# SBC service integrated into MiVoice 5000 Server and C2IC

06/2019
AMT/PTD/PBX/0138/2/0/EN
IMPLEMENTATION MANUAL

Mitel®

**Notice**

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®).

The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries.

Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

# CONTENTS

# 1 ABOUT THIS DOCUMENT

## 1.1 PURPOSE OF THIS DOCUMENT

This document describes how to implement the SBC service in a MiVoice 5000 environment.

## 1.2 ABBREVIATIONS

| | |
|---|---|
| **Mitel 5000 Gateways** | This term refers to all XS, XL and XD iPBXs. |
| **MiVoice 5000 or MiVoice 5000 Server**: | Telephony switching system running on a Linux Redhat or Centos PC |
| **XS, XL, XD**: | MiVoice 5000 series physical gateways. |
| **XS**: | This term includes XS, XS12 and XS6 systems |
| **MiVoice 5000 Manager**: | Systems management centre |
| **CAC**: | Call Admission Control |
| **DoS**: | Denial of Service |
| **DDoS**: | Distributed Denial of Service |
| **DMZ**: | Demilitarised zone |
| **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 |
| **MMC**: | Man Machine Command, iPBX command. |
| **RTP**: | Real Time Protocol |
| **SBC**: | Server Base Computing |
| **SIP**: | Session Internet Protocol |
| **VPN**: | Virtual Private Network |
| **WAN**: | Wide Area Network |

## 1.3 REFERENCE DOCUMENTS

**Reference documents**

- Mitel 5000 Gateways - Functional description and hardware installation - AMT/PTD/PBX/0150/EN
- Mitel 5000 Gateways and MiVoice 5000 Server Implementation - AMT/PTD/PBX/0151/EN
- MiVoice 5000 Web Admin XD-XL-XS-XS12-MiVoice 5000 Server – Operating manual AMT/PTD/PBX/0080/EN
- MiVoice 5000 Manager Installation manual - AMT/PTD/NMA/0040/EN
- MiVoice 5000 Manager User Manual - AMT/PUD/NMA/0003/EN
- Mitel BluStar 8000i Desktop Media Phone SIP Call server Administration Guide release 4.1.1 - AMT_PTD_TLA_0066/EN
- Video terminal BluStar 8000i - Addendum to MiVoice 5000 Installation - AMT/PTD/TLA/0063/EN

## 1.4 REMINDER CONCERNING THE LAW ON INFORMATION TECHNOLOGY

The user is reminded that the use of PBXs in the workplace must comply with the recommendations of the IT law in force.

The user's attention is also drawn to any clauses applicable in laws relating to the confidentiality of calls transmitted by means of telecommunications.

# 2 GENERAL INFORMATION

## 2.1 INTRODUCTION

The SBC TRUNK offered in the solution allows NAT management in case of access to an SIP (SIP trunk) operator for whom the NAT problems cannot be directly solved by the operator.

As of R5.4, the SBC service is integrated into MiVoice 5000 Server and into Mitel 5000 Compact.

The service can be implemented from Web Admin and consists in configuring the different IP addresses on the public and private side for address translations in the architecture in question.

The integrated service also contains some security upgrades using some filters on the IP address lists to protect themselves from DDoS and DoS type attacks.

Video sessions are also taken into account with this service.

### 2.1.1 REMINDER ON NAT RELATED PROBLEMS

NAT network devices (routers, firewall, etc.) translate addresses, for security reasons and/or due to lack of public IPv4 addresses. The addresses are translated on the IP header, but not always on encapsulated IP addresses (on the application header).

The SIP conveys private RTP negotiation IP addresses/ports. The (RTP) audio flow may be locked by the client's NAT network devices due to unknown (untranslated) addresses.

The solution proposed via the SBC service allows you to offer telephone services to an SIP operator, by passing through the network devices of the client managing the NAT, and if necessary, compensating for the NAT for the network devices that do not fully manage the NAT for encapsulated IP addresses.

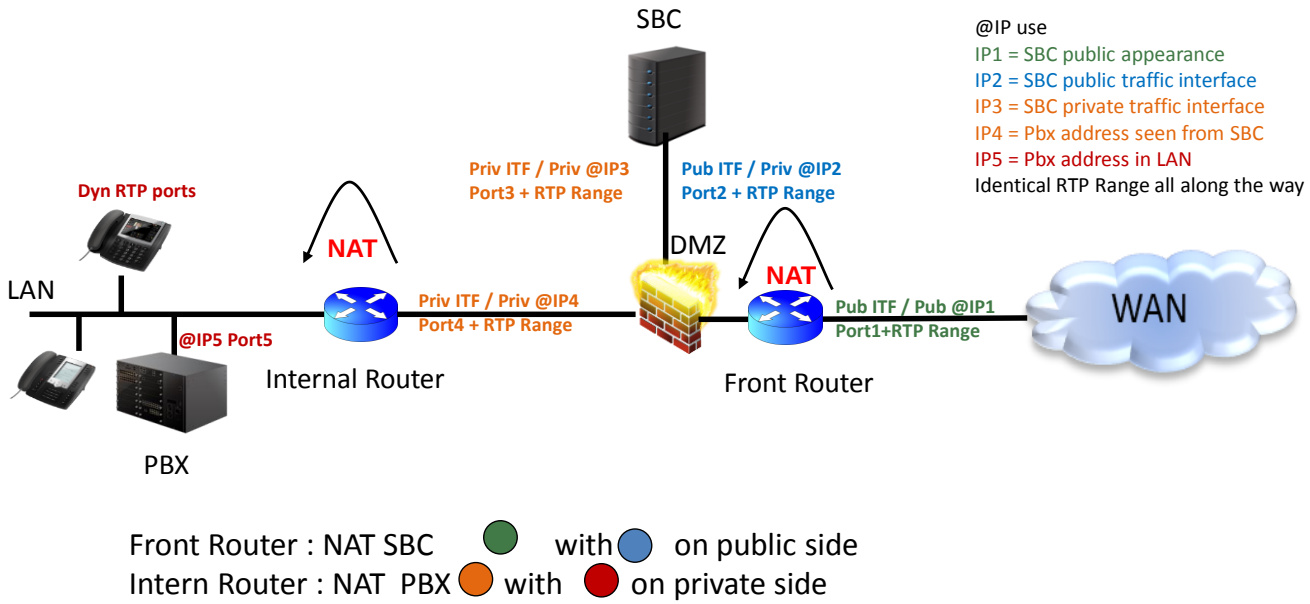
## 2.2 RESTRICTIONS ON THE USE OF THE SBC TRUNK SERVICE

This service can only be used for SIP trunk connections. (No remote subscribers)

## 2.3 SBC TRUNK SERVICE ARCHITECTURE

Different architecture cases must be considered. This paragraph only describes the most frequent cases.

### 2.3.1 STANDALONE SBC IN THE DMZ (DOUBLE NAT)

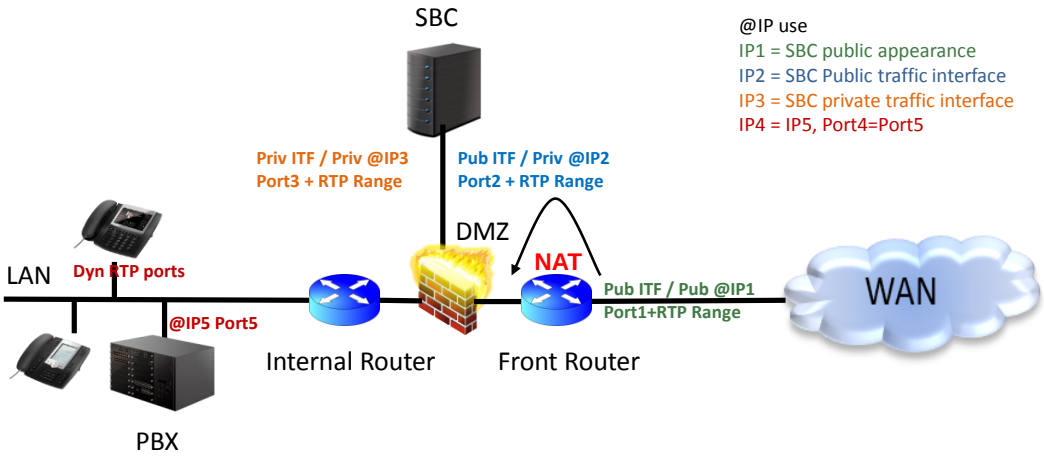



In this architecture, the address is translated on both sides:

- Between the LAN and DMZ (private side)
- Between the WAN (the internet) and DMZ (public side).

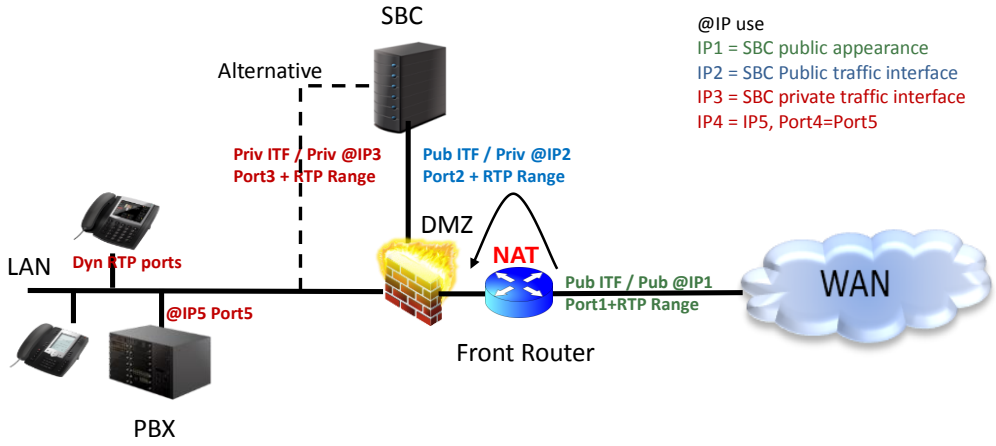
Other alternatives are possible from this general case. See the following sections.

## 2.3.2 NAT ON THE PUBLIC SIDE WITH IPBX AND SBC MODULE ON DIFFERENT NETWORKS (SIMPLE NAT WITH ROUTER)



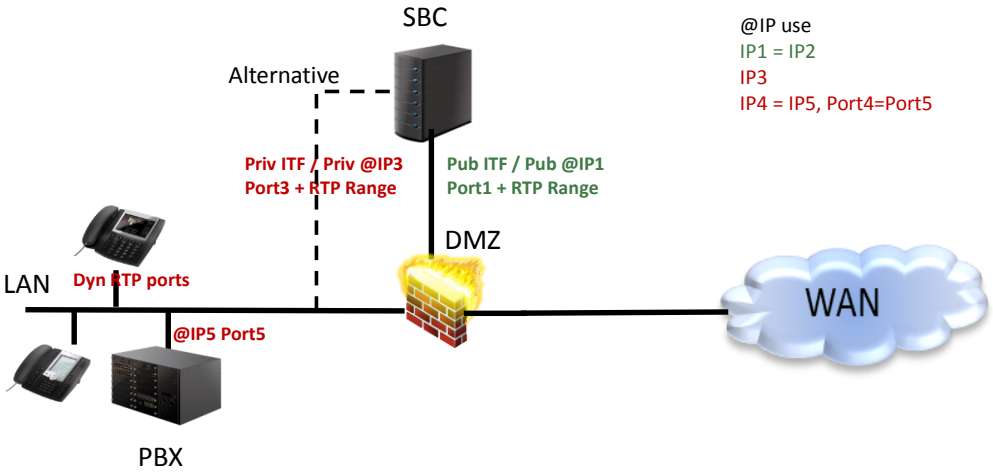

Front Router : NAT SBC 🟢 with 🔵 on public side
Intern Router : No NAT. But PBX and SBC in ≠ subnets.
PBX reachable by SBC with 🔴

### 2.3.3 NAT ON THE PUBLIC SIDE WITH IPBX AND SBC MODULE ON THE SAME NETWORK (SIMPLE NAT)




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

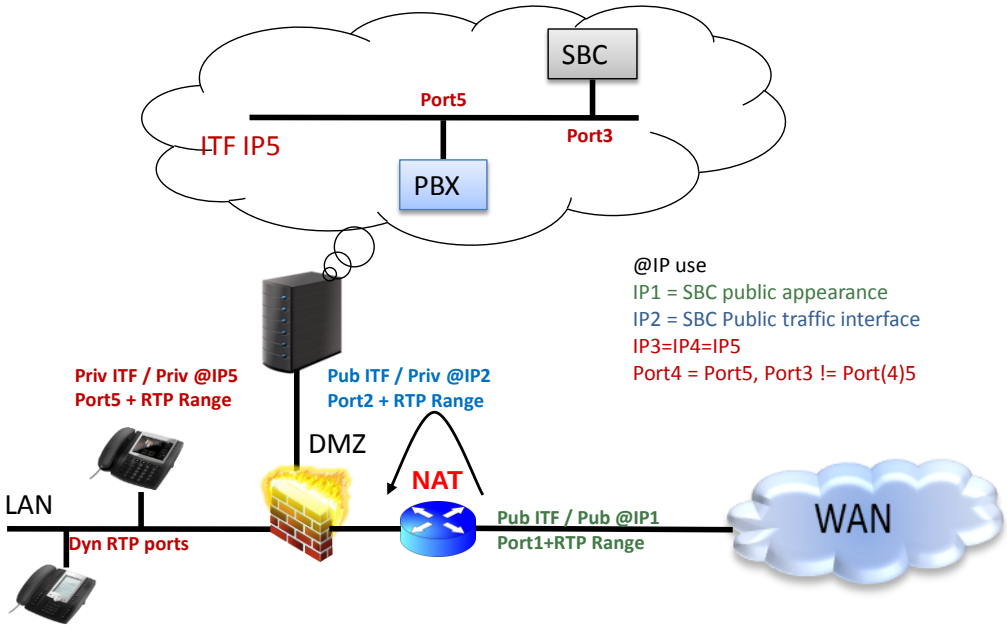
### 2.3.4 NO NAT



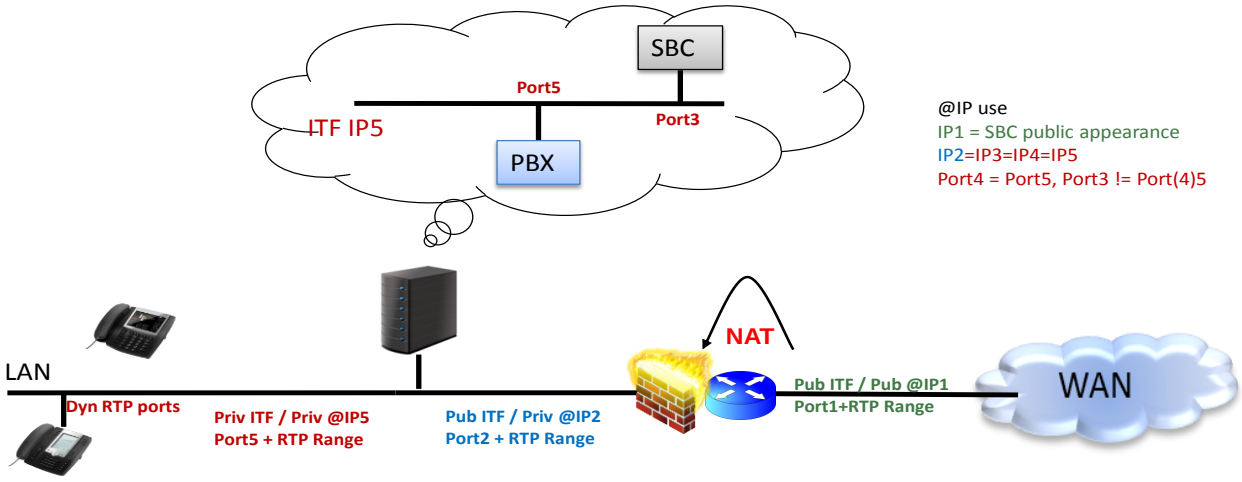

Front Router : No NAT. SBC reachable from internet through

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

### 2.3.5 SBC AND IPBX LOCATED IN THE SAME DMZ



### 2.3.6 SBC AND IPBX LOCATED ON THE LAN WITHOUT DMZ



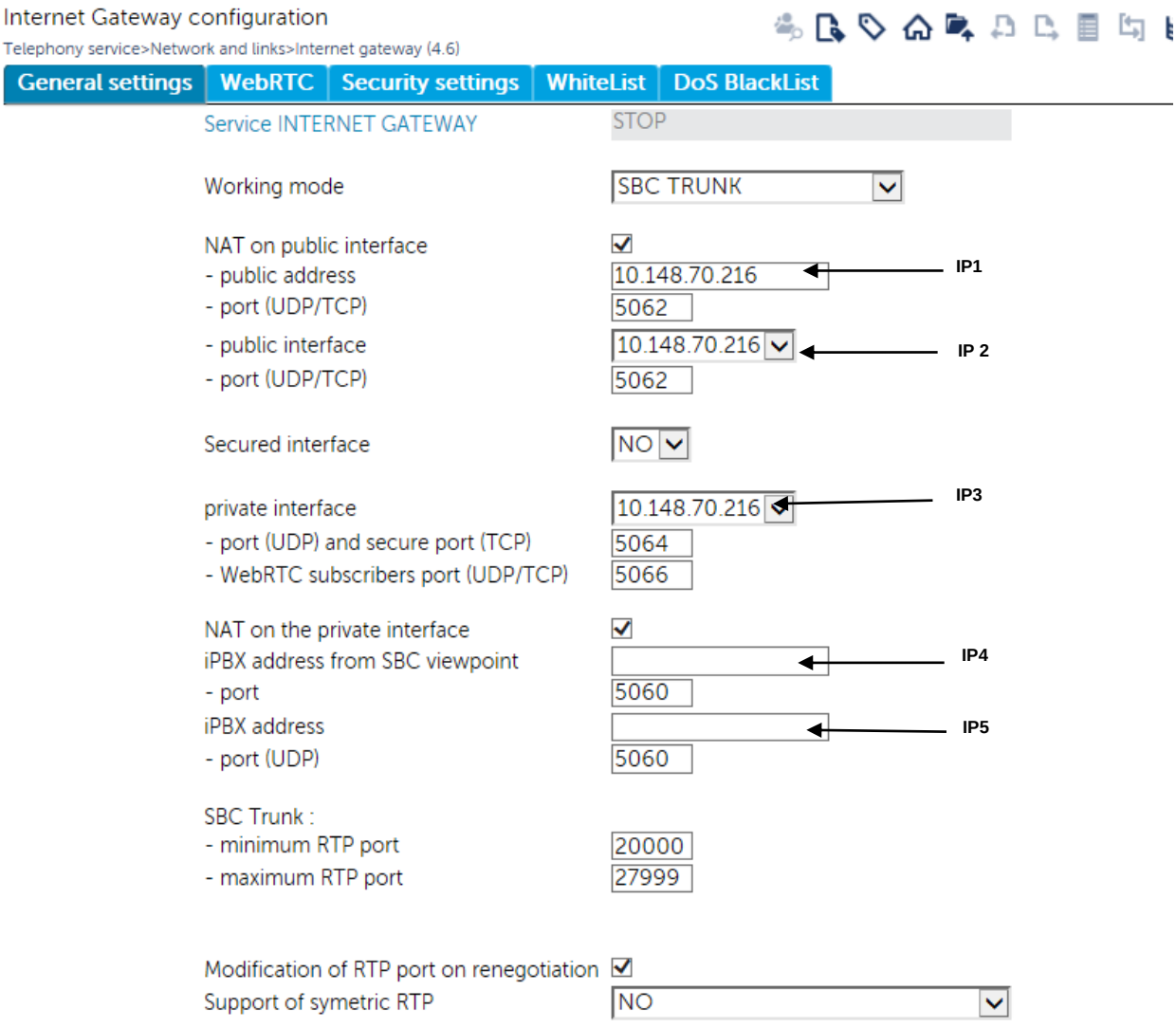

# 3

# 3 CONFIGURING THE SBC SERVICE FROM WEB ADMIN

## 3.1 GENERAL PARAMETERS OF THE INTEGRATED SBC SERVICE

Depending on the network architecture chosen (See Paragraph 2.3), the menu **NETWORK AND LINKS>Internet Gateway – General parameters** tab is used to define the different addresses and ports associated with the SBC service:

- **IP1**: public IP address and port dedicated to the SBC service (used by the remote client to reach the SBC)
- **IP2**: private IP address and port of the SBC interface managing public traffic. This address must be chosen from the system interfaces.
- **IP3**: private IP address and port of the SBC interface managing private traffic. This address must be chosen from the system interfaces.
- **IP4**: private IP address and port dedicated to the SBC service used to reach the iPBX.
- **IP5**: IP address of the iPBX. By default, the address and port are those of the iPBX SIP service.




**Note : The INTERNET GATEWAY Service line indicates the status of the SBC service. To modify it, click the hypertext link which redirects to the services configuration menu.**

**NAT on the public interface**

The box must be ticked when the NAT is implemented on the public network side.

- Enter the IP1 and IP2 addresses (respectively the SBC public address and interface).

**Note : On the company's Firewall router, the static NAT must be implemented between IP1 and IP2.**

If there is no NAT on the public side (the SBC has an interface with a public IP address):

- Enter **IP2** only.

**IP1** is then automatically entered with the same value as **IP2**.

**NAT on the private interface**

The box must be activated when the NAT is performed on the private network side.

- Enter the **IP3** address and **IP4** address (private interface and address respectively).

If there is no NAT on the private side:

- Enter **IP3** only.

**IP4** is then automatically entered with the same value as **IP3**.

Note that **IP1** and **IP4** can receive all the possible IP addresses. On the other hand, **IP2** and IP3 are restricted only to the IP addresses of the machine on which the MMC is executed.

The fifth address (**IP5**) is the PBX address, with its port (signalling part).

The RTP configuration includes the RTP port variation range (example 20,000 to 28,000) and the choice of RTP port change on an SIP renegotiation (audio/video flow part). The static NAT must be implemented on the router/firewall if IP2 does not have any public IP address.

Entering an incorrect IP address displays a "syntax error" message. The IP addresses 0.0.0.0 and 255.255.255.255 are not authorised.

Entering an incorrect RTP port displays the message "outside base stations", indicating the possible variation range. At least 4 ports are required for a radio communication (1 public RTP, 1 public RTCP, 1 private RTP and 1 private RTCP) and 8 in video.

## 3.2 STARTING THE INTEGRATED SBC SERVICE

Menu Telephony **service>System>Configuration>Services (2.3.1)** is used to Start / Stop / Restart the SBC service.

## 3.3 LICENCE

The SBC service does not require any special licence.

## 3.4 SECURITY LEVEL

### 3.4.1 PRINCIPLE

The SBC provides the following services on MiVoice 5000 Server only and for trunk calls:

- NAT signalling/media
- Audio/video transport
- Defence against SIP DoS (flooding or Malicious call) and SIP DDoS attacks.

The security service can be activated to protect the system against certain Flooding-type DoS or DDos attacks:

- **DoS**, using a white list (trusted IP addresses) and a black list
- **DDoS**, using a filter.

As the SBC service is dedicated to the SIP trunk, the protection against **Force Brute** attacks is not implemented.

Regardless of the activation of security, the SBC is protected against Malicious Call-type DoS attacks.

The white list ( **Whitelist tab)** comprises some trusted IP addresses declared by the installer. However, these IP addresses remain subject to checks against Malicious Call attacks.

The black list (**Blacklist DoS** tab) is not configurable and is filled in dynamicallly by the IP addresses considered as attacking.

These IP addresses are contained in the security criteria defined for SIP DoS (flooding or Malicious call) attacks.

The IP addresses are entered for a configurable period (1 hour by default). The list can also be cleaned by the installer (see next paragraphs).

### 3.4.2 CHOOSING THE SECURITY LEVEL

Menu **NETWORK AND LINKS> Internet Gateway – Security parameters** tab

The first parameter is used to configure the implemented security parameter.

The options proposed by the dropdown list are:

- **None**
- **Self protection**
- **Whitelist only**

Description of the different options:

**None:**

The **Whitelist** tab is not accessible.

Even if security is disabled, Malicious Call check is systematically made; the **DoS BlackList** tab is proposed.

### Self-protection

For the "self protection" level the **Whitelist** and **Blacklist DoS** tabs serve as a filter.

The **Whitelist** tab contains the list of IP addresses entered by the operator.

The **Blacklist DoS** tab contains the list of IP addresses identified by the SBC as coming from devices considered as attacking.

These IP addresses are contained in the security criteria defined for SIP DoS (flooding or Malicious call) attacks.

These addresses are automatically removed from the list after a configurable period (one hour by default).

The list of IP addresses on the Blacklist is configurable. When this limit is reached, the oldest entries are deleted.

Any request from a blacklisted IP address is not answered.

It is used to see, at an instant T, the non-trustworthy IP addresses preceded by the registration date and time.

**Whitelist only**

In this case, only the **Whitelist** tab is proposed, with the list of IP addresses entered by the operator.

It is used to manually define 100 trusted IP addresses .

**DoS security parameters**

The following three parameters concern DoS security.

- **Threshold**: 10 to 5000 (number of SIP requests authorised by window before incoming requests are blocked)
- **Window** (seconds): 2 to 10 (sampling period in seconds)
- **Period**: period after which the content of the DoS blacklist is deleted; possible values are 30 seconds, 5 minutes, 30 minutes, 1 hour, 1 day, 1 week, indefinite.

**DDoS security parameters**

The following two values concern DDoS

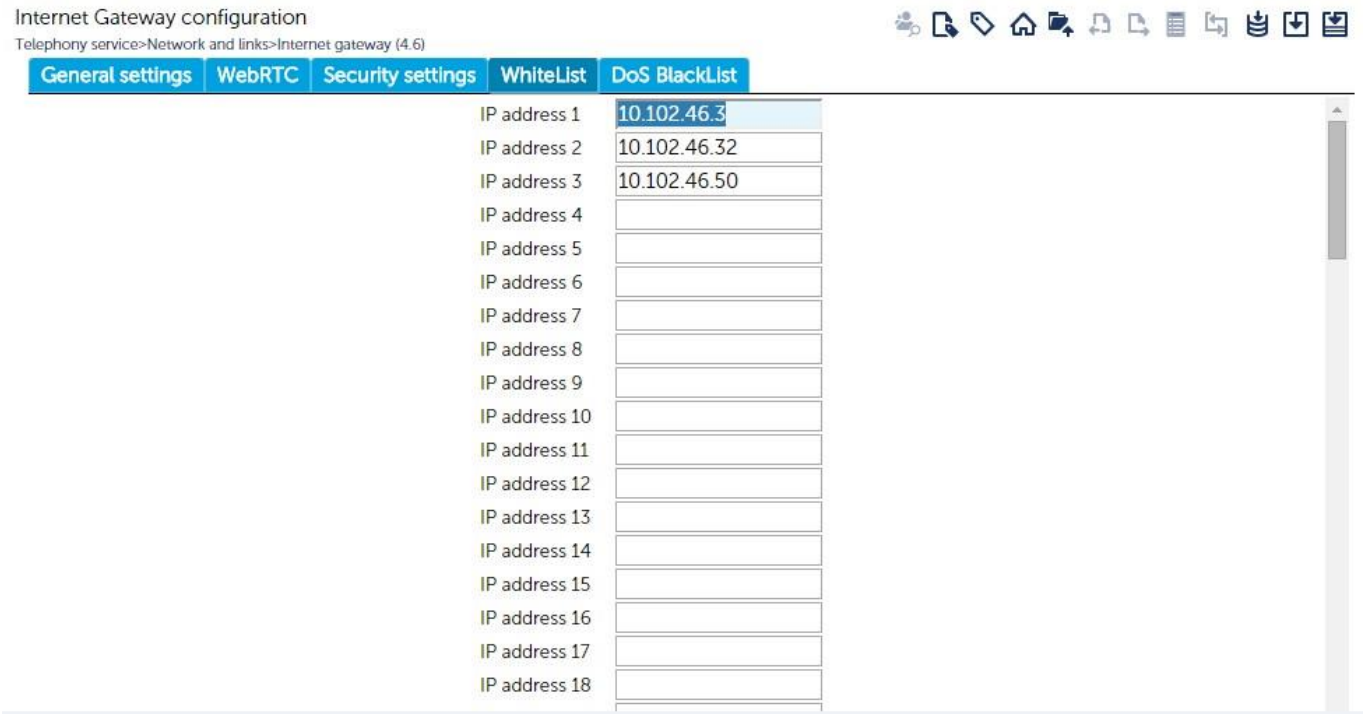
- **Threshold**: 10 to 5000 (number of SIP requests authorised by window before incoming requests are blocked)
- **Window** (seconds): 2 to 10 (sampling period in seconds)

**Delete DoS blacklist**

After confirming the delete action, this option allows all the DoS blacklist inputs to be deleted.

### 3.4.3 MANAGE WHITELIST

Menu **NETWORK AND LINKS> Internet Gateway** – **WhiteList** tab

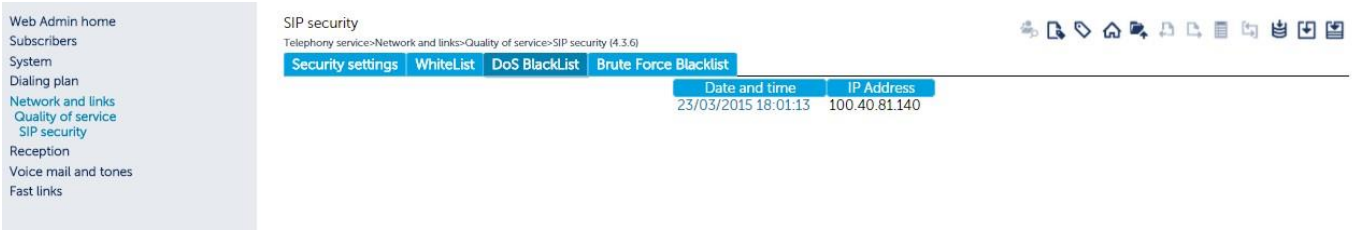



In this tab, each line is used to enter an IP address.

100 trusted IP addresses may be entered.

An error message is displayed when the field is validated.

### 3.4.4 MANAGE DOS BLACKLIST




Menu **NETWORK AND LINKS>Internet Gateway** – **Dos BlackList** tab

Each line of the table displays a blacklisted address and is used to select the address to be deleted.

To delete an address, click on the hypertext link in the first column.

On this screen, the deletion is only effective if the confirmation button is pressed.

After the deletion, the DoS Blacklist is automatically opened.

On the deletion screen, the repeated command is possible, which is used to delete a series of addresses selected on the list of existing addresses from the one selected.

### 3.4.5 SECURITY LEVEL STATUS DURING A FIRST INSTALLATION OF R6.1

During a first installation, the security level is set to **self-protection.**

### 3.4.6 SECURITY LEVEL STATUS WHEN THE SOFTWARE IS UPGRADED TO R6.1

Upgrade strictly for releases below **R5.4 SP2 to R6.1**:

The level of security is on **None** (no SBC service available in initial releases).

Upgrading releases **R5.4 SP2 or later to R6.1**:

If the SBC security was deactivated, the security level will be on **Self-protection.**

If the SBC security was activated, the security level will be on **Self-protection** and the static Whitelist will be updated.