Implementación RPKI

RIPE Validator, Huawei y Mikrotik

Ariel Weher, LACNOG

https://eventos.nog.lat

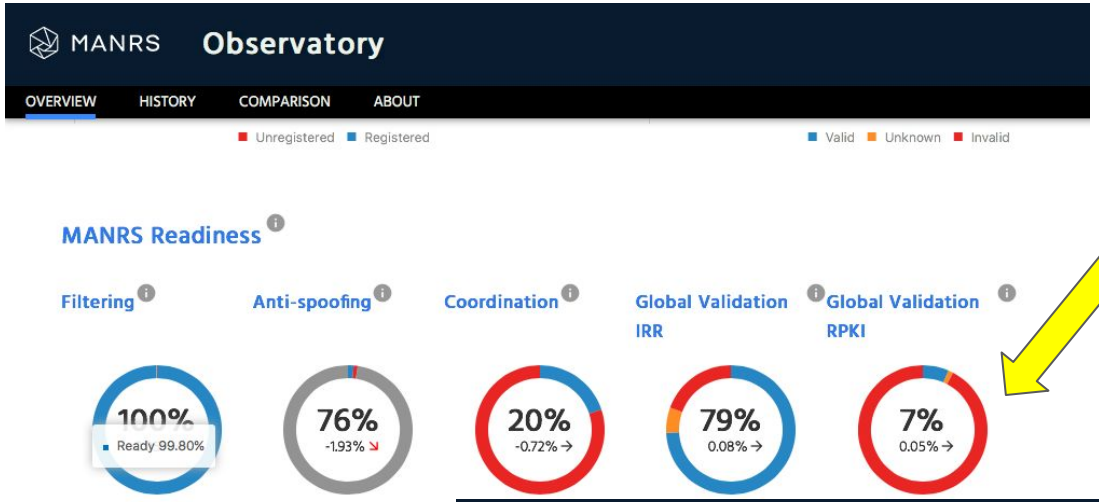
agosto 2020

28 ago. Ariel Weher, "Implementando RPKI: RIPE NCC RPKI Validator, Huawei y Mikrotik" WEBINAR

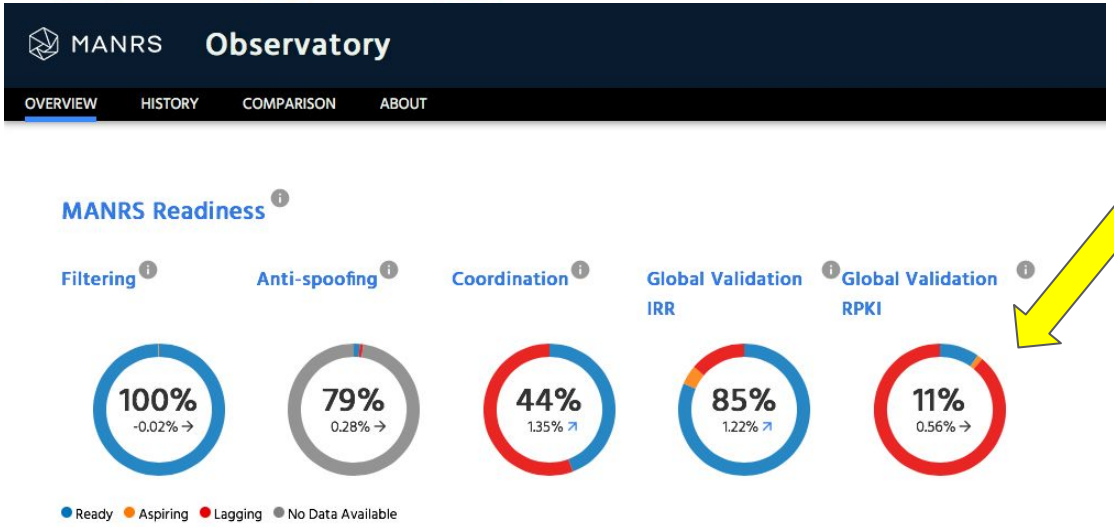
14 ago. Carlos Martínez, Celsa Sanchez, "Implementando RPKI: FORT & Cisco" WEBINAR

julio 2020

17 jul. Carlos Martínez, Tomás Lynch, "Implementando RPKI en Juniper" WEBINAR



LACNIC:
RPKI
(julio 2019)



LACNIC:
RPKI
(julio 2020)

https://observatory.manrs.org

Esta es una herramienta en línea que mide los niveles de conformidad con las acciones MANRS, un indicador clave del estado de seguridad de enrutamiento y resistencia de Internet.

Evento

https://www.lacnic.net/lacnic34
#lacnog10

#LACNOGWebinar

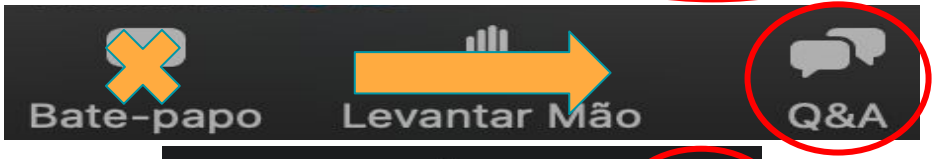
¡Bienvenidos!

Formato del Webinar

- Sesión moderada por **Lia Solís y Carmen Denis**
- Los oradores hablarán en español
- La sesión está siendo grabada
- También estamos transmitiendo en vivo en nuestra Página de Facebook https://www.facebook.com/lacnog/
- Por favor no realicen preguntas en el chat
  - Usar la herramienta de preguntas y respuestas de Zoom

Zoom versión Español

Zoom versión Portugués



Zoom versión Inglés

Orador:

Ariel Weher, LACNOG

Breve intro a RPKI

Problema que queremos solucionar

MANRS #4

En este **ejemplo**, supongamos:

- Usted tiene un ASN
- Usted tiene asignados prefijos
- Los publica usando BGP a sus proveedores de tránsito IP y demás peerings.
- Alguien no autorizado publica sus redes desde otro ASN.
  - Ya sea por un error humano o malintencionadamente.
  - Generalmente el error humano se evita cuando las dos partes del peering configuran filtros adecuados.
    - Pero lamentablemente esto no pasa en todos los casos.
- Usted desea evitar al máximo posible que alguien más publique y utilice las redes que le pertenecen.
  - Utilizar un mecanismo para declarar qué numero de ASN publicará cierto prefijo que a usted le pertenece.
  - De acuerdo a todas las declaraciones hechas en el mundo, usted establece filtros en sus routers tratar de manera especial las publicaciones que le llegan, en donde lo publicado no coincide con lo declarado.
- La solución absoluta depende de que todas las partes hagan su trabajo.
  - Los dueños de los recursos **deben** declarar qué ASN publica.
  - El resto de los AS **deben** validar esa información a la hora de aceptar rutas entrantes.

Pasos a completar para resolver el problema

El encargado de las IP declara qué ASN va a publicar sus redes y con qué largo de prefijo.	→	Crear ROAs en el RIR (LACNIC).
El encargado de las IP publica de acuerdo a lo declarado (ASN origen y largo de prefijo).	→	Publicación BGP tradicional.
El resto del mundo instala el software que lee los ROAs desde los 5 RIRs y los guarda en una base de datos local.	→	Instalar un RPKI Validator (FORT, RIPE, Routinator, etc).
Configurar para que cada router de borde obtenga los prefijos desde la base de datos local del validator.	→	Generar una sesión de RTR entre los routers de borde y los validators.
Hacer una política de ruteo que de un trato específico a las rutas según su origen sea válido, inválido o desconocido.	→	Agregar validación de origen a las políticas de ruteo vigentes.


¿Qué queremos?
¡Que no secuestren nuestras IPs!
¿Qué haremos?
¡Publicar nuestros ROA!


¿Qué queremos?
¡No aceptar tráfico de redes secuestradas!
¿Qué haremos?
¡Implementar RPKI!

LAC-2019-12: ROAs RPKI con ASN 0

MANRS
#4

Durante 2019 y 2020 la comunidad de LACNIC discutió en el Foro Público de Políticas una propuesta en donde LACNIC va a firmar ROAs de los bloques IP aun no asignados con origen en el AS 0.

De esta manera, quienes hagan validación de origen de rutas podrían filtrar de manera automatizada los secuestros de ruta de bloques no asignados, dado que se volverían inválidos al ser anunciados por otro AS.

Esta política llegó a consenso y fué ratificada por el directorio de LACNIC.

Actualmente LACNIC se encuentra en proceso de implementación de esta política.

RIPE NCC
RPKI Validator 3

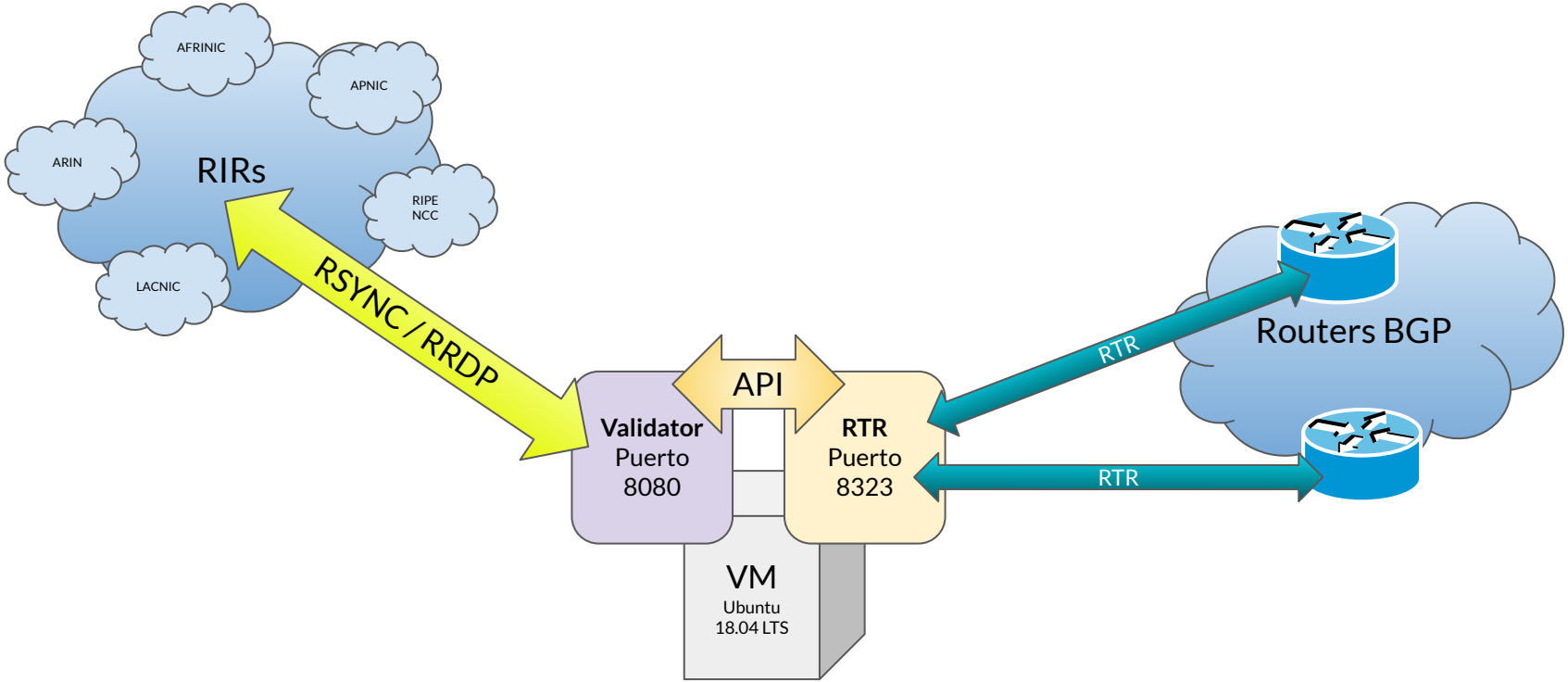
¿Qué necesito para instalar RIPE Validator?

- Una PC, servidor o máquina virtual.
  - 1 core de CPU (se recomienda 2+).
  - 2 gigabytes de RAM (se recomienda 4+ gigabytes).

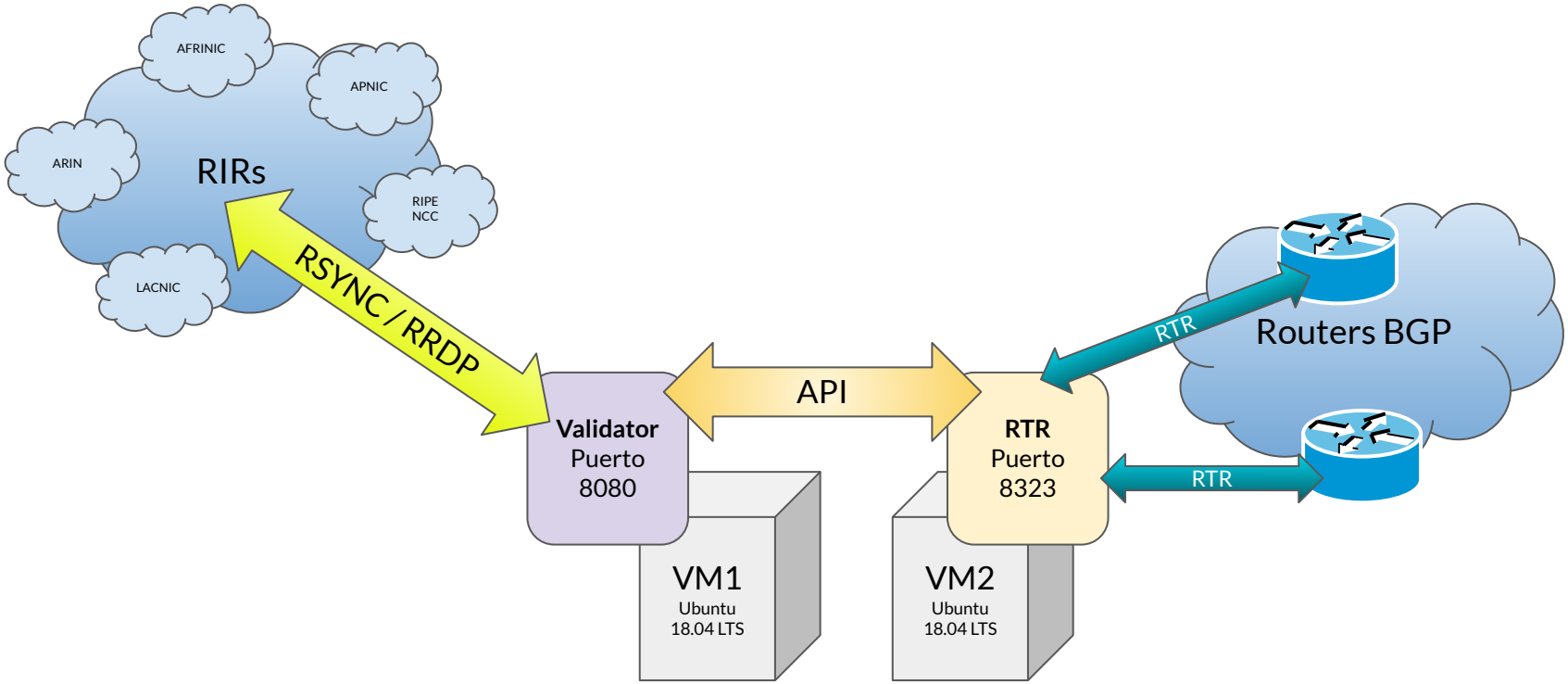
- En los ejemplos que mostraremos a continuación, usamos un sistema operativo recién instalado.
  - Ubuntu Linux 18.04 LTS Server (en una VM).
    - Durante la instalación, solo agregamos el paquete de SSH.
    - 2 Cores.
    - 4 GB de RAM (2,1 GB usados con todos los sistemas andando).
    - 20 GB de disco rígido (10 GB usados con todos los sistemas andando).
    - OpenJDK8+ y RSYNC.

- El RIPE Validator en su versión 3 se divide en dos procesos distintos.
  - El Validator, que obtiene los ROAs desde los RIRs y los procesa.
  - El Servidor RTR, que se comunica con los routers BGP que soportan RPKI.

RIPE NCC RPKI Validator 3



RIPE NCC RPKI Validator 3 (distribuído)



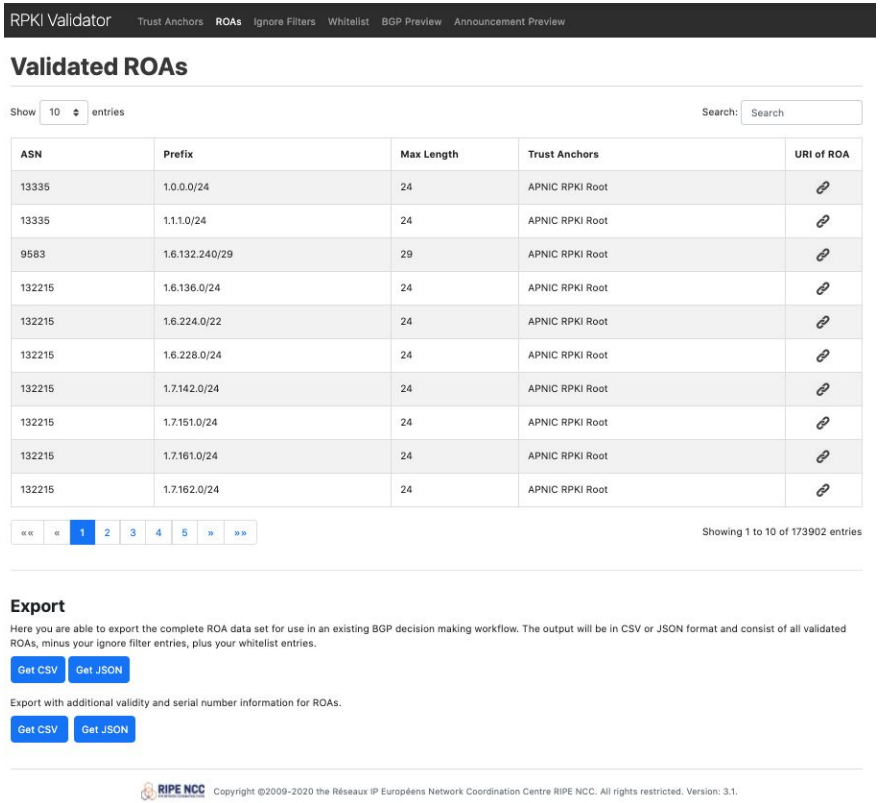
Panel de control de RIPE RPKI Validator 3

RPKI Validator | Trust Anchors | ROAs | Ignore Filters | Whitelist | BGP Preview | Announcement Preview

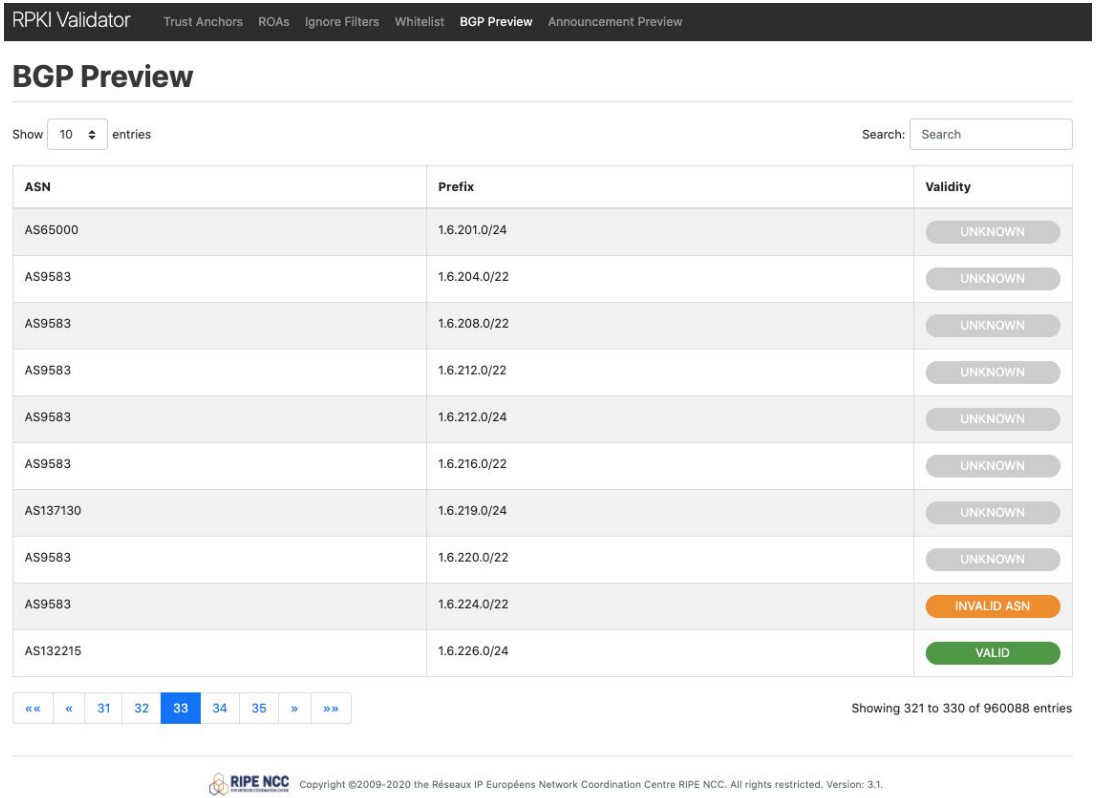
Configured Trust Anchors

Trust Anchors	Processed Items	Last Updated (UTC)
AfriNIC RPKI Root	1670 0 0	2020-08-24 23:48:59
APNIC RPKI Root	21379 0 3	2020-08-24 23:54:43
ARIN	17362 0 0	2020-08-24 23:53:29
LACNIC RPKI Root	10341 4 0	2020-08-24 23:54:41
RIPE NCC RPKI Root	55717 0 1	2020-08-24 23:26:14

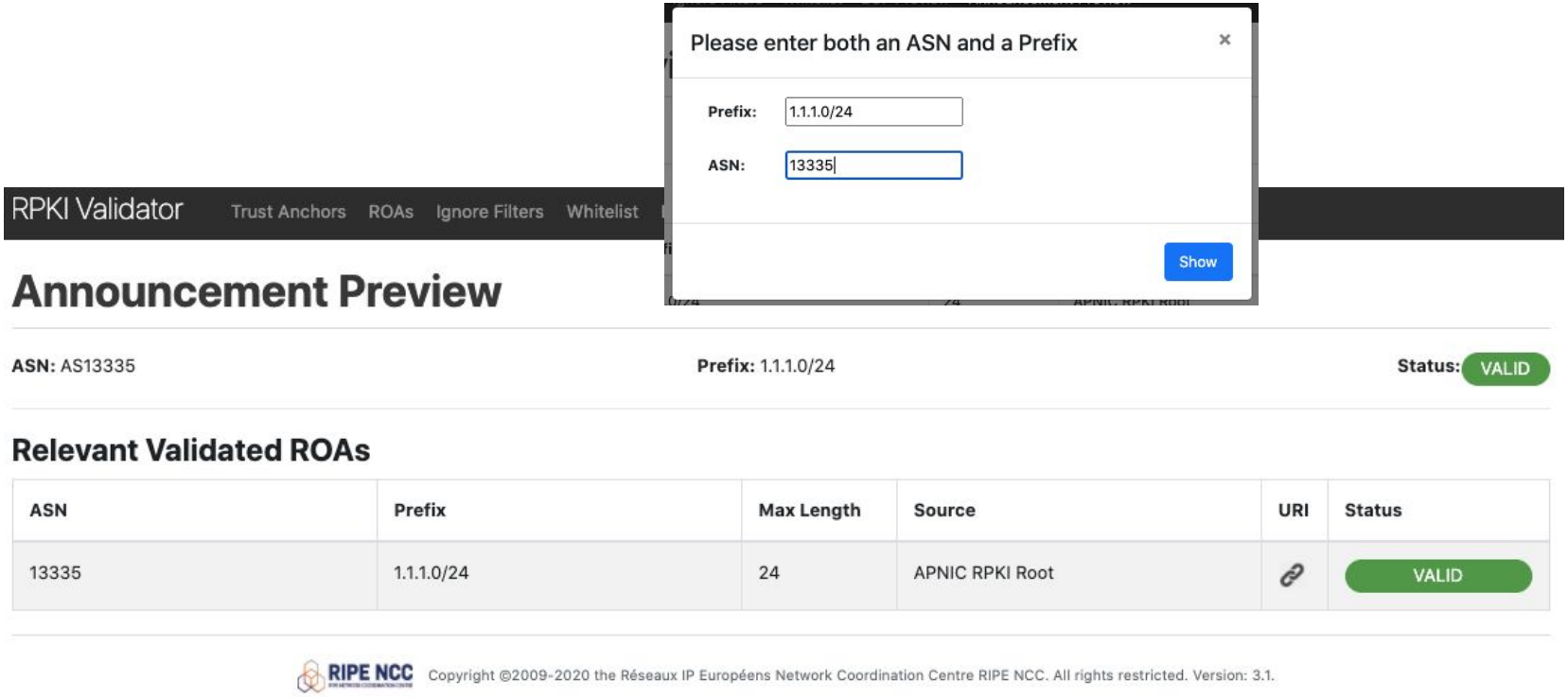
Panel de control de RIPE RPKI Validator 3



Panel de control de RIPE RPKI Validator 3



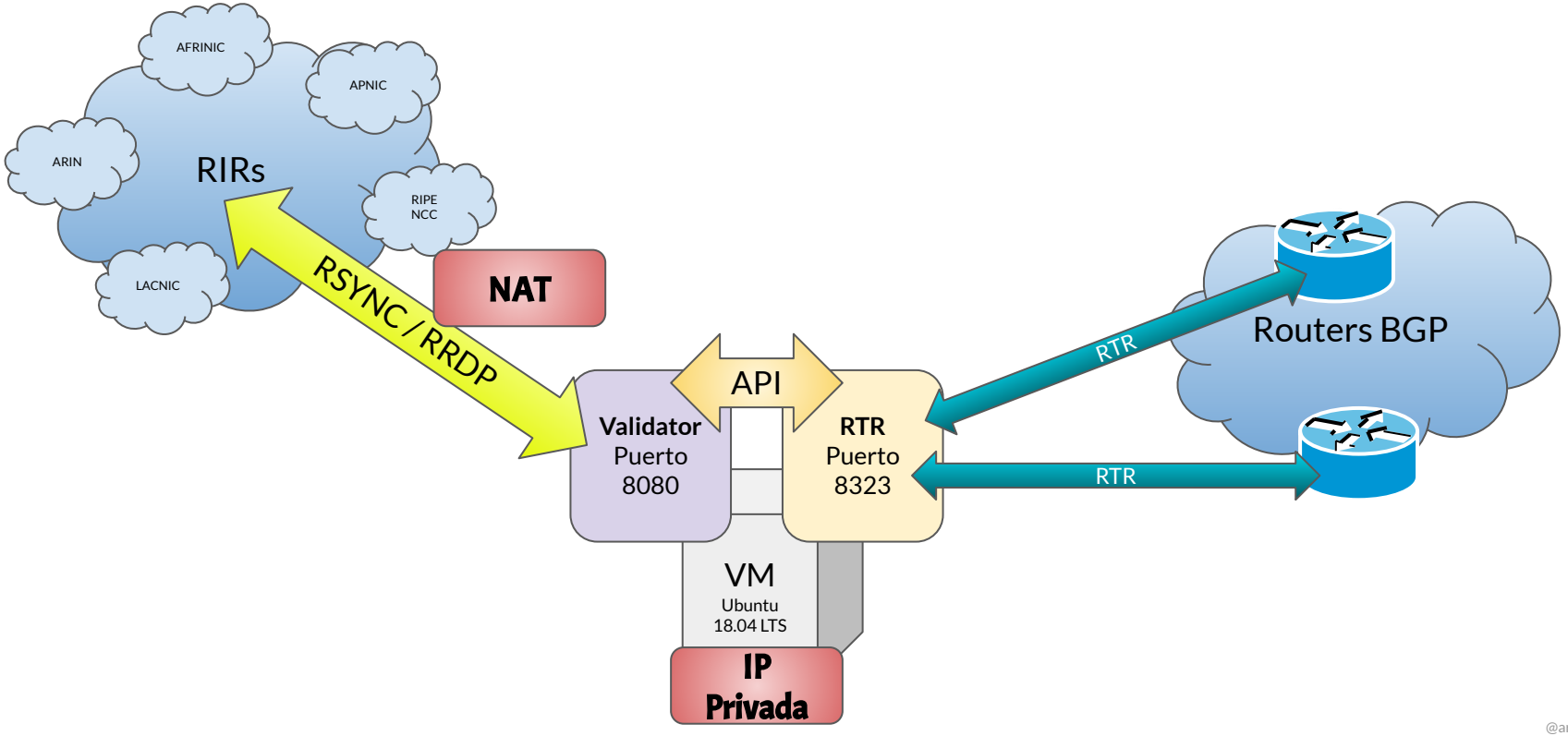
Panel de control de RIPE RPKI Validator 3



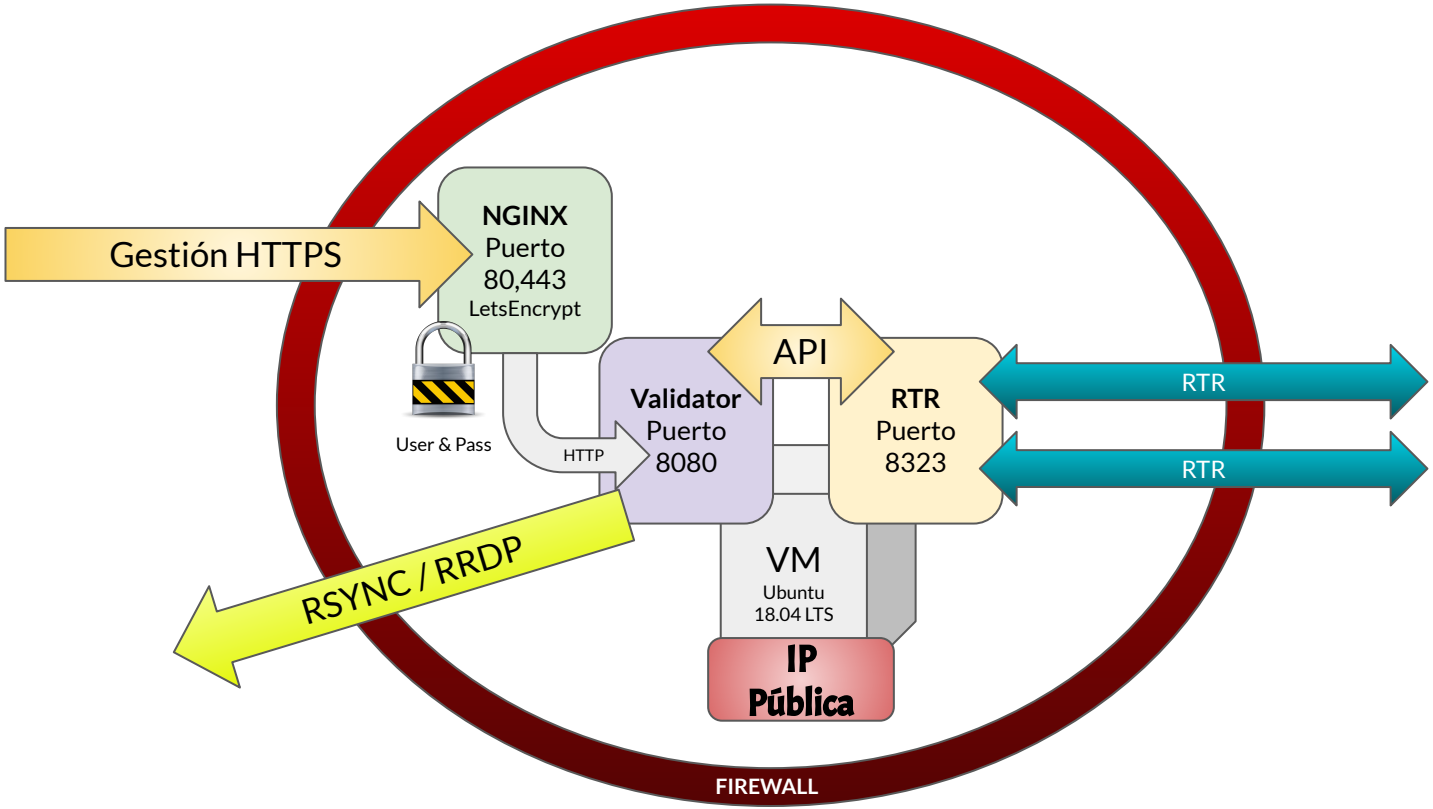
Instalación

http://bit.ly/lacnog-ripevalidator3

Instalación en una red totalmente privada



Instalación en una red pública



Instalación (6’ 20”)


```
 * Support:        https://ubuntu.com/advantage

  System information as of Tue Aug 25 00:57:00 UTC 2020

  System load:  0.06              Processes:           109
  Usage of /:   10.9% of 62.74GB  Users logged in:     0
  Memory usage: 4%                IP address for eth0: 181.199.160.43
  Swap usage:   0%

 * Are you ready for Kubernetes 1.19? It's nearly here! Try RC3 with
   sudo snap install microk8s --channel=1.19/candidate --classic

   https://microk8s.io/ has docs and details.

0 packages can be updated.
0 updates are security updates.


 _       _   ___ _   _ ___  ___
| |     / \ / __| \ | |/ _ \ / __|
| |    / _ \| |  |  \| | | | | _
| |___ / ___ \ |__| |\  | |_| | |_| |
|_____/_/   \_\____|_| \_|\___/ \____|

Este es un sistema privado y todo acceso sin autorizacion sera reportado y perseguido
por la ley. Por favor cierre sesion.

You have new mail.
Last login: Tue Aug 25 00:48:51 2020 from 172.30.0.1
```

Validación de Origen de Rutas usando RPKI Validator

Huawei

RPKI en Huawei

- Huawei Net Engine 40E M2K-B
- Versión de software V800R011C10 SPC100
  - Disponible desde V800 R009 C10

```
# Configuración básica (2 sesiones RTR máx)
rpki
 # Servidor RTR1
 session 198.18.88.10
  tcp port 8323
  timer aging 3600
  timer refresh 1200
  rpki-limit 512000 alert-only
 # Servidor RTR2
 session 2001:DB8:BEBA:CAFE::A
  tcp port 8323

# BGP
bgp 65000
ipv4-family unicast
 prefix origin-validation enable
 bestroute origin-as-validation allow-invalid
ipv6-family unicast
 prefix origin-validation enable
 bestroute origin-as-validation allow-invalid
#
```

Chequeando comunicación con el servidor RTR

```
[~rpki-test]display rpki session

 Total number of RPKI session : 2
 Session in up state : 2

  Session                    State          Age            IPv4/IPv6 record    VPN
  198.18.88.10               Established    2d19h43m59s    146339/24482        _public_
  2001:DB8:BEBA:CAFE::A      Established    3d23h02m20s    146339/24481        _public_

[~rpki-test]display rpki table

 Total number of RPKI record entry  : 292678

  Network                 Maxlen     OriginAS       Session                 VPN
  1.0.0.0/24              24         13335          198.18.88.10            _public_
  1.0.0.0/24              24         13335          2001:DB8:BEBA:CAFE::A   _public_
  1.1.1.0/24              24         13335          198.18.88.10            _public_
  1.1.1.0/24              24         13335          2001:DB8:BEBA:CAFE::A   _public_
[...]
```

Chequeando comunicación con el servidor RTR

```
[~rpki-test]display bgp routing-table

BGP Local router ID is 10.0.0.18
 Status codes: * - valid, > - best, d - damped, x - best external, a - add path,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 RPKI validation codes: V - valid, I - invalid, N - not-found


 Total Number of Routes: 612099
      Network            NextHop                MED        LocPrf    PrefVal Path/Ogn
[...]
 *>    I 2.58.228.0/24      10.0.0.17                                      0      64512 7049 3549 3356 6762 40676i
 *>    V 2.58.229.0/24      10.0.0.17                                      0      64512 7049 3549 3356 2914 40676i
 *>    I 2.58.230.0/24      10.0.0.17                                      0      64512 7049 3549 3356 6762 40676i
 *>    V 2.58.232.0/22      10.0.0.17                                      0      64512 7049 3549 3356 49544 62370i
 *>    V 2.58.242.0/24      10.0.0.17                                      0      64512 11664 19037 6762 2914 134522i
 *>    V 2.58.243.0/24      10.0.0.17                                      0      64512 11664 19037 6762 2914 134522i
 *>    N 2.58.244.0/22      10.0.0.17                                      0      64512 7049 6939 9312 41717i
 *>    N 2.58.248.0/22      10.0.0.17                                      0      64512 7049 6939 9312 41717i
```

Chequeando validez de un prefijo

ASN	Prefix	Validity
AS40676	2.58.230.0/24	INVALID ASN
AS137571	2.58.230.0/24	VALID

Click to see announcement preview

```
[~rpki-test]display bgp routing-table 2.58.230.0

 BGP local router ID : 10.0.0.18
 Local AS number : 65000
 Paths:   1 available, 1 best, 1 select, 0 best-external, 0 add-path
 BGP routing table entry information of 2.58.230.0/24:
 From: 10.0.0.17 (10.169.94.195)
 Route Duration: 0d01h47m29s
 Direct Out-interface: GigabitEthernet0/3/8
 Original nexthop: 10.0.0.17
 Qos information : 0x0
 Community: <759:101>
 AS-path 64512 7049 3549 3356 6762 40676, origin igp, pref-val 0, valid, external, best, select, pre 255, validation invalid
```

Chequeando validez de origen en los filtros

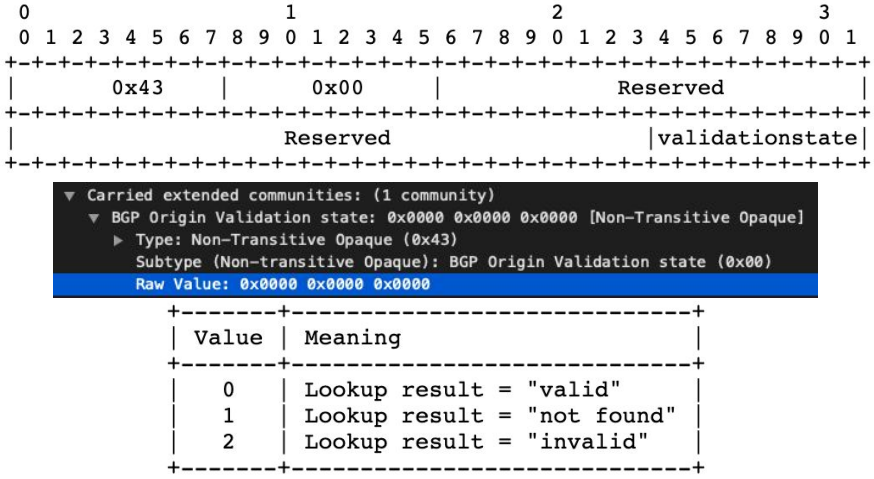
```
#
route-policy BGPin deny node 10
 if-match rpki origin-as-validation invalid
#
route-policy BGPin permit node 20
 if-match rpki origin-as-validation valid
 apply local-preference 110
#
route-policy BGPin permit node 30
 if-match rpki origin-as-validation not-found
 apply community 65000:1000 additive
#
route-policy BGPin deny node 1000
#
```

RPKI, Huawei y los Peers iBGP

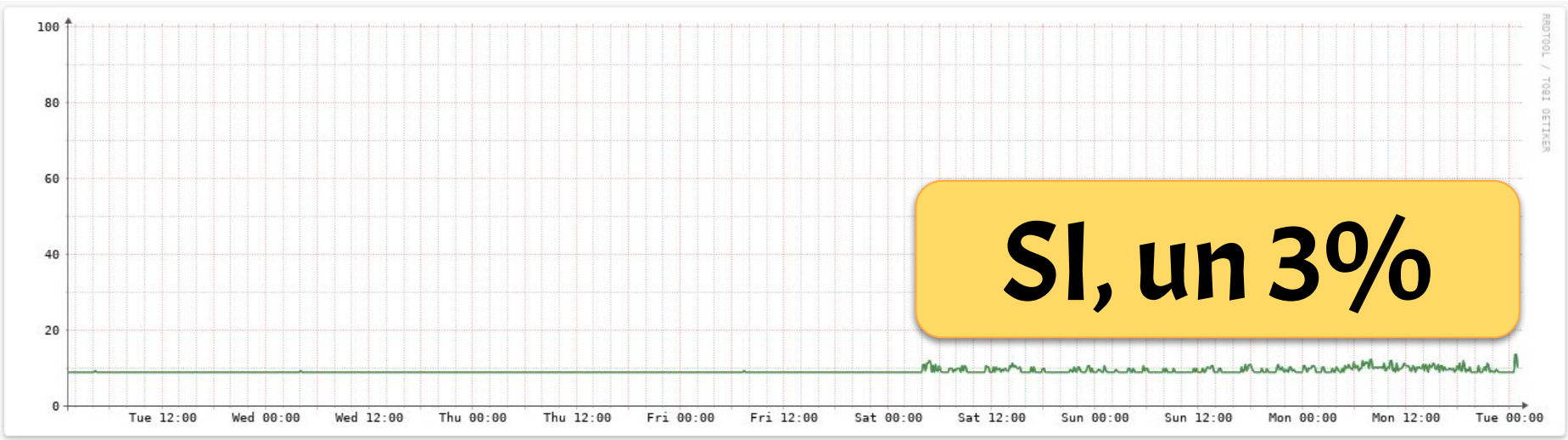
En Huawei todo lo que se aprende por iBGP por defecto es marcado como origen válido.

Si quiero transmitir mi información de validez de prefijos a mis peers de iBGP debo utilizar lo definido en RFC8097.

```
bgp 65000
 peer 10.0.0.22 as-number 65000
 #
 ipv4-family unicast
  prefix origin-validation enable
  bestroute origin-as-validation allow-invalid
  peer 10.0.0.22 enable
  peer 10.0.0.22 route-policy iBGPin import
  peer 10.0.0.22 route-policy iBGPout export
  peer 10.0.0.22 advertise-ext-community
# solo en peers iBGP
  peer 10.0.0.22 advertise origin-as-validation
```



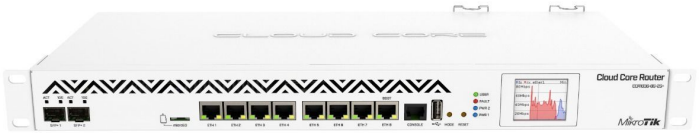
¿Esto afecta el consumo de recursos de mi equipo?



Validación de Origen de Rutas usando RPKI Validator

Mikrotik RouterOS v7.1beta2

RPKI en Mikrotik



- Mikrotik CCR 1036-8G-2S+
- Versión de software v7.1beta2
- BETA

RPKI es un feature que se viene pidiendo desde hace mucho tiempo en el foro oficial de Mikrotik.

Los desarrolladores han prometido soporte de RPKI para la versión 7, que aún está en desarrollo.

Se recomienda **NO UTILIZAR v7** en entornos de producción, dado que el software está incompleto.

Toda la configuración se realiza por consola o SSH, dado que Winbox aún no cuenta con los menúes que dan acceso a BGP y RPKI.

Mikrotik hizo en su v7 un rediseño absoluto del protocolo BGP, soportando cosas muy interesantes, tales como un draft de IETF titulado "*`Route Leak Prevention using Roles in Update and Open messages`*", entre otros.

En el laboratorio hemos enviado la tabla mundial de BGP en el AF IPv4 unicast, y hemos interconectado el equipo contra dos Validadores igual que en el caso de Huawei.

Configuración de RPKI en Mikrotik v7

```
# Conectar con los RTR
/routing bgp rpki add address=198.88.18.10 group=RPKITest port=8323
/routing bgp rpki add address=2001:db8:beba:cafe::a group=RPKITest port=8323

# Crear Filtros
# En la versión actual no tenemos todavía el soporte de alterar local-preference como en el ejemplo anterior
/routing filter rule
add chain=BGPin rpki-verify=RPKITest
add action=reject chain=BGPin match-rpki=invalid
add action=accept chain=BGPin match-rpki=valid
add action=accept chain=BGPin match-rpki=unknown

# Crear Peering
/routing bgp template
set default as=65000 input.filter=BGPin multihop=yes
/routing bgp connection
add listen=yes local.address=10.0.0.22 .role=ibgp remote.address=10.0.0.21 template=default
/routing bgp connection
add listen=yes local.address=172.30.0.2 .role=ebgp remote.address=172.30.0.1 template=default
```

Chequeos


```
[admin@RPKITEST] /routing/bgp/rpki> print
Flags: X - disabled
 0   group=RPKITest address=198.18.88.10 port=8323
 1   group=RPKITest address=2001:db8:beba:cafe::a port=8323

[admin@RPKITEST] /routing> rpki-check origin-as=13335 prfx=1.1.1.0/24 group=RPKITest
    valid
[admin@RPKITEST] /routing> rpki-check origin-as=15169 prfx=8.8.4.0/24 group=RPKITest
    unknown
[admin@RPKITEST] /routing> rpki-check origin-as=13335 prfx=103.21.244.0/24 group=RPKITest
    invalid
```

En el */ip route print* actualmente no se pueden ver los detalles de validación RPKI, la única manera de ver las inválidas (si las aceptamos) es cambiando algún atributo como por ejemplo cambiar el tipo de ruta a 'blackhole'.

Q&A

http://bit.ly/listadecorreo-lacnog

FACEBOOK: @LACNOG
https://www.facebook.com/Lacnog/

TWITTER: @LACNOG
https://twitter.com/LACNOG

LINKEDIN: LACNOG
https://www.linkedin.com/in/lacnog-b776291a7/

INSTAGRAM: @LACNOGLAT
https://www.instagram.com/lacnoglat/

¡Muchas gracias por participar!

Los esperamos en los próximos webinars