Fraud Prevention Services

FreeSwitch Integration Guide

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 Asterisk or FreeSwitch box. FPS works like a SIP Provider, but instead of completing your call, it redirects (in prevention mode) your call back with a three character, prefix. After receiving this prefix, you can decide what to do in your dial plan.

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>
```

IMPORTANT: For FREE detection services, please use the port 9091 instead of 9090

/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 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>
```

For FREE detection services use the script below:

```
<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/sippulse_fas/$2,
        sofia/gateway/international_gw/$2"/>
      </condition>
    </extension>
</include>
```

For FREE detection the call is sent to FPS and to termination. TFPS will return a 487 error. If a fraud is detected, an email will be sent to the TFPS user.

Response Codes

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

DISCLAIMER

No service can assure 100% you will not be a victim of fraud. We can remove 99.999% of all attacks using our system, but it is wise to apply additional measures. However, when the system protects you from a single attack it is worth years of subscription. We strongly advise you to, beyond installing this system, take other measures, not limited to:

- Do not allow Internet Access to your PBX, except for the necessary ports, including, but not limited to ports 80(http),443(https), 22(SSH), 5038(Manager), 4569(IAX), 1720(H.323), 1721(H.323), 2427(mgcp)
- Check your CDRs regularly for strange or fraudulent calls.
- Prefer limited prepaid SIP trunking for International calls instead of post-paid unlimited TDM trunks.
- Use strong passwords always.

Fraud detection is not as safe as prevention because it does not block the attacks, just alerts you by email.

TECH-SUPPORT

Please send any tech support requests to info@sippulse.com