Dynamic SIP Security

Me

Simon Woodhead

CEO, Simwood eSMS Limited

Director, LINX

https://simwood.com

http://blog.simwood.com

http://woody.is

@simwoodesms

3 things

1 idea

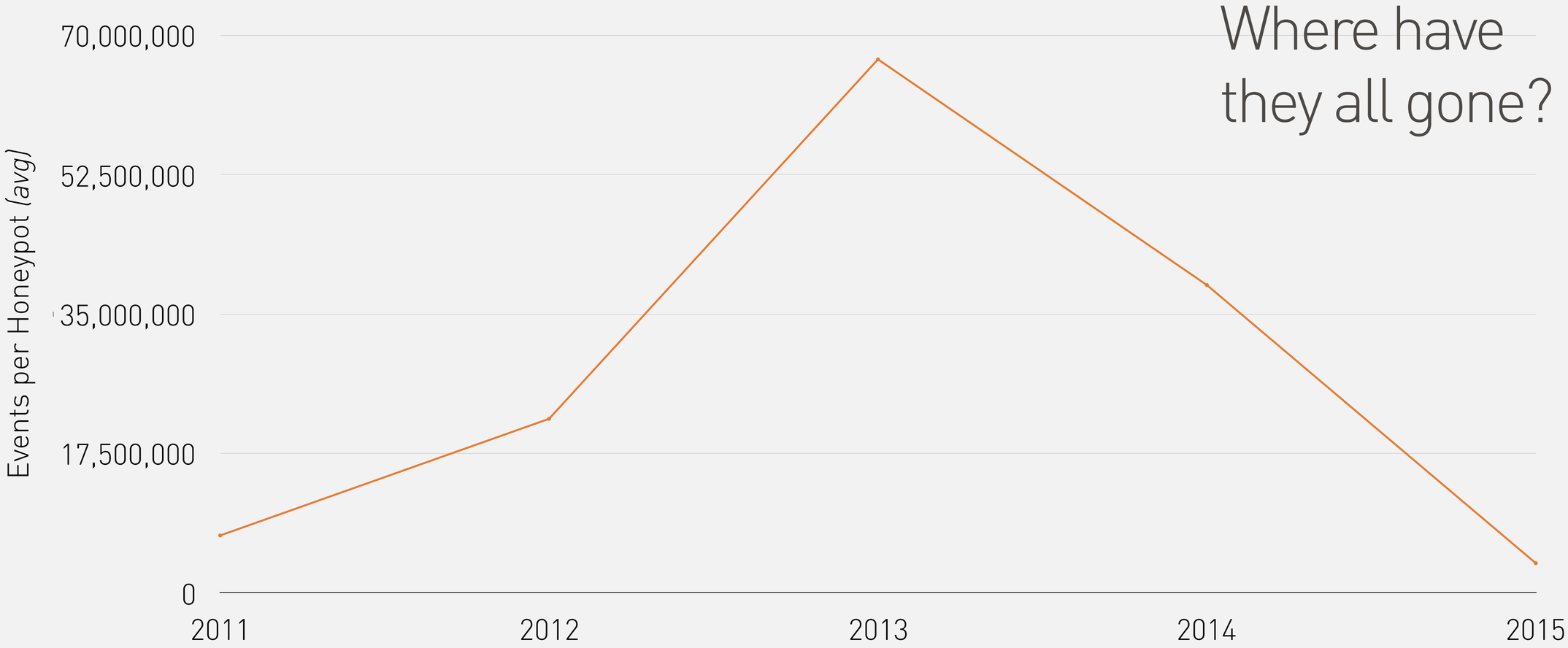
Contention

"The majority of you will be controlling your IP network in code within 5 years, most likely 3."

VoIP Fraud Update

Enumeration

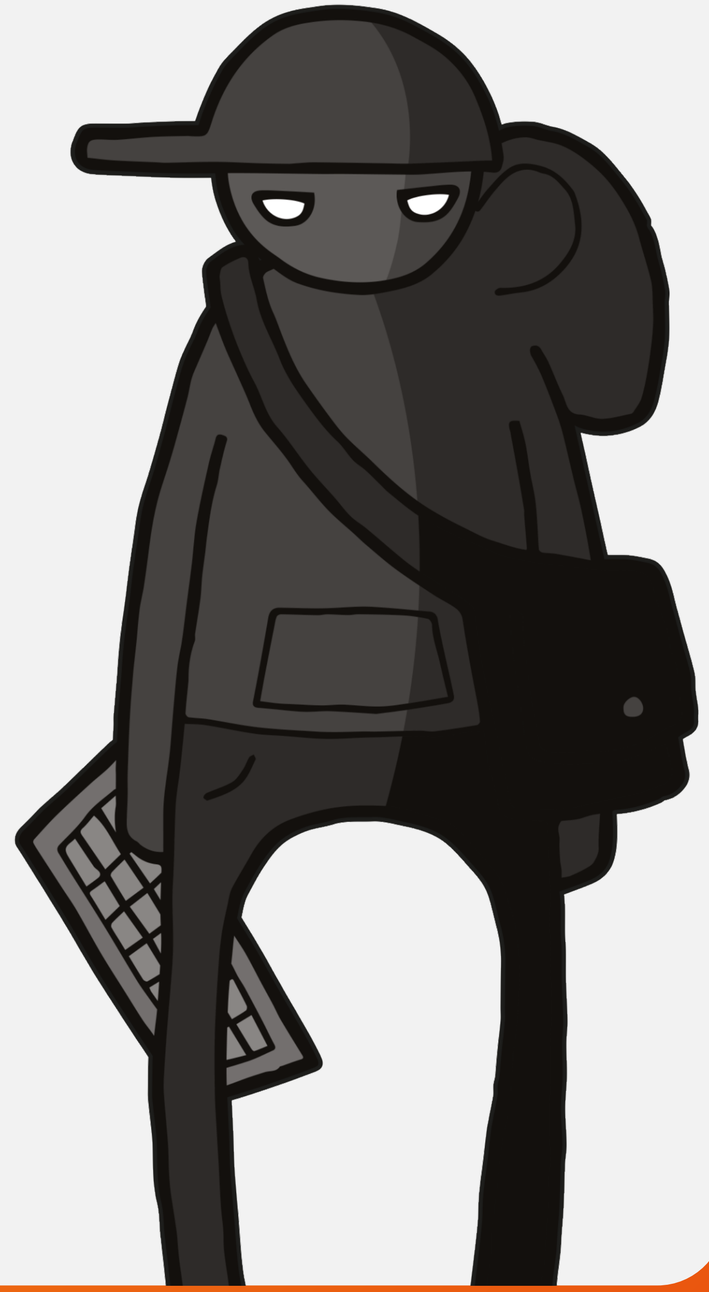
SIP **REGISTER** attempts



Enumeration

OPTIONS

to enumerate users



Enumeration

Reply where user **exists**.

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP XXX.XXX.XXX.XXX:5060
     ;branch=z9hG4bK-25245-1-0;received=XXX.XXX.XXX.XXX;rport=5060
From: sipp <sip:sipp@XXX.XXX.XXX.XXX:5060>;tag=1
To: <sip:201@XXX.XXX.XXX.XXX>;tag=as6bcdbe08
Call-ID: 1-25245@XXX.XXX.XXX.XXX
CSeq: 1 OPTIONS
Server: Asterisk PBX 10.5.1
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH
Supported: replaces, timer
Contact: <XXX.XXX.XXX.XXX:5060>
Accept: application/sdp
Content-Length: 0
```

Enumeration

Reply where user **does not exist**.

```
SIP/2.0 404 Not Found
Via: SIP/2.0/UDP XXX.XXX.XXX.XXX:5060
     ;branch=z9hG4bK-25231-1-0;received=XXX.XXX.XXX.XXX;rport=5060
From: sipp <sip:sipp@XXX.XXX.XXX.XXX:5060>;tag=1
To: <sip:unknown@XXX.XXX.XXX.XXX>;tag=as4c0176b1
Call-ID: 1-25231@XXX.XXX.XXX.XXX
CSeq: 1 OPTIONS
Server: Asterisk PBX 10.5.1
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH
Supported: replaces, timer
Accept: application/sdp
Content-Length: 0
```

Enumeration

fail2ban won't help you here

Our SIP ~~IPS~~ IDS*

* The P comes later!

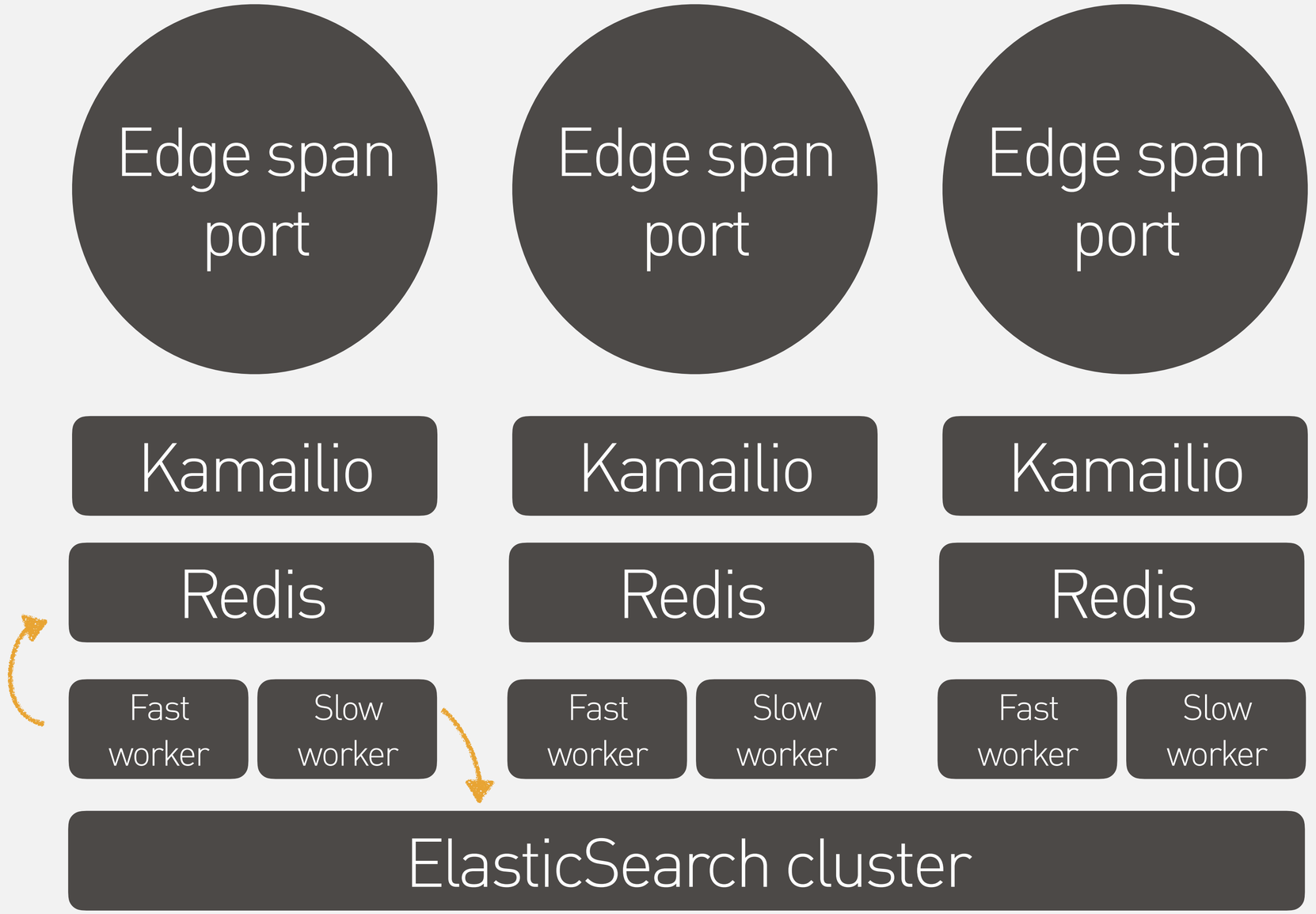
Honeypot architecture

FreeSWITCH

Splunk

http://mirror.simwood.com/honeypot

IDS architecture



Kamailio

```
# ----------------- setting module-specific parameters ---------------

modparam("sipcapture", "raw_socket_listen", "10.0.0.1:5060-5090")
modparam("sipcapture", "raw_socket_listen", "10.0.0.2:5060-5090")
modparam("sipcapture", "raw_moni_capture_on", 1)
modparam("sipcapture", "capture_on", 1)
#Note typo. Doesn't appear to do anything - promiscuous forced in rc.local
modparam("sipcapture", "promiscious_on", 1)
#db not used but necessary
modparam("sipcapture", "db_url", “mysql://homer_user:homer_password@localhost/homer_data")
modparam("sipcapture", "table_name", "sip_capture_call")
modparam("ndb_redis", "server", “name=local;addr=000.000.000.000;port=6379”)
```

```
request_route {
    redis_cmd("local","MULTI","r");
    redis_cmd("local","HSET event:$(ci{s.escape.common}) @timestamp $TS","r");
    redis_cmd("local","HSET event:$(ci{s.escape.common}) sourceip $si","r");
    redis_cmd("local","HSET event:$(ci{s.escape.common}) toip $Ri","r");
    redis_cmd("local","HSET event:$(ci{s.escape.common}) method $(rm{s.escape.common})","r");
    redis_cmd("local","HSET event:$(ci{s.escape.common}) from $(fu{s.escape.common})”,"r");
    redis_cmd("local","HSET event:$(ci{s.escape.common}) to $(tu{s.escape.common})","r");
    redis_cmd("local","HSET event:$(ci{s.escape.common}) dialled '$(tU{s.escape.common})'","r");
    redis_cmd("local","HSET event:$(ci{s.escape.common}) ua $(ua{s.escape.common})","r");
    $var(user_agent)=$(ua{re.subst,/^([a-zA-Z0-9-]+)(.*)/\1/});
    redis_cmd("local","HSET event:$(ci{s.escape.common}) short_ua $(var(user_agent){s.escape.common})","r");
    redis_cmd("local","HSET event:$(ci{s.escape.common}) node $HN(n)","r");
    redis_cmd("local","EXPIRE event:$(ci{s.escape.common}) 10","r");
    redis_cmd("local","LPUSH rate_events $(ci{s.escape.common})","r");
    redis_cmd("local","LPUSH events $(ci{s.escape.common})","r");
    redis_cmd("local","EXEC","r");
    drop;
}
```

Fast Worker

Node.js

Updates rate counters for all SIP traffic

Output to Redis only

Slow Worker

Node.js

Categorises & flags

Queries reputation cache

Inserts relevant events to ElasticSearch

Output to voice routing

Real-time test number blacklist

Output to IP routing

Real-time source IP to block

Real-time 4-tuple to block

SIMWOOD

- Home
- Commercial
- Analysis
- Threats new
- Trunk Management
- Inbound Numbers (DIDs)
- Mobile
- Voice CDR
- SMS CDR
- Accounts
- Notifications
- SMS & FAX
- Geo Porting
- Payments

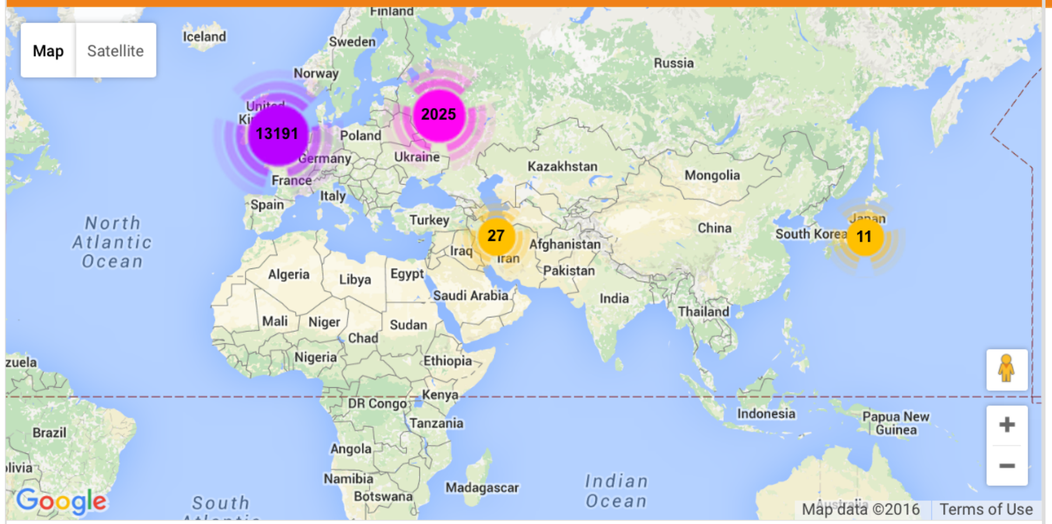
You are here: Home → Threats Analysis

help!

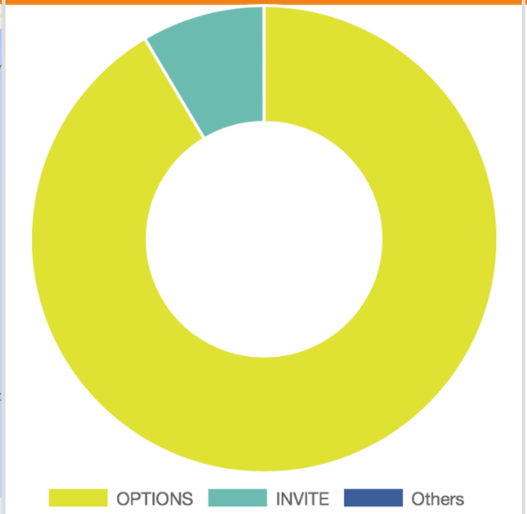
Today · Yesterday · Last week · last 30 days

2016-05-12 → 2016-05-18 - grey only

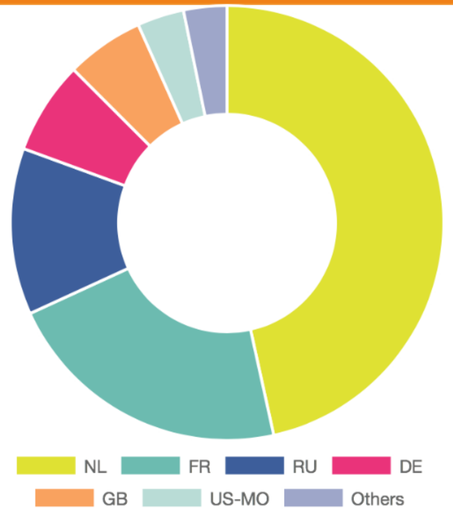
Threats map



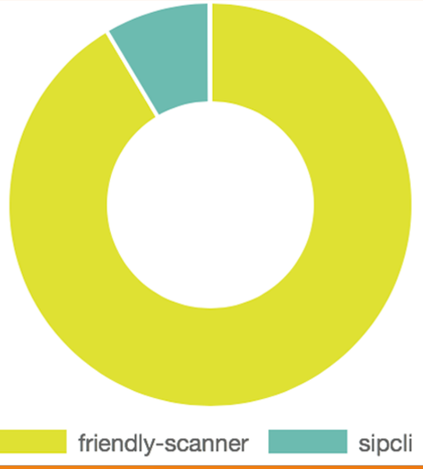
SIP Method



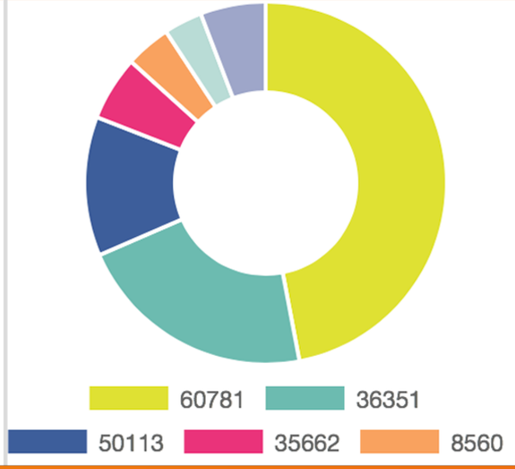
Country



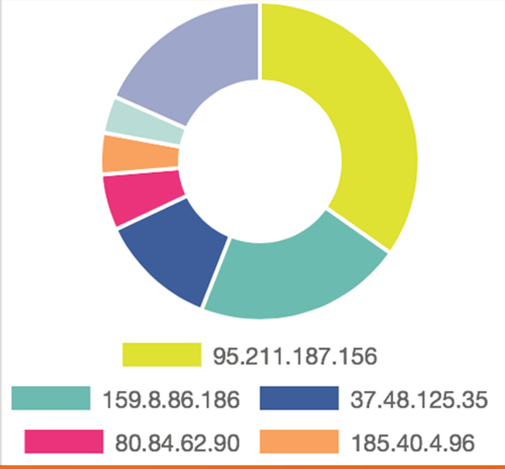
User Agent



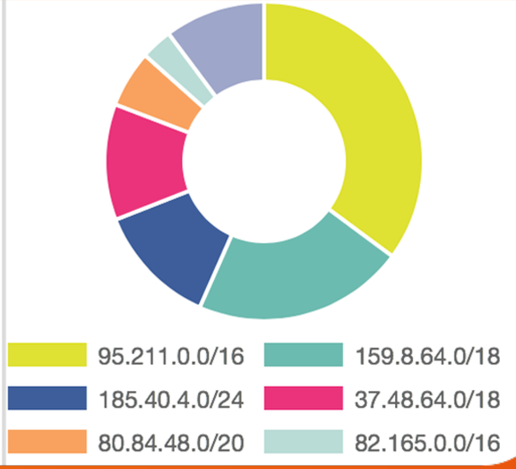
Source ASN



Source IP



Source Prefix



Network protection

How do we block them?

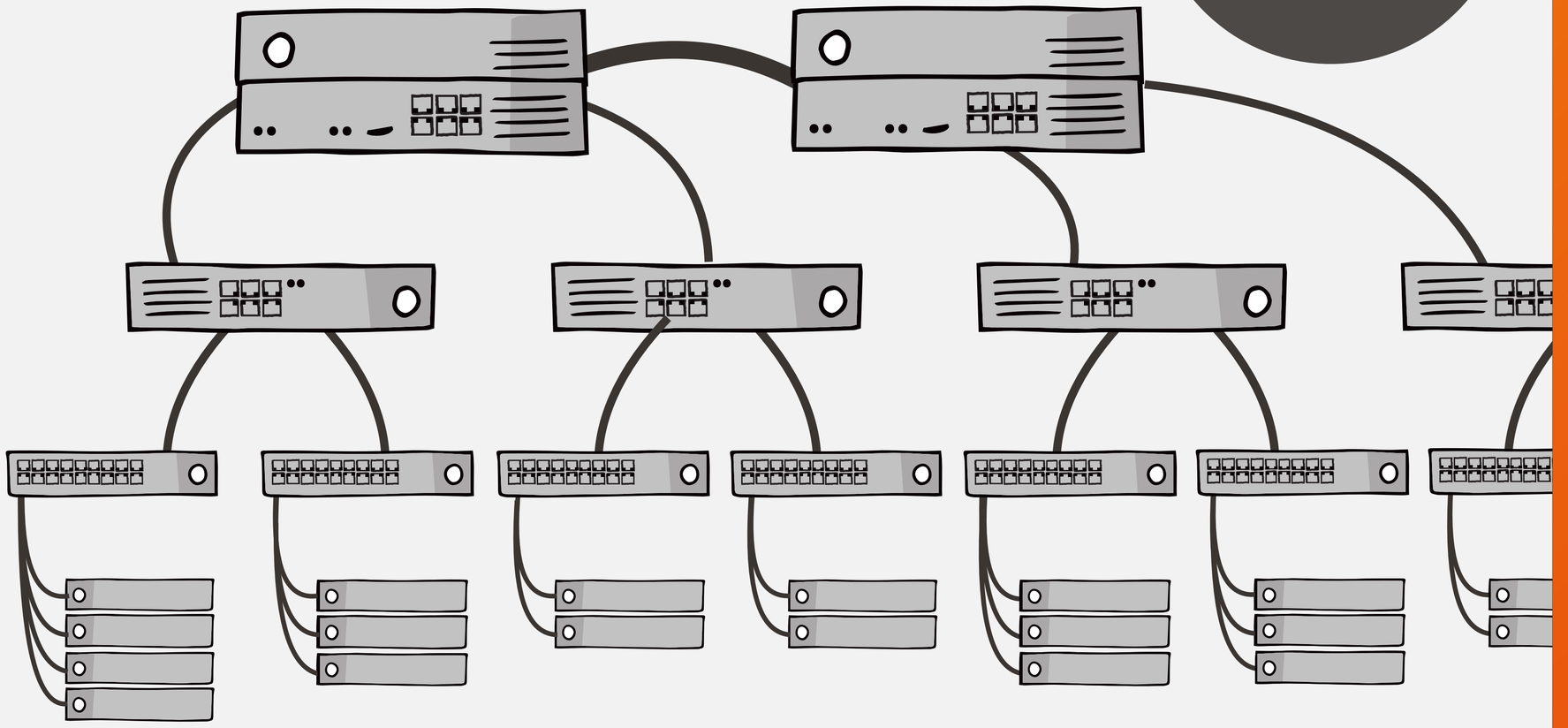
Traditional network

Core

Aggregation

Access

Hosts



None scale

All have a place in the mix but do not *effectively* scale to network or international level

Solution

Use the *network* to protect itself. Add additional measures where appropriate.

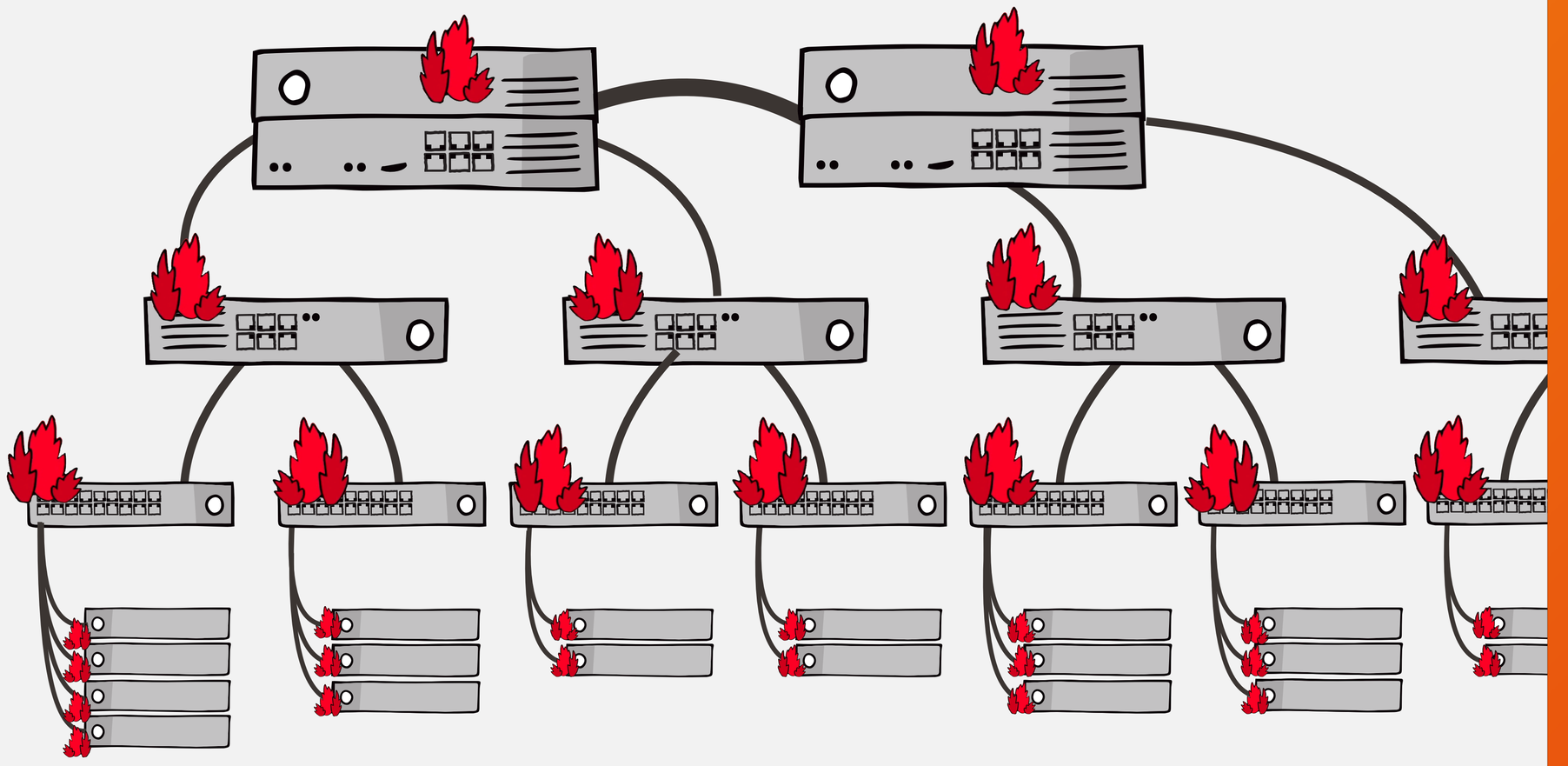
Traditional network

Core

Aggregation

Access

Hosts



How?

ACL

Applied per port by console

Not feasible to change dynamically network-wide

Good for relatively static config

BGP

Great for dynamic config at Internet scale

BGP alone = blackhole destination

BGP + loose uRPF = blackhole source + destination

Control from software

Nuclear option: address blocked not flow*

* Unless using FlowSpec on Juniper platforms

SDN

Abstracts control from forwarding (sound familiar?)

Software controller(s)

Total control at layer 2+

On paper: programme your network

Reality: Vendor-hyped & viewed cautiously

Merchant silicon / White boxes

Linux OS

Tb/s+ per U
in hardware!

APIs
XMPP
Your code

The future!

Hugely exciting.
Hopefully more at ClueCon!

Summary

3 things

1. VoIP Fraud evolution
2. Dynamic detection
3. Dynamic prevention

Summary

1 idea

"The majority of you will be controlling your IP network in code within 5 years, most likely 3."

Any questions?