

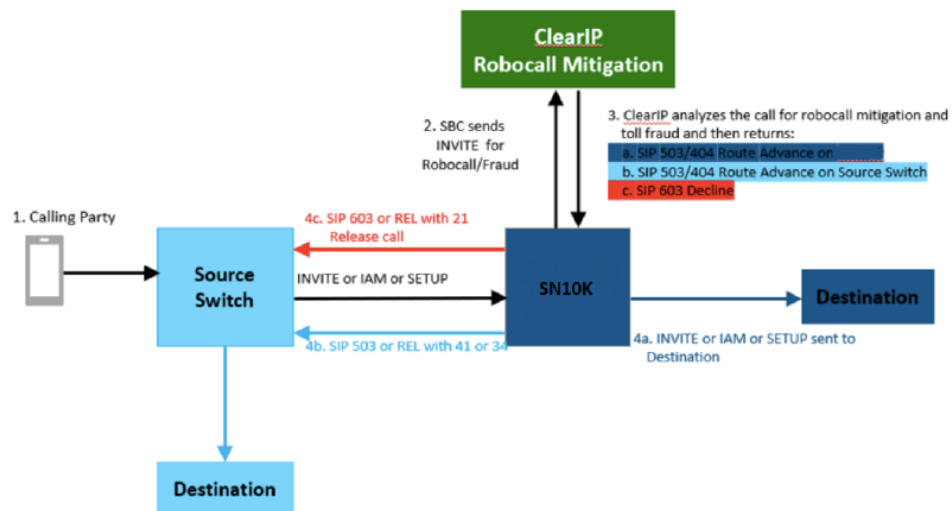
SN10K Configuration for Robocall Mitigation with Transnexus ClearIP service

Introduction

This document provides instructions on how to configure SN10K to operate with the TransNexus ClearIP server for Robocall Mitigation. ClearIP is a SIP redirect server that provides advanced Least Cost Routing (LCR), fraud control and STIR (Secure Telephony Identity Revisited) / SHAKEN (Secure Handling of Asserted information using toKENs) features. SN10K smartmedia **3.0.90** or a later version is needed to support Robocall Mitigation with TransNexus.

Typical Call Scenarios

This section provides the simplified network diagram with typical call flows.



1. Source of Service Provider sends a call to SN10K.

2. SN10K forwards the call to ClearIP for Robocall Mitigation process

3. ClearIP analyzes the call for robocall mitigation and toll fraud, then sends one of the following responses to SN10K

- `_3_a._SIP_404_Not_Found:_No_fraud_is_detected,_not_a_robotcall._`

- `_3b.SIP 503 Service unavailable: No fraud is detected, not a robocall.`

- `_4_c._SIP_603_Decline:_Fraud_is_detected,_block_the_call._`

4. Upon receiving 404 or 503

4a: - SN10K returns SIP 503 (or mapping to the TDM cause code) to the Source switch to perform route advance

Call Source (TDM or SIP) -----Invite or SETUP or IAM -----> SN10K ----Invite--> ClearIP

Call Source (TDM or SIP) <---SIP 503 or REL with 41 or 34 ----- SN10K < ----503---- ClearIP

4b: - SN10K route advances on SIP 503 and sends call to next destination, does not return response to the Source switch

Call Source (TDM or SIP) ---Invite or SETUP or IAM ----> SN10K ----Invite--> ClearIP

SN10K < ----503---- ClearIP

SN10K ----Invite---Next Routes

5. Upon receiving 603

4c: SN10K returns SIP 603 (or mapping to the TDM cause code) to the Source switch, then release the call

Call Source (TDM or SIP) ----Invite or SETUP or IAM -----> SN10K ----Invite--> ClearIP

Call Source (TDM or SIP) <---SIP 603 or REL with 21 ----- SN10K < ----603---- ClearIP

SN10K Configuration

This section provides SN10K configuration for the solution.

Configure Routing Script

SN10K is configured to use routing script to send some SIP headers to ClearIP to identify the source of the call.

1. Enable routing script

Gateway->Use script

2. Load routing scripts

Gateway->Routes->Routing Script->Import Script File

File->ClearIP_Query.rb

ScriptType->filter

Load on startup->checked

Gateway->Routes->Routing Script->Edit the main script:

- •_- Add the "require 'ClearIP_Robo' unless defined?(ClearIPQuery)" statement at the top of the main script.
- •_- Add the "include ClearIPQuery" statement in the main routing class.
- •_- Add the filter " before_filter :method => :ClearIP_query" in the main routing class.

Configure Transport Server for ClearIP NAP

SIP -> Create New Transport Server

Name->TS_TCP_5060

Port Type->TCP

Port->5060

IP Interface-> Select the IP interface which can reach to ClearIP on the public network

Configure ClearIP NAP

NAPs->Create New NAP

Name->NAP_CLEARIP

Proxy address->sip.clearip.com (FQDN of ClearIP-A)

Configure Routes

You need to configure other routes after the ClearIP routes if you want SN10K to perform route advances.

Configure Route Retry Action

Route retry action of 3xx, 404 and 603 must be configured to allow SN10K to perform failover, fraud control and SHAKEN AS/VS request.

Profiles->Edit Reason Cause Mapping

404 Not found->Route retry action->Continue call

503 Service unavailable->Route retry action->Continue call

603 Decline->Route retry action->Stop call

Notes:

- •_The_default_route_retry_action_of_404_is_Stop_call._
- •_The_default_route_retry_action_of_603_is_Continue_call._