

# **Route Servers, fonctionnalités et sécurités**

Arnaud FENIOUX - FrancelIX

@afenioux #FRnOG25

2015-11-13





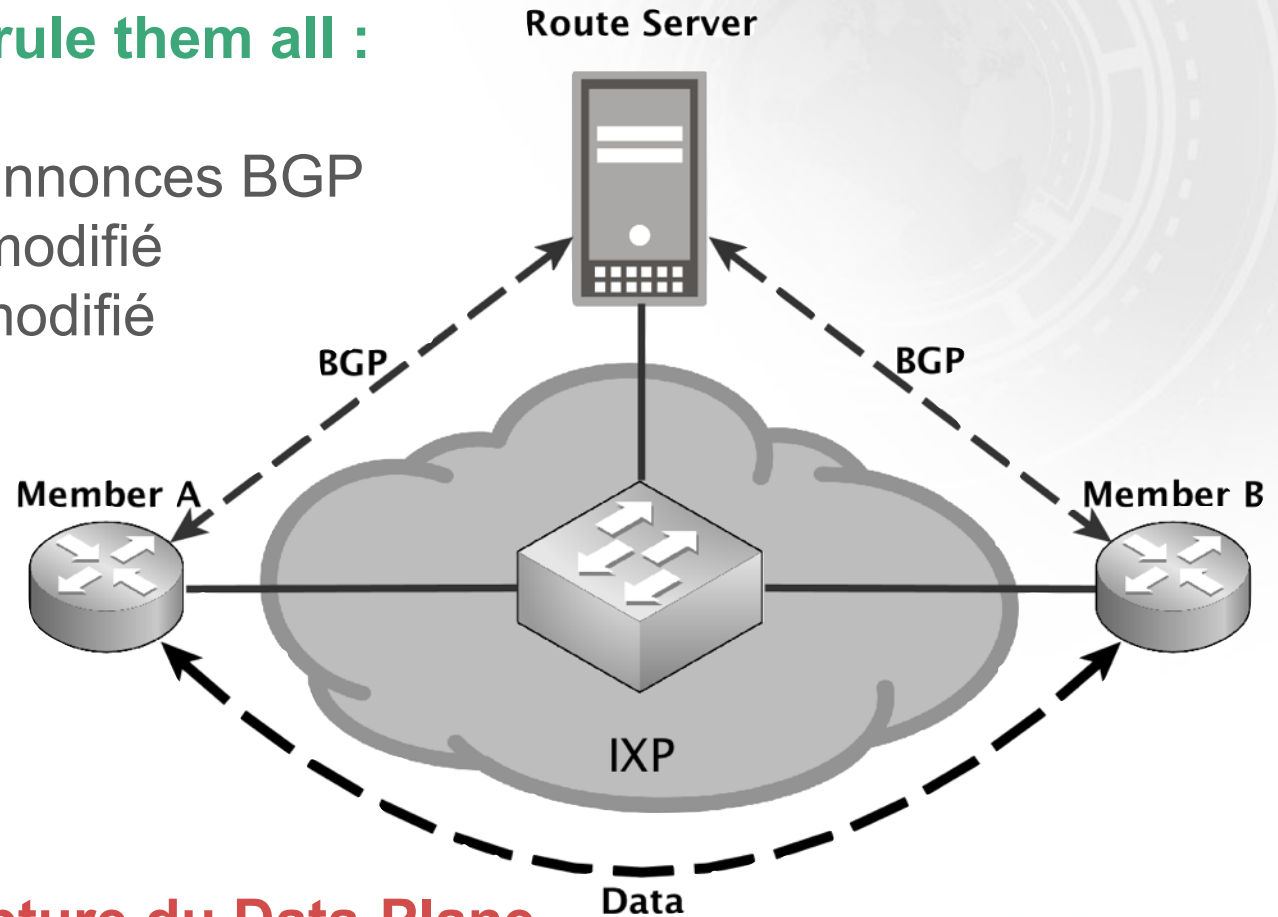
# Route Server

## Fonctionnalités

# Data plane vs Control plane

## One session to rule them all :

- Centralise les annonces BGP
- AS-PATH non modifié
- Next-hop non modifié
- Trafic en direct



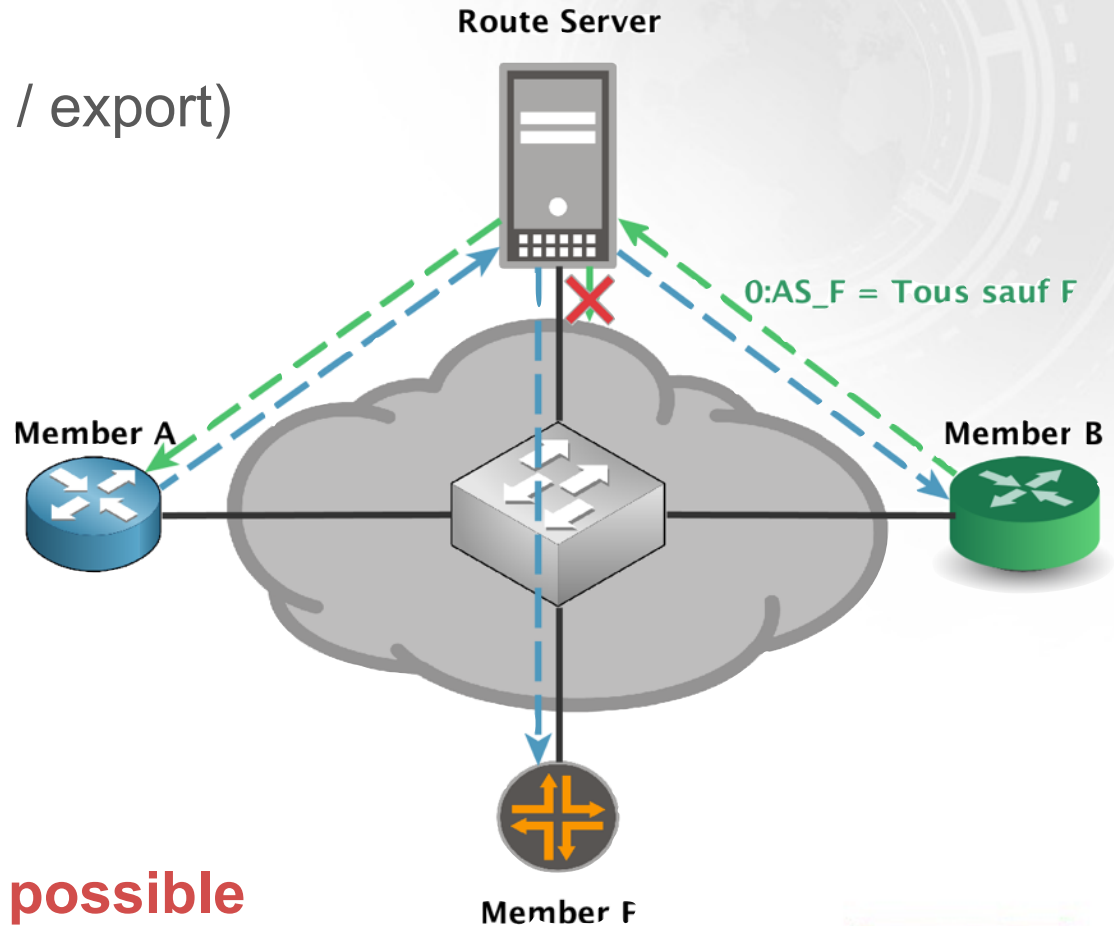
**!! Blackholing si rupture du Data-Plane**

# Annonces sélectives

via:

- Communautés BGP
- IRR (aut-num import / export)
  
- Filtrage
- AS-PATH prepending
- Ré-écriture de la MED

0:peer-as = Don't send route to this peer AS



**!! Asymétrie de trafic possible**



# Route Server

## Sécurités

# Fat finger errors

## Martians (IPv4 et v6)

- Filtrage des préfixes martiens  
<https://www.team-cymru.org/bogon-dotted-decimal.html>

## Max prefix limit

- Limite le nombre de préfixes appris par peer sur les RS  
Coupe la session BGP si le seuil est dépassé

## Prefix length

- IPv4 : /8 a /24 sont autorisés
- IPv6 : /19 a /48 sont autorisés

## Protège contre :

- leaks massifs / leaks de routes internes

# “Thin” finger errors

## Next-hop

- Vérification que l'IP next-hop dans l'update BGP est aussi l'IP source du paquet

## First AS in AS-PATH

- Vérification que le premier AS de l'AS-PATH est l'AS du peer BGP

## Protège contre :

- Les annonces BGP falsifiées
- Redirection de trafic vers une victime
- Masquage de l'AS attaquant

# IRR Lock Down AS-SET ou ASN

- N'autorise que les préfixes enregistrés par certains AS-SET ou ASN

**AS-SET -> AUT-NUM -> ROUTE(6) -> INETNUM(6)**

IRR Explorer + BGPQ3 = <3

<http://irrexplorer.nlnog.net/>

<http://peering.readthedocs.org/en/latest/PrefixLists.html>

## Protège contre :

- Hijacking de préfixes

**!! dépend de la qualité des données dans les IRR**



# IRR Lock Down **import/export**

```
-----  
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
```

# RPKI / ROA

## RPKI / ROA

- Valide que l'AS à l'origine de l'annonce est autorisé à annoncer ce préfixe.

Enregistrement via le LIR Portal :

<https://www.ripe.net/manage-ips-and-asns/resource-management/certification/resource-certification-roa-management>

## Evite :

- Certains hijacking de prefixes

**!! Ne valide pas la transitivité**

# Comparatif

	<i>AMS-IX (Falcon)</i>	<i>DE-CIX</i>	<i>LINX</i>	<i>FranceIX</i>	<i>LyonIX</i>
<i>Martians</i>	<b>Y</b>	<b>Y</b>	<b>Y</b>	<b>Y</b>	<b>Y</b>
<i>Max prefix</i>	<b>Y</b>	<b>Y</b>	<b>Y</b>	<b>Y</b>	<b>Y</b>
<i>Pfx Length</i>	-	<b>Y</b>	-	<b>Y</b>	<b>Y</b>
<i>Next-hop</i>	<b>Y</b>	<b>Y</b>	-	<b>Y</b>	<b>Y*</b>
<i>First AS</i>	<b>Y</b>	-	-	<b>Y</b>	<b>Y*</b>
<i>IRR</i>	<b>Y</b>	<b>Y</b>	-	<b>Soon!</b>	<b>Y</b>
<i>RPKI/ROA</i>	<b>Y</b>	-	-	<b>Soon!</b>	<b>Y*</b>

\* Non présent sur tous les RS

# Références

## **Euro-IX 27 : Route Server Policies @ IXPs**

<https://euro-ix.net/m/uploads/2015/10/27/e-BH-20150921-Euro-IX-Route-Server-Filtering-at-IXPs.pdf>

## **RIPE 70 : IRR Lockdown**

[https://ripe70.ripe.net/wp-content/uploads/presentations/52-RIPE70\\_jobsnijders\\_irrlockdown.pdf](https://ripe70.ripe.net/wp-content/uploads/presentations/52-RIPE70_jobsnijders_irrlockdown.pdf)

## **AMS-IX Falcon class Route Servers**

<https://ams-ix.net/technical/specifications-descriptions/ams-ix-route-servers/falcon-class-route-servers>

## **Euro-IX 27 : Peering Observations 2007 vs. 2015**

<https://euro-ix.net/m/uploads/2015/10/23/27th-euro-ix-peering-observations.pdf>

## **NANOG 51 : Route Servers, Mergers, Features and More**

<https://www.nanog.org/meetings/nanog51/presentations/Tuesday/Malayter-Router%20Server%20Presentation%204.pdf>

**Merci !**

Arnaud FENIOUX  
@afenioux



**DONT TOUCH MY  
INTERNET**