Service SBC embarqué sur MiVoice 5000 Server et Mitel 5000 Compact

06/2019
AMT/PTD/PBX/0138/2/0/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 A PROPOS DE CE DOCUMENT

1.1 OBJET DE CE DOCUMENT

Ce document décrit la mise œuvre du service SBC en environnement MiVoice 5000.

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
MitelMiVoice 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
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 REFERENCE

Documents de référence

- Mitel 5000 Gateways Description fonctionnelle et Installation matérielle - **AMT/PTD/PBX/0150/FR**
- Mitel 5000 Gateways et MiVoice 5000 Server Mise en service - **AMT/PTD/PBX/0151/FR**
- MitelMiVoice 5000 Web Admin XD-XL-XS-XS12-MiVoice 5000 Server - Manuel d'exploitation - **AMT/PTD/PBX/0080/FR**
- Manuel d'Installation de MitelMiVoice 5000 Manager (MiVoice 5000 Manager)- **AMT/PTD/NMA/0040/FR**
- Manuel d'Utilisation de MitelMiVoice 5000 Manager (MiVoice 5000 Manager) - **AMT/PUD/NMA/0003/FR**
- Mitel BluStar 8000i Desktop Media Phone SIP Call server Administration Guide release 4.1.1 - **AMT_PTD_TLA_0066/FR**
- Terminal Video BluStar 8000i - Complément d'Installation Solution MiVoice 5000 - **AMT/PTD/TLA/0063/FR**

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 GENERALITES

2.1 INTRODUCTION

Le Service SBC TRUNK délivré dans la solution permet la gestion de la NAT dans le cas d'un accès à un opérateur SIP (trunk SIP) pour lequel les problèmes de NAT ne peuvent pas être résolus directement par l'opérateur.

A partir de R5.4, le service SBC est intégré à le MiVoice 5000 server et au système Mitel 5000 Compact.

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

Le service embarqué 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.

2.1.1 RAPPEL DE LA PROBLEMATIQUE DE LA NAT

Les équipements réseaux NAT (routeurs, pare-feu, etc.) réalisent une translation d'adresses, pour des raisons de sécurité et/ou de manque d'adresses publiques IPv4 ou IPV6. La translation 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.

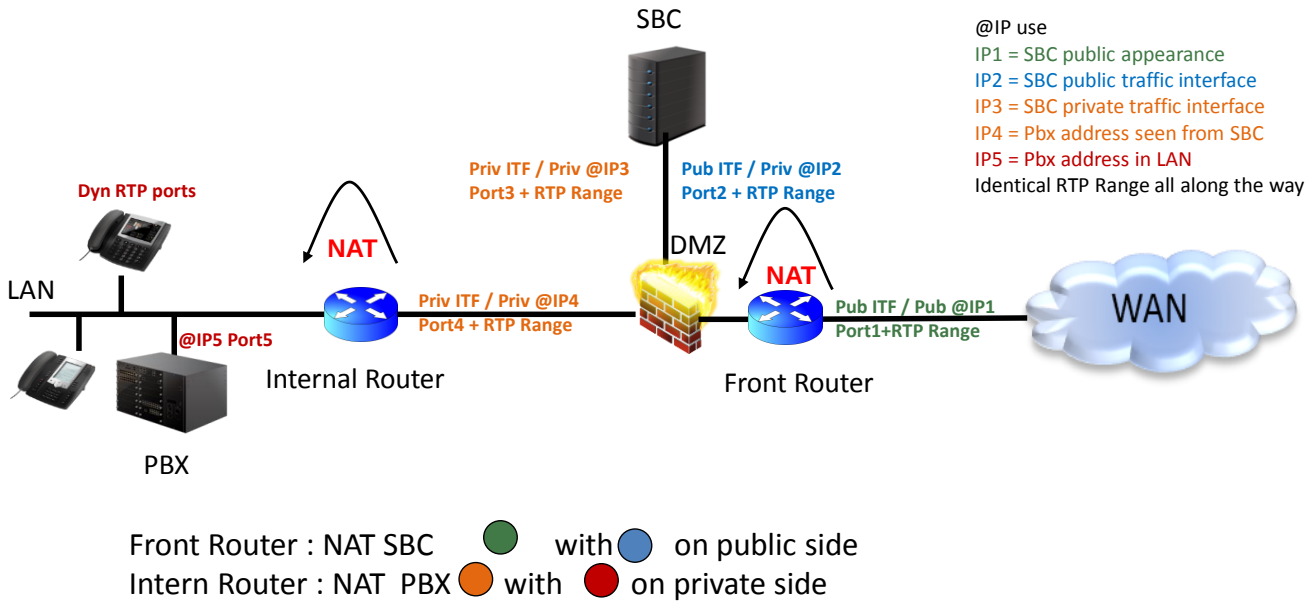
2.2 RESTRICTIONS D'UTILISATION DU SERVICE SBC TRUNK

Ce service est utilisable que pour les connexions de trunk SIP. (Pas abonnés distants)

2.3 ARCHITECTURE DU SERVICE SBC TRUNK

Différents cas d'architecture sont à considérer. Ce paragraphe ne présente que les cas les plus fréquents.

2.3.1 SBC STAND ALONE DANS LA DMZ (DOUBLE NAT)

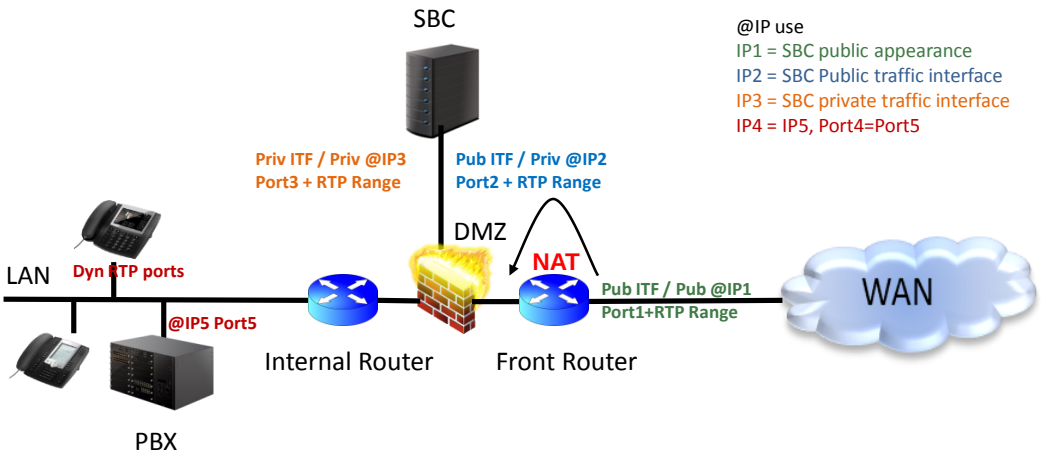


Dans cette architecture, la translation d'adresse est réalisée des deux côtés :

- Entre le LAN et la DMZ (Côté privé)
- Entre le WAN (Internet) et la DMZ (Côté public).

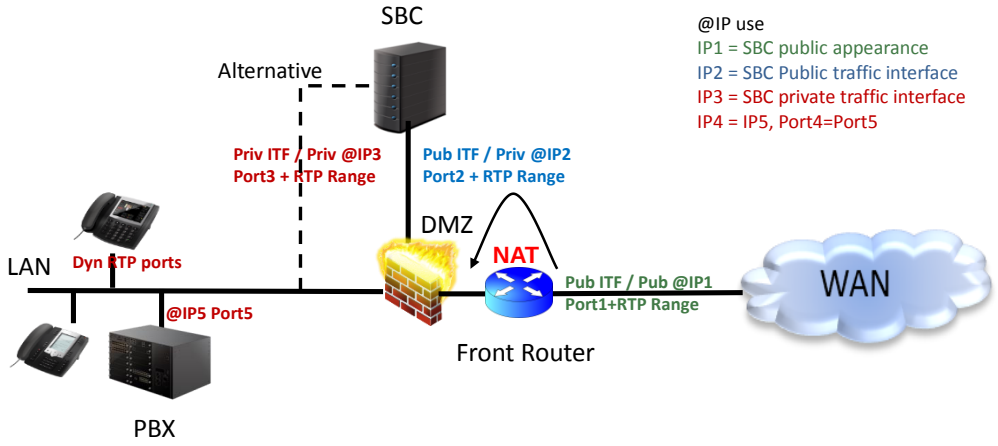
À partir de ce cas général, d'autres alternatives sont envisageables. Se référer aux paragraphes suivants.

2.3.2 NAT COTE PUBLIC AVEC IPBX ET MODULE SBC DANS DES RESEAUX DIFFERENTS (SIMPLE NAT AVEC ROUTE)



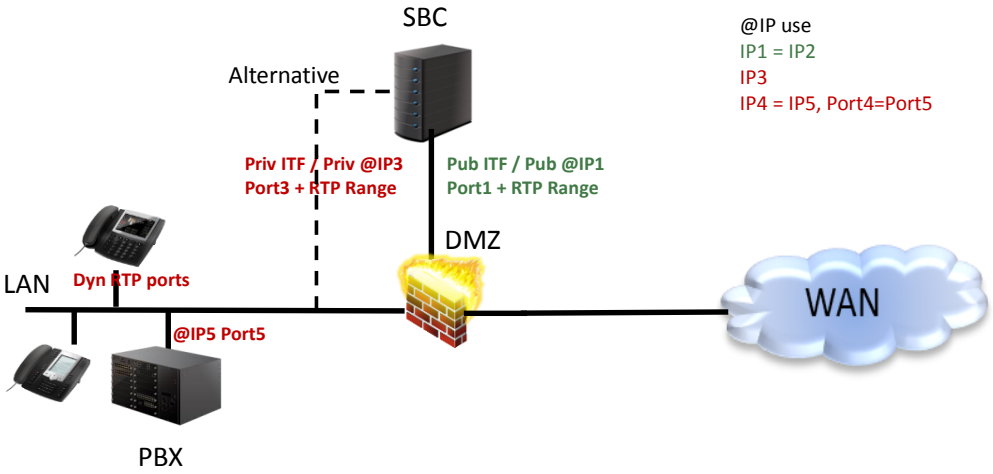
Front Router : NAT SBC with on public side
Intern Router : No NAT. But PBX and SBC in ≠ subnets.
PBX reachable by SBC with

2.3.3 NAT COTE PUBLIC AVEC IPBX ET MODULE SBC DANS LE MEME RESEAU (SIMPLE NAT)



Front Router : NAT SBC with on public side
Intern Router : No NAT. PBX and SBC in same subnet

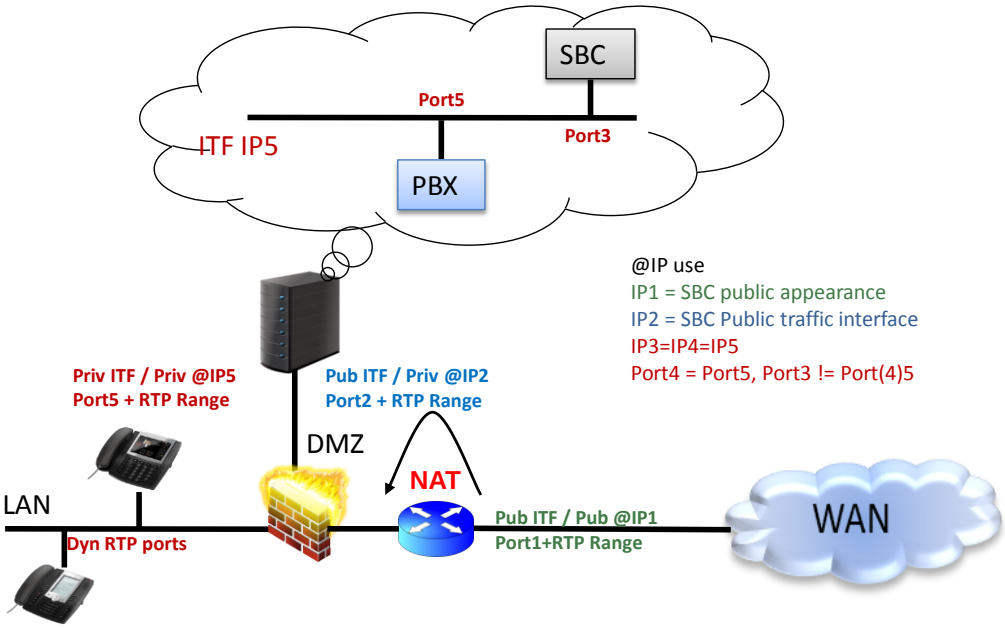
2.3.4 PAS DE NAT



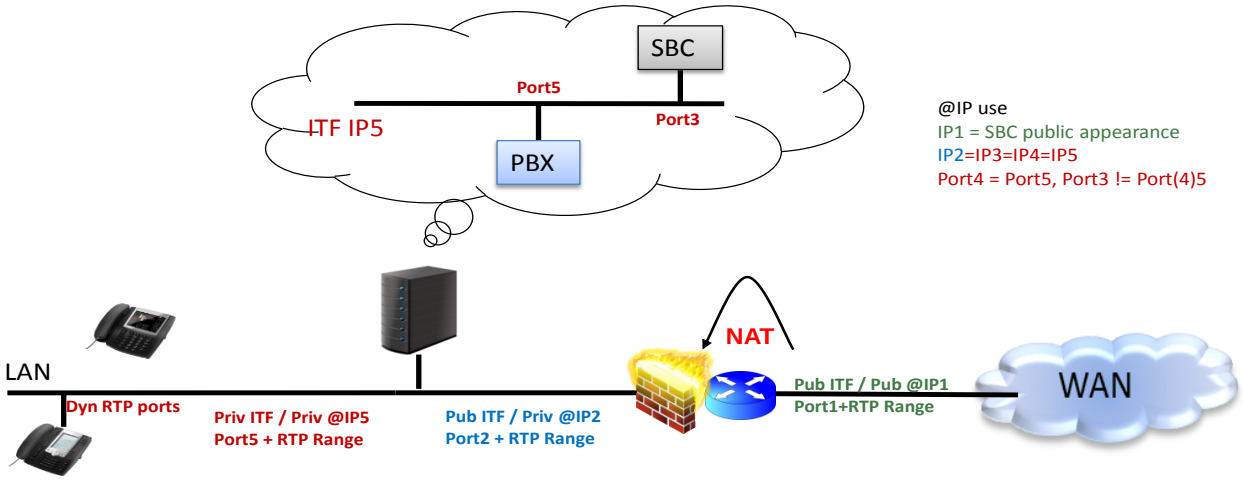
Front Router : No NAT. SBC reachable from internet through

Intern Router : No NAT. PBX and SBC in same subnet

2.3.5 SBC ET IPBX COLOCALISES DANS LA DMZ



2.3.6 SBC ET IPBX COLOCALISES DANS LE LAN SANS DMZ



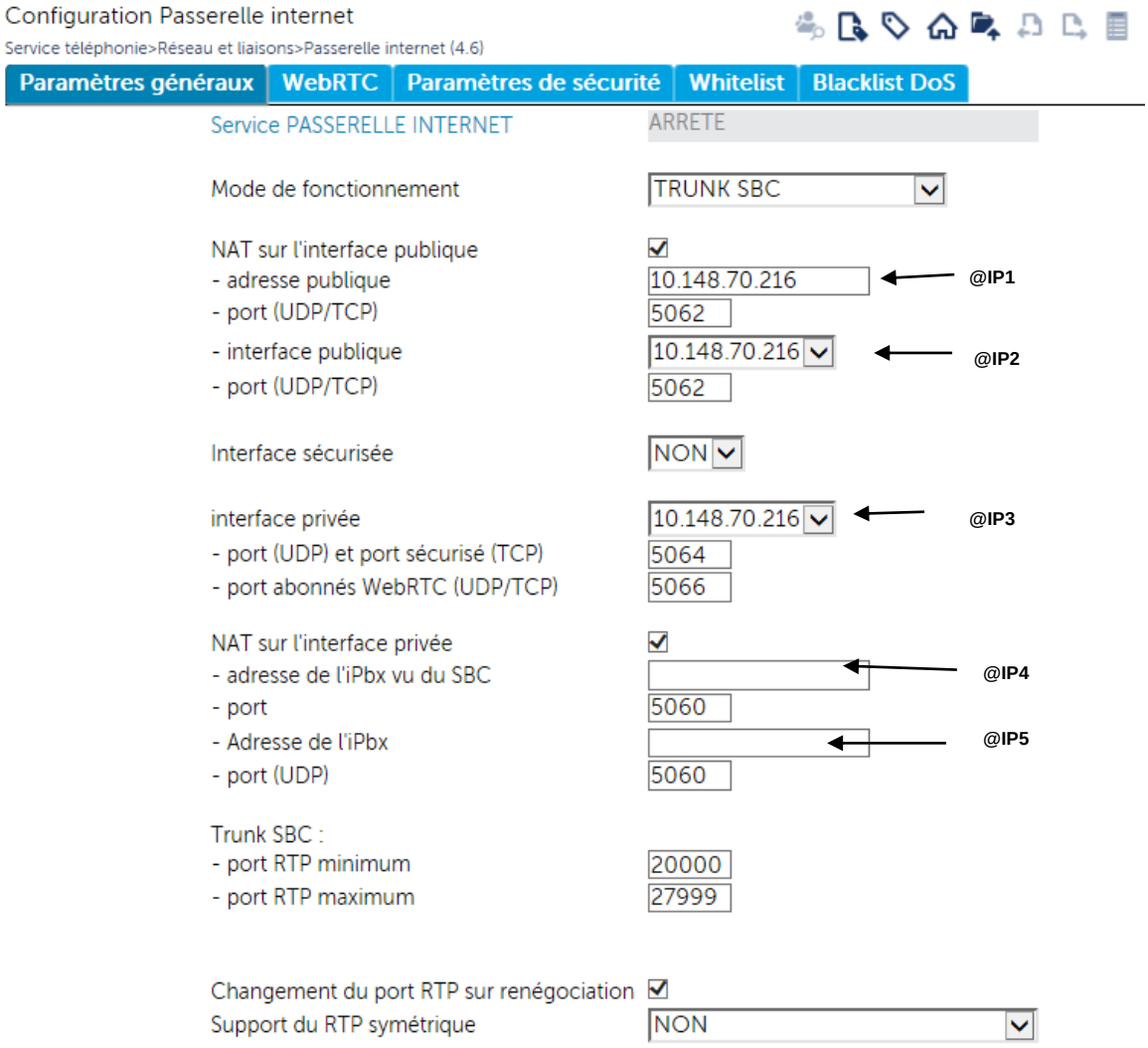
3

3 CONFIGURATION DU SERVICE SBC A PARTIR DE LE WEB ADMIN

3.1 PARAMETRES GENERAUX DU SERVICE SBC EMBARQUE

Selon l'architecture réseau choisie (Voir le paragraphe2.3), le Menu **RESEAU ET LIAISONS>SBC Trunk** – Onglet **Paramètres généraux** permet de définir les différentes adresses et ports associés du service SBC :

- **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.

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.

IP1 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 coté 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.

IP4 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 IP2 et IP3 sont restreintes aux seules adresses IP de la machine sur laquelle est exécutée la RHM.

La cinquième 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 IP2 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.

3.2 DEMARRAGE DU SERVICE SBC EMBARQUE

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

3.3 LICENCE

Le service SBC ne nécessite aucune licence particulière.

3.4 NIVEAU DE SECURITE

3.4.1 PRINCIPE

Le SBC fournit – uniquement sur MiVoice 5000 Server et pour les appels trunk - 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 **Whitelist)** 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 **Blacklist 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).

3.4.2 CHOIX DU NIVEAU DE SECURITE

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**
- **Whitelist seule**

Description des différents choix :

Aucun :

L'onglet **Whitelist** n'est pas accessible

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

Auto protection

Pour le niveau « auto protection » les onglets **Whitelist** et **Blacklist DoS** servent de filtre.

L'onglet **Whitelist** comporte la liste des adresses IP saisies par l'opérateur.

L'onglet **Blacklist 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 Blacklist 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.

Whitelist seule

Dans ce cas, seul l'onglet **Whitelist** 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 blacklist 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.

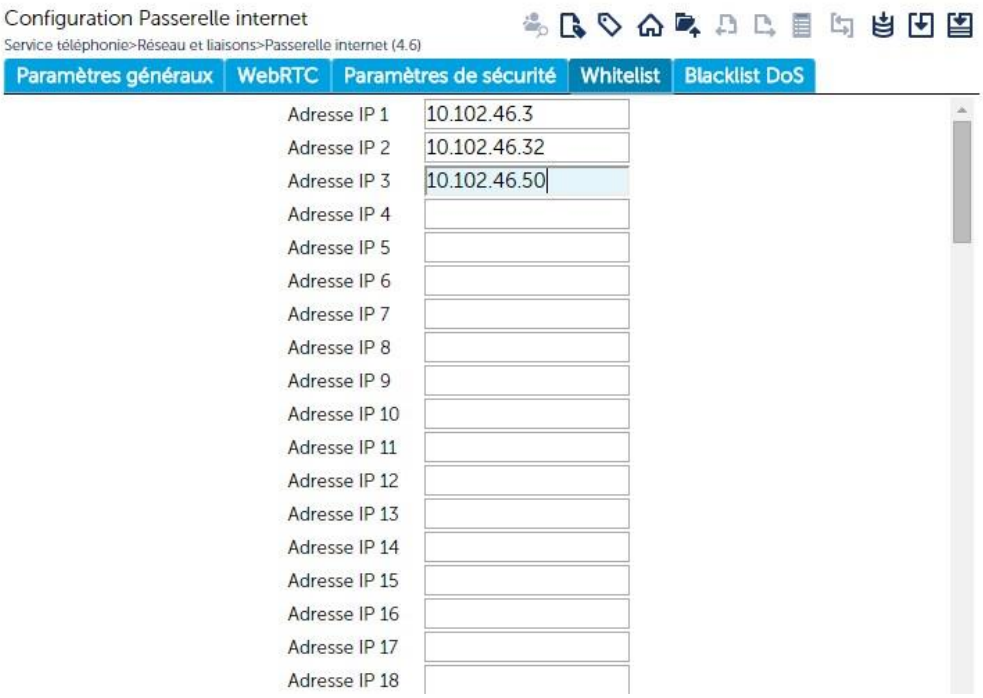
- **Seuil** : 10 à 5000 (Nombre de requêtes SIP autorisées par fenêtre avant le blocage des requêtes entrantes)
- **Fenêtre** (secondes) : 2 à 10 (période en secondes d'échantillonnage

Effacement de la BlackList DoS

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

3.4.3 GESTION DE LA WHITELIST

Menu **RESEAU ET LIAISONS> Passerelle internet** – Onglet **WhiteList**



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.

3.4.4 GESTION DE LA BLACKLIST DOS

Menu **RESEAU ET LIAISONS>Passerelle internet** – Onglet **WhiteList**

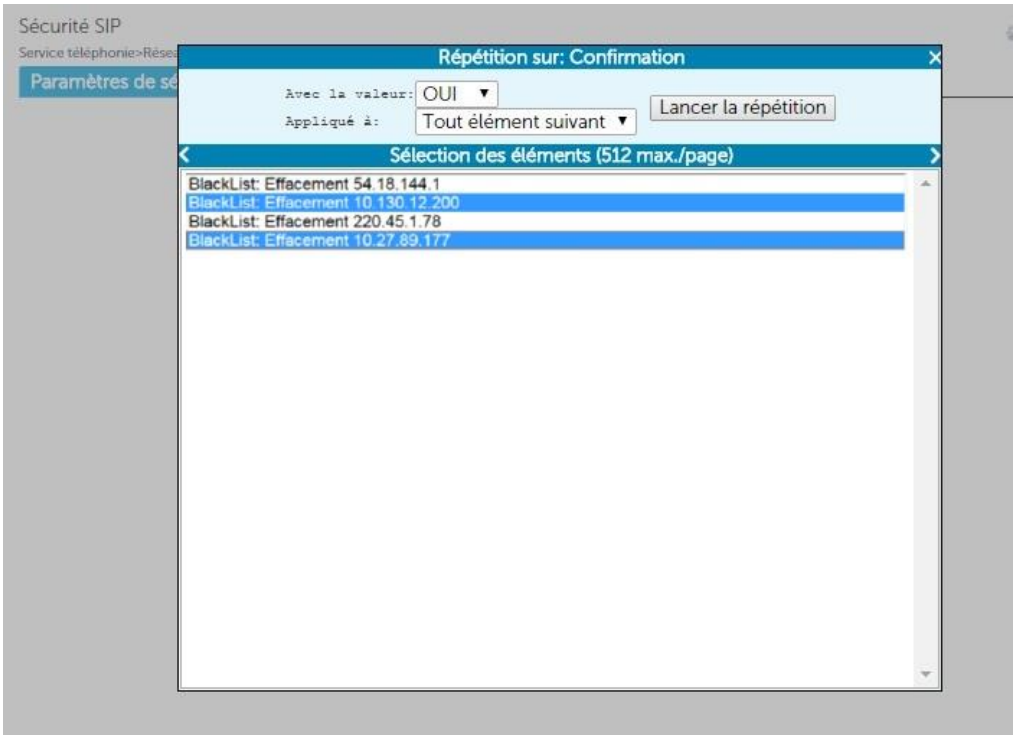
Chaque ligne du tableau présente une adresse blacklistée et permet de sélectionner l'adresse en vue de sa suppression.

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.

Suite à la suppression on revient automatiquement sur la Blacklist 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



3.4.5 ETAT DU NIVEAU DE SECURITE LORS D'UNE PREMIERE INSTALLATION

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

3.4.6 ETAT DU NIVEAU DE SECURITE LORS D'UNE MISE A JOUR LOGICIELLE VERS VERSIONS SUPERIEURES OU EGALES A R6.0 SP2

Mise à jour pour les versions strictement inférieures à **R5.4 SP2 vers versions supérieures ou égales R6.1 SP2** :

Le niveau de sécurité est à **Aucun** (pas de service SBC disponible dans les versions initiales).

Mise à jour pour les versions égales ou supérieures à **R5.4 SP2 vers versions supérieures ou égales R6.1 SP2** :

- Si la sécurité SBC était désactivée, le niveau de sécurité sera à **Autoprotection**
- Si la sécurité SBC était activée, le niveau de sécurité sera à **Autoprotection** et la Whitelist statique sera mise à jour.