RPKI + ROA, sécuriser enfin le routage BGP ?

Stéphane Bortzmeyer
AFNIC
bortzmeyer@nic.fr

Vide, exprès

Définir le problème

- 24 février 2008, Pakistan Telecom prive la planète de YouTube, sans pirater un seul routeur,
- 8 avril 2010, China Telecom détourne une partie du trafic (FoxNews dit que c'est grave),
- 23 juin 2011, Open Transit annonce (entre autres) les routes de l'AFNIC.

À noter que, quoi qu'en dise FoxNews, les trois cas étaient des erreurs.

Rappel BGP

1. Le protocole standard d'échange des routes sur l'Internet,
2. Réseau de pairs configurés à la main : un pair transmet à son voisin les routes qu'il connait. Elles sont ensuite retransmises aux autres voisins.
3. Une annonce de route comprend un **préfixe** IP et un **chemin d'AS**. L'AS d'**origine** est le plus à droite. (AS = *Autonomous System*, typiquement un opérateur)
4. Contrairement au DNS, ce n'est pas un arbre mais un graphe (bordélique).

Principes de la solution

1. Une infrastructure de distribution de **certificats numériques** prouvant qu'on contrôle un préfixe IP : la **RPKI** (*Resource Public Key Infrastructure*),
2. Des objets signés par le titulaire du préfixe, les **ROA** (*Route Origin Authorizations*). Un ROA est une **déclaration authentifiée** disant « Le préfixe `2001:db8:42::/48` peut être originé par l'AS 65584 ».

RFC 6480, `http://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html`

RPKI

La *Resource Public Key Infrastructure* est une infrastructure de distribution de :

- Quoi ? Des certificats **X.509**, utilisant les extensions du RFC 3779. Le sujet du certificat n'est pas important, ce qui compte est le `IPAddrBlocks`.
- Par qui ? [IANA ->] RIR -> LIR -> Client (pas les AC traditionnels)
- Comment ? `rsync -av rsync://rpki.ripe.net/repository /var/RPKI`

RFC 6487 et 6481

ROA

Test pour entretien d'embauche d'un admin' BGP :
« savez-vous ce qu'est un ROA ? »

Route Origin Authorizations

Un fichier CMS signé avec la clé du certificat (ci-dessus), listant les AS qui peuvent être l'**origine** d'un ou plusieurs préfixe(s).

Émis par le titulaire du préfixe.

RFC 6482

Le ROA de l'AFNIC

```
% certification-validator --print -f e6Y1dFuFnChdD1ZZ2AcNN_Xqp3I.ro
Object Type: Route Origin Authorisation object
Signing time: 2012-05-02T14:57:28.000Z
ASN: AS2486
Prefixes:
    2001:67c:2160::/48
    2001:67c:217c::/48
```

Détails : RTR

1. Le routeur route, il vaut mieux ne pas trop le charger.
2. Charger les ROA, valider, etc, est bien lourd pour le petit processeur d'un Cisco.
3. On va donc découpler :
   1. Un **cache/validateur**, typiquement une machine Unix, le **serveur** RTR,
   2. Le routeur, le **client** RTR.

   Entre les deux : RTR (*RPKI/Router Protocol*)
4. RFC pas encore publié mais presque.
5. RTR transmet juste des assertions (« l'AS 2486 peut originer `2001:67c:2160::/48` »), **c'est le routeur qui décide**.

Détails : qui allez-vous appeler ?

- Si on se fie à l'expérience de PGP/X.509/DNSSEC, il y aura des problèmes.
- Votre routeur rejette une route car signature invalide : *Who you gonna call ?*
- whois ? Qualité variable...
- *Ghostbusters !*
- Des vCard dans la RPKI

Mises en œuvres, gestion des certificats

Mélange de logiciel d'une AC X.509 et d'une solution IPAM.

- Il y en a sur le *cloud* (voir plus loin celui du RIPE-NCC)
- Au moins deux logiciels libres (pas testés), rcynic et Local Certification Service

Mises en œuvres, cache/validateur

- Solution du RIPE-NCC, en Java, RPKI Validator
- Solution ISC/ARIN, en C, rcynic
- D'autres apparaissent (BBN).

Mises en œuvres, routeur

Rappel : il suffit au routeur d'être client RTR et d'avoir un mécanisme permettant d'utiliser les assertions dans son processus de décision.

- Cisco IOS (publiée avec Classic 15.2(1)S et XE 3.5)
- Juniper (pas officiellement publiée, pour la 12.2 quelque part en 2012 ?)
- Quagga (patch disponible, nommé BGP-SRX)
- Bibliothèque cliente RTR libre, RTRlib (utilisée par BIRD)

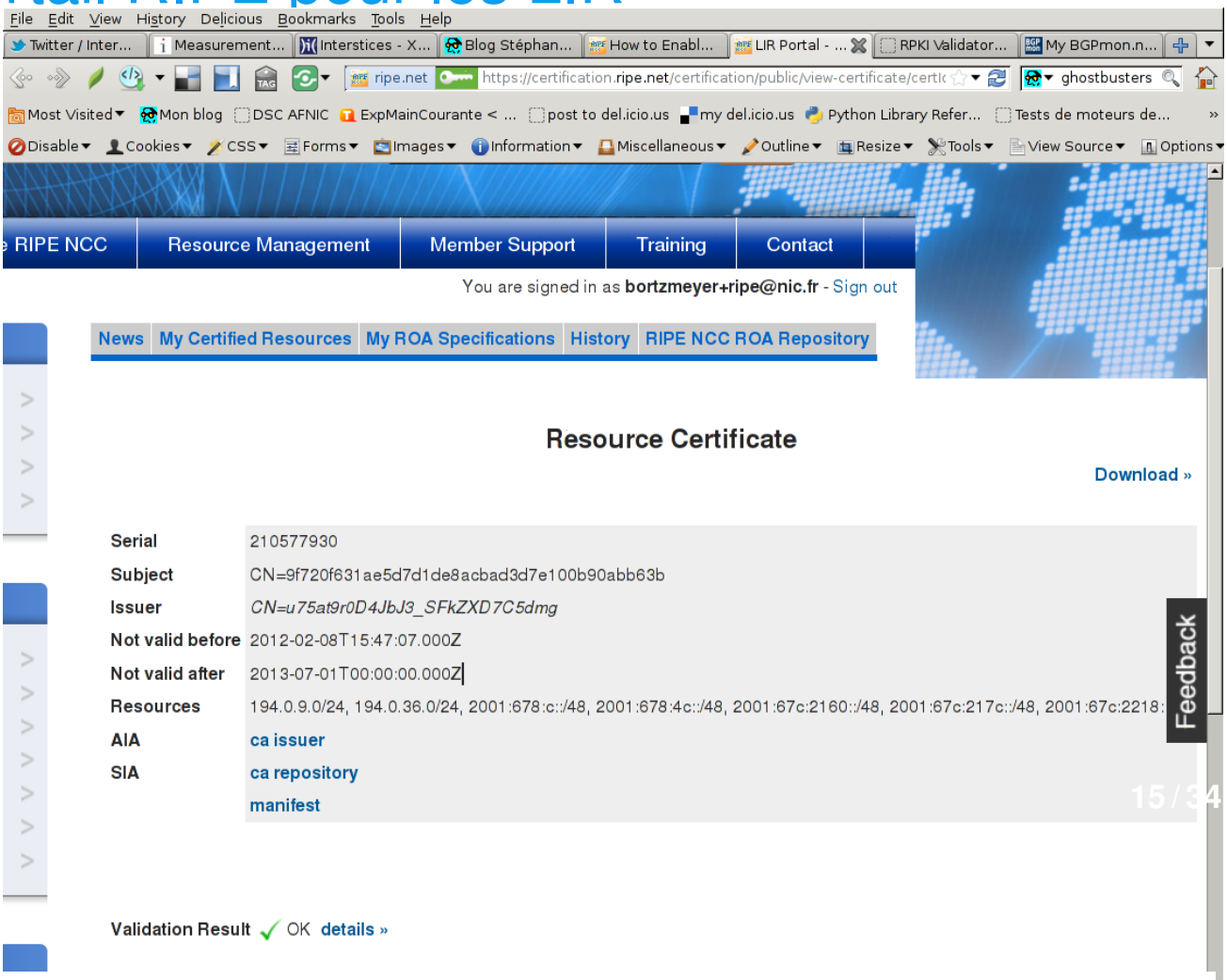
Client RTR sur Juniper :

```
rpki@lr1.ham1.de> show validation session
Session                                 State   Flaps     Uptime #
195.13.63.18                            Up       1015   00:53:27 1
```

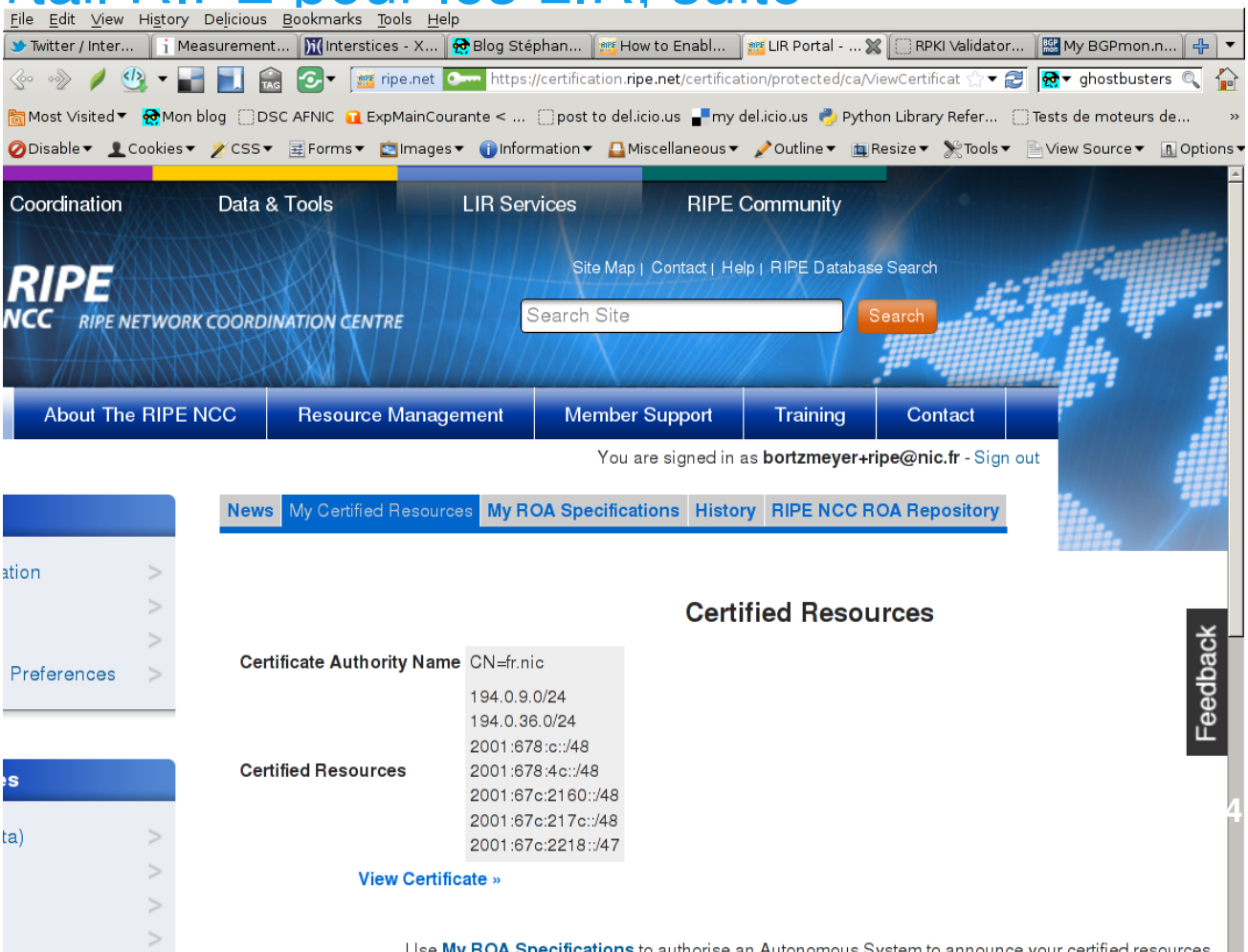

RTR en action, avec RTRlib

```
2012-05-29T09:07:22Z + 2800:38::   32 - 128  27808
2012-05-29T09:07:22Z + 2001:67c:2160::  48 -  48  2486
2012-05-29T09:07:22Z + 2001:1448:: 32 -  32   16245
2012-05-29T09:07:22Z + 2a02:d28::  32 - 120   5580
2012-05-29T09:07:22Z + 2a00:8640::  32 -  32  57771
2012-05-29T09:07:22Z + 2001:4190::  32 -  32    8246
```

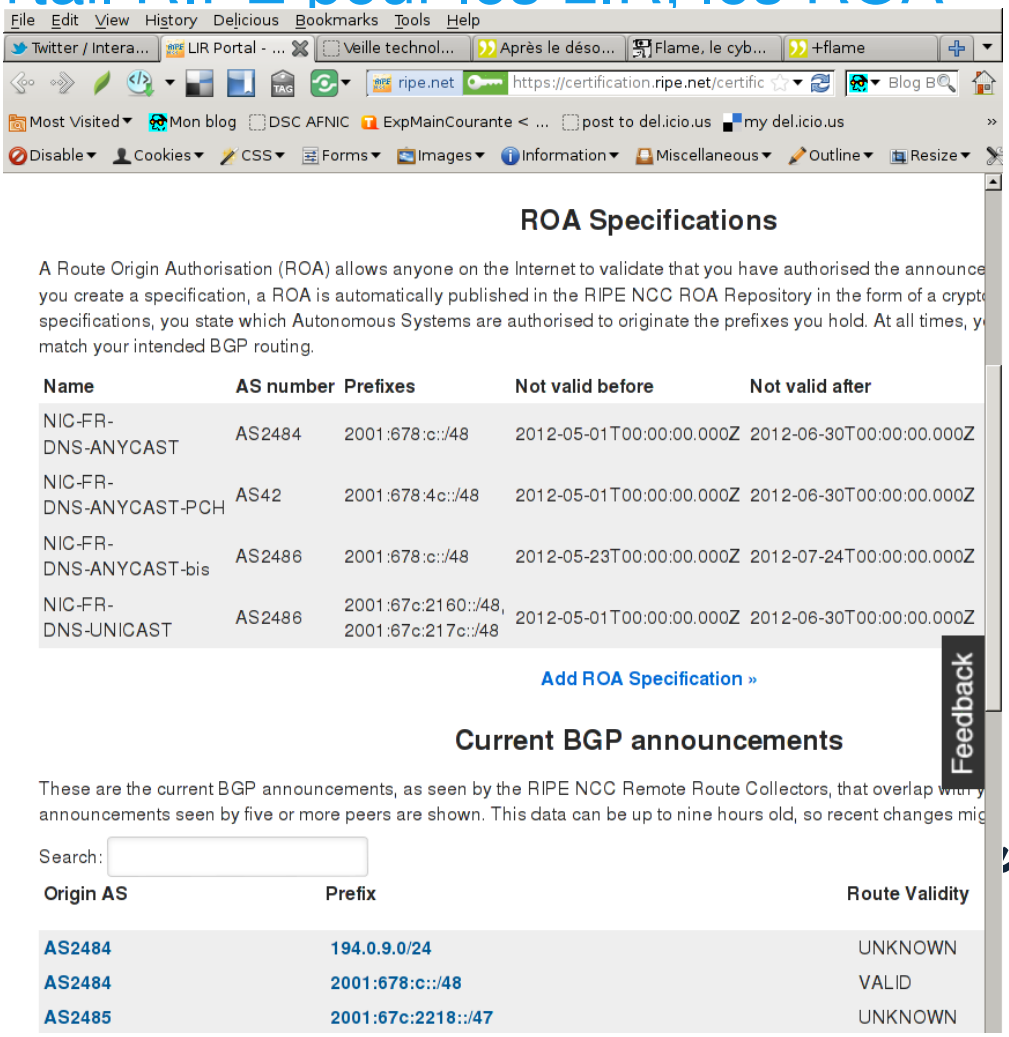
Portail RIPE pour les LIR



Portail RIPE pour les LIR, suite



Portail RIPE pour les LIR, les ROA

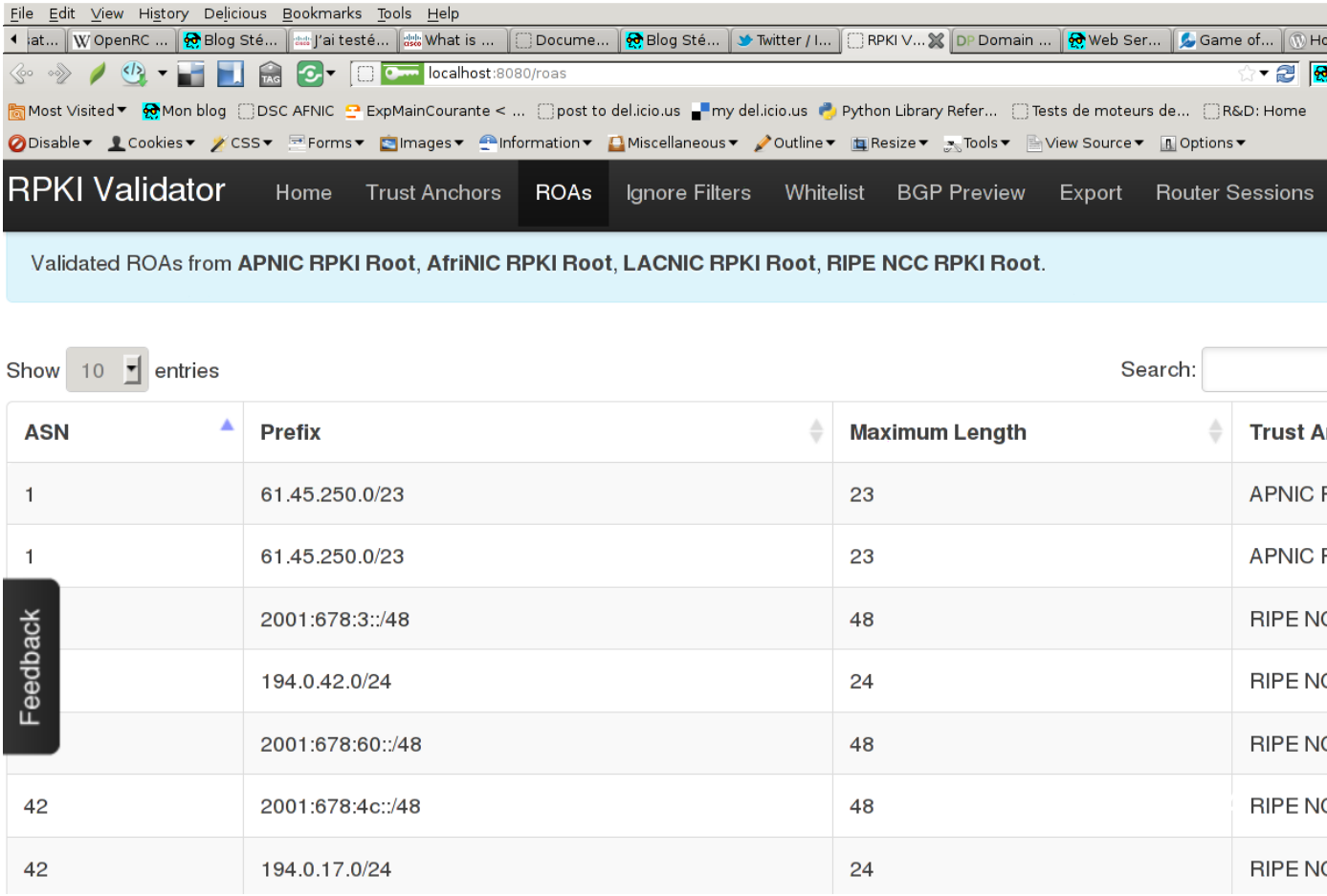


Outils RIPE

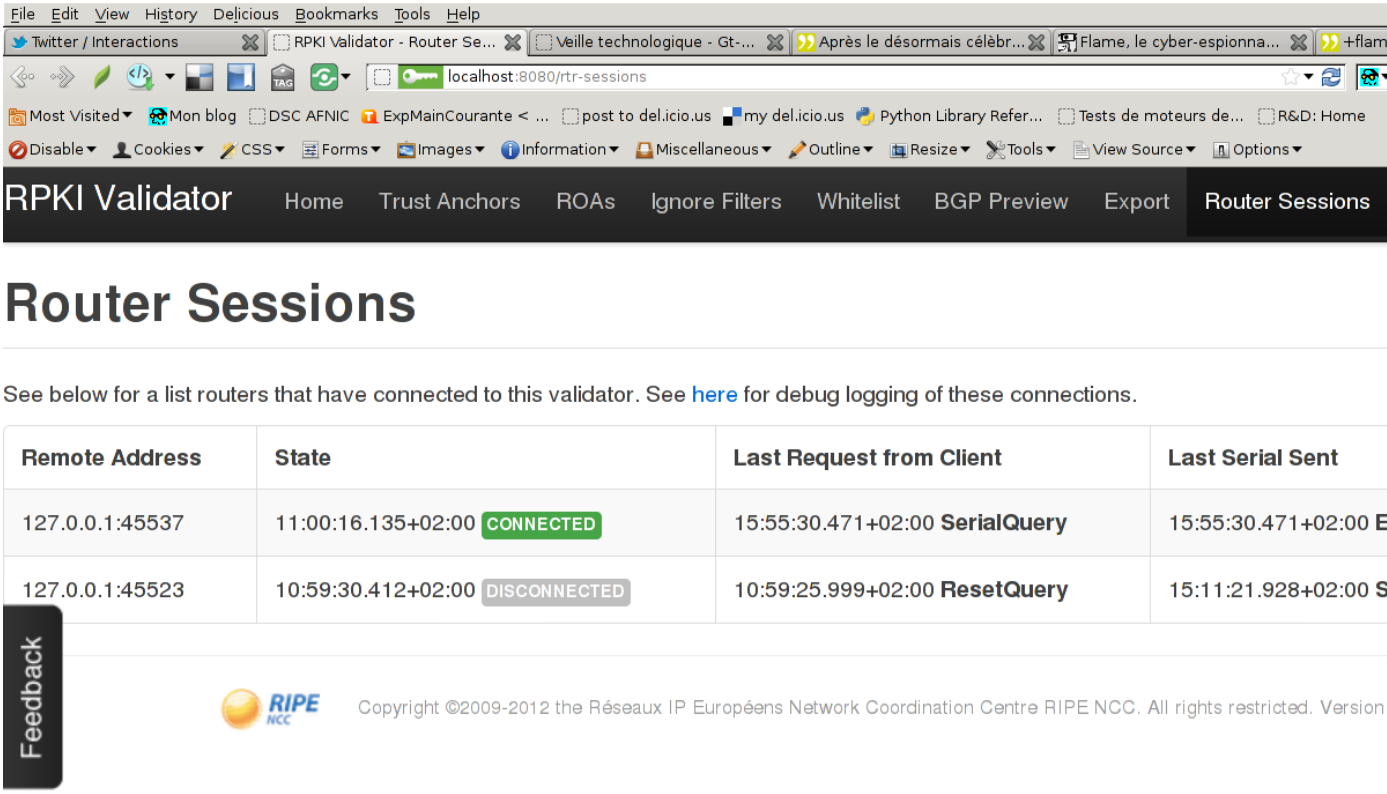
RPKI Validator fournit un cache/validateur, des outils en ligne de commande, une interface Web conviviale-graphique-pour-zutilisateurs...

Contrairement à tant d'outils en Java, ça semble tourner sur une machine 100 % libre (Debian).

RIPE RPKI Validator en local



Routeurs connectés au validateur du RIPE



Outil ligne de commande du RIPE

```
% certification-validator  --print -f  roa-5574190.roa
Content type: 1.2.840.113549.1.9.16.1.24
Signing time: 2011-01-11T19:04:18.000Z
ASN: AS559
Prefixes:
    193.5.26.0/23 [24]
    193.5.152.0/22 [24]
    193.5.168.0/22 [24]
    193.5.22.0/24
    193.5.54.0/23 [24]
    193.5.58.0/24
    193.5.60.0/24
    193.5.80.0/21 [24]
```


Autre outil, rcynic

rcynic fournit une AC RPKI (pas testée), un cache/validateur, des outils en ligne de commande.

Dépend de OpenSSL : attention sur Debian où le OpenSSL standard n'a toujours pas les extensions du RFC 3779 :-(

Démos de rcynic

```
% find_roa  /var/rcynic 2001:660::/32
ASN 2200 prefix 2001:660::/32 \
       ROA /var/rcynic/data/authenticated.2012-05-02T13:35:03Z/rpki

% print_roa /var/rcynic/data/authenticated.2012-05-02T13:35:03Z/rpk
...
asID:           2200
...
 addressFamily: 2
     IPaddress: 2001:660::/32
```


Outils génériques

OpenSSL peut gérer les certificats de la RPKI

```
% openssl x509 -inform DER -text \
    -in ./q3C8zU6hYpb7zVqmpjlVY5BBWE.cer
...
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=5XxoZDVUZvaNYJcVATAgTQ2ifLQ
        Validity
            Not Before: Dec 14 15:26:48 2010 GMT
            Not After : Jul  1 00:00:00 2011 GMT
...
            sbgp-ipAddrBlock: critical
                IPv4:
                  85.118.184.0/21
                  93.175.146.0/23
                IPv6:
                  2001:7fb:fd02::/47
```

Outils non locaux

Le serveur whois de BGPmon

```
Avant la création du ROA :

% whois -h whois.bgpmon.net " --roa 2486 2001:67c:2160::/48"
1 - Not Found

Après :

% whois -h whois.bgpmon.net " --roa 2486 2001:67c:2160::/48"
0 - Valid
------------------------
ROA Details
------------------------
Origin ASN:       AS2486
Not valid Before: 2012-05-01 00:00:00
Not valid After:  2012-06-30 00:00:00  Expires in 57d17h16m11s
Trust Anchor:     rpki.ripe.net
Prefixes:         2001:67c:217c::/48
                  2001:67c:2160::/48
```


Looking Glasses, voir la RPKI à distance

- http://www.labs.lacnic.net/rpkitools/looking_glass/

Configuration du routeur

Configuration du client RTR sur un Cisco :

```
bgp rpki server tcp 2001:db8:1000:2000::f00d port 8282 refresh 180

route-map test-rpki permit 10
 match rpki invalid
 set local-preference 50
```

État d'une route sur un Cisco (rappel : le routeur décide de ce qu'on fait d'une route invalide) :

```
rpki-rtr>show ip bgp 62.73.128.0
BGP routing table entry for 62.73.128.0/19, version 1865228
...
  12654 50300 15533
    193.0.4.1 from 193.0.4.28 (193.0.4.28)
      Origin IGP, localpref 110, valid, external, best
      path 58970BAC RPKI State valid
```


État du déploiement

- Tous les RIR sauf ARIN distribuent des certificats et des ROA,
- Au 12 mai 2012, dans les 1200 ROAs (bancs de tests exclus), en croissance très rapide dans RIPEland,
- Logiciels qui commencent à devenir stables mais peu de clients RPKI dans les images officielles des routeurs,
- Quasiment aucun routeur de production ne valide.

Futur

1. Les ROAs n'authentifient que l'**origine**. C'est largement suffisant contre les erreurs.
2. Mais un attaquant type Kapela&Pilosov va respecter l'origine et ne sera pas détecté
3. Prochaine étape, déjà en cours à l'IETF, utiliser la RPKI et un nouvel attribut BGP pour signer le chemin d'AS complet. Cette fois, cela modifiera BGP.
   1. IRR et systèmes d'alerte $\longrightarrow$ BGPbrut
   2. RPKI+ROA $\longrightarrow$ BGPdemisec
   3. Validation du chemin $\longrightarrow$ BGPsec

Critiques techniques

- Complexité, et dépendance vis-à-vis de nouvelles infrastructures pas maîtrisées,
- Risques de faux positifs (comme avec les IRR, où beaucoup de routes seraient rejetées si on filtrait),
- Les ROA protègent contre les accidents, pas contre les attaques.

Rover

- La RPKI est la solution « officielle » à l'IETF et chez les RIR. Y a-t-il une alternative technique ?
- ROVER propose de mettre la même information (AS d'origine et, demain, chemin) dans le DNS, signé avec DNSSEC. Même niveau de sécurité que la RPKI. Fini, X.509.
- Réutilise logiciels et hiérarchies existantes.
- Nettement moins testé et soutenu que la RPKI. Mais plus simple et moins risqué.
- Beaucoup de problèmes (risques de faux positifs, problèmes politiques) sont les mêmes avec ROVER et la RPKI.

```
c.7.1.2.c.7.6.0.1.0.0.2.ip6.arpa. SRO AS2486 ; NIC-FR-DNS-UNICAST-P
```


Politique

- Autrefois, les RIR n'avaient qu'un rôle indicatif : n'importe qui pouvait annoncer n'importe quel préfixe. En criant assez fort, ça passait. Inversement, une annulation d'allocation par un RIR (RBN. . .) n'avait pas d'importance pratique.
- Si la RPKI+ROA est déployé, avec refus des annonces non ou mal signées, cela sera différent. Une révocation pourrait rendre un préfixe largement inaccessible. **Les RIR auraient gagné un rôle opérationnel.**
- Il va falloir réviser son code pénal néerlandais.
- Les discussions policitiennes sur la gouvernance de l'Internet se focalisent sur l'excitant `.xxx` et oublient les problèmes concrets comme la RPKI.

Comparaison avec DNSSEC

1. Mêmes problèmes des faux positifs (bien plus nombreux que les vrais),
2. Mêmes optimistes jurant que tout ira bien (tu parles),
3. Même question fondamentale : « la sécurité vaut-elle une telle dépense ? »,
4. Même nécessité de montée en compétence et même résultat : éliminer les petits,
5. Moins de problèmes politiques : le DNS était déjà arborescent.

Observatoire de la résilience de l'Internet

Concepts :

1. appréhender la résilience de l'Internet français ;
2. promouvoir les bonnes pratiques ;
3. définition et mesures d'indicateurs techniques représentatifs de la résilience.

Rapport 2011 : analyse sur les données BGP & DNS de janvier à novembre 2011

- les co-auteurs sont présents et disponibles ;
- des copies papier peuvent être récupérées.