

SIP Pulse TFPS

February

2016

User
Administrator
Guide

Versão do Sistema: 2.0.1

This document is targeted to SIPPulse TFPS users. All rights reserved. ©2009/2016 SIPPulse Tecnologia Ltda.

Sumário

1. INTRODUCTION	3
2. PROTECTION	4
3. SYSTEM ENTITIES	5
3.1 BASE SYSTEM	5
3.2 TFPS	5
3.3 DOMAIN	5
3.4 SUBSCRIBER	5
3.5 SECURITY POLICIES	5
3.6 RESPONSE CODES	5
3.7 BLACK AND WHITE LISTS	5
4. OPERATIONAL REQUIREMENTS	6
5. OPERATIONAL MODEL	7
6. OPERATING TFPS	7
6.1 DOMAIN BASED CONTRACT	7
6.2 SUBSCRIBER BASED CONTRACT	7
7. OPERATING TFPS: DOMAIN BASED	8
7.1 LOGGING ON AS A DOMAIN ADMINISTRATOR	8
7.2 RESPONSE CODES	9
7.3 SECURITY POLICIES	10
7.4 SUBSCRIBERS	13
7.5 SYSTEM ADMINISTRATORS	13
7.6 FRAUD REPORT	15
7.7 HISTORY REPORT	16
7.8 LOGGING OFF	16
8. OPERATING TFPS: SUBSCRIPTION (ACCOUNT) BASED	16
8.2 RESPONSE CODES	17
8.3 SUBSCRIBERS	18
8.4 MANAGING SECURITY POLICIES	18
8.5 FRAUD REPORT	21
8.6 HISTORY REPORT	22
8.7 LOGGING OFF	23
9. LIMITATION	23
9.1 SECURE ENVIRONMENTS	23
9.2 USAGE CONDITIONS	23
9.3 TFPS CONTRACT CONDITIONS	24
10. HOW TO INTEGRATE TFPS TO YOUR PBX/SOFTSWITCH	25
SINGLE POLICY INTEGRATION	25
MULTIPLE POLICY INTEGRATION	25

<i>IP+CLI</i>	25
<i>IP+X-TFPS</i>	25
INTEGRATION USING SIP REDIRECT	26
INTEGRATION VIA WEBSERVICE	28
INTEGRATION EXAMPLE WITH ASTERISK	30
<i>sip.conf</i>	30
<i>extensions.conf</i>	30
<i>Response Codes</i>	31
INTEGRATION EXAMPLE WITH FREESWITCH	31
<i>/usr/local/freeswitch/conf/sip_profiles/external/tfps_gw.xml</i>	31
<i>/usr/local/freeswitch/conf/dialplan/default/tfps_dialplan.xml</i>	31
<i>Response Codes</i>	32
INTEGRATION EXAMPLE WITH OPENSIPS	32
OPENSIPS INTEGRATION	33
<i>/etc/opensips/opensips.cfg</i>	33
<i>Response Codes</i>	34
INTEGRATION EXAMPLE WITH ELASTIX/FREEPBX	34
<i>FreePBX Integration</i>	34
<i>extensions_custom.conf</i>	35
<i>Response Codes</i>	36
11. DISCLAIMER AND LIMITATION OF LIABILITY	37

1. Introduction

While technology has brought several improvements for our day-to day personal and professional lives, it has also created a growing field of opportunities for fraudsters to act. Ever since the World Wide Web became the birth of most B2B and B2C transactions, a group of people have been dedicated to find new ways to fraud authentic business.

It has not been different with telephone networks. Fraud in this business is not new. In the past, with analog technology, the most common ways to fraud was related to subscription and unauthorized use directly in to end user terminals. In some cases tampering with physical networks were also an issue, while in all cases the focus was to steal services. Today, however, as telephony networks migrated to the IP world, fraud has become more and more sophisticated and fraudsters are now targeting financial gains way beyond just services.

In recent years, worldwide telephone operators have reported around US\$50B in yearly fraud, of which around 30% are related to traffic pumping (premium rate numbers and traffic revenue share), a method in which PBX systems and/or telephone operators are hacked to generate traffic over long distance international calls. Because of international traffic agreements, revenue generated by such calls are shared between originating and destination operators. In some cases, the destination number are special services which pay a rebate fee to the destination call customer, hence becoming of interest to fraudsters.

2. Protection

SIPPulse TFPS adds in a new method of real time protection against traffic pumping by adopting a crowdsourcing approach in which potentially fraudulent event is stored in a knowledge base used for every follow on check by every TFPS user.

TFPS acts integrated to PBX/Softswitch, which needs to be programmed to submit elected calls to TFPS. The system will then verify the call against a set of parameters, managed by users, rules run by a specially designed algorithm and a knowledge base performing a real time query on selected calls to check against the probability of being a fraudulent call, thus reducing the exposure of PBX and Softswitch environment.

Parameters set by the user are:

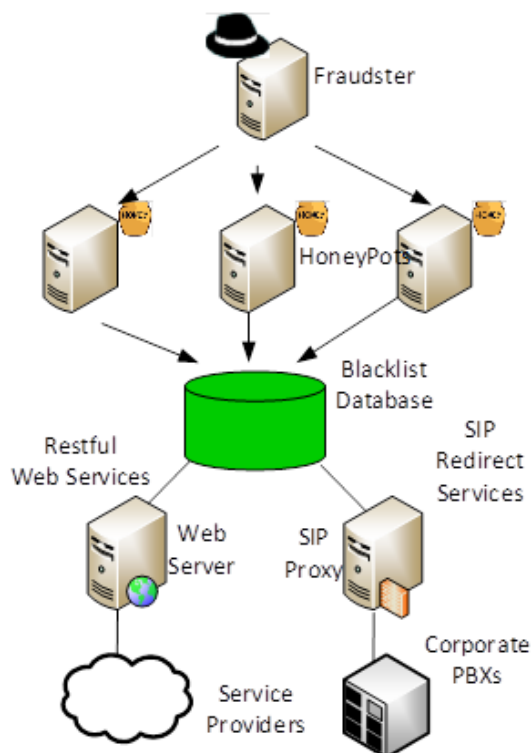
- Number of sequential calls in a given period;
- Number of concurrent calls and daily quota, for working hours and off hours;
- Off-hours rules;
- Call Origin and Call Destination (Forbidden and Allowed);
- White and Black list for each policy.

Once user parameters are verified, TFPS will check a series of system parameters and records to determine the call status. The main system parameters check are:

- IP Black list
- B Number black list
- User Agent Black list
- Other system defined data and algorithm

These black lists and algorithms are build and feed by every event checked by the system during user operations as well as a series of honey-pots kept by SIPPulse around the world wide web.

The system will not take any action over the call itself. It will mark the call with specifically defined codes, and return the call to the PBX/Softswitch, which should be programed to tack action against the call according to the reason code returned.



3. System Entities

3.1 Base System

The base system is your existing PBX or softswitch system. Not every system will work with TFPS. Since TFPS does not take any action over the call it-self (it is not a link between you base system and the PSTN), but rather it will only add a Response Code to the header of the call invitation message. Your base system must be able to handle these response codes. Check with SIPPulse whether your base system is compatible or not.

3.2 TFPS

The highest entity of the TFPS environment is TFPS Knowledge base and Algorithm. The knowledge base contains a set of cumulative data used by an evolving algorithm used to check selected outgoing calls. These components are nested, under the tfps.com root domain.

3.3 Domain

A domain is the second highest entity in TFPS. It typically represent a group of users (subscribers) under a similar set of rules. Domains are typically associated to telephone operators.

3.4 Subscriber

TFPS Works with a set of rules associated to a subscriber entity. Rules are based on usage and user parameters. Subscribers can associated under a specific domain or to TFPS (tfps.com domain which is the root domain in the system. Subscribers are typically represented by a PBX system.

3.5 Security Policies

Security Policies are a set of rules defined by a Domain manager or a Subscriber Manager that composes the first check TFPS performs on a selected call.

Security policies can complement those set on you base system. If your base system is properly configured, the amount of queries in to TFPS will be reduced, thus your monthly fee, so will your exposure to fraud.

3.6 Response Codes

Response codes are a set of codes added by TFPS to the header of the call invitation. These Response Codes will indicate the level of threat a potential of being a fraudulent call. Response codes are pre-set on TFPS and will work as same for all customers using TFPS

3.7 Black and White Lists

Optionally, the customer can add or remove phone numbers and IP in the black and whitelist avoiding the detection and fixing potential false positives.

4. Operational requirements

TFPS does not require any special equipment to operate for SIP based systems, with adherence to SIP Redirect functions. The only requirement in such cases are a reliable and safe network connection to TFPS system.

However, for non SIP (or SIP systems with no support to Redirect Functions) based PBX or Softswitch system TFPS can function through SIPPulse SBC system, which have TFPS capability natively integrated.

As a SIP CPE s, SIPPulse SBC can also be configured to operate as a TFPS gateway avoiding overhead on the base system;

5. Operational Model

TFPS is available to customers as a Domain Based or as a Subscriber. Domain Based is primary intended for telephone operators. In such model, operators can create multiple accounts (subscribers) and have different set of rules for each customer.

Subscribers are generally used by PBX systems, either under an domain managed by an operator (under a domain) or under the root domain managed by SIPPulse.

TFPS contracts are based on the number of queries per second (or CPS). Each level of CPS will have a predefined number of queries per month. Domain based contracts will also have a predefined number of subscribers. Queries and accounts in excess of the predefined volume will be admitted by the system, however affecting the on-going contract. Upon requesting new accounts under its domains, administrators will be asked to validate and confirm his/hers selection as it might affect the contract.

6. Operating TFPS

6.1 Domain based contract

A domain based contract will allow you to create several subscriptions under your domain. This is the recommended model for operators, which will allow you to create and manage a set of security policies per customer (subscriber) or grant them access to manage and create by themselves.

6.2 Subscriber based contract

Subscriber is defined in TFPS as an account that represent an environment (one or more telephony system linked to this account) under a domain, for which you assign a security policy.

A subscription based contract will operate under a domain (either TFPS root domain or an Operator's domain) and will not be able to create additional accounts.

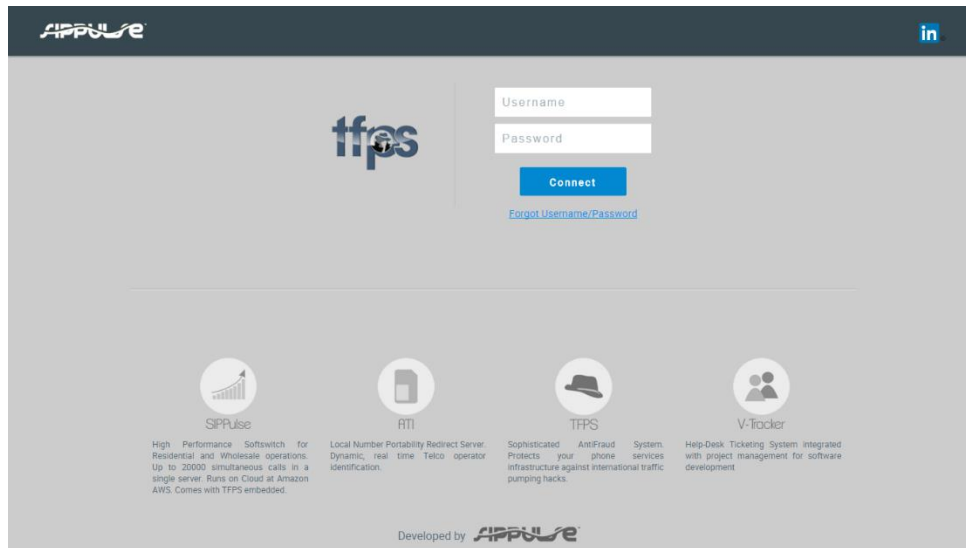
This operational model is typically used by end user companies, which needs a single set of rules to operate TFPS.

7. Operating TFPS: Domain Based

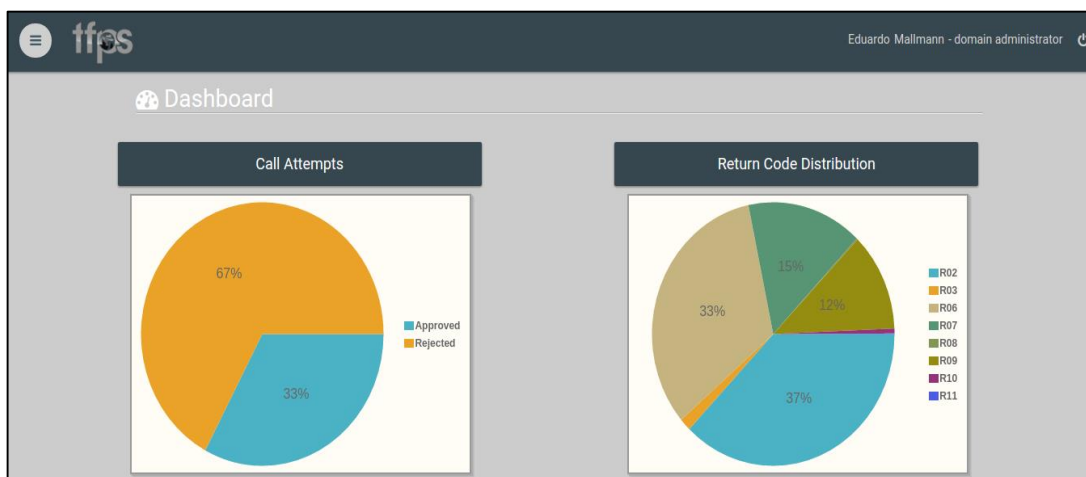
A domain based, contract allows you to create multiple security policies, subscribers and system administrators (additional domain or subscriber's administrator).

7.1 Logging on as a Domain Administrator

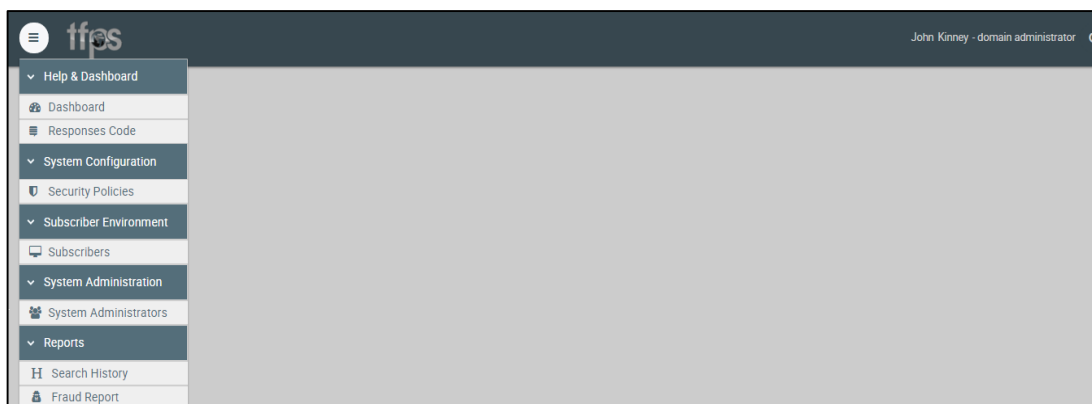
As you contract TFPS you will receive a set of username/ password which you will use to log on the system.



As you log on to the system, you will be directed to dashboard screen which contains performance information for the current day.

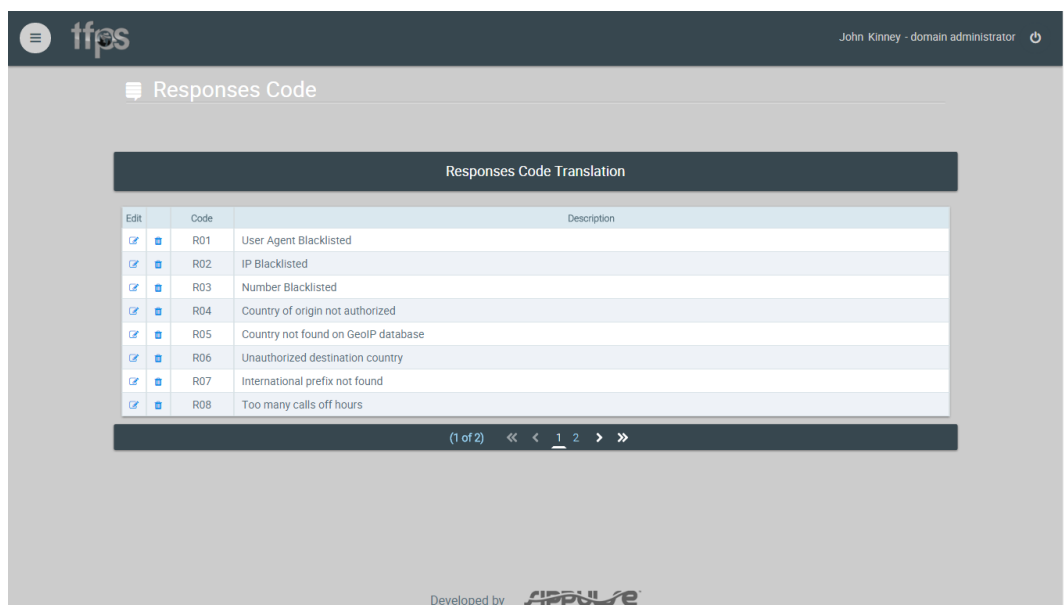


As you click on the options button on the upper right side of you screen a series of commands will be available to you, which will allow you to navigate through the system.



7.2 Response Codes

By selecting, this option you will be displayed a list of responses codes in use by the system. These codes will be used at your base system to handle each call.



Current Response codes are:

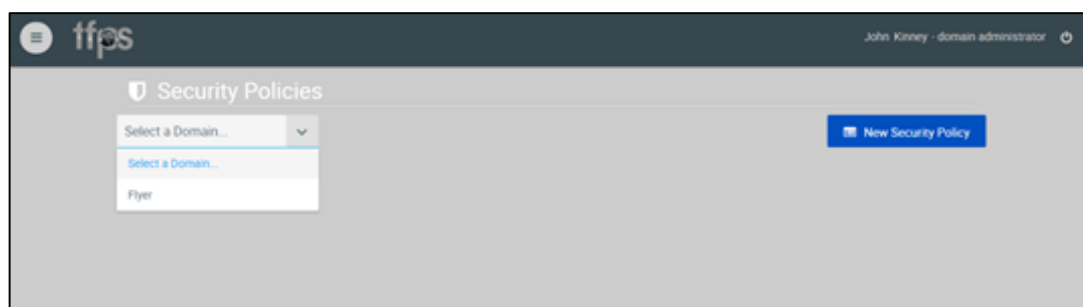
R01	User Agent Black Listed	UA identified as typically used for fraud
R02	IP Blacklisted	IP for originating calls known as fraud source
R03	Number Blacklisted	Destination number included in fraudster black list
R04	Unauthorized Originating Country	Country not allowed for originating a call
R05	Country (Origin or Dest) not found in GeoIP DB	Country not found
R06	Unauthorized Destination Country	Destination country for call not authorized
R07	International Prefix not found	Call dialed with a non-existing Country Code
R08	Too many off-hour calls	Current calls exceeded for offhours
R09	Off hours quota exceeded	Calls exceeded the quota for offhours
R10	Too many normal hours calls	Current calls exceeded for normal hours
R11	Normal hours quota exceeded	Calls exceeded the quota for normal hours
R12	Palestine Gang	Calls coming from a specific set of address
R13	Too Many Simultaneous calls	Calls with same origin and destination on a given time

We can add new response codes on future versions. Reason code displayed on the Domain or Subscriber Administrator interface are for information purpose only. Only SIPPulse team members can add new reason code, which can later be used to configure your system.

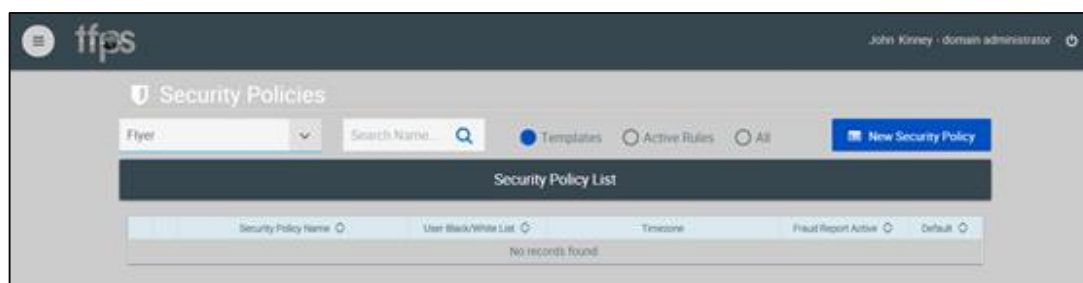
7.3 Security Policies

Security policies are a set of rules defined by user administrators that will complement TFPS internal algorithms and knowledge base to analyze and mark a call with the corresponding Response Code. As an administrator you can set template policies which can be used by your subscribers as a base to their own set of rules.

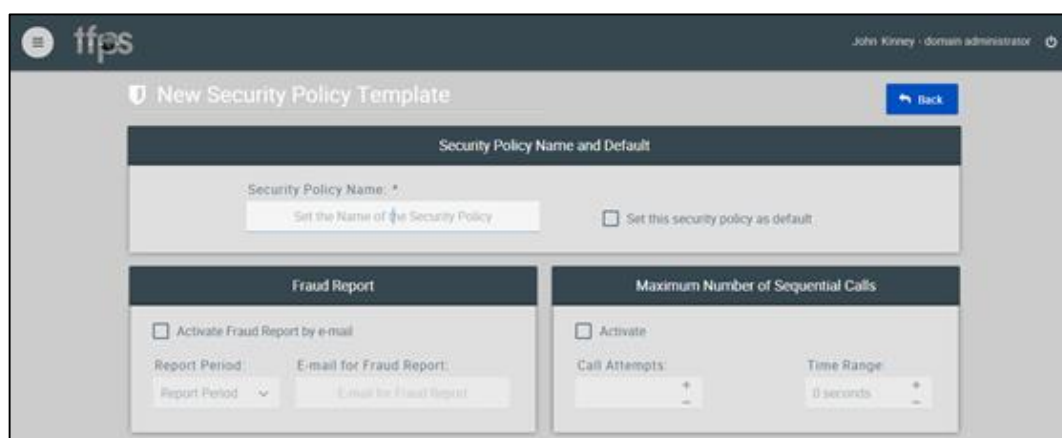
By selecting the Security Policies command, the following screen will be presented:



You must then select the domain to which the policy will be assigned to. A set of pre-existing policies, if any, will be displayed.



By pressing the “New Security Policy” button you will be presented with the following screen:



You then define the name that will be assigned to this specific policy, and mark it as a default policy if that policy should be the basic policy for your domain. Each subscriber will be assigned the default policy if none is set for later. You must also define the destination email for fraud reports and the recurrence it shall be send.

You must also define whether you want TFPS to limit the number of sequential calls on a given period. This will have TFPS mark all calls that exceed this limit with the according response code.

The screenshot displays a web interface for configuring call policies. It is divided into two main sections: 'Call Policy' and 'Off Hours Rules'.

Call Policy Section:

- Max. Concurrent Calls:** A numeric input field with a '+' button above and a '-' button below.
- Daily Quota:** A numeric input field with a '+' button above and a '-' button below.
- Max. C. C. Off-Hours:** A numeric input field with a '+' button above and a '-' button below.
- Daily Quota Off-Hours:** A numeric input field with a '+' button above and a '-' button below.

Off Hours Rules Section:

- Time Zone:** A dropdown menu with the option 'Set the Time Zone...'.
- Day:** A numeric input field with a '+' button above and a '-' button below.
- Month:** A dropdown menu with the option 'All Months'.
- Weekday From:** A dropdown menu with the option 'All Weekdays'.
- Weekday To:** A dropdown menu with the option 'All Weekdays'.
- Hours From:** A numeric input field with a '+' button above and a '-' button below.
- Hours To:** A numeric input field with a '+' button above and a '-' button below.
- Use DST Time Zone:** A checkbox.
- Pattern:** A button labeled 'Pattern'.
- Add:** A blue button labeled 'Add'.

Below the 'Pattern' button, there is a message: 'No records found.'

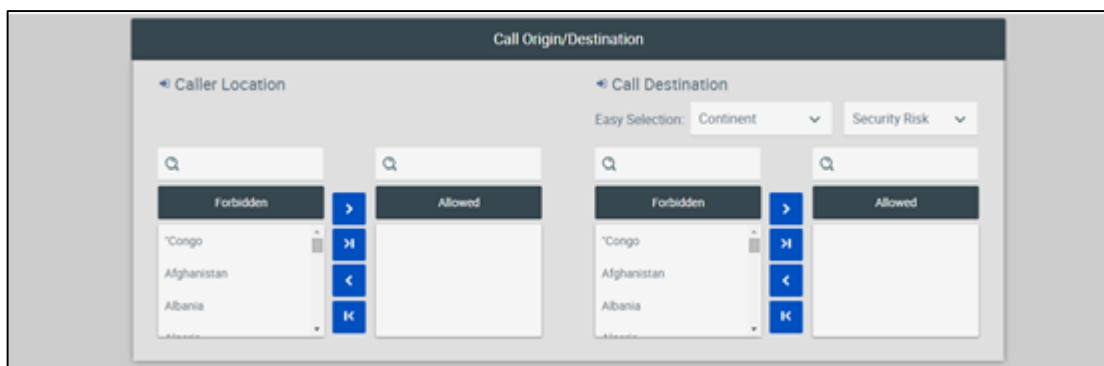
You can also define the maximum number of concurrent calls and a daily quota of calls your system can submit. You can also select the number of concurrent calls and daily quota of calls for off-hours. If you select to use off hours restrictions, these will override the rules set for full day, during the off hours. Off-hours and regular on-hours daily quota will not add up to each other.

You must also define all off-hour period for you operations. For such you must select the time zone, number of days to be applied (leave zero if perpetual), months of the year, days of the week and time period (begin and end of period). You can add as many periods as you wish. However we recommend you to keep it as simple as possible to reduce management complexity. As you add off hour rules, they will be shown on this screen.

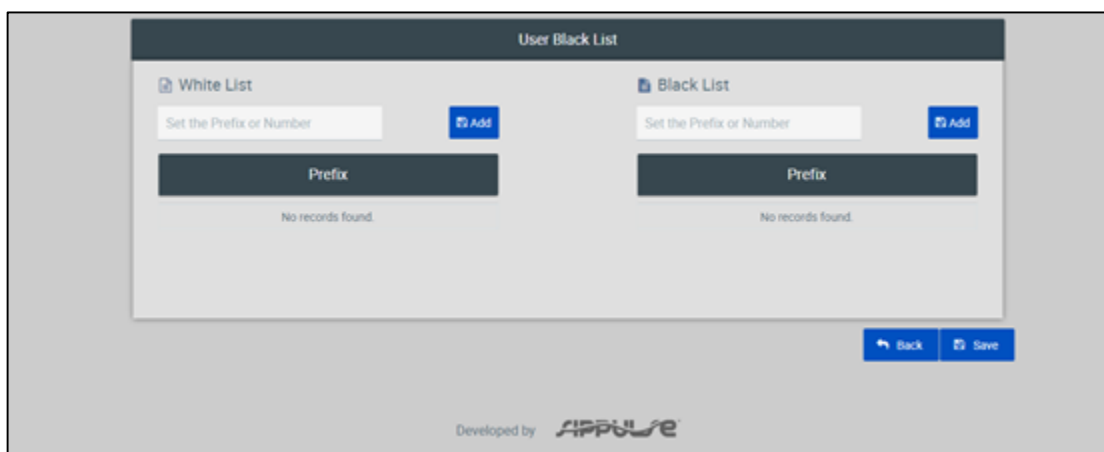
As you submit calls to TFPS analysis, it will check calls against your rules and mark them with the corresponding reason code.

The following rules will define from which countries your policy will accept originating calls and to which countries calls will be allowed to. You can chose to use continents or select a predefined list of countries set base on a risk analysis (low, medium and high risk).

Predefined risk origin and destination are based on aggregated knowledge of origin and destination countries for risk. These predefined risk assessment changes constantly. Please check this list regularly since, once selected it will become static on your rules



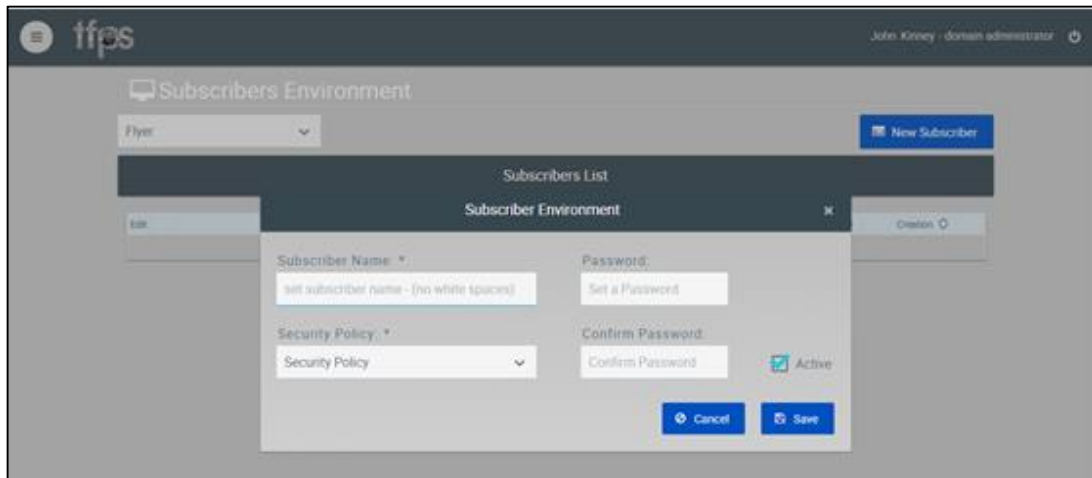
You can finally define a set of white list destination numbers for which TFPS will not perform a check. Numbers included on the policy white list will override the system black list for those subscribers using this policy. You can also add numbers to policy black list. These numbers will not affect other policies. Should you elect to remove a number from a policy white or black list, please contact SIPPulse.



After editing you policy rules, click on the “Save” button and proceed to create new policies or to create your subscribers.

7.4 Subscribers

Subscriber is an account that represent an environment (one or more telephony system linked to this account) under a domain, for which you assign a security policy.



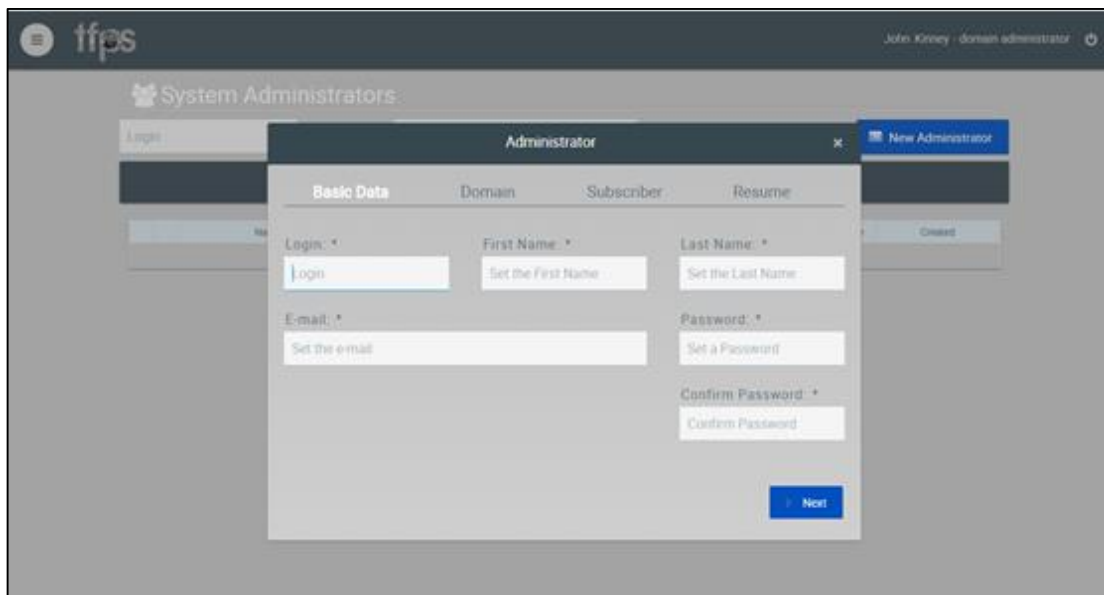
The screenshot shows the 'tfps' interface with the 'Subscribers Environment' section. A modal window titled 'Subscriber Environment' is open, displaying fields for 'Subscriber Name' (with a hint 'set subscriber name - (no white spaces)'), 'Password' (with a hint 'Set a Password'), 'Security Policy' (a dropdown menu), and 'Confirm Password' (with a hint 'Confirm Password'). There is also an 'Active' checkbox and 'Cancel' and 'Save' buttons at the bottom.

Upon creating a subscriber you must assign a username and a password and select a security policy. Once you save your subscriber, you can create additional subscribers.

7.5 System Administrators

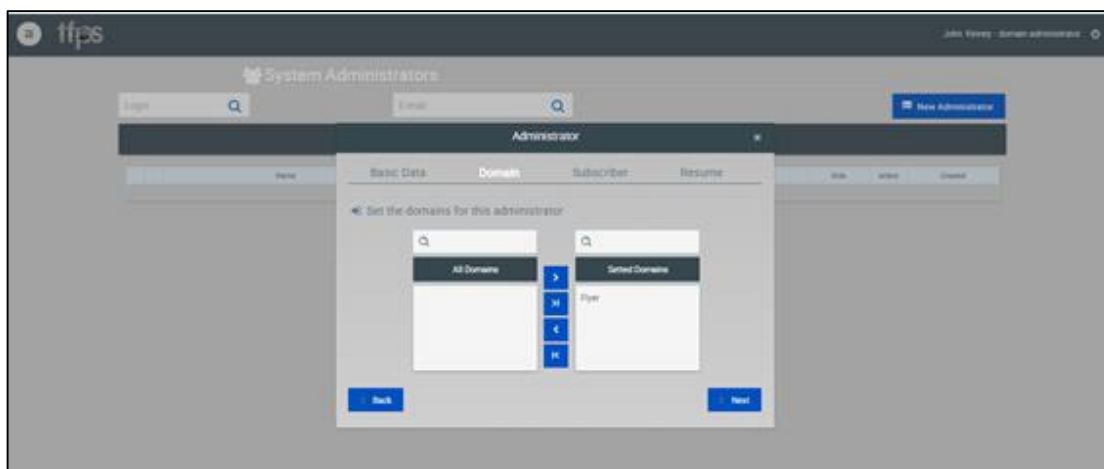
As a domain administrator, you can create both Subscriber Administrator for the subscribers under your domain..

To Create new administrators, select the proper function from the Menu Button and fill in the identification fields shown in the screen below:

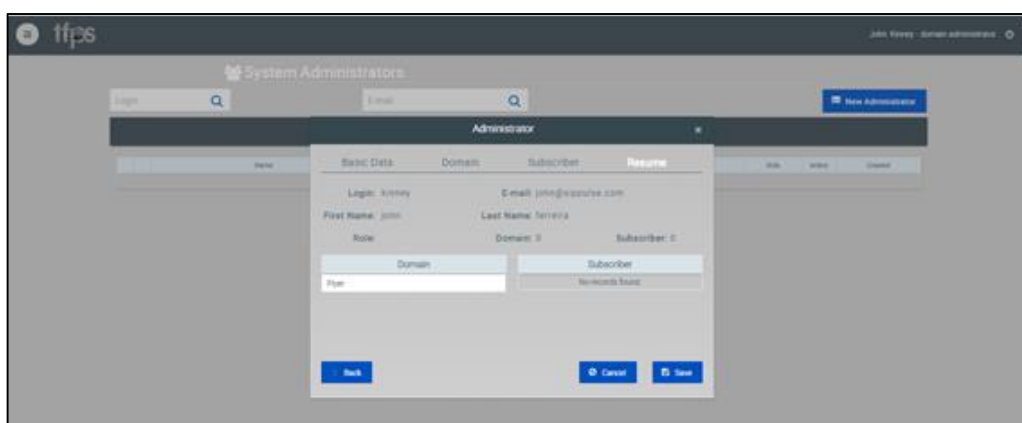


The screenshot shows the 'tfps' interface with the 'System Administrators' section. A modal window titled 'Administrator' is open, displaying fields for 'Login' (with a hint 'Login'), 'First Name' (with a hint 'Set the First Name'), 'Last Name' (with a hint 'Set the Last Name'), 'E-mail' (with a hint 'Set the e-mail'), 'Password' (with a hint 'Set a Password'), and 'Confirm Password' (with a hint 'Confirm Password'). There is also a 'Next' button at the bottom.

Click on the “Next” button so you can move to select the domain associated to that administrator. If SIPPUse assigns you multiple domains, you see them on the left side window. You need to select the domain you wish to retrieve the subscribers which will be assigned to the Subscriber Administrator.

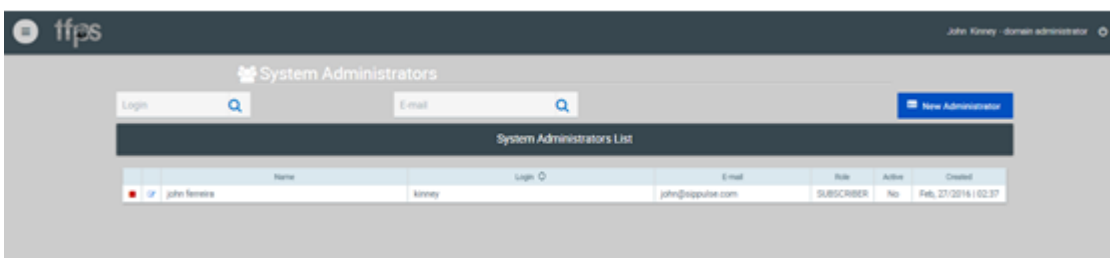


Then select the domain and subscribers you wish to link to the subscriber administrator you are creating. Refer to section 7.4 on how to create subscribers.



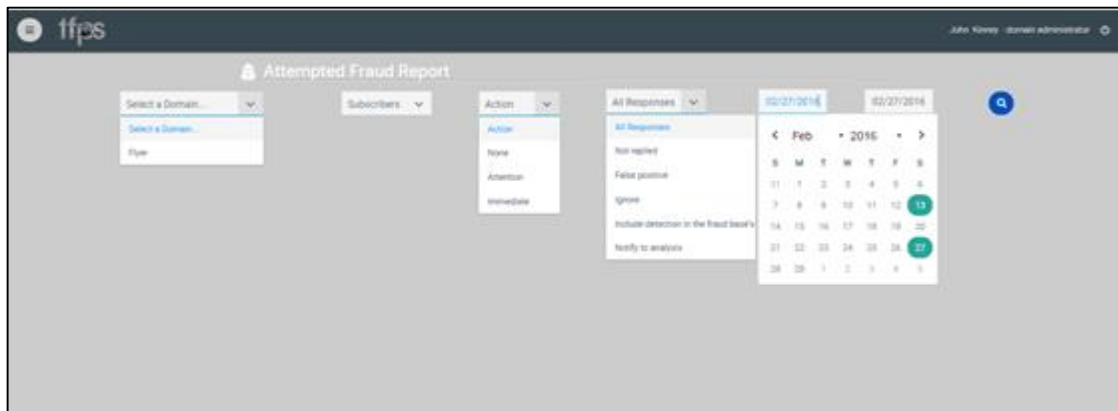
A summary page will then be shown before you can finally save this administrator. Once you review the page, click on Save button or (Back if you need to change any configuration)

To activate this administrator, click on the red selection box shown on the left side his entry row on the Administrator’s list.

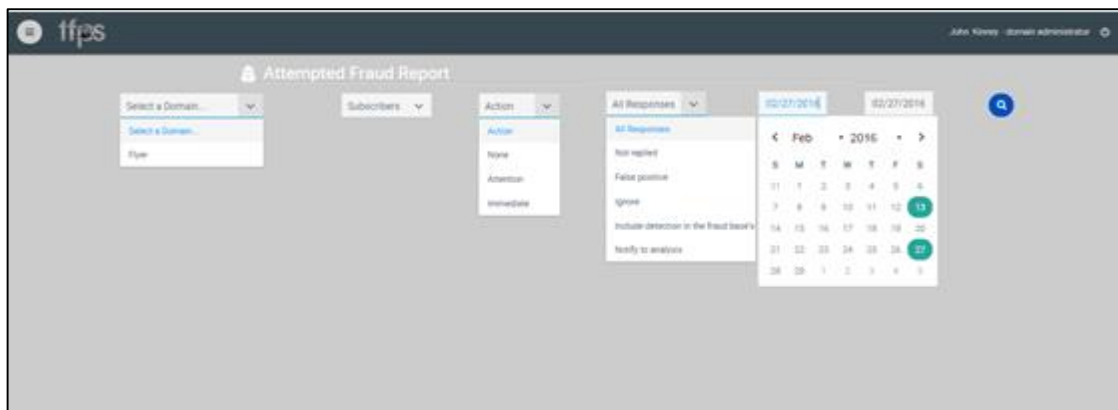


7.6 Fraud Report

Fraud report will allow administrators and subscribers to generate reports of fraud suspected events over transactions checked by TFPS for the corresponding account (or accounts under domains managed by and administrator).



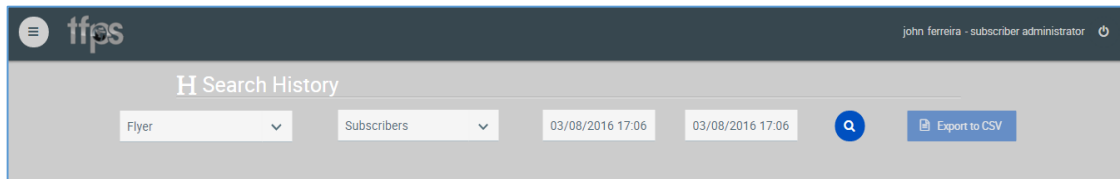
From the pull down menu's shown on the Fraud Report page, select the Domain, Subscriber, Action (which action was taken over the call), response type and beginning and end date for the report.



From the pull down menu's shown on the Fraud Report page, select the Domain, Subscriber, Action (which action was taken over the call), response type and beginning and end date for the report.

7.7 History Report

History report will allow administrators and subscribers to generate reports of queries on the system.



Select the domain and account (only the user account will be displayed if the user is a subscriber) and the beginning and end dates.

7.8 Logging off

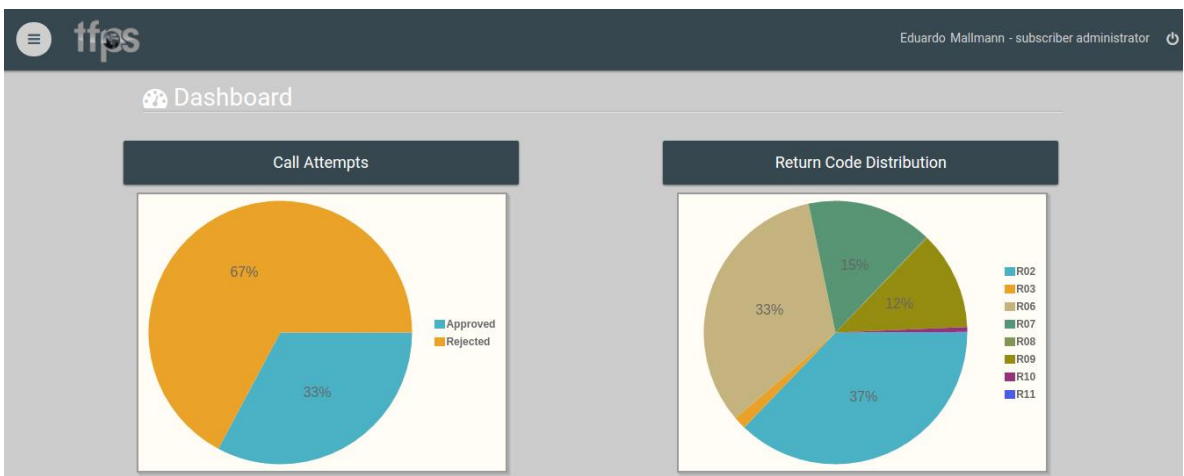
To log off from TFPS, click on the on-off button on the upper right side of your screen and click on the “Logoff” option.



8. Operating TFPS: Subscription (account) Based

Subscription based accounts has fewer management options over the platform. Subscribers will be assigned a security rule predefined by the manager of the domain on which it is nested. However, once the subscriber administrator gains access to the platform, it will be able to manage and changer rules for policies assigned to each subscriber assigned to his administration.

As you log on to the system, you will be directed to dashboard screen which contains performance information for the past 7 days.

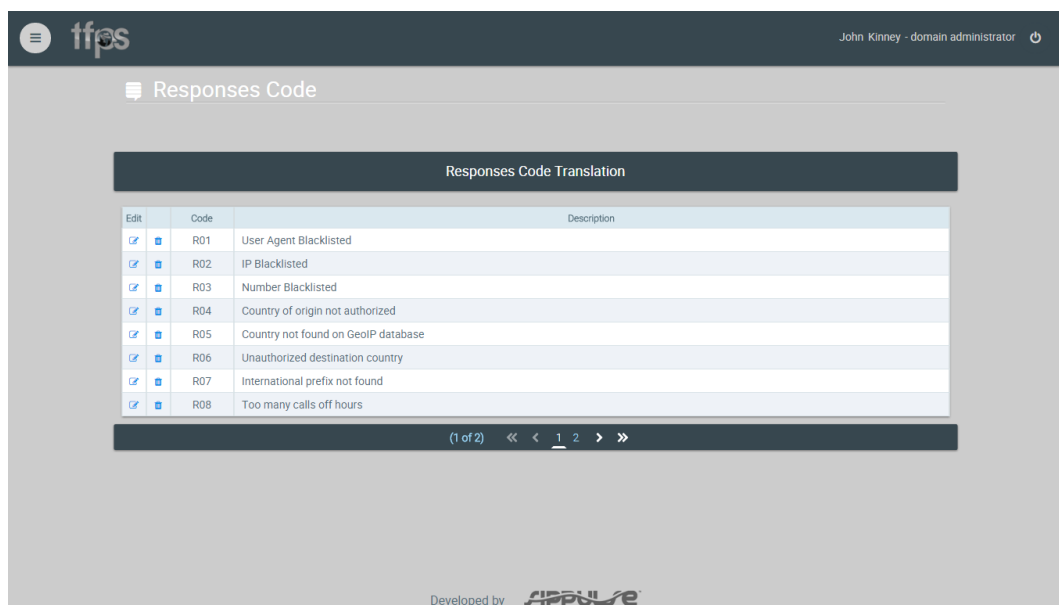


As you click on the Menu button on the upper left side of you screen a series of commands will be available to you, which will allow you to navigate through the system



8.2 Response Codes

By selecting this option you will be displayed a list of responses codes in use by the system. These codes will be used at your base system to handle each call.



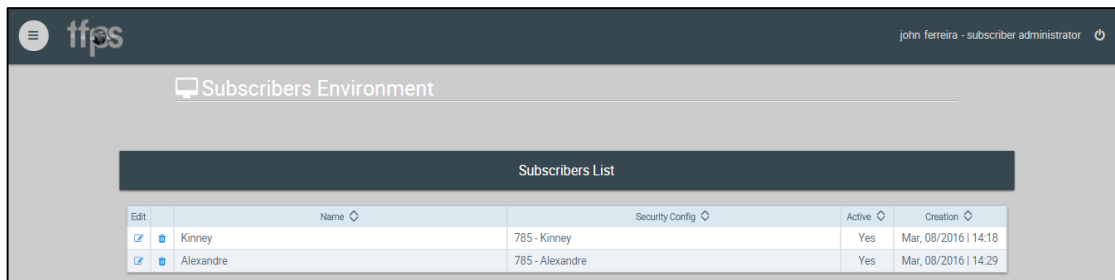
Current Response codes are:

R01	User Agent Black Listed	UA identified as typically used for fraud
R02	IP Blacklisted	IP for originating calls known as fraud source
R03	Number Blacklisted	Destination number included in fraudster black list
R04	Unauthorized Originating Country	Country not allowed for originating a call
R05	Country (Origin or Dest) not found in GeoIP DB	Country not found
R06	Unauthorized Destination Country	Destination country for call not authorized
R07	International Prefix not found	Call dialed with a non existing Country Code
R08	Too many off-hour calls	
R09	Off hours quota exceeded	
R10	Too many normal hours calls	
R11	Normal hours quota exceeded	
R12	Palestine Gang	
R13	Too Many Simultaneous calls	Calls with same origin and destination on a given time

New response codes can be added on future versions. Reason code displayed on the Domain or Subscriber Administrator interface are for information purpose only. Only SIPPulse team members can add new reason code, which can later be used to configure your system.

8.3 Subscribers

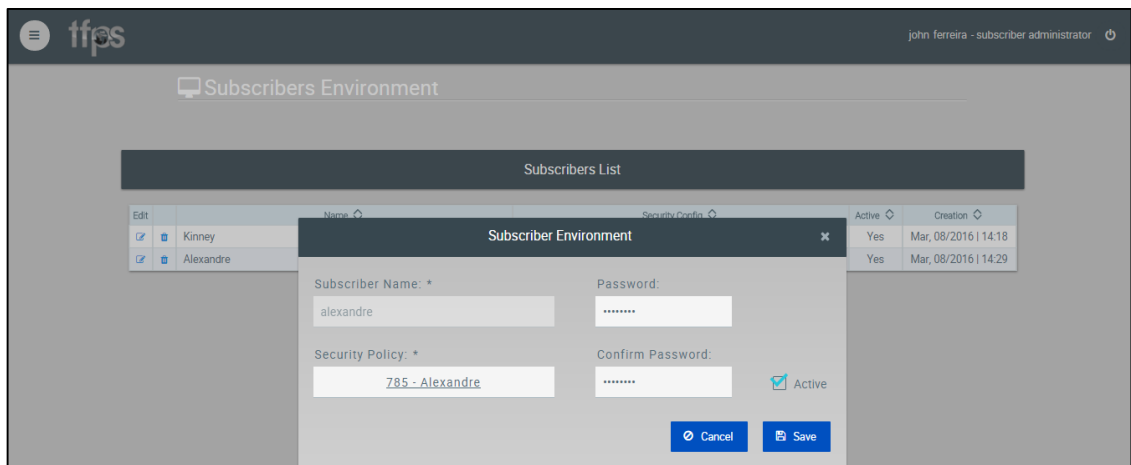
To manage security policies for subscribers under your administration, chose the Subscriber option under the menu button. A list of subscribers environment will be shown.



The screenshot shows the 'Subscribers Environment' page with a 'Subscribers List' table. The table has columns for Edit, Name, Security Config, Active, and Creation. Two subscribers are listed: Kinney and Alexandre.

Edit	Name	Security Config	Active	Creation
<input checked="" type="checkbox"/>	Kinney	785 - Kinney	Yes	Mar, 08/2016 14:18
<input checked="" type="checkbox"/>	Alexandre	785 - Alexandre	Yes	Mar, 08/2016 14:29

Chose the subscriber you wish to edit and the following screen will be shown. A pre-defined security policy has been created based on the defaults set by your domain manager.



The screenshot shows the 'Subscriber Environment' form for editing the 'Alexandre' subscriber. The form includes fields for Subscriber Name, Password, Security Policy, and Confirm Password. The 'Security Policy' field is set to '785 - Alexandre'. There are 'Cancel' and 'Save' buttons at the bottom.

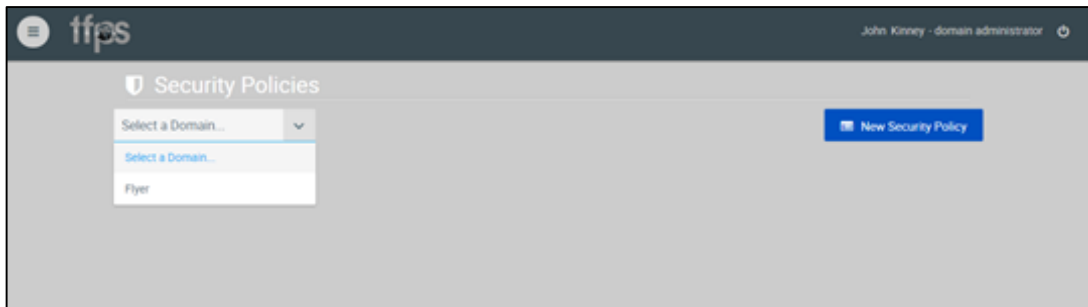
You can click security policy to edit it.

You will be shown information for the subscriber's security policy. You can edit the assigned rules (follow instructions on section 8.4).

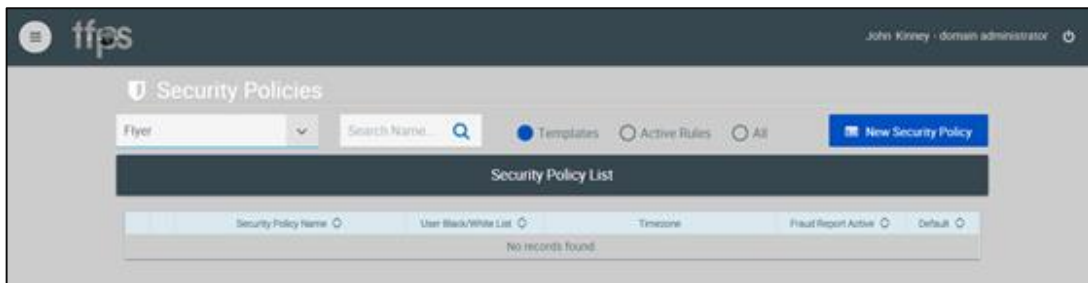
8.4 Managing Security Policies

Security policies are a set of rules defined by user administrators that will complement TFPS internal algorithms and knowledge base to analyze and mark a call with the corresponding Response Code. As an administrator you can set template policies which can be used by your subscribers as a base to their own set of rules.

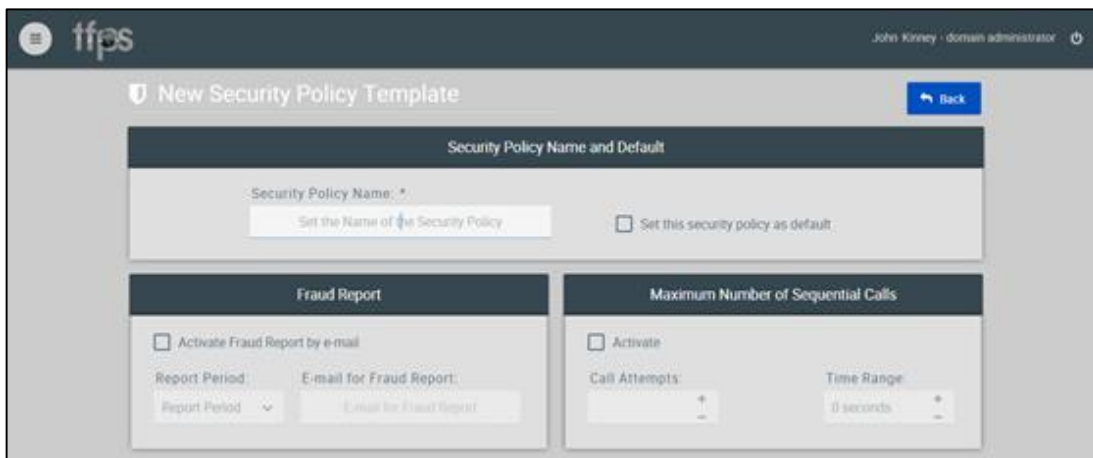
By selecting the Security Policies command, the following screen will be presented:



You must then select the domain to which the policy will be assigned to. A set of pre-existing policies, if any, will be displayed.



By pressing the “New Security Policy” button you will be presented with the following screen:



You then define the name that will be assigned to this specific policy, and mark it as a default policy if that policy should be the basic policy for your domain. Each subscriber will be assigned the default policy if none is set for later. You must also define the destination email for fraud reports and the recurrence it shall be send.

You must also define whether you want TFPS to limit the number of sequential calls on a given period. This will have TFPS mark all calls that exceed this limit with the according response code.

The screenshot shows a web interface for configuring call policies. It is divided into two main sections: 'Call Policy' and 'Off Hours Rules'.

Call Policy Section:

- Max. Concurrent Calls:** A numeric input field with a '+' button.
- Daily Quota:** A numeric input field with a '+' button.
- Max. C. C. Off-Hours:** A numeric input field with a '+' button.
- Daily Quota Off-Hours:** A numeric input field with a '+' button.

Off Hours Rules Section:

- Time Zone:** A dropdown menu with the option 'Set the Time Zone...'.
- Day:** A numeric input field with a '+' button.
- Month:** A dropdown menu with the option 'All Months'.
- Weekday From:** A dropdown menu with the option 'All Weekdays'.
- Hours From:** A numeric input field with a '+' button.
- Hours To:** A numeric input field with a '+' button.
- Weekday To:** A dropdown menu with the option 'All Weekdays'.
- Pattern:** A text input field with a placeholder 'No records found'.
- Use DST Time Zone:** A checkbox.
- Add:** A blue button with a plus icon.

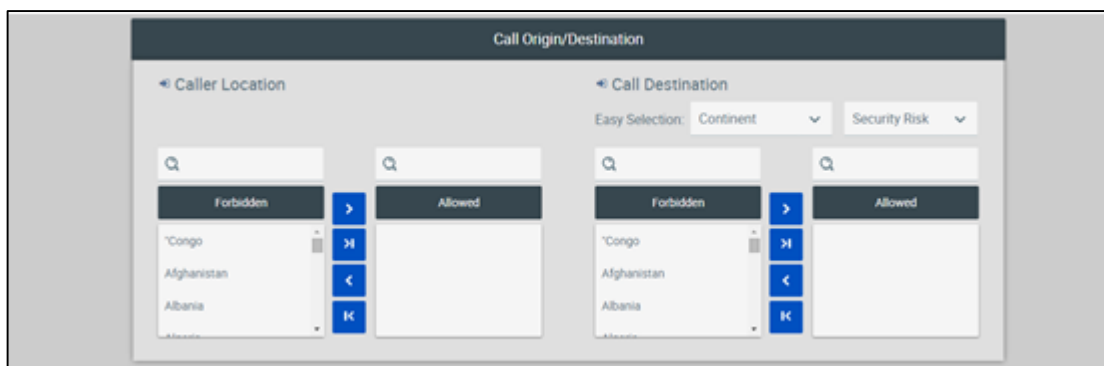
You can also define the maximum number of concurrent calls and a daily quota of calls your system can submit. You can also select the number of concurrent calls and daily quota of calls for off-hours. If you select to use off hours restrictions, these will override the rules set for full day, during the off hours. Off-hours and regular on-hours daily quota will not add up to each other.

You must also define all off-hour period for you operations. For such you must select the time zone, number of days to be applied (leave zero if perpetual), months of the year, days of the week and time period (begin and end of period). You can add as many periods as you wish. However we recommend you to keep it as simple as possible to reduce management complexity. As you add off hour rules, they will be shown on this screen.

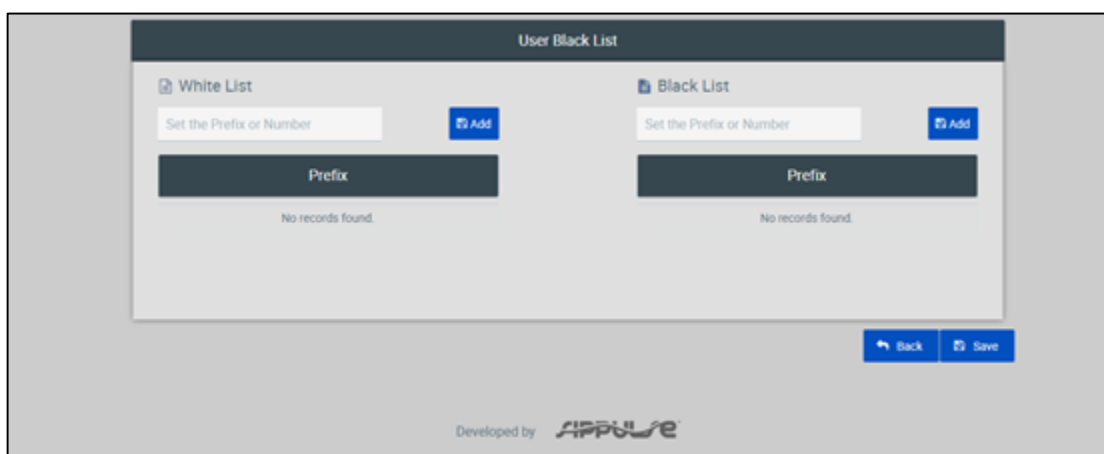
As you submit calls to TFPS analysis, it will check calls against your rules and mark them with the corresponding reason code.

The following rules will define from which countries your policy will accept originating calls and to which countries calls will be allowed to. You can chose to use continents or select a predefined list of countries set base on a risk analysis (low, medium and high risk).

Predefined risk origin and destination are based on aggregated knowledge of origin and destination countries for risk. These predefined risk assessment changes constantly. Please check this list regularly since, once selected it will become static on your rules



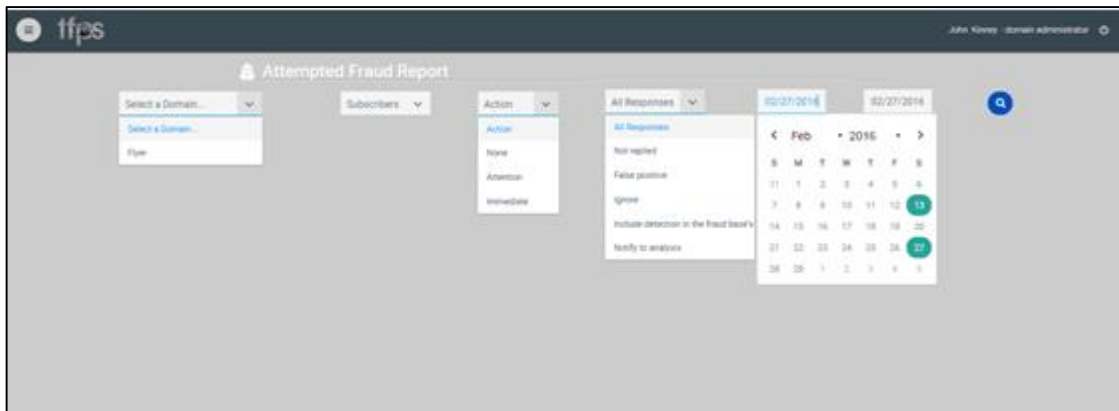
You can finally define a set of white list destination numbers for which TFPS will not perform a check. Numbers included on the policy white list will override the system black list for those subscribers using this policy. You can also add numbers to policy black list. These numbers will not affect other policies. Should you elect to remove a number from a policy white or black list, please contact SIPPulse.



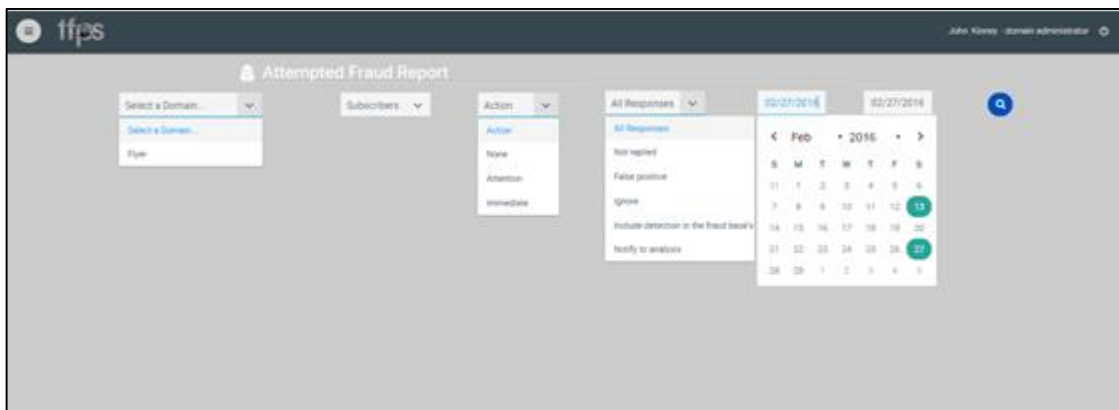
After editing you policy rules, click on the “Save” button and proceed to create new policies or to create your subscribers.

8.5 Fraud Report

Fraud report will allow administrators and subscribers to generate reports of fraud suspected events over transactions checked by TFPS for the corresponding account (or accounts under domains managed by and administrator).



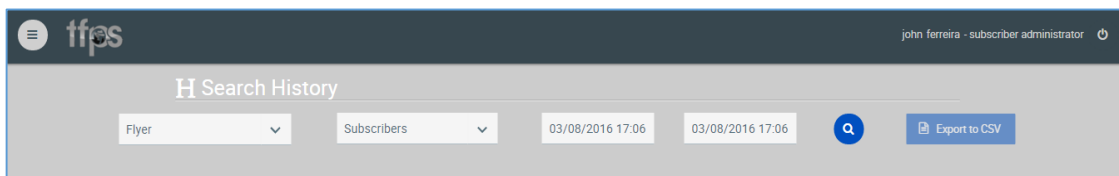
From the pull down menu's shown on the Fraud Report page, select the Domain, Subscriber, Action (which action was taken over the call), response type and beginning and end date for the report.



From the pull down menu's shown on the Fraud Report page, select the Domain, Subscriber, Action (which action was taken over the call), response type and beginning and end date for the report.

8.6 History Report

History report will allow administrators and subscribers to generate reports of queries on the system.



Select the domain and account (only the user account will be displayed if the user is a subscriber) and the beginning and end dates.

8.7 Logging off

To log off from TFPS, click on the on-off button on the upper right side of your screen and click on the “Logoff” option.



9. Limitation

9.1 Secure environments

Rather than being a solution, Security is a discipline that is built and practiced by several components including, but not limited to, solutions such as TFPS. Security Discipline must be complemented by rules that govern systems usage, user access policies, regular audit on your systems and many other actions which your security staff shall enforce and practice.

TFPS is not designed nor intended to secure your infrastructure. For such there are several state-of-the-art solutions and practices that can be used by your team to protect your system's integrity. TFPS will act over your functional operation: that is, telephone calls which can also be originated outside of your systems, thus outside of your rules and protection.

While TFPS is a crowdsourcing and self-evolving solution, it adds value to its protection capabilities from each event that it experiences. However fast the solution and its knowledge base grow, hackers tend to act with similar speed to discover and develop new ways of tampering and defrauding IT (and telephony systems). It is advisable that your company periodically review security and usage policies as well as constantly monitor your systems.

9.2 Usage conditions

TFPS offers an auxiliary mechanism to reduce exposure to fraud. However, it does not offer full protection and does not offer any compensation for false positive and false negative response from the system nor liability compensations of any kind and value in case of actual occurrence of fraud against your system.

TFPS will not forward any calls to phone services operators. TFPS is a query system that operates in parallel to your phone system. Once TFPS marks your query with a response code, this query is returned to your phone system (or TFPS configured SIP Pulse SBC). Your phone system should be programmed to forward or deny calls based according to the response code informed by TFPS.

9.3 TFPS contract conditions

By signing up and using TFPS you agree on the general terms and conditions set for in the usage conditions clauses made available to your company. You also agree to observe the limitations and values on domains, subscribers, queries per second and total monthly queries set on your choice of services.

Should you add subscribers above your contracted number of accounts, TFPS will not limit your operations. If you exceed the number of subscribers originally contracted, SIPPulse will add the corresponding amount to your following monthly invoice. Likewise, transactions in excess of the contract query volume will be charged to the following monthly invoice.

Should you exceed the number of CPS from your selected plan, the system will not analyze the exceeding calls, resulting in a lack of response code. You can program your base system to time out such calls to avoid them of being forwarded without being checked. While this ensures reduction to fraud exposure reduces your services quality. Please contact SIPPulse to expand your contract to meet your CPS demand.

10. How to Integrate TFPS to your PBX/Softswitch

The objective of this guide is to show you how to interconnect your softswitch with the Telephony Fraud Prevention Tool. In this guide, we are going to cover:

1. Single Policy Integration
2. Multiple Policy Integration
3. Integration via Sip Redirect
4. Integration via WebService
5. Integration example using Asterisk
6. Integration example using FreeSwitch
7. Integration example using OpenSIPS
8. Integration example using FreePBX

Single Policy Integration

The use of a single policy is recommended for IP-PBXs, The MD5 challenge authentication standard on HTTP and SIP are used in this case. All you have to do is to pass the correct user name and password. You may also authenticate by IP. The IP authentication is configured by tech support.

Multiple Policy Integration

When you have a softswitch you may have different policies for different users. In this case the authentication is IP based. You have two methods to pass username and domain to select the policy. You need to have your own domain account in the system to create users and have access to the interface.

IP+CLI

The authentication policies are set by the tech support. The user has to simply set the correct from user and from domain. Set the From header with the username and domain associated to the security policy.

IP+X-TFPS

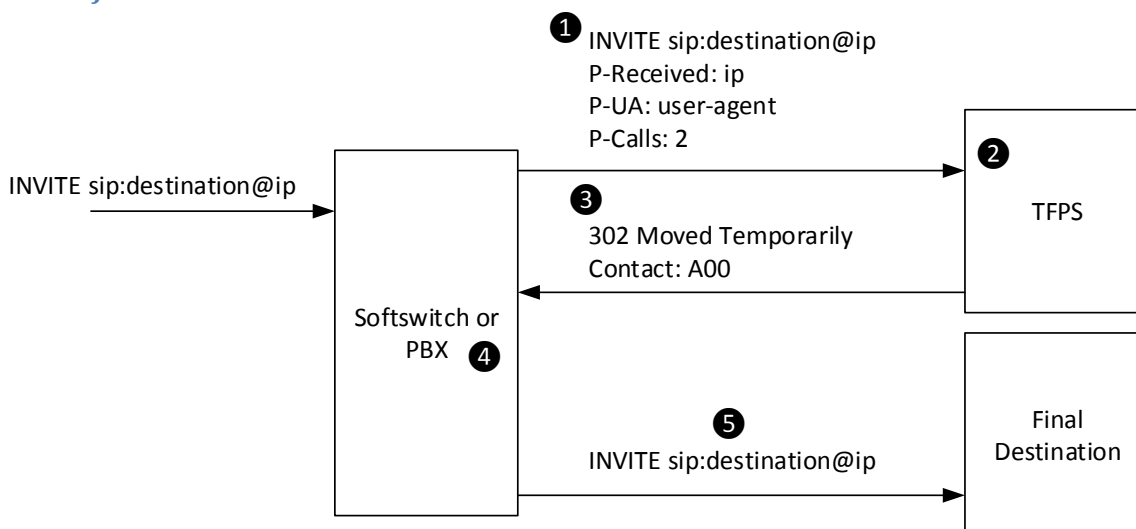
You can optionally send the username and domain sending the Sip header X-TFPS like below:

X-TFPS: username@domain

Integration using SIP redirect

The SIP redirect method is simple, fast and asynchronous. It is very easy to use and similar to sending a call to a VoIP provider. Check the picture below to understand how it works.

Successful Call



❶ After receiving the call establishment (INVITE) from the customer, the softswitch will send the SIP request to the TFPS SIP server. The destination number MUST be in the e164 format with no plus sign (e.g. 5548987654321). The softswitch SHOULD add three SIP headers to the request:

- a. P-Received: The original IP received from the customer
- b. P-UA: The original user agent received by the customer
- c. P-Calls: The number of simultaneous calls for this specific user

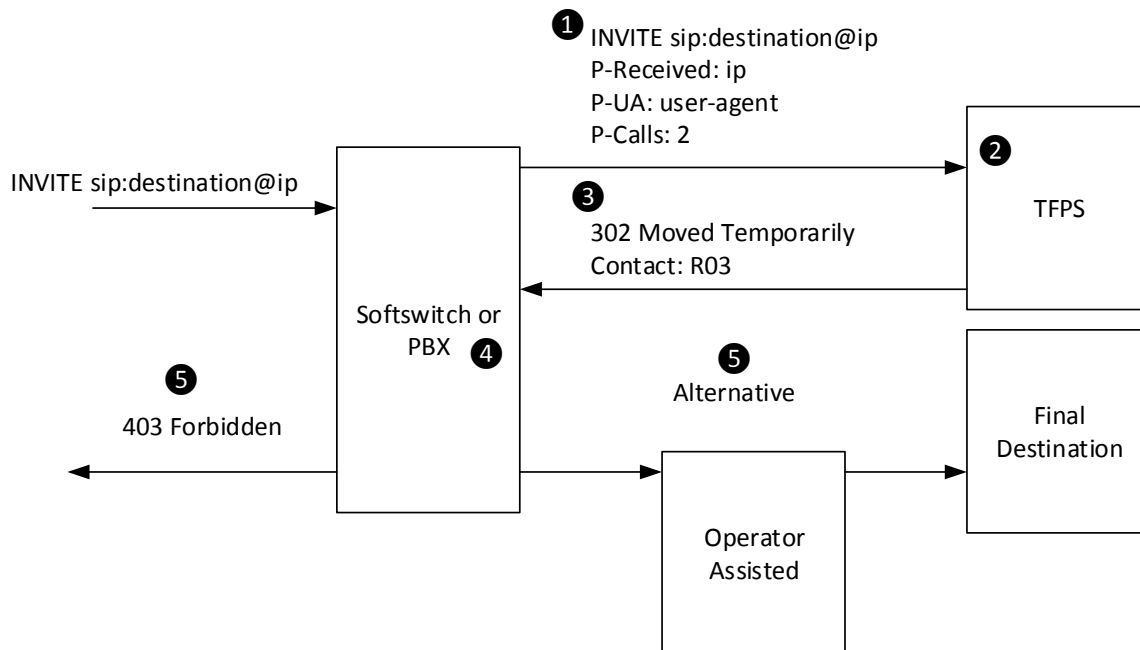
❷ The TFPS server analysis the headers against the security policies and blacklists

❸ The TFPS server returns a SIP reply “302 Moved Temporarily” with a positive (Starting with A, approved) code back to the Softswitch.

❹ The Softswitch reads the code and if it starts with “A” complete the call to the final destination.

❺ The call is finally sent to the final destination. The whole process takes usually less than 3ms and it is asynchronous.

Unsuccessful Call



❶ After receiving the call establishment (INVITE) from the customer, the softswitch will send the SIP request to the TFPS SIP server. The softswitch adds three SIP headers to the request:

- a. P-Received: The original IP received from the customer
- b. P-UA: The original user agent received by the customer
- c. P-Calls: The number of simultaneous calls for this specific user

❷ The TFPS server analysis the headers against the security policies and blacklists

❸ The TFPS server returns a SIP reply “302 Moved Temporarily” negative (Starting with R, rejected) code back to the Softswitch.

❹ The Softswitch reads the code and if it starts with “R”

❺ The call generates a 403 Forbidden reply to the user.

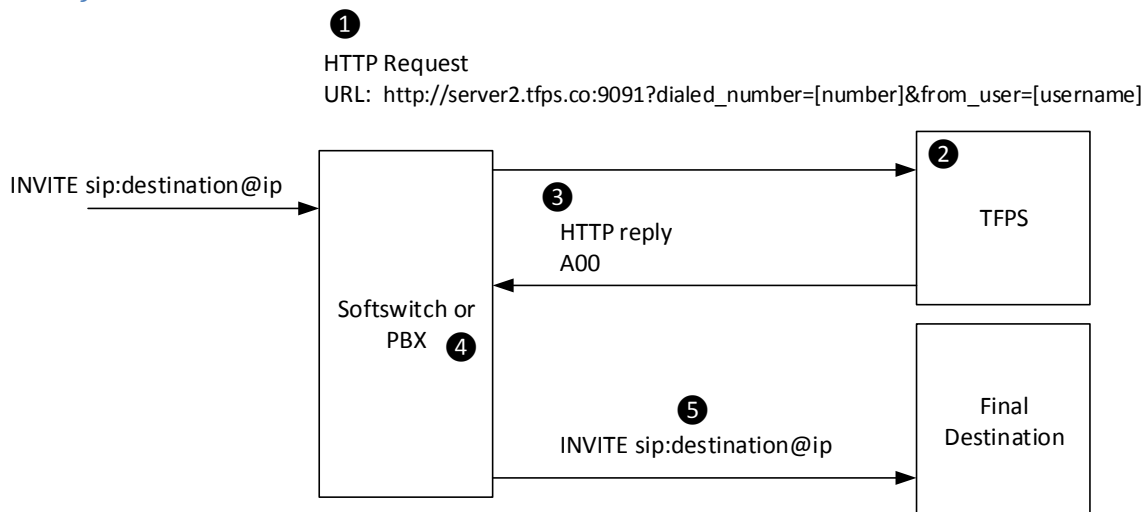
❻ As an alternative, it is also possible to send the call to a human operator for screening before sending to the final destination.

You can see later the examples for common softswitches such as Asterisk and FreeSwitch.

Integration via Webservice

The fraud check may also use the web service mechanism. The figure below shows how the webservice works:

Successful Call



1 After receiving the call establishment (INVITE) from the customer, the softswitch will send an HTTP request to the TFPS server. The format is like below:

[http://server2.tfps.co:9091?dialed_number=\[numero\]&from_user=\[usuario\]](http://server2.tfps.co:9091?dialed_number=[numero]&from_user=[usuario])

Mandatory Parameters:

- dialed_number – Number dialed by the user in e164 format (e.g 554898754321) with no + sign
- from_user – The user to be authenticated

Optional Parameters:

- domain – Domain used in the authentication
- source_ip – IP received from the original user
- user_agent – User Agent received from the original user
- sim_calls – Current calls on this user.

P-Received: The original IP received from the customer

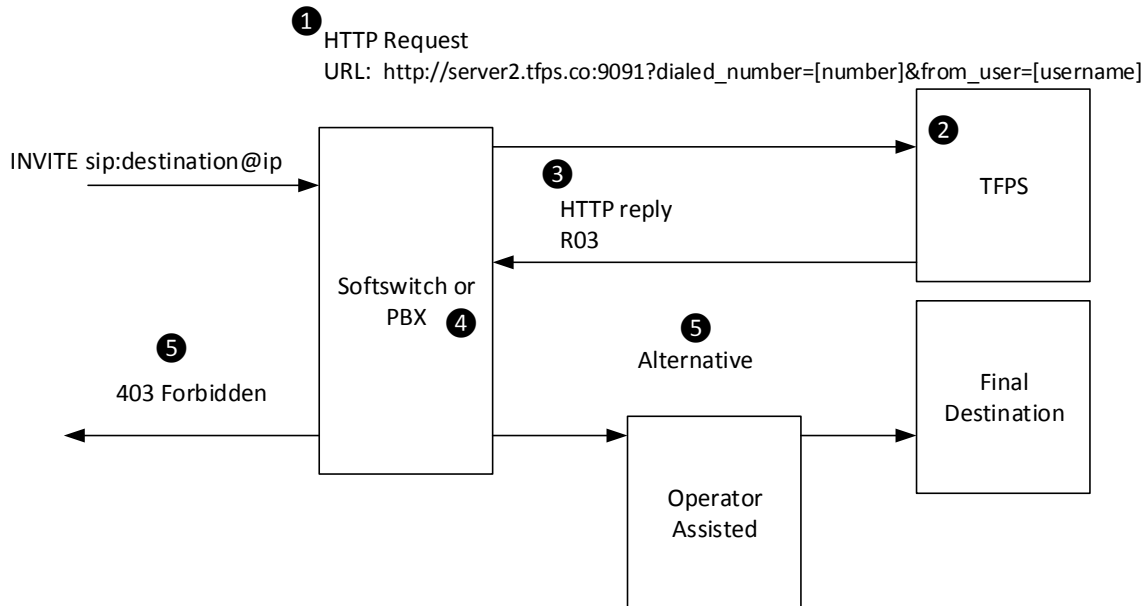
- a. P-UA: The original user agent received by the customer
- b. P-Calls: The number of simultaneous calls for this specific user

2 The TFPS server analysis the headers against the security policies and blacklists

3 The TFPS server returns an HTTP reply with a positive (Starting with A, approved) code back to the Softswitch.

- ④ The Softswitch reads the code and if it starts with “A” complete the call to the final destination.
- ⑤ The call is finally sent to the final destination. The whole process takes usually less than 5ms and it is synchronous using a connection-oriented protocol.

Unsuccessful call



- ① After receiving the call establishment (INVITE) from the customer, the softswitch will send an HTTP request to the TFPS server. The format is like below:

[http://server2.tfps.co:9091?dialed_number=\[numero\]&from_user=\[usuario\]](http://server2.tfps.co:9091?dialed_number=[numero]&from_user=[usuario])

Mandatory Parameters:

- dialed_number – Number dialed by the user in e164 format (e.g 554898754321) with no + sign
- from_user – The user to be authenticated

Optional Parameters:

- domain – Domain used in the authentication
- source_ip – IP received from the original user
- user_agent – User Agent received from the original user
- sim_calls – Current calls on this user.

P-Received: The original IP received from the customer

- c. P-UA: The original user agent received by the customer
- d. P-Calls: The number of simultaneous calls for this specific user

- ② The TFPS server analysis the headers against the security policies and blacklists
- ③ The TFPS server returns an HTTP reply with a positive (Starting with R, rejected) code back to the Softswitch.
- ④ The Softswitch reads the code and if it starts with “R”
- ⑤ The call generates a 403 Forbidden reply to the user.
- ⑤ As an alternative, it is also possible to send the call to a human operator for screening before sending to the final destination.

Integration example with Asterisk

To integrate FPS with Asterisk you need to modify two files, sip.conf and extensions.conf in the way shown below:

sip.conf

```
[fps]
type=peer
context=fps
host=server1.tfps.co
port=9090
username=<username>
fromuser=<username>
fromdomain=tfps.co
secret=<secret>[from-internal]
```

extensions.conf

```
[from-internal] ; Set there the context for your users
;FPS for International Calls
exten=_011[1-9].,1,set(ip=${CHANNEL(recvip)})
same=>n,SIPAddHeader(P-Received: ${ip})
same=>n,set(ua=${CHANNEL(useragent)})
same=>n,SIPAddHeader(P-UA: ${ua})
same=>n,set(GROUP( )=fps)
same=>n,set(ncalls=${GROUP_COUNT(fps)})
same=>n,SIPAddHeader(P-Calls: ${ncalls})
same=>n,set(_original=${EXTEN})
same=>n,dial(SIP/fps/${EXTEN:2})

[fps]
;For calls not approved
exten=_R.,1,Answer( )
```

```

same=>n,playback(unauthorized); (Customize here to generate an
error message)
same=>n,hangup(21)

;For calls approved
exten=_A.,1,Answer()
same=>n,Dial(SIP/provider/${original});(Customize here to send
the call ahead)
same=>n,hangup(16)

```

Where DAHDI/g0 is the channel available in the example for International Calls. This channel can be DAHDI, SIP or any other channel capable to make international calls.

Response Codes

- A00 – Call Approved
- RXX – Full codes are available only for customers

Integration example with FreeSwitch

To integrate FPS with FreeSwitch you need to create a SIP profile and change the Dialplan.

[/usr/local/freeswitch/conf/sip_profiles/external/tfps_gw.xml](#)

```

<include>
  <gateway name="tfps">
    <param name="username" value="<username>"/>
    <param name="realm" value="tfps.co"/>
    <param name="from-domain" value="tfps.co"/>
    <param name="password" value="<password>"/>
    <param name="proxy" value="server1.tfps.co:9090"/>
    <param name="register" value="false"/>
  </gateway>
</include>

```

[/usr/local/freeswitch/conf/dialplan/default/tfps_dialplan.xml](#)

```

<include>
  <extension name="High Cost Route">
    <condition field="destination_number" expression="^(00)(\d*)">
      <action application="export"
data="sip_redirect_context=default"/>
      <action application="set"
data="sip_h_P_Received=${network_addr}"/>
      <action application="set" data="sip_h_P_UA=${sip_user_agent}"/>
      <action application="set"
data="sip_h_P_Calls=${inter_call_count}"/>
      <action application="set_global"
data="inter_call_count=${expr(${inter_call_count}+1)}"/>
      <action application="bridge" data="sofia/gateway/tfps/$2"/>
    </condition>
  </extension>

```

```

</extension>

<extension name="International_accepted">
  <condition field="destination_number" expression="^(A\d\d)(\d*)">
    <action application="set_zombie_exec"/>
    <action application="answer" data=""/>
    <action application="playback"
data="shout://translate.google.com/translate_tts?tl=en&q=Call+Approved"/>
    <!--<action application="bridge"
data="sofia/gateway/international_gw/$2"/>-->
    <action application="hangup" data=""/>
    <action application="set_global"
data="inter_call_count=${expr(${inter_call_count}-1)}/>
  </condition>
</extension>

<extension name="International_Refused">
  <condition field="destination_number" expression="^(R\d\d)(\d*)">
    <action application="set_zombie_exec"/>
    <action application="answer" data=""/>
    <action application="playback"
data="shout://translate.google.com/translate_tts?tl=en&q=Call+Refused"/>
    <action application="hangup" data="NORMAL_CIRCUIT_CONGESTION"/>
    <action application="set_global"
data="inter_call_count=${expr(${inter_call_count}-1)}/>
  </condition>
</extension>
</include>

```

Response Codes

- A00 – Call Approved
- RXX – Full user codes are available only for customers

Integration Example with OpenSIPS

FPS is a simple system to protect your PBX/softswitch from fraudulent calls. There are a few differences between the integrations using Asterisk/FreeSwitch and the integration using OpenSIPS/SER/OpenSER.

1. OpenSIPS do not support digest authentication (IP authentication will be required)
2. Many OpenSIPS working in service providers will need different policies for different customers

In this case, we suggest the Service Provider to request its own domain name at TFPS. With its own domain, a Service Provider can create a default user with a default policy and can create specific policies by ANI. After creating your account and setting your calling policies, you will need to configure your OpenSIPS. Below it is an example of this configuration. We recommend you to hire a specialist in OpenSIPS to customize the code below. It is not complicated for those familiarized with OpenSIPS syntax.

OpenSIPS Integration

To integrate TFPS with OpenSIPS you will need to create one Route and one Failure_Route.

[/etc/opensips/opensips.cfg](#)

Add these lines to the end of the file:

```
route[fpshosted] {
    #Rota com prevencao a fraude
    $avp(original)=$ru;
    t_on_reply("1");
    if(is_method("INVITE")) t_on_failure("5");
    $rd="server1.tfps.co";
    $rp="9090";

    #Identify the user
    create_dialog();
    $var(userid)=""$fU+"@"+"$fd;
    if(is_method("INVITE") && $DLG_status!=NULL && $var(userid)!=null)
        set_dlg_profile("caller",$var(userid));

    #Count calls for this user
    get_profile_size("caller",$var(userid),"$var(calls)");

    #Add headers
    append_hf("P-Received: $avp(srcip)\r\n");
    append_hf("P-UA: $ua\r\n");
    append_hf("P-Calls: $var(calls)\r\n");
    if (!t_relay()) {
        sl_reply_error();
    }
    exit;
}

#Failure_route for FPS Hosted
failure_route[5] {
    if (t_check_status("302")) {
        get_redirects("");
        xlog("L_INFO","P4 - FPS RESULT - $rU
[$rm/$si/$fu/$ru/$ci]");
        if($rU=~"^A00") {
            #Call approved restore original uri
            $ru=$avp(original);
            if(is_method("INVITE")){
                if(!t_relay()) {
                    sl_reply_error();
                    exit;
                }
            }
        }
    }
}
```

```

        } else {
            xlog("L_INFO", "Unauthorized Call, return code
$rU");

            t_reply("403", "Forbidden");
            exit;
        }
    } else {
        xlog("L_WARN", "Failed to contact fps hosted");
        t_reply("503", "Service Unavailable");
        exit;
    }
}

```

Response Codes

- A00 – Call Approved
- RXX – Full codes are available only for customers

Integration Example with Elastix/FreePBX

FPS is a simple system to protect your PBX from fraudulent calls. It is very easy to integrate to your PBX. After creating your account and setting your calling policies, you will need to configure your FreePBX (Elastix, Trixbox and others). FPS works like a SIP Provider, but instead of completing your call, it redirects your call back with a three character prefix. After receiving this prefix, you can decide what to do in your dial plan. Below a series of steps required to implement the FPS on FreePBX.

FreePBX Integration

To integrate FPS with FreePBX you need:

- Add a trunk to FPS
- Add a trunk to PSTN
- Add the FPS code to extensions_custom.conf

Step 1: Add a trunk to FPS

Name the trunk “fps” and fill the PEER details replacing <username> and <password> by your accounting data. Leave the USER details empty.

Outgoing Settings

Trunk Name:

PEER Details:

```

host=server1.tfps.co
username=<username>
secret=<password>
fromuser=<username>
fromdomain=tfps.co
port=9090
type=peer
context=tfps

```

Step 2: Add the FPS instructions to
/etc/asterisk/extensions_custom.conf

extensions_custom.conf

```

[from-internal-custom]
exten => h,1,Hangup()
include => agentlogin
include => conferences
include => calendar-event
include => weather-wakeup
include => tfpsdial

[tfpsdial]
exten=_00[1-9].,1,set(ip=${CHANNEL(recvip)})
same=>n,SIPAddHeader(P-Received: ${ip})
same=>n,set(ua=${CHANNEL(useragent)})
same=>n,SIPAddHeader(P-UA: ${ua})
same=>n,set(GROUP())=tfps
same=>n,set(ncalls=${GROUP_COUNT(tfps)})
same=>n,SIPAddHeader(P-Calls: ${ncalls})
same=>n,set(_original=${EXTEN})
same=>n,dial(SIP/tfps/${FILTER(0-9,${EXTEN:2})})

[tfps]
;For calls not approved
exten=_R.,1,Answer()
same=>n,playback(ss-noservice); (Customize here to generate an
error message)
same=>n,hangup(21)

```

```
;For calls approved  
exten=_A.,1,Answer()  
same=>n,set(OUTBOUND_TRUNK=SIP/International) ; Set here your PSTN  
trunk  
same=>n,Dial(${OUTBOUND_TRUNK}/${original})  
same=>n,hangup(16)
```

Response Codes

- A00 – Call Approved
- RXX – Full codes are available only for customers

11. Disclaimer and limitation of liability

You should not rely exclusively on TFPS to secure your phone operations.

TFPS is a powerful tool to help you protect your telephone services traffic and to detect unwanted services usage. However, TFPS is not an insurance services nor it has provision to compensate you and or your company for any event suffered by your system, detected or not detected by TFPS. Thus SIPPulse nor any of its business partners shall be liable to any compensation for damages and losses caused from direct or indirect consequence of the use of TFPS.