annoy fraudsters using hash tables

Sebastian Damm

E: damm@sipgate.de

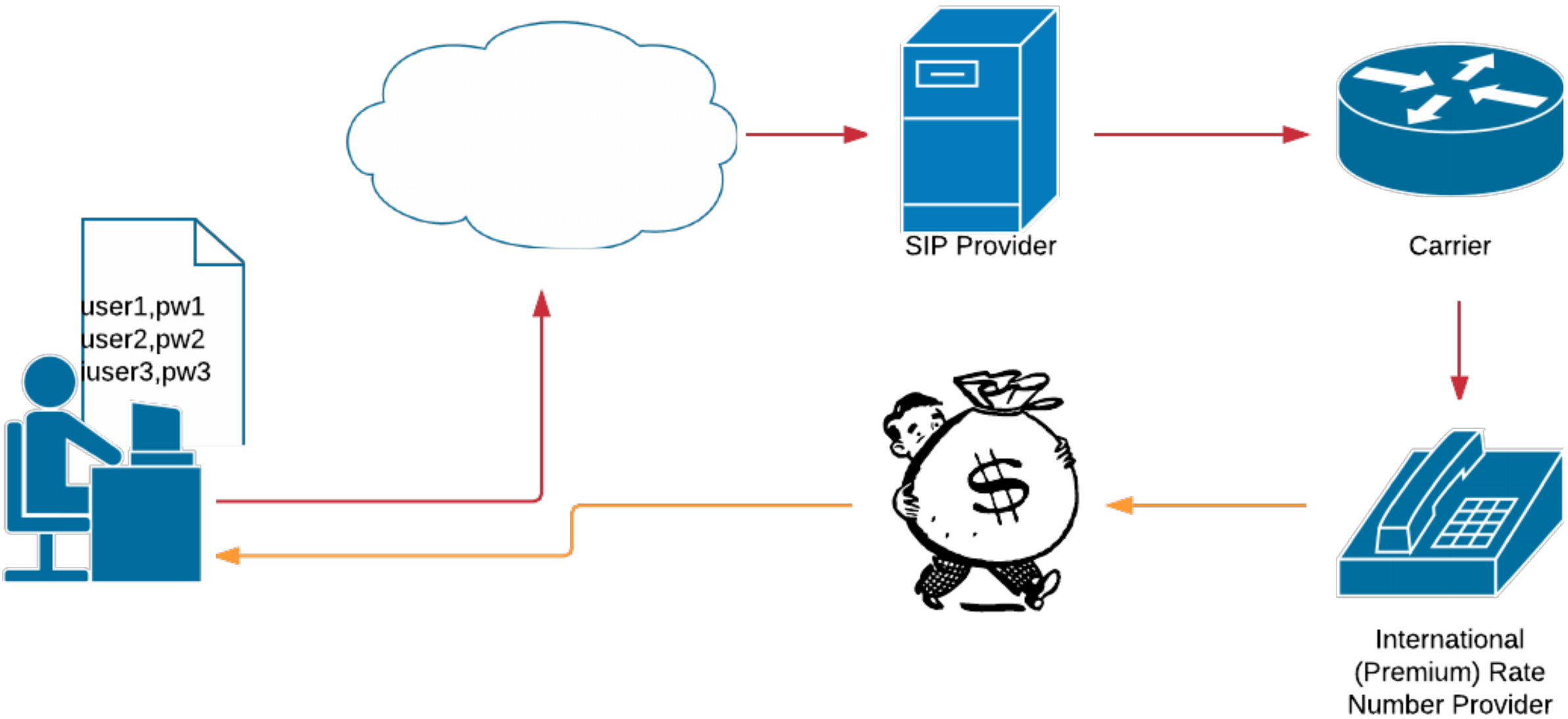
T: @_SebastianDamm

Who we are, what we do

- Düsseldorf based VoIP provider (since 2004)
- Active in Germany and UK
- Full MVNO in the Telefónica network
- Private and Business customers
- VoIP and Mobile products
- Some 100k active customers
- More than 100 million minutes each month

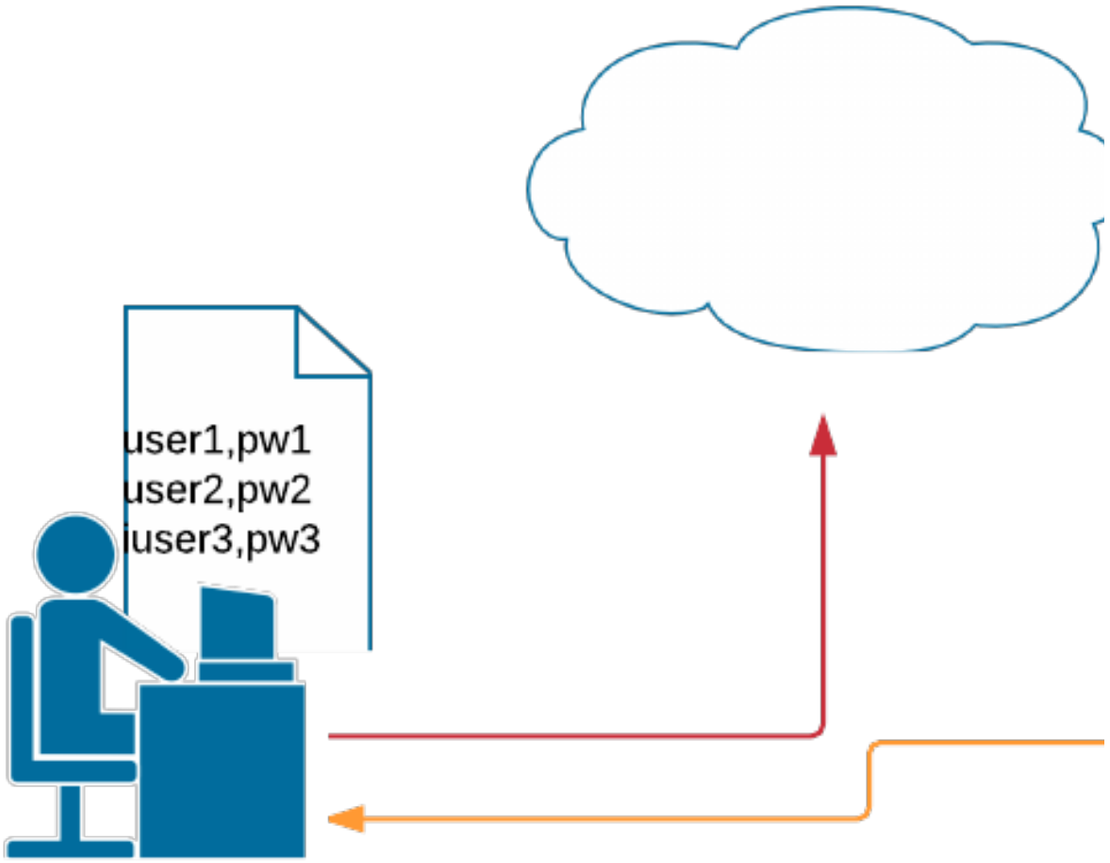
IRSF

International Revenue Share Fraud



IRSF

International Revenue Share Fraud



FIND OPEN ROUTES AND CHOOSE YOUR BEST SOLUTION

Search: GET RATE LIST

	Solution	Payout
	Russia	€ 0.1
	Russia	€ 0.045
	Sao Tome	$ 0.24
	Sao Tome	$ 0.24
	Senegal	$ 0.08
	Senegal A	$ 0.12
	Seychelles	$ 0.18
	Somalia A	€ 0.16
	Spain Mobile	€ 0.018
	St. Lucia	$ 0.04
	Tanzania	$ 0.09
	Tanzania	$ 0.09
	Togo	€ 0.22
	Tunisia	$ 0.1
INFO	Solution	Payout

Somalia A 252800 flat, Term: 40 days EOM, Test number: 252800000750

Showing 307 to 320 of 320 entries

Previous 1 ... 15 16 17 18 19 Next

INTERPREMIUM
Our revenue is your profit NET

Special Promotions

France 336400 – EUR 0.07/min
WEEKLY
test number: +33640002090

Bosnia 38764 – EUR 0.11/min
WEEKLY
test number: +387644118600

Bosnia 38765 – EUR 0.11/min
WEEKLY
test number: +38765045680

UK 4478933 - EUR 0.04/min
WEEKLY
test number: +447893313200

UK 4487018 - EUR 0.05/min
45 days EOM
test number: +448701863650

UK 4487049 – EUR 0.05/min
45 days EOM
test number: +448704944900

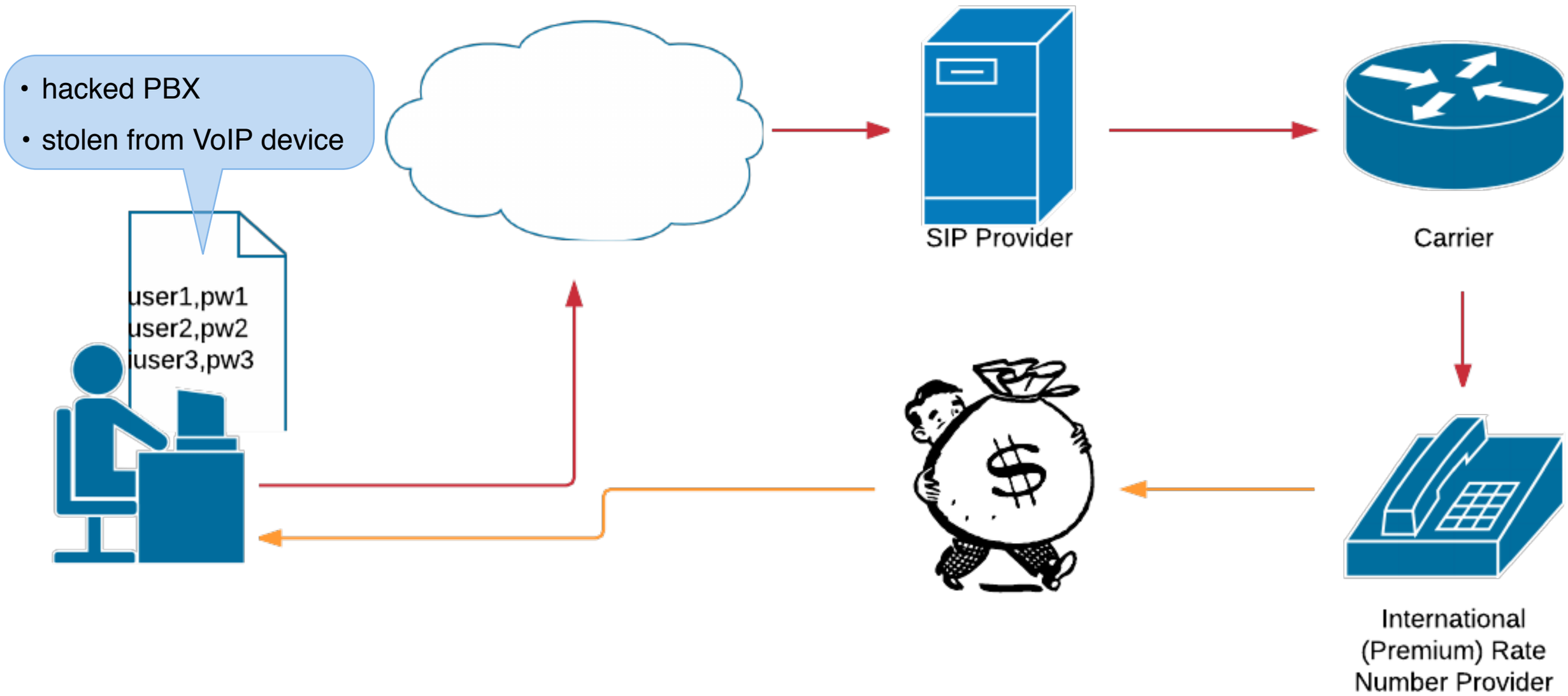
UK 4487134 – EUR 0.05/min
45 days EOM
test number: +448713460120

UK 4487145 - EUR 0.05/min
45 days EOM
test number: +448714531520

sipgate

IRSF

International Revenue Share Fraud



IRSF

International Revenue Share Fraud

IRSF

Customer satisfaction

- high costs
- argue about the cause
- maybe even lose the customer
- VoIP is insecure!

Kamailio modules

- pike
- ratelimit/pipelimit
- permissions
- geoip
- userblacklist
- dialog

Prevent IRSF

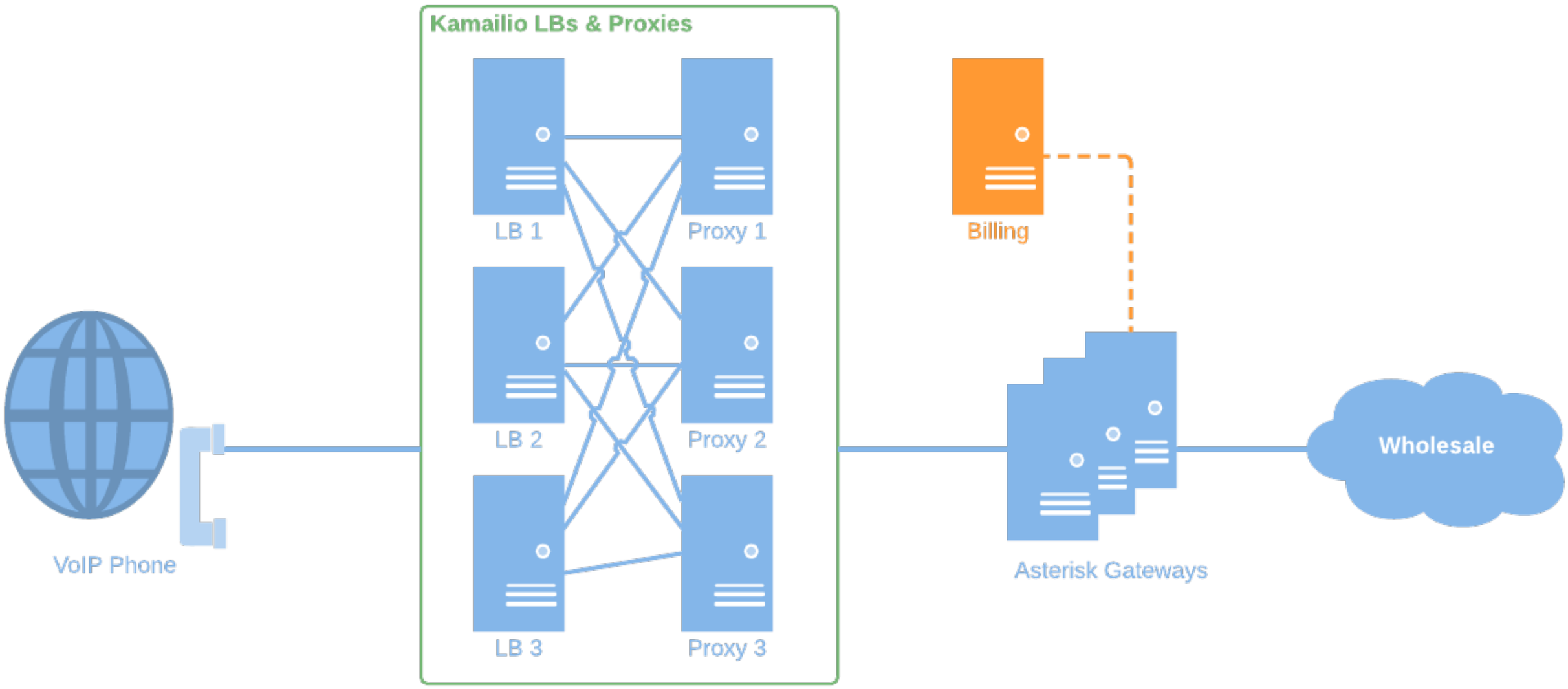
- Detect abused accounts
- Block the IP address temporarily

Prevent IRSF

- Detect abused accounts
- Block the IP address temporarily

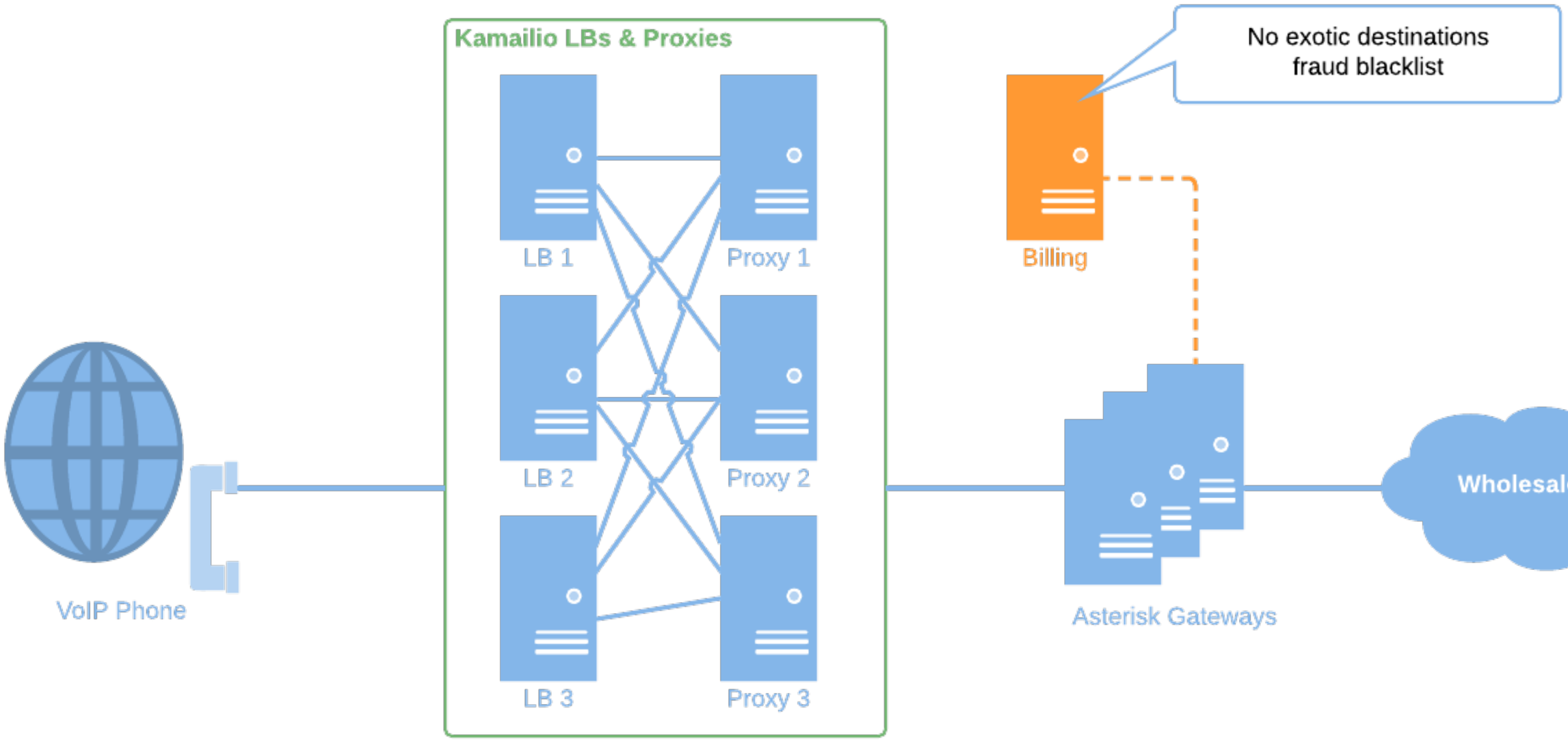
Kamailio Fail2Ban

Detecting international revenue share fraud



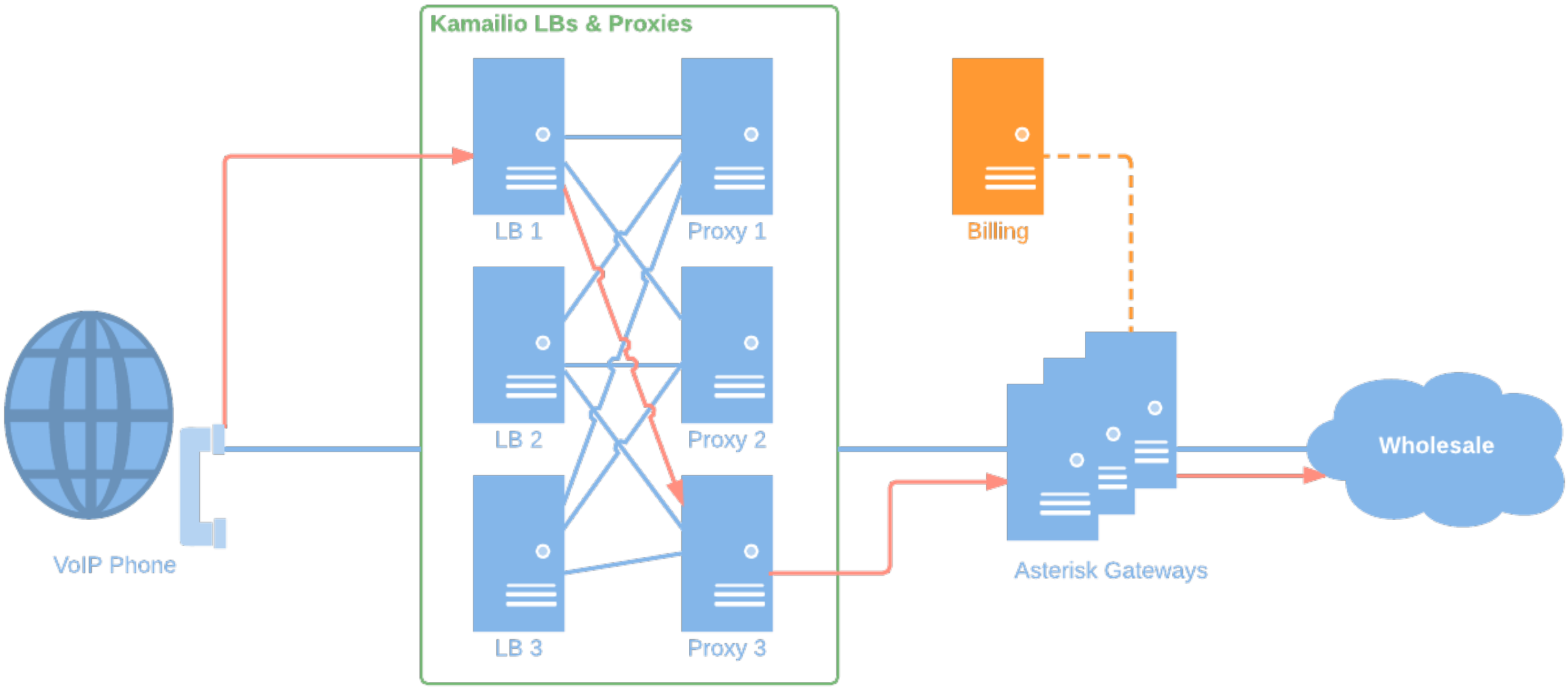
Kamailio Fail2Ban

Detecting international revenue share fraud



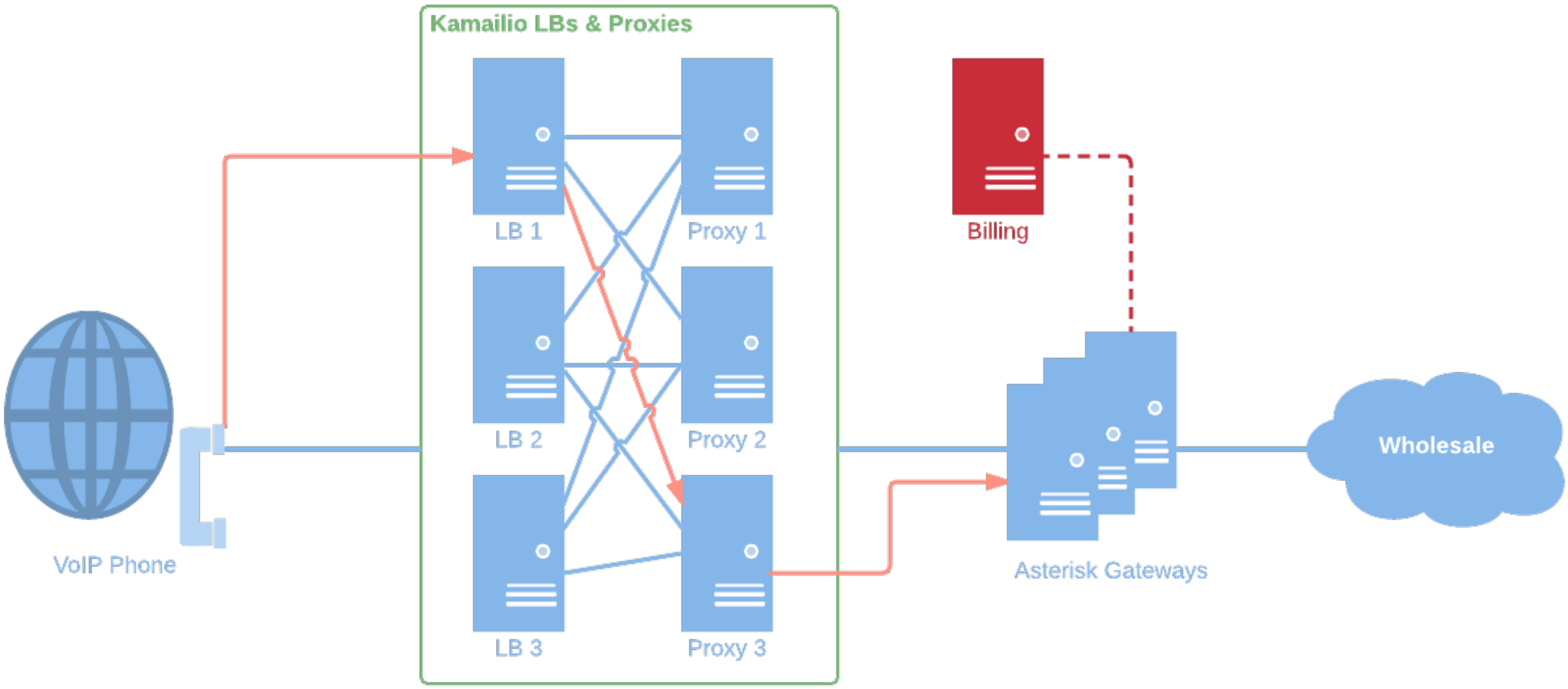
Kamailio Fail2Ban

Detecting international revenue share fraud



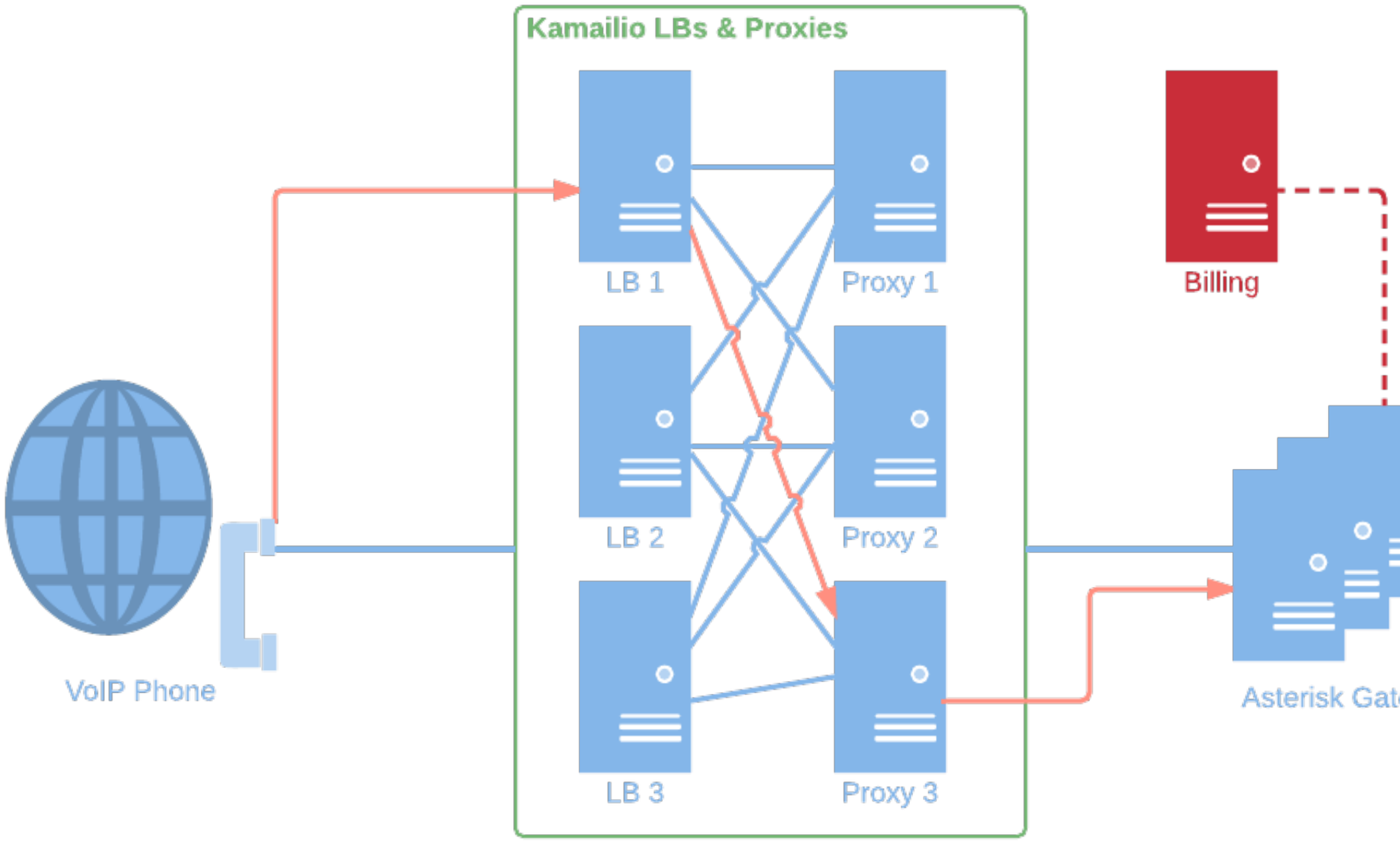
Kamailio Fail2Ban

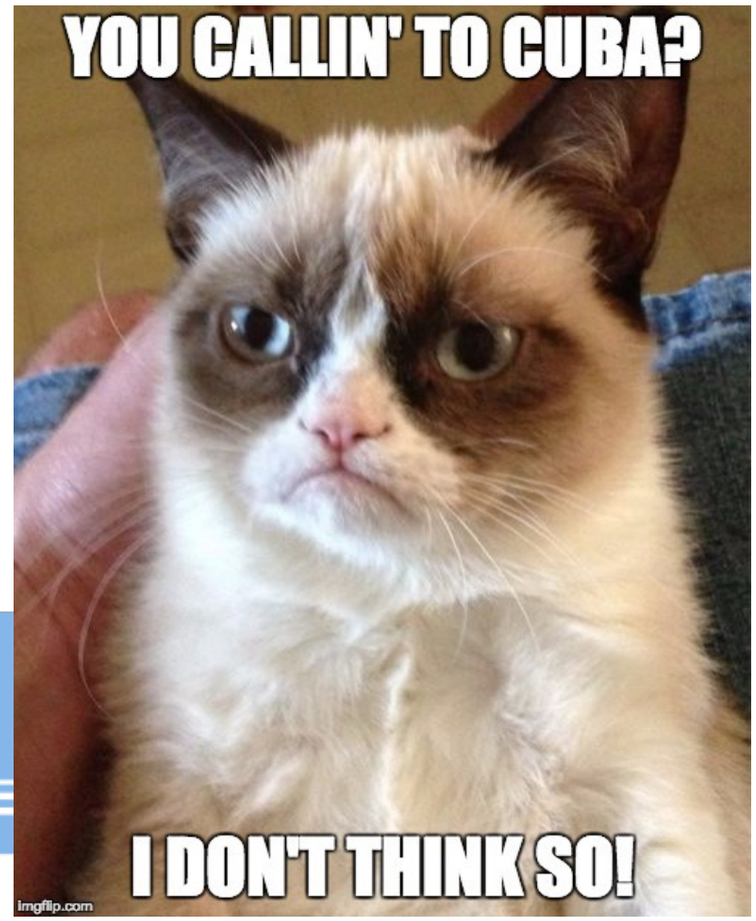
Detecting international revenue share fraud



Kamailio Fail2Ban

Detecting international revenue share fraud



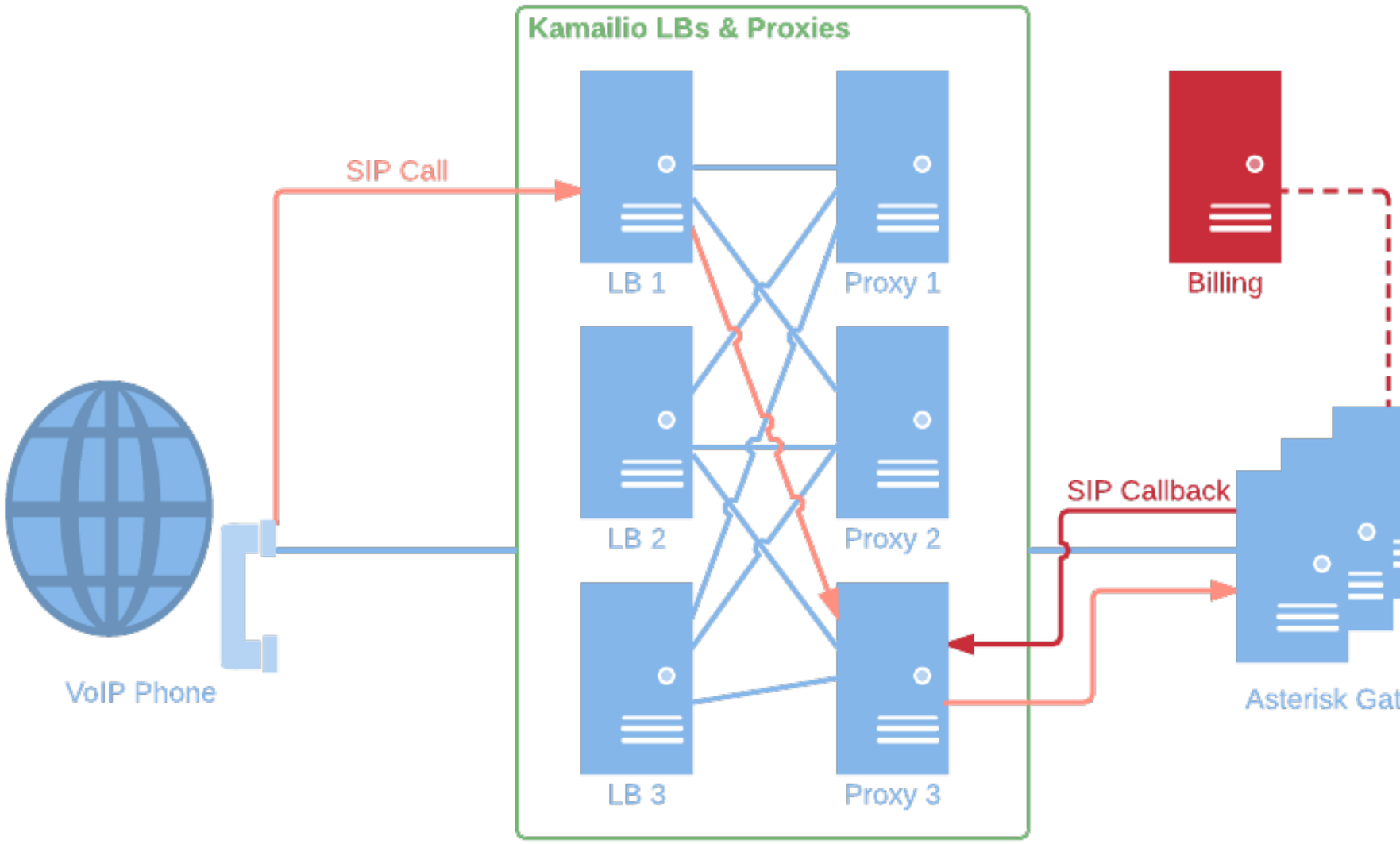


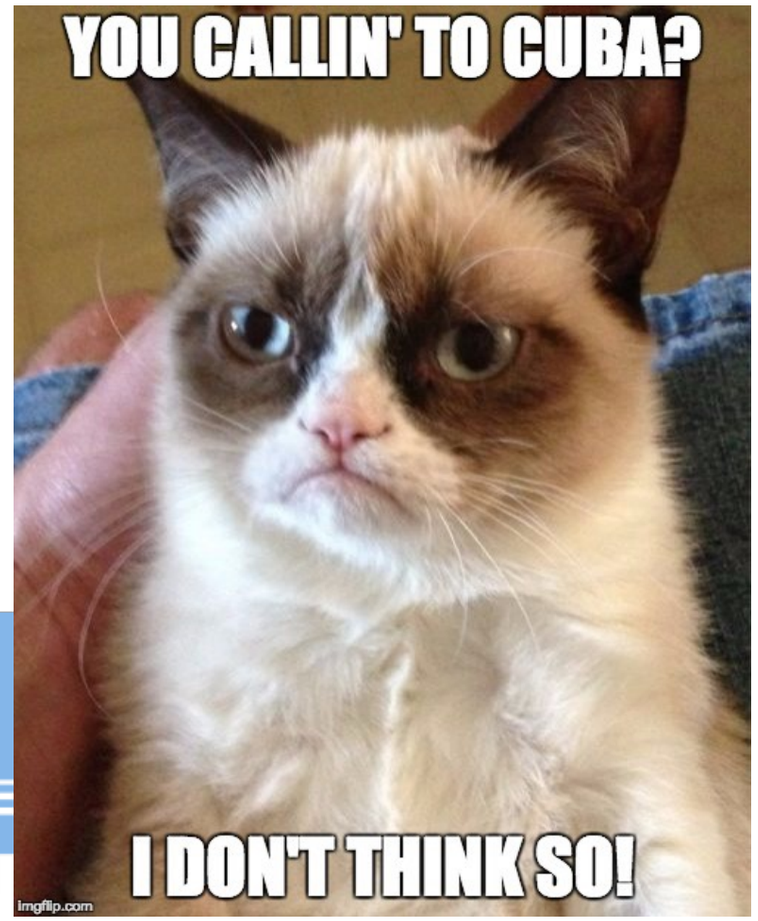
Kamailio Fail2Ban

Detecting international revenue share fraud

Kamailio Fail2Ban

Detecting international revenue share fraud





Kamailio Fail2Ban

Detecting international revenue share fraud

```
#!/usr/bin/perl

$gateway_ip = $AGI->get_variable("CHANNEL(peerip)");
```

Kamailio Fail2Ban

Detecting international revenue share fraud

```
#!/usr/bin/perl

$gateway_ip = $AGI->get_variable("CHANNEL(peerip)");

$sock = IO::Socket::INET->new(
   PeerAddr => $gateway_ip,
   PeerPort => 5060,
   Proto    => 'udp') or die('Could not open socket connection: '.$!);
};
```

Kamailio Fail2Ban

Detecting international revenue share fraud

```
#!/usr/bin/perl

$gateway_ip = $AGI->get_variable("CHANNEL(peerip)");

$sock = IO::Socket::INET->new(
   PeerAddr => $gateway_ip,
   PeerPort => 5060,
   Proto    => 'udp') or die('Could not open socket connection: '.$!);
};

print $sock "SIPGATE sip:BLACKLIST\@sipgate.de SIP/2.0\n".
   "From: $sipid <sip:$sipid\@$source_ip>;tag=".(int rand(1000000000))."\n".
   "To: beggar_notify <sip:$destination\@sipgate.de>\n".
   "Via: SIP/2.0/UDP 127.0.0.1:5060;branch=z9hG4bK".(int rand(1000000000))."\n".
   "Call-ID: ".(int rand(1000000000))."\n".
   "Cseq: 1 SIPGATE\n".
   "X-SIPUSERAGENT: $useragent\n".
   "Content-length: 0\n".
   "\n";

$sock->close;
```

Kamailio Fail2Ban

Detecting international revenue share fraud

```
modparam("htable", "htable", "evilCalls=>size=14;autoexpire=1800;")
modparam("htable", "htable", "blacklistedIPs=>size=7;autoexpire=7200;")
```

Kamailio Fail2Ban

Detecting international revenue share fraud

```
modparam("htable", "htable", "evilCalls=>size=14;autoexpire=1800;")
modparam("htable", "htable", "blacklistedIPs=>size=7;autoexpire=7200;")

route{
..
   if (method == "SIPGATE") {
      if ($rU == "BLACKLIST") {
         $vn(bl_src_ip) = $fd;
         $vn(bl_status) = $rU;
         route(registerEvilCalls);
      }
      exit;
   }
..
```

Kamailio Fail2Ban

Detecting international revenue share fraud

```
modparam("htable", "htable", "evilCalls=>size=14;autoexpire=1800;")
modparam("htable", "htable", "blacklistedIPs=>size=7;autoexpire=7200;")

route{
..
   if (method == "SIPGATE") {
      if ($rU == "BLACKLIST") {
         $vn(bl_src_ip) = $fd;
         $vn(bl_status) = $rU;
         route(registerEvilCalls);
      }
      exit;
   }
..
   if (is_method("INVITE")) {
      if (defined $sht(blacklistedIPs=>$var(src_ip))) {
         sl_send_reply("403", "Call prohibited"); exit;
      }
   }
..
}
```

Kamailio Fail2Ban

Detecting international revenue share fraud

```
modparam("htable", "htable", "evilCalls=>size=14;autoexpire=1800;")
modparam("htable", "htable", "blacklistedIPs=>size=7;autoexpire=7200;")

route[registerEvilCalls] {

   $vn(uniqcid) = $ci + $Ts + $ft;
   $vn(tkey) = $vn(bl_src_ip) + '-' + $(var(uniqcid){s.md5}{s.substr,0,10});
   $sht(evilCalls=>$(var(tkey))) = 1;
   $vn(uniqcid) = $null;
   $vn(tkey) = $null;
```

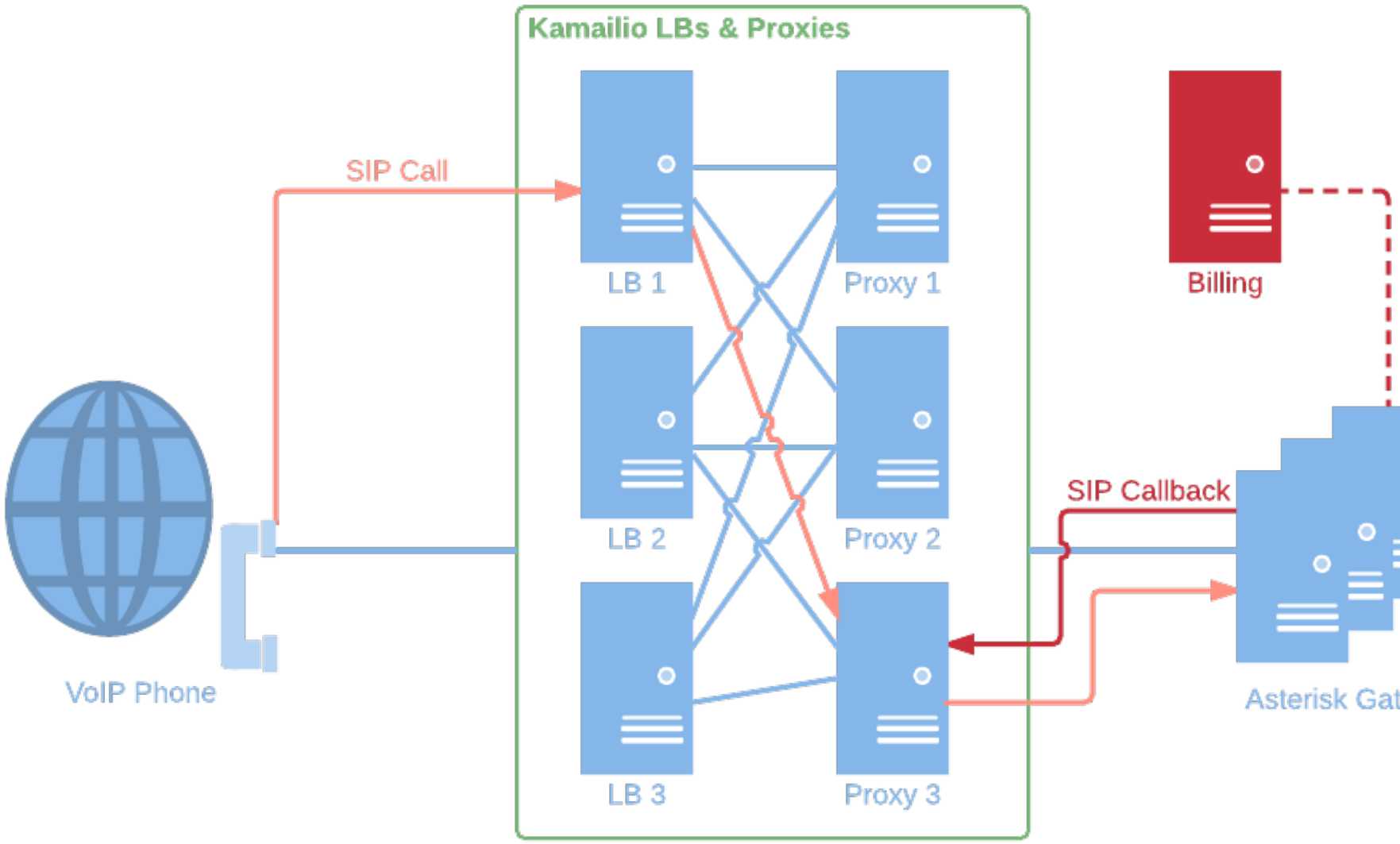
Kamailio Fail2Ban

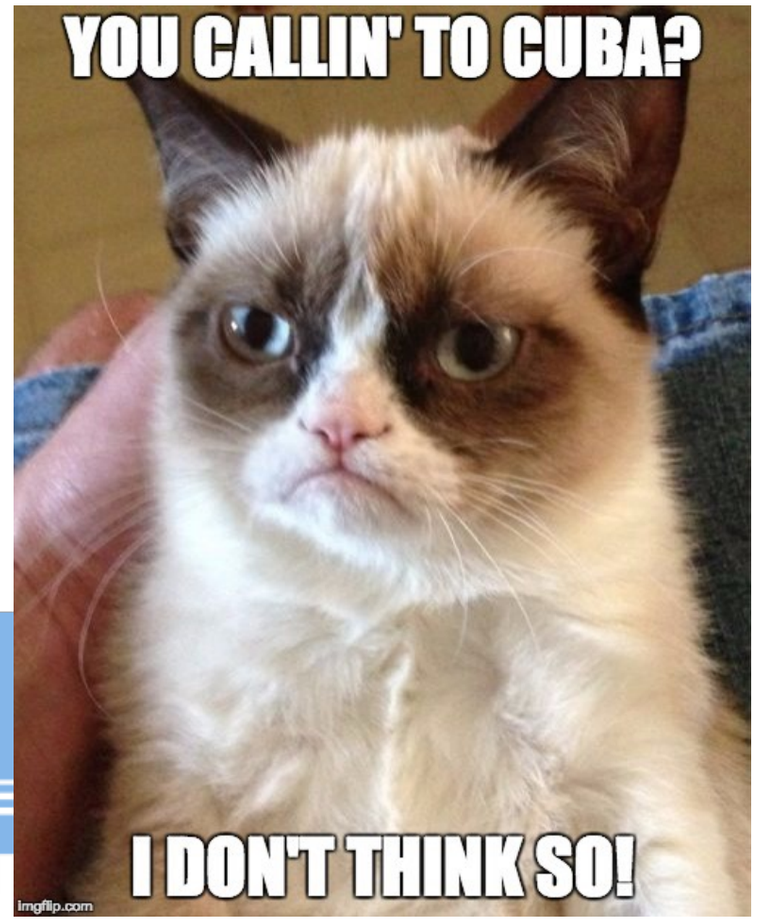
Detecting international revenue share fraud

```
modparam("htable", "htable", "evilCalls=>size=14;autoexpire=1800;")
modparam("htable", "htable", "blacklistedIPs=>size=7;autoexpire=7200;")

route[registerEvilCalls] {

    $vn(uniqcid) = $ci + $Ts + $ft;
    $vn(tkey) = $vn(bl_src_ip) + '-' + $(var(uniqcid){s.md5}{s.substr,0,10});
    $sht(evilCalls=>$(var(tkey))) = 1;
    $vn(uniqcid) = $null;
    $vn(tkey) = $null;

    # Count Entries and block the user if needed
    $var(blcount) = $shtcn(evilCalls=>%~$vn(bl_src_ip));
    if ($var(blcount) > 19) {
        $sht(blacklistedIPs=>$vn(bl_src_ip)) = 1;
    }
}
```

Kamailio Fail2Ban

Detecting international revenue share fraud





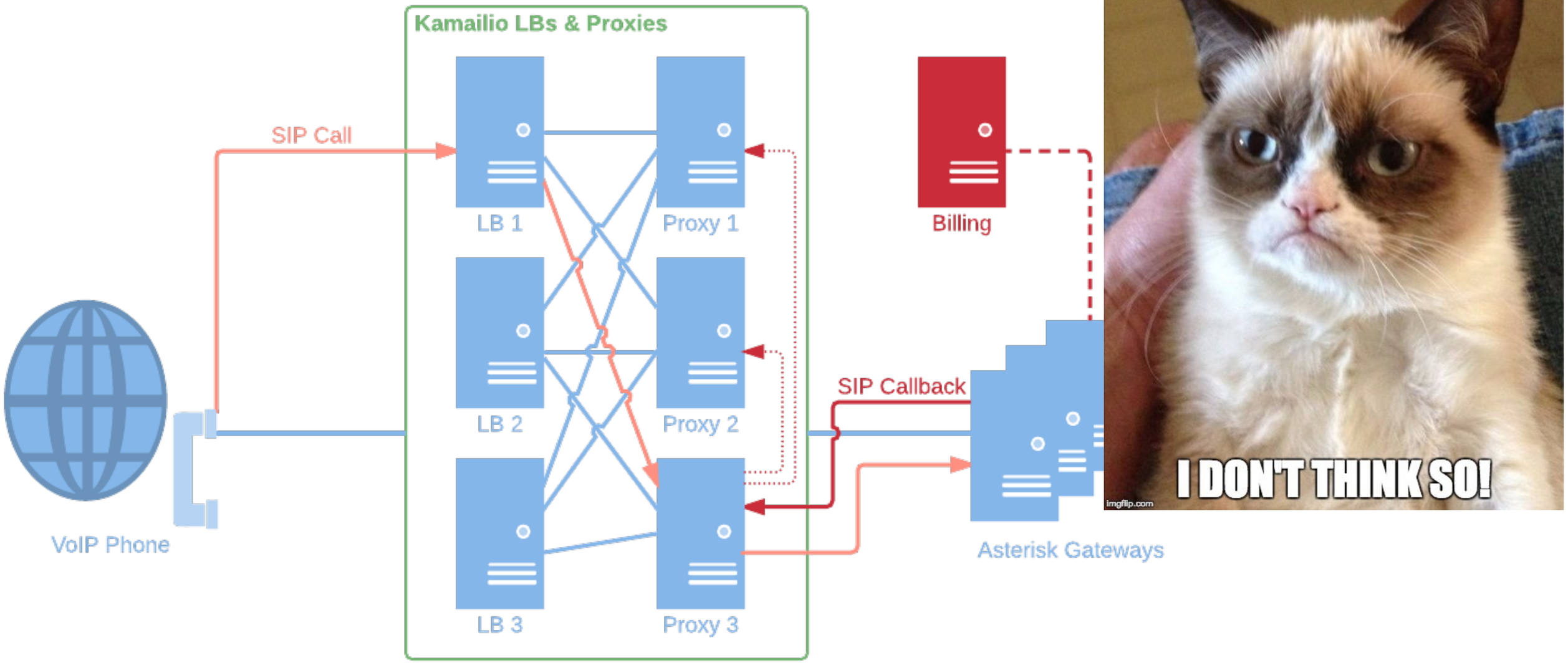
Kamailio Fail2Ban

Detecting international revenue share fraud

```
modparam("htable", "enable_dmq", 1)
modparam("htable", "htable", "evilCalls=>size=14;autoexpire=1800;dmqreplicate=1;")
modparam("htable", "htable",
                        "blacklistedIPs=>size=7;autoexpire=7200;dmqreplicate=1;")

route[registerEvilCalls] {

   $var(uniqcid) = $ci + $Ts + $ft;
   $var(tkey) = $vn(bl_src_ip) + '-' + $(var(uniqcid){s.md5}{s.substr,0,10});
   $sht(evilCalls=>$(var(tkey))) = 1;
   $var(uniqcid) = $null;
   $var(tkey) = $null;

   # Count Entries and block the user if needed
   $var(blcount) = $shtcn(evilCalls=>%~$vn(bl_src_ip));
   if ($var(blcount) > 19) {
      $sht(blacklistedIPs=>$vn(bl_src_ip)) = 1;
   }
}
```

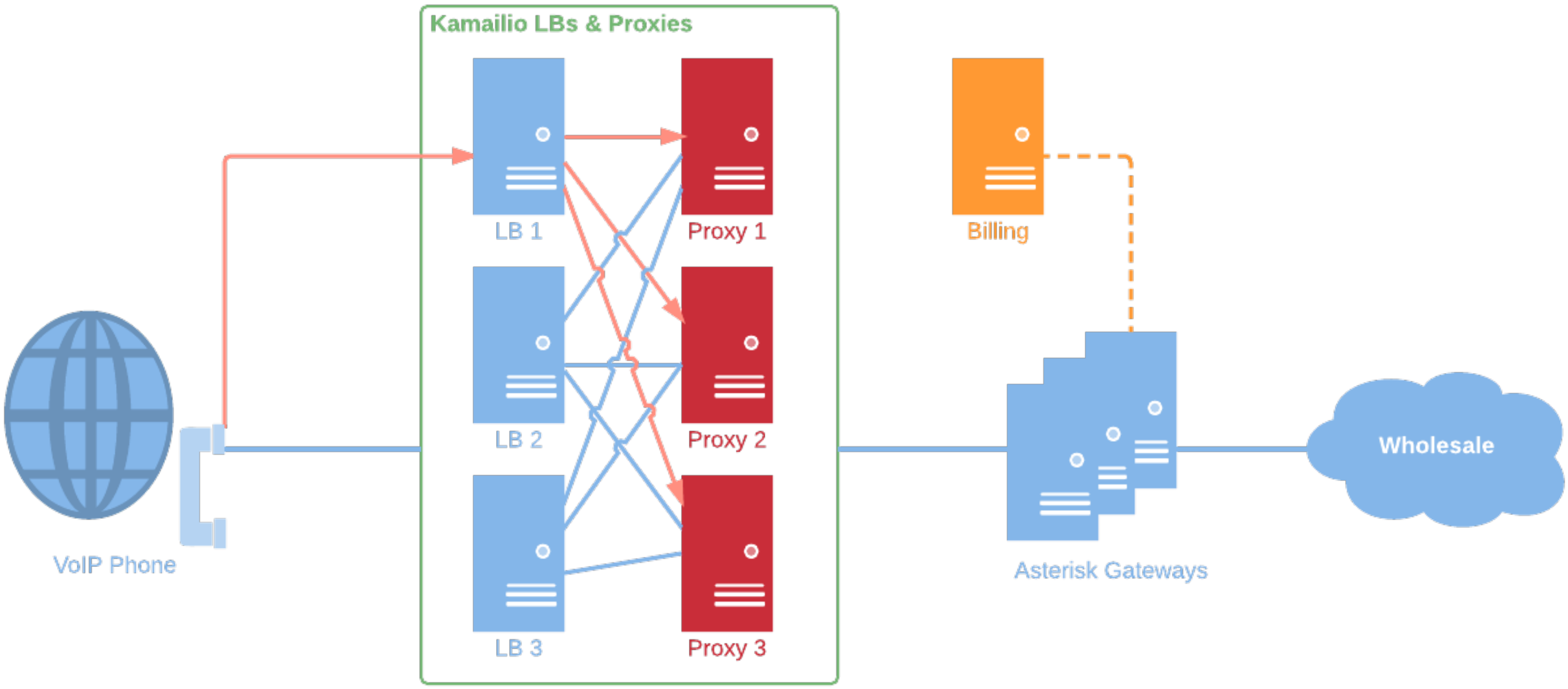
Kamailio Fail2Ban

Detecting international revenue share fraud



Kamailio Fail2Ban

Detecting international revenue share fraud



Kamailio Fail2Ban

Detecting stolen accounts

```
modparam("htable", "htable", "evilUAs=>size=14;autoexpire=1200;")
modparam("htable", "htable", "blacklistedIPs=>size=7;autoexpire=7200;")
```

Kamailio Fail2Ban

Detecting stolen accounts

```
modparam("htable", "htable", "evilUAs=>size=14;autoexpire=1200;")
modparam("htable", "htable", "blacklistedIPs=>size=7;autoexpire=7200;")

route[registerBadClients] {
   if (!allow_trusted("$var(src_ip)", "any")) {
      if (defined $ua && $(ua{s.len}) > 0 && $ua =~ "ua1|ua2") {
         $vn(tkey) = $var(src_ip) + '-' + $au;
         $vn(tval) = $(ua{s.md5});
         $sht(evilUAs=>$var(tkey)) = $var(tval);
         $vn(tkey) = $null;
         $vn(tval) = $null;
```

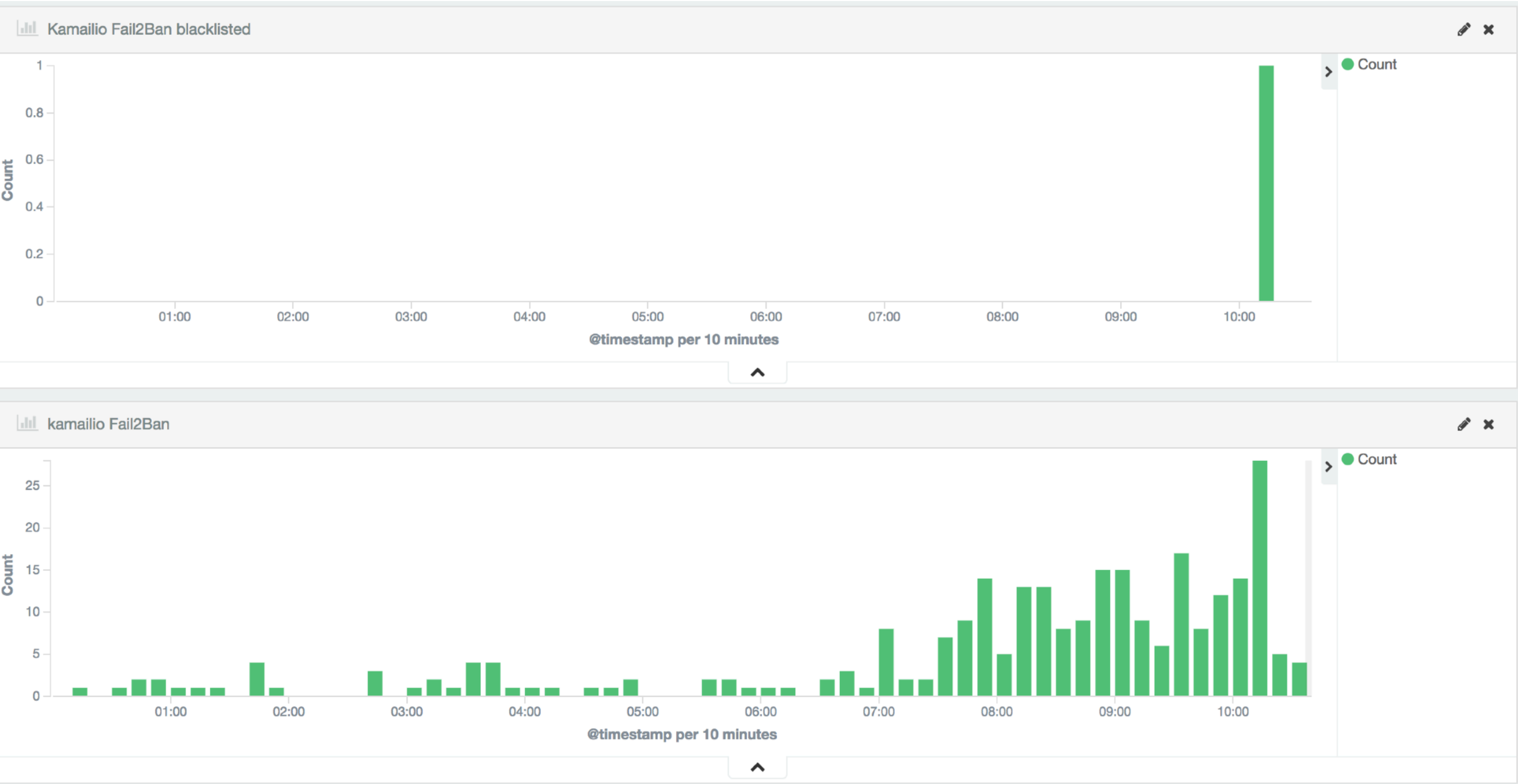
Kamailio Fail2Ban

Detecting stolen accounts

```
modparam("htable", "htable", "evilUAs=>size=14;autoexpire=1200;")
modparam("htable", "htable", "blacklistedIPs=>size=7;autoexpire=7200;")

route[registerBadClients] {
   if (!allow_trusted("$var(src_ip)", "any")) {
      if (defined $ua && $(ua{s.len}) > 0 && $ua =~ "ua1|ua2") {
         $vn(tkey) = $var(src_ip) + '-' + $au;
         $vn(tval) = $(ua{s.md5});
         $sht(evilUAs=>$var(tkey)) = $var(tval);
         $vn(tkey) = $null;
         $vn(tval) = $null;

         # Count Entries and block the IP if needed (5 different users)
         $var(blcount) = $shtcn(evilUAs=>%~$var(src_ip));
         if ($var(blcount) > 4) {
            if (!defined $sht(blacklistedIPs=>$var(src_ip)))
               $sht(blacklistedIPs=>$var(src_ip)) = 1;
         }
      }
   }
}
```

Kamailio Fail2Ban

Does it work?



sipgate

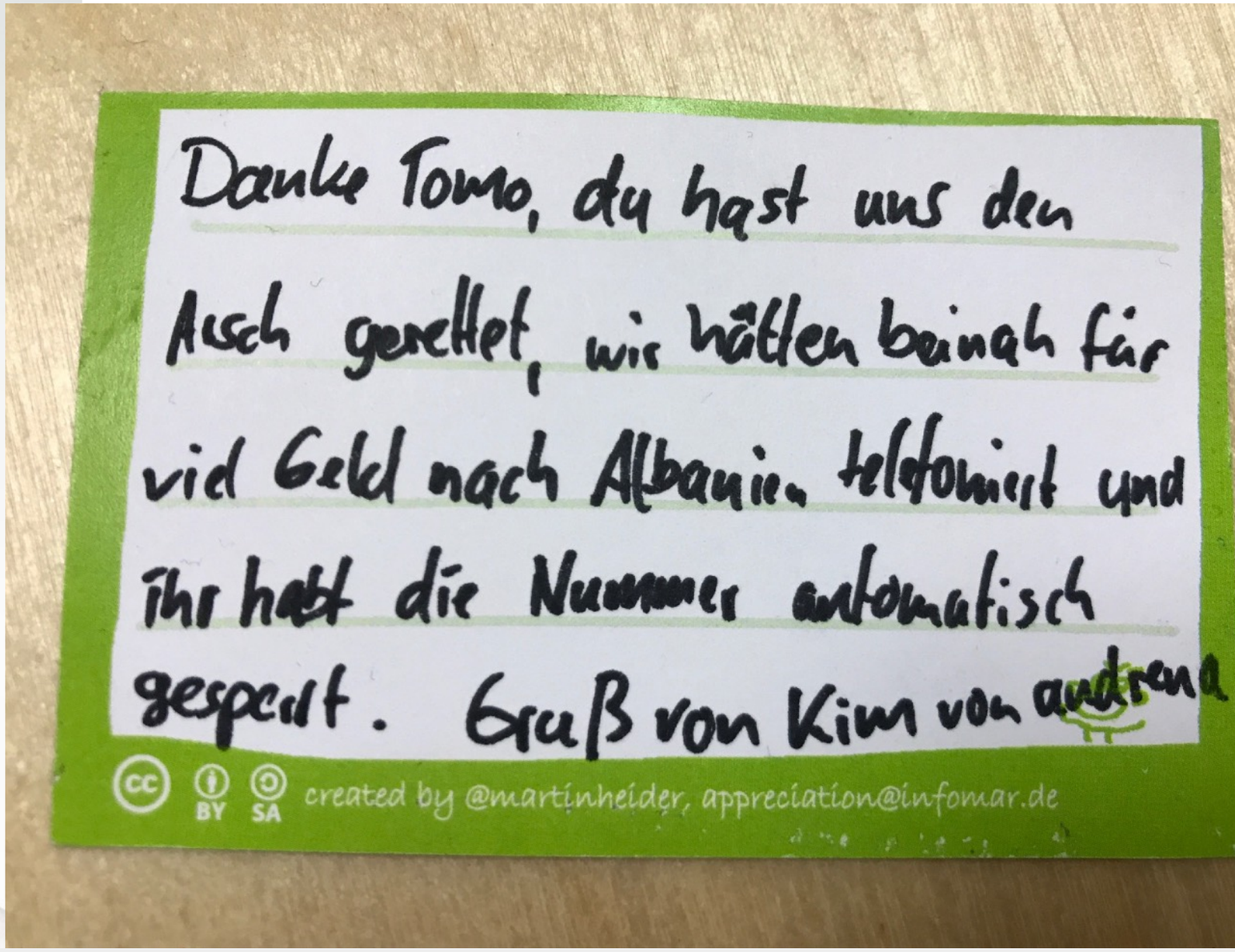
ISRF

Customer satisfaction

- (almost) no costs
- inform customers before anything happens
- customers can use their account as usual
- get praised

ISRF

Customer satisfaction



That's it

Questions?