SIP Express Media Server
SBC
KamailioWorld 2014

Stefan Sayer, CTO FRAFOS GmbH
stefan.sayer@frafos.com

VoIP Services Consulting and Development
e-mail/xmpp:stefan.sayer@gmail.com
Contents

- The SIP Express Media Server
- SEMS SBC

........................ snip ........................

- #MoreCrypto
• Originates from the same team as SER (Kamailio/OpenSER/...) at Fraunhofer FOKUS
• SIP Media and Application Server
• Developed at various related companies (iptelorg, IPTEGO, ...)
• Since 2010 mainly at FRAFOS
• Open Source community since 2003
FRAFOS ABC SBC

- Full-fledged SBC, turn-key solution
- Border security, monitoring, SIP control and mediation, registration offload, transcoding etc
- Software only, on FRAFOS-provided hardware or virtualized deployment (incl EC2)
- HA with active-hot standby (SIP+RTP)
- 100% rule based administration through GUI
- Application offloading and integration through open APIs and programming platform
- WebRTC gateway
SEMS project focus

- Telecoms applications, carrier environment
  - High volume prompts, voicemail, conferencing, …
  - B2BUA / SBC
- Speed and reliability
- Only SIP, not multi-protocol (almost)
- Versatile and easy to use app server for SIP networks

- Built for purpose
SEMS SBC application

- B2BUA, completely transparent to fully opaque
- Handles SIP and (optional) RTP
- Flexible and programmable
- "The Swiss Army Knife of call stateful SIP processing"
SEMS SBC features

- B2BUA, network separation
- SIP message manipulation & mediation, header/message filter
- SIP NAT handling, TCP/UDP, DNS SRV w/failover
- SST enforcement
- Registration Caching
- SIP client auth
- CDR generation, call timer, parallel call limits, prepaid, ...
SBC: media features

- RTP relaying
- Near & far end NAT traversal
- Codec filter, SDP filter
- Transcoding
SBC: Profile based control

set_fromto.sbcprofile.conf

URI=$tU@sbc1.mypeer.net
From=<$fU@mynet.net>
To=<sip:$tU@mypeer.net>
Call-ID=$ci_leg2
enable_rtprelay=yes

# U 210.13.3.122:5080 -> 210.13.3.100:5060
INVITE sip:+49123@sbc1.mynet.net SIP/2.0
From: "John" <sip:+431556221@mynet.net>;tag=12
To: "Clara" <+49123@mynet.net>
Call-ID: 3cde5d1a960a-dez6oz34ll04
...

SEMS SBC

# U 210.13.3.100:5060 -> 213.192.59.75:5060
INVITE sip:+49123@sbc1.mypeer.net SIP/2.0
From: <+431556221@mynet.net>;tag=3213
To: <sip:+49123@mypeer.net>
Call-ID: 3cde5d1a960a-dez6oz34ll04_leg2
...

known
SER
pseudo-variables
SBC example: auth_b2b

- Identity change
- SIP auth upstream
- Set e.g. In headers
  - $P(name)$ selects name from P-App-Param

Test:
```bash
if (uri="^sip:\+49.*") {
  remove_hf("P-App-Name");
  remove_hf("P-App-Param");
  append_hf("P-App-Name: sbc\r\n");
  append_hf("P-App-Param: u=8708138;d=sipgate.de;p=mypassword\r\n");
  force_send_socket(192.168.2.32:5060);
  t Relay_to_udp("192.168.2.34","5060");
  exit;
}
```
Some profile options

RURI=$r
From=$f
To=$t
Contact=<sip:$Ri>
Call-ID=$ci_leg2

outbound_proxy=sip:192.168.5.106:5060
force_outbound_proxy=yes
next_hop=192.168.5.106:5060
outbound_interface=extern

enable_reg_caching=yes
min_regExpires=3600
max UA expires=60

dlgNatHandling=yes

enable_rtprelay=yes
rtprelay_force_symmetric_rtp=yes
aleg_rtprelay_interface=intern
rtprelay_interface=default

header_filter=blacklist
header_list=P-App-Param,P-App-Name
sdp_filter=whitelist
sdpfilter_list=g729,g723,ilbc,speex,gsm

append_headers="P-Src-IP: $si\r\n"

enable_session_timer=yes
session_expires=120
minimum_timer=90

enable_auth=yes
auth_user=$P(u)
auth_pwd=$P(p)

...
SBC: programmability

• Modules included e.g.
  ▪ Blacklist from REDIS: bl_redis
  ▪ SIP/feature control from http (REST) API: rest

• Simple Call Control API - start()/connect()/end()

• Extended Call Control API
  ▪ Control each message in detail
  ▪ Switch call legs PBX style, e.g. Mid-call prompts
  ▪ Program also with DSM script
SBC programmability example

```plaintext
transition "state changed" RUN - legStateChange / logParams(3) -> RUN;

transition "timer hit" RUN - timer(#id == 1) / {
    -- save other leg's ltag
    dlg.getOtherId($b_ltag);

    -- don't send hold, keep media session
    sbc.disconnect(false, true);

    -- instruct other leg to hang up
    set($cmd="hangup");
    set($call_id=@local_tag);
    postEvent($b_ltag, cmd;call_id);

    setInputPlaylist();
    connectMedia();
    playFile("wav/default_en.wav");
    sbc.streamsSetReceiving(false, false);
}

} -> PLAYING_FILE;

state PLAYING_FILE;
```
E stands for Express?

- Excellent signaling performance
- RTP: fills 2x1 GbE to ~55% line rate (G711)
  - Limit: high PPS (loss NIC-kernel)
  - Perf testing without packet loss detection is meaningless!
- tuning:

Makefile.defs:

```
USE_THREADPOOL=yes
MAX_RTP_SESSIONS=...
```

/etc/init.d/sems:

```
ulimit -n 100000
```

/etc/sems/sems.conf:

```
session_processor_threads=32
media_processor_threads=32
rtp_receiver_threads=32
sip_server_threads=16
```

start with cores x 2

- HT on/off
#MoreCrypto - Motivation

- Too much centralization of power is dangerous
  - e.g. see Joseph Nacchio case
- Who is going to participate in society and politics in a 100% controlled Orwellian state with ubiquitous surveillance?
- I want to live in a free society under rule of law
  - Secret laws with secret courts are NOT rule of law
- Where people also contribute to common good
  - Not only to the interests of rich & powerful few
#MoreCrypto - WebRTC

- Widespread consumer use of encryption with DTLS-SRTP

- Great VoIP UA stack in browser and mobile
  - e.g. webrtc for android app anyone?

- FRAFOS ABC SBC
  - WebRTC-gateway (to vanilla-SIP)
  - TLS, SDES/SRTP & DTLS-SRTP, ICE in SEMS
#MoreCrypto - RedPhone

- Android VoIP app with ZRTP from Open Whisper Systems (makers of TextSecure)
- Elegant app, doesn't get in your way
- Signaling: HTTP-websocket-ish

HTTPS Initiate: (GET +491234567)

200 OK
rtprelay1...

NAT open (UDP)

ZRTP

Initiate via PUSH or SMS: GET +491234567 rtprelay1...

HTTPS: Ringing...

Google CGM or SMS

NAT open (UDP)

rtprelay1.whispersystems.org

ZRTP

rtprelay1.whispersystems.org
# MoreCrypto - RedPhone-SIP-GW

- Based on SEMS, DSM, mod_httpd
- Challenges
  - Extend libmicrohttpd with websockets
  - Testing on real Android instead of simulator
  - Will have to implement codec (PT) negotiation
- WIP – need help!
  - Join OWS ML, join dev @github/sanchi/, PM
#MoreCrypto - #redecentralize

- Need to decentralize signaling (as in p2psip)
  - Each user her own DNS domain too complex
  - Location DB on P2P overlay (MaidSafe?)
- Distributed NAT handling (ICE, TURN)
  - Use friend's, or FOAF's server as turn server?
- Call hash(pubkey) instead of name/telnr
- Keys from namecoin, DNS, keyserver, webfinger, QR-code, NFC …
- Add to Freedombox, ArkOS?
Questions?

Thanks for your attention.
Links and References

- SEMS homepage: http://iptel.org/sems
- Code: sems repo at git.sip-router.org
- DSM documentation
  http://git.sip-router.org/cgi-bin/gitweb.cgi?p=sems;a=tree;f=doc/dsm
- FRAFOS website: www.frafos.com