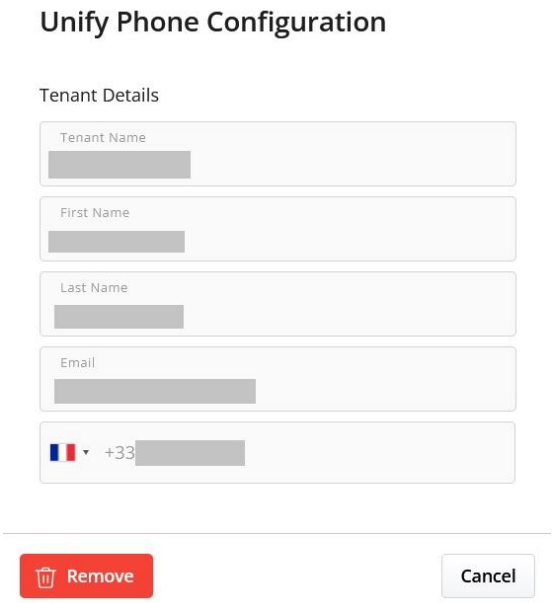
Note : Cette interface est aussi disponible dans le menu Account, section Integrations.

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

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

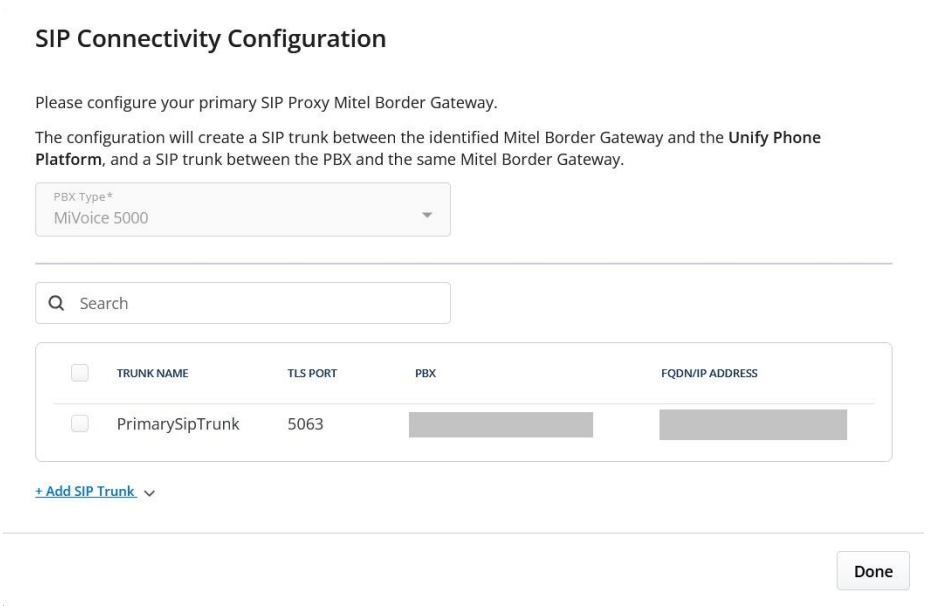
- Dans l'onglet **Mitel**, chercher l'intégration **Unify Phone** et cliquer sur le bouton **Add** associé.
- Cliquer sur **Done** pour fermer la fenêtre**.**
- Cliquer sur le rouage de la ligne **Unify Phone** pour configurer Unify Phone.

Écran d'informations à renseigner pour Unify Phone :



- Cliquer sur l'hyperlien **Available features** pour afficher le paramètre SIP Connectivity.
- Cliquer sur le rouage de la ligne **SIP Connectivity** pour configurer le trunk SIP dédié à Unify Phone.

Écran d'informations à renseigner pour le trunk SIP :



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.

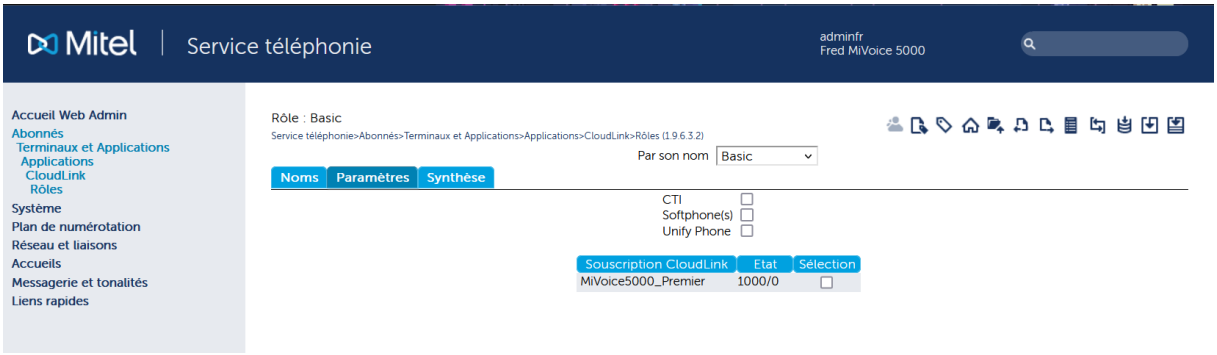
La resynchronisation assure l'affichage des paramètres CloudLink et Unify Phone sur le MiVoice 5000.

4.2.5.1 ACCORDER LES DROITS UNIFY PHONE AUX RÔLES CLOUDLINK

L'attribution des fonctionnalités d'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 configuration des utilisateurs CloudLink, se référer au document **CloudLink – Guide de Déploiement avec MiVoice 5000**.

Dans l'onglet **Paramètres** :



ASA : Capture à changer quand possible (Softphone non disponible en SP3)

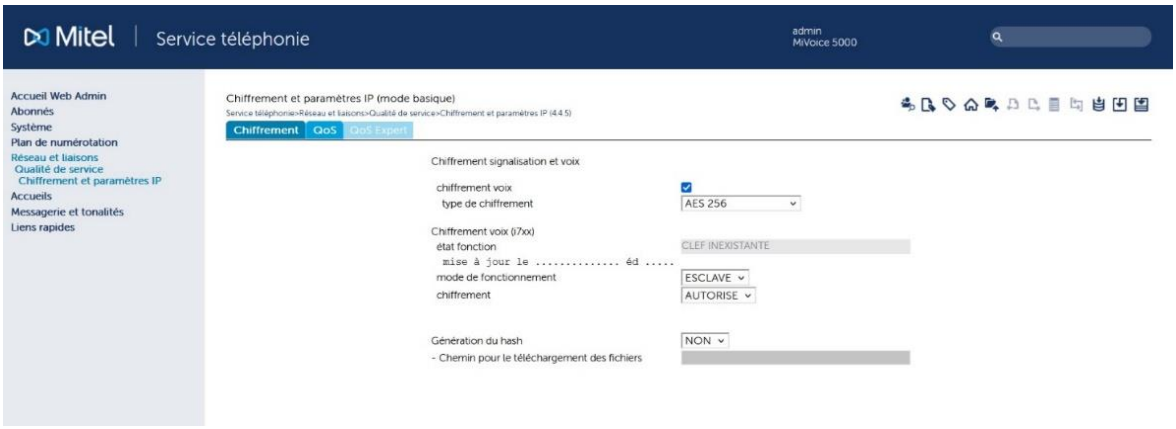
- Dans la liste déroulante **Par son nom**, sélectionner le rôle CloudLink à modifier
- Cocher la case **Unify Phone**. Cette option n'apparait que si la configuration de la CloudLink Gateway est faite pour utiliser Unify Phone.

Menu **Service téléphonie > Abonnés > Abonnements > Caractéristiques**, onglet **Caractéristiques**

- Sur les fiches abonnés considérées, sélectionner le rôle CloudLink créé ou modifié pour Unify Phone dans la liste déroulante **Rôle CloudLink**.

4.2.5.2 VÉRIFIER LE CHIFFREMENT DE LA VOIX

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



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