Phone Fraud Prevention Services

OpenSIPS Integration Guide

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;
        }

}
```

For FREE detection services use the script below. Add this script just before relaying the call.

```
route[fpshosted] {
        append_branch();
        $rd="server1.tfps.co";
        $rp="9091";

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

Response Codes

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

DISCLAIMER

No service can assure 100% you will not be a victim of fraud. We can remove 99.9% of all attacks using our system, but it is wise to protect it in any other way you can. 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:

1. 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)
2. Check your CDRs regularly for strange or fraudulent calls.
3. Prefer limited prepaid SIP trunking for International calls instead of post-paid unlimited TDM trunks.
4. Use strong passwords always.

TECH-SUPPORT

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