Normas de Mutuo Acuerdo para el Enrutamiento Seguro (MANRS)

Guía de Implementación

Versión 1.0, series BCOP
Fecha de publicación: 25 de enero de 2017

Índice

1. Que es un BCOP?

BCOP, por sus siglas en inglés, Best Current Operational Practices es un documento que describe las mejores prácticas actuales para un tema en particular, en acuerdo por los expertos en la materia del asunto en cuestión, y revisado periódicamente por la comunidad de Internet.

2. Resumen

Las BCOP de las "Mutually Agreed Norms for Routing Security" (MANRS) ["Normas de Mutuo Acuerdo para el Enrutamiento Seguro"], proveen una guía para facilitar el desarrollo de las medidas requeridas por MANRS y están orientadas para las redes "stub" (redes terminales) y pequeños proveedores y las redes de los clientes que tiene una conexión única activa hacia Internet. El documento también debe ayudar a revisar si la configuración de la red cumple con MANRS.

3. MANRS

A lo largo de la historia de Internet, la colaboración entre los participantes y la responsabilidad compartida por su buen funcionamiento y operación han sido los dos pilares de soporte para el tremendo crecimiento y éxito de Internet hoy en día, así como de su seguridad y resiliencia. Las soluciones tecnológicas son un elemento escencial aquí, pero la tecnología por sí sola no es suficiente. Para estimular mejoras visibles en esta área, se necesita generar un gran cambio hacia la cultura de responsabilidad colectiva.

Como tal, hacemos un llamado a los operadores de red alrededor del mundo a que se unan a la Iniciativa de Routing Resilience Manifesto, y a que entren en acuerdo con los principios de Normas de Mutuo acuerdo para Enrutamiento Seguro (MANRS por sus siglas en inglés).

3.1. Los Principios de MANRS

- Nosotros (los ISP/ Operadores de Redes) reconocemos la naturaleza interdependiente del sistema global de enrutamiento y nuestro rol en contribuir a una Internet segura y su resiliencia.
- Nosotros incorporaremos las mejores prácticas actuales vinculadas con el enrutamiento seguro y con su resiliencia en nuestros procesos de gestión de redes, acorde con nuestas acciones.

- Nosotros estamos comprometidos con prevenir, detectar y mitigar incidentes de enrutamiento mediante la colaboración y coordinación con otros pares y con otros ISPs alineados con las acciones.
- Nosotros animamos a nuestros pares y a nuestros clientes a adoptar estas Acciones y Principios.

3.2. Las Acciones de MANRS

1. Filtración – Previniendo la propagación de información de enrutamiento incorrecta.
   - Operador de Red define Políticas de enrutamiento claras e implementa un sistema que asegura la exactitud de sus anuncios y los anuncios de sus clientes hacia las redes adyacentes, conteniendo información granular de los prefijos y AS-path.
   - Operador de Red es capaz de comunicarse con las redes adyacentes cuyos anuncios son correctos.
   - Operador de Red se aplica con debida diligencia cuando revisa la exactitud de los anuncios de sus clientes, específicamente que los anuncios de sus clientes sean los legítimos usuarios de los ASN y prefijos que anuncian.
2. Anti-Spoofing – Previniendo tráfico con direcciones IP origen suplantadas.
   - Operador de Red implementa un sistema que habilita la validación de direcciones origen por lo menos para las redes de los clientes que tienen una conexión única activa hacia Internet (stub-Network), las redes de sus propios usuarios y las redes de su infraestructura. Operadores de Red implementa filtración de anti-suplantación para prevenir que paquetes con direcciones IP origen suplantadas, entren o salgan de la red.
3. Cooordinación – Facilitando la comunicación operacional global y la coordinación entre los operadores de Red.
   - Operador de Red mantiene Información de contacto actualizada y accesible globalmente.
4. Validación Global – Facilitando la validación de la información de enrutamiento a escala global.
   - Operador de Red publica documentación de las politicas de enrutamiento, ASNs y prefijos que se pretenden anunciar a terceros.

3.3. Convirtiéndose en Miembro de MANRS

Operadores de Red que estén de acuerdo con los Principios e Implementen al menos una de las Acciones (pero no sólo la Acción de Coordinación) pueden convertirse en Miembros de MANRS. Esto los acredita a usar la insignia MANRS, serán listados en el sitio Web de *routingmanifiesto.org* y podrán contribuir a este documento y otros documentos afines.

Las recomendaciones propuestas, referidas como Acciones en la documentación de MANRS y en este BCOP, habla acerca de los casos más comunes, y están diseñadas para minimizar los costos y riesgos incurridos cuando se implementan. Cualquier Acción en particular no es una solución exhaustiva al problema expuesto.

4. Líneas guía de implementación para las Acciones de MANRS

La selección de acciones se basó en una evaluación del balance entre pequeños, costos individuales incrementales y el potencial beneficio común. Ellos definen una línea base de seguridad mínima. Cualquier Acción particular no es una solución exhaustiva a los problemas descritos.

Para ejemplos de configuración, se usa una topología simple, presentada en la figura 1.

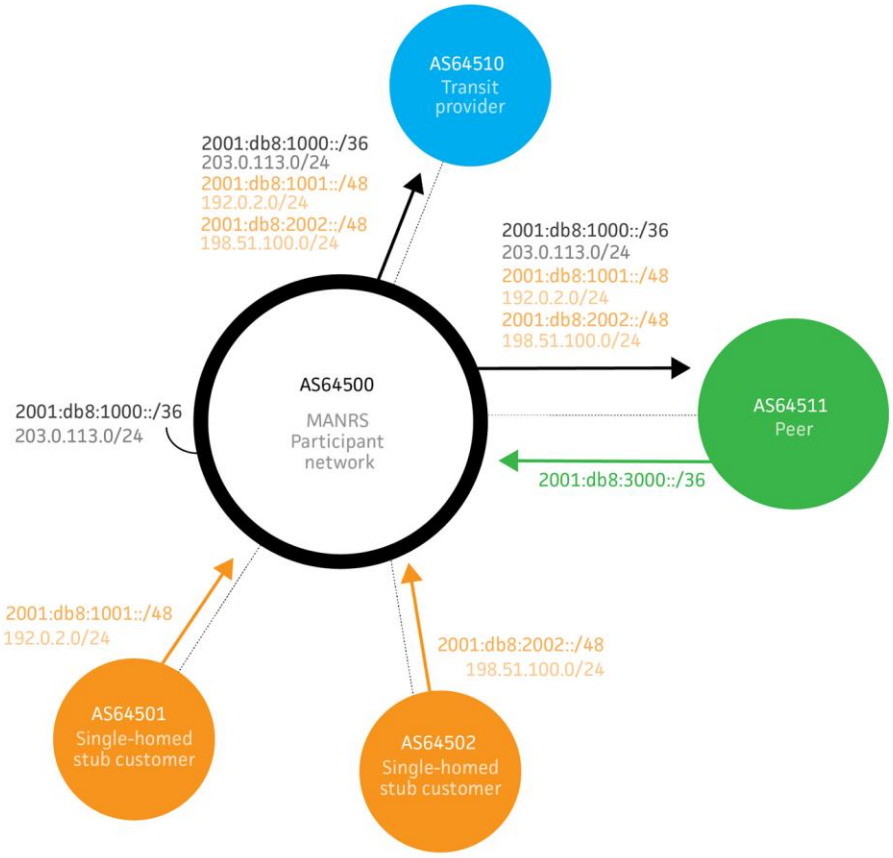


Fig. 1. Topología de red simple

El objetivo es asegurar que los operadores de red tengan información de contacto precisa para que puedan contactarse entre sí cuando sea necesario; que el tráfico que sale de su red use direcciones de red origen válidas, y que toda la información de enrutamiento que es intercambiada entre sistemas autónomos es correcta y que puede ser verificada.

4.1. Coordinación – Facilitando la comunicación operacional global y la coordinación entre operadores de red

Acciones MANRS relevantes que se esperan:

- Los operadores de red mantienen información de contacto actualizada y accesible globalmente

La información de contacto actualizada y de acceso público es esencial para promover la comunicación y la colaboración entre operadores de red. Se aconseja a los operadores de red mantener su información de contacto en lugares comunes tales como PeeringDB, en objetos registrados en bases de datos WHOIS de RIR, tales como RADB and RIPE, así como también en su sitio web público. Como mínimo, un operador de red debería registrar y mantener información de contacto 24/7 en al menos una de estas bases de datos. Esta información de contacto debería incluir la información de punto de contacto actual del operador para el NOC de su ASN, todos los bloques de red y nombres de dominio. La información adicional es bien recibida y recomendada, como por ejemplo documentación de la política de enrutamiento en un IRR e información de contacto en una página web pública, proveer una URL de *looking glass* público en el campo apropiado de su registro PeeringDB, etc.

A continuación, se detallan estos lugares comunes junto con recomendaciones sobre cual información debería mantenerse y cómo puede presentarse. Como mínimo, un operador de red debería registrar y mantener información de contacto 24/7 en al menos uno de estos recursos.

4.1.1. Manteniendo Información de Contacto en Registros Regionales de Internet (RIRs): AFRINIC, APNIC, RIPE

Mientras que todos estos RIRs requieren que los registrantes mantengan su información de contacto primaria actualizada, los RIRs también ofrecen la capacidad de agregar contactos adicionales e información de contacto para registros en sus bases de datos. Se anima a los operadores a agregar/mantener la información de contacto de NOC de donde ellos tienen objetos

RIR. También se anima a los operadores a hacer uso de los campos ´remark´ [comentarios] (cuando aplique) para ayudar más a los usuarios a hacer más fácil de obtener la información de contacto u otra información útil.

AFRINIC, APNIC y RIPE mantienen un sistema *whois* que combina el registro de recursos de Internet con su propio Registro de Enrutamiento de Internet. Para los objetos en estas bases de datos, los operadores deben crear/mantener un objeto de rol NOC e incluir dicho objeto en el atributo "tech-c" de los objetos AUT-NUM, INETNUM, INET6NUM, AS-SET y ROUTE-SET. El uso del atributo 'remarks' también se considera para documentar información de contacto, y puede ser agregado a los tipos de objetos mencionados antes, así como también a los objetos ROUTE y ROUTE6 (discutido más adelante).

4.1.1.1. Objetos MNTNER

Un objeto mantenedor (o MNTNER) en una base de datos de IRR se usa para administrar la autorización y autenticación. Otros objetos se refieren a mantenedores usando, por ejemplo, uno o más atributos "mnt-by". Tal atributo proteje esos objetos mediante permitir únicamente cambios cuando el actualizador se puede autenticar a sí mismo como uno de los mantenedores.

4.1.1.1.1. Creación de un nuevo mantenedor en el IRR AFRINIC

Para crear un nuevo mantenedor en el IRR AFRINIC primero se necesita una persona existente o un objeto de rol que se use como contacto para el mantenedor. El RIR AFRINIC permite crear un objeto persona y/o rol que no esté protegido por un mantenedor. Mientras que no se recomienda información sin protección en el IRR, sí provee un punto de inicio. Primero se crea un objeto PERSON en la base de datos enviando un correo electrónico a auto-dbm@afrinic.net con un texto como el siguiente:

```
person:    Some Random Person
address:   Somewhere
           7300 XX Apeldoorn
           The Netherlands
phone:     +31-55-0000000
e-mail:    someone@example.com
nic-hdl:   AUTO-1
notify:    someone@example.com
changed:   someone@example.com
source:    AFRINIC
```

El '*nic-hdl*' especifica el identificador al que otros objetos pueden referirse. Al especificar AUTO-1 durante la creación, el sistema genera un identificador único de forma automática, el cual se verá

en el correo electrónico de confirmación que se recibe de la base de datos, después de que el objeto ha sido creado. En este ejemplo, se asume que el nuevo identificador es “SRP9999-AFRINIC”

Ahora que se tiene una persona de contacto en la base de datos, puede crearse un mantenedor enviando un correo electrónico a auto-dbm@afrinic.net con un texto como el siguiente:

```
mntner:     MAINT-AS64500
descr:      Some Random Person’s maintainer
admin-c:    SRP9999-AFRINIC
upd-to:     someone@example.com
auth:       MD5-PW $1$cu/QEuCu$qKl69lv4c4t0by7XNQqRX.
mnt-by:     MAINT-AS64500
changed:    someone@example.com
source:     AFRINIC
password:   SomePassword
```

El atributo “auth:” contiene el hash de la contraseña, el cual se puede crear en http://www.afrinic.net/services/ip-tools/whoiscrypt. El método CRYPT-PW, ya no es considerado seguro, por lo que no debe usarse.

Este ejemplo usa un atributo *mnt-by* que hace referencia a sí mismo. Esto significa que los datos para este mantenedor están protegidos por él mismo. Para probar que realmente está autorizado para crear el mantenedor, se tiene que proveer, como un atributo adicional, la contraseña que coincida con el atributo *auth,* al enviar la actualización. Este atributo de la contraseña no se almacenará en la base de datos IRR.

Ahora que se tiene un MNTNER, es necesario proteger con él al objeto PERSON; de otro modo, cualquiera podría hacerle modificaciones. Para actualizar un objeto existente, se envia una versión modificada del objeto a auto-dbm@afrinic.net:

```
person:     Some Random Person
address:    Somewhere
            7300 XX Apeldoorn
            The Netherlands
phone:      +31-55-0000000
e-mail:     someone@example.com
nic-hdl:    SRP9999-AFRINIC
notify:     someone@example.com
mnt-by:     MAINT-AS64500
changed:    someone@example.com
source:     AFRINIC
password:   SomePassword
```

En este ejemplo, se agrega un atributo *mnt-by* para proteger a la persona. Recordar usar el *nic-hdl* real para la persona al enviar la actualización, de manera que la base de datos IRR sepa actualizar el objeto persona en lugar de crear uno nuevo. Para mostrar que se está autorizado para agregar este mantenedor también se debe proveer la contraseña del mismo al enviar la actualización. De nuevo, este atributo de la contraseña no será almacenado en la base de datos IRR.

Ahora se tiene un PERSON (nic-hdl: SRP99999-AFRINIC) y un mantenedor (mntner: MAINT-AS64500) el cual puede usarse para publicar más información en el IRR.

4.1.1.1.2. Creación de un nuevo mantenedor en el IRR APNIC

APNIC automáticamente crea un objeto mantenedor y rol para todos los nuevos miembros. Si los miembros desean crear un nuevo objeto mainteiner, lo pueden crear por medio del portal MyAPNIC en https://myapnic.net: MyAPNIC → Resources → Whois updates → Add → Mnter

4.1.1.1.3 Creación de un nuevo mantenedor en el IRR RIPE

El IRR RIPE no permite objetos sin protección. Por tanto, no es posible crear primero un objeto PERSON y luego crear un MNTNER que referencie a esa persona. Tampoco es posible crear primero un MNTNER porque necesita una referencia a un PERSON.

Para resolver este problema, el NCC de RIPE provee una interfaz web para crear una persona y un mantenedor al mismo tiempo en:
http://apps.db.ripe.net/db-web-ui/#/webupdates/create/person/self.
Para poder acceder a esta página se necesta tener una cuenta de acceso RIPE NCC, la cual puede crearse en https://access.ripe.net/registration.

El mantenedor es automáticamente vinculado a la cuenta de acceso, de modo que se es autenticado de forma automática como ese mantenedor al editar objetos IRR por medio de la interfaz web. También se puede editar el mantenedor y agregar un atributo “auth: MD5-PW”; eso permite enviar actualizaciones por medio de correo electrónico a auto-dbm@ripe.net en la misma forma que se describió antes para el IRR AFRINIC.

4.1.1.2 Objetos ROLE

Los objetos PERSON son puntos importantes de contacto, especialmente en organizaciones muy pequeñas, aunque también son muy limitados para una estructura organizacional más compleja.

En muchos casos el punto de contacto apropiado es un departamento, una función laboral o un grupo de personas. Por ello, el sistema IRR soporta objetos ROLE.

Un objeto ROLE puede referenciarse donde sea que un objeto PERSON pueda. Ambos se identifican por su atributo *nic-hdl.* La ventaja de usar un objeto ROLE es que mientras las personas pueden cambiar de empleo y moverse a una organización diferente, un rol no cambia. Un objeto ROLE puede, de hecho, opcionalmente, referir a otro objetos PERSON, agregando información sobre personas de contacto para un grupo específico o un departamento.

Este es un ejemplo de un típico objeto ROLE el cual utiliza el atributo *"remarks"* para brindar información adicional. En este ejemplo, el operador de red provee detalles de contacto para el objeto "*role*", pero también provee información de resumen en el atributo *"remarks"* no sólo para información de su NOC, sino para sus contactos de abuso y seguridad, y una URL a la página de información PeeringDB del operador:

```
role:           AS64500 NOC
remarks:        NOC: noc@example.net
remarks:        Security issues: security@example.net
remarks:        https://as64500.peeringdb.com/
e-mail:         noc@example.net
abuse-mailbox:  abuse@example.net
nic-hdl:        AS64500NOC-RIPE
mnt-by:         MAINT-AS64500
created:        2012-10-27T12:14:23Z
last-modified:  2016-02-27T12:33:15Z
source:         RIPE
```

4.1.1.3. Objetos INETNUM y INET6NUM

Los IRRs se usan para documentar información sobre recursos, tales como bloques de direcciones IP y números de sistemas autónomos (AS). Los bloques IPv4 y prefijos IPv6 se documentan usando objetos INETNUM y INET6NUM.

El objeto ROLE anterior se referencia en el atributo 'tech-c' en este ejemplo de objeto INET[6]NUM. El atributo 'remarks' también provee información adicional.

```
inet6num: 2001:db8::/32
netname:        EXAMPLE-NET
descr:          An example allocation
remarks:        NOC: noc@example.net
remarks:        Security issues: security@example.net
remarks:        https://www.peeringdb.com/asn/64500
country:        CH
status:         ALLOCATED PA
```

```
org:            ORG-AS64500-RIPE
admin-c:        AS64500NOC-RIPE
tech-c:         AS64500NOC-RIPE
mnt-by:         RIPE-NCC-HM-MNT
mnt-lower:      MAINT-AS64500
mnt-routes:     MAINT-AS64500
created:        2012-10-27T12:14:23Z
last-modified:  2016-02-27T12:33:15Z
source:         RIPE
```

Los IRRs que son vinculados a la base de datos RIR no permiten que los usuarios creen sus propias asignaciones de nivel superior. Esas se crean automáticamente por el RIR y a menudo sólo se pueden editar a través de su portal web.

En el ejemplo dado arriba puedes ver que el mantenedor para el objeto es RIPE-NCC-HM-MNT, el mantenedor del mismo RIPE NCC. Como usuario, solamente se permite mantener (crear) objetos de nivel inferior, tales como las tareas que se hacen desde esta asignación y objetos ROUTE/ROUTE6 para documentar prefijos de enrutamiento.

4.1.1.4. Objetos AUT-NUM

Los números AS (ASNs) se documentan usando objetos AUT-NUM. Estos objetos contienen información sobre el ASN y sus políticas de *peering.* El nivel de detalle que las organizaciones publican en sus objetos AUT-NUM varía. Esta sección se enfoca en la información de contacto. Para información sobre publicación de políticas de enrutamiento y su uso para validación de información de enrutamiento consultar las secciones 4.3 y 4.4.

Ejemplo de un objeto AUT-NUM mínimo, es:

```
aut-num: AS64500
descr:          Provider 64500
mp-import:      from AS64510 accept ANY except FLTR-BOGONS
mp-export:      to AS64510 announce AS64500:AS-ALL
admin-c:        AS64500NOC-RIPE
tech-c:         AS64500NOC-RIPE
mnt-by:         MAINT-AS64500
created:        2012-10-27T12:14:23Z
last-modified:  2016-02-27T12:33:15Z
source:         RIPE
```

4.1.2. Mantenimiento de la información de contacto en Registros Regionales de Internet (RIRs): LACNIC

LACNIC usa un sistema diferente en donde los propietarios de recursos pueden actualizar su información de contacto a través de la interfaz web de lacnic.net. A pesar de que el formato de la información se ve igual que en los IRRs, hay diferencias significativas. Por ejemplo, no hay tipo de objeto INET6NUM, ambos espacios de direccionamiento IPv4 e IPv6 usan INETNUMs. Los atributos posibles para los tipos de objetos también son diferentes.

La información de contacto puede actualizarse en el sistema administrativo de LACNIC: http://lacnic.net/cgi-bin/lacnic/stini.
Al iniciar sesión con el userID se puede acceder información sobre el usuario personal, información de la organización e información de recursos.

- En la pestaña "ID UPDATE[userID]" se puede actualizar información sobre el usuario personal.
- Haciendo click en cualquier organización bajo la sección "Entities" se podrá cambiar el POC (*Point of Contact* -Punto de Contacto) de dicha identidad (POC del administrador, POC de facturación y/o POC de membresía).
- Finalmente, todavía en la organización seleccionada, se podrá cambiar el POC técnico o de abuso de un recurso específico asociado a tal organización haciendo click en el ASN o bloque IP deseado.

Nuevos POCs se deben crear previamente en www.lacnic.net/newid.

Con el objeto de modificar información general sobre la organización, se debes enviar un correo electrónico a hostmaster@lacnic.net.

Ejemplo de registro POC:

```
nic-hdl:   SRA
person:    Sergio Rojas Astigarraga
e-mail:    sergio@LACNIC.NET
address:   Rambla Rep. de México, 6125,
address:   1400 - Montevideo -
country:   UY
phone:     +598 2 6042222 []
created:   20090904
changed:   20161205
```

Ejemplo Org:

```
owner:          LACNIC DEBOGON TESTER
ownerid:        UY-OPPL-LACNIC
responsible:    Sergio Rojas
address:        Rambla Republica de México, 1234,
address:        11400 - Montevideo - MV
country:        UY
phone:          +598 2 6041111 []
owner-c:        SRA
created:        20100222
changed:        20161205

nic-hdl:        SRA
person:         Sergio Rojas Astigarraga
e-mail:         sergio@LACNIC.NET
address:        Rambla Rep. de México, 6125,
address:        1400 - Montevideo -
country:        UY
phone:          +598 2 6042222 []
created:        20090904
changed:        20161205

aut-num:        64500
inetnum:        2001:db8:1000::/36
inetnum:        203.0.113.0/24
```

4.1.3. Mantenimiento de la información de contacto en Registradores Regionales de Internet (RIRs): ARIN

Para ARIN, el proceso para crear contactos es ligeramente diferente al de los ejemplos antes descritos para AFRINIC/APNIC/RIPE y LACNIC. Para los registros de ARIN, un operador debe crear primero un registro de Punto de Contacto (POC) en su base de datos. Una vez que el POC ha sido creado, el operador puede asociar el registro del POC a los recursos de su red (ASN, direcciones IP) como un POC de NOC.

4.1.3.1. Ejemplo de objeto Punto de Contacto (POC):

Este es un ejemplo típico de cómo se ve un registro de POC para un registro de ARIN:

```
Name:           Example ISP NOC
Handle:         EXAMPLENOC-ARIN
Company:        Example ISP
Address:        123 X Street
City:           New York
StateProv:      NY
PostalCode:     10011
Country:        US
RegDate:        2015-01-01
Updated:        2015-01-01
Phone:          +1-800-555-1212
```

```
Email:          noc@example.net
```

4.1.3.2. OrgNOCHandle en el ejemplo de objeto Network:

Lo siguiente aparecería en los resultados de búsquedas *whois* para el ASN y recursos de red de un operador, después de que el POC se ha configurado como un contacto de NOC:

```
OrgNOCHandle:    EXAMPLENOC-ARIN
OrgNOCName:      Example ISP NOC
OrgNOCPhone:     +1-800-555-1212
OrgNOCEmail:     noc@example.net
OrgNOCRef:       https://whois.arin.net/rest/poc/EXAMPLENOC-ARIN
```

4.1.4. Mantenimiento de Información de Contacto en Registros de Enrutamiento de Internet

Puesto que los Registros de Enrutamiento de Internet se usan para validar información de enrutamiento, es importante también mantener actualizada la información de contacto para esos objetos.

Para crear/mantener un contacto de NOC y agregarlo como un atributo 'tech-c' en los objetos AUT-NUM, AS-SET y ROUTE-SET en un registro de ruta, por favor referirse a los ejemplos de AFRINIC/APNIC/LACNIC/RIPE bajo Registros Regionales de Internet.

Los objetos ROUTE/ROUTE6 no permiten el atributo 'tech-c'. La forma recomendada para agregar/mantener información de contacto de un objeto ROUTE es usar el atributo 'remarks' para hacer esta información fácilmente accesible. Por ejemplo:

```
route6:          2001:db8:1000::/36
descr:           Provider 64500
origin:          AS64500
remarks:         Abuse/UCE: abuse@example.net
remarks:         Network: noc@example.net
remarks:         Security issues:
                 security@example.net
remarks:         https://as64500.peeringdb.com/
mnt-by:          MAINT-AS64500
created:         2012-10-27T12:14:23Z
last-modified:   2016-02-27T12:33:15Z
source:          RIPE
```

Para propósitos de depuración es útil documentar una dirección IP que sea alcanzable con *ping* desde el exterior y un contacto para preguntas sobre esa dirección:

```
route6:          2001:db8:1000::/36
descr:           Provider 64500
origin:          AS64500
pingable:        2001:db8:1000::1
```

```
ping-hdl:        AS64500NOC-RIPE
mnt-by:          MAINT-AS64500
created:         2012-10-27T12:14:23Z
last-modified:   2016-02-27T12:33:15Z
source:          RIPE
```

4.1.5. Mantenimiento de Información de Contacto en PeeringDB

PeeringDB (https://www.peeringdb.com) es una fuente abierta para que las redes compartan entre ellas su información de par (*peering*) y otra información relevante. Las redes son las responsables de mantener sus registros en la base de datos. Tener un registro en PeeringDB le permite consolidar la información de su red en una sola ubicación, y como operador, le permite investigar otras redes y obtener información adicional tal como enlaces al *looking glass* del operador, lo que facilita su *peer in*, información de contacto, etc.

Hay tres pasos principales para preparar un nuevo registro en PeeringDB:

1) Definición de una cuenta de usuario
    1) Haga click en "Register" desde el encabezado o visite https://www.peeringdb.com/register para comenzar el proceso.
2) Validación del ASN
    1) Se asocia la cuenta de usuario con una organización.
    2) La asociación entre el usuario y la organización será validada por el equipo de PeeringDB para nuevas organizaciones.
    3) El administrador del equipo de PeeringDB intentará validar su petición.
    4) Se enviará un correo electrónico de confirmación cuando su organización sea aprobada.
3) Preparación de su registro inicial de PeeringDB
    1) Iniciar sesión con la cuenta de usuario creada.
    2) Hacer click en el icono de navegación ubicado en la esquina superior derecha y seleccionar la organización.
    3) Completar y guardar la información básica de la organización.
    4) Navegar hacia el final de la pantalla, hacia la sección "Manage" y seleccionar "Add Network".
    5) Completar el formulario de "Add Network" y hacer click en "Submit Network".
    6) La red será revisada por el equipo de PeeringDB antes de que esté disponible públicamente.
4) Agregar detalles al registro de PeeringDB
    1) Iniciar sesión con la cuenta de usuario creada.

2) Hacer click en el ícono de navegación ubicado en la esquina superior derecha y seleccionar la organización.
3) Navegar hacia el final de la pantalla a la sección "Networks" y seleccionar su red.
4) Aparecerá la vista estándar de PeeringDB para una red. Hacer click en el botón "Edit" para actualizar la información en la página.
5) Desde la vista "Edit", se puede hacer lo siguiente:
    1) Administrar contactos – Ingresar la información de contacto para los contactos importantes de la red, tales como el NOC, el equipo de seguridad y el contacto de la política de *peering*.
    2) Agregar información secundaria – Información como la URL de *Looking Glass*, número de rutas, etc.
    3) Administrar instalaciones de *peering* privados – Estas son ubicaciones donde un operador puede asociarse (*peer*) a la red.
    4) Administrar puntos de intercambio – Estos son Intercambios de Internet donde la red puede participar.

4.1.6. Sitio web de la empresa

Proveer una fuente adicional de contacto e información de la política de enrutamiento en un sitio web es beneficioso para aquellos operadores que aún no están familiarizados con PeeringDB o consultar a un RIR.

Para ayudar con el apoyo a la comunicación abierta, se define a continuación una lista de puntos para que los operadores de red consideren publicar en sus sitios web:

Información de contacto (buzones RFC2142 y números de teléfono, si aplica)

- Operaciones de red
- Soporte
- Abuso
- Seguridad
- Otros contactos importantes

Política de enrutamiento

- Comunidades BGP (clientes y *peer*)
- Política para filtrado de BGP (entrante y saliente)

- Política para rutas inestables (route dampening)
- Politica de soporte para MED (Multi-Exit Discriminator)

4.2. Validación Global - Facilitando la validación de información sobre enrutamiento a una escala global

Acciones MANRS relevantes que se esperan:

- *Que el Operador de Red sea capaz de comunicar a sus redes vecinas cuáles de sus anuncios de enrutameinto son correctos;*
- *Que el Operador de Red haga pública su documentación sobre politicas de enrutamiento, ASNs y prefijos que se pretendan anunciar hacia Redes externas a ellos.*

La información sobre el enrutamiento de Internet deberá estar disponible a una escala global con el fin de facilitar su validación, incluyendo las políticas de enrutamiento, ASNs y los prefijos de Red que se pretenden anunciar a los otros Operadores. Como el alcance de Internet es global, dicha información deberá estar disponible públicamente en un lugar bien referenciado y usando un formato común.

Los Mienbros participantes de MANRS deberán mantener actualizada la información pública con el fin de facilitar la validación del enrutamiento en Internet. Deberán incluir los siguientes datos :

Objeto	Fuente	Descripción
aut-num	IRR	Documentación de Politica
route/route6	IRR	NLRI/origen
as-set	IRR	Customer cone
ROA	RPKI	NLRI/origen

4.2.1. Documentación de Origen Válido

El propósito de la validación del Origen es verificar que el originador de un AS_PATH, es decir el que está más a la derecha, es correcto. Esto puede ser verificado al correlacionar el direccionamiento (o prefijos) y los ASNs, y para facilitar esto, todos los participantes de MANRS deberán hacer pública su información pertinente en bases de datos tales como IRRs. También

deberán promover y motivar (posiblemente insistir) a sus clientes de tránsito IP a hacer lo mismo con sus propios espacios de direccionamiento.

Los dos métodos más comúnmente usados para comunicar la autorización de origen son :

- Objetos route/route6 registrados en una de las bases de datos IRR y
- La publicación de las ROAs en el sistema RPKI

Siendo que los dueños de los recursos no conocen de antemano cuál fuente de información será usada por un tercero para validar dicha información, los dueños de los recursos deberían utilizar ambos métodos.

4.2.1.1. Publicando información a través del sistema IRR

La manera para publicar información en un IRR dependerá de cuál IRR corresponda para la zona geográfica en la que esté ubicado el operador de Red o su centro de operaciones. En las regiones donde el RIR facilita un IRR (todos menos LACNIC) se recomienda el uso del IRR.

Los recursos de Proveedores Agregables (PA) y recursos de Proveedores Independientes (PI) asignados a la(s) organización(es) deberán ser registrados en el RIR IRR. Se deberán crear los Objetos de rutas asociadas al ASN de la organización.

En el IRR también se deberá crear un objeto AS-SET usando un nombre significativo para su Registro Local de Internet (LIR Local Internet Registry) o para la Red de su organización. El propósito de los AS-SET es agrupar los ASNs de forma significativa. Por ejemplo se crea el AS-SET AS64500:AS-CUSTOMERS el cual contiene a todos los clientes de AS64500 (AS64501 y AS64502) y se crea el AS-SET AS64500:AS-ALL el cual contiene tanto al ASN persé, como también a sus clientes. Esto se hace para facilitarle a todos especificar las políticas de enrutamiento.

Para la región de LACNIC, se recomienda el uso de RADB o el IRR de NTTCOM puesto que LACNIC no provee un servicio por cuenta propia (sin embargo debe mencionarse que para usar RADB se debe tener una relación comercial con Merit y para el IRR de NTTCOM se requiere una relación comercial con NTT).

La siguiente tabla resume las recomendaciones del registro de RUTAS:

Región	IRR preferido	IRR Alternativo
ARIN	ARIN	RADB / NTTCOM
AFRINIC	AFRINIC	RADB / NTTCOM
APNIC	APNIC	RADB / NTTCOM
RIPE	RIPE NCC	RADB / NTTCOM
LACNIC	RADB	NTTCOM

Se recomienda también un registro complementario en los NIRs (National Internet Registry) donde la calidad de los datos nacionales son lo importante (por ejemplo, el uso de JPNIC NIR para LIR dentro de Japón).

4.2.1.1.1. Registrar Anuncios esperados en los IRR

Para documentar cuales prefijos de direcciones un ASN tiene permito anunciar, se deben utilizar objetos ROUTE/ROUTE6 con el propósito de vincular un AUT-NUM con un INETNUM/INET6NUM.

El siguiente ejemplo muestra la documentación donde el AS64500 está permitido que anuncie el prefijo de RED 2001:db8:1000::36

```
route6:         2001:db8:1000::/36
descr:          Provider 64500
origin:         AS64500
mnt-by:         MAINT-AS64500
created:        2012-10-27T12:14:23Z
last-modified:  2016-02-27T12:33:15Z
source:         RIPE
```

Se deberá crear un objeto ROUTE/ROUTE6 exactamente for cada prefijo de Red y ASN que se desee observar en la tabla de enrutamiento.

4.2.1.2. Proporcionar información a través de el sistema RPKI

El repositorio RPKI puede almacenar información acerca de los prefijos de red que se originan en su Red en la forma de objetos ROA (Route Origing Authorization) Autorización de Origen de Ruta. Hay que tener en cuenta que estos objetos ROA no incluyen los anuncios de sus clientes, sino que sólo prefijos de red que pertenecen a su ASN Únicamente se verifica el origen del ASN, no la trayectoria completa.

4.2.1.2.1. Servicios de Certificación de Recursos provistos por los RIR

Todos los Registradores Regionales de Internet (RIR) ofrecen un servicio llamado "Servicio de Certificación de Recursos" donde llaves son almacenadas y administradas por el RIR y todas las operaciones son ejecutadas en los servidores del RIR.

El procedimiento de registro y uso del portal de gestión de los objetos ROA es diferente para cada RIR.

En los enlaces que se proveen a continuación, encontrará información pertinente:

- ARIN: https://www.arin.net/resources/rpki/index.html#howtoparticipate
- RIPE: https://www.ripe.net/manage-ips-and-asns/resource-management/certification/using-the-rpki-system
- APNIC: https://www.apnic.net/manage-ip/apnic-services/resource-certification
- LACNIC: http://www.lacnic.net/en/web/lacnic/certificacion-de-recursos-rpki
- AfriNIC: https://www.afrinic.net/en/initiatives/resource-certification

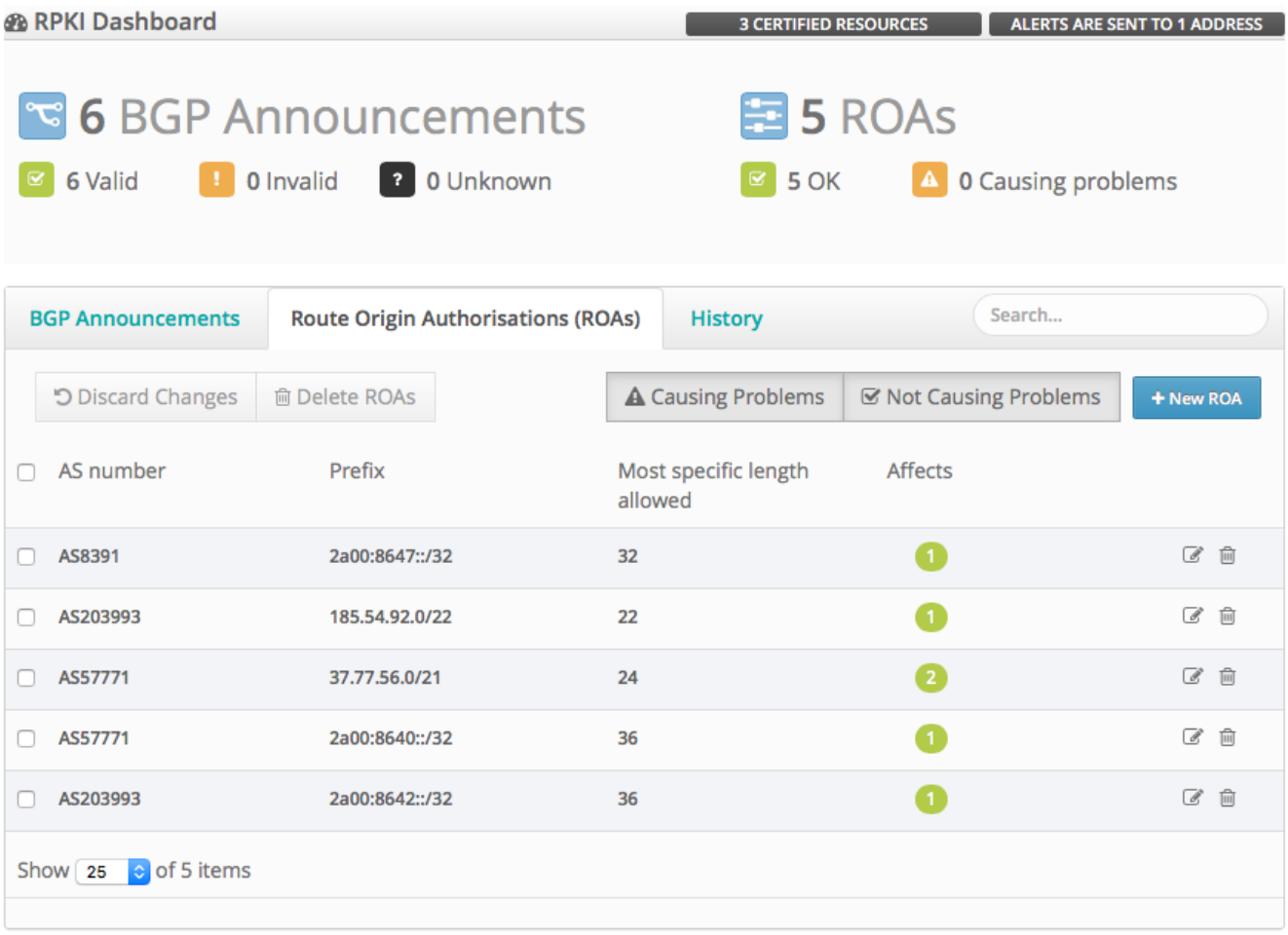
A pesar de que cada RIR es diferente, los siguientes requerimientos son comunes para obtener un certificado :

- Membresía válida con el RIR
- Acceso al portal de gestión de recursos
- Aceptar los términos y condiciones del servicio

4.2.1.2.2. Portal RIR

Un portal RIR ofrece una interfaz para ejecutar varias operaciones con los objetos ROAs: creación y publicación, modificación, eliminación. Algunos portales ofrecen herramientas para generar objetos ROAs a partir de los anuncios BGP observados, comparar ROAs creados con anuncios BGP y determinar el impacto de la publicación de un ROA en los anuncios BGP existentes.

El siguiente es un ejemplo de la interfaz en RIPE NCC RPKI ROA:



A la hora de crear un ROA, se debe poner especial atención al campo de "longitud máxima" (maximun length). Si se coloca la longitud del prefijo, entonces ese ROA podría invalidar el anuncio de prefijos de red más específicos, a menos que hayan otros ROAs creados para dichos prefijos más específicos. Un emisor de un ROA DEBERÁ anunciar todos los prefijos cubiertos por el ROA, hasta llegar al prefijo de longitud máxima. En caso de no hacerlo, entonces un adversario o competidor podría anunciar un prefijo más específico anteponiéndole un ASN autorizado. Entonces este adversario o competidor desviará el tráfico, interceptándolo (reenviándolo después al destinatario legítimo) o, aún más común, simplemente desviándolo a que se pierda, provocando un ataque de DoS.

4.2.1.2.3. Utilizando RPKI y requerir que los clientes registren ROA

La idea básica para automatizar la validación de los anuncios de los clientes con RPKI es la misma que para el IRR. Sin embargo, el uso de RPKI en estos casos requiere que los clientes administren completamente su espacio de direccionamiento en el sistema que sea soportado por el RIR que

les ha entregando el direccionamiento. Para los pequeños clientes o los clientes que han recibido su direccionamiento IP de los Proveedores de servicio de Internet (ISP), este proveedor podría decidir hacer la administración de RPKI en nombre de los clientes.

4.2.1.2.4. Asegurarse que el(los) Certificados RPKI y los registros ROAs se mantengan actualizados

Establecer un procedimiento que garantice que cada vez que implemente un nuevo prefijo en su red se registre o se modifique el registro ROA correspondiente para reflejar dicho cambio o adición. Esto deberá convertirse en un proceso integrado dentro de los procedimientos de su Centro de Operaciones de Red (NOC Network Operation Center)

4.2.1.3. Lecturas adicionales

Podrá encontrar información adicional en :

- Resource Public Key Infrastructure
  https://en.wikipedia.org/wiki/Resource_Public_Key_Infrastructure
- NRO Information on RPKI
  https://www.nro.net/wp-content/uploads/RPKI.pdf
- NRO video on Resource Certification
  https://youtu.be/rH3CPosGNjY

4.2.2. Documentación de Politicas de Enrutamiento

Mientras que los objetos ROUTE/ROUTE6 son en su mayoria utilizados para recolectar información requerida en la construcción de filtros de validación de origen, un punto inicial para muchos conjuntos de herramientas son las políticas de enrutamiento para un ASN contenido en el objeto aut-num.

Esta política de enrutameinto se puede hacer disponible describiéndola mediante el uso de Lenguaje de Especificación de Política de Enrutamiento RPSL (Routing Policy Specification Language, RPSL – RFCs 4012, 2622 y otros), en los atributos “mp-import” y “mp-export” de un objeto aut-num registrado en la base de datos del IRR.

La opción de cómo representar una Política en RPSL variará de un ASN a otro, y es común que exista más de una forma de describir una política dada. Sin embargo, la mayoría de las declaraciones incluyen el uso de objetos as-set para agrupar juntos los ASNs de los clientes.

4.2.2.1. Documentación Básica de Política

El siguiente ejemplo muestra la política del AS64500 de la figura 1.

```
aut-num:        AS64500
descr:          Provider 64500
remarks:        ++ Customers ++
mp-import:      from AS64501 accept AS64501 [AR2]
mp-export:      to AS64501 announce ANY
mp-import:      from AS64502 accept AS64502
mp-export:      to AS64502 announce ANY
remarks:        ++ Peers ++
mp-import:      from AS64511 accept AS64511:AS-ALL
mp-export:      to AS64511 announce S64500:AS-ALL
remarks:        ++ Transit ++
mp-import:      from AS64510 accept ANY except FLTR-BOGONS
mp-export:      to AS64510 announce AS64500:AS-ALL
mnt-by:         MAINT-AS64500
created:        2012-10-27T12:14:23Z
last-modified:  2016-02-27T12:33:15Z
source:         RIPE
```

Un enfoque común que usualmente se utiliza entre pares (peers) y muy poco a proveedores de tránsito, es el uso de aut-num, as-set y otros sets de objetos derivados de la documentación de las politicas de los AS y luego expandiéndolos a objetos de enrutamiento, expresiones de filtrado específico, etc., para la creación de los filtros requeridos.

Por ejemplo, un tercero AS64511, podría tomar el objeto aut-num del AS64500, obtener el cono del cliente (AS64500:AS-CUSTOMERS), obtener los objetos relacionados ROUTE/ROUTE6 (algunas veces expandiendo otros incluídos los sets y filtros explícitos) y obtener así una lista de prefijos que representan los anuncios legítimos de AS64500 para sus pares o peers.

No siempre queda claro a partir de las políticas de un objeto aut-num cual de los objetos as-set debería ser usado para crear un filtro como el del parrafo anterior. Por lo cual se recomienda que los participantes miembros de MANRS coloquen adicionalmente el nombre del as-set en el campo del “Registro IRR” el registro del peeringDB.

4.2.2.2. Documentación avanzada de las politicas

A pesar de que el RPSL es un lenguaje enriquecido, y que se puede usar para construir políticas complejas, es un reto lograrlo en un formato usable (fácil de entender por seres humanos o analizable por máquina). Un ejemplo de lo que se puede hacer, se muestra acontinuación:

```
mp-import:          afi ipv4.unicast
                    from AS64510 192.0.2.1 at 192.0.2.2
                    action pref = 10; med = 0;
                    community.append(64500:10);
                    aspath.prepend(AS64500, AS64500)
                    accept ANY except FLTR-BOGONS
mp-export:          protocol BGP4 into OSPF
                    to AS64500 announce ANY
default:            to AS64510 192.0.2.100 at 192.0.2.101
```

Ya sea que se haga de manera simple o que se documente hasta el último detalle de su configuración dependerá más que todo de las políticas de su organización. Los participantes de MANRS con políticas inusuales o complicadas pueden también escoger documentarlas por separado en formato más facil de entender, y compartir dicha documentación con otros operadores de Red a través de un vínculo hacia la localización del documento en el atributo "Remarks" (comentarios) de sus objetos aut-num y/o en el campo "Notes" de su registro peeringDB.

4.2.2.3. Resumen

RPSL puede ser usado para documentar cada router, interfaz, sesiones de pares, filtros y mapas de ruta.

Sin embargo en la práctica hay muy pocas organizaciones que publican documentación tan extensiva. La razón de esto es por el esfuerzo requerido para un correcto mantenimiento, y también, por razones de confidencialidad de los detalles en los acuerdos de peering y renuencia de administración para permitir publicar documentación sobre las prácticas de negocio. Como mínimo, se recomienda documentar al menos cada una de las sesiones de pares de los ASNs con una definición razonable de las rutas intercambiadas.

4.2.3. Lecturas adicionales

- Using RPSL in Practice
  https://tools.ietf.org/html/rfc2650
- Routing Policy Specification Language
  https://tools.ietf.org/html/rfc2622

- Routing Policy Specification Language next generation
  https://tools.ietf.org/html/rfc4012
- Routing Policy System Security
  https://tools.ietf.org/html/rfc2725

4.3. Anti-Spoofing - Previniendo tráfico con direcciones IP origen suplantadas

Acciones MANRS relevantes que se esperan:

- *Que el Operador de Red implemente un sistema de validación de direcciones origen por lo menos para su infraestructura, sus propios usuarios finales y las redes de los clientes que tienen una conexión única activa hacia Internet (stub-Network). Los operadores de red implementan filtros anti-spoofing para prevenir que paquetes con direcciones IP origen suplantadas logren entrar y/o salir hacia internet.*

Usar direcciones IP de origen suplantadas es la práctica de generar datagramas IP con una dirección IP origen diferente a la que tiene asignado el anfitrión originador de los datagramas IP. En términos sencillos, el anfitrión pretende ser un anfitrión diferente. Esto puede ser explotado de varias formas, siendo la más destacada la de ejecutar un ataque de Denegación de Servicio por amplificación de reflexión (Denial of Service reflection-amplification), el cual provoca que los anfitriones reflectores envíen tráfico a la dirección suplantada que se utilizó.

Hay muchas recomendaciones para prevenir suplantación de direcciones IP origen usando filtros de ingreso, por ejemplo revisar la dirección origen de los datagramas IP cerca del borde de la red. ***La mayor parte de los fabricantes de equipos soportan de alguna forma el uso de filtros de ingreso. Desde el año 2005, el despliegue de técnicas de anti-spoofing (anti-suplantación) no representa un sacrificio en el desempeño de los equipos de comunicación. Ha sido más una limitación del deseo y voluntad de desplegar y darle mantenimiento a las configuraciones de anti-spoofing.***

Irónicamente, el costo de las consecuencias de un ataque de amplificación de DoS puede ser alto para los proveedores de Servicios de Internet. Las consecuencias crean un daño directo al nombre del operador, daña las operaciones de sus clientes y genera daños y costos colaterales que impactan a otros clientes. Estos ataques amplificados de DoS son prevenibles. Sería imposible realizarlos sin utilizar suplantación de direcciones IP origen.

Con esto se demuestra que no se han desplegado suficientemente los filtros de ingreso. Lamentablemente se cree que no hay beneficios para un proveedor de servicios el hacer un despliegue de filtros de ingreso en su infraestructura. También existe una creencia ampliamente distribuida de que los filtros de ingreso solo ayudan cuando están desplegados universalmente.

Enfoques comunes para resolver este problema involucran el uso de funciones de software tales como SAV (Source-Address Validation), validación de dirección de origen en redes de cable-modem o la validación estricta de uRPF (unicast Reverse-Path Forwarding) en las redes de enrutamiento. Estos métodos pueden aliviar la sobrecarga del trabajo administrativo en los casos donde el enrutamiento y las topologías sean relativamente dinámicas. Otro enfoque podría ser el usar información de filtros de prefijos entrantes para crear filtrado de paquetes, los cuales sólo permitirán paquetes con direcciónes IP origen para los que la Red del operador está legitimada a anunciar alcanzabilidad.

Para las mayoría de redes con arquitectura pequeña y sencilla, la forma más facil de prevenir spoofing es el uso del modo estricto de uRPF (Unicast Reverse Path Forwarding). Para filtrar direcciones origen usando dispositivos en un dominio de capa-2 se puede hacer con SAVI (Source Address Validation Improvements). En los equipos que no tengan funciones de filtrado automático, se pueden usar Listas de Control de Acceso (ACLs) para implementar funcionalidades equivalentes al filtrado de direcciones origen. Todas estas tecnologías están explicadas más adelante.

4.3.1. Principios guía para Arquitecturas de Anti-Spoofing

Para lograr la mayor eficacia posible con las técnicas anti-spoofing, estas deberán implementarse lo más cerca del orígen como sea posible. En las redes empresariales, las direcciones origen asignadas para cada dispositivo con frecuencia están configuradas y controladas por la administración, por lo cual las auditorias de seguridad pueden fácilmente identificar exactamente qué dispositivo envia qué paquete de red.

Para lograr la implementación de MANRS, dicha granularidad no es necesaria pues MANRS se enfoca en la seguridad del enrutamiento y anti-spoofing a nivel de la red. Por lo tanto, las arquitecturas anti-spoofing comúnmente se enfocan en lograr que los clientes no envíen paquetes con la dirección origen suplantada.

El hacer cumplir que los clientes no envíen paquetes con la dirección origen suplantada tiene el beneficio que los clientes no podrán hacerse pasar por otros clientes, enviando paquetes con las

direcciones origen de otros clientes, con lo cual se evita que unos generen problemas a otros entre sí, lo que resulta a menudo difícil de depurar.

Si por alguna razón no se logra hacer cumplir que cada cliente no envíe paquetes con la dirección origen que no sea de las direcciones de él, entonces una alternativa es la de forzar la validación de direcciones origen en los puntos de agregación, de manera que esos clientes estén al menos limitados en cuáles direcciones puedan suplantar. Como mínimo deberían haber tecnicas anti-spoofing a nivel del ISP, de manera que sus clientes no puedan suplantar las direcciones origen de clientes de otros ISP u otras organizaciones y ocasionar problemas más allá de su propio ISP.

4.3.2. Unicast RPF

El BCP38 uRPF (Reenvío de ruta inversa de unidifusión) en modo estricto con el estilo RFC1998++ de multiconexión (un BCP para multiconexión) es un enfoque que puede trabajar en configuraciones simétricas (mono conexión) y asimétricas (multiconexión), y que fue desplegado operativamente en el año 2002. Ciertamente, hay muchos que piensan que "uRPF no funciona por la asimetría del enrutamiento", pero no es cierto. En la documentación del 2001, el libro blanco del ISP (version de Google 2.9) y el Libro Esencial del ISP[1] y a lo largo de implementaciones en varios reconocidos Proveedores de Servicio, han demostrado que uRPF en modo esctricto es una técnica viable.

uRPF tiene cuatro algorítmos – modo estricto (revisión del IP origen y proximidad), Modo suelto (solo revisión de la dirección IP origen), trayectoria factible (revisión de dirección IP origen con las alternativas de la base de información de reenvío FIB), y el modo VRF (permitir/denegar revisión en una tabla separada de la base de información de reenvío). Cada una de estas opciones de uRPF está diseñada para funciones específicas de anti-spoofing en diferentes partes de la red.

- uRPF modo estricto – BCP38 del lado de la frontera cliente-proveedor de Servicios (SP). Cada paquete que ingresa es probado con la base de información de reenvío FIB (Forwarding Information Base) y, si la interfaz de entrada no es la mejor trayectoria reversa de reenvío, el paquete es descartado.
- uRPF modo suelto – sRTBH (Source-based Remotely Triggered Black Hole) se implementa en cualquier parte de la red – pero solo revisa si la ruta está en la base de información de reenvío; si no está, entonces el paquete es descartado. Si está en la base de información de

[1] ISBN 1587050412

reenvío, lo deja pasar. Es recomendable para mitigar algunos tráficos con IP origen suplantada en la fronteras entre pares.

- uRPF trayectoria factible – sRTBH se implementa en cualquier parte de la red y BCP38 para clientes de multi-conexión y enrutameinto asimétrico. En modo factible la base de información de reenvío mantiene rutas alternas hacia una dirección IP dada. Si la interfaz de entrada coincide con cualquiera de las rutas asociadas con dicha dirección IP, entonces el paquete se deja pasar. En cualquier otro caso el paquete es descartado.
- uRPF modo VRF (Virtual routing and forwarding) – asegurarse que el BGP basado en políticas de pares o un sRTBH más granular (NOTA: el modo VRF podría ser usado como BCP38, pero no se ha probado operacionalmente)

uRPF puede ser útil en muchos lugares de la red. Es utilizado mayormente en los bordes de las redes donde consumidores, servidores y/o clientes se conectan, porque el modo estricto funciona bien ahí. Los operadores de red se sienten dudosos de utilizar uRPF en el núcleo de sus redes por el temor de accidentalmente descartar paquetes válidos que hayan tomado una trayectoria inesperada a través de su red. El uRPF modo de trayectoria factible debería ser usado para solventar dichos problemas.

Tanto Cisco como Juniper implementan modo estricto y modo suelto. A continuación, se muestra como usar modo estricto. Utilize los siguientes comandos para configurar uRPF modo estricto en las interfaces de cara hacia los clientes :

Cisco:

```
ip verify unicast reachable-via rx
ipv6 verify unicast reachable-via rx
```

Juniper:

```
family inet {
     rpf-check;
}
family inet6 {
     rpf-check;
}
```

Esto asegurará que los clientes puedan usar solamente las direcciones IP que se enruten hacia ellos. En situaciones donde se sea un cliente de otro ISP, en la que exista una ruta por defecto apuntando hacia ese ISP, se deberá usar :

Cisco:

```
ip verify unicast reachable-via rx allow-default
ipv6 verify unicast reachable-via rx allow-default
```

Juniper:

Los Routers Juniper adaptan automáticamente su filtrado uRPF basándose hacia donde apunta la ruta por defecto. Usar los mismos comandos de arriba.

La opción `allow-default` (permitir de forma predeterminada), es necesaria porque por defecto la dirección origen será contrastada sólo con las rutas específicas, ignorando la ruta por defecto. Mientras que contrastando con la ruta por defecto pareciera que fuera lo mismo que permitir todo, en efecto no lo es. Se asegura que su conexión de subida (upstream) no le envíe tráfico para el cual se tengan rutas más específicas direccionadas a través de otras conexiones, tales como sus propias redes y las redes de sus clientes. Con esto se protegerá del tráfico suplantado proveniente de otros.

4.3.3. Listas de Acceso Dinámicas (Radius & Diameter)

La forma estándar para establecer listas de acceso de usuarios autenticados por Radius es a través del atributo 11 (Filter-Id[2]). Con este atributo se le podrá indicar al router que aplique una lista de acceso pre-existente a la conexión del usuario. Sin embargo, esto requiere contar con un método fuera de banda para provisionar a todos los routers con las listas de acceso correctas.

Algunos fabricantes tienen opciones adicionales que pueden ser usadas para provisionar dinámicamente estas listas de acceso a través del Radius. Por ejemplo, Cisco provee funcionalidades extra con los atributos `cisco-avpair`:

```
cisco-avpair = "ip:inacl#5=permit ip 192.0.2.0 0.0.0.255 any"
cisco-avpair = "ip:inacl#99=deny ip any any"
```

Con este ejemplo se permitirá pasar únicamente los paquetes provenientes del cliente que tengan la dirección IP orgien dentro del rango 192.0.2.0/24

4.3.4. SAVI

SAVI (Source Address Validation Improvements), Mejoras en la Validación de Dirección Origen, es el nombre del grupo de trabajo dentro del IETF (Internet Engineering Task Force) que trabaja en

[2] https://tools.ietf.org/html/rfc2865#section-5.11

este tema. Para la validación de la dirección origen de un cliente, se utiliza comúnmente la solución de SAVI para DHCP en el RFC 7513. Esta versión de SAVI mantiene un registro de todas las direcciones IP que han sido asignadas a cada dispositivo husmeando los paquetes de DHCPv4 y los DHCPv6 que transitan en el switch al que el cliente está conectado. Si el cliente llegara a utilizar una dirección IP origen diferente, entonces el switch descartará el paquete.

Los fabricantes suelen usar su propia terminología para describir las características SAVI. En Cisco por ejemplo, estas características son referidas como DHCP Snooping, Source Guard y Prefix Guard.

4.3.5. Verificación de la IP origen

Las redes Ethernet son dominios de broadcast, y por defecto no se valida quién tiene permitido enviar qué paquetes usando cuál interfaz. Para configurar los switches Cisco de manera que verifiquen la dirección IP origen utilizada por los dispositivos, se puede utilizar en la configuración la opción "`ip verify option`".

Se tienen tres variantes para esta configuración:

- `ip verify source`
- `ip verify source port-security`
- `ip verify source tracking port-security`

La primer variante verifica la dirección IP origen, la segunda variante verifica además la dirección MAC y en la tercera variante se rastrean adicionalmente las asociaciones entre las direcciones IP y las direcciones MAC. Para prevenir que los clientes utilicen una dirección física (MAC Address) diferente, esta última variante es recomendada. Todo esto está basado en los datos obtenidos de la información de DHCP.

Primero se deberá configurar al switch para que capture información con el comando "`ip dhcp snooping`" husmeando los paquetes DHCP del tráfico que circula a través de él, de manera que posteriormente pueda basar sus decisiones usando dicha información. Para mantener un rastro de en cuales puertos Ethernet están conectados qué clientes DHCP, se deberá usar "DHCP opción 82" con el comando "`ip dhcp snooping information option`". Esto es necesario porque con la opción "`verify port-security`" el switch no aprenderá la dirección MAC sino que hasta que el servidor DHCP le haya asignado la dirección IP al dispositivo conectado. La opción 82 es por lo tanto necesaria para que el switch recuerde donde estaba conectado el cliente.

Son varios los pasos necesarios a seguir para habilitar el rastreo seguro de dispositivos y verificar su dirección origen. El primer paso es habilitar en el switch "`IP device tracking`" a nivel global. Esto, para asegurar que el switch pueda rastrear qué dirección IP pertenece a qué dirección MAC. Luego, en cada interfaz, hay que definir el número de dispositivos que están permitidos conectarse, usando el comando "`ip device tracking maximum num`" donde "`num`" puede tomar el valor entre 1 y 10. Ahora, habilitar "`switchport port-security`" en cada interfaz para asegurar que sólo las direcciones MAC permitidas se puedan usar. Finalmente habilitar la función de verificación que vincula todo junto con el comando "`ip verify source tracking port-security`".

Ahora el switch tiene toda la información que necesita para husmear el tráfico DHCP, vincular la dirección IP con la dirección MAC y verificar que todos los paquetes enviados a través del switch estan conformes con la configuración colectiva del switch la cual está basada en las respuestas del servidor DHCP. Aquellos paquetes que no estén en conformidad con lo que el servidor DHCP haya asignado, serán descartados.

4.3.6. Verificación de la fuente de cable-modems

Las redes de cable-modem son en muchas formas muy parecidas a las redes Ethernet. A menos que se configuren de manera diferente, los usuarios pueden suplantar direcciones origen o robarse las direcciones IP de otros usuarios en las redes de cable-modem. La funcion "`source-verify`" de los cable-modem Cisco, permite a los operadores CMTS (Cable Modem Termination System) Sistema de Terminación de Cable módem, limitar cuales direcciones origen le están permitidas usar al usuario/cliente.

Hay dos variantes de esta característica:

- `cable source-verify`
- `cable source-verify dhcp`

Ambas variantes afectan cual dirección origen de la subred de cable-modem está permitido usar. La primer variante sólo previene que un cliente/usuario pueda robarse la dirección IP de otro cliente/usuario y, por lo tanto, no es suficiente para los objetivos de MANRS. Veremos entonces la segunda variante.

Configurando "`cable source-verify dhcp`" le dice al CMTS que todas las direcciones origen deberán ser verificadas con los préstamos DHCP que hayan circulado a través del CMTS. Si un

paquete es enviado con una dirección IP origen diferente, entonces el CMTS lo descartará. Esto prevendrá que los usuarios/clientes usen direcciones IP que no hayan sido asignadas vía DHCP.

Cuando un CMTS es reiniciado podrían ocurrir algunos problemas. En estos casos el CMTS habrá perdido los registros de direcciones IP asignadas por DHCP a los clientes y podría descartar tráfico legítimo. Para resolver esta situación, el CMTS puede configurarse para que use el protocolo DHCP leaseQuery. Esto le permite al CMTS preguntarle al servidor DHCP sobre las asignaciones de direcciones IP del tráfico que está viendo pasar. Una vez que el servidor DHCP confirme que existe una asignación legítima para dicha dirección IP, el CMTS la agregará a su caché y permitirá que el tráfico pase.

Para lograr que el CMTS no confíe en los ARP de las redes de cable-modem, se debe configurar con "`no cable arp`". Con esto se asegurará que sólo la información de los paquetes DHCP y LeaseQuery será confiable cuando se verifiquen las direcciones origen.

La función "`cable source-verify`" sólo protege a la subred de cable-modem. Para prevenir a los clientes que hagan suplantación de direcciones origen de otros, y permitir el tráfico de clientes que tienen enrutadas subredes permitidas, también se deberá configurar "`ip verify unicast source reachable-via rx`" para habilitar en modo estricto uRPF en la red de cable-modem. Con esto de revisarán todas las direcciones origen que no están directamente en la red cable-modem, y permitirá validarlas, por ejemplo, con las rutas estáticas para subredes enrutadas hacia los clientes.

4.3.7. Listas de Control de Acceso (ACLs)

Las ACLs están comúnmente desplegadas en la frontera del proveedor de servicios y la frontera del cliente, pero también son muy útiles en otras secciones de la red, como por ejemplo, en el borde hacia los servidores del proveedor, hacia los clientes y hacia la red de infraestructura, con el objetivo de prevenir comportamientos extraños en los dispositivos. Una estrategia optimizada de ACL podría ser colocar un filtro explícito de permitir en la interfaz del cliente. Los filtros explícitos de permitir especifican rangos de direcciones y deniegan todo lo demás. Por ejemplo, si el cliente de un operador se le ha asignado el bloque de direcciones 192.0.2.0/24, el BCP 38 ACL permitirá todas las direcciones origen de 192.0.2.0/24 y denegará todos los paquetes cuya dirección origen sea diferente de 192.0.2.0/24.

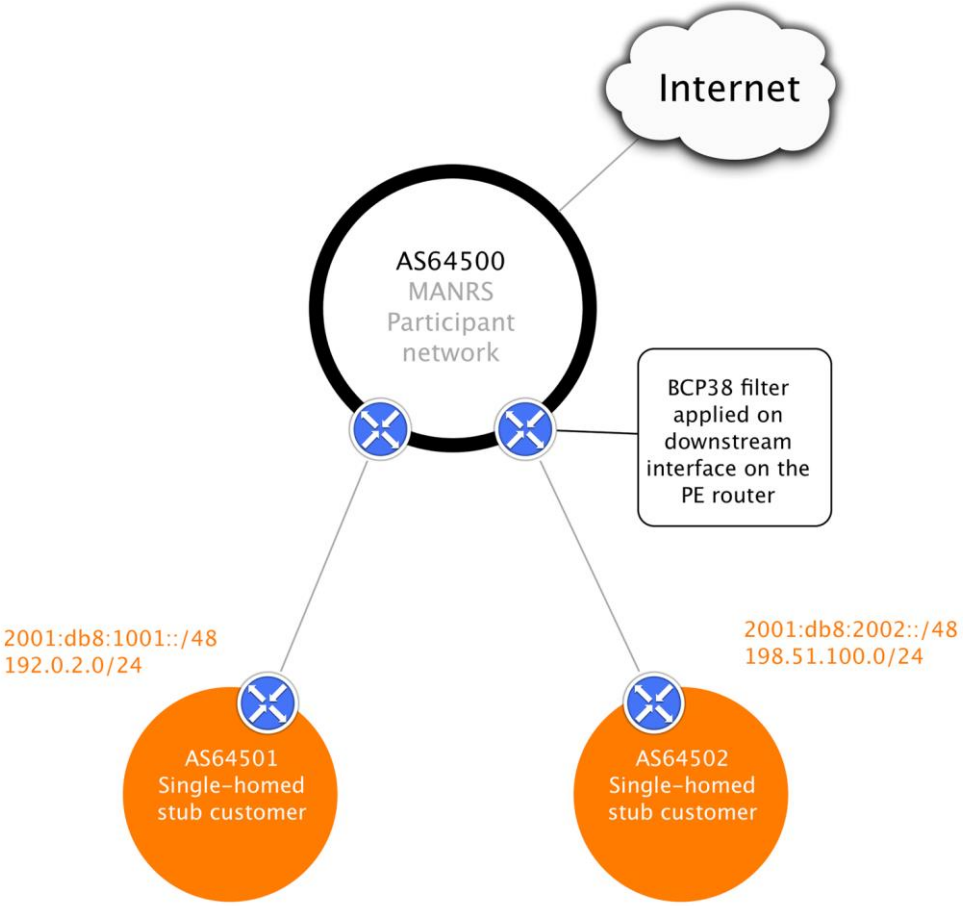


Fig 2. Filtro de Ingreso en un PE router

BCP 38 Filter = Permitir sólo paquetes con dirección IP origen de la red del cliente (2001:db8:1001::/48, 2001:db8:2002::/48, 192.0.2.0/24, 198.51.100.0/24)

En las interfaces del ISP hacia los clientes, deberán haber filtros que verifiquen las direcciones IP origen utilizadas por los clientes. Si no se puede usar uRPF, entonces se necesita configurar manualmente ACLs.

Veamos las configuraciones para el primer cliente del diagrama anterior:

Cisco:

```
ip access-list extended customer1-in-ipv4
permit ip 192.0.2.0 0.0.0.255 any
!
ipv6 access-list customer1-in-ipv6
permit ipv6 2001:db8:1001::/48 any
!
interface x
ip access-group customer1-in-ipv4 in
ipv6 traffic-filter customer1-in-ipv6 in
```

Juniper:

```
firewall {
     family inet {
          filter customer1-in-ipv4 {
               term allowed-sources {
                    from {
                         source-address {
                              192.0.2.0/24;
                         }
                    }
                    then accept;
               }
          }
     }
     family inet6 {
          filter customer1-in-ipv6 {
               term allowed-sources {
                    from {
                         source-address {
                              2001:db8:1001::/48;
                         }
                    }
                    then accept;
               }
          }
     }
}
interfaces x {
     unit 0 {
          family inet {
               filter {
                    input customer1-in-ipv4;
               }
          }
          family inet6 {
               filter {
                    input customer1-in-ipv6;
               }
          }
     }
}
```

4.3.7.1. Puntos de agregación

Cuando las ACLs en el borde entre el proveedor y el cliente no se pueden establecer, por ejemplo, porque múltiples clientes están conectados a la misma red capa-2 y los dispositivos de red capa-2

no posean las características para filtrar basándose en información de capa-3, entonces el filtrado en los puntos de agregación es la segunda mejor solución.

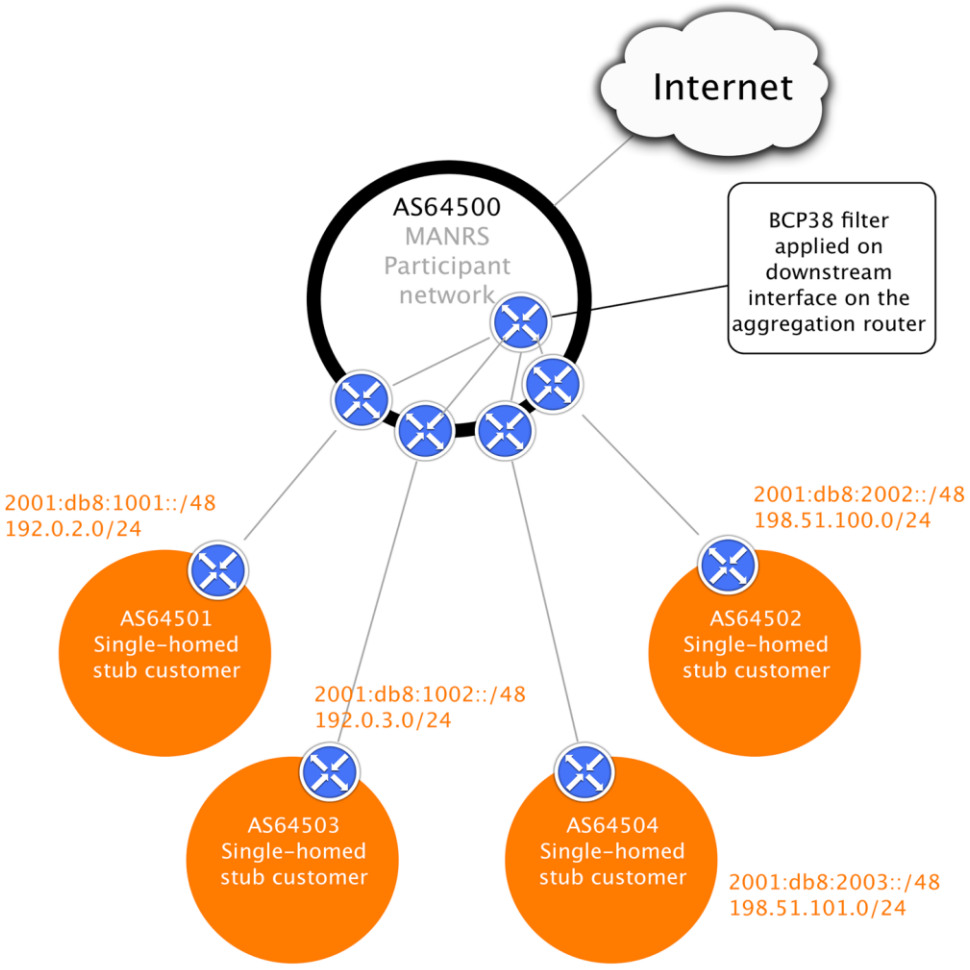


Fig 3. Filtros de ingreso en los routers de agregación
Filtro BCP 38 = Permitir sólo paquetes con dirección IP origen de las redes de los clientes, agregadas (2001:db8:1000::/44, 2001:db8:2000::/44, 192.0.2.0/23, 198.51.100.0/23)

En este ejemplo, por alguna razón no especificada, no es posible filtrar por cada /24 de cada cliente. Entonces, filtrando sobre 96.0.18..0/23 y 96.0.20.0/23 en el punto de agregación cerca de las conexiones de los clientes, al menos podrá al limitar las posibilidades de suplantación de direcciones IP origen, para ese grupo de clientes, a un rango más pequeño de direcciones.

La configuración se realiza de la misma forma como se mostró en la sección anterior, con la excepción que ahora se realiza en un router diferente, en una localización más centralizada.

4.3.8. NAT a nivel de Operador – ¿Es NAT una herramienta anti-suplantación ?

Por defecto, muchas implementaciones de NAT no filtran la dirección origen de los clientes. Veamos por ejemplo una configuración sencilla de NAT en un router Cisco:

```
ip nat inside source list INSIDE pool OUTSIDE overload
```

Esta regla NAT traducirá las direcciones de los paquetes con dirección origen incluida en la lista de acceso INSIDE y cambiará la dirección origen a una dirección del pool OUTSIDE. Sin embargo, paquetes con direcciones IP origen suplantadas que no estén incluidas en la lista de acceso INSIDE serán reenviados sin cambio alguno en su direccion origen, resultando en la circulación en internet, de paquetes con direcciones IP origen suplantadas. Cuando un paquete con dirección origen suplantada coincide con las direcciones de la lista de acceso INSIDE será entonces modificado, según las direcciones especificadas en el OUTSIDE pool, entonces Internet no verá circular un paquete con dirección IP origen suplantada pero será imposible para el operador del NAT rastrear los paquetes con direcciones IP origen interna hacia su dispositivo original.

Esto muestra que NAT no es una herramienta anti-suplantación de direcciones IP origen. Aún cuando se usa NAT, la dirección origen usada por los clientes debería ser revisada lo más cerca del cliente como sea posible, igual como en los casos donde no se utiliza NAT mostrados en las secciones anteriores de este capítulo. Sólo entonces se podrá prevenir que paquetes con direcciones IP origen suplantada y/o paquetes no rastreables circulen en Internet.

4.3.9. Lecturas Adicionales

- RIPE Anti-Spoofing Task Force HOW-TO
  https://www.ripe.net/publications/docs/ripe-431
- Source Address Validation Improvements (SAVI) Solution for DHCP
  https://tools.ietf.org/html/rfc7513
- Setting Access Lists with Radius
  http://blog.ipspace.net/2010/09/setting-access-lists-with-radius.html
- Cisco: IPv6 First-Hop Security Configuration Guide
  http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-sy/ip6f-15-sy-book.html
- Cisco: Configuring DHCP Snooping, IP Source Guard, and IPSG for Static Hosts
  http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/15-02SG/configuration/guide/config/dhcp.html

- Cisco: Configuring DHCP Features and IP Source Guard http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_53_se/configuration/guide/2960scg/swdhcp82.html
- Cisco: Cable Source-Verify and IP Address Security http://www.cisco.com/c/en/us/support/docs/broadband-cable/cable-security/20691-source-verify.html

4.4. Filtrado – Prevención la propagación de información incorrecta de enrutamiento

Las acciones MANRS importantes que se esperan son:

- *Que los operadores de red definan una política de enrutamiento clara e implementen un sistema que asegure la exactitud de sus propios anuncios y los de sus clientes hacia redes adyacentes con granularidad a nivel de prefijos y AS-path.*
- *Que los operadores de red apliquen la debida diligencia al revisar la exactitud de los anuncios de sus clientes, específicamente que los clientes tengan legítimamente el ASN y los bloques de direcciones que anuncian.*

Lo más importante es asegurar los anuncios de enrutamiento entrantes, particularmente de las redes cliente, a través del uso de filtros explícitos a nivel de prefijo o mecanismos equivalentes.

En segundo lugar, los filtros AS-path podrían ser usados para requerir que la red del cliente sea explícita sobre cuál o cuáles sistemas autónomos (ASes) están en el flujo descendente hacia ese cliente. De forma alterna, los filtros AS-path que bloqueen anuncios de clientes de ASs con los cuales el proveedor tiene relaciones libres de pago (*settlement-free*) puedan prevenir algunos tipos de "fuga" de rutas (*routing "leaks"*).

Recordar que un error común ocurrer al escribir *(typos)* las direcciones IP anunciadas, lo que causa que se anuncien direcciones incorrectas desde un ASN permitido. Por tanto, por sí solo, el filtrado por AS-path de los anuncios BGP del cliente no es suficiente para prevenir problemas catastróficos de enrutamiento a un nivel sistémico.

De forma similar, el filtrado de anuncios salientes hacia *peers* que no son clientes no es suficiente cuando el operador provee servicios a clientes con múltiples proveedores (*multi-homed*). Considérese por ejemplo el escenario en el que un cliente anuncie un grupo de prefijos más largos a solamente uno de varios proveedores de tránsito: tales prefijos más largos serían aprendidos por los otros proveedores del cliente vía *peering* libre de pagos (*settlement-free*) o de sus propios

tránsitos, pero, puesto que los prefijos pertenecen a un cliente válido, no serían filtrados a la salida, cuando sean dirigidos a otros que no son clientes, si tales filtros se basan solamente en la coincidencia de prefijos. En consecuencia, el proveedor en cuestión anunciará el alcance de tránsito hacia esos prefijos más específicos, a pesar de que su cliente nunca se los anunció directamente. Los operadores solamente deben anunciar tránsito para los prefijos que los clientes les han anunciado directamente, no prefijos aprendidos desde otros caminos.

Antes de crear filtros es importante aplicar debida diligencia y revisar si la información proveída por el cliente sobre su identidad y recursos, es correcta. Los filtros pueden verificar que el AS64501 tiene permitido anunciar 1920.2.0/24; pero sólo la verificación de identidad puede determinar si el cliente realmente tiene la asignación del AS64501.

Existen varias formas de crear estos filtros:

1. Usar Registros de Enrutamiento de Internet (IRRs – Internet Routing Registries) y solicitar a los clientes el registro de objetos de ruta (route objects).
2. Usar RPKI (Resource Public Key Infraestructure, un sistema de certificación de recursos) y solicitar a los clientes crear Autorizaciones de Origen de Ruta (ROAs – Route Origin Authorizations).
3. Usar una base de datos interna con la información brindada como parte del proceso de aprovicionamiento.

Este documento solamente se enfocará en los primeros dos casos, ya que el tercero es propietario.

En general, un prefijo observado en el sistema de enrutamiento puede validarse parcialmente, que su origen proviene del ASN correcto (i.e. solamente contra el ASN más a la derecha en el atributo AS_PATH), o validarse completamente contra la lista ordenada de ASNs en el AS_PATH. A esto se le conoce como validación de origen y validación de camino, respectivamente. Mientras que los anteriores son conceptos relacionados y pueden desarrollarse mediante el uso de un conjunto de herramientas superpuestas, difieren significativamente con respecto a la fuente autorizada de validación de información como se describe a continuación, y por lo tanto, en la información que un participante de MANRS necesita mantener.

4.4.1. Uso de un IRR y requerimiento de registro de objetos de ruta de los clientes

Los IRR (Internet Routing Registries – Registros de Enrutamiento de Internet) son lugares centralizados donde se publica la información de enrutamiento. Ellos documentan cuáles ASNs

están autorizados para anunciar cuáles direcciones IP, y cuáles son las políticas para el intercambio de rutas entre ASNs. Esta información se puede usar en la configuración de enrutadores (*routers*) para validar las rutas recibidas.

Es de notar que no todos los IRRs son autenticados contra fuentes autorizadas. Los IRRs de AFRINIC, APNIC y RIPE sólo permiten que los usuarios ingresen registros que coincidan con los recursos que tienen asignados. Otros IRRs pueden tener mecanismos de autenticación menos estrictos para evitar que sus usuarios ingresen datos falsos.

4.4.1.1. Uso del IRR para producir filtros de prefijos

Para el propósito de esta sección, se asume que esta se refiere a filtros de prefijos en las siguientes circunstancias (una lista no exhaustiva):

1. Filtrado saliente de prefijos específicos de la red para *peers* y tráficos ascendentes [*upstreams*] (obligatorio)
2. Filtrado entrante de prefijos específicos provenientes de los clientes (obligatorio)
3. Filtrado entrante de prefijos específicos de los *peers* hacia la red (recomendado)

Los autores notan que (1) debería lograrse, solamente dados los registros propios del operador. (2) es deseable y debería ser fácilmente sintetizable desde el AS-SET del operador en el IRR (asumiendo que los registros de las redes de los clientes se hacen en el IRR) y (3) generalmente es visto como algo bueno, si se logra, dado el tamaño y complejidad del registro de las redes del *peer.*

Ya sea que (3) se desarrolle o no, debería ser el caso que las redes no deseadas (tales como las redes BOGON y los propios prefijos del operador) se filtren en todo momento.

Debe notarse que un cuarto escenario: filtrado específico, parcial o completo, de prefijos entrantes de *upstring* (para aquellos que dependen de conectividad de un tercero), está fuera del alcance de este documento (pero el punto concerniente al filtrado de BOGON mencionado en (3) debe considerarse sin embargo, para todas las conexiones).

En un escenario típico, un operador requerirá que sus clientes registren los anuncios que se esperan de ellos, como objetos de ruta en un IRR seleccionado. Para el ejemplo de la topología de red en la figura 1, la red AS64500 solicitará al AS64501 que registre los siguientes objetos:

```
route:          192.0.2.0/24
descr:          Cust 64501
origin:         AS64501
```

```
mnt-by:          MAINT-AS64501
createed:        2015-09-27T12:14:23Z
last-modified:   2015-09-27T12:14:23Z
source:          RIPE
route6:          2001:db8:1001::/48
descr:           Cust 64501
origin:          AS64501
mnt-by:          MAINT-AS64501
created:         2015-09-27T12:14:23Z
last-modified:   2015-09-27T12:14:23Z
source:          RIPE
```

Y objetos similares para su otro cliente – AS64502

El mismo AS64500 registrará los siguientes objetos:

```
route:           203.0.113.0/24
descr:           Provider 64500
origin:          AS64500
mnt-by:          MAINT-AS64500
created:         2012-10-27T12:14:23Z
last-modified:   2016-02-27T12:33:15Z
source:          RIPE

route6:          2001:db8:1000::/36
descr:           Provider 64500
origin:          AS64500
mnt-by:          MAINT-AS64500
created:         2012-10-27T12:14:23Z
last-modified:   2016-02-27T12:33:15Z
source:          RIPE

as-set:          AS64500:AS-CUSTOMERS
members:         AS64501
members:         AS64502
mnt-by:          MAINT-AS64500
created:         2012-10-27T12:14:23Z
last-modified:   2016-02-27T12:33:15Z
source:          RIPE

as-set:          AS64500:AS-ALL
members:         AS64500
members:         AS64500:AS-CUSTOMERS
mnt-by:          MAINT-AS64500
created:         2012-10-27T12:14:23Z
last-modified:   2016-02-27T12:33:15Z
source:          RIPE

aut-num:         AS64500
descr:           Provider 64500
mp-import:       from AS64500:AS-CUSTOMERS
                 accept PeerAS AND <^PeerAS+$>
mp-export:       to AS64500:AS-CUSTOMERS announce ANY
```

```
mp-import:       from AS64510 accept ANY except FLTR-BOGONS
mp-export:       to AS64510 announce AS64500:AS-ALL
mnt-by:          MAINT-AS64500
created:         2012-10-27T12:14:23Z
last-modified:   2016-02-27T12:33:15Z
source:          RIPE
```

Ahora, una herramienta inteligente podría inspeccionar el objeto aut-num que documenta la política del AS64500, recopilar todos los objetos a los que hace referencia, extraer los prefijos y crear los filtros entrantes y salientes necesarios.

Ejemplos de software que genera configuraciones de router para filtros, a partir de datos de IRR son: IRRToolset, BGPQ3 y IRRPT. Todos, de código abierto.

4.4.1.2. Herramientas de configuración para filtros de prefijos

El rango de herramientas en feature-set (y su correspondiente complejida) del generador prefix-list (BGPQ3) para el procesador de plantillas de configuración de enrutador (IRRToolset).

4.4.1.2.1. Ejemplo de BGPQ3

BGPQ3 es una herramienta simple de línea de comando que se conecta a la base de datos del IRR y crea listas de prefijos a partir de los datos recolectados.

Para crear una lista de prefijos con formato Cisco IOS para todos los prefijios IPv4 en un AS-SET:

```
$ bgpq3 -4 -l AS64500-v4 AS64500:AS-ALL
no ip prefix-list AS64500-v4
ip prefix-list AS64500-v4 permit 203.0.113.0/24
ip prefix-list AS64500-v4 permit 192.0.2.0/24
ip prefix-list AS64500-v4 permit 198.51.100.0/24
```

Para crear una lista de prefijos con formato Cisco IOS para todos los prefijos IPv6 en un AS-SET:

```
$ bgpq3 -6 -l AS64500-v6 AS64500 AS64500:AS-CUSTOMERS
no ipv6 prefix-list AS64500-v6
ipv6 prefix-list AS64500-v6 permit 2001:db8:1000::/36
ipv6 prefix-list AS64500-v6 permit 2001:db8:1001::/48
ipv6 prefix-list AS64500-v6 permit 2001:db8:2002::/48
```

La opción `-l` define el nombre de la lista y las opciones `-4/-6` seleccionan IPv4/IPv6. Como se puede ver en el ejemplo IPv6, es posible especificar múltiples AS-SETs en la línea de comando. BGPQ3 las combinará de forma automática.

4.4.1..2.2. Ejemplo de IRRPT

IRRPT genera listas de prefijos del mismo modo que BGPQ3, pero usa archivos de configuración para opciones y ASNs; da seguimiento a los prefjios modificados entre ejecuciones, y puede alertar a los administradores de tales cambios.

Después de descargar IRRPT, primero se ejecuta el script `configure.php` para definir de forma automática las opciones más comunes en el archivo de configuración. Luego se adapta el archivo de configuración en `conf/irrpt.conf` a las necesidades propias. Las opciones de configuración incluyen la dirección de correo electrónico, estilo de sintaxis de la configuración de enrutador predeterminado, etc. Finalmente, se define en `conf/irrdb.conf`, el AS-SET que se usa para cada ASN con el que se tiene relación. Cada ASN solamente puede tener un AS-SET asociado. Por tanto, no es posible usar un AS-SET diferente para IPv4 e IPv6 o configurar una combinación de AS-SETs.

Cuando todos los archivos de configuración han sido actualizados, se ejecuta la herramienta irrpt_fetch, la cual buscará todos los prefijos incluídos en el AS-SET especificado para cada ASN y enviará correos electrónicos sobre los cambios, a los administradores.

```
$ ./bin/irrpt_fetch
Processing AS64500 (Record 1)
      - Importing ./db/64500 version 1.1
      - Importing ./db/64500.4 version 1.1
      - Importing ./db/64500.6 version 1.1
      - Importing ./db/64500.agg version 1.1
      - Importing ./db/64500.4.agg version 1.1
      - Importing ./db/64500.6.agg version 1.1
      - Sending update notification to hostmaster@example.com
```

Después de buscar todos los prefijos, IRRPT ahora puede generar scripts de configuración de enrutador:

```
$ ./bin/irrpt_pfxgen 64500
conf t
no ip prefix-list CUSTOMER:64500
no ip prefix-list CUSTOMERv6:64500
ip prefix-list CUSTOMER:64500 permit 203.0.113.0/24
ip prefix-list CUSTOMER:64500 permit 192.0.2.0/24
ip prefix-list CUSTOMER:64500 permit 198.51.100.0/24
ipv6 prefix-list CUSTOMERv6:64500 permit 2001:db8:1000::/36 le 48
ipv6 prefix-list CUSTOMERv6:64500 permit 2001:db8:1001::/48 le 48
ipv6 prefix-list CUSTOMERv6:64500 permit 2001:db8:2002::/48 le 48
end
write mem
```

De forma predeterminada, IRRPT permite prefijos más específicos, hasta una máxima longitud de prefijo configurada. En este ejemplo, las máximas longitudes de prefijos configuradas fueron /24 para IPv4 y /48 para IPv6.

4.4.1.3 Herramientas para el aprovisionamiento de enrutadores

Una vez se genera la configuración, se debe seleccionar un medio o plataforma que pueda transmitir e implementar esta configuración en una infraestructura viva. Medios comunes de implementación incluyen SNMP + (T)FTP, vty (usualmente sobre SSH) y NETCONF (de nuevo, usualmente sobre SSH). En términos de plataformas, el stack de orquestación de código abierto Ansible y Network Service Orchestrator de Cisco, preveen soluciones más completas.

4.4.1.4. Una nota de precaución

Se debe tener aún mucha precaución antes de desplegar esta configuración en una infraestructura viva. Un simple error puede hacer que el tráfico se filtre incorrectamente, especialmente cuando se da servicios de tránsito.

Los autores recomiendan los siguientes mecanismos para asegurar que filtros erróneos (a aún la mala configuración de los filtros) no terminen siendo implementados:

Revisión simple de sintaxis

- Asegurar que los filtros generados no estén vacíos, que estén bien formados y que no tengan errores de sintaxis. Hay que notar que algunas plataformas de enrutamiento tratan las listas de prefijos vacías como "*allow any*" implícitos.
- Asegurar que los filtros no hagan referencia a direcciones y máscaras imposibles.
- Asegurar que no bloquearán inadvertidamente cualquier cosa que esté configurada de forma explícita para permitirse o pasar.

Revisiones delta

- Asegurar que si el filtro cambia por un delta o más del (n) porciento (donde *n* es un número acordado internamente, por ejemplo, 20%), entonces el filtro no sea implementado y que se evite la creación y/o implementación de cualesquiera otros filtros hasta que una persona revise la salida.

Prefijos baliza *(beacon prefixes)*

- Asegurar que los prefijos especiales para la organización están permitidos para pasar.
- Asegurar que los prefijos bogon nunca se les permitan atravesar el filtro.

4.4.1.5. Subcontratación del filtrado

Algunos IXPs proveerán servidores de rutas que estén pre-configurados para realizar filtrado de IRR. Al momento de escribir este documento, se les llama AMS-IX, DE-CIX, LONAP, INEX, NWAX, LyonIX, FIXO-IX y MSK-IX. Los servidores de rutas con filtros IRR se están volviendo más y más populares, así que se puede revisar con el IXP al que se conecta, si ofrece este servicio.

La subcontratación de filtros de salida en un IXP no cumple con MANRS. Eso sería como decir que se puede tirar basura y ser bien portado sólo porque alguien más lo va a limpiar. Ser bien portado significa no tirar basura desde un principio. Para cumplir con MANRS se tiene que estar seguro que la red que se posee tiene buen comportamiento. Los operadores pueden escoger confiar en esto para el filtrado entrante en los IXPs bajo su propio riesgo (sección 4.4.1.1 punto 3).

Las ventajas de hacer filtrado de IRR en servidores de rutas de IXP son:

- Ahorro de tiempo y esfuerzo para el operador de red
- Usualmente los IXP proveen múltiples servidores de rutas ejecutando diferente software para redundancia.
- Servidores de rutas con mantenimiento profesional, por tanto, menos posibilidad de errores.

Las desventajas de usar filtrado de IRR en servidores de rutas de IXP son:

- El filtrado saliente en servidores de rutas de IXP no es suficiente para cumplir con MANRS.
- Menos control sobre el filtrado
- Dependencia adicional en un tercero
- Dificultad para hacer excepciones

4.4.1.6. Lecturas adicionales

- IRR Power Tools (IRRPT)
  https://github.com/6connect/irrpt
- Internet Routing Registry Toolset (IRRToolset)
  https://github.com/irrtoolset/irrtooset
- BGPQ3
  https://github.com/snar/bgpq3

- Ansible
  http://www.ansible.com/
- Cisco Network Services Orchestrator
  http://www.cisco.com/go/nso
- IRR Explorer
  http://irrexplorer.nlnog.net/

4.4.2. Uso de RPKI para validar orígenes de rutas

La idea básica de validar los anuncios de rutas con RPKI es la misma que para los IRR. Un operador de red registra sus anuncios es forma de ROAs, y subsecuentemente, estos son usados por los operadores ya sea, para generar filtros (pseudo-IRR) o para etiquetar/validar anuncios usando técnicas más avanzadas como el protocolo RPKI-to-router.

RPKI trabaja con anclas confiables que son los puntos de inicio para verificar ROAs. Todos los RIRs publican anclas de confianza para el espacio de direccionamiento para el que son autoridad. ARIN requiere que los usuarios acepten un Acuerdo de la Parte que Confía (*Relaying Party Agreement*[3]), los otros RIRs hacen disponibles sus anclas de confianza sin restricciones.

4.4.2.1. Uso del validor RPKI de RIPE NCC

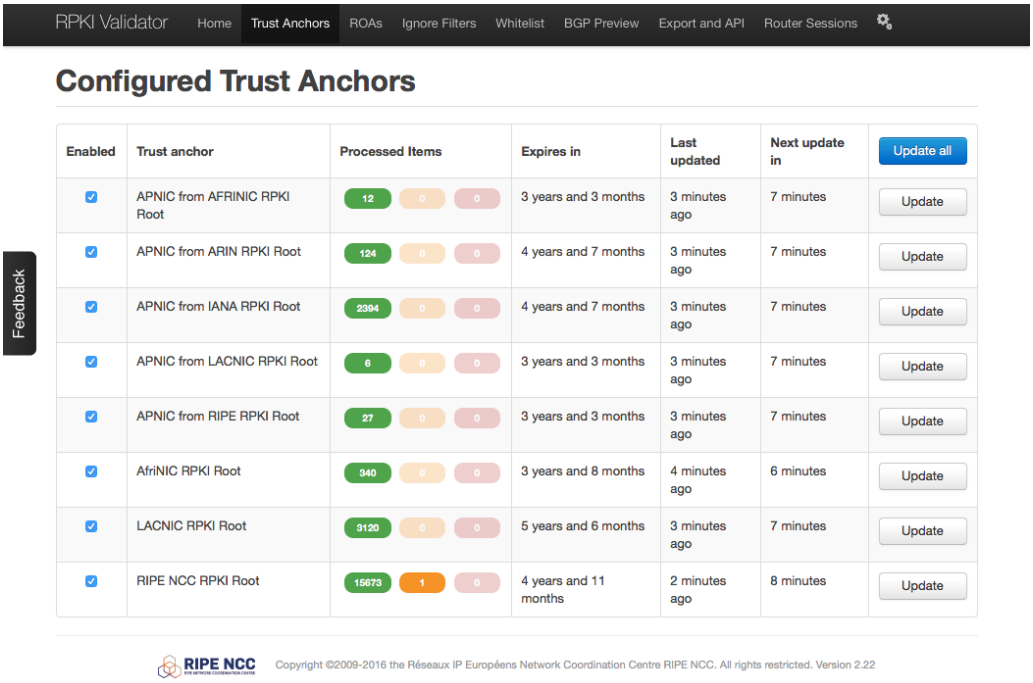
El validador RPKI de RIPE NCC está implementado con Java y brinda una excelente interfaz web para consultar manualmente los datos que ha recopilado. El validador se descarga del sitio web de RIPE NCC[4], se descomprime y se ejecuta:

```
rpki-validator.sh start
```

Esto inicia el software de validación, el cual provee un servidor web en el puerto 8080. La interfaz web permite supervizar la sincronización con las anclas de confianza:

[3] https://www.arin.net/resources/rpki/tal.html

[4] https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources



También permite consultar la base de datos de ROAs, contrastar los ROAs contra la tabla de enrutamiento de BGP (así vista por recolectores de rutas de RIPE NCC) y exportar los ROAs como objetos ROUTE/ROUTE6 para integrarlos con herramientas que puedan usar datos de IRR.

El validador también provee una interfaz RPKI-to-Router en el puerto 8282. Más adelante se muestra cómo hacer que un enrutador use este servicio.

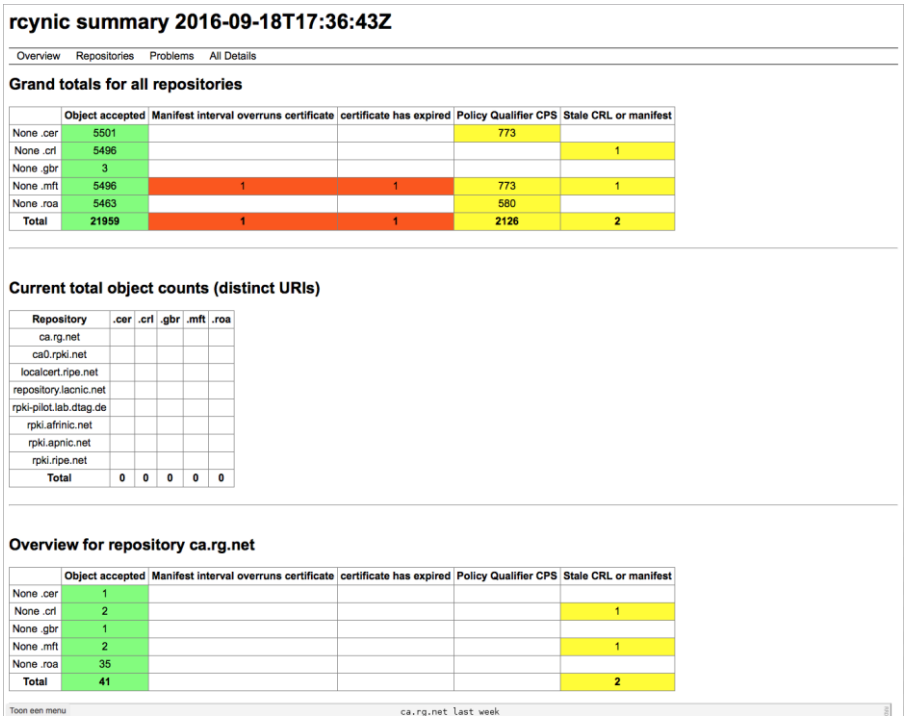
4.4.2.2. Uso de RPKI Tookit de Dragon Research Labs

La manera más fácil de usar el RPKI Toolkit es ejecutarlo en Ubuntu Xenial o Debian Jessie usando los repositorios APT[5] brindados. El software (validador) de Relaying Party se instala con:

```
apt install rpki-rp
```

Esto instalará todas las dependencias y un *cron-job* para actualizar cada hora el caché local. Las estadísticas se escriben como archivos HTML en /var/www/rcynic, los cuales pueden accederse comúnmente por medio del servidor web en http://<hostname>/rcynic/:

[5] https://download.rpki.net/APTng/



rcynic summary 2016-09-18T17:36:43Z

Overview Repositories Problems All Details

Grand totals for all repositories

	Object accepted	Manifest interval overruns certificate	certificate has expired	Policy Qualifier CPS	Stale CRL or manifest
None .cer	5501			773	
None .crl	5496				1
None .gbr	3				
None .mft	5496	1	1	773	1
None .roa	5463			580	
Total	**21959**	**1**	**1**	**2126**	**2**

Current total object counts (distinct URIs)

Repository	.cer	.crl	.gbr	.mft	.roa
ca.rg.net					
ca0.rpki.net					
localcert.ripe.net					
repository.lacnic.net					
rpki-pilot.lab.dtag.de					
rpki.afrinic.net					
rpki.apnic.net					
rpki.ripe.net					
Total	**0**	**0**	**0**	**0**	**0**

Overview for repository ca.rg.net

	Object accepted	Manifest interval overruns certificate	certificate has expired	Policy Qualifier CPS	Stale CRL or manifest
None .cer	1				
None .crl	2				1
None .gbr	1				
None .mft	2				1
None .roa	35				
Total	**41**				**2**

Toon een menu ca.rg.net last week

El paquete rpki-rp también brinda una interfaz RPKI-to-router por medio de xinetd en el puerto 323. Más adelante se muestra cómo hacer que un enrutador use este servicio.

4.4.2.3. Conexión de un enrutador a una interfaz RPKI-to-Router

El sitio web de RIPE NCC provee innumerables ejemplos sobre cómo configurar enrutadores para que usen un validador RPKI. Los siguientes ejemplos básicos están basados en su documentación.

4.42.3.1. Juniper JunOS

Primero se conecta el enrutador al validador RPKI. En el siguiente ejemplo, el enrutador con dirección 192.0.2.1 se conecta a un validador RPKI con dirección 192.0.2.2:

```
routing-options {
      validation {
            group rpki-validator {
                  session 192.0.2.2 {
                        refresh-time 120;
                        hold-time 180;
                        port 8282;
                        local-address 192.0.2.1;
                  }
            }
      }
}
```

El enrutador ahora llevará registro sobre cuáles rutas son válidas de acuerdo a los ROAs, cuáles rutas no son válidas y cuáles no están cubiertas por ROAs. Eso se puede usar en la política de enrutamiento:

```
policy-options {
      policy-statement validation {
            term valid {
                  from {
                        protocol bgp;
                        validation-database valid;
                  }
                  then {
                        validation-state valid;
                        community add origin-validation-state-valid;
                        next policy;
                  }
            }
            term invalid {
                  … etc …
```

Se pueden usar comando bajo `show bgp rpki` para verificar las sesiones al validador, los datos recibidos, etc:

```
#show bgp ipv4 unicast rpki servers
BGP SOVC neighbor is 192.0.2.2/8282 connected to port 8282
Flags 64, Refresh time is 60, Serial number is 60, Session ID is 914
InQ has 0 messages, OutQ has 0 messages, formatted msg 30
Session IO flags 3, Session flags 4008
      Neighbor Statistics:
      Prefixes 25773
      Connection attempts: 250
      Connection failures: 244
      Errors sent: 0
      Errors received: 2

Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 255
Local host: 192.0.2.1, Local port: 46721
Foreign host: 192.0.2.2, Foreign port: 8282
… etc …
```

4.4.2.3.3. Cisco IOS XR

El validador RPKI puede configurarse bajo el proceso de enrutamiento BGP:

```
router bgp 64500
      rpki server 192.0.2.2
            transport tcp port 8282
```

El enrutador llevará registro sobre cuáles rutas son válidas de acuerdo a los ROAs, cuáles rutas no son válidas y cuáles rutas no están cubiertas por ROAs. Eso puede usarse en la política de enrutamiento:

```
route-policy rpki
     if validation-state is valid then
          set local-preference 999
     endif
     … etc …
```

Se pueden usar comandos baso `show bgp rpki` para verificar las sesiones al validador, los datos recibidos, etc.:

```
# show bgp rpki summary
RPKI cache-servers configured: 1
RPKI global knobs
     Origin-AS validation is ENABLED globally
     Origin-AS validity WILL NOT affect bestpath selection globally
     Origin-AS validity signaling towards iBGP is DISABLED globally
RPKI database
     Total IPv4 net/path: 23854/24733
     Total IPv6 net/path: 3368/3507
```

4.4.2.4. Lecturas adicionales

Documentación técnica sobre RPKI y los protocolos subyacentes:

- The IETF SIDR working group (donde se desarrolla RPKI) https://tools.ietf.org/wg/sidr/
- An Infrastructure to Support Secure Internet Routing https://tools.ietf.org/html/rfc6480
- RPKI Relying Party tools https://rpki.net/wiki/doc/RPKI/RP
- RIPE NCC RPKI Validator https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources
- Dragon Research Labs RPKI Tookit https://github.com/dragonresearch/rpki.net

- Cisco: IOS XE – BGP Configuration Guide – Origin AS Validation http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-16/irg-xe-16-book/bgp-origin-as-validation.html
- Cisco IOS XR – BGP Prefix Origin Validation Based on RPKI http://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r4-2/routing/configuration/guide/b_routing_cg42asr9k/b_routing_cg42asr9k_chapter_00.html#concept_A84818AD41744DFFBD094DA7FCD7FE8B
- Juniper: Configuring Origin Validation for BGP http://www.juniper.net/documentation/en_US/junos16.1/topics/topic-map/bgp-origin-asvalidation.html

4.4.3. Validación de camino (PATH)

La validación de caminos (path validation) busca validar el atributo AS_PATH dentro de un anuncio de prefijo. Para estos propósitos, un camino se considera válido si es consistente con las políticas de enrutamiento de cada AS recorrido por el camino. Por tanto, tal validación requiere que una descripción autorizada de la política de enrutamiento de cada ASN, esté disponible públicamente.

La validación automática (con ciertas limitaciones) de un AS_PATH puede lograrse "concatenando juntas" de forma lógica las políticas documentadas de los ASs individuales en el camino. Por tanto, los participantes de MANRS deberán expresar su propia política tan profundamente como sea posible, para facilitar la validación por redes de terceros.

Como mínimo, según se describe antes, cualquier operador que provea servicios de tránsito a redes de clientes con potencialmente múltiples proveedores (independientemente si tales clientes operan un AS o no) deberán implementar un mecanismo de filtrado en los anuncios salientes hacia sus peers que no son clientes, para asegurar que solamente se aprendan prefijos de cliente directamente de los clientes (en lugar de otra vía tal como una red intermedia).

Mientras que es posible crear filtros de AS_PATH describiendo todos los posibles caminos válidos del cliente, tal aproximación puede escalar pobremente con el tiempo, dadas las herramientas actuales. Una aproximación alterna es la de agregar un atributo de comunidad a las rutas recibidas de los clientes, a medida se importan, y configurar filtros salientes en dirección a los peers que no son clientes, de modo que filtren solamente las rutas que llevan el atributo de comunidad correcto (adicionalmente a los basados en prefijo, descritos antes).

5. Resumen

Ser un operador de red responsable requiere tanto publicar información de contacto y de la política de enrutamiento, así como usar la información publicada por otros para verificar la información en la tabla de enrutamiento.

5.1. Publicación de información – Lista de verificación

Existen muchos lugares donde se puede publicar información. Este resumen puede usarse como una lista de verificación al publicar y actualizar información, y puede incluirse en los procesos y procedimientos de la organización.

- Para la región de AFRINIC, APNIC y RIPE NCC:
    - Publicar información de contacto para roles/departamentos como objetos ROLE Opcionalmente: crear objetos PERSON para miembros del staff y vincular desde los ROLE.
    - Crear objetos IRR y referirlos a los POCs correctos desde esos objetos; documentar la política de enrutamiento:
        - INETNUM y INET6NUM
            - admin-c: referirse a los administradores de IPAM (Administrador de direcciones IP).
            - tech-c: referirse a los administadores de los sistemas en la red.
        - AUT-NUM
            - admin-c: referirse la coordinador de peering.
            - tech-c: referirse al NOC.
            - mp-import/mp-export: documentar las conexiones BGP.
        - ROUTE y ROUTE6
            - remarks: documentar contactos para el NOC, escritorio de abuso, etc.
            - ping-hdl: referirse al NOC.
    - Crear ROAs RPKI para todos los prefijos que se anuncian desde el ASN.
    - Publicar en PeeringDB las ubicaciones de peering, políticas y contactos.
    - Publicar en el sitio web las ubicacioines de peering, políticas y contactos.
    - Publicar en el sitio web los contactos para el NOC y abuso.

- Para la región de LACNIC:

- Publicar información de contacto para roles/departamentos como objetos POC.
- Publicar información de contacto para las organizaciones responsables de recursos (asignados directamente por LACNIC o re-asignados por un LIR).
- Publicar el DNS que provee la resolución inversa para bloques IP.
- Referenciar los POCs correctos para los recursos: tech-c: referirse al administador de IPAM (Administrador de direcciones IP). abuse-c: referirse al escritorio de abuso de la red.
- Crear ROAs RPKI para todos los prefijos que se anuncian desde los ASNs.
- Publicar las ubicaciones de peering, política y contactos en PeeringDB.
- Publicar las ubicaciones de peering, política y contactos en el sitio web.
- Publicar los contactos de NOC y abuso en el sitio web.

- Para la región de ARIN:
  - Publicar información de contacto para roles/departamentos como objetos POC.
  - Hacer las referencias a los POCs desde los recursos.
    - NET
      - NOC POC: referirse al NOC y opcionalmente a los administradores de sistemas.
      - Tech POC: referirse a los administradores de IPAM.
      - Abuso POC: referirse al escritorio de abuso de sistemas.
    - ASN
      - NOC POC: referirse al NOC y coordinador de peering.
      - Tech POC: referirse a los administradores de IPAM.
      - Abuse POC: referirse al escritorio de abuso de sistemas.
  - Crear objetos IRR y referirlos a los POCs correctos. Documentar la política de enrutamiento:
    - INETNUM e INET6NUM
      - admin-c: referirse a los administradores de IPAM.
      - tech-c: referirse a los administradores de los sistemas.
    - AUT-NUM
      - admin-c: referirse a los coordinadores de peering.
      - tech-c: referirse al NOC.
      - mp-import/mp-export: documentar las conexiones BGP
    - ROUTE y ROUTE6

        - remarks: documentar contactos para el NOC, escritorio de abuso, etc.
    - Crear ROAs RPKI para todos los prefijos anunciados desde los ASNs.
    - Publicar las ubicaciones de peering, políticas y contactos en PeeringDB.
    - Publicar las ubicaciones de peering, políticas y contactos en el sitio web.
    - Publicar los contactos para el NOC y abusos en el sitio web.

5.2. Validación de la información – Lista de verificación

La operación responsable de una red requiere la validación del tráfico que el operador y sus clientes envían al resto de Internet, así como la validación de las rutas que los upstreams, peers y clientes le anuncian al operador. La falta de validación de cualquiera de ellas vuelve a la red vulnerable al secuestro de rutas y origen potencial de tráfico de ataques DDOS.

- Aplicar a las conexiones de clientes ACLs y/o filtros uRPF.
- Aplicar a las redes propias ACLs, filtros uRPF y/o filtros SAVI.
- Usar la información en los IRRs para filtrar rutas que los vecinos anuncien.
- Verificar las rutas en la tabla de enrutamiento contra los ROAs RPKI

6. Información adicional

- Denegar prefijos IPv6 en sesiones BGP IPv4.
- Al momento, no se pueden encontrar filtrado de rutas bogon en este documento 0/8, 10/8, 127/8, 172.16/12, 169.254/16, 192/24, 192.0.2/24, 192.168/16, 198.18/15, 198.51.100/24, 203.0.113/24, 224/4, 240/4. Se recomienda negar también 100.64/10.
- ::/128, ::1/128, ::FFFF:0:0/96, ::<ipv4-address>/96, 100::/64, fe80::/10, fc00::/7, 2001:db8::/32, 2001:10::/28, ff00::/8 (en sesiones unicast).
- Seguridad BGP (MD5, TCP AO)
- Filtrado de backbone / infraestructura, tal como PTP, loopbacks, etc.

7. Materiales antecedentes históricos

Este documento está hecho sobre décadas de trabajo de profesionales de redes y seguridad alrededor del mundo, quienes han desarrollado, implementado y comunicado técnicas que dan lugar a una Internet más robusta. La siguiente lista de materiales trata de capturar todo el trabajo sobre el cual este documento está basado.

[Comenzar agregando todas las pláticas entre todos los NOGs como un primer paso allá por 1996]

RFC2827 también conocido como BCP38
Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
http://www.ietf.org/rfc/rfc2827.txt

SSAC004
Securing the Edge
http://www.icann.org/committees/security/sac004.txt

SSAC008
DNS Distributed Denial of Service (DDoS) Attacks
http://www.icann.org/committees/security/dns-ddos-advisory-31mar06.pdf

Spoofer Project
https://spoofer.caida.org/

RFC3024 - Reverse Tunneling for Mobile IP, revised
ftp://ftp.rfc-editor.org/in-notes/rfc3024.txt

ISOC Anti-Spoofing Page
http://www.Internetsociety.org/deploy360/anti-spoofing/

"Network Hygiene Pays Off" - The Business Case for IP Source Address Verification - Joao Luis Silva Damas & Daniel Karrenberg, https://www.ripe.net/publications/docs/ripe-432

“RIPE Anti-Spoofing Task Force HOW-TO”, https://www.ripe.net/publications/docs/ripe-431

Comparative Evaluation of Spoofing Defenses - Ezra Kissel, University of Delaware and Jelena Mirkovic, USC/ISI

Understanding the Efficacy of Deployed Internet Source Address Validation Filtering - Robert Beverly MIT CSAIL, Arthur Berger MIT CSAIL, Young Hyun CAIDA, k claffy CAIDA

RFC 4948 - Report from the IAB workshop on Unwanted Traffic March 9-10, 2006

8. Agradecimientos

Los autores principales de este documento son David Freedman, Brian Foust, Barry Greene, Ben Maddison, Andrei Robachevsky, Job Snijders y Sander Steffann. También agradecemos a Will van Gulik, Jakob Heitz y Aris Lambrianidis, Kevin Meynell y Massimiliano Stucchi por sus revisiones y contribuciones a este documento.

La traducción al castellano fue realizada por Enrique Fernández y Daniel Aguilar, del Capítulo ISOC de El Salvador, Mayo de 2020, como parte del programa de capacitación de Internet Society a los capítulos.