Technical update part 2

Arnaud Fenioux
France-IX GM-2016

Oxidized

It's a RANCID replacement!

Written in ruby to backup equipment's configuration into a git repository

Lots of Vendor OS supported

Web interface to check status

Automatically adds/removes threads to meet configured retrieval interval

Able to trigger config backup from syslog

RESTful API to fetch configurations (and more)

Source backend (easy to automate) :

- CSV (router.db file)
- SQL / SQLite
- HTTP

TACACS+

AAAh!

Authentication, Authorization, and Accounting (AAA) services

Because Cisco equipment don't support RADIUS for Accounting

Deployed on all our equipment :

Production network

OOB Network

TACACS+

AAAh!

Authentication, Authorization, and Accounting (AAA) services

Read-Only account for **Oxidized**

Super-admin accounts for **each users**

Accounting messages are written in a **dedicated file**

Local account configured on equipment only as a fallback if **TACACS server** is down

ELK

"The Incredible ELK!"

Elasticsearch, Logstash, Kibana :
real-time data analytics tool for logs

Collecting logs from **Production** and **OOB Network** and **Linux servers**

Logstash : process and parse different kinds of logs

Cisco VS Unix logs
Accounting messages from **TACACS+**

ELK

"The Incredible ELK!"

Elasticsearch, Logstash, Kibana :
real-time data analytics tool for logs

Elasticsearch : search engine to filter messages by groups, types…

Kibana : Web interface with histograms and filters to access logs

- filtering **TACACAS+** messages with '`fields.tacacs:accounting`'

ElastAlert

Easy & flexible alerting framework with ElasticSearch

OpenSource tool developed by Yelp

YAML format to configure patterns to match and rules :

- Match on frequency, rates (spike or threshold), and more…

Built in alert types :

- Email, Slack, Telegram…

We decided to alert on all “Emergency”, “Alert” and “Critical” syslog messages

FranceIX Infrastructure AS57734

Replacement of the Transit routers on TH2 and ITX PAR5

Old J4350 routers replaced with Linux and Bird daemon

- Remember to change sysclt net.ipv6.route.max_size !

Utilisation of Bird single-RIB with secondary option :

```
secondary;
import keep filtered on;
```

FranceIX Infrastructure AS57734

Replacement of the Transit routers on TH2 and ITX PAR5

ASA Firewall/VPN replaced with :

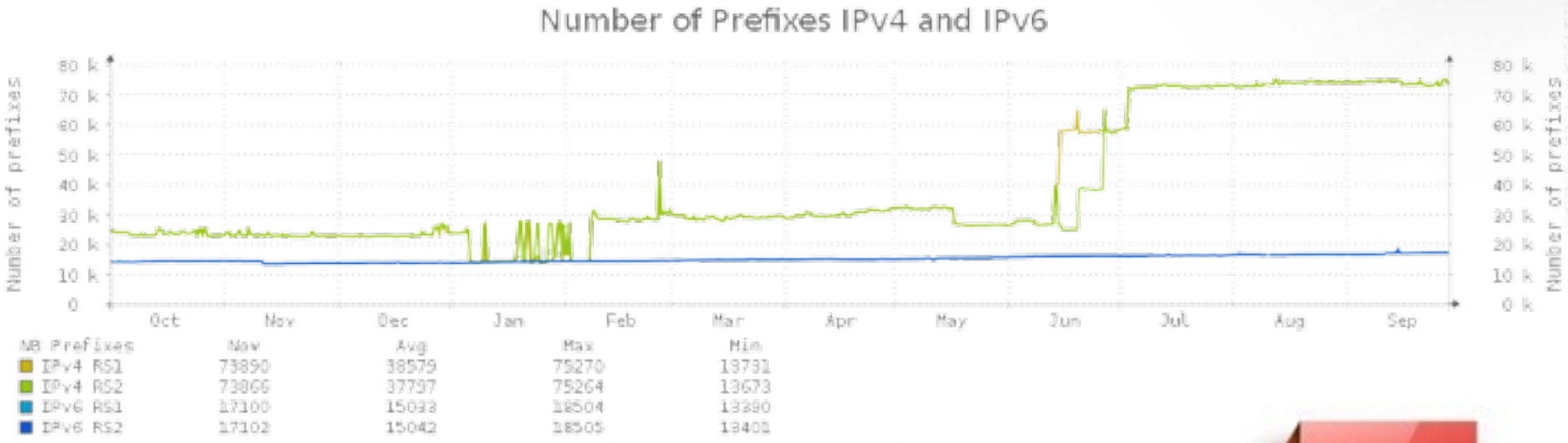
- iptables and ip6tables
- KeepAlived for managing the VIP
- conntrackd to synchronise firewall's sessions states (only active/passive mode is safe)
- OpenVPN

Route Servers

AS51706

Paris

- **264** IPv4 BGP sessions established
- **184** IPv6 BGP sessions established
- **73653** Unique IPv4 Routes
- **17042** Unique IPv6 Routes

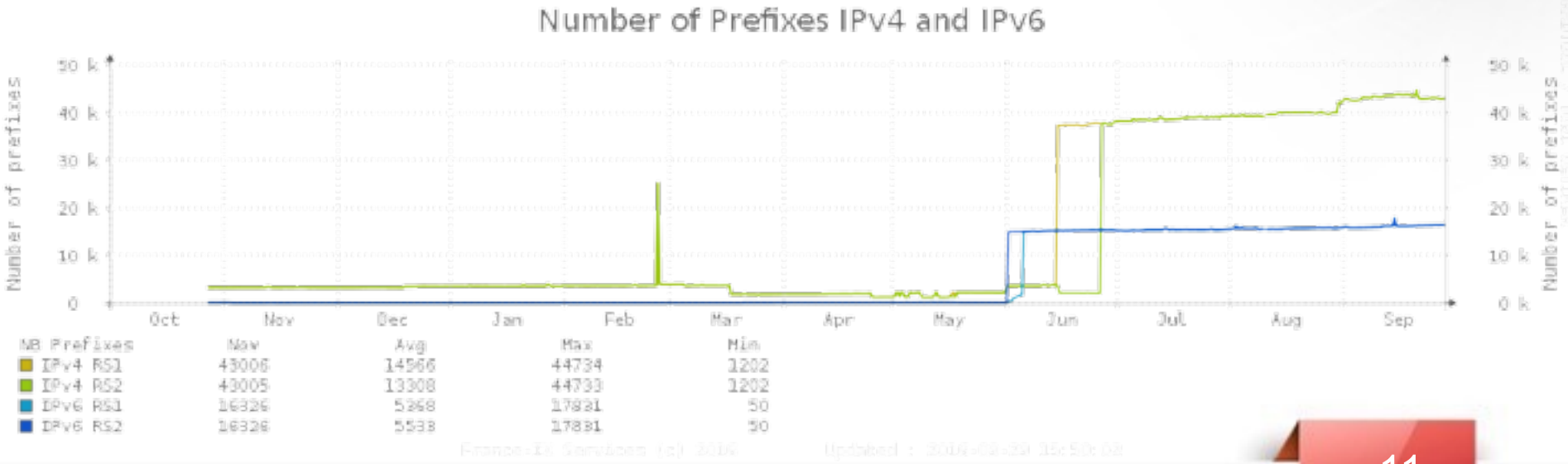


Route Servers

AS51706

Marseille

- **24** IPv4 BGP sessions established
- **20** IPv6 BGP sessions established
- **43053** Unique IPv4 Routes
- **16266** Unique IPv6 Routes



Route Servers RFC-ization

RFC 7947 : Internet Exchange BGP Route Server
outlines a specification for multilateral interconnections at Internet exchange points.

RFC 7948: Internet Exchange BGP Route Server Operations
describes operational considerations for multilateral interconnections at IXPs.

[I-D.kklf-sidr-route-server-rpki-light]
defines the usage of the BGP Prefix Origin Validation State Extended Community to signal prefix origin validation results from a route-server to its peers.

[I-D.ietf-sidr-origin-validation-signaling]

IRR Lock Down aut-num object

```
- - - - -
import:        from AS51706 accept      ANY
export:        to     AS51706 announce AS-EDXNETWORK

- - - - -
import-via:    AS51706 from  AS-ANY accept      ANY
export-via:    AS51706 to      AS-ANY announce AS-IELO

- - - - -
import-via:     afi ipv6.unicast AS51706 from AS-ANY accept ANY
export-via:     afi ipv6.unicast AS51706 to     AS-ANY announce AS-JAGUAR-V6

- - - - -
mp-import:     afi ipv4.unicast,ipv6.unicast from AS51706 accept ANY
mp-export:     afi ipv4.unicast,ipv6.unicast to AS51706 announce AS-HIVANE
```

Route Servers

RPKI/ROA and IRR

Number of AS parsed : 264

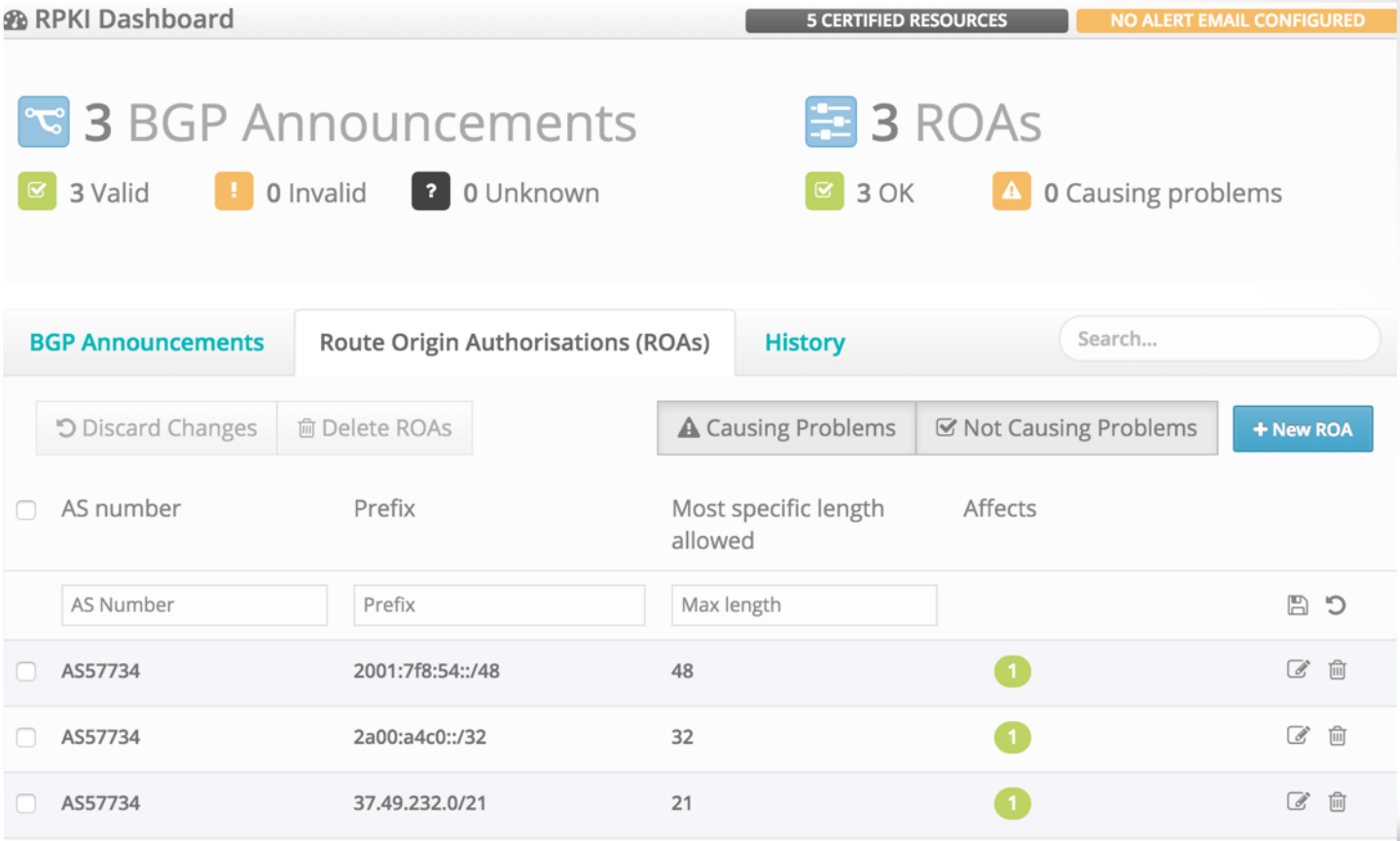
Number of AS-SET found for IPv4 : 48 (~20%)
Number of AS-SET found for IPv6 : 50 (~20%)

Number of IPv4 prefixes validated with IRR : 5495 (7.5%)
Number of IPv6 prefixes validated with IRR : 1608 (9.4%)

Number of IPv4 prefixes validated with ROA : 3997 (5.4%)
Number of IPv6 prefixes validated with ROA : 1868 (11%)

RPKI / ROA : Creation

- Very easy to setup via the RIPE web interface
- https://my.ripe.net/#/rpki



Merci !

Arnaud FENIOUX
@afenioux