KAMAILIO SIP ROUTER

SIP Router para operadores pequeños y medianos

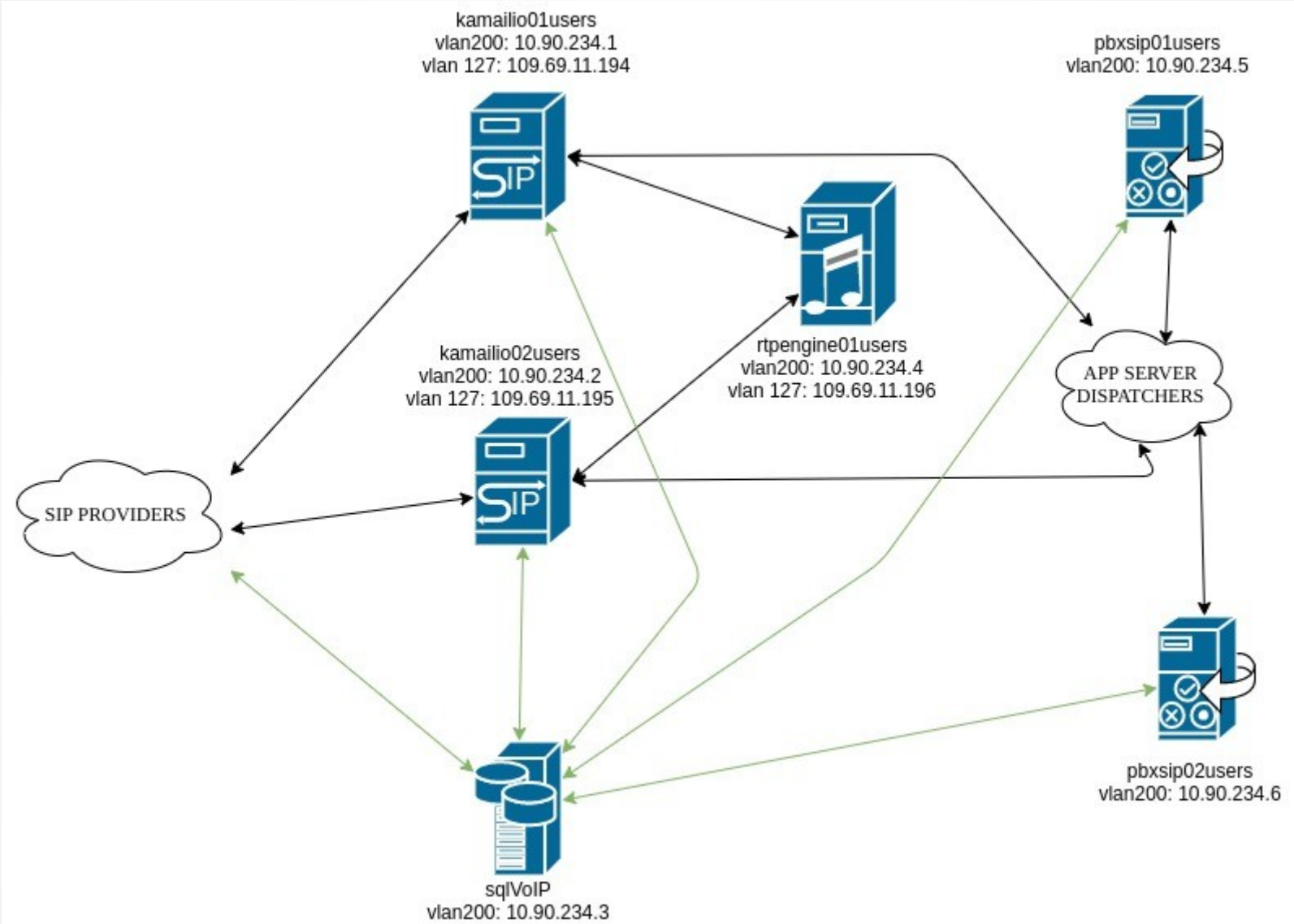
Àngel Elena Medina
Técnico de VozIP y Redes
craem@craem.net

Qué es KAMAILIO ?

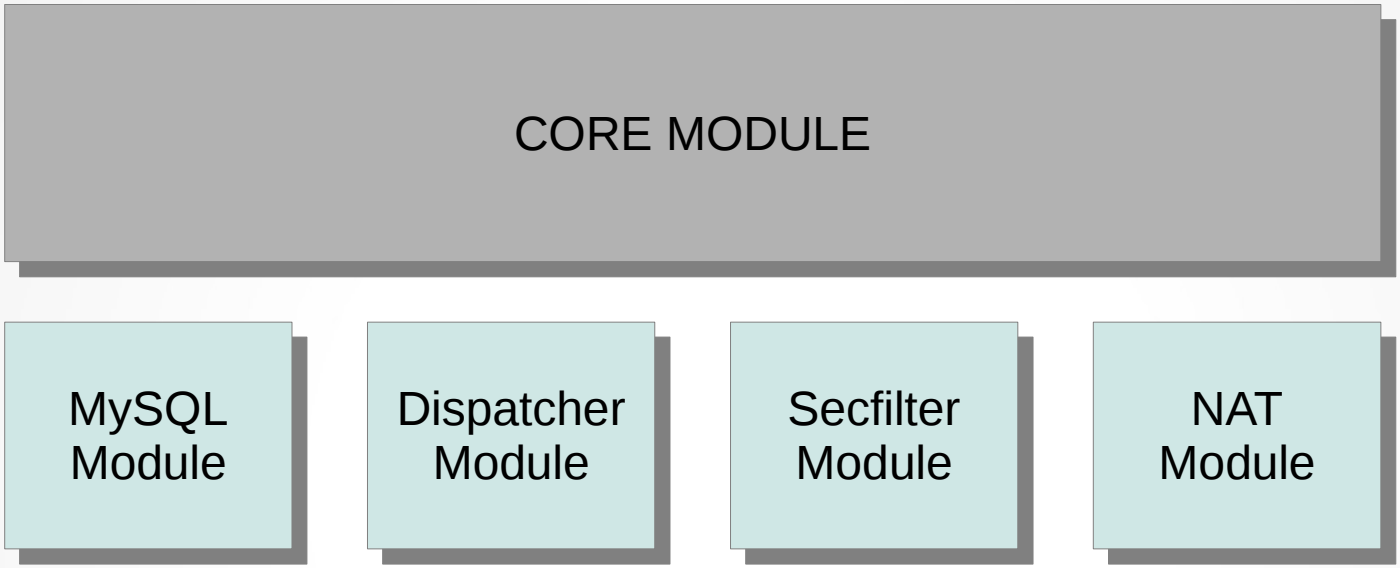
- Sip Proxy Server
- Sip Registrar Server
- Sip Location Server
- Sip Dispatcher Server
- Sip Application Server
- Open Source
- Escalable
- TCP / UDP / TLS

- NO es una centralita IP
- NO sabe de buzones
- NO sabe de audio/codecs
- NO sabe de extensiones
- NO es sencillo de administrar

Esquema típico



Arquitectura



Configuración básica

```
#!KAMAILIO
#!define WITH_MYSQL
#!define WITH_AUTH
#!define WITH_IPAUTH
#!define WITH_USRLOCDB
#!define WITH_PERMISSIONS
#!define WITH_ACCDB
#!define WITH_NAT
#!define WITH_DIALOG
#!define WITH_DEBUG
#!define WITH_MULTIDOMAIN
#!define WITH_PRESENCE

#!define LISTEN_UDP_PUBLIC udp:109.69.11.194:5060
#!define LISTEN_UDP_PRIVATE udp:10.90.234.1:5060
#!define MYSQL_URL "mysql://kamailio:kamailio@10.90.234.3/kamailio"

# ----- rtpproxy params -----
modparam("rtpengine", "rtpengine_sock", "udp:10.90.234.4:2223")
#modparam("rtpengine", "setid_avp", "$avp(setid)")
modparam("nathelper", "received_avp", "$avp(s:received)")
modparam("nathelper", "sipping_bflag", FLB_NATSIPPING)
modparam("nathelper", "natping_interval", 120)
modparam("nathelper", "ping_nated_only", 1)
modparam("nathelper", "sipping_from", "sip:pingsrv@109.69.11.194")

modparam("dialog", "enable_stats", 1)
modparam("dialog", "dlg_flag", FLT_DIALOG)
modparam("dialog", "hash_size", 4096)
modparam("dialog", "profiles_with_value", "callquota")
modparam("dialog", "default_timeout", 28800)
modparam("dialog", "dlg_match_mode",2)
modparam("dialog", "detect_spirals", 1)
modparam("dialog", "db_mode", 1)
modparam("dialog", "db_url", DBURL)
modparam("dialog", "ka_timer", 10)
modparam("dialog", "ka_interval", 100)
```

```
####### Local Configuration ########
include_file "entrada.cfg"

####### Routing Logic ########
# main request routing logic

route {
	route(SANITY_CHECK);

	route(NATDETECT);

	loose_route();

	route(WITHINDLG);

	# CANCEL processing
	if (is_method("CANCEL")) {
		rtpengine_manage();
		if (t_check_trans()) {
			route(RELAY);
		}
		exit;
	}
	t_check_trans();

	# Set DLG flag to track dialogs using dialog2
	if (!is_method("SUBSCRIBE|PUBLISH")) {
		setflag(FLT_DLGINFO);
		dlg_manage();
	}
	# handle requests within SIP dialogs

	route(AUTH);
	# Handle registrations
	if (is_method("REGISTER")) {
		route(REGISTRAR);
	}
```

Configuración básica

```
avp_delete("*");
	xlog("L_INFO","SELECT username,rpid,rpid_callerid FROM subscriber where username=$au \n");
	if (avp_db_query("SELECT username,rpid,rpid_callerid FROM subscriber where username='$au'", "$avp(s:idusername);$avp(s:rpid);$avp(s:rpid_callerid)")
	 {
	    xlog("L_INFO", "..... avp(s:idusername) = $avp(s:idusername)..... \n");
	    xlog("L_INFO", "..... avp(s:rpid) = $avp(s:rpid) avp(s:rpid_callerid) = $avp(s:rpid_callerid) ..... \n");
	 }
	$fu = "sip:" + $avp(s:rpid) +"@"+ $fd;
	xlog("L_INFO", "time [$Tf] method ($rm) r-uri ($ru) 2nd via ($hdr(via[1])) el valor de fu $fu $fU para final \n");

	# quitamos la cabecera p-asserted mal y ponemos la buena
	xlog("L_INFO","..... CABECERA $re es $re ..... \n");
	if ($var(privacidad) == "full" ) {
	 append_rpid_hf("","party=calling;privacy=full;screen=no");
	} else {
	 append_rpid_hf("","party=calling;privacy=off;screen=no");
	}
	remove_hf("P-Asserted-Identity");
	append_hf("P-Asserted-Identity: <sip:$avp(s:rpid)@$fd>\r\n");
	remove_hf("P-Preferred-Identity");
	append_hf("P-Preferred-Identity: <sip:$avp(s:rpid)@$fd>\r\n");

	# fin modificacion cabeceras
	# round robin dispatching on gateways group '1'
	# record routing for dialog forming requests (in case they are routed)
	# - remove preloaded route headers
	xlog("L_INFO","..... el valor de gateway $var(GATEWAY) ....\n");
	if (is_method("INVITE|REFER")) {
		if (isflagset(FLAG_FROM_PEER)) {
			if(!ds_select_dst("$var(GATEWAY)", "4")) {
				send_reply("404", "No destination");
				exit;
			}
			$rd = $dd ;
		}
	}
```

¿ y para el audio ?

- Kamailio no administra sesiones de audio y necesita un agente externo para ello, como por ejemplo RTPProxy o RTPEngine.

- RTPproxy lleva muchos años de desarrollo.

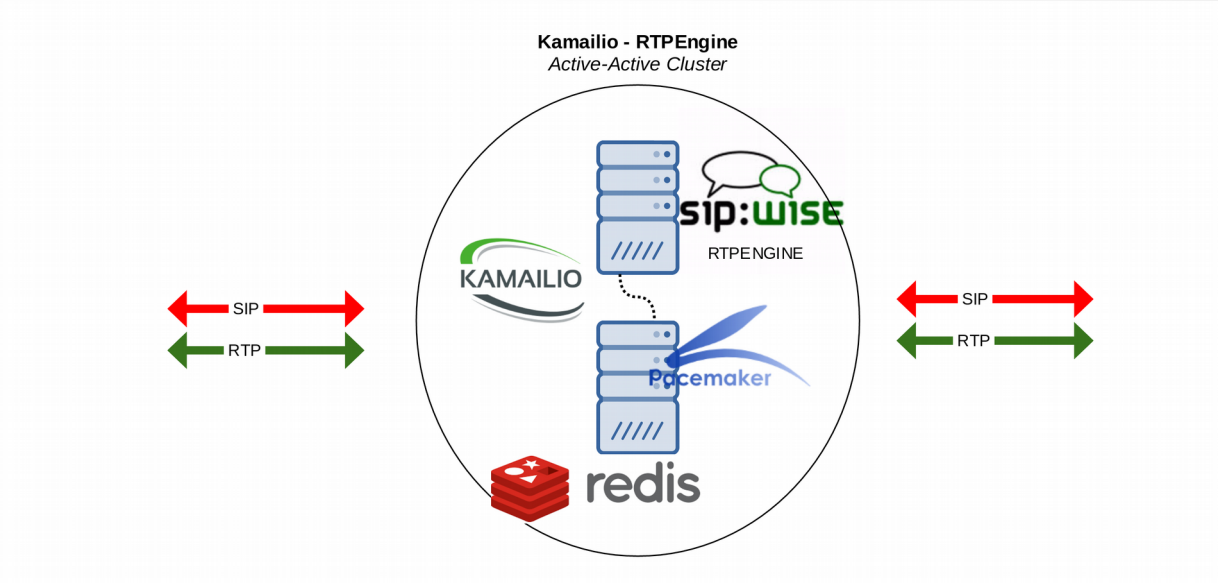
- RTPEngine se integra con el kernel – Iptables de linux y su rendimiento es muy superior.

- RTPEngine se puede poner el H.A, junto con REDIS, COROSYNC y PACEMAKER.

- RTPEngine se aconseja colocar en una máquina separada al proxy

rtpengine

```
[rtpengine]

table = 0
# no-fallback = false
### for userspace forwarding only:
# table = -1

interface = priv/10.90.13.234.4;pub/109.69.11.196


RUN_RTPENGINE=yes

Listen-ng = 10.90.234.4:2223
listen-tcp = 25060
listen-udp = 12222

timeout = 60
silent-timeout = 3600
tos = 184
# delete-delay = 30
# final-timeout = 10800

# foreground = false
pidfile = /var/run/ngcp-rtpengine-daemon.pid
num-threads = 16

port-min = 20000
port-max = 50000
max-sessions = 15000

recording-dir = /var/spool/rtpengine
recording-method = proc
recording-format = raw
```



¿Qué más puede hacer?

Uff !!!! vaya tostón !!!!!! ME ABURRO !!!!!!! explica algo más interesante ….

VoIP Hacking

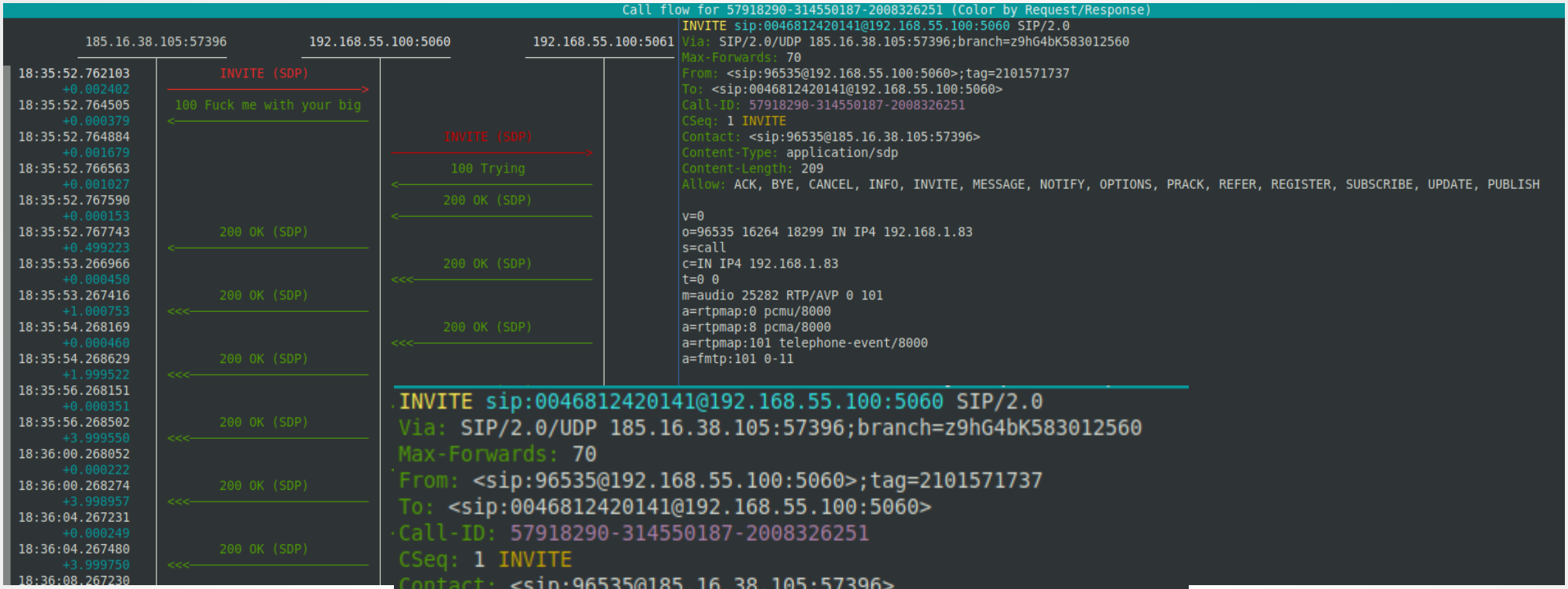
Abro mi SIP server al exterior……. ¿problemas?

Pillando cacho !!!!

```
                                                                    sngrep - SIP messages flow viewer
Current Mode: Online [any]                  Dialogs: 14
Match Expression:                           BPF Filter:
Display Filter:
     ^Idx Method     SIP From                  SIP To                    Msgs  Source                Destination           Call State
[ ] 1    INVITE     96535@192.168.55.100:5060 0046812420141@192.168.55. 26    185.16.38.105:57396   192.168.55.100:5060   CALL SETUP
[ ] 2    INVITE     19565@192.168.55.100:5060 000441730635300@192.168.5 26    193.29.14.123:50877   192.168.55.100:5060   CALL SETUP
[ ] 3    INVITE     16652@192.168.55.100:5060 00048221530704@192.168.55 26    185.16.38.107:65127   192.168.55.100:5060   CALL SETUP
[ ] 4    INVITE     17078@192.168.55.100:5060 441674728002@192.168.55.1 26    193.29.14.124:60149   192.168.55.100:5060   CALL SETUP
[ ] 5    INVITE     89390@192.168.55.100:5060 9006436685424@192.168.55. 26    185.16.38.109:54745   192.168.55.100:5060   CALL SETUP
[ ] 6    INVITE     96535@192.168.55.100:5060 00046812420141@192.168.55 16    185.16.38.105:53366   192.168.55.100:5060   CALL SETUP
[ ] 7    OPTIONS    asterisk@192.168.55.100:5 192.168.2.5               2     192.168.55.100:5061   192.168.2.5:5060
[ ] 8    REGISTER   899@192.168.55.100:5060   899@192.168.55.100:5060   3     5.39.66.199:57986     192.168.55.100:5060
[ ] 9    REGISTER   899@192.168.55.100:5060   899@192.168.55.100:5060   3     5.39.66.199:58013     192.168.55.100:5060
[ ] 10   REGISTER   899@192.168.55.100:5060   899@192.168.55.100:5060   3     5.39.66.199:58014     192.168.55.100:5060
[ ] 11   REGISTER   899@192.168.55.100:5060   899@192.168.55.100:5060   3     5.39.66.199:57990     192.168.55.100:5060
[ ] 12   REGISTER   899@192.168.55.100:5060   899@192.168.55.100:5060   3     5.39.66.199:57999     192.168.55.100:5060
[ ] 13   INVITE     19565@192.168.55.100:5060 900441730635300@192.168.5 14    193.29.14.123:54001   192.168.55.100:5060   CALL SETUP
[ ] 14   INVITE     17078@192.168.55.100:5060 +441674728002@192.168.55. 12    193.29.14.124:64332   192.168.55.100:5060   CALL SETUP
```

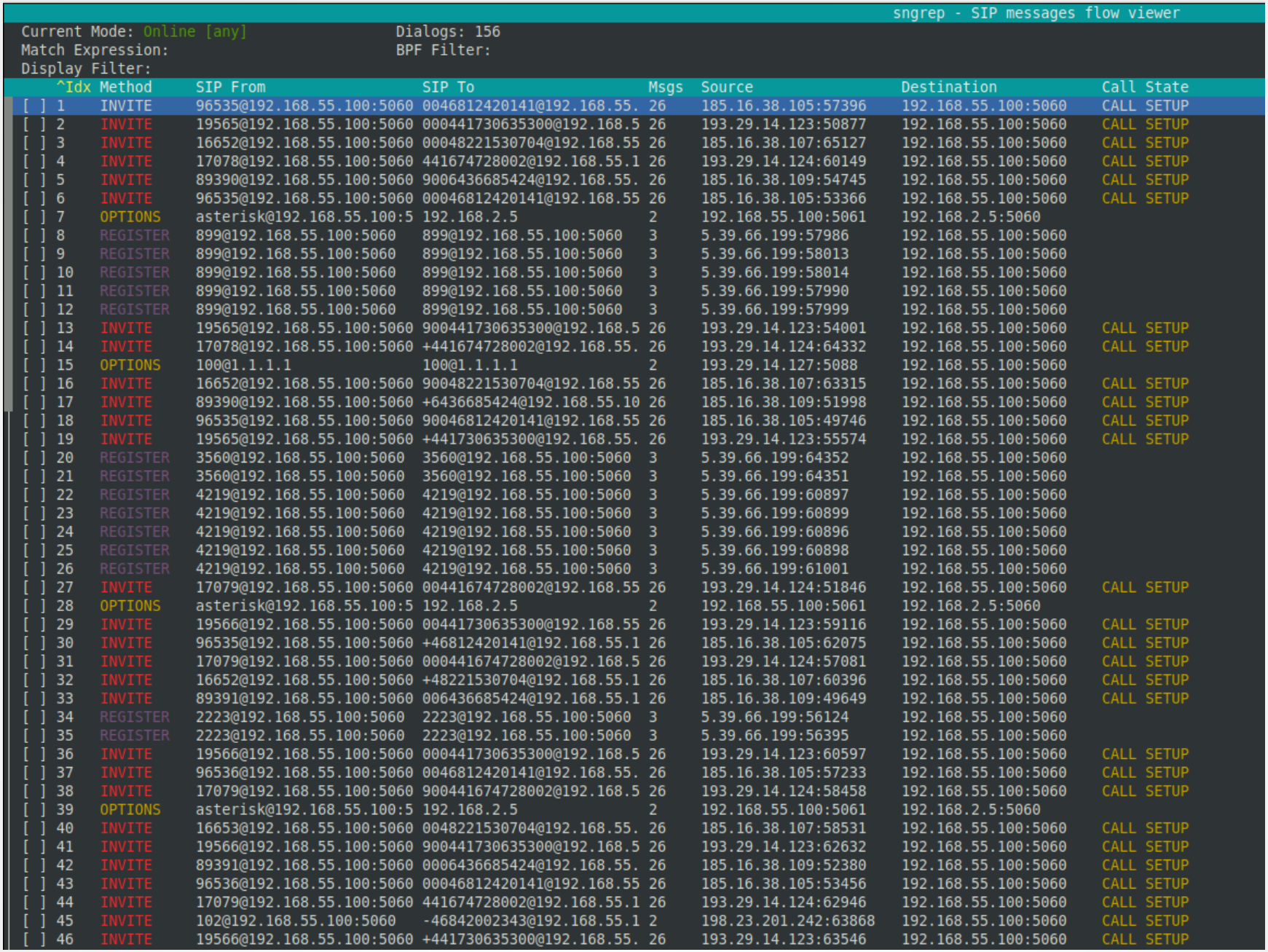
Abro inocentemente mi centralita PBX a internet (o las 10.x de guifi.net) y empiezo a tener conexiones extrañas…… ip’s que no conozco, intentos de llamadas y miles de PP’s.

Analicemos un poco….



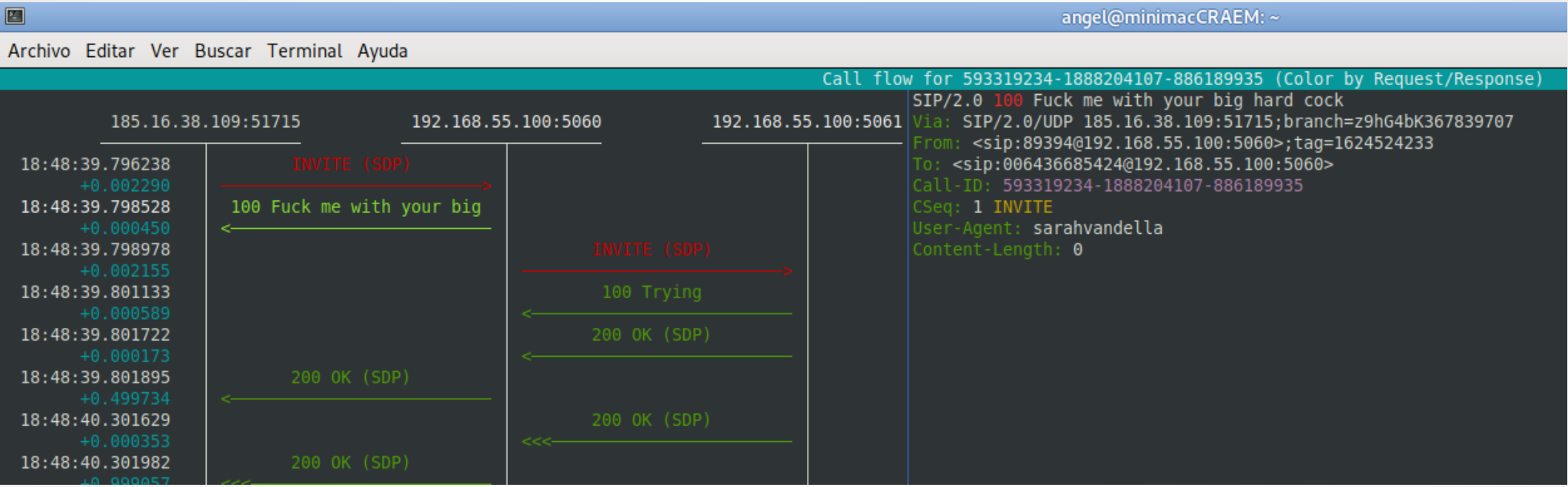

```
INVITE sip:004681242014l@192.168.55.100:5060 SIP/2.0
Via: SIP/2.0/UDP 185.16.38.105:57396;branch=z9hG4bK583012560
Max-Forwards: 70
From: <sip:96535@192.168.55.100:5060>;tag=2101571737
To: <sip:004681242014l@192.168.55.100:5060>
Call-ID: 57918290-314550187-2008326251
CSeq: 1 INVITE
Contact: <sip:96535@185.16.38.105:57396>
Content-Type: application/sdp
Content-Length: 209
Allow: ACK, BYE, CANCEL, INFO, INVITE, MESSAGE, NOTIFY, OPTIONS,

v=0
o=96535 16264 18299 IN IP4 192.168.1.83
s=call
c=IN IP4 192.168.1.83
t=0 0
m=audio 25282 RTP/AVP 0 101
a=rtpmap:0 pcmu/8000
a=rtpmap:8 pcma/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-11
```

Y seguimos……



	^Idx	Method	SIP From	SIP To	Msgs	Source	Destination	Call State
[ ]	1	INVITE	96535@192.168.55.100:5060	0046812420141@192.168.55.	26	185.16.38.105:57396	192.168.55.100:5060	CALL SETUP
[ ]	2	INVITE	19565@192.168.55.100:5060	000441730635300@192.168.5	26	193.29.14.123:50877	192.168.55.100:5060	CALL SETUP
[ ]	3	INVITE	16652@192.168.55.100:5060	00048221530704@192.168.55	26	185.16.38.107:65127	192.168.55.100:5060	CALL SETUP
[ ]	4	INVITE	17078@192.168.55.100:5060	441674728002@192.168.55.1	26	193.29.14.124:60149	192.168.55.100:5060	CALL SETUP
[ ]	5	INVITE	89390@192.168.55.100:5060	9006436685424@192.168.55.	26	185.16.38.109:54745	192.168.55.100:5060	CALL SETUP
[ ]	6	INVITE	96535@192.168.55.100:5060	00046812420141@192.168.55	26	185.16.38.105:53366	192.168.55.100:5060	CALL SETUP
[ ]	7	OPTIONS	asterisk@192.168.55.100:5	192.168.2.5	2	192.168.55.100:5061	192.168.2.5:5060	
[ ]	8	REGISTER	899@192.168.55.100:5060	899@192.168.55.100:5060	3	5.39.66.199:57986	192.168.55.100:5060	
[ ]	9	REGISTER	899@192.168.55.100:5060	899@192.168.55.100:5060	3	5.39.66.199:58013	192.168.55.100:5060	
[ ]	10	REGISTER	899@192.168.55.100:5060	899@192.168.55.100:5060	3	5.39.66.199:58014	192.168.55.100:5060	
[ ]	11	REGISTER	899@192.168.55.100:5060	899@192.168.55.100:5060	3	5.39.66.199:57990	192.168.55.100:5060	
[ ]	12	REGISTER	899@192.168.55.100:5060	899@192.168.55.100:5060	3	5.39.66.199:57999	192.168.55.100:5060	
[ ]	13	INVITE	19565@192.168.55.100:5060	900441730635300@192.168.5	26	193.29.14.123:54001	192.168.55.100:5060	CALL SETUP
[ ]	14	INVITE	17078@192.168.55.100:5060	+441674728002@192.168.55.	26	193.29.14.124:64332	192.168.55.100:5060	CALL SETUP
[ ]	15	OPTIONS	100@1.1.1.1	100@1.1.1.1	2	193.29.14.127:5088	192.168.55.100:5060	
[ ]	16	INVITE	16652@192.168.55.100:5060	90048221530704@192.168.55	26	185.16.38.107:63315	192.168.55.100:5060	CALL SETUP
[ ]	17	INVITE	89390@192.168.55.100:5060	+6436685424@192.168.55.10	26	185.16.38.109:51998	192.168.55.100:5060	CALL SETUP
[ ]	18	INVITE	96535@192.168.55.100:5060	900468124201 41@192.168.55	26	185.16.38.105:49746	192.168.55.100:5060	CALL SETUP
[ ]	19	INVITE	19565@192.168.55.100:5060	+441730635300@192.168.55.	26	193.29.14.123:55574	192.168.55.100:5060	CALL SETUP
[ ]	20	REGISTER	3560@192.168.55.100:5060	3560@192.168.55.100:5060	3	5.39.66.199:64352	192.168.55.100:5060	
[ ]	21	REGISTER	3560@192.168.55.100:5060	3560@192.168.55.100:5060	3	5.39.66.199:64351	192.168.55.100:5060	
[ ]	22	REGISTER	4219@192.168.55.100:5060	4219@192.168.55.100:5060	3	5.39.66.199:60897	192.168.55.100:5060	
[ ]	23	REGISTER	4219@192.168.55.100:5060	4219@192.168.55.100:5060	3	5.39.66.199:60899	192.168.55.100:5060	
[ ]	24	REGISTER	4219@192.168.55.100:5060	4219@192.168.55.100:5060	3	5.39.66.199:60896	192.168.55.100:5060	
[ ]	25	REGISTER	4219@192.168.55.100:5060	4219@192.168.55.100:5060	3	5.39.66.199:60898	192.168.55.100:5060	
[ ]	26	REGISTER	4219@192.168.55.100:5060	4219@192.168.55.100:5060	3	5.39.66.199:61001	192.168.55.100:5060	
[ ]	27	INVITE	17079@192.168.55.100:5060	00441674728002@192.168.55	26	193.29.14.124:51846	192.168.55.100:5060	CALL SETUP
[ ]	28	OPTIONS	asterisk@192.168.55.100:5	192.168.2.5	2	192.168.55.100:5061	192.168.2.5:5060	
[ ]	29	INVITE	19566@192.168.55.100:5060	00441730635300@192.168.55	26	193.29.14.123:59116	192.168.55.100:5060	CALL SETUP
[ ]	30	INVITE	96535@192.168.55.100:5060	+46812420141@192.168.55.1	26	185.16.38.105:62075	192.168.55.100:5060	CALL SETUP
[ ]	31	INVITE	17079@192.168.55.100:5060	000441674728002@192.168.5	26	193.29.14.124:57081	192.168.55.100:5060	CALL SETUP
[ ]	32	INVITE	16652@192.168.55.100:5060	+48221530704@192.168.55.1	26	185.16.38.107:60396	192.168.55.100:5060	CALL SETUP
[ ]	33	INVITE	89391@192.168.55.100:5060	006436685424@192.168.55.1	26	185.16.38.109:49649	192.168.55.100:5060	CALL SETUP
[ ]	34	REGISTER	2223@192.168.55.100:5060	2223@192.168.55.100:5060	3	5.39.66.199:56124	192.168.55.100:5060	
[ ]	35	REGISTER	2223@192.168.55.100:5060	2223@192.168.55.100:5060	3	5.39.66.199:56395	192.168.55.100:5060	
[ ]	36	INVITE	19566@192.168.55.100:5060	000441730635300@192.168.5	26	193.29.14.123:60597	192.168.55.100:5060	CALL SETUP
[ ]	37	INVITE	96536@192.168.55.100:5060	0046812420141@192.168.55.	26	185.16.38.105:57233	192.168.55.100:5060	CALL SETUP
[ ]	38	INVITE	17079@192.168.55.100:5060	900441674728002@192.168.5	26	193.29.14.124:58458	192.168.55.100:5060	CALL SETUP
[ ]	39	OPTIONS	asterisk@192.168.55.100:5	192.168.2.5	2	192.168.55.100:5061	192.168.2.5:5060	
[ ]	40	INVITE	16653@192.168.55.100:5060	0048221530704@192.168.55.	26	185.16.38.107:58531	192.168.55.100:5060	CALL SETUP
[ ]	41	INVITE	19566@192.168.55.100:5060	900441730635300@192.168.5	26	193.29.14.123:62632	192.168.55.100:5060	CALL SETUP
[ ]	42	INVITE	89391@192.168.55.100:5060	0006436685424@192.168.55.	26	185.16.38.109:52380	192.168.55.100:5060	CALL SETUP
[ ]	43	INVITE	96536@192.168.55.100:5060	00046812420141@192.168.55	26	185.16.38.105:53456	192.168.55.100:5060	CALL SETUP
[ ]	44	INVITE	17079@192.168.55.100:5060	441674728002@192.168.55.1	26	193.29.14.124:62946	192.168.55.100:5060	CALL SETUP
[ ]	45	INVITE	102@192.168.55.100:5060	-46842002343@192.168.55.1	2	198.23.201.242:63868	192.168.55.100:5060	CALL SETUP
[ ]	46	INVITE	19566@192.168.55.100:5060	+441730635300@192.168.55.	26	193.29.14.123:63546	192.168.55.100:5060	CALL SETUP

-Cazando al ladrón -




```
    # Al recibir un intento de llamada, modificamos el destino para que siempre llame a la extensión 100
if (is_method("INVITE")) {

    xlog("L_INFO","..... afegim a ip blocades $si $tu $rU ... \n");
    avp_db_query("INSERT into logs_ataque (ip,destino,src,method,userAgent) values ('$si','$tu','$fU','invite','$ua')");
    xlog("L_INFO", "$fU (with IP:$si) is trying to call to $rU\n");
    $rU = "6969";
    $du = "sip:192.168.55.100:5061";
    $rd = $dd;
    $td = $dd;
    record_route();
    xlog("L_INFO", "enviem trucada a blackhole $rU\n");
    route(RELAY);
}
```

Generando un HoneyPOT

```
mysql> select * from logs_ataque;
+---------+---------------+-----------------------------------------+-------+---------------------+----------+-----------------------------+-----------+
| id      | ip            | destino                                 | src   | date                | method   | userAgent                   | procesado |
+---------+---------------+-----------------------------------------+-------+---------------------+----------+-----------------------------+-----------+
| 2398910 | 185.16.38.109 | sip:9006436685424@192.168.55.100:5060   | 89380 | 2021-02-10 18:00:18 | invite   | <null>                      |         0 |
| 2398911 | 185.16.38.107 | sip:90048221530704@192.168.55.100:5060  | 16642 | 2021-02-10 18:00:18 | invite   | <null>                      |         0 |
| 2398912 | 185.16.38.105 | sip:9004681242014l@192.168.55.100:5060  | 96520 | 2021-02-10 18:00:21 | invite   | <null>                      |         0 |
| 2398913 | 193.29.14.124 | sip:00441674728002@192.168.55.100:5060  | 17066 | 2021-02-10 18:00:28 | invite   | <null>                      |         0 |
| 2398914 | 193.29.14.123 | sip:000441730635300@192.168.55.100:5060 | 19549 | 2021-02-10 18:00:30 | invite   | <null>                      |         0 |
| 2398915 | 185.16.38.105 | sip:+46812420141@192.168.55.100:5060    | 96520 | 2021-02-10 18:00:56 | invite   | <null>                      |         0 |
| 2398916 | 193.29.14.124 | sip:000441674728002@192.168.55.100:5060 | 17066 | 2021-02-10 18:01:03 | invite   | <null>                      |         0 |
| 2398917 | 193.29.14.123 | sip:900441730635300@192.168.55.100:5060 | 19549 | 2021-02-10 18:01:04 | invite   | <null>                      |         0 |
| 2398918 | 185.16.38.109 | sip:+6436685424@192.168.55.100:5060     | 89380 | 2021-02-10 18:01:11 | invite   | <null>                      |         0 |
| 2398919 | 185.16.38.107 | sip:+48221530704@192.168.55.100:5060    | 16642 | 2021-02-10 18:01:14 | invite   | <null>                      |         0 |
| 2398920 | 5.39.66.199   | sip:2882@192.168.55.100:5060            | 2882  | 2021-02-10 18:01:26 | register | ims                         |         0 |
| 2398921 | 5.39.66.199   | sip:2882@192.168.55.100:5060            | 2882  | 2021-02-10 18:01:26 | register | ims                         |         0 |
| 2398922 | 185.16.38.105 | sip:0046812420141@192.168.55.100:5060   | 96521 | 2021-02-10 18:01:36 | invite   | <null>                      |         0 |
| 2398923 | 193.29.14.124 | sip:900441674728002@192.168.55.100:5060 | 17066 | 2021-02-10 18:01:37 | invite   | <null>                      |         0 |
| 2398924 | 193.29.14.123 | sip:+441730635300@192.168.55.100:5060   | 19549 | 2021-02-10 18:01:38 | invite   | <null>                      |         0 |
| 2398925 | 185.16.38.109 | sip:006436685424@192.168.55.100:5060    | 89381 | 2021-02-10 18:02:05 | invite   | <null>                      |         0 |
| 2398926 | 185.16.38.107 | sip:0048221530704@192.168.55.100:5060   | 16643 | 2021-02-10 18:02:09 | invite   | <null>                      |         0 |
| 2398927 | 193.29.14.124 | sip:441674728002@192.168.55.100:5060    | 17066 | 2021-02-10 18:02:11 | invite   | <null>                      |         0 |
| 2398928 | 185.16.38.105 | sip:0046812420141@192.168.55.100:5060   | 96521 | 2021-02-10 18:02:11 | invite   | <null>                      |         0 |
| 2398929 | 193.29.14.123 | sip:00441730635300@192.168.55.100:5060  | 19550 | 2021-02-10 18:02:12 | invite   | <null>                      |         0 |
| 2398930 | 5.39.66.199   | sip:4218@192.168.55.100:5060            | 4218  | 2021-02-10 18:02:12 | register | ims                         |         0 |
| 2398931 | 5.39.66.199   | sip:4218@192.168.55.100:5060            | 4218  | 2021-02-10 18:02:13 | register | ims                         |         0 |
| 2398932 | 5.39.66.199   | sip:4218@192.168.55.100:5060            | 4218  | 2021-02-10 18:02:13 | register | ims                         |         0 |
| 2398933 | 5.39.66.199   | sip:4218@192.168.55.100:5060            | 4218  | 2021-02-10 18:02:13 | register | ims                         |         0 |
```

Recopilando datos ……

```
mysql> select * from ips_ataques_extended;
+-----+-----------------+-------------+-----------------+---------+---------+-----------------------------------------------------------------------------------------------------------------+--------------+
| id  | ip              | as_number   | inet_num        | country | netname | description                                                                                                     | hints_ataques |
+-----+-----------------+-------------+-----------------+---------+---------+-----------------------------------------------------------------------------------------------------------------+--------------+
|   1 | 103.145.13.140  | 213371      | 103.145.13.0/24 | IN      | 0       | SQUITTER-NETWORKS, NL                                                                                           |          262 |
|   2 | 185.116.194.75  | 202958      | 185.116.194.0/24| KZ      | 0       | HOSTER-, KZ                                                                                                     |            1 |
|   3 | 185.124.31.143  | 12479       | 185.124.31.0/24 | ES      | 0       | UNI2-AS, ES                                                                                                     |            1 |
|   4 | 51.195.7.14     | 16276       | 51.195.0.0/16   | FR      | 0       | OVH, FR                                                                                                         |         1261 |
|   5 | 62.210.101.43   | 12876       | 62.210.0.0/16   | FR      | 0       | Online SAS, FR                                                                                                  |            5 |
|   6 | 167.114.156.189 | 16276       | 167.114.128.0/18| CA      | 0       | OVH, FR                                                                                                         |       120641 |
|   7 | 88.119.29.163   | 8764        | 88.119.0.0/18   | LT      | 0       | TELIA-LIETUVA, LT                                                                                               |            1 |
|   8 | 192.99.45.32    | 16276       | 192.99.0.0/16   | CA      | 0       | OVH, FR                                                                                                         |         3173 |
|   9 | 95.111.239.138  | 51167       | 95.111.238.0/23 | DE      | 0       | CONTABO, DE                                                                                                     |            2 |
|  10 | 45.143.221.96   | 213371      | 45.143.221.0/24 | NL      | 0       | SQUITTER-NETWORKS, NL                                                                                           |        14957 |
|  11 | 51.75.145.188   | 16276       | 51.75.0.0/16    | FR      | 0       | OVH, FR                                                                                                         |            4 |
|  12 | 195.154.40.99   | 12876       | 195.154.0.0/16  | FR      | 0       | Online SAS, FR                                                                                                  |           21 |
|  13 | 51.75.86.211    | 16276       | 51.75.0.0/16    | FR      | 0       | OVH, FR                                                                                                         |           31 |
|  14 | 103.145.12.227  | 213371      | 103.145.12.0/24 | IN      | 0       | SQUITTER-NETWORKS, NL                                                                                           |         2103 |
|  15 | 46.249.32.234   | 50673       | 46.249.32.0/19  | NL      | 0       | SERVERIUS-AS, NL                                                                                                |            3 |
|  16 | 51.158.29.207   | 12876       | 51.158.0.0/15   | FR      | 0       | Online SAS, FR                                                                                                  |           44 |
|  17 | 45.143.220.250  | 213371      | 45.143.220.0/24 | NL      | 0       | SQUITTER-NETWORKS, NL                                                                                           |         1572 |
|  18 | 54.36.164.183   | 16276       | 54.36.0.0/16    | FR      | 0       | OVH, FR                                                                                                         |          188 |
|  19 | 51.195.7.137    | 16276       | 51.195.0.0/16   | FR      | 0       | OVH, FR                                                                                                         |        26892 |
|  20 | 45.148.121.19   | 64425       | 45.148.121.0/24 | NL      | 0       | SKB-ENTERPRISE, NL                                                                                              |        14458 |
|  21 | 103.145.13.22   | 213371      | 103.145.13.0/24 | IN      | 0       | SQUITTER-NETWORKS, NL                                                                                           |            6 |
|  22 | 51.210.113.204  | 16276       | 51.210.0.0/16   | FR      | 0       | OVH, FR                                                                                                         |           30 |
|  23 | 45.148.121.137  | 64425       | 45.148.121.0/24 | NL      | 0       | SKB-ENTERPRISE, NL                                                                                              |          115 |
|  24 | 212.83.177.158  | 12876       | 212.83.160.0/19 | FR      | 0       | Online SAS, FR                                                                                                  |          381 |
|  26 | 193.176.86.200  | 9009        | 193.176.86.0/24 | RO      | 0       | M247, GB                                                                                                        |            1 |
|  27 | 103.145.13.129  | 213371      | 103.145.13.0/24 | IN      | 0       | SQUITTER-NETWORKS, NL                                                                                           |            6 |
|  28 | 156.96.58.114   | 46664       | 156.96.58.0/24  | US      | 0       | VDI-NETWORK, US                                                                                                 |        17914 |
|  29 | 156.96.117.187  | 46664       | 156.96.112.0/21 | US      | 0       | VDI-NETWORK, US                                                                                                 |         5876 |
|  30 | 84.17.43.179    | 60068       | 84.17.42.0/23   | GB      | 0       | CDN77, GB                                                                                                       |          121 |
```

Vale…. Superguai…. Y ahora qué hacemos con las ip’s / rangos que nos atacan ?

- Blacklist IPTABLES
- Secfilter module kamailio
- BlackHole …
- Mi imaginación….

SecFilter kamailio

```
route[REQINIT] {

       secf_check_ip();
       $var(baneada) = $?;
       xlog("L_ALERT",".... VALOR TRANSACC::2:: $rm $si $? $var(baneada) ..............\n");
       if ($var(baneada) == -2) {
             xlog("L_ALERT", "$rm from $si blocked because IP address is blacklisted");
             sl_send_reply("200","Fuck me with your big hard cock");
             exit;
             }


       # Si detectamos el User-Agent de un escáner conocido, mostramos una alerta
       if($ua == "friendly-scanner" || $ua == "sundayddr" || $ua == "sip-scan" || $ua == "iWar" || $ua == "sipsak") {
              xlog("L_ALERT", "Attack attempt! IP:$si:$sp - R:$ruri - F:$fu - T:$tu - UA:$ua - $rm\n");
       }

       # Al recibir un intento de registro, devolvemos siempre un OK
  if (is_method("REGISTER")) {
       avp_db_query("INSERT into logs_ataque (ip,destino,src,method,userAgent) values ('$si','$tu','$fU','register','$ua')");
       xlog("L_INFO", "Get Register for user $fU (IP: $si)\n");

     if ($fU != "100")
        sl_send_reply("407","Proxy Authentication Required");
  }
```

- Podemos filtrar por IP y denegar la conexión
- Podemos filtrar por user-agent
- Podemos bloquear por iptables.

Colorín colorado…..