“Know your enemy”
Sun Tzu's The Art of War

Using OpenSIPS as a single entry point for a SIP network

Flavio E. Goncalves
OpenSIPS Training/SipPulse

About me

Author of the book – “Building Telephony Systems with OpenSIPS”

CEO of SipPulse, www.sippulse.com, a turnkey OpenSIPS solution for Telcos and Hosted PBX.

Member of the OpenSIPS foundation.

Central de Assinantes

Welcome,
Demo Demo (logoff)

System Configuration
- Domains
- Profiles
- Regular Expression
- Dial Plan
- Management Dial Plan
- System Administrators
- System Components
- Servers RTP
- System Configuration

Manage Subscribers
- Subscribers
- Subscribers Management
- Add Credit
- Recharge Credit Log
- IP Authentication

Monitoring
- Dashboard
- Sip Trace
- Gateway's ASR
- Subscriber's ASR
- Gateway's CFR

Dymanic Routing
- Providers
- Gateways
- Gateways List
- Rules
- Rules Management
- Hunt Group
- Time Routing
- DID configuration
- DID's Import
- Prefix To Domain

Reports
- Call Detail Records Outgoing
- Call Detail Records Incoming
- Call Detail Records (Gateway)
- Summary by Providers
- Subscriber Missed Calls
- Timeout Calls
- Reason for Shutdown
- Rentability By Resellers
- Rentability By Providers
- Rentability By Account Code
- Rentability By Route

Resellers
- Reseller Definition
- Add Credit
- Recharge Credit Log

Recorder
- Recorder Settings
- Search Recordings

STFC
- Trunks
- Areas of Matrix
- Non-Geographic Codes
- Cadup
- Tariffs Plan Detraf

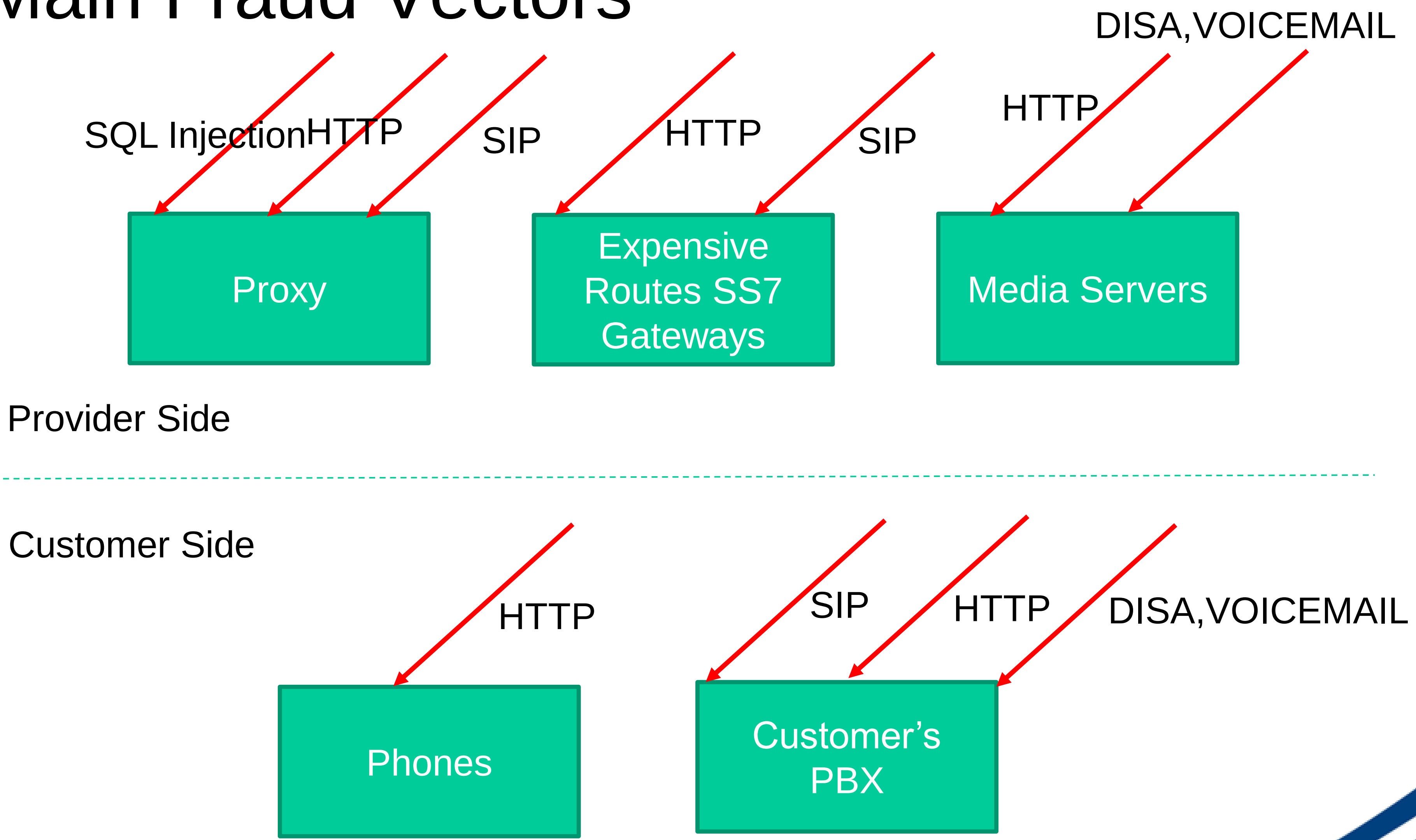
Schedule Tasks
- Schedule a new Task
- History of Scheduled Tasks

System Audit
- Execution History

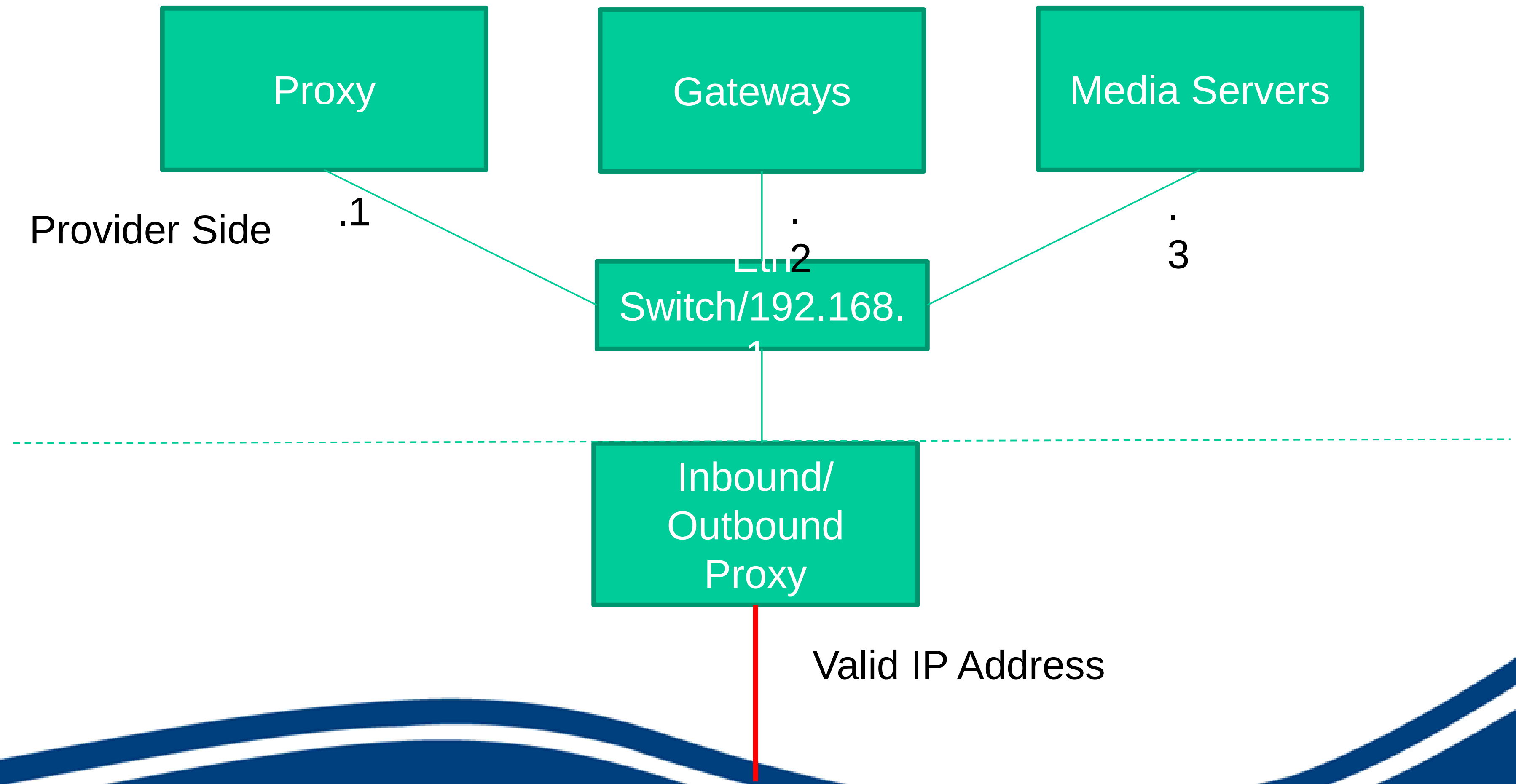
Agenda

1. Strategies to protect a SIP network
2. How to handle SIP
3. Handling Internal and External Users
4. How to handle RTP
5. Extra measures for fraud prevention

Main Fraud Vectors



Using OpenSIPS as a single entry point

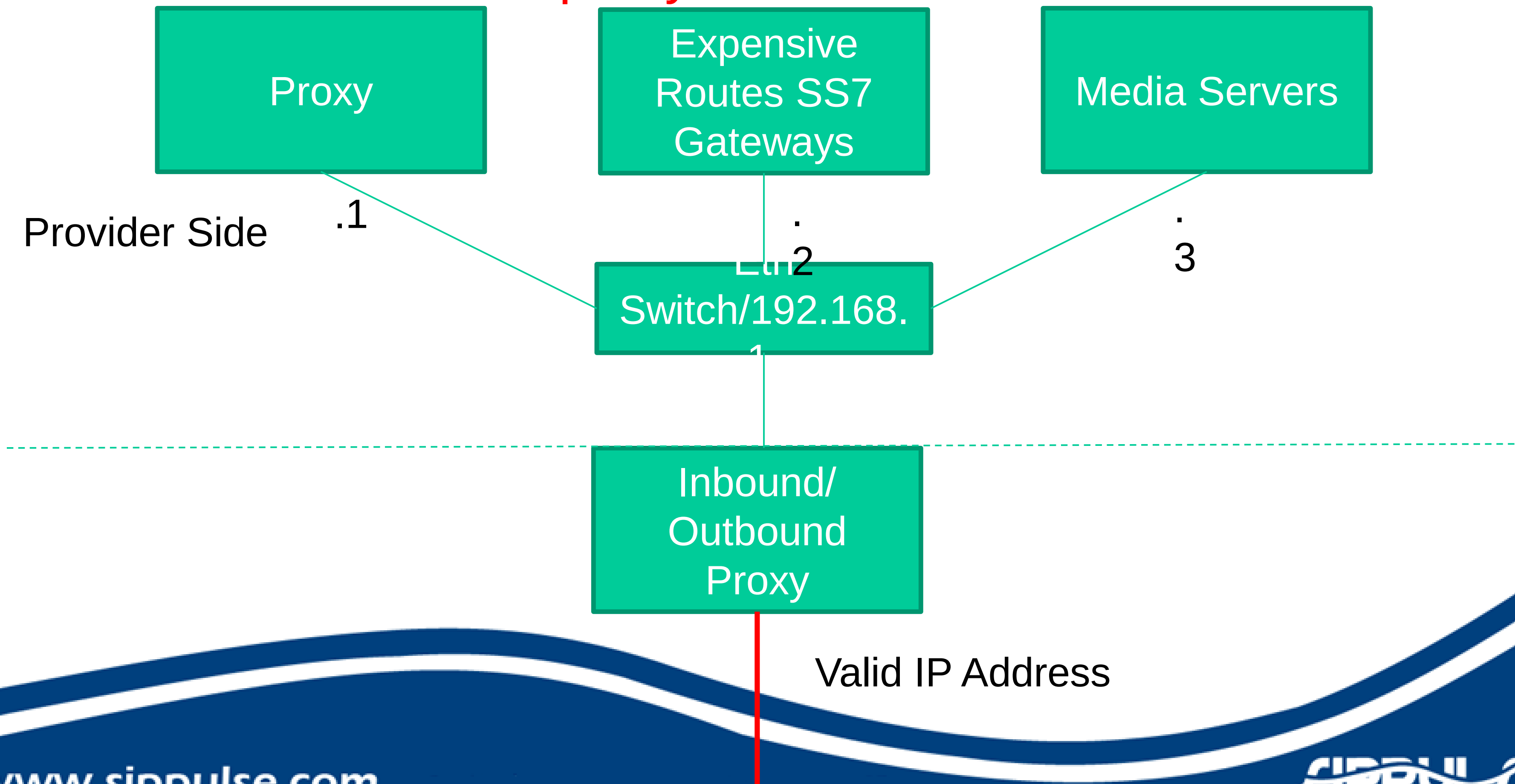


Let’s Split the Problem!

SIP / RTP

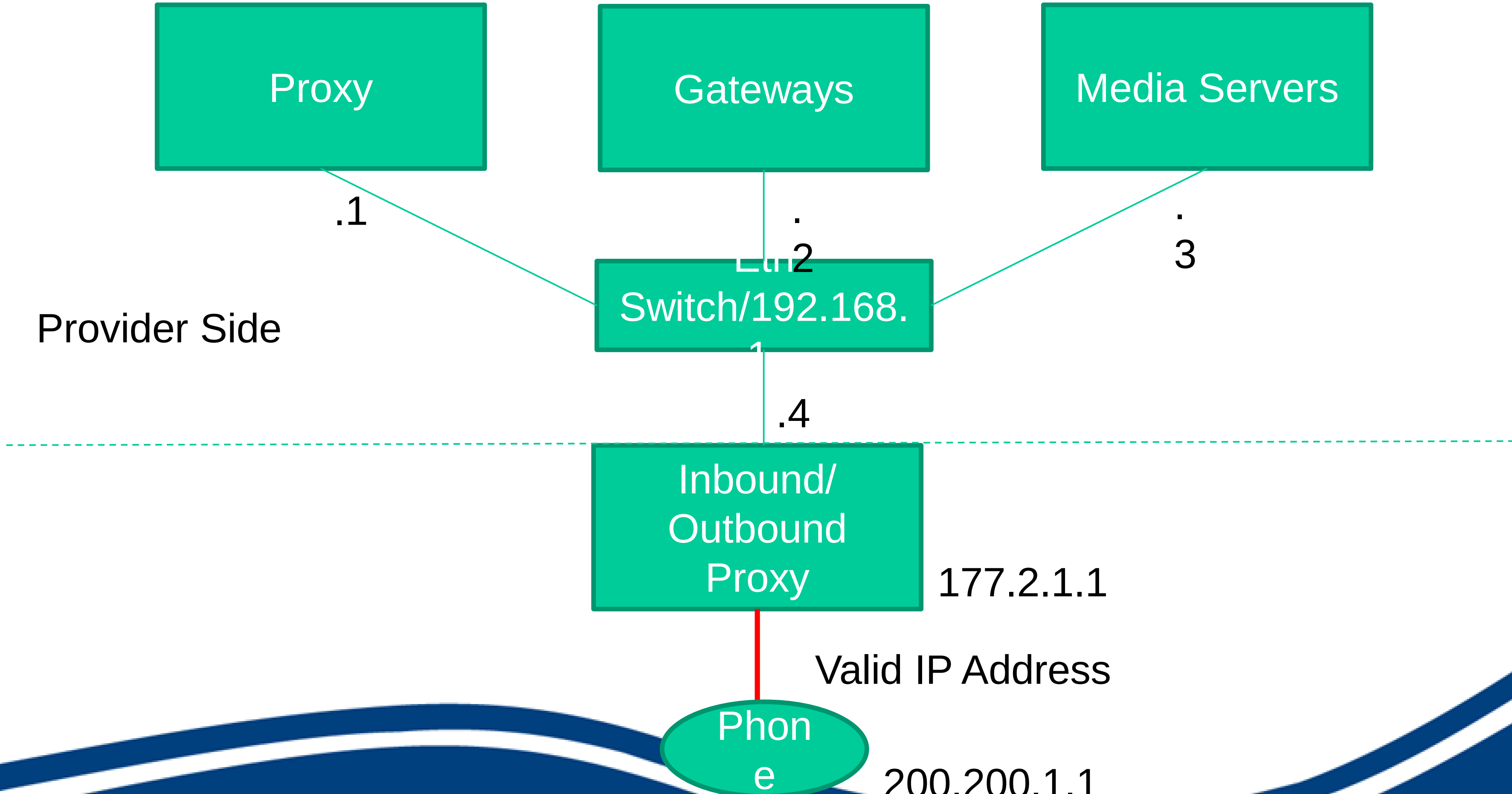
Solving the SIP Problem INVITE Outbound to Inbound

Simply set the outbound proxy in the client



Calling a user registered from the outside

How to force the delivery over the outbound proxy?
Which address do you have in the location table?



PATH

AOR:: 4733800000@dev.sippulse.com

Contact:: sip:4733800000@192.168.255.1:16422;rinstance=822b066c35fedb81;nat=yes Q=

Expires:: 3479

Callid:: ZTQ1NDE0ZWEyYzY2M2MxMGVhOWI0MWU5NWFiOWJhZTM

Cseq:: 2

User-agent:: Bria 3 release 3.5.5 stamp 71238

Path:: <sip:192.168.254.129;r2=on;lr>,<sip:192.168.255.134;r2=on;lr>

State:: CS_SYNC

Flags:: 0

Cflags::

Socket:: udp:192.168.254.135:5060

Methods:: 5951

PATH Module

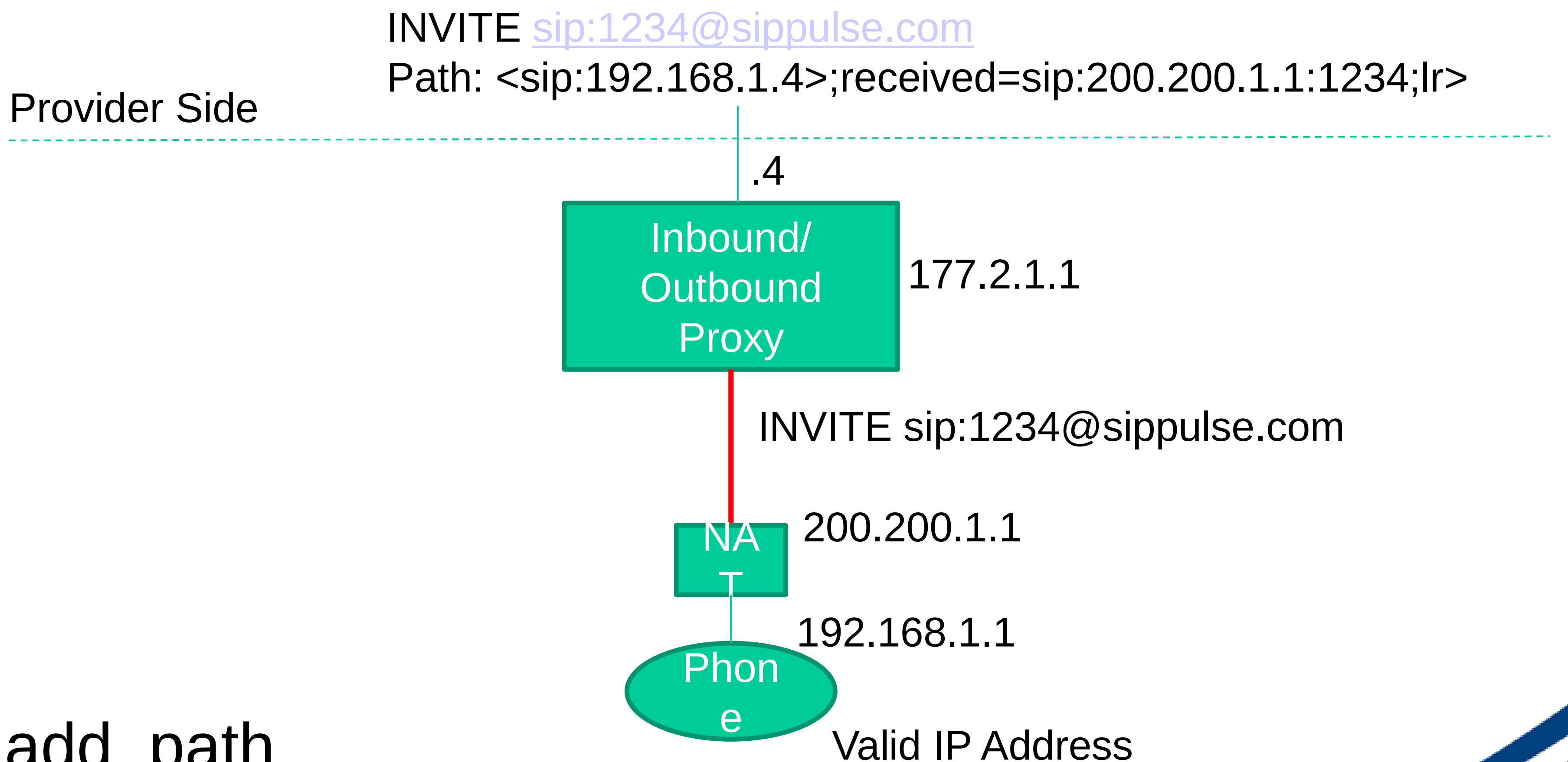
Path Module

OpenSIPS – Path Module

Asterisk - (12 Only)

FreeSwitch – Yes, Using fs_path

OpenSIPS



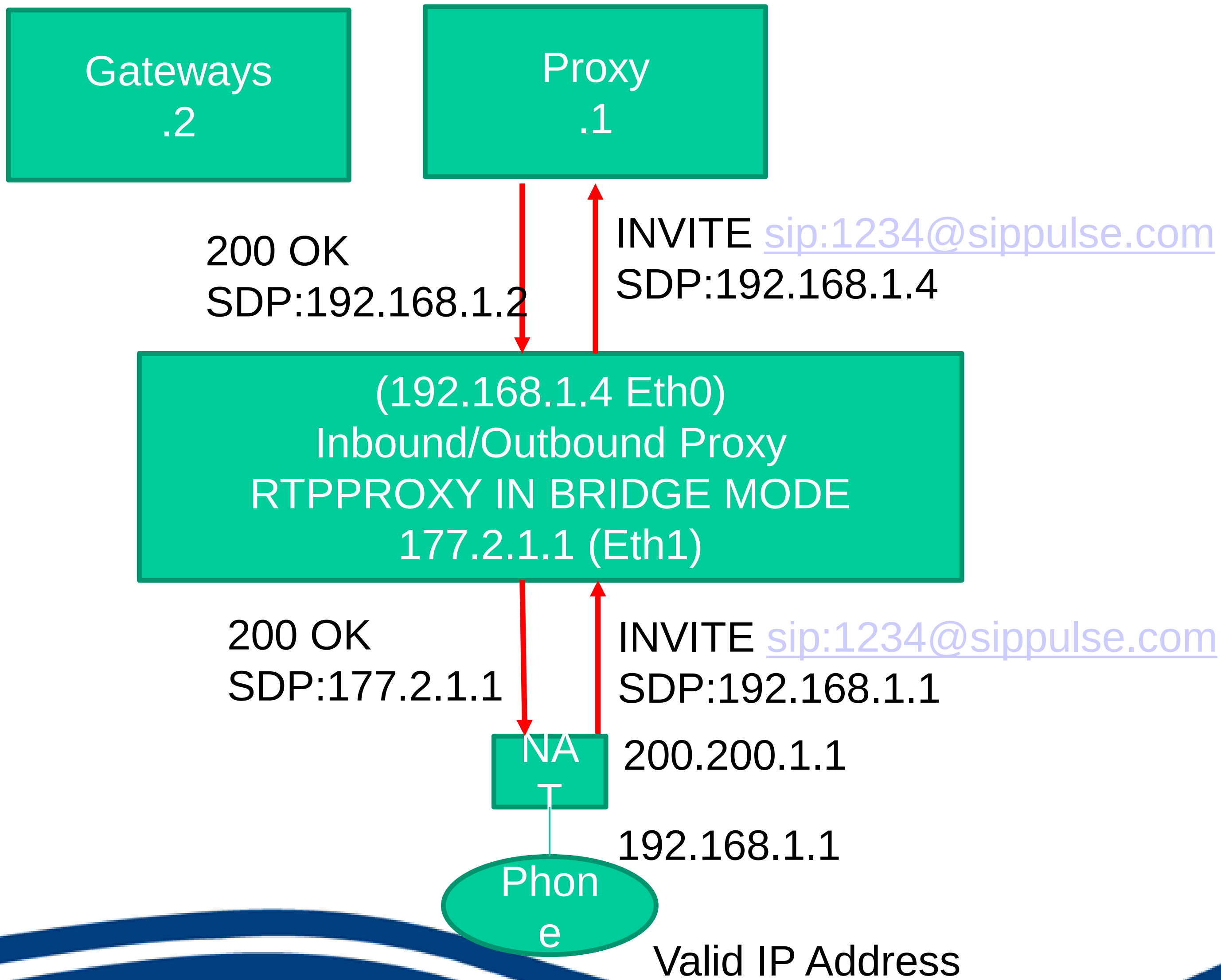
add_path

add_path_received

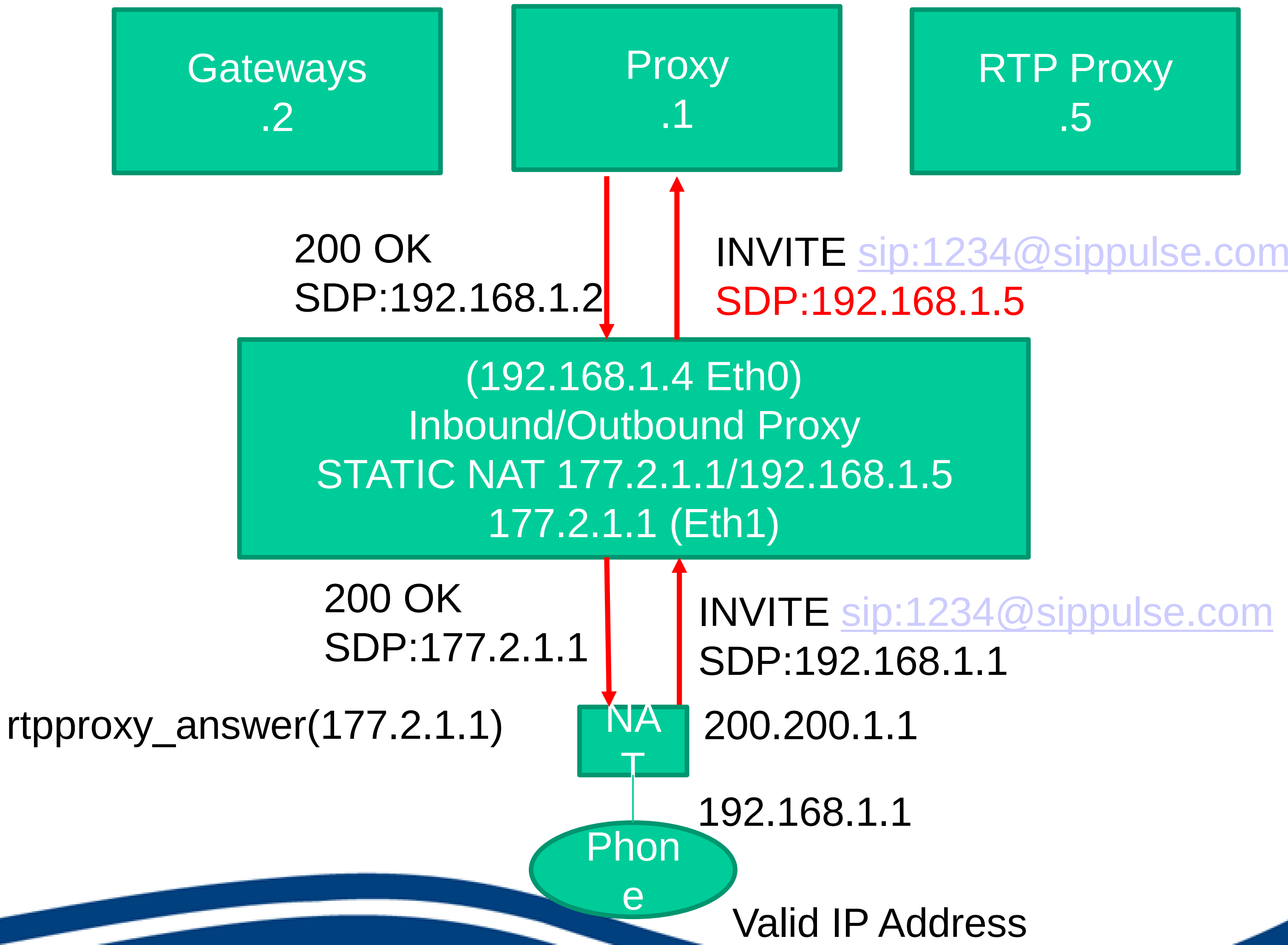
Path Headers

Path: <sip:192.168.255.134;r2=on;lr>.
X-SOURCE-URI:
sip:192.168.255.1:16422;transport=udp.

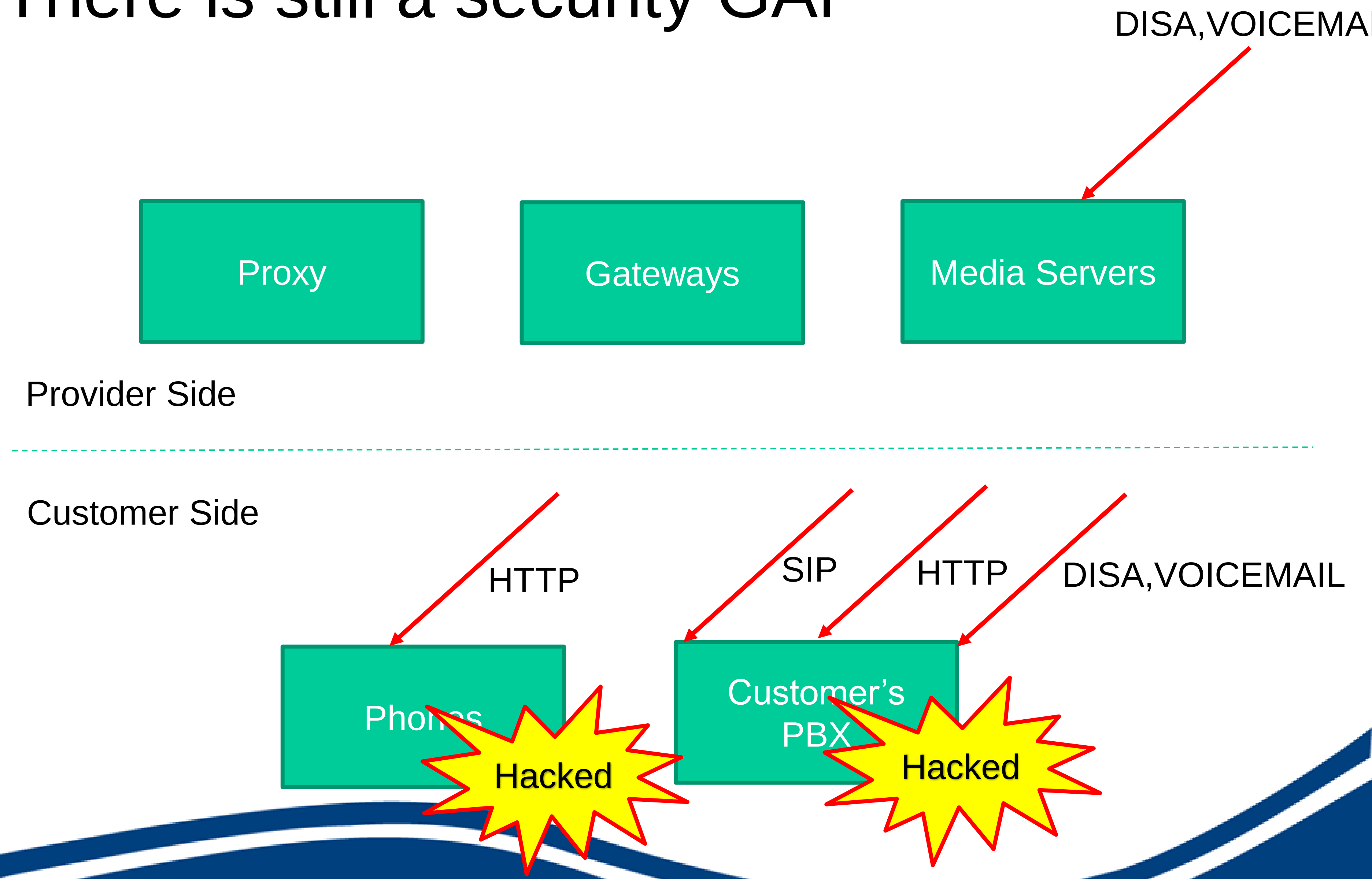
Solving the RTP Problem



Alternative



There is still a security GAP



The problem with Customer's being hacked

Traffic is authenticated, Ok

No failed attempts, Ok

User Agent, From User Ok

All normal security procedures passed

Anti-Fraud Systems are Mandatory

- Pre-paid accounts
  - Limit losses
  - Very hard to enforce for some clients
- Quotas
  - Limit losses
  - You have to manage

Security Configuration | Allow outbound calls TO | Allow inbound calls FROM

Calls on working hours: 5
Number of Simultaneous Calls

Calls off-hours: 1
Number of Simultaneous Calls

Quota on working hours: 20
Quota of Daily Calls

Quota off-hours: 2
Quota of Daily Calls

Timezone: Brazil/East

Use DST Timezone

Define off-hours

Hour: To Day: * To * Day of Month * Month * ADD ...

Pattern	
00:00-08:00,1-5,*,*	
18:00-23:59,1-5,*,*	
00:00-23:59,6-7,*,*	

- Collaborative protection. One PBX hacked automatically blocks the IP for the others
- Blacklists
  - Source IP, Dialed Number, Protocol Signatures
- Policies
  - Hour of the day, Simultaneous Calls, Quota
- Mechanism, SIP Redirect
  - Fast over UDP (<2 ms)
  - Available on almost any SIP implementation

Using TFPS in OpenSIPS

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

Using TFPS in OpenSIPS

```
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 {
    t_reply("403", "Forbidden");
    exit;
  }
 } else {
  t_reply("503", "Service Unavailable”);
  exit;
 }
}
```

What's Next

- SBC
  - Support for Attended Call Transfers
  - Support for Call Pickup
- TFPS
  - Integration of a Security Scanner

e-mail: flavio@sippulse.com

skype: flaviogoncalves1

THANK YOU!