Lessons Learned

USING APIBAN IN PRODUCTION

Fred Posner • qxork.com

AGENDA

AGENDA

Let's Talk about the Talk

1. Introduction
2. What is APIBAN?
3. Using APIBAN with Kamailio
    1. IPTABLES-API
4. Using APIBAN without Kamailio
5. Questions

INTRODUCTION

HI. I'M FRED.

- **Fred Posner**
- **qxork.com**
- **VoIP Consultant**
- **US Based 🇺🇸**
- **Matrix: qxork.com/matrix**

WHAT IS APIBAN?

APIBAN.ORG

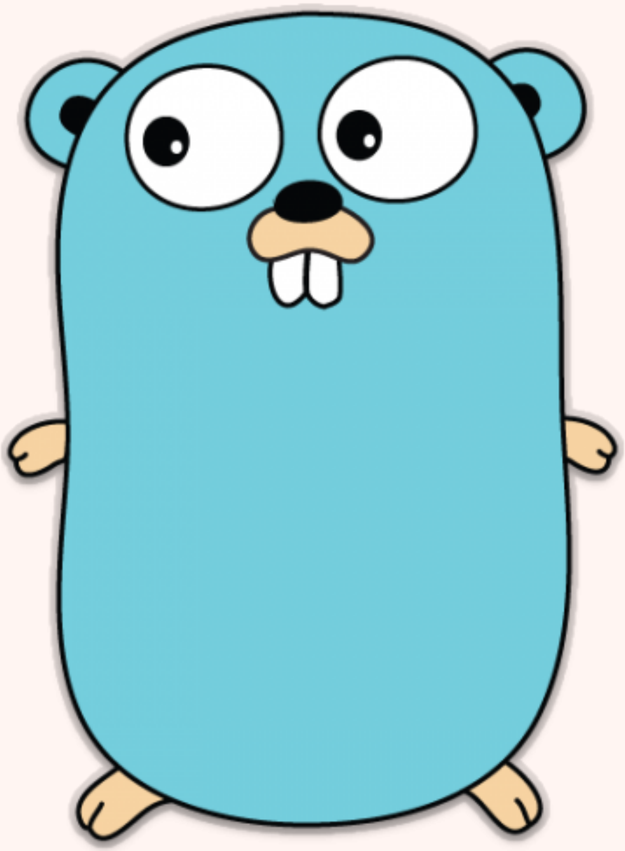
- **Elevator pitch:**
  APIBAN helps prevent **unwanted** SIP traffic by **identifying** addresses of known bad actors **before** they attack your system.

- **Globally deployed honey pots**

- **FREE service**
  (thank you sponsors!)

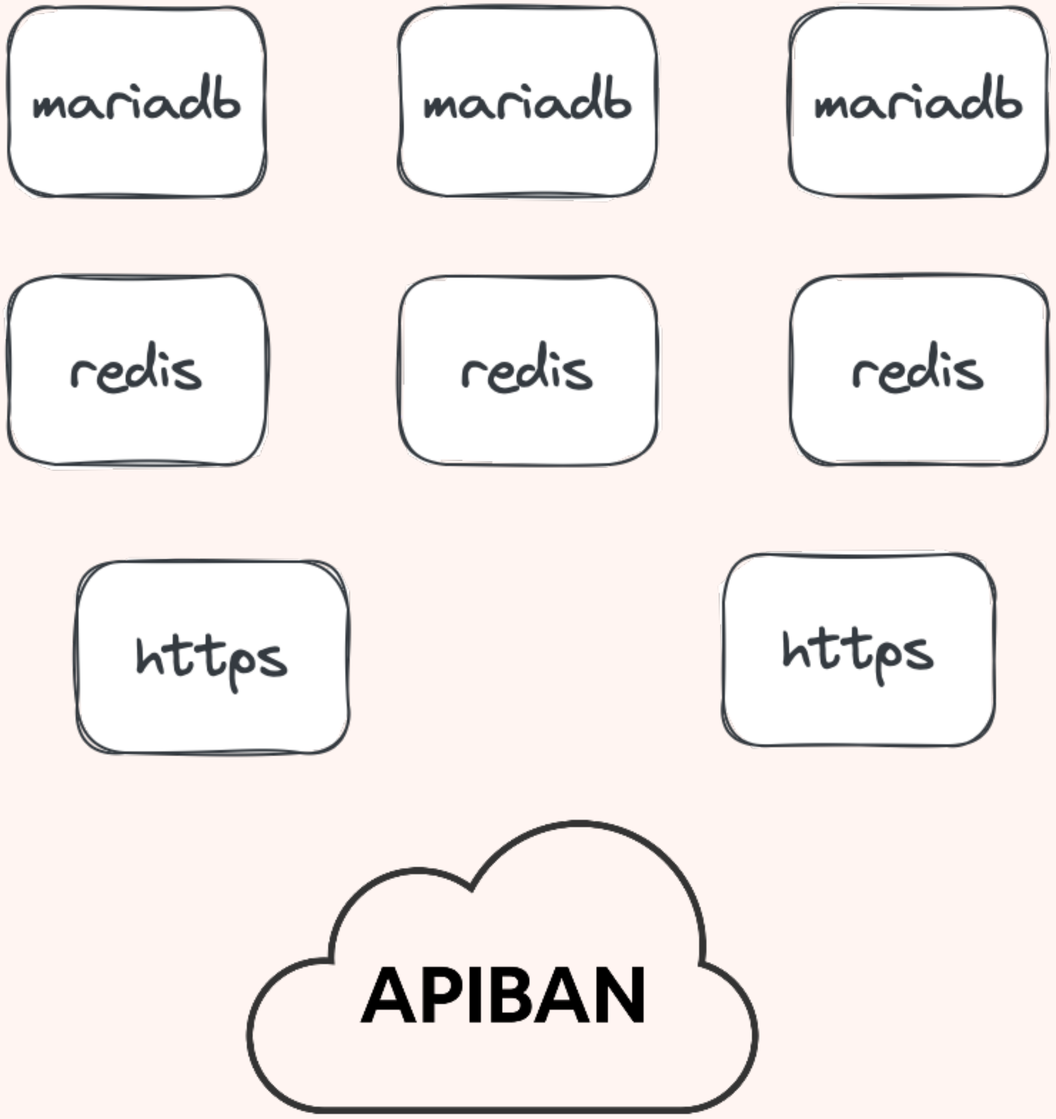
API

- Written in Go
- Banned
  - Returns list of active address in sets of 250
- Check
  - Checks individual addresses



NEW IN 2023

- Improved Architecture / HA
- IPSET now includes
  - Cisco
  - Juniper
- More Honeypots


mariadb
mariadb
mariadb
redis
redis
redis
https
https
APIBAN

FUN FACTS

- **Current most active CIDR:**
  205.210.31.0/24 (Palo Alto)
- **Most active CIDR all time:**
  128.90.0.0/16 (17k) (phmgmt)
- **Avg IP addresses per day:**
  185
- **Honeypot Data:**
  kwancro.com/honeypotdata/
- **Most active country:**
  USA

USING APIBAN WITH KAMAILIO

APIBAN & KAMAILIO

- Store Control ID and IPs in HTABLE
- RTIMER to run periodic checks
- HTTP_CLIENT to get data
- JANSSON to parse data
- MAX_WHILE_LOOPS >= 250

HTABLE / RTIMER

- **MODPARAM:**
```
modparam("htable", "htable", "apiban=>size=11;")
modparam("htable", "htable", "apibanctl=>size=1;initval=0;")
```

- **MODPARAM:**
```
modparam("rtimer", "timer", "name=apiban;interval=300;mode=1;")
modparam("rtimer", "exec", "timer=apiban;route=APIBAN")
```

APIBAN ROUTE

```
route[APIBAN] {
 $var(apikey) = "MYAPIKEY";
 $var(apiget) = "https://apiban.org/api/" + $var(apikey) + "/banned/"
+ $sht(apibanctl=>ID);

 xlog("L_INFO","APIBAN: Sending API request to $var(apiget)\n");
 http_client_query("$var(apiget)", "$var(banned)");
 if($rc!=200) {
  xlog("L_INFO","APIBAN: Non 200 response. $var(banned)\n");
  exit;
 }

 (continued)
```

APIBAN ROUTE (CONT)

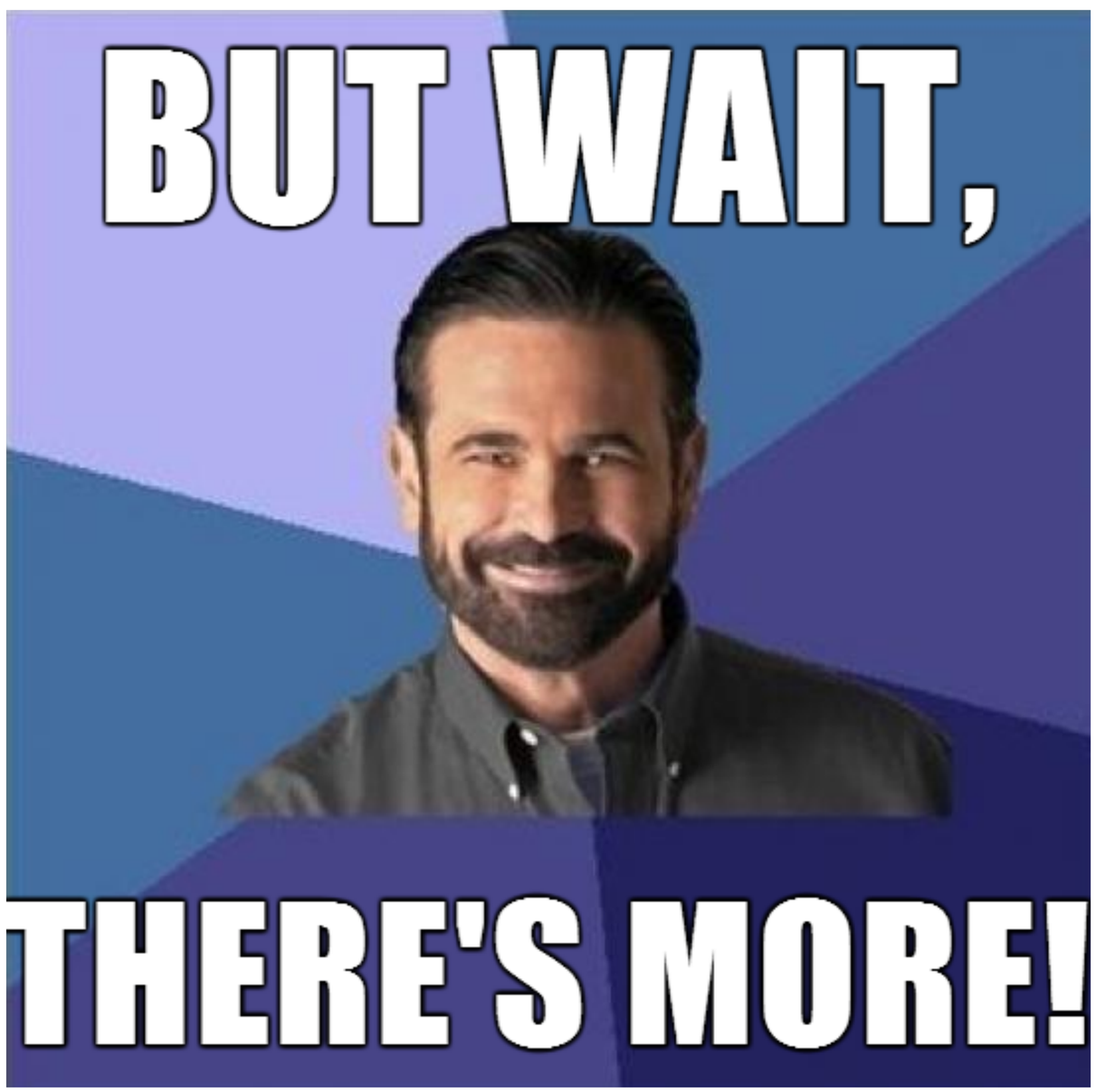
```
 $var(count) = 0;
 jansson_array_size("ipaddress", $var(banned), "$var(size)");
 while($var(count) < $var(size)) {
  jansson_get("ipaddress[$var(count)]", $var(banned),
"$var(blockaddr)");
  $sht(apiban=>$var(blockaddr)) = 1;
  xlog("L_INFO","APIBAN: Adding block ipaddress[$var(count)] ==
$var(blockaddr)\n");
  $var(count) = $var(count) + 1;
 }

 jansson_get("ID", $var(banned), "$var(apiid)");
 xlog("L_INFO","APIBAN: New ID is $var(apiid)\n");
 $sht(apibanctl=>ID) = $var(apiid);
}
```

LOAD HTABLE ON STARTUP

```
event_route[htable:mod-init] {
 # pre load apiban
 route(APIBAN);
}
```

CALL IN REQINIT (OR SIMILAR)

```
if($sht(apiban=>$si)!=$null) {
    // ip is blocked from apiban.org
    xdbg("request from apiban.org blocked IP - $rm from $fu (IP:$si:$sp)\n");
    exit;
}
```


BUT WAIT,
THERE'S MORE!

IPTABLES-API

IPTABLES-API

- Open Source API for adding/removing addresses from IPTABLES (or IP6TABLES)
- IPv4 and IPv6
- Fast, Simple
- Allows adding removing via simple curl
- One liner super lazy install
- https://github.com/palner/iptables-api

EASY INTEGRATION

```
modparam("htable", "htable", "ipban=>size=8;autoexpire=600;")

...

if (!pike_check_req()) {
  xlog("L_ALERT","ALERT: pike blocking $rm from $fu (IP:$si:$sp)\n");
  $sht(ipban=>$si) = 1;
  http_client_query("http://localhost:8082/addip/$si", "$var(apinfo)");
  exit;
}

...

event_route[htable:expired:ipban] {
  xlog("mytable record expired $shtrecord(key) => $shtrecord(value)\n");
  http_client_query("http://localhost:8082/removeip/$shtrecord(key)", "$var(apinfo)");
}
```

WHY?

```
top - 16:17:31 up 23 days, 20:27,  1 user,  load average: 0.35, 0.09, 0.03
Tasks: 161 total,   1 running, 160 sleeping,   0 stopped,   0 zombie
%Cpu(s):  7.4 us,  2.1 sy,  0.0 ni, 88.9 id,  0.0 wa,  0.0 hi,  1.7 si,  0.0 st
MiB Mem :    921.7 total,    252.0 free,    220.1 used,    449.5 buff/cache
MiB Swap:    100.0 total,    100.0 free,      0.0 used.    639.6 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
 6489 kamailio  20   0  842124   6292   4456 S   3.3   0.7   0:00.59 kamailio
 6491 kamailio  20   0  842124   6292   4456 S   3.0   0.7   0:00.58 kamailio
 6485 kamailio  20   0  842124   6292   4456 S   2.6   0.7   0:00.57 kamailio
 6487 kamailio  20   0  842124   6292   4456 S   2.6   0.7   0:00.54 kamailio
 6493 kamailio  20   0  842124   6292   4456 S   2.6   0.7   0:00.57 kamailio
 6495 kamailio  20   0  842124   6292   4456 S   2.6   0.7   0:00.57 kamailio
 6497 kamailio  20   0  842124   6292   4456 S   2.6   0.7   0:00.58 kamailio
 6499 kamailio  20   0  842124   6292   4456 S   2.3   0.7   0:00.56 kamailio
   11 root      20   0       0      0      0 S   1.6   0.0   0:16.11 ksoftirqd/0
 6571 root      20   0   11260   3232   2532 R   1.3   0.3   0:03.11 top
  695 root      20   0  386500  27264  22052 S   0.7   2.9 305:51.15 rtpengine
   12 root      20   0       0      0      0 I   0.3   0.0   4:30.78 rcu_sched
  319 avahi     20   0    7544   3744   2724 S   0.3   0.4  39:26.58 avahi-daemon
 6519 kamailio  20   0  842124   6164   4328 S   0.3   0.7   0:00.19 kamailio
    1 root      20   0   33836   8624   6748 S   0.0   0.9   0:40.51 systemd
    2 root      20   0       0      0      0 S   0.0   0.0   0:02.46 kthreadd
    3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
    4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
    8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
    9 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_rude_
   10 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_trace
   13 root      rt   0       0      0      0 S   0.0   0.0   0:00.61 migration/0
   14 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
   15 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/1
   16 root      rt   0       0      0      0 S   0.0   0.0   0:00.50 migration/1
   17 root      20   0       0      0      0 S   0.0   0.0   0:01.39 ksoftirqd/1
   20 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/2
   21 root      rt   0       0      0      0 S   0.0   0.0   0:00.45 migration/2
   22 root      20   0       0      0      0 S   0.0   0.0   0:05.58 ksoftirqd/2
   25 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/3
   26 root      rt   0       0      0      0 S   0.0   0.0   0:00.39 migration/3
   27 root      20   0       0      0      0 S   0.0   0.0   0:01.27 ksoftirqd/3
```

INVITEs with “exit”
750cps
Raspberry-PI

```
op - 16:18:36 up 23 days, 20:28,  1 user,  load average: 0.40, 0.15, 0.05
asks: 161 total,   1 running, 160 sleeping,   0 stopped,   0 zombie
Cpu(s):  0.1 us,  0.4 sy,  0.0 ni, 99.4 id,  0.0 wa,  0.0 hi,  0.1 si,  0.0 st
iB Mem :    921.7 total,    251.6 free,    220.1 used,    449.9 buff/cache
iB Swap:    100.0 total,    100.0 free,      0.0 used.    639.6 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
 6599 root      20   0   11244   3008   2456 R   1.3   0.3   0:00.35 top
  695 root      20   0  386500  27264  22052 S   0.7   2.9 305:51.67 rtpengine
 6347 root      20   0   14492   7032   6096 S   0.7   0.7   0:00.50 sshd
    1 root      20   0   33836   8624   6748 S   0.0   0.9   0:40.51 systemd
    2 root      20   0       0      0      0 S   0.0   0.0   0:02.46 kthreadd
    3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
    4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
    8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
    9 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_rude_
   10 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_trace
   11 root      20   0       0      0      0 S   0.0   0.0   0:16.54 ksoftirqd/0
   12 root      20   0       0      0      0 I   0.0   0.0   4:30.87 rcu_sched
   13 root      rt   0       0      0      0 S   0.0   0.0   0:00.61 migration/0
   14 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
   15 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/1
   16 root      rt   0       0      0      0 S   0.0   0.0   0:00.50 migration/1
   17 root      20   0       0      0      0 S   0.0   0.0   0:01.39 ksoftirqd/1
   20 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/2
   21 root      rt   0       0      0      0 S   0.0   0.0   0:00.45 migration/2
   22 root      20   0       0      0      0 S   0.0   0.0   0:05.58 ksoftirqd/2
   25 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/3
   26 root      rt   0       0      0      0 S   0.0   0.0   0:00.39 migration/3
   27 root      20   0       0      0      0 S   0.0   0.0   0:01.27 ksoftirqd/3
   30 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kdevtmpfs
   31 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
   35 root      20   0       0      0      0 S   0.0   0.0   0:00.00 kauditd
   37 root      20   0       0      0      0 S   0.0   0.0   0:01.53 khungtaskd
   38 root      20   0       0      0      0 S   0.0   0.0   0:00.00 oom_reaper
```

INVITEs with “exit”
****Blocked in IPTABLES**
750cps
Raspberry-PI

EXAMPLE BLOCK IP

```
route[BLOCKIP] {
 if ((src_ip!=myself) && (!dmq_is_from_node()) && (!
ds_is_from_list())) {
  xlog("L_INFO","[R-BLOCKIP] blocking $rm from $fu (IP:$si:$sp)\n");
  $sht(ipban=>$si) = 1;
  $var(apiget) = "http://localhost:8082/blockip/" + $si;
  http_client_query("$var(apiget)", "$var(block)");
  xlog("L_INFO","[R-BLOCKIP] edgeapi: $var(block) \n");
 } else {
  xlog("L_INFO","[R-BLOCKIP] NOT BLOCKING $rm (IP:$si:$sp)\n");
 }

 return;
}
```

BLOCKING

```
route[REQINIT] {
    if ($sht(ipban=>$si)!=$null) {
        xdbg("request from blocked IP - $rm from $fu (IP:$si:$sp)");
        exit;
    }
    if ($sht(apiban=>$si)!=$null) {
        xdbg("request from apiban.org blocked IP - $rm from $fu (IP:$si:$sp)");
        route(BLOCKIP);
        exit;
    }
    if (src_ip!=myself) {
        if (!pike_check_req()) {
            xlog("L_ALERT","ALERT: pike blocking $rm from $fu (IP:$si:$sp)");
            route(BLOCKIP);
            exit;
        }
    }
    if ($ua =~ "friendly-scanner|sipcli|VaxSIPUserAgent") {
        xlog("L_INFO","[R-REQINIT] script kiddies from IP:$si:$sp - dropping and blocking");
        route(BLOCKIP);
        exit;
    }
...
```

STARTUP / CLEANUP

```
#-- run when ipban htable value expires
event_route[htable:expired:ipban] {
  xlog("L_INFO","[htable:expired:ipban] record expired $shtrecord(key);
  http_client_query("http://localhost:8082/removeip/$shtrecord(key)",
"$var(apinfo)");
}

#-- run at startup
event_route[htable:mod-init] {
  #-- pre load apiban
  xlog("L_INFO","[R-htable:mod-init] load apiban");
  route(APIBAN);

  #-- flush apibanlocal
  xlog("L_INFO","[R-htable:mod-init] flush apibanlocal");
  http_client_query("http://localhost:8082/flushchain", "$var(apinfo)");
...
```

DON’T FORGET BAD SIP

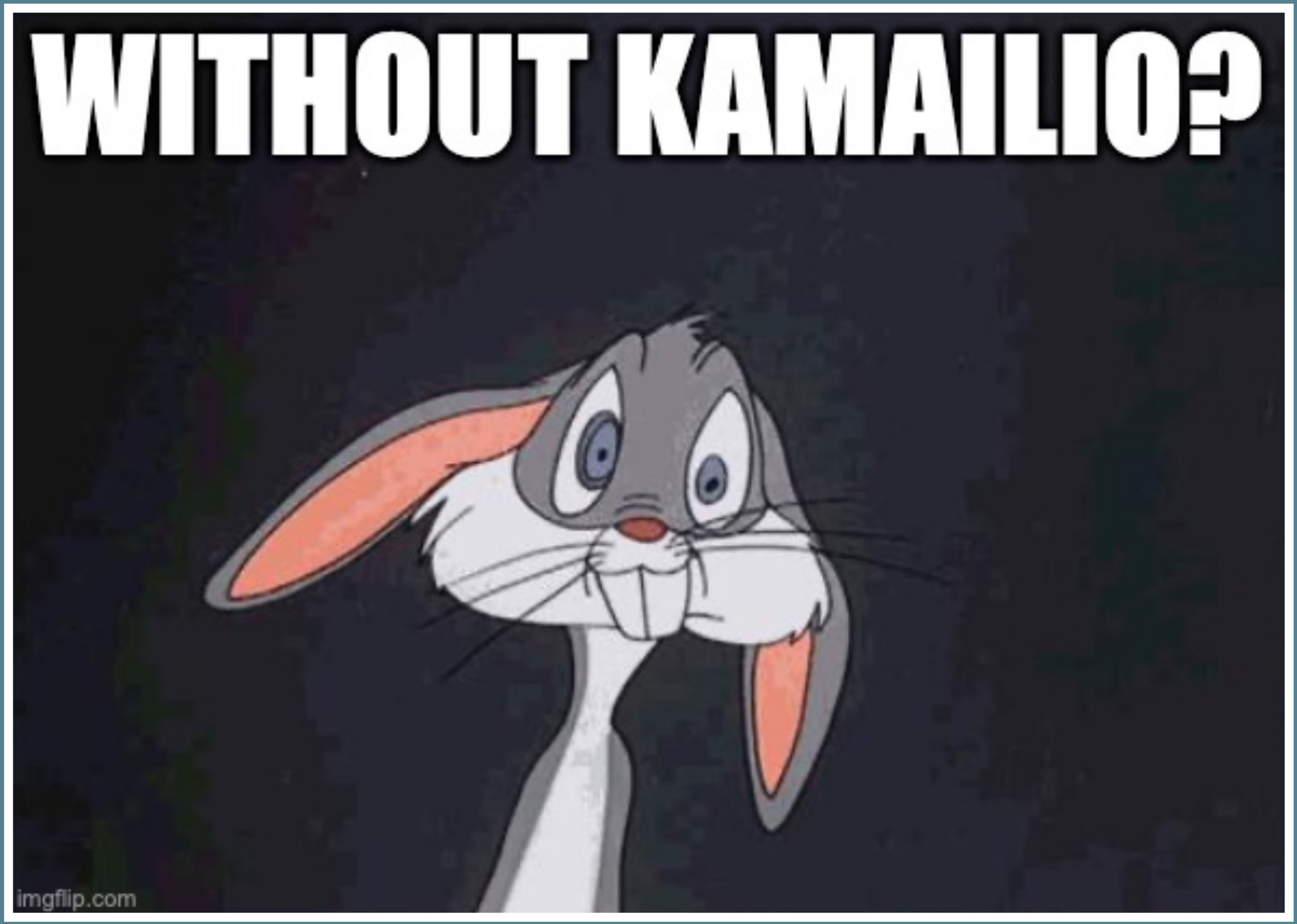
BAD SIP

```
#-- sip parse errors
event_route[core:receive-parse-error] {
 xlog("L_ALERT", "[CORE:parse]: got a parsing error from $si:$sp,
message $mb");
 route(BLOCKIP);
 exit;
}
```

KAMAILIO

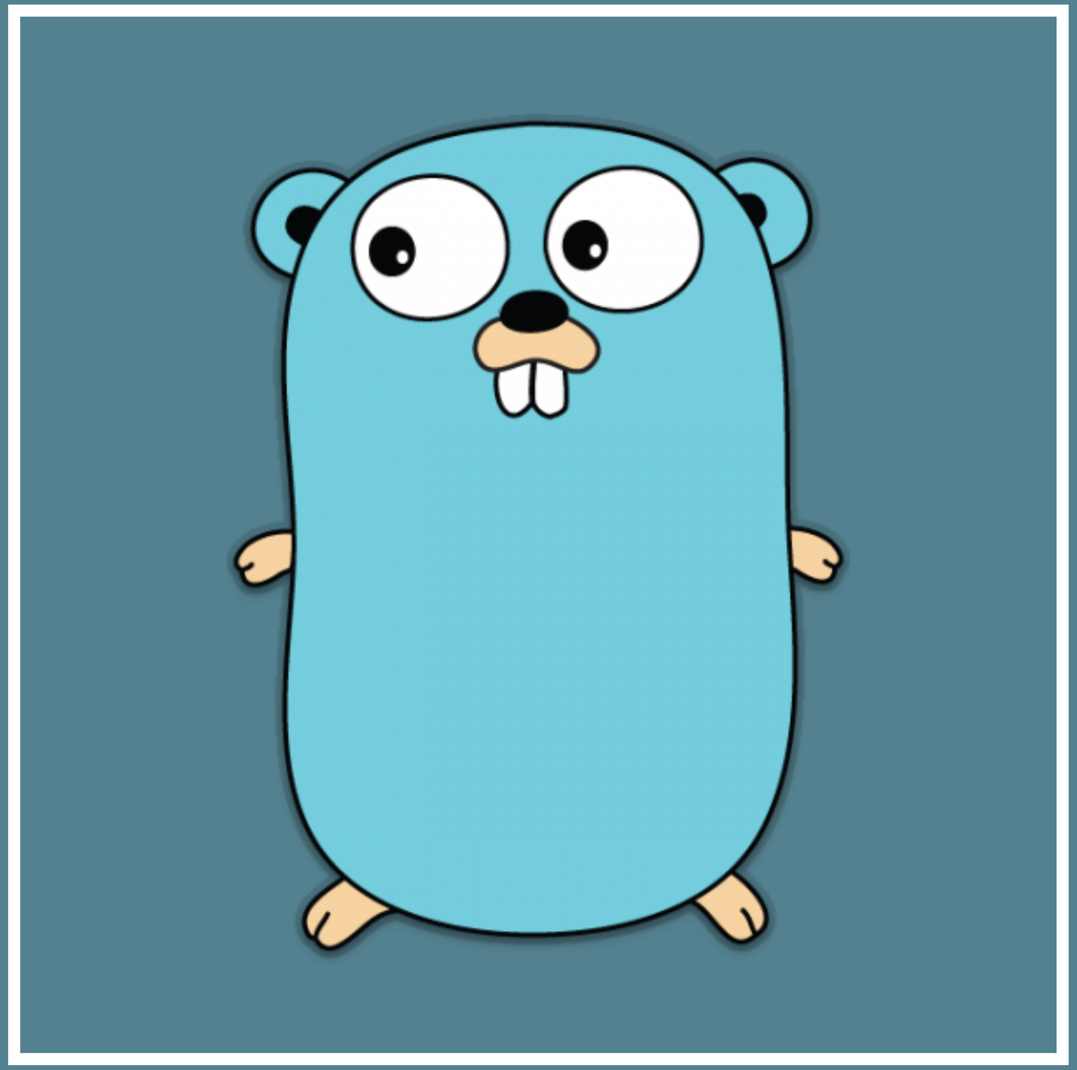
- Block with IPTABLES
- Catch Parse Errors
- Use DMQ to share APIBAN / IPBAN data
- Clean / Flush on expire/restart
- KAMCLI

USING APIBAN WITHOUT KAMAILIO


WITHOUT KAMAILIO?
imgflip.com

GO CLIENT

- Open Source
- Easy, Simple Install
- Auto-Flush
- Works on Linux
- https://github.com/palner/apiban



API BASED...

- IPSET
  - OpnSense, PFSense, Cisco, Juniper
- CHECK
  - Individual IP checks, KAMCLI
- Examples on Github
  - Including Homer, SIP3, OpenSIPS
- https://github.com/palner/apiban

Thank You!

QUESTIONS?