MANRS

Mutually Agreed Norms for Routing Security

Mauricio Oviedo

Email: mauricio@socium.cr

Emmanuel Serrano

Email: isc.emmanuel.serrano@gmail.com

Temas Sesiones

Sesión 1: Introducción a MANRS

Sesión 2: Acciones de MANRS

I. IRRs, RPKI, and PeeringDB

II. Coordinación y Validación Global

III. Filtrado: prevención de la propagación de información de enrutamiento incorrecta

IV. Anti-Suplantación: Prevención del tráfico con direcciones IP de origen falsificadas

IRRs, RPKI, and PeeringDB

Objetivo

Entender las bases de datos y repositorios que los participantes en MANRS pueden utilizar las políticas de ruteo y los datos de contacto principales.

Aprenderá qué objetos de las bases de datos debe utilizar para documentar las la información de enrutamiento relacionada con su red y cómo registrar la información en el sistema de RPKI.

Aprenderá a como utilizar Peering DB y otras bases de datos para publicar su información de contacto.

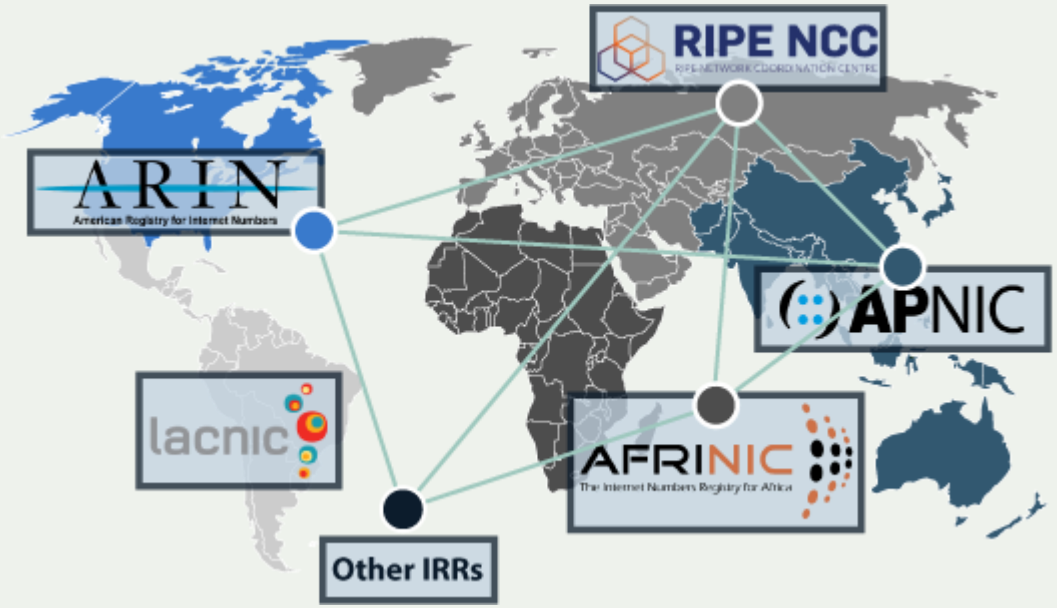
Introducción

Para cumplir con todas las acciones de MANRS, los operadores de red necesitan publicar información sobre sus redes en diversas bases de datos y repositorios.

- Internet Routing Registries – IRRs
- Resource Public Key Infraestructure – RPKI
- Peering DB.

Internet Routing Registries – IRRs

Internet Routing Registries – IRRs



Los IRRs mantienen el Registro de Enrutamiento de Internet y es una base de datos pública de los objetos de ruteo de Internet.

Los IRRs se utilizan para determinar y compartir rutas y otra información relacionada con la configuración de los ruteadores, con el fin de evitar problemas en la publicación global de rutas en Internet.

Si el *Registro Regional de Internet (**RIR)*** en su región opera un IRR, debe de utilizarlo para documentar su Política de Enrutamiento de redes y los anuncios de rutas relacionados.

Internet Routing Registries – IRRs

Existe una gran cantidad de IRRs.

- El más conocido es RADB

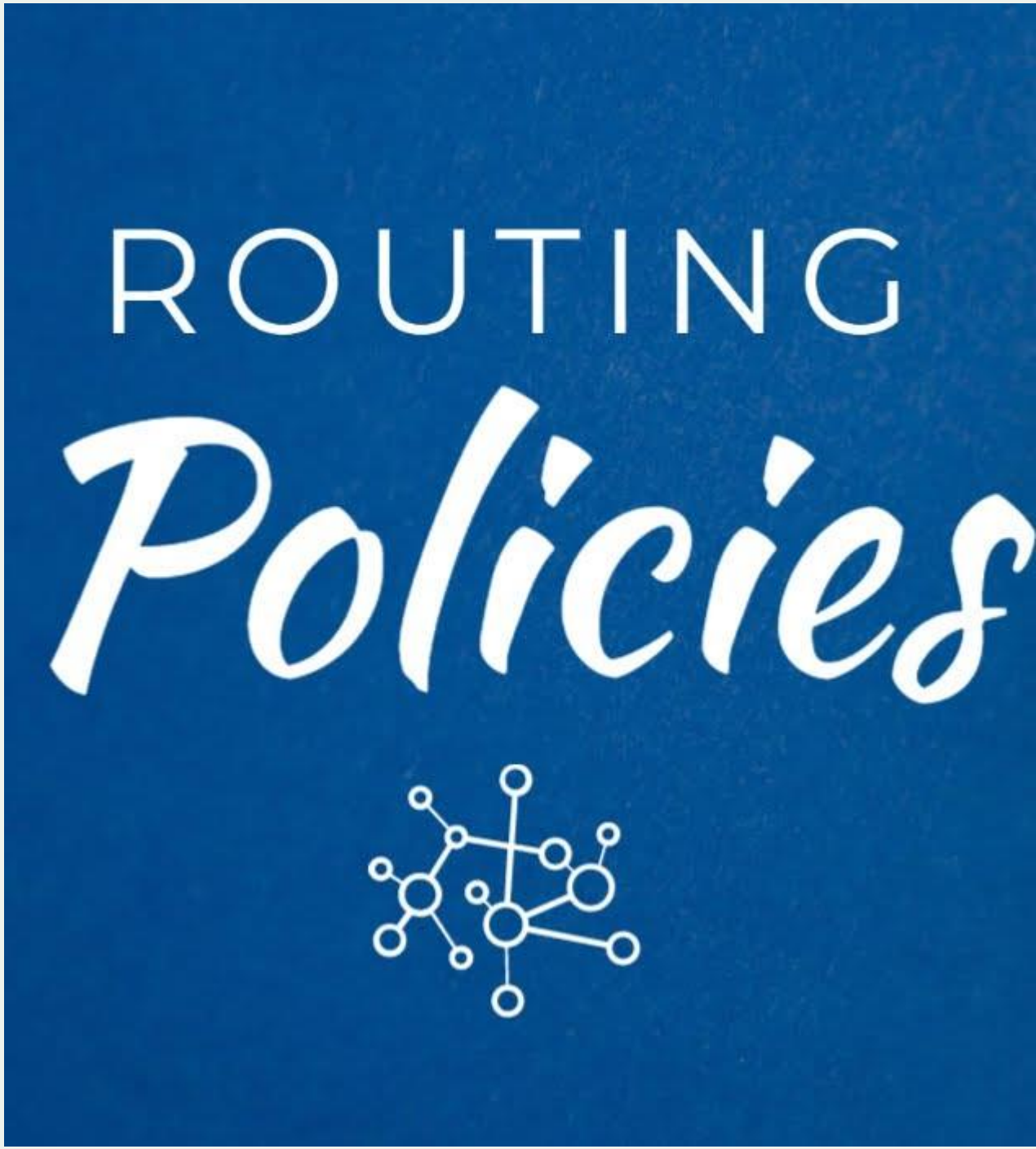
Para nuestra región ya LACNIC cuenta con su propio IRR.

Region	Preferred IRR	Alternative IRR
America	ARIN	RADb/NTTCOM
Africa	AFRINIC	RADb/NTTCOM
Asia Pacific	APNIC	RADb/NTTCOM
Europe	RIPE NCC	RADb/NTTCOM
Latin America and Caribbean	LACNIC	NTTCOM

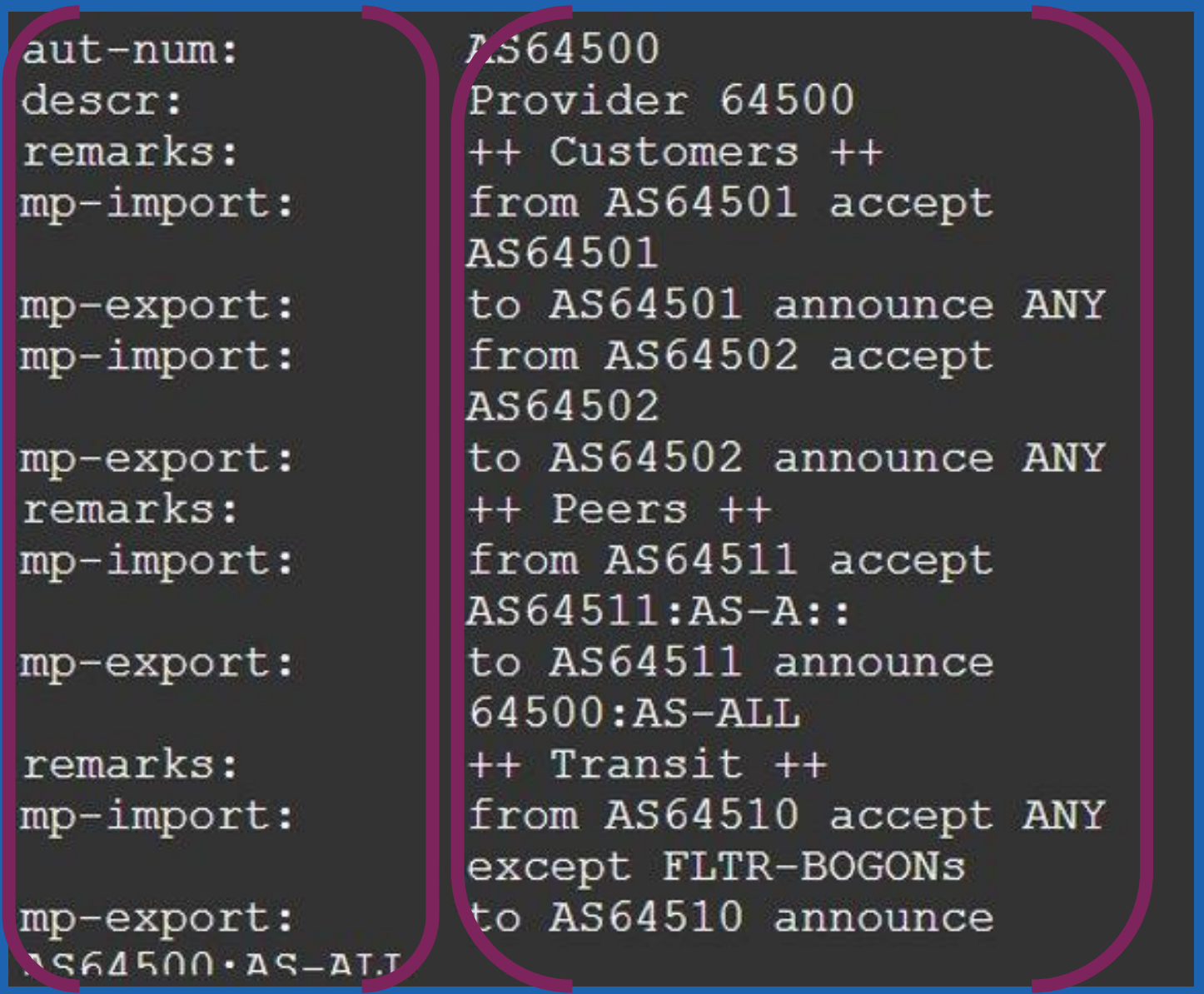
Network Routing Policy

Una de las acciones de MANRS requiere que los participantes se aseguren que la información del enrutamiento de su red se encuentre disponible públicamente.

Esta información de enrutamiento es conocida como **Network Routing Policy,** se documenta mediante el **Routing Policy Specificatión Language (RPSL)**, y se almacena en una base de datos del IRRs.



Atributos de los objetos



Valores de los Atributos

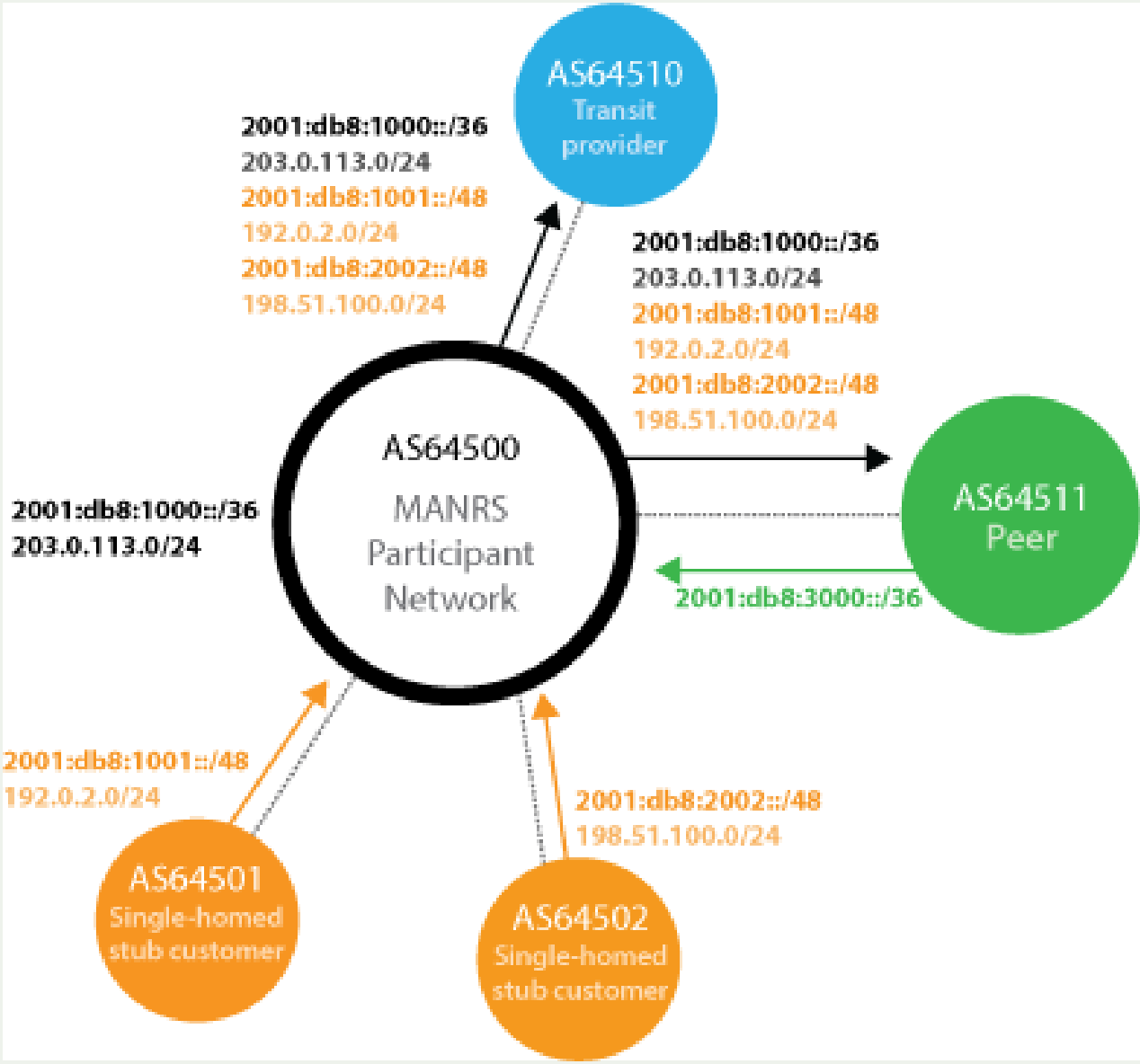
Network Routing Policy

Información relacionada con los recursos de Internet, o funciones soportadas, son contenidas dentro de los objetos de RPSL y almacenadas en un IRRs, algunos objetos son:

AUT-NUM

Los objetos AUT-NUM contienen los detalles del registro de un Número de Sistema Autónomo que ha sido asignado a un Sistema Autónomo (AS) por un IRR.

También permiten publicar las Políticas de Enrutamiento de la Red por un IRR.



AUT-NUM

Los objetos AUT-NUM contienen los detalles del registro de un Número de Sistema Autónomo que ha sido asignado a un Sistema Autónomo (AS) por un IRR.

También permiten publicar las Políticas de Enrutamiento de la Red por un IRR.

```
aut-num:        AS64500
descr:          Provider 64500
remarks:        ++ Customers ++
mp-import:      from AS64501 accept
                AS64501
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-A::
mp-export:      to AS64511 announce
                64500:AS-ALL
remarks:        ++ Transit ++
mp-import:      from AS64510 accept ANY
                except FLTR-BOGONs
mp-export:      to AS64510 announce
AS64500:AS-ALL
```

ROUTE/ROUTE6

Contienen información de enrutamiento para los recursos de espacio de direccionamiento IPv4 e IPv6.

Muestran las rutas que origina un AS.

```
route:          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
```

El objeto *route6* muestra que el AS 64500 puede anunciar del prefijo /36

AS-SET

Los AS-SET se utilizan para agrupar los ASN de forma significativa para facilitar la especificación de la política de enrutamiento.

Un AS-SET se utiliza para describir el cono de clientes de su red; un conjunto de ASNs que son propiedad de sus clientes.

```
as-set:          AS64500:AS-CUSTOMERS
descr:           AS64500 regional customers
members:         AS64501, AS64502
tech-c:          EXAMPLE1-AP
admin-c:         EXAMPLE2-AP
mnt-by:          MAINT-AS64500
last-modified:   2008-09-04T06:40:26Z
source:          APNIC
```

El ejemplo contiene todos los clientes del AS 64500 que incluyen los del AS64501 y AS64502 puede anunciar del prefijo /36

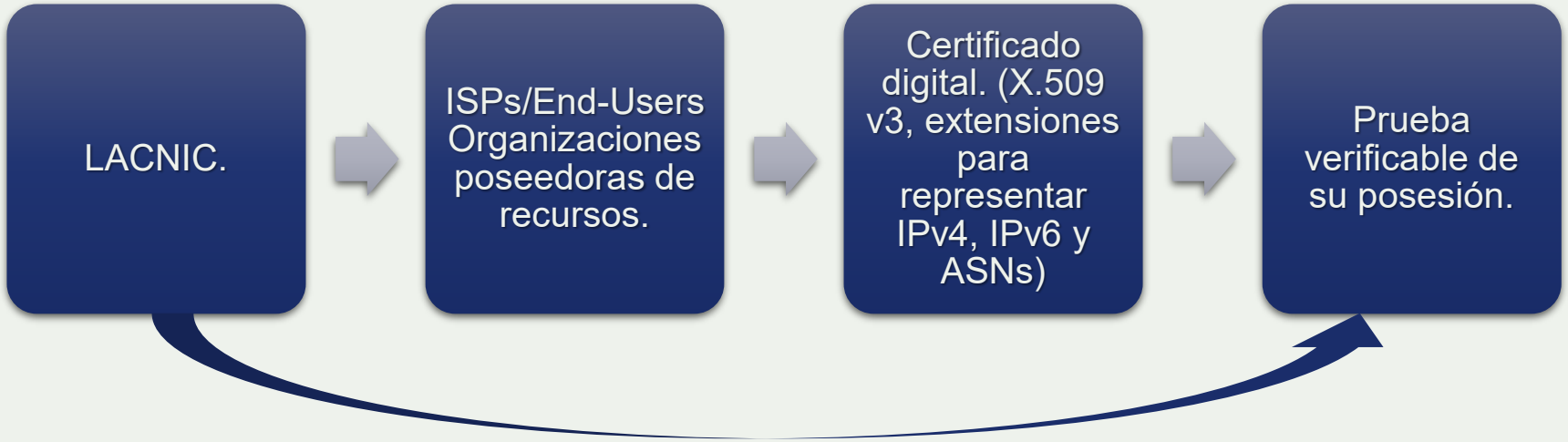
RPKI

¿Qué es RPKI?

Resource Public Key Infraestructure o RPKI, es una estructura de seguridad de enrutamiento que permite a validar el derecho de una organización de utilizar un recurso de Internet determinado.

Define una infraestructura de clave especializada para ser aplicada al enrutamiento.

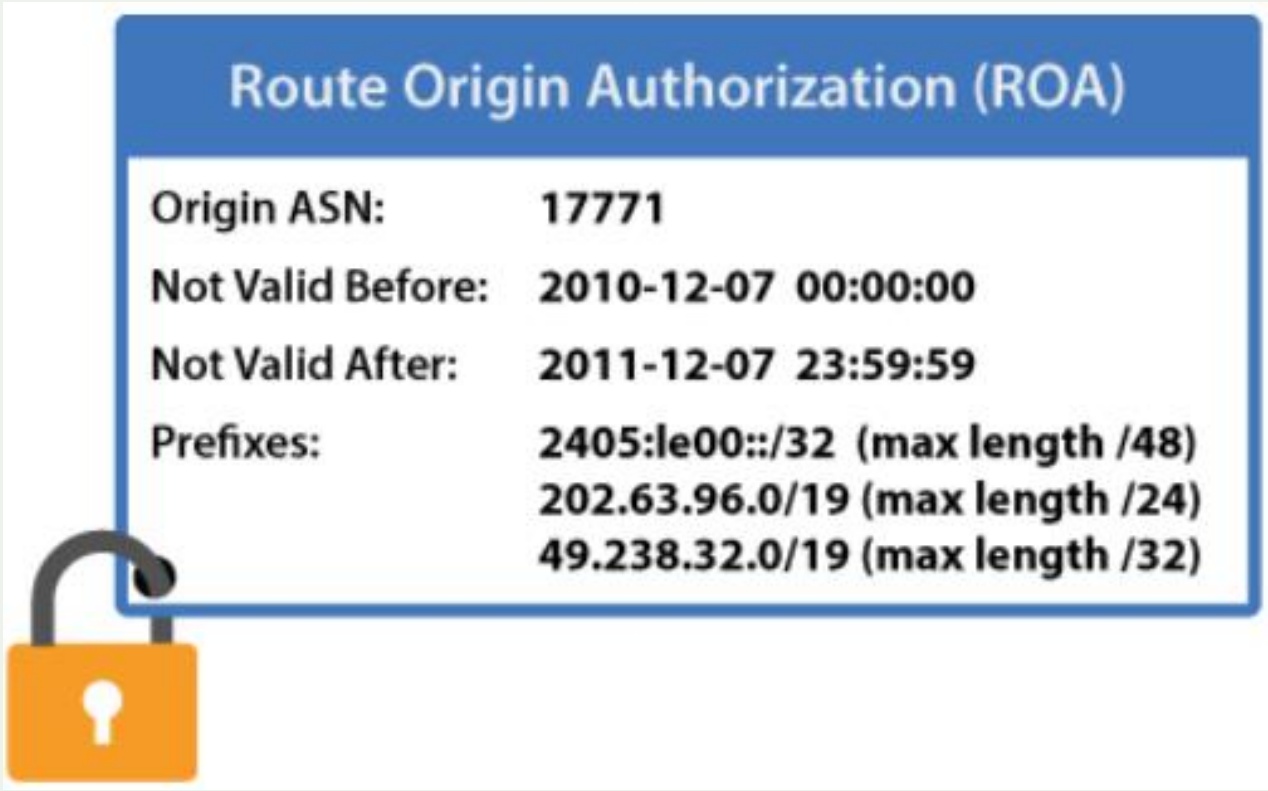
En particular, para BGP.



ROA

Además de proporcionarle información a un sistema IRR, se recomienda registrar las rutas que origina y anime a sus clientes para que registren sus rutas en el repositorio RPKI, creando allí un objeto de Autorización de Origen de Ruta (ROA).

Los objetos ROA, son objetos firmados criptográficamente que indican los prefijos que un AS está autorizado a originar.



RPKI

Cuando se crean ROAs, hay que poner especial atención al campo: **Most specific length allowed.**

Esto indica la longitud del prefijo IP más especifico permitido que el AS está autorizado a anunciar.

Si se establece la longitud del prefijo, un ROA puede invalidar los anuncios de prefijos más específicos, a menos que también se creen otros ROAs

AS number	Prefix	Most specific length allowed	Affects
AS8391	2a00:8647::/32	32	1
AS203993	185.54.92.0/22	22	1
AS57771	37.77.56.0/21	24	2
AS57771	2a00:8640::/32	36	1
AS203993	2a00:8642::/32	36	1

Peering DB

PeeringDB

Es un recurso abierto para las redes que compartan su información de peering y otra información relevante entre ellos.

Los operadores de redes son responsables de mantener sus registros.

Un registro de PeeringDB le permite consolidar la información de su red en un solo punto y observar la información de otras redes.

Los registros de PeeringDB se utilizan para complementar la información de enrutamiento almacenada en los IRRs y en los repositorios de RPKI.

Le permite publicar información para que otras redes conozcan su red y sepan cómo contactar con ella, y es la primera parada al momento de decidir con dónde y con quién hacer peering.

PeeringDB

Para utilizar PeerinDB debe de tener una cuenta registrada. Después de registrarse debe de solicitar la afiliación de su organización o AS para desbloquear el acceso a los datos.

Autoevaluación

En este momento, iniciemos con los procesos de autoevaluación de nuestros recursos.

- Registros de RPKI
- Generación de ROAS.
- Registro en PeeringDB

Autoevaluación

- Certificación de Recursos de LACNIC:
  - https://www.lacnic.net/502/1/lacnic/certificacion-de-recursos-rpki
- PeeringDB:
  - https://www.peeringdb.com/
- IRR:
  - https://lacnic.zendesk.com/hc/es/articles/360038527114-Que-es-el-IRR-
  - http://www.irr.net/docs/list.html
- AS Routing Consistency:
  - https://stat.ripe.net/widget/as-routing-consistency#w.resource=[ASN]

MANRS

Nota: Sustituir [ASN] por el valor de su ASN

Referencias

- RPKI:
  - https://www.iar.mx/jsf/static_content/services/current_services/resources_certification/rpkInfrastructure.jsf
- RPKI –Validación de Origen BGP:
  - https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2016/15551-EC/7A.pdf
- LACNIC RPKI
  - https://lacnic.zendesk.com/hc/es/sections/206490008-RPKI

Autocapacitación

- Webinar: Seguridad de red con RPKI – LACNIC Junio 2021
  - https://www.lacnic.net/5407/1/lacnic/

- Tutorial Enrutamiento Seguro – LACNIC36 Octubre 2021
  - https://youtu.be/NVXkay3w358

Acción 3: Coordinación Global

Acciones de MANRS

Los participantes de MANRS deberán realizar las siguientes acciones para facilitar la **comunicación global entre los operadores de redes.**

- Mantener accesible globalmente y actualizada la información del contacto.

Introducción a la Coordinación.

La prevención y mitigación exitosa de los incidentes de enrutamiento dependen en gran medida de la efectiva comunicación operativa y coordinación efectiva entre los operadores de redes alrededor del mundo.

Es esencial que se mantenga actualizada la información de contacto en las bases de datos de acceso público.

Se recomienda a los operadores de red mantengan su información de contacto en varias bases de datos.

- Como mínimo, se debe registrar y mantener su información de contacto 24/7 en al menos una de estas bases de datos.

POC

Esta información de contacto debe de incluir Punto de Contacto (POC) actual de su:

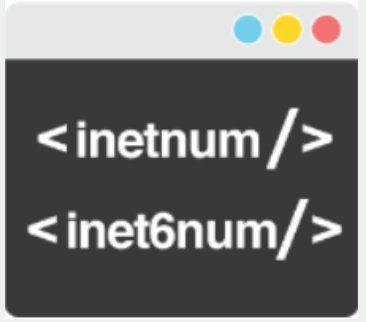
- Centro de Operación de Red (Network Operation Center – NOC)
- Bloques de Red.
- Nombre de Dominio.

Base de Datos WHOIS

Base de Datos WHOIS del RIR

Si bien todos los RIRs requieren que sus registrantes mantengan actualizada su información de contacto principal, también ofrecen la función de añadir contactos e información de contacto adicionales a los registros de sus bases de datos.

AFRINIC, APNIC y RIPE mantienen un sistema Whois que combina el registro de recursos de Internet con su propio IRR. Esto significa que existen objetos adicionales que debe crear, incluyendo **mntner, role** e **inetnum/inetnum6**.



mnter

Un objeto mantenedor (mnter) en la base de datos Whois del RIR es utilizado para administrar la autorización y autenticación. Protege a otros objetos de ser actualizados por personas no autorizadas.

Para proteger a otros objetos, uno o varios atributos 'mnt-by' hacen referencia al objeto "mntner". Con el objeto protegido, solo se admiten cambios a los objetos cuando el actualizador puede autenticarse a sí mismo como uno de los mantenedores.

Role

Un objeto de **rol** se puede registrar en una base de datos Whois del RIR y se identifica por su atributo **nic-hdl**.

Tiene una función similar al objeto persona, ya que ambos objetos hacen referencia a un Punto de Contacto (POC) importante.

Sin embargo, se prefiere un objeto de rol porque, si bien la gente cambia de trabajo con frecuencia, su rol no se modifica.

```
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
```

Este es un ejemplo de un típico objeto de rol que utiliza el atributo "remark" para proporcionar información adicional.

Inetnum/inet6num

La información sobre los recursos como los bloques de direcciones IP y los números de AS son registrados en los RIRs, los rangos de IPv4 y los prefijos de IPv6 se documentan utilizando los objetos **inetnum** e **inet6num**.

Hay atributos como "**tech-c**" que deberían hacer referencia a objetos que contienen información de contacto

```
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
```

Este es un ejemplo de un objeto **inet6num**.Hace referencia al objeto de **rol** del atributo tech-c (usando el nombre especificado en el atributo **nic-hdl** del objeto de rol).

Lectura Adicional

Dado que los IRR se utilizan para validar la información de enrutamiento, debe mantener la información de contacto dentro de los distintos objetos que contienen información de enrutamiento (por ejemplo, objetos aut-num, as-set y route-set).

Para hacerlo, simplemente añada un atributo **tech-c** a todos los objetos y haga referencia a un objeto rol o persona.

Los objetos route/route6 no admiten la adición de un atributo **tech-c**. En lugar de ello, debe utilizar el atributo **remarks** e indicar dónde se puede encontrar información de contacto.

```
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
```

Base de Datos IRR

Base de Datos

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

Como se mencionó, se puede consultar la información de contacto en la mayoría de los objetos de IRR (AUT-NUM, AS-SET y ROUTE-SELF) mediante el atributo **tech-c.**

Objetos route/route6

```
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
```

Los objetos route/route6 no admiten un atributo "tech-c". En lugar de ello, la forma recomendada para agregar información de contacto a los objetos ROUTE/ROUTE6 es consultar la información de contacto mediante el atributo "remarks".

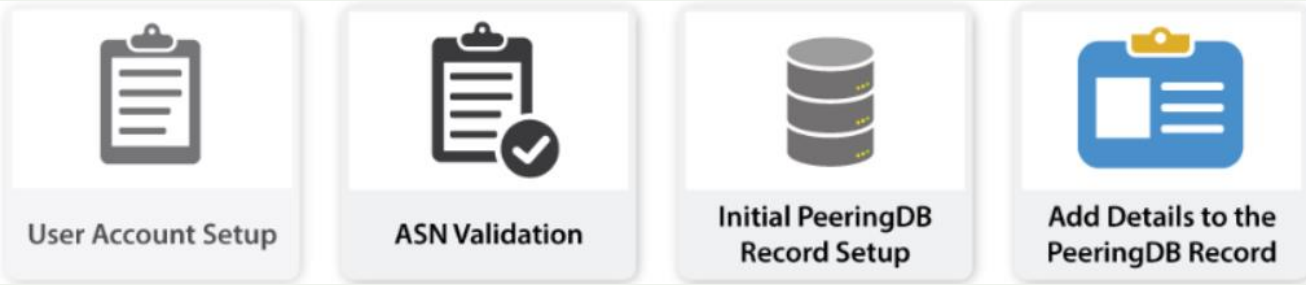
PeeringDB

PeeringDB

Es un recurso abierto para que las redes compartan entre sí su información de intercambio de tráfico y otra información pertinente.

Las redes son responsables de mantener sus registros en la base de datos. Contar con un registro PeeringDB le permite consolidar la información de su red en una sola ubicación.

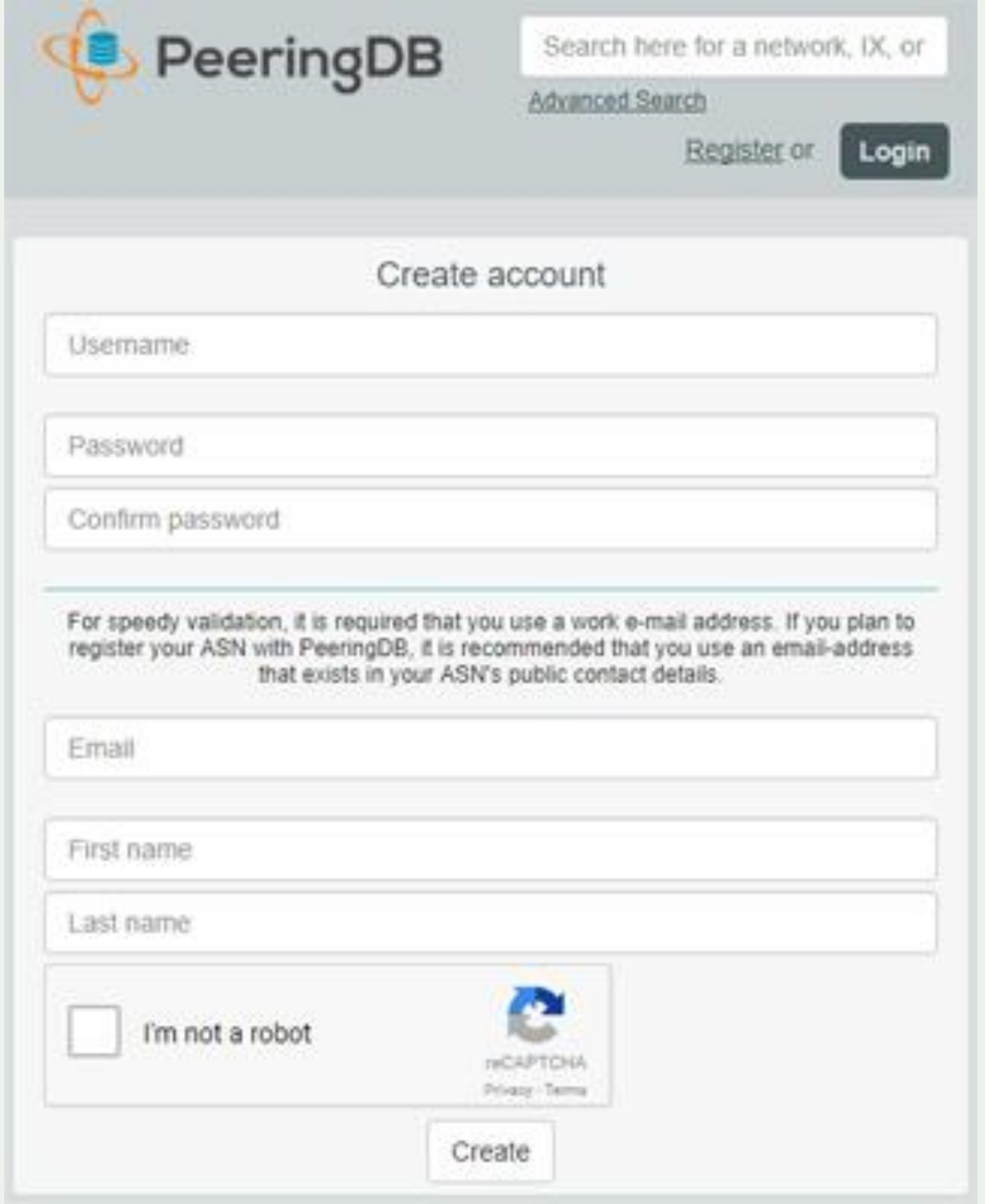
Los participantes de MANRS deben crear y mantener su información de contacto en PeeringDB. Hay cuatro pasos para configurar un nuevo registro de PeeringDB.



1. Crear cuenta de usuario

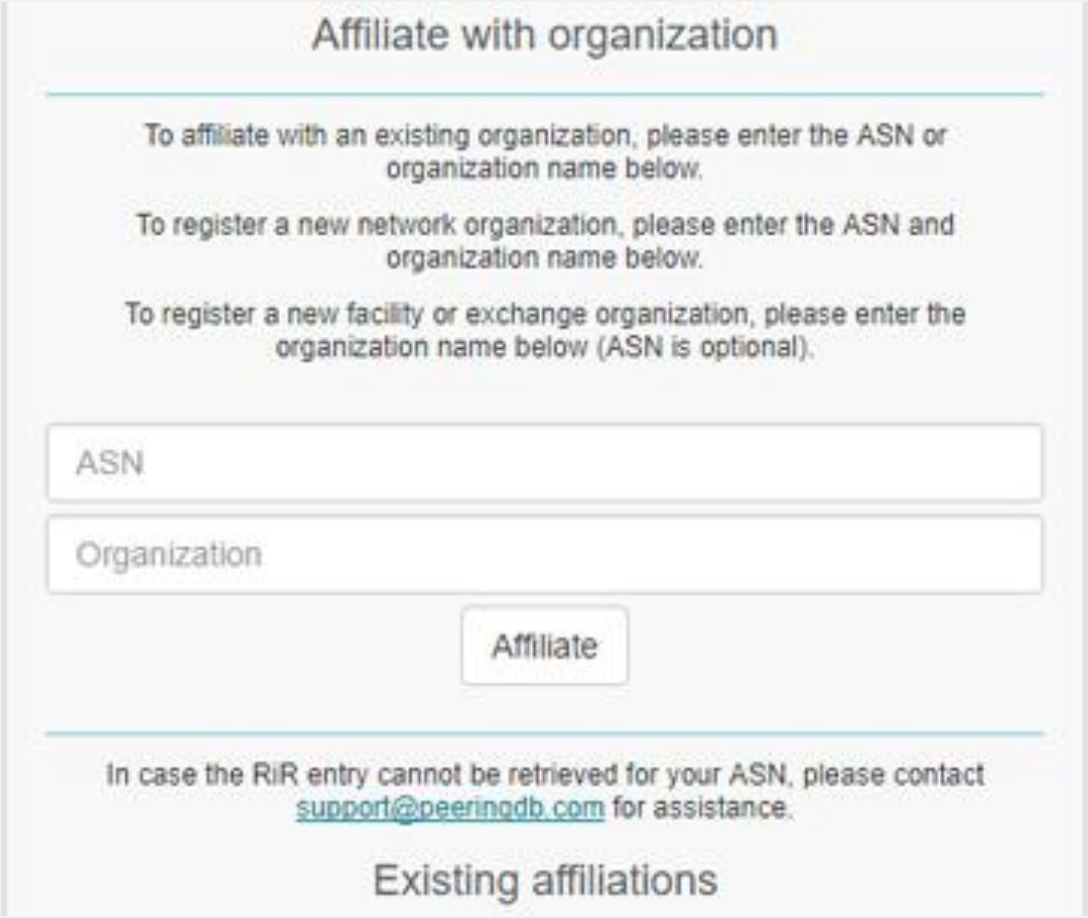
Debe de crear una cuenta en el portal www.peeringdb.com/register y proporcionar los siguientes datos:

- Nombre de usuario
- Contraseña
- Dirección de correo
- Su Nombre



2. Validación de ASN.

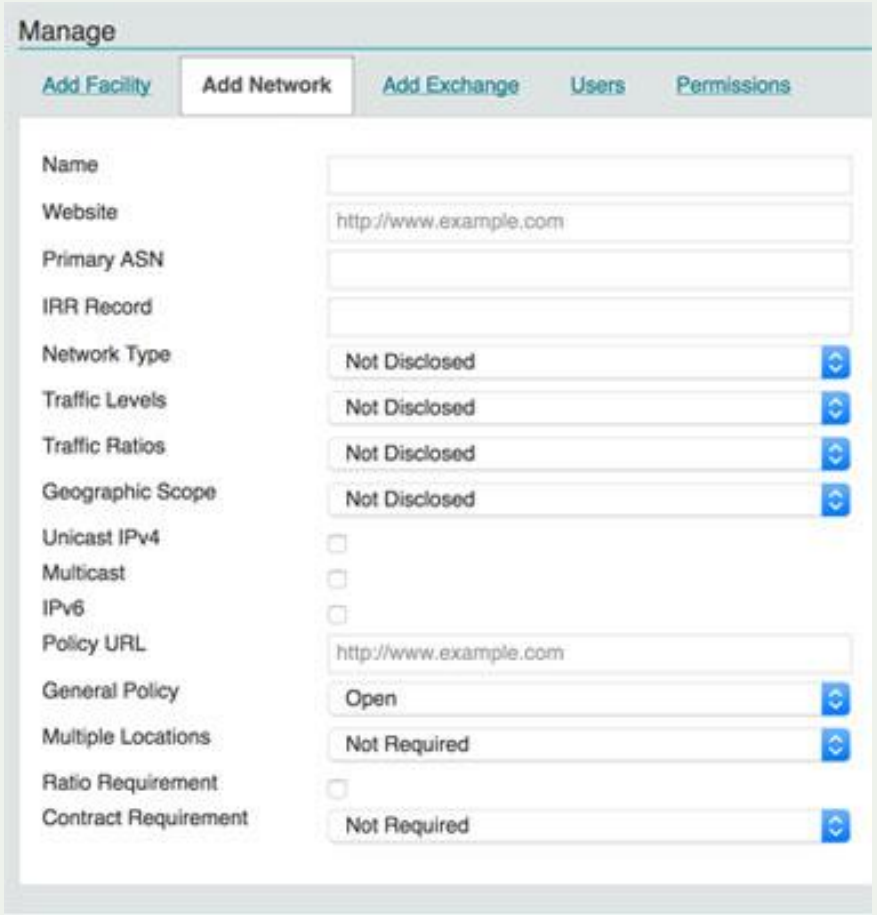
- Asocie su cuenta de usuario a una organización.
- La asociación entre usuario y organización se validará por el equipo de PeeringDB para las organizaciones nuevas.
- El equipo de administración de PeeringDB intentará validar su solicitud de creación de cuenta de usuario.
- Se enviará un correo electrónico de confirmación cuando su organización haya sido aprobada.



3. Configuración inicial del registro en PeeringDB

Una vez que se haya validado su ASN, siga los siguientes pasos para configurar su registro inicial de PeeringDB:

- Inicie sesión en su cuenta de usuario.
- Seleccione el ícono de navegación ubicado en la esquina superior derecha y seleccione "Su organización".
- Complete y guarde la información básica de su organización.
- Desplácese hacia la parte inferior de la pantalla hasta la sección "Administrar" y seleccione "Agregar red".
- Complete el formulario de "Agregar red" y haga clic en "Enviar red".



4. Agregar detalles en el registro de PeeringDB

Una vez que el personal de PeeringDB haya revisado su registro inicial de PeeringDB, podrá agregar más detalles a su registro del siguiente modo:

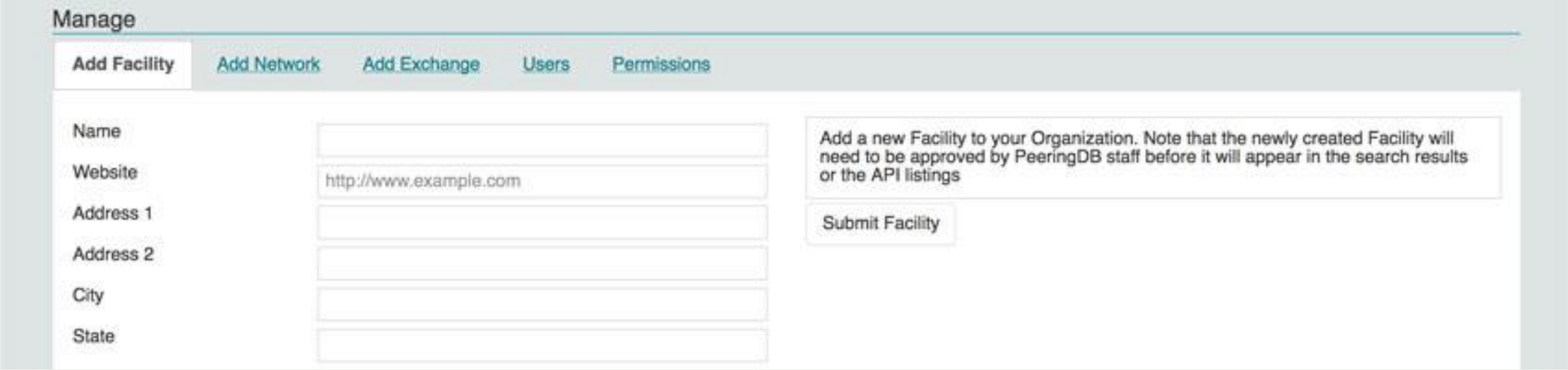
- Inicie sesión en su cuenta de PeeringDB.
- Seleccione el icono de navegación y luego "Su organización".
- Desplácese a la sección "Redes" y seleccione su red.

Aparecerá la vista estándar de PeeringDB para una red.

- Haga clic en el botón "Editar" para actualizar los datos de esta página.
- Desde la vista "Editar", puede gestionar contactos, añadir información secundaria, gestionar instalaciones de intercambio de tráfico privado y gestionar puntos de intercambio.

Agregar detalles en el registro de PeeringDB

En la vista “Edit”, puede administrar Contactos, agregar Información secundaria, gestionar instalaciones de intercambio de tráfico privado y gestionar puntos de intercambio



Manage Contacts

Add Secondary Information

Manage Private Peering Facilities

Manage Exchange Points

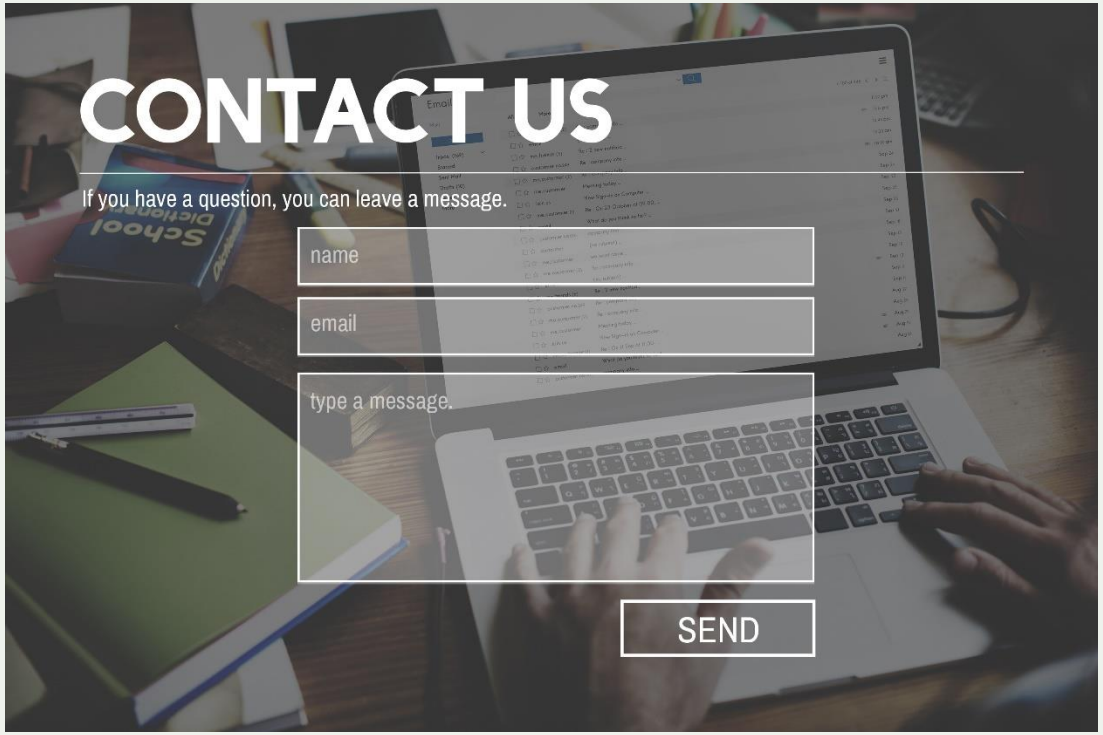
Sitio Web de la Compañía

Proporcionar una fuente adicional de información de contacto y políticas de enrutamiento en el sitio web de una empresa resulta beneficioso para aquellos operadores que aún no están familiarizados con PeeringDB o que consultan un RIR.

Para contribuir a la comunicación abierta, los operadores de redes deberían considerar la posibilidad de publicar algunos elementos en su sitio web

Deben incluir los siguientes detalles de contacto en el sitio web de su empresa:

- Centro de operaciones de red
- Equipo de soporte
- Equipo para casos de abuso.
- Equipo de seguridad.

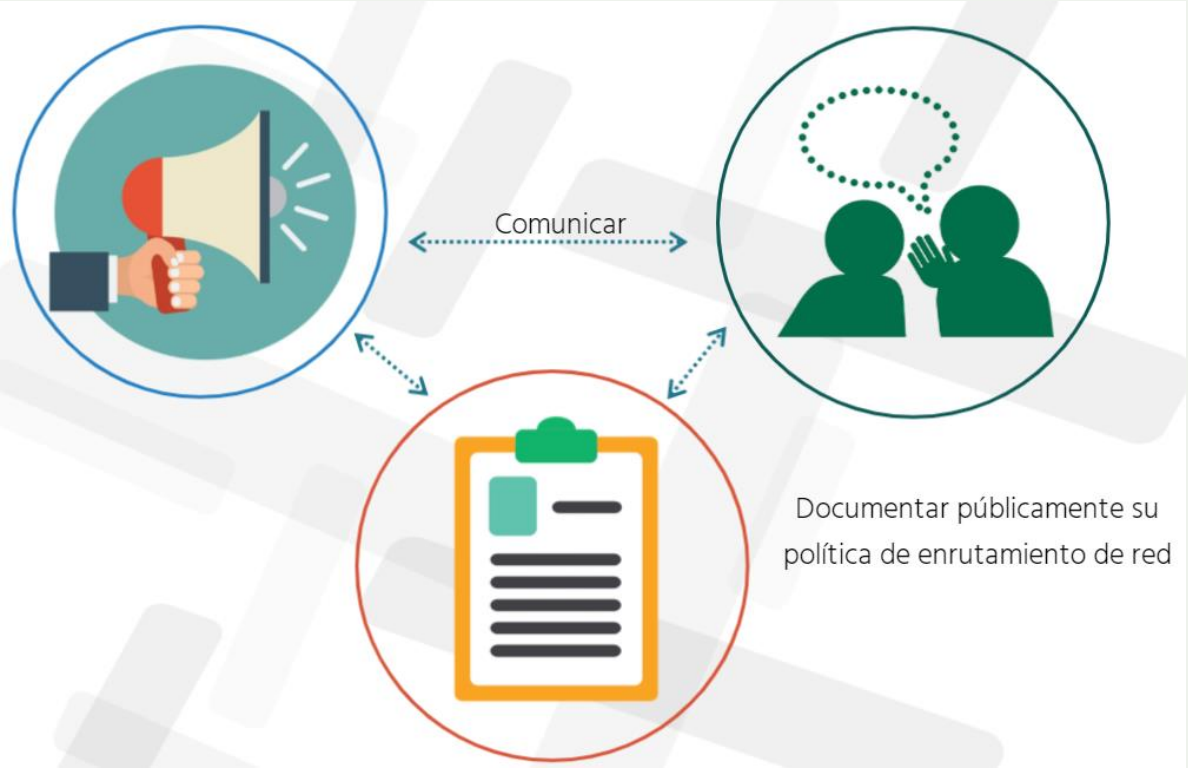


Acción 4: Validación Global

Acciones de MANRS

Los participantes de MANRS deberán realizar las siguientes acciones para facilitar ***la validación de la información de enrutamiento.***

- Comunicar sus anuncios correctos a las redes adyacentes a la suya.
- Documentar públicamente su Política de enrutamiento de redes, los ASNs y los prefijos que se pretende anunciar a terceros.

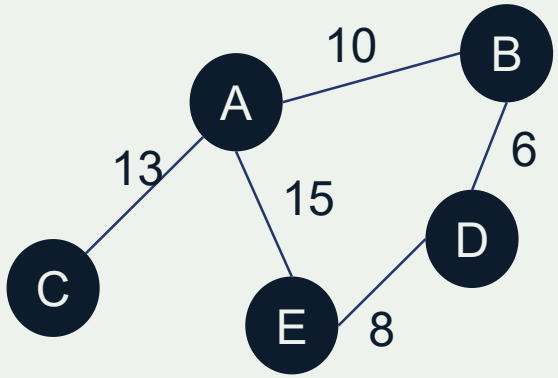


Introducción

Con el fin de validar los anuncios de enrutamiento en una escala global, la Política de Enrutamiento de Redes de su organización debe ponerse a disposición de otras redes.

Dado que cualquier red que participe en el protocolo Border Gateway Protocol (BGP) podría requerir esta información, se debe publicar en un lugar conocido utilizando un formato estándar.

Anuncios



La acción de Validación Global, requiere que los operadores de redes aseguren que su información de enrutamiento de redes este disponible públicamente.

Esto incluye los anuncios que la red origina, así como la política de enrutamiento que describe cómo se maneja el intercambio de información de accesibilidad con otra red

Lo que cubren específicamente las rutas son:

- Anuncios de otras redes.

Supuesto de secuestro de rutas

Para operar una red de manera responsable es preciso validar el tráfico que usted y sus clientes envían al resto de Internet.

También es preciso validar las rutas que le anuncian su tráfico ascendente, pares y clientes.

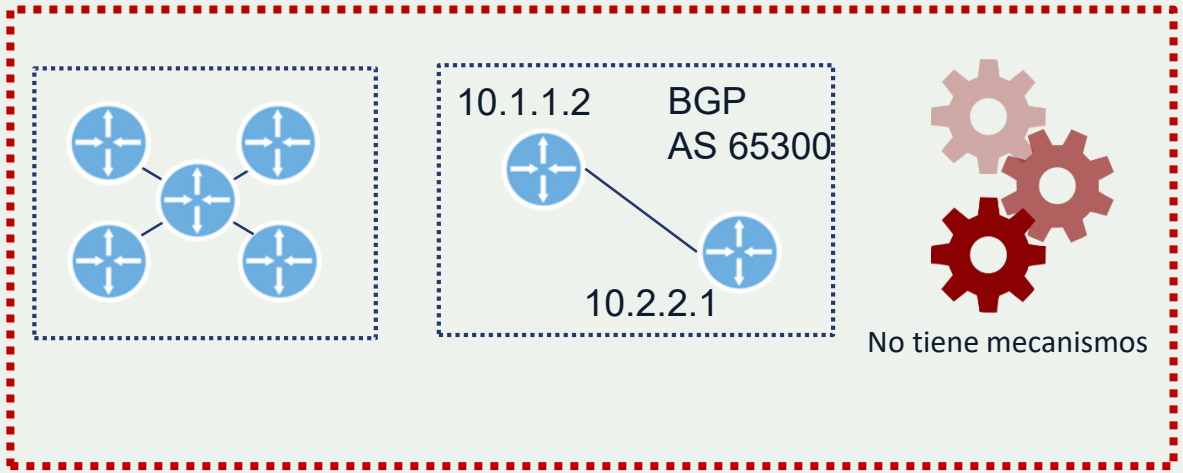
Si no valida alguno de estos elementos, su red se vuelve vulnerable a los secuestros de rutas y se convierte en una fuente potencial de tráfico de ataques DDOS.

Supuesto de secuestro de rutas

Los Sistemas autónomos utilizan el protocolo BGP para comunicar la información de enrutamiento.

No obstante, el protocolo BGP carece de mecanismos integrados para autenticar la asignación de prefijos de IP.

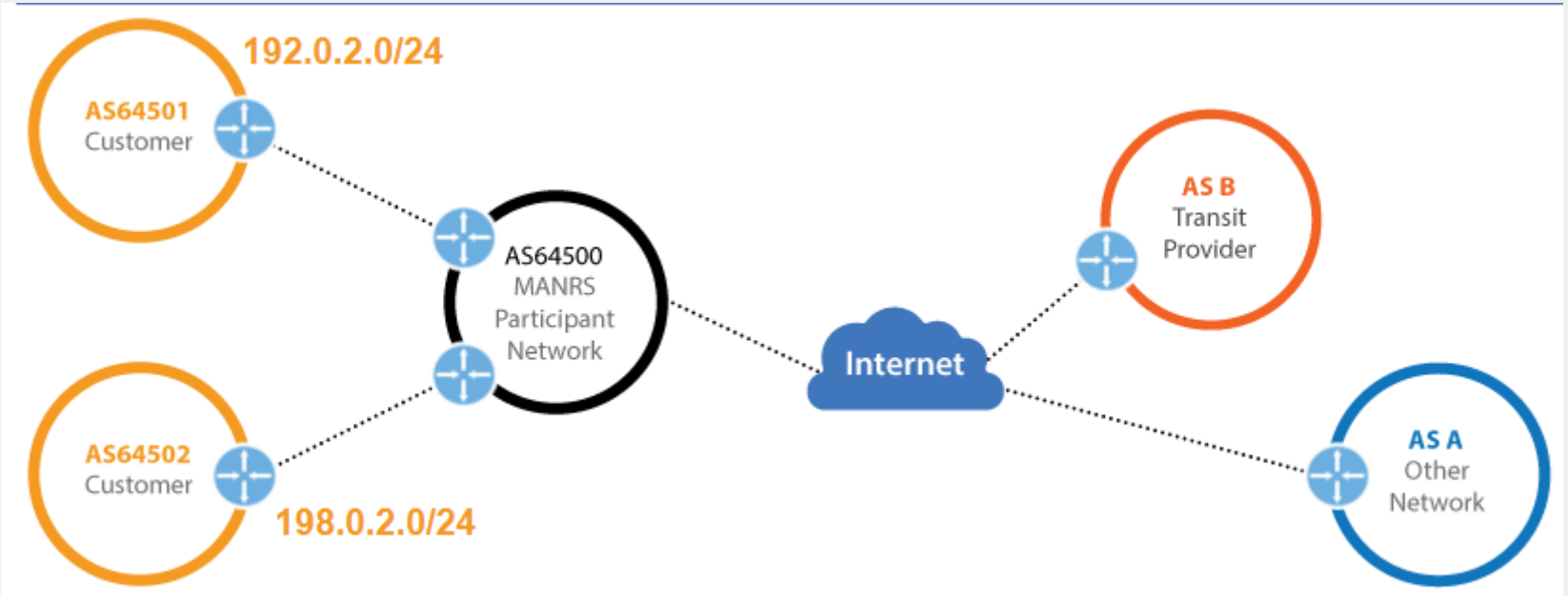
Esto puede conllevar a una vulnerabilidad que puede ser aprovechada por un atacante.



¿Por qué es importante validación de la información de enrutamiento?

¿Cómo podemos solucionar el problema de las vulnerabilidades?

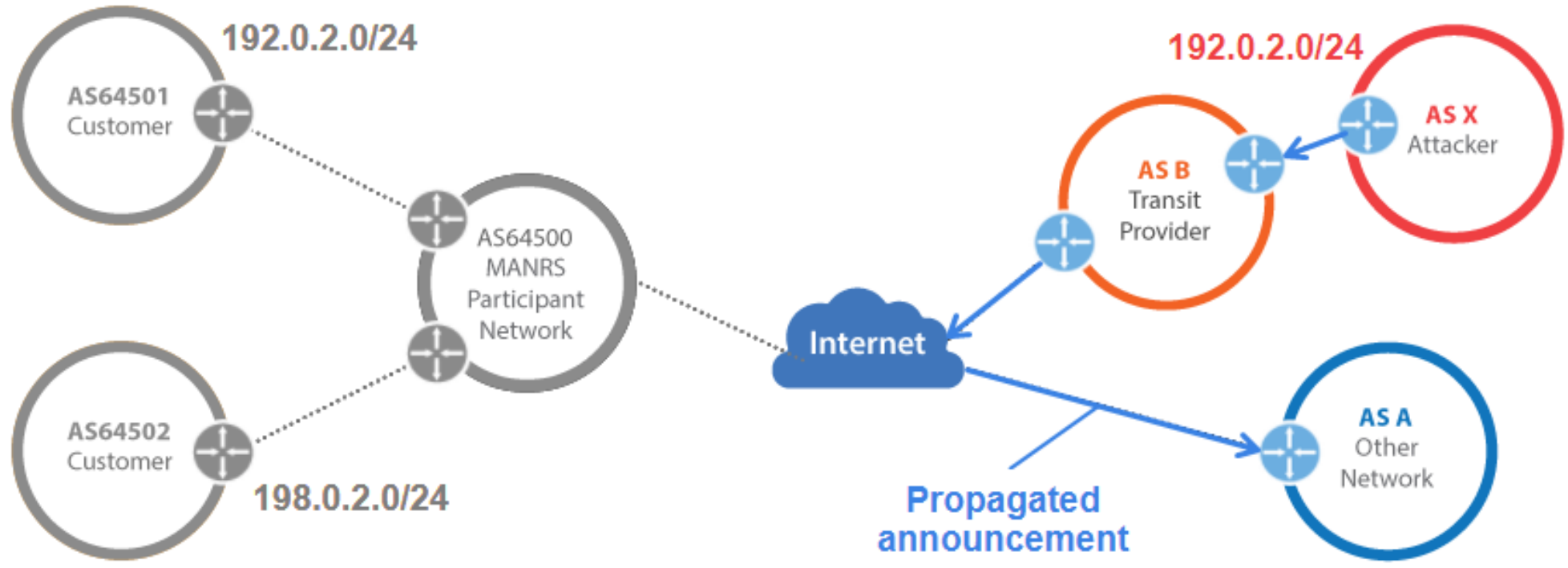
¿Por qué es importante la validación de la información de enrutamiento?



Los AS utilizan el protocolo BGP para comunicar la información de enrutamiento. BGP carece de mecanismos integrados para autenticar la asignación de prefijos de IP. Como tal, un actor malicioso puede aprovechar esta vulnerabilidad para llevar a cabo un ataque utilizando el secuestro de prefijos (**Prefix Hijacking**)

Para resolver el problema, los operadores de red pueden seguir los siguientes pasos para validar la información del enrutamiento.

Validación de la información de enrutamiento

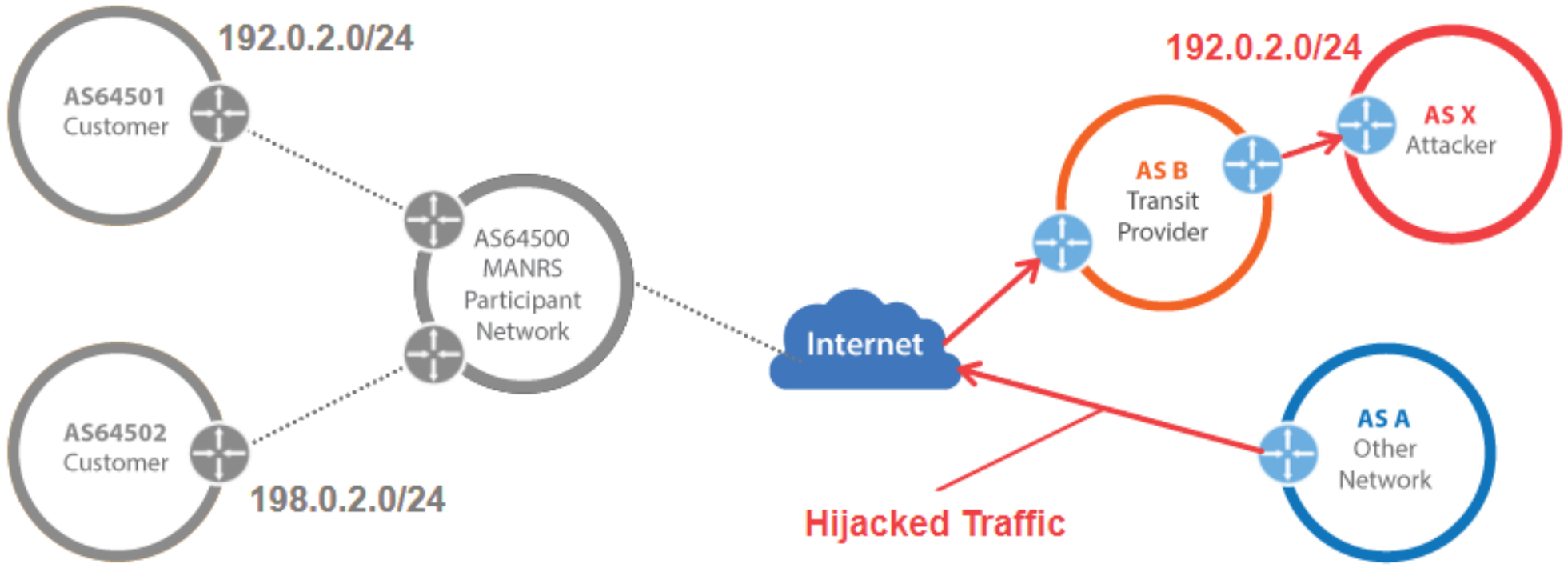


PASO 1:

Un atacante anuncia el prefijo de otra red (por ejemplo, AS X anuncia el prefijo perteneciente a AS64501), lo cual es aceptado por sus AS vecinos.

- AS A y AS B propagan a otras redes de Internet.
- AS A y AS B aceptan esta información de enrutamiento incorrecta debido a la falta de validación.

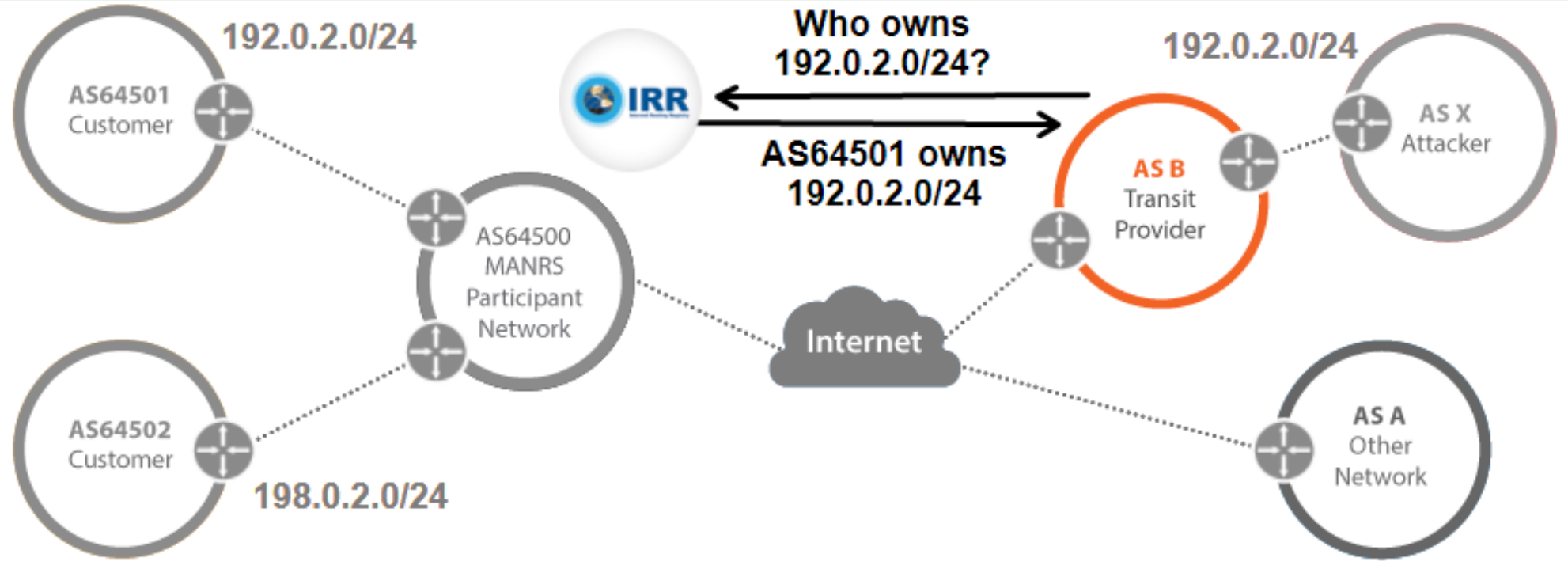
Validación de la información de enrutamiento



PASO 2:

El anuncio del atacante hace que el tráfico destinado a AS64501 se dirija al AS del atacante (AS X)

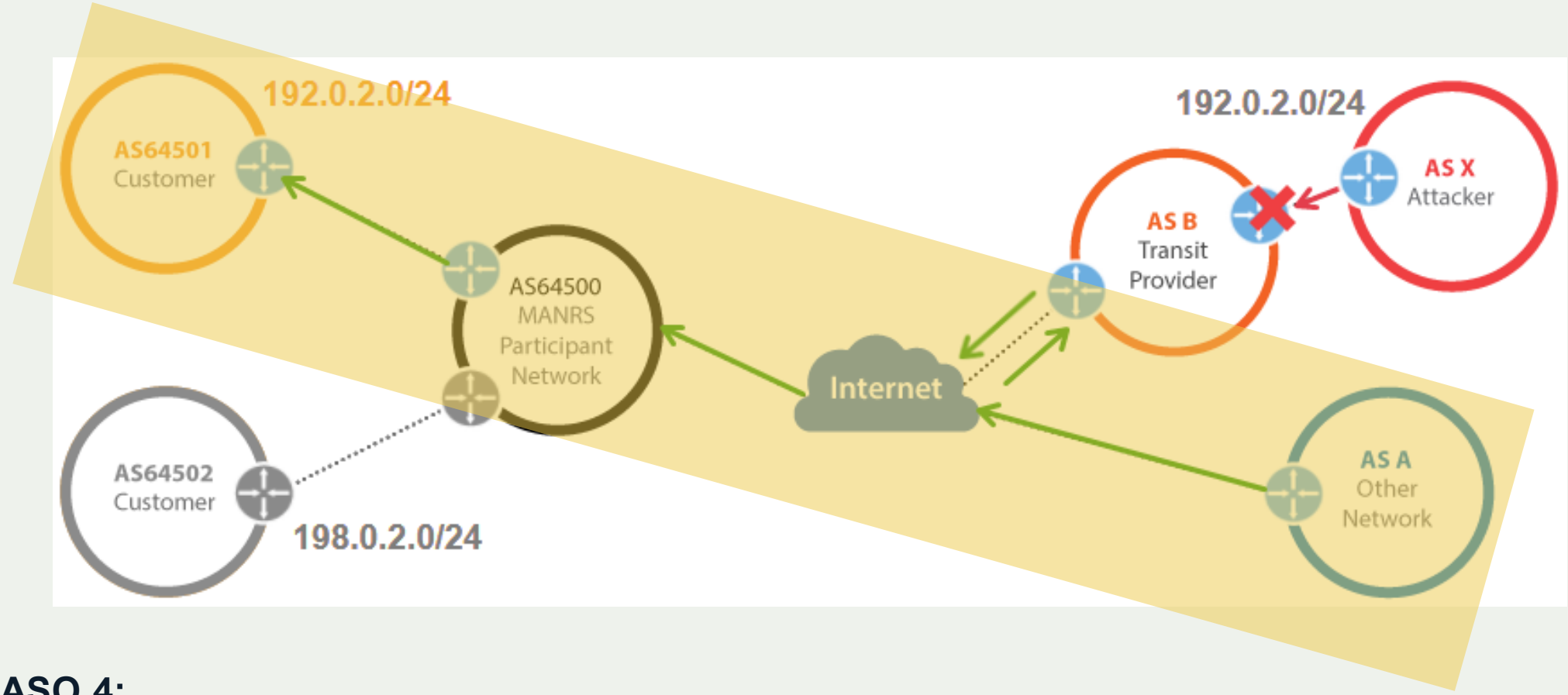
Validación de la información de enrutamiento



PASO 3:

- Si AS64501 publica una Política de enrutamiento de redes, puede mitigar la amenaza del secuestro de prefijos.
- AS B (y otras redes) pueden buscar la información de enrutamiento de AS64501 para determinar quién es el verdadero propietario del prefijo anunciado

Validación de la información de enrutamiento



PASO 4:

El tráfico se dirige al AS correcto (AS64501) independientemente de si el atacante ha anunciado el prefijo de AS64501.

Esto se conoce como **Validación de origen.**

Documentación de los Anuncios de Ruta Esperados

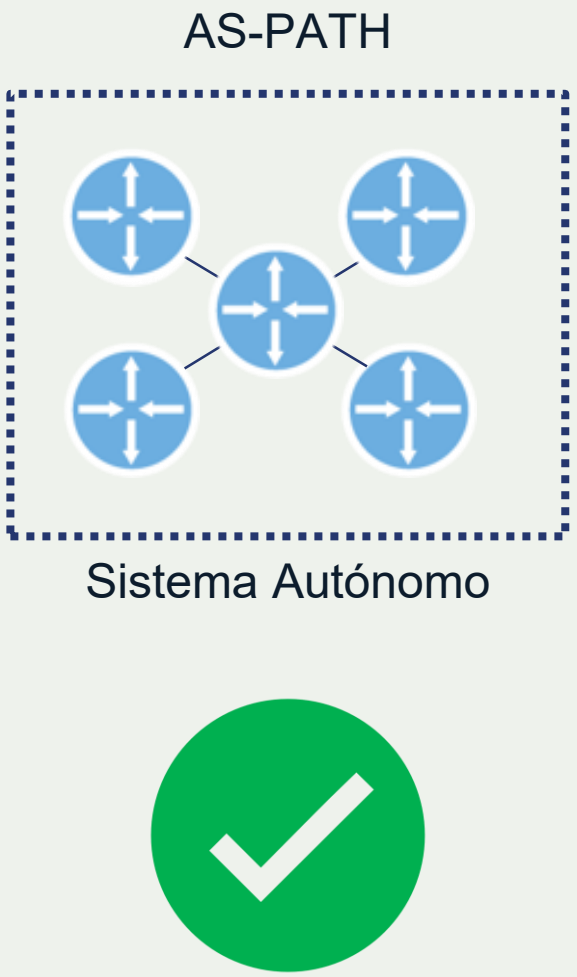
Documentación de los Anuncios de ruta Esperados

Los participantes de MANRS deben mantener información de contacto actualizada para facilitar la validación de la información de enrutamiento.

- Es importante entender el objetivo de la validación de origen para documentar los anuncios.

La validación de origen tiene como objetivo verificar que la Red del sistema autónomo que está más a la derecha (también llamada originador) de un AS_PATH sea correcta.

- Esto se puede verificar mediante la correlación del espacio de direcciones (o prefijos) y los ASN.



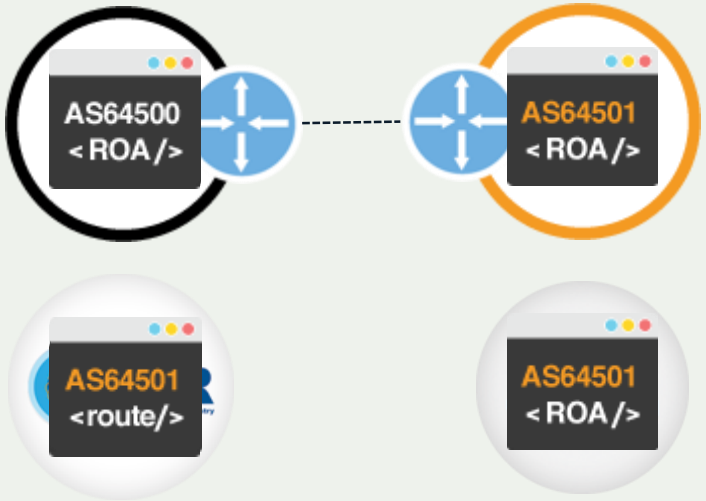
Documentación de los Anuncios de ruta Esperados

1. Registrar su Política de enrutamiento de redes (objeto **aut-num**) y sus anuncios previstos (objeto **route**).

2. Documentar su cono de clientes (objeto **as-set**).

3. Asegurar que sus clientes registren sus anuncios previstos (objeto **route**).

4. Registrar sus anuncios previstos (objeto **ROA**) en un repositorio RPKI y procurar que sus clientes hagan lo mismo.



Comunicar la autorización de origen.

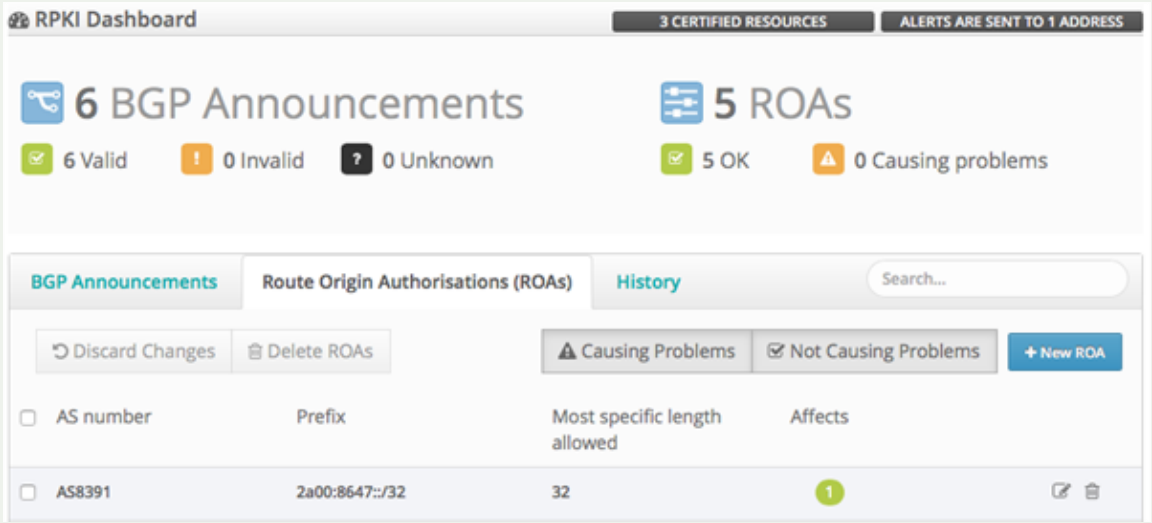
Se observa cómo se requiere que los participantes de MANRS publiquen su política de enrutamiento de red y otra información de enrutamiento asociada en una base de datos de IRR y un repositorio de RPKI.

Los dos métodos utilizados para comunicar la autorización de origen son:

- Los objetos route/route6 registrados en las bases de datos de los IRRs.
- Los ROAs publicadas en el sistema RPKI.

RPKI

Proporcionando información al repositorio RPKI



Además de proporcionar información al sistema de IRR, también debe documentar los anuncios previstos de su red, que se almacenarán dentro de un objeto ROA en un repositorio RPKI.

Los ROA son objetos firmados criptográficamente e indican que prefijos (no la ruta completa) son autorizados a originar por un AS.

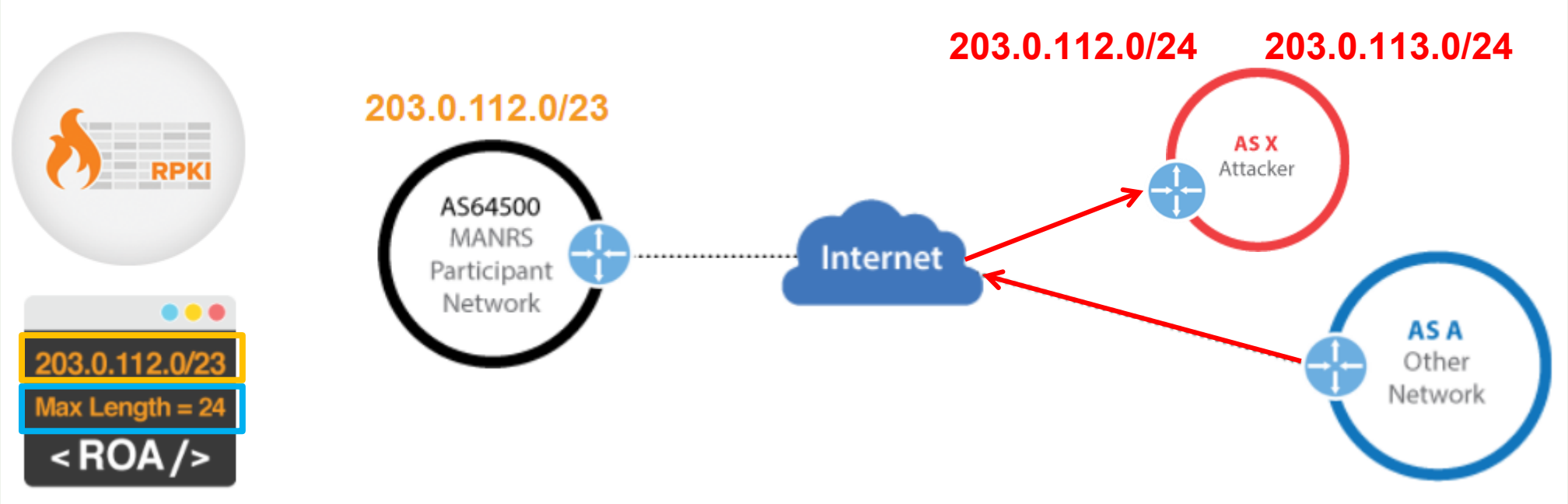
Un tablero de RPKI ofrece una interfaz para realizar varias operaciones con las ROA:

- Creación y publicación
- Modificación
- Eliminación

Proporcionando información al repositorio RPKI

MANRS

Campo de Longitud Máxima



El AS64500 es propietario de un ROA con prefijo 203.0.112.0**/23** y a longitud máxima se ha establecido en **/24.**

Si AS64500 no anuncia 203.0.112.0**/24** y 203.0.113.0**/24**, un atacante puede anunciar uno de estos prefijos más específicos desde su AS, con el ASN autorizado antepuesto, sin que el ROA de AS64500 invalide el anuncio.

MANRS

Recomendaciones

Nuevos prefijos

- Debe establecer un proceso para procurar que cada vez que origine un prefijo nuevo desde su red, se cree o modifique una ROA correspondiente para reflejar este cambio. Esto debe convertirse en parte de sus procesos cotidianos de Centro de operaciones de red(NOC).

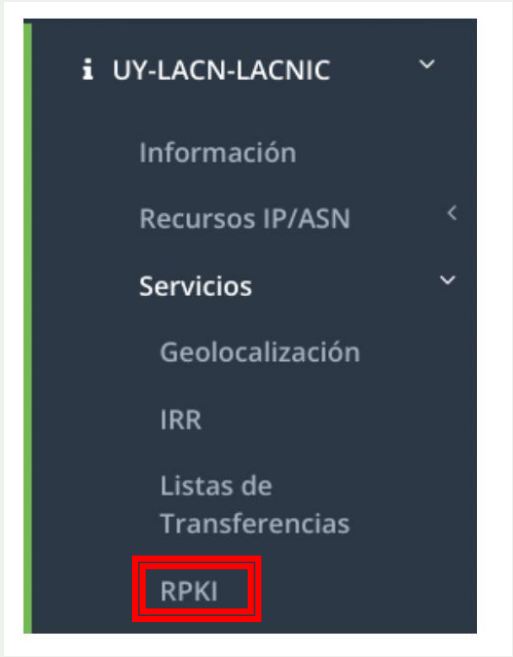
Espacio de direcciones del cliente.

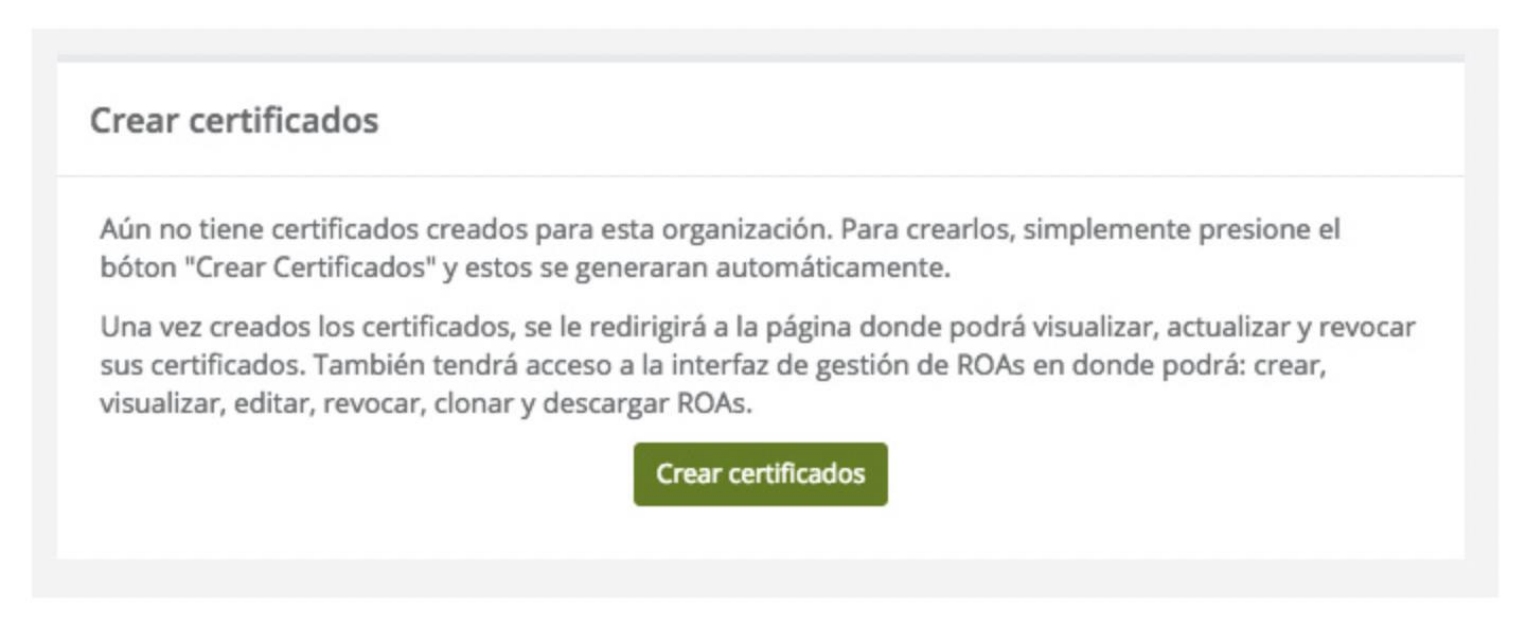
- Para usar RPKI a fin de automatizar la validación de los anuncios de clientes se precisa que el cliente administre plenamente su espacio de direcciones. Respecto de clientes más pequeños o clientes que recibieron su espacio de direcciones como una asignación de su proveedor, el proveedor puede optar por encargarse de la administración de RPKI en nombre del cliente.

Servicio de Certificación de recursos alojados en RIR.

- Todos los Registros regionales de Internet (RIR) ofrecen un servicio de certificación de recursos, mediante el cual el RIR mantiene y gestiona las claves y todas las operaciones se efectúan en los servidores de RIR.

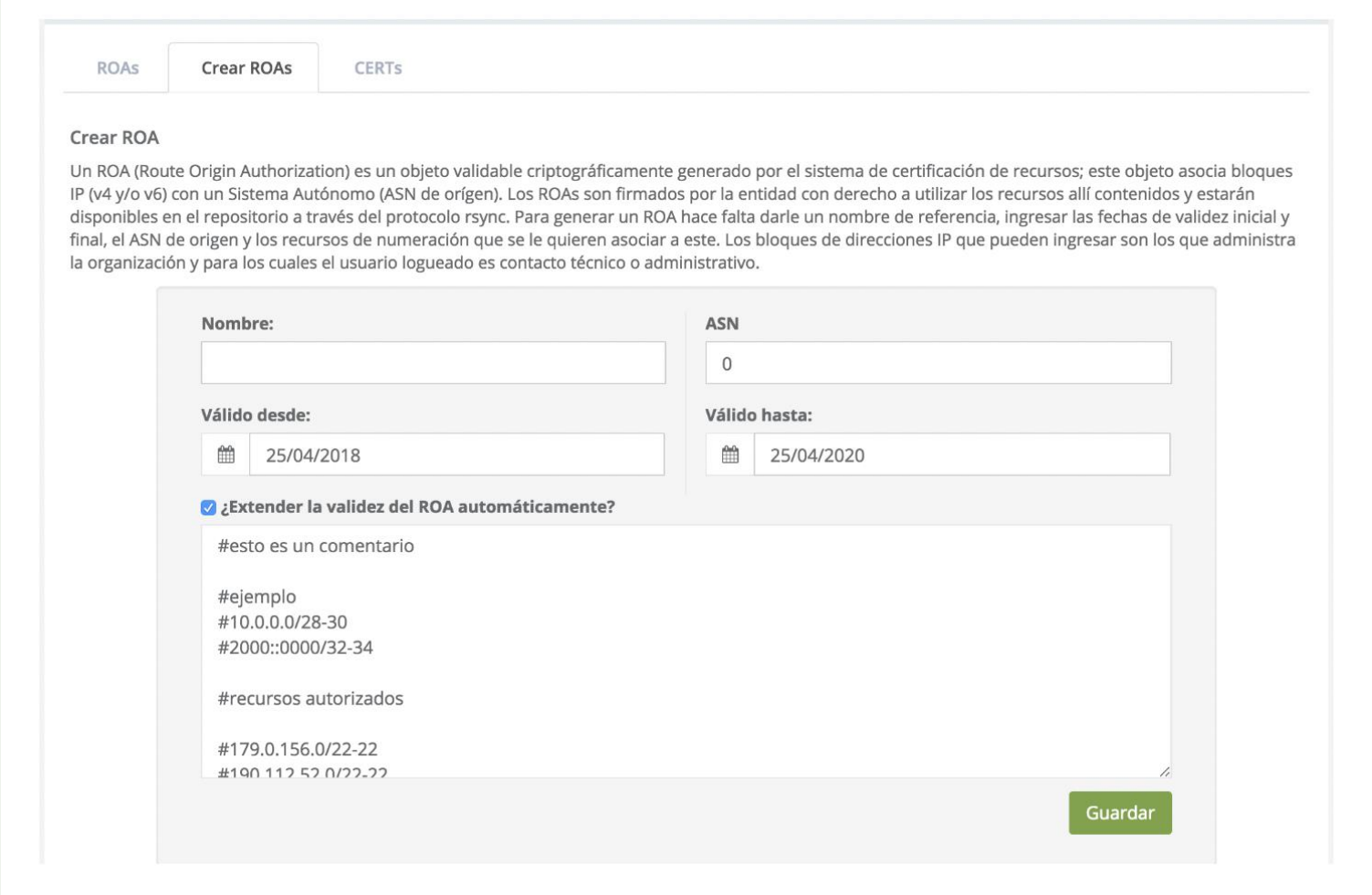
Creación de Certificado - MiLACNIC





https://lacnic.zendesk.com/hc/es/articles/232074808-RPKI-crear-certificados-y-ROAs

Creación de ROA - MiLACNIC



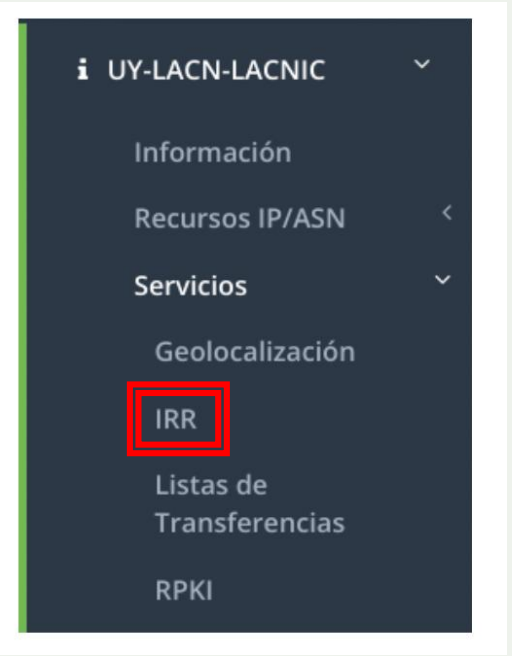
https://lacnic.zendesk.com/hc/es/articles/232074808-RPKI-crear-certificados-y-ROAs

IRR / MiLACNIC

[Servicios] / [IRR]

[Generar objetos y habilitar creación de as-set]

[Confirmar]



Objetos creados autómaticamente:

mntner: Entidad responsable de objetos IRR
person: Diferentes contactos en los objetos
aut-num: Sistemas autónomos
route y route6: ASN que origina un anuncio BGP y sus redes IPv4/IPv6

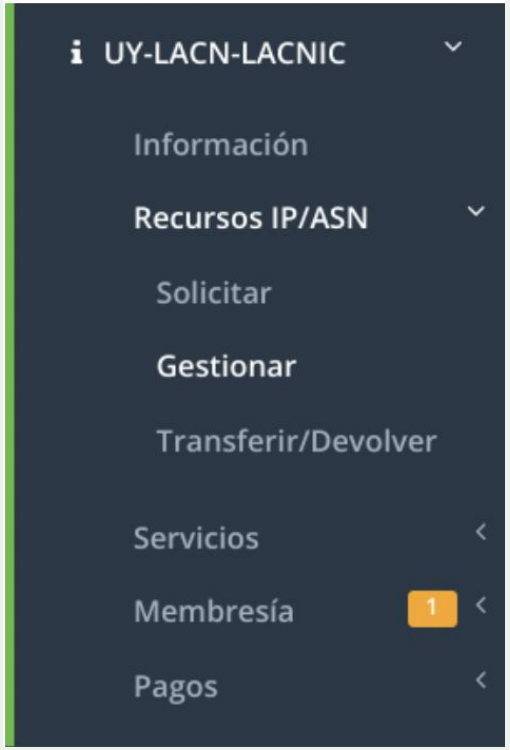
Objeto de creación manual:

as-set: Conjunto ASN

https://lacnic.zendesk.com/hc/es/articles/360038666774-Comenzar-a-usar-el-IRR-de-LACNIC

AS-SET / MiLACNIC

[Recursos IP/ASN] / [Gestionar]



Seleccionar el ASN

[ASSET] / [Agregar]

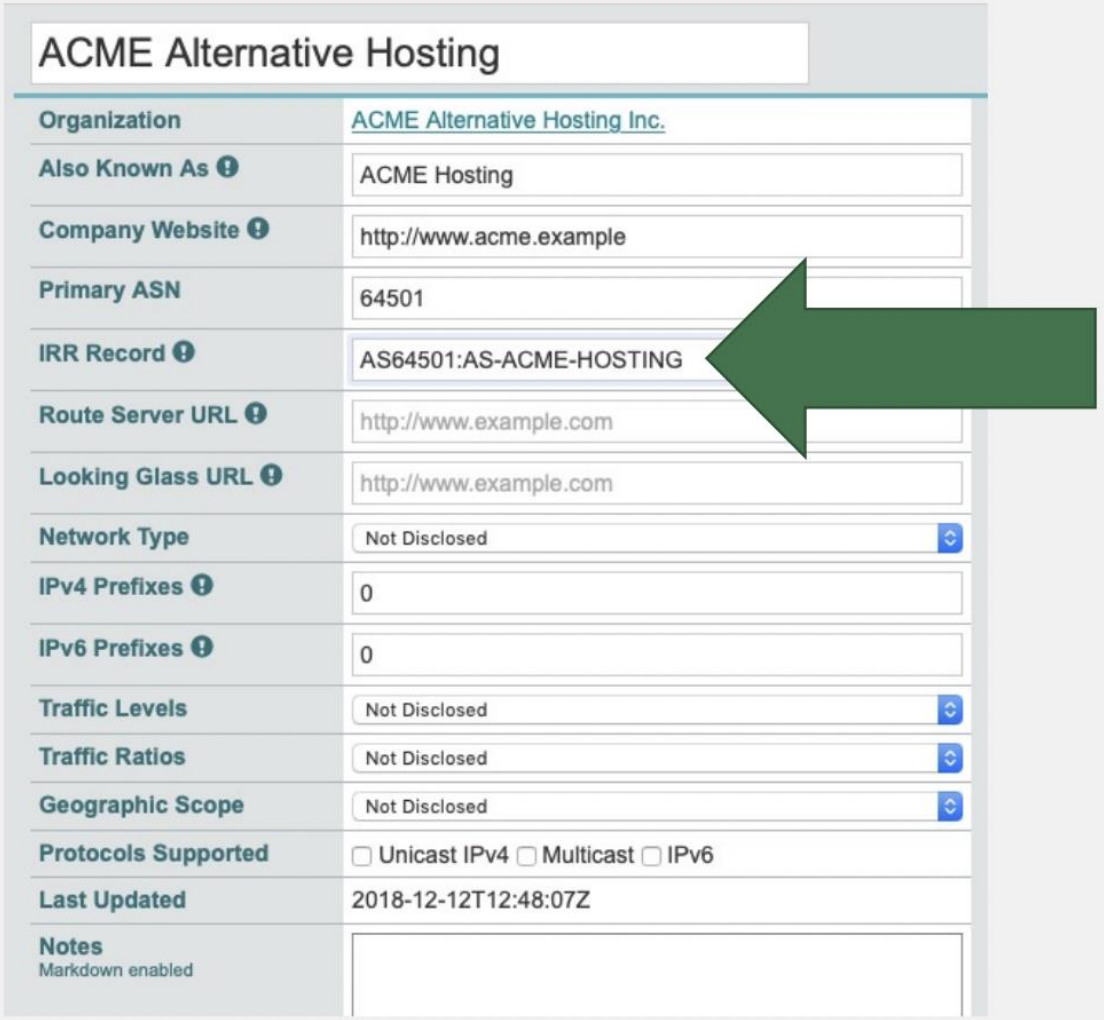
Completar Datos

- Nombre (Identificador
- ASN Members
- AS-SET Members
- Remarks

***Nota:** EL nombre del as-set va ha ser un texto único compuesto por el nombre del AS + una descripción con el prefijo AS. Ej: AS28000:AS-DESCRIPCION.*

https://lacnic.zendesk.com/hc/es/articles/360039152373-Crear-as-set

AS-SET en PeeringDB



Network Information

- Registro IRR
  - **AS-Macro (AS-SET)**
  - Registrado en Base de datos IRR (por ejm. LACNIC)
  - Crear el AS-Set si aún no se tiene

Resumen de pasos - MiLACNIC

Resumen de pasos - MiLACNIC

1. RPKI: Crear el Certificado y los ROA
2. Habilitar la creación automática de registros IRR
3. Crear los AS-SET
4. Registrar el AS-SET en PeeringDB

Dudas o Preguntas

Acción 1: Filtrado

Prevención de la propagación de información de enrutamiento incorrecta

Objetivos

- ¿Por qué es importante filtrar los anuncios de sus clientes.?
- ¿Cómo se pueden construir los filtros, incluidas las herramientas que se utilizan para crearlos.?
- Cómo verificar la precisión de los anuncios de sus clientes y la legitimidad de la propiedad del espacio de direcciones anunciados.
- Cómo señalar a otras redes qué anuncios de la red son correctos.

Acciones

Los participantes de MANRS deben realizar las siguientes acciones para evitar la propagación de información de enrutamiento incorrecta .

- Definir una Política de enrutamiento de redes clara.
- Implementar un sistema que garantice la exactitud de sus propios anuncios y de los anuncios de sus clientes en redes adyacentes con granularidad a nivel de prefijo y AS-path.
- Ejercer la diligencia debida al verificar la exactitud de los anuncios de sus clientes, en particular, que el cliente sea el titular legitimo del ASN y el espacio de direcciones que anuncia.

Introducción

Para evitar la propagación de información de enrutamiento incorrecta, los participantes de MANRS deben implementar el filtrado de prefijos.

Al implementar el filtrado de prefijos, puede permitir o denegar anuncios de ciertos prefijos de AS vecinos.

Lo más importante es que los operadores de red deben proteger los anuncios de enrutamiento entrante, en particular de las redes de los clientes, mediante el uso de filtros de nivel de prefijo.

En segundo lugar, los filtros de ruta de AS (AS-Path) se pueden utilizar para requerir que la red del cliente sea explícita sobre qué sistemas autónomos (AS) se encuentran más abajo de ese cliente.

Introducción al filtrado

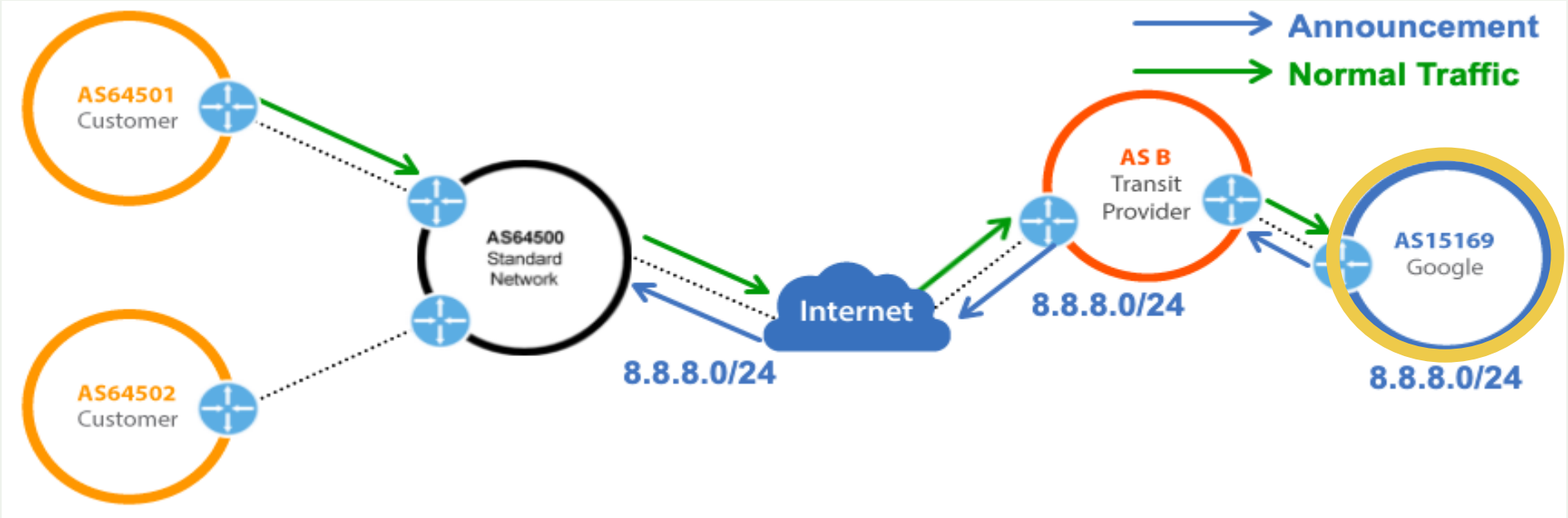
Problemas de BGP

El Secuestro de Rutas o Prefijos o BGP Hijacking, ocurre cuando de manera malintencionada, se anuncian prefijos de otras redes hacia los equipos vecinos, esto con el fin de disfrazar o engañar a los sistemas para redirigir el tráfico hacia el.

Esto impacta de manera critica a los Sistemas Autónomos (AS) ya que, si esta información es aceptada, puede comprometer el RouteMap del protocolo, pues este puede ir propagándose a través de la red.

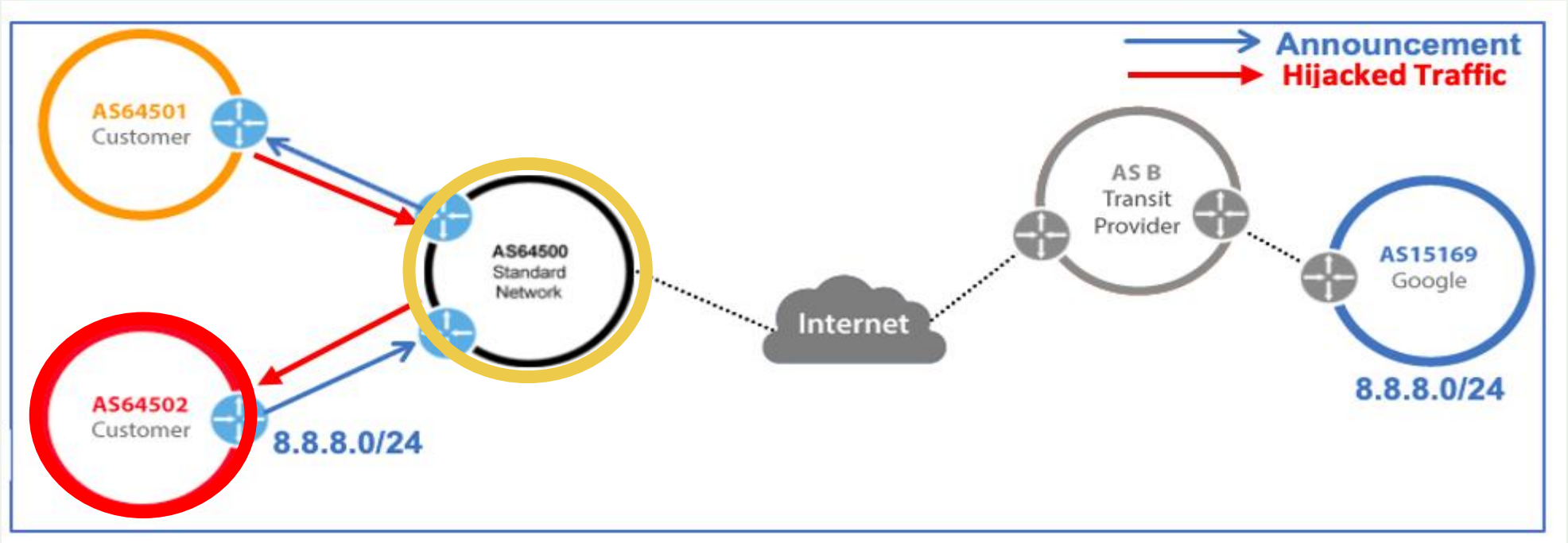
Antes de crear filtros, es esencial realizar una verificación de diligencia sobre la identidad del cliente y de la información que proporciona.

Secuestro de prefijos



En el diagrama siguiente, puede ver lo que ocurre cuando AS15169 anuncia su prefijo (8.8.8.0/24) y el tráfico de AS64501 se dirige hacia AS15169. Sin la implementación de filtros de prefijos, un atacante puede aprovechar el protocolo BGP y anunciar el mismo prefijo.

Secuestro de prefijos



En el siguiente diagrama, puede ver que AS64502 anuncia el prefijo 8.8.8.0/24, que pertenece a AS15169. Este anuncio se propaga a los sistemas autónomos **AS64500** y AS64501 vecinos. El anuncio que efectúa AS64502 hace que el tráfico destinado a AS15169 sea secuestrado y dirigido a AS64502. Esto es un ejemplo de secuestro de prefijos.

Ejemplo Hijacking

Possible Hijack	*Expected Origin AS:* COGENT-174, US (AS 174) *Detected Origin AS:* Unknown (AS 60667)

https://bgpstream.crosswork.cisco.com/event/292772

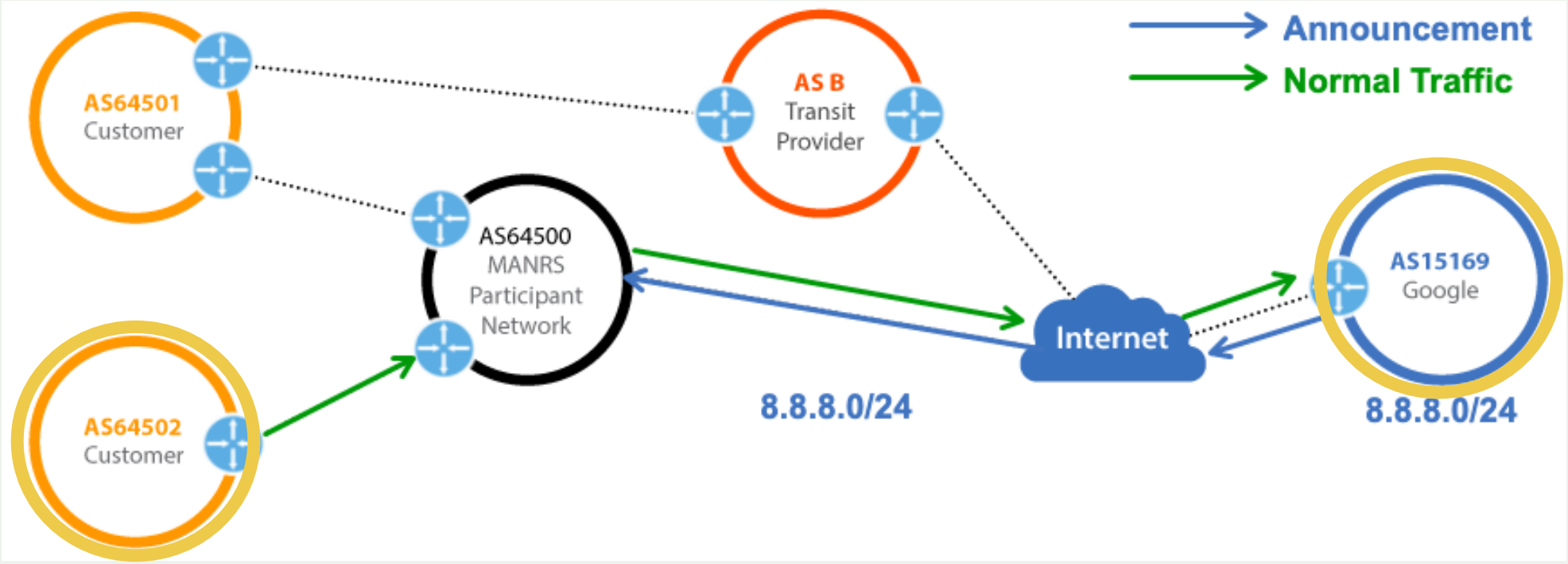
Fuga de Rutas (Route Leak)

Se presentan cuando un operador de red anuncia, ya sea de manera accidental, o no, hacia sus proveedores que tiene una ruta de destino hacia otro ISP.

- Esto implica un flujo de datos continuo a través del AS.
- O de manera intencional, para el espionaje y análisis de tráfico de paquetes.

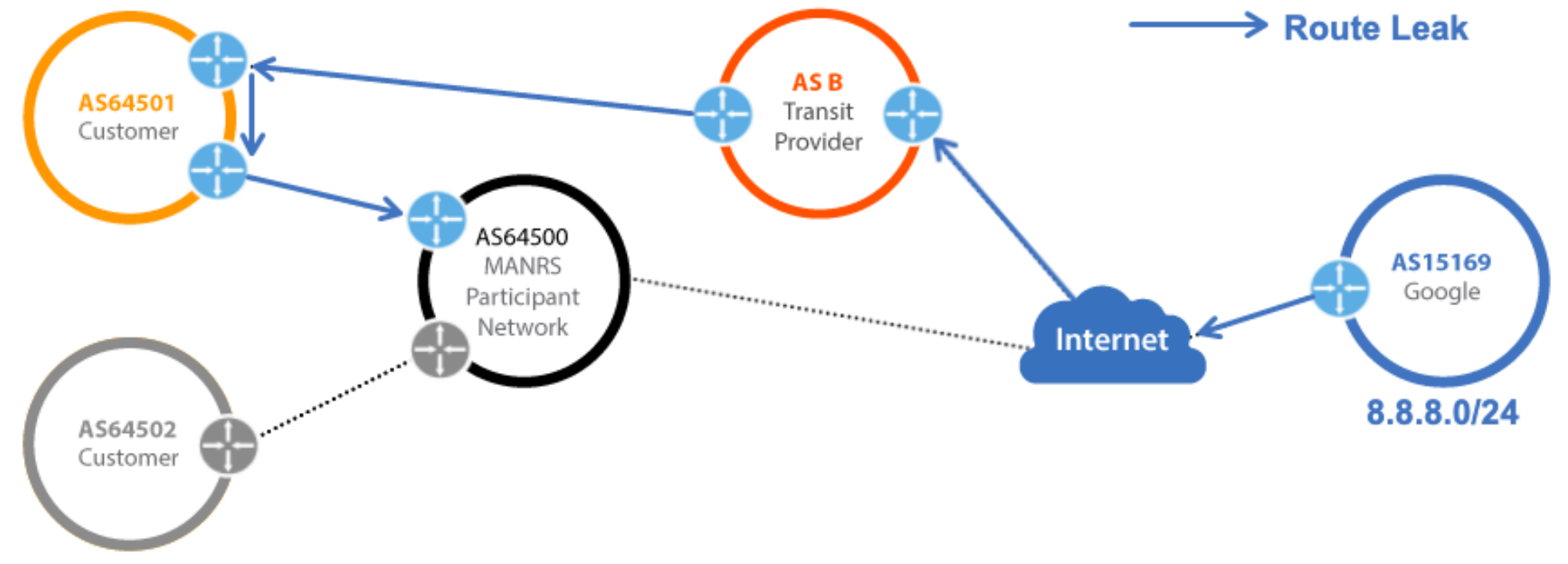
Algunas consecuencias del secuestro de prefijos o de fuga de rutas, puede ser la Denegación de Servicios (DDoS), Spoofing, Sobrecargas, Blackholes, Perdida de datos entre otros.

Fugas de ruta



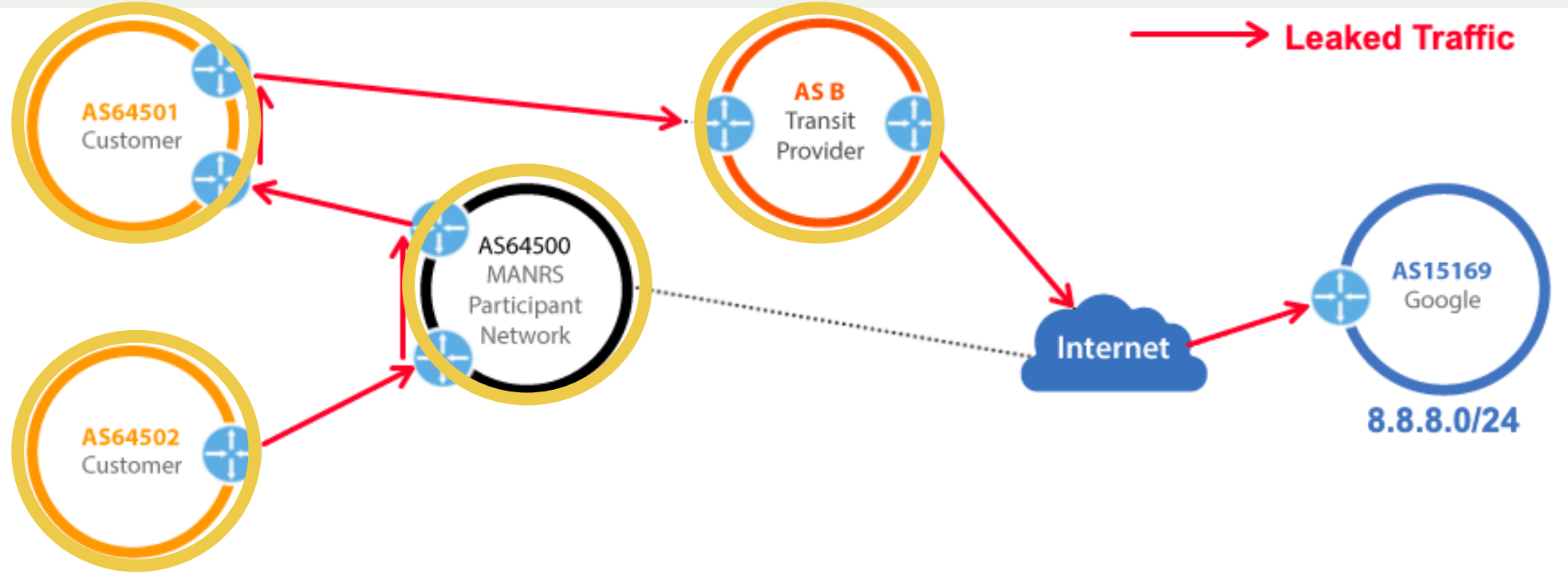
En el diagrama siguiente, se puede ver lo que ocurre cuando AS15169 anuncia su prefijo (8.8.8.0/24) y el tráfico de AS64502 se dirige hacia AS15169. Sin la implementación de filtros de prefijos, puede haber fugas de rutas.

Fugas de ruta



Una fuga de rutas es la propagación de anuncio(s) de enrutamiento fuera de su alcance previsto. Puede ocurrir cuando un cliente anuncia las rutas que obtuvo de un proveedor de tránsito a otro proveedor de tránsito.

Fugas de ruta



La fuga de ruta, como en el actual caso, hace que el tráfico de AS64502 se dirija a AS15169 a través de **AS64500**, AS64501 y AS B.

Ejemplo BGP Leak

BGP Leak	*Origin AS:* INNOVATIVE-TELESYSTEMS-AS, RU (AS 49575) *Leaker AS:* TELE-PLUS-AS, RU (AS 30855)

https://bgpstream.crosswork.cisco.com/event/292767

Creación de filtros de prefijos

A fin de crear filtros de prefijos para sus clientes, necesita saber qué anuncios esperar de ellos.

Puede solicitar directamente a sus clientes que proporcionen información sobre su identidad y recursos. No obstante, este método no es eficiente y es obsoleto.

En lugar de ello, el enfoque recomendado es solicitar a sus clientes que registren la información sobre sus anuncios de enrutamiento en un repositorio público.

Creación de filtros de prefijos

Antes de construir filtros, es importante que aplique la debida diligencia y verifique si la información proporcionada por el cliente sobre su identidad y recursos es correcta.

Recuerde siempre que un filtro es tan bueno como la información que se utilizó para crearlo.

Si su cliente afirma incorrectamente que tiene el espacio de direcciones de otra persona, sin verificaciones adicionales, su filtro permitirá que se produzca este anuncio falso.

Creación de filtros de prefijos

Se recomienda encarecidamente que compruebe la titularidad de los recursos numéricos de Internet asignados, el ASN y el espacio de direcciones anunciado.

Puede hacer esto consultando la base de datos 'whois' del RIR para la región en la que opera su cliente.

Servicios https://stat.ripe.net como pueden ayudarlo a identificar la región y el RIR correspondiente de sus clientes.

MyLACNIC: https://query.milacnic.lacnic.net/home

¿Qué se puede hacer?

- No enviar trafico basura.
  - Filtrar tus propios anuncios.
  - Filtrar a tus clientes.

- No acepte tráfico basura.
  - Filtrar tus propios anuncios.
  - Filtrar tus peers

- Ayuda a otros a mitigar el impacto – Política de Enrutamiento.

Creación de filtros de prefijos

Se recomienda que los participantes de MANRS deben crear filtros de prefijo de las siguientes maneras:

IRR

IRR

Los Registros de Enrutamiento de Internet son lugares centrales donde se publica información de enrutamiento.

Documentan qué ASN tienen permiso para anunciar qué direcciones IP, y cuáles son las políticas vigentes para el intercambio de rutas entre ASN.

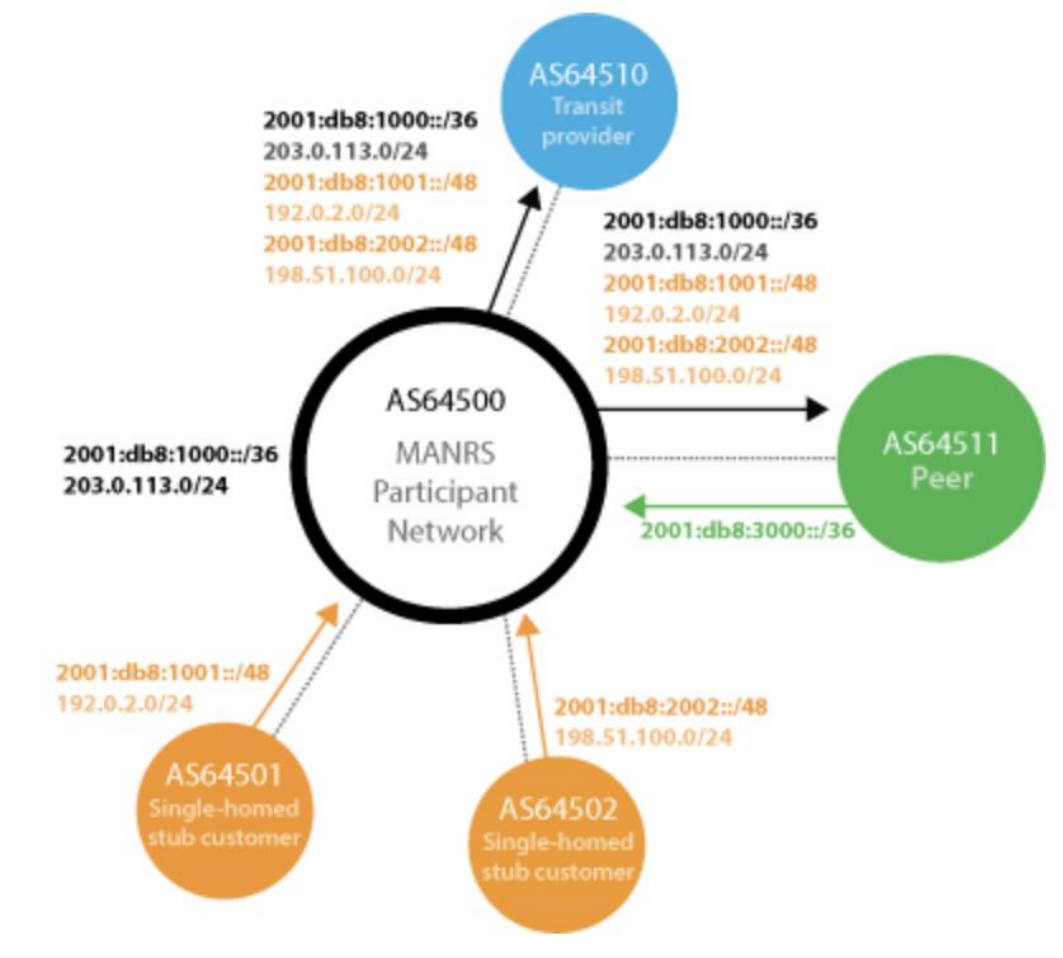
IRR

Esta información se puede utilizar en la configuración de enrutadores para validar las rutas recibidas.

Se puede usar un IRR para producir filtros de prefijos en las siguientes circunstancias:

1. Filtrado saliente de prefijos específicos de su red hacia los pares y tráficos ascendentes (upstreams) (obligatorio).
2. Filtrado entrante de prefijos específicos provenientes de los clientes (obligatorio).
3. Filtrado entrante de prefijos específicos de los pares hacia su red (recomendado).

IRR



En un ejemplo típico, un operador (**AS64500**) requerirá que sus clientes, como AS64501, registren sus anuncios previstos como objetos de ruta (ROA).

Por ejemplo, en la topología de red que muestra la siguiente figura, la red **AS64500** le pedirá a AS64501 que registre sus anuncios.

IRR

La siguiente figura muestra cómo un objeto de ruta AS64501 registra sus anuncios. AS64500 también requerirá que AS6402 registre sus anuncios previstos de la misma manera.

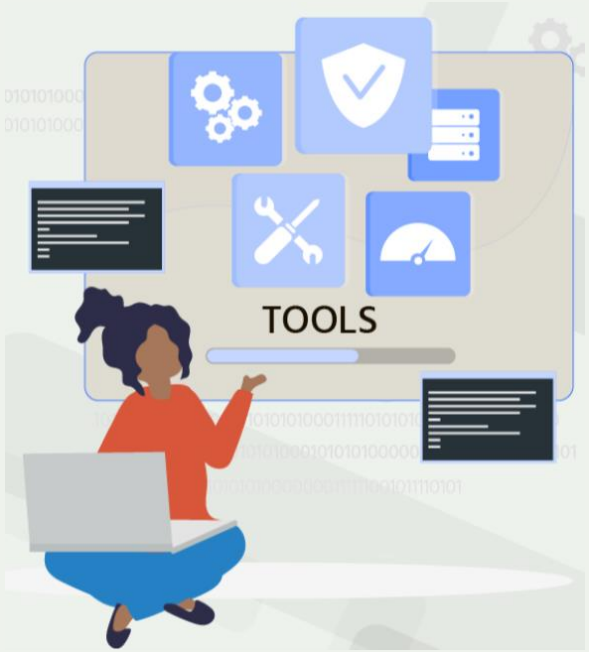
Objeto de ruta AS64502

```
route:198.51.100.0/24
descr:Cust 64502
origin: AS64502
mnt-by: MAINT-AS64502
created:2015-09-27T12:14:23Z
last-modified: 2015-09-27T12:14:23Z
source: RIPE

route6: 2001:db8:2002::/48
descr:Cust 64502
origin: AS64502
mnt-by: MAINT-AS64502
created:2015-09-27T12:14:23Z
last-modified: 2015-09-27T12:14:23Z
source: RIPE
```

Herramientas para crear filtros de prefijos

Hay herramientas disponibles que están diseñadas para funcionar con políticas de IRR. Dichas herramientas pueden crear filtros de ingreso y egreso automáticamente. Esto se hace analizando el objeto *aut-num* que documenta la política de enrutamiento de AS para recopilar todos los objetos a los que se hace referencia y extraer los prefijos.

- IRR Toolset
- BGPQ3
- IRRPT



Verificación de filtros

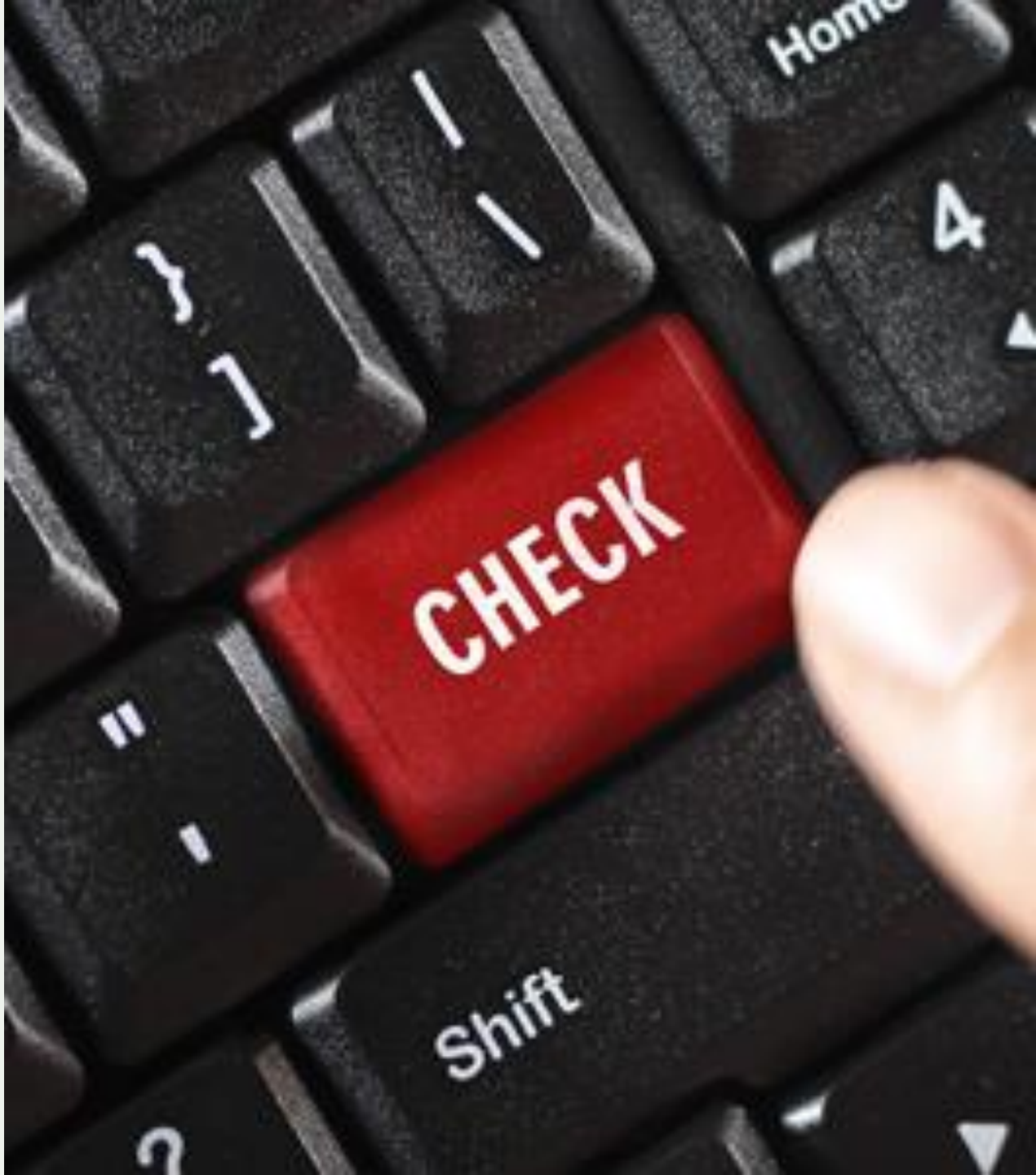
Verificación de sus filtros

Al implementar filtros de prefijos en una infraestructura productiva, los operadores de redes deben ejercer extrema cautela.

Un simple error puede hacer que el trafico no se filtre correctamente.

Antes de implementar sus filtros de prefijos, debe realizar algunas verificaciones. Se recomienda usar los siguientes mecanismos para evitar los filtros defectuosos.

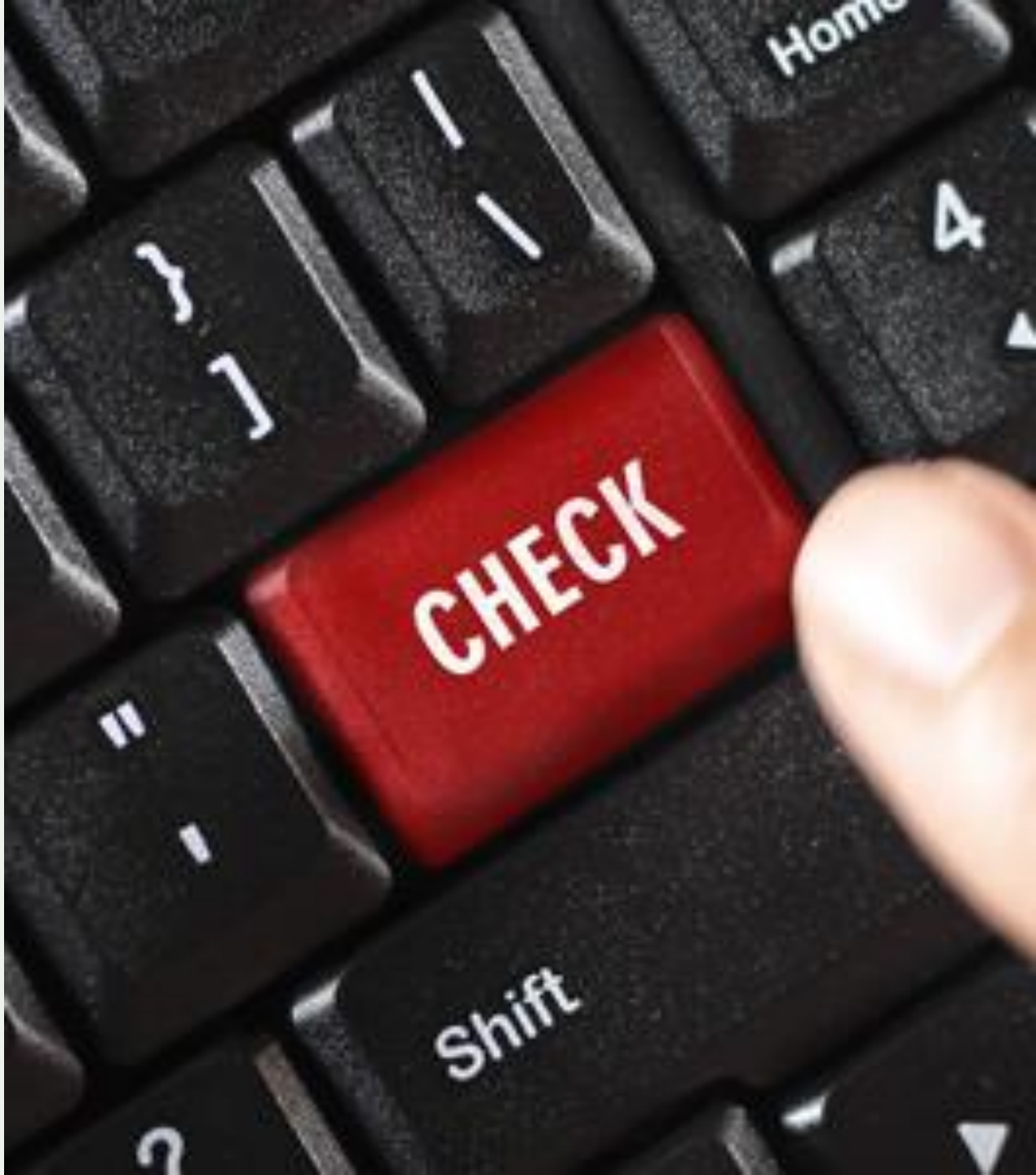
- Verificaciones de sintaxis
- Verificaciones de delta.
- Prefijos baliza.



Verificaciones de sintaxis

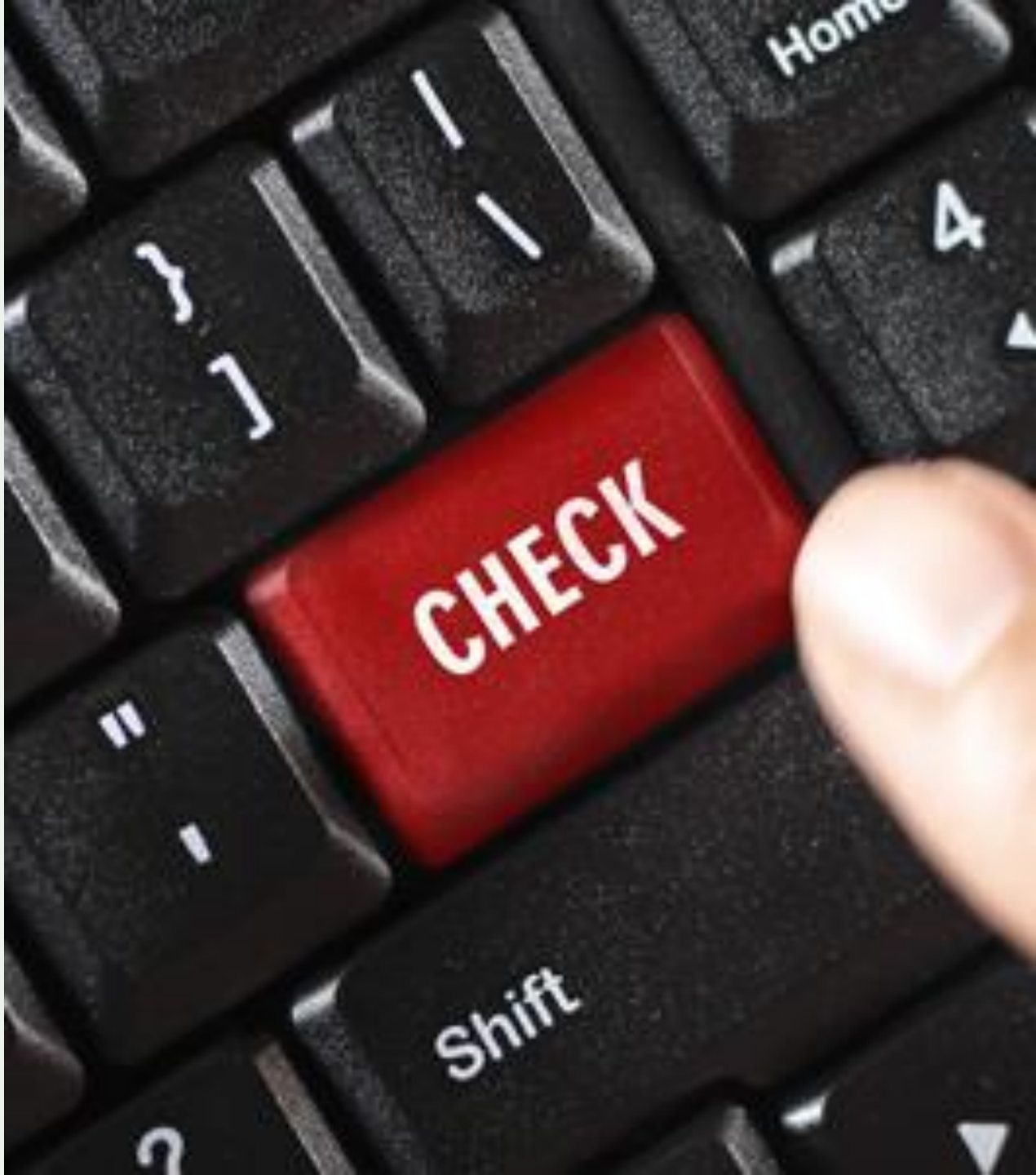
Debe realizar algunas simples verificaciones de sintaxis para procurar que sus filtros de prefijos:

- No estén vacíos, estén bien formados y no contengan errores de sintaxis. Algunas plataformas de enrutamiento tratan las listas de prefijos vacías como un "permitir cualquiera" implícito.
- No hagan referencia a direcciones y mascaras imposibles.
- No bloqueen inadvertidamente cualquier cosa que esté explícitamente configurada para pasar.



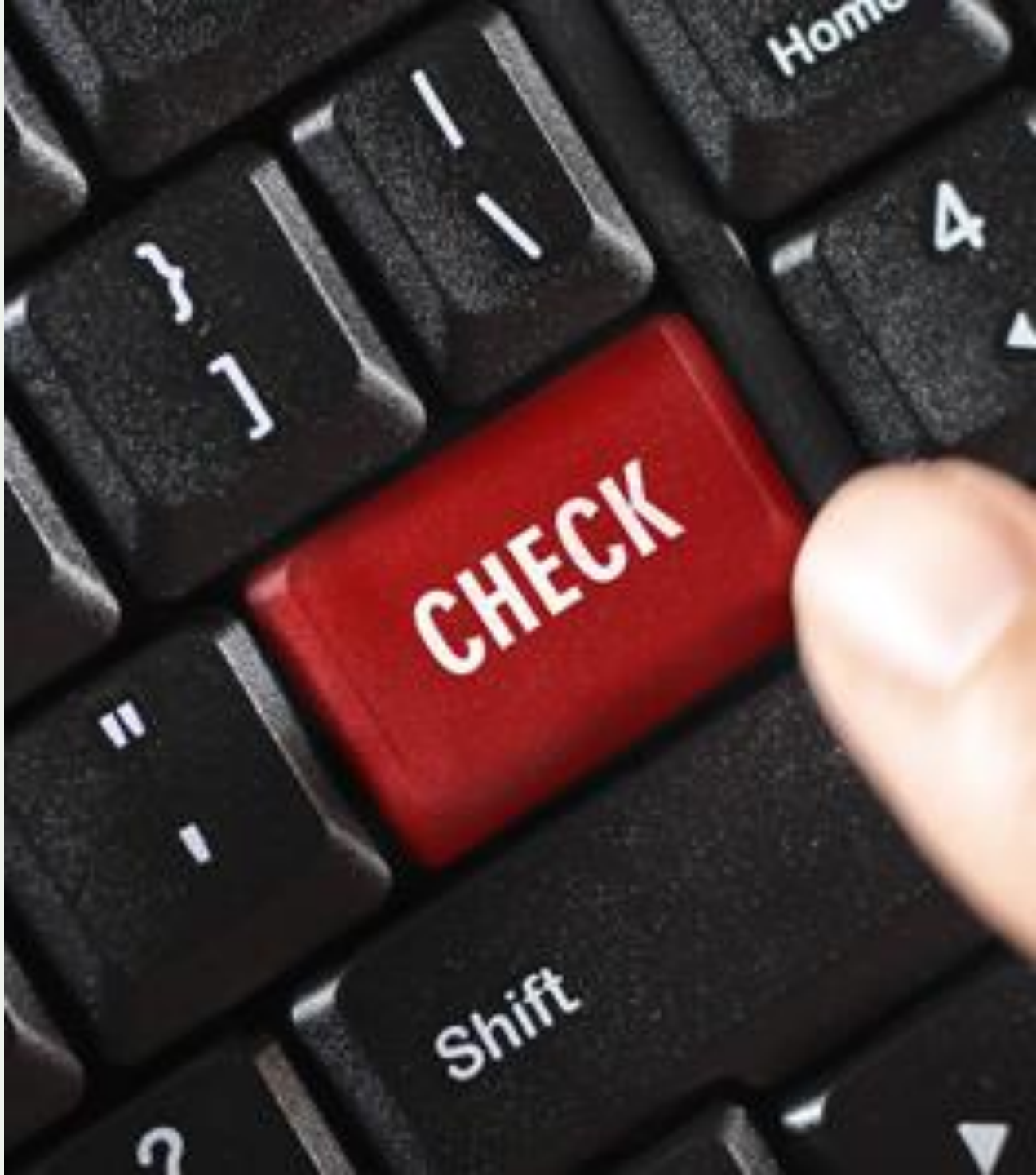
Verificaciones delta

- Como parte de las verificaciones delta, debe procurar que si un filtro cambia por un delta de más de (n)% usted no implemente dicho filtro.
- Asimismo, no se deben crear más filtros hasta que alguien revise el resultado.
  - Donde (n)% es un número internamente acordado, p. ej., 20 %



Prefijos baliza

- Se permite el paso de prefijos especiales o importantes a su red.
- Nunca se permite que los prefijos ***bogon*** pasen a través de sus filtros de prefijos



Ejemplos: Creando filtrado Bogons IPv4

```
ip prefix-list BOGONS_v4 deny 0.0.0.0/8 le 32
ip prefix-list BOGONS_v4 deny 10.0.0.0/8 le 32
ip prefix-list BOGONS_v4 deny 100.64.0.0/10 le 32
ip prefix-list BOGONS_v4 deny 127.0.0.0/8 le 32
ip prefix-list BOGONS_v4 deny 169.254.0.0/16 le 32
ip prefix-list BOGONS_v4 deny 172.16.0.0/12 le 32
ip prefix-list BOGONS_v4 deny 192.0.2.0/24 le 32
ip prefix-list BOGONS_v4 deny 192.88.99.0/24 le 32
ip prefix-list BOGONS_v4 deny 192.168.0.0/16 le 32
ip prefix-list BOGONS_v4 deny 198.18.0.0/15 le 32
ip prefix-list BOGONS_v4 deny 198.51.100.0/24 le 32
ip prefix-list BOGONS_v4 deny 203.0.113.0/24 le 32
ip prefix-list BOGONS_v4 deny 224.0.0.0/4 le 32
ip prefix-list BOGONS_v4 deny 240.0.0.0/4 le 32
```

Ejemplos: Creando filtrado Bogons IPv6

```
ipv6 prefix-list BOGONS_v6 deny ::/8 le 128
ipv6 prefix-list BOGONS_v6 deny 100::/64 le 128
ipv6 prefix-list BOGONS_v6 deny 2001:2::/48 le 128
ipv6 prefix-list BOGONS_v6 deny 2001:10::/28 le 128
ipv6 prefix-list BOGONS_v6 deny 2001:db8::/32 le 128
ipv6 prefix-list BOGONS_v6 deny 2002::/16 le 128
ipv6 prefix-list BOGONS_v6 deny 3ffe::/16 le 128
ipv6 prefix-list BOGONS_v6 deny fc00::/7 le 128
ipv6 prefix-list BOGONS_v6 deny fe80::/10 le 128
ipv6 prefix-list BOGONS_v6 deny fec0::/10 le 128
ipv6 prefix-list BOGONS_v6 deny ff00::/8 le 128
```

Aplicando el prefix-list

```
router bgp 64500
 no synchronization
 neighbor 203.0.113.255 remote-as 64501
 neighbor 203.0.113.255 prefix-list BOGONS_v4 in
 neighbor 203.0.113.255 prefix-list BOGONS_v4 out
 no auto-summary
 !
 neighbor 2001:db8:1000:FFFE::B prefix-list
BOGONS_v6 in
  neighbor 2001:db8:1000:FFFE::B prefix-list
BOGONS_v6 out
```

```
router bgp 64500
 address-family ipv4
  neighbor 203.0.113.251 prefix-list BOGONS_v4 in
  neighbor 203.0.113.251 prefix-list BOGONS_v4 out
 !
 address-family ipv6
  neighbor 2001:db8:1000:FFFD::B prefix-list
BOGONS_v6 in
  neighbor 2001:db8:1000:FFFD::B prefix-list
BOGONS_v6 out
```

Ejemplos: Filtrado Bogons con ASN (AS-PATH)

bgp as-path access-list bogon-asns deny 23456

bgp as-path access-list bogon-asns deny 64496-131071

bgp as-path access-list bogon-asns deny 4200000000-4294967295

```
ip as-path regex-mode asn

ip as-path access-list bogon-asns permit _0_ any
ip as-path access-list bogon-asns permit _23456_ any
ip as-path access-list bogon-asns permit _[64496-64511]_ any
ip as-path access-list bogon-asns permit _[65536-65551]_ any
ip as-path access-list bogon-asns permit _[64512-65534]_ any
ip as-path access-list bogon-asns permit _[4200000000-
4294967294]_ any
ip as-path access-list bogon-asns permit _65535_ any
ip as-path access-list bogon-asns permit _4294967295_ any
ip as-path access-list bogon-asns permit _[65552-131071]_
any

route-map Import-Peer deny 7
   match as-path bogon-asns
!
```

RPKI

RPKI

La idea básica de validar los anuncios de rutas con RPKI es la misma que para los IRR. Un operador de redes registra sus anuncios en forma de objetos de Autorización de origen de ruta (ROA).

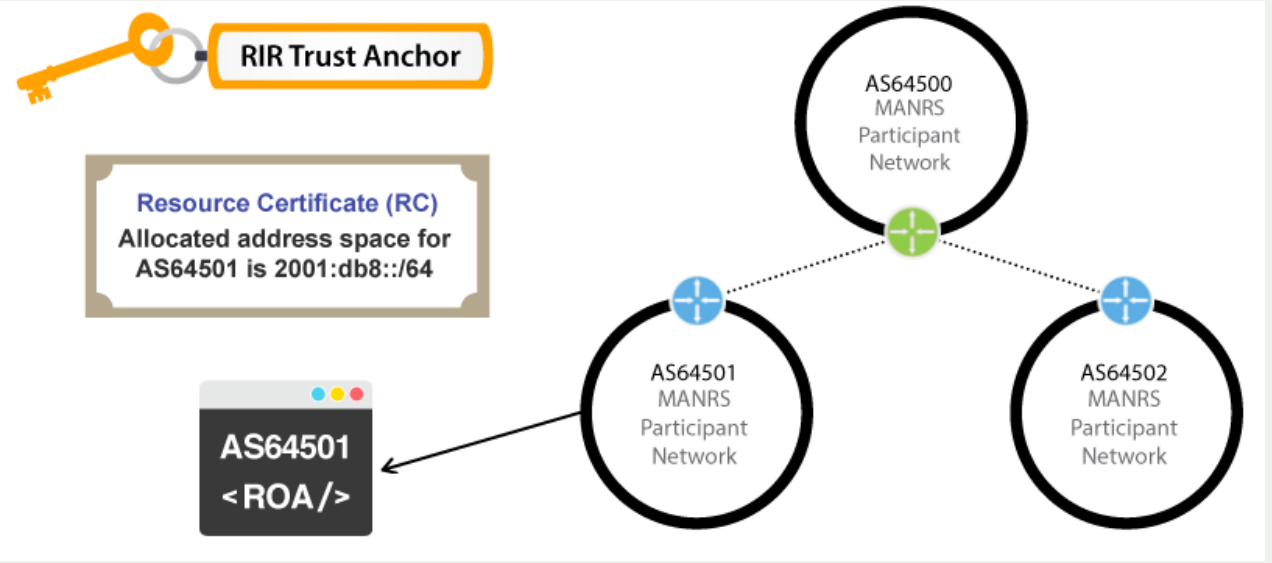
Los operadores utilizan posteriormente los anuncios para generar filtros o para validar los anuncios utilizando una técnica más avanzada como el protocolo RPKI-a-enrutador.

Los objetos ROA son objetos firmados criptográficamente que indican qué Sistema Autónomo (ASA) está autorizado a originar un determinado prefijo.

RPKI

La RPKI trabaja con anclas de confianza emitidas por Certificados de Recursos (RC) de un RIR que indican qué espacio de direcciones se ha asignado a un AS y los objetos ROA que crean sus clientes.

Suponga que AS64501 anuncia 2001:db8::/64. Se utiliza un ancla de confianza para firmar el Certificado de recursos (RC). El RC firmado se utiliza luego para firmar la ROA. Si AS64502 también anuncia 2001:db8::/64, entonces la ROA firmada invalidará el anuncio.



Ejemplo

El validador RPKI se puede configurar conforme al proceso de enrutamiento de BGP.

```
apt install rpki-rp
```

Ahora el enrutador, registrará que rutas son validas según las ROAs, cuales son no válidas y que rutas no están cubiertas por las ROAS. Puede usar esto en su Política de Enrutamiento.

```
#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
```

Ejemplo

```
router bgp 64500
 bgp log-neighbor-changes
 bgp rpki server tcp 10.1.1.6
 address-family ipv4
  bgp bestpath prefix-validate disable
 address-family ipv6
  bgp bestpath prefix-validate disable
!
route-map ebgp-in deny 1
 match rpki invalid
!
```

```
router bgp 64500
  # configure RTR
  rpki cache 10.1.1.6
    host 10.1.1.6
    local-interface Loopback0
  !
  # enable origin validation
  rpki origin-validation
    ebgp local
!
```

Mejores Practicas de Filtrado

- No aceptar prefijos RFC1918 etc (Bogons).
- No acepte su propio prefijo
- No acepte el prefijo por defecto (a menos que lo necesite)
- No acepte prefijos más largos que /24
- Considere el Filtrado de la Política de Enrutamiento de la red.

Autoevaluación

En este momento, iniciemos con los procesos de autoevaluación de nuestros recursos.

- Comprobar que el ASN no anuncia Bogons. IPv4 IPv6
- Comprobar que el ASN no estuvo implicado en incidentes recientes.
- Validación de registros de RPKI
- Verificar si se validan los ROAs internamente

Referencias

- Recursos: https://stat.ripe.net
- IRR Toolset: https://github.com/irrtoolset/irrtoolset
- BGPQ3: https://github.com/snar/bgpq3
- IRRPT: https://github.com/6connect/irrpt
- Validador RPKI: https://rpki-validator.ripe.net/
- Uso de IRR en LACNIC: https://labs.lacnic.net/Uso-de-IRR-LACNIC/
- Filtros BGP, seguridad e ingeniería de tráfico:
  - https://peruix.net/2021/02/15/filtros-bgp-seguridad-e-ingenieria-de-trafico/
- Manual de referencia MANRS (Filtrado): https://www.manrs.org/isps/guide/filtering/
- Ejemplos: https://bgpfilterguide.nlnog.net/

Lecturas Recomendadas

RFC2827: https://datatracker.ietf.org/doc/html/rfc2827

RFC3704: https://datatracker.ietf.org/doc/html/rfc3704

BCP38: http://bcp38.info/

Acción 2: Anti-Suplantación:

Prevención del tráfico con direcciones IP de origen falsificadas

Objetivos

- Identificar los puntos y los dispositivos dentro de la topología de red donde deben aplicarse medidas antisuplantación.
- Explicar cómo se pueden utilizar técnicas tales como el filtrado de ACL y uRPF para proteger su red contra la suplantación de direcciones IP.
- Configurar sus dispositivos para impedir la suplantación de direcciones IP y verificar que la protección funcione.

Introducción

Hay algunas de las acciones MANRS que son relevantes y pertinentes para la antisuplantación. Los participantes de MANRS deben realizar las dos acciones para evitar el tráfico con direcciones IP de origen suplantadas.

- Implementar un sistema que permita la validación de direcciones de origen para, al menos, las redes de clientes, sus propios usuarios finales y la infraestructura.

- Implementar un filtrado antisuplantación para evitar que los paquetes que contengan direcciones IP de origen incorrectas entren y salgan de la red.

Introducción a la antisuplantación

¿Qué es IP address Spoofing?

Paquetes con una dirección IP de origen falsa o suplantada.

Mala configuración.

- Problema de software

Simulación y Pruebas

- Pruebas de rendimiento

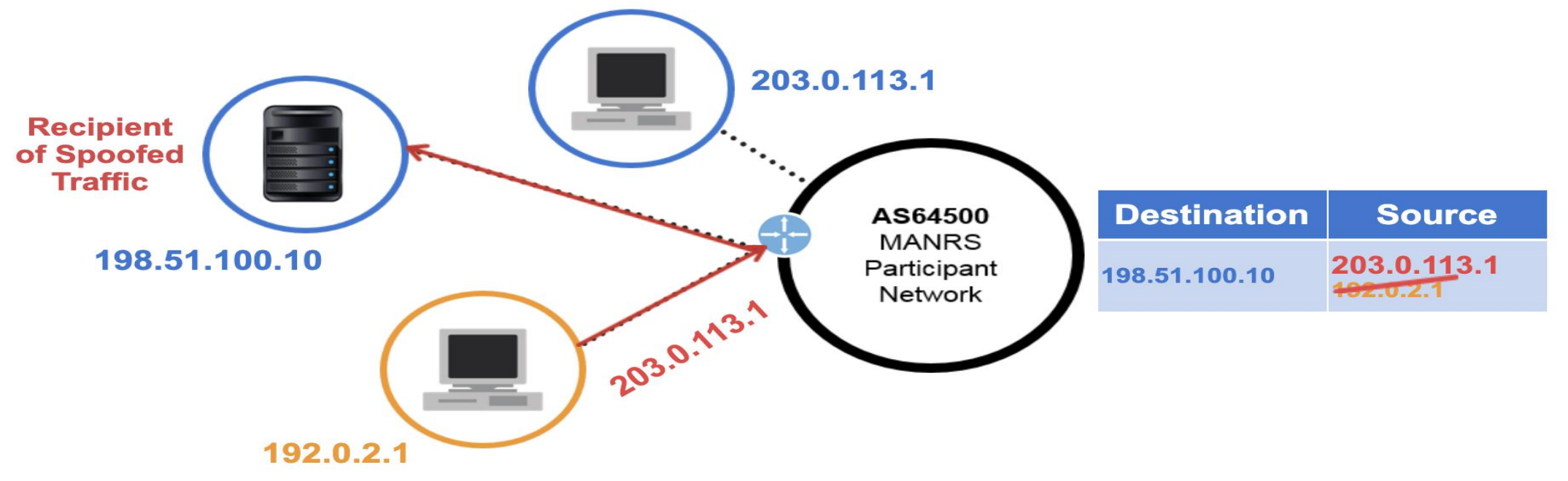
Intentos maliciosos

- Oculta la identidad del origen
- Hacerse pasar por otro host

Utilizado con mayor frecuencia para ataques de denegación de servicio DDoS

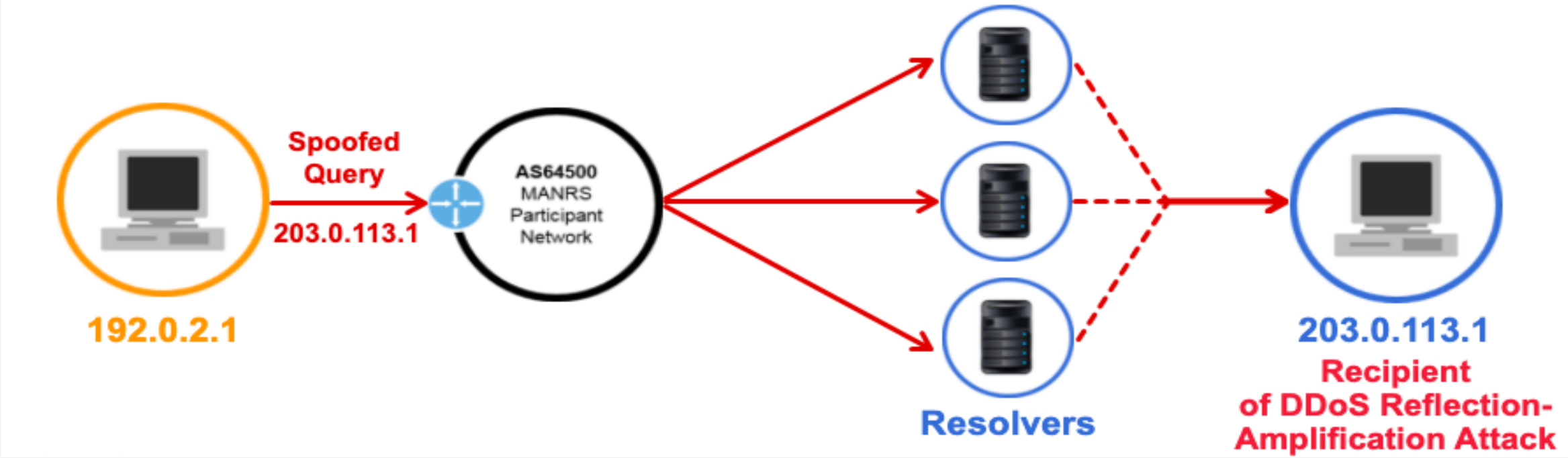
¡Cualquiera puede ser una víctima!

Suplantación de direcciones IP



La suplantación de direcciones IP de origen es la práctica de originar datagramas de IP con direcciones de origen distintas de las asignadas al host de origen. En términos simples, el host finge ser otro host.

Suplantación de direcciones IP



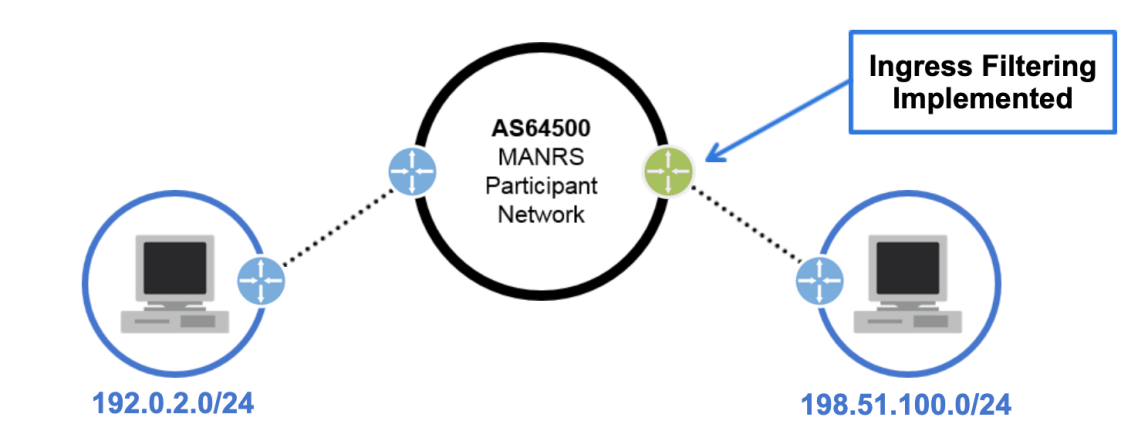
La reflexión ocurre cuando un atacante envía tráfico a una víctima a través de un tercero. La amplificación se logra mediante consultas pequeñas que generan respuestas mucho mayores. Los resolutores DNS y servidores NTP abiertos se utilizan comúnmente como reflectores/amplificadores.

¿Cómo podemos prevenir el ataque DDoS de amplificación y reflexión?

Hay varias recomendaciones para evitar la suplantación de direcciones IP mediante el filtrado de ingreso; p. ej.,

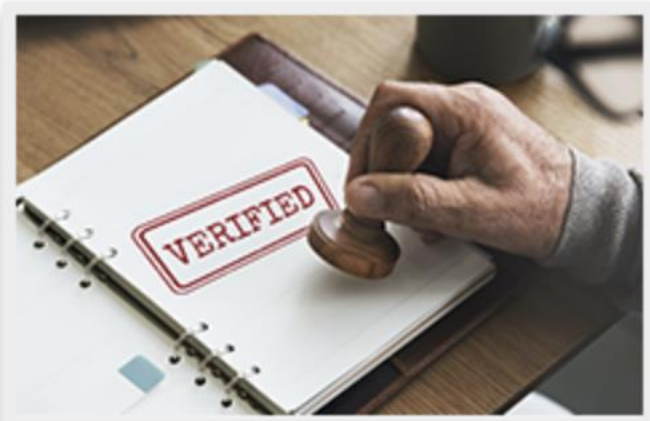
- verificando las direcciones de origen de los datagramas IP cercanos al borde de la red.

La mayoría de los proveedores de equipos admiten alguna forma de filtrado de ingreso



¿Cómo podemos prevenir el ataque DDoS de amplificación y reflexión?

Para evitar la suplantación de direcciones IP de origen, se recomienda implementar métodos de filtrado de ingreso. Entre estos métodos se incluyen:

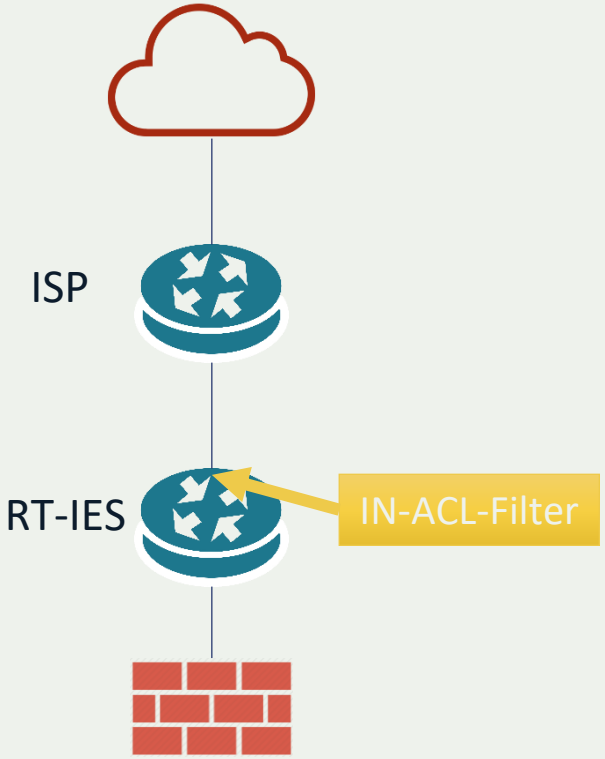


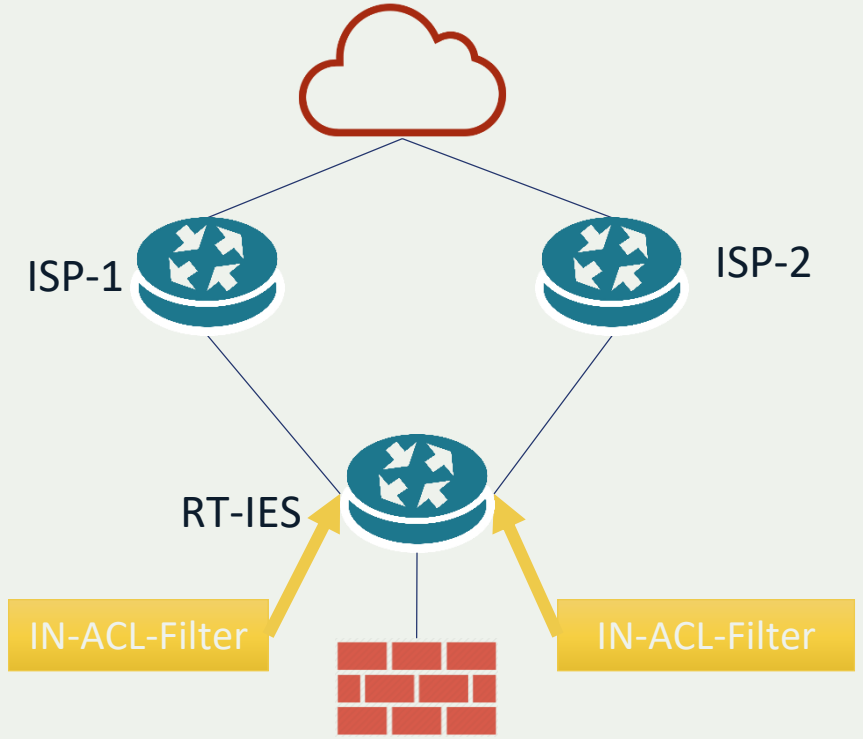
Access Control Lists

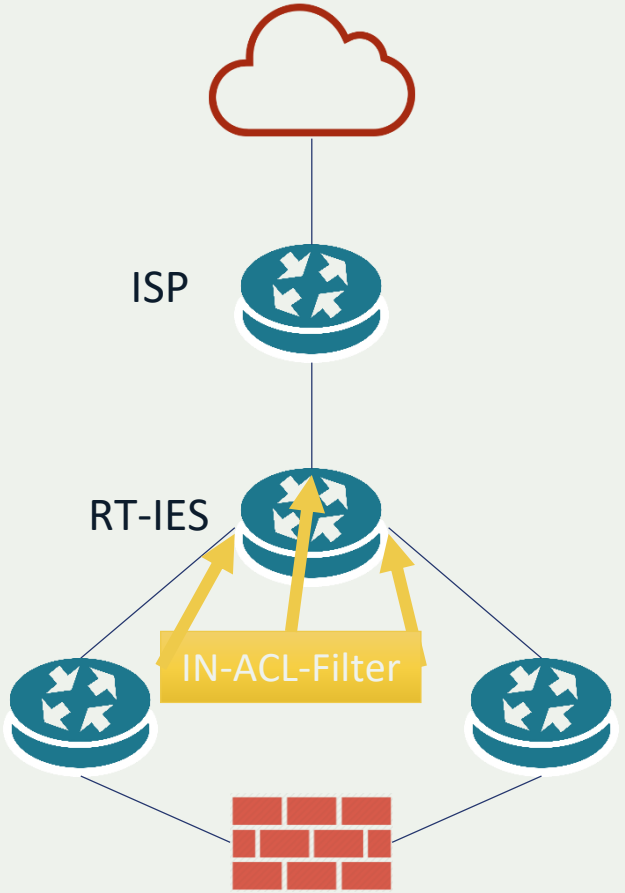
uRPF

ACL

ACL

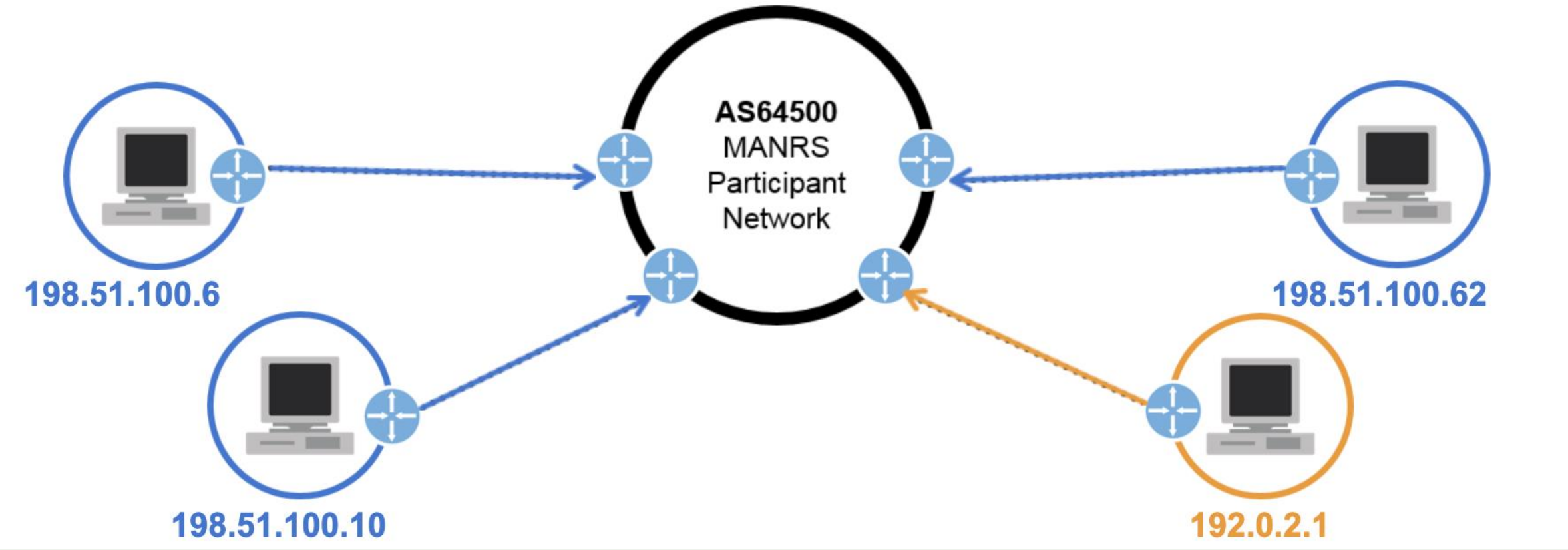

ISP
RT-IES
IN-ACL-Filter


ISP-1
ISP-2
RT-IES
IN-ACL-Filter
IN-ACL-Filter


ISP
RT-IES
IN-ACL-Filter

ACL

Las listas de control de acceso (ACL) se utilizan para filtrar el tráfico de red al controlar si los paquetes enrutados se reenvían o bloquean en las interfaces del enrutador. Las ACL se configuran para admitir rangos específicos de direcciones y denegar todos los demás.



ACL

Si el bloque de IPs del cliente de un ISP es 198.51.100.0/24, la ACL admitiría paquetes con direcciones de origen de 198.51.100.0/10 y denegaría paquetes que se originan desde distintas IPs de origen, por ejemplo, 192.0.2.1. Las ACL deben implementarse en las interfaces descendentes del ISP para verificar las direcciones de origen que utilizan sus clientes.

ACL 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
```

ACL Juniper

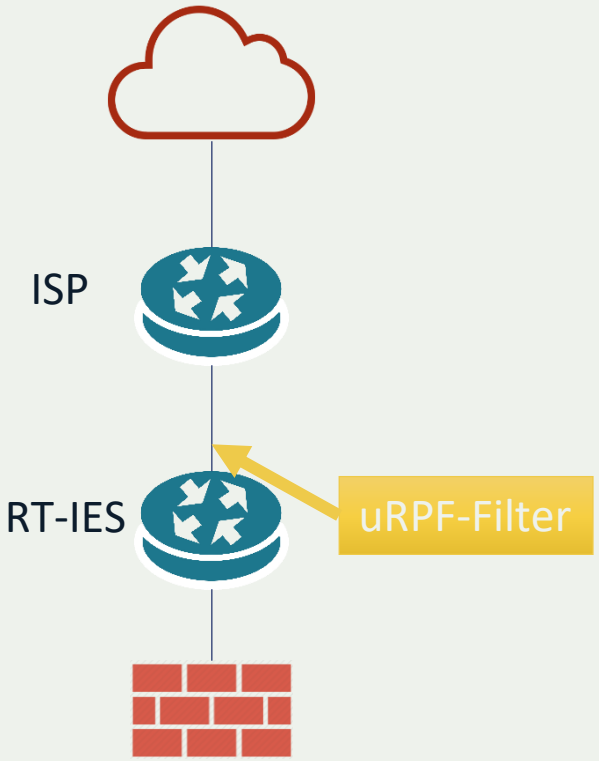
```
firewall {
    family inet {
        filter customer1-in-ipv4 {
            term allowed-sources {
                from {
                    source-address {
                        192.0.2.0/24;
                    }
                }
                then accept;
            }
        }
    }
```

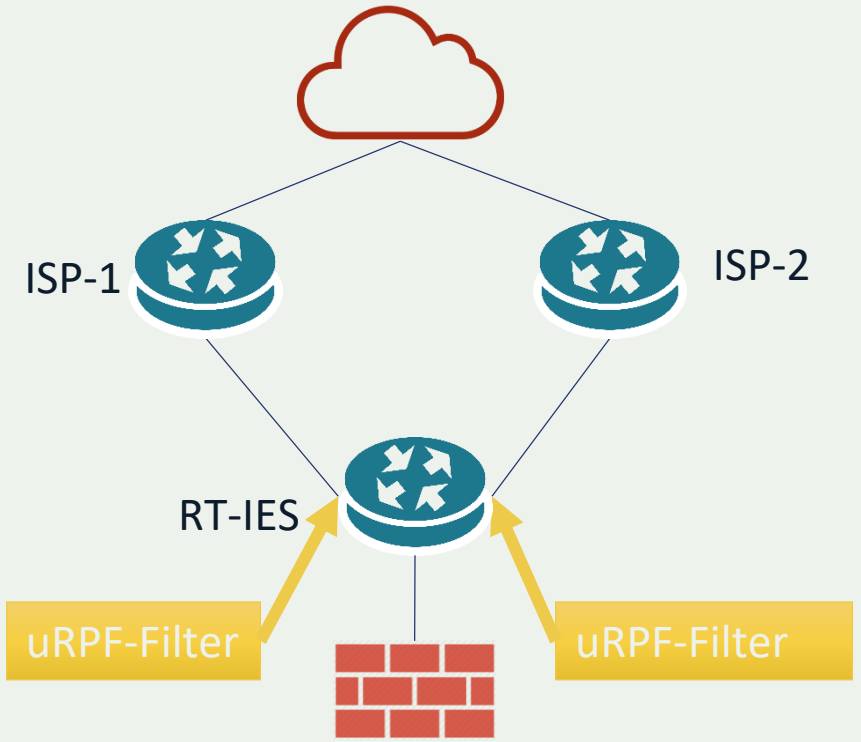
ACL MikroTik

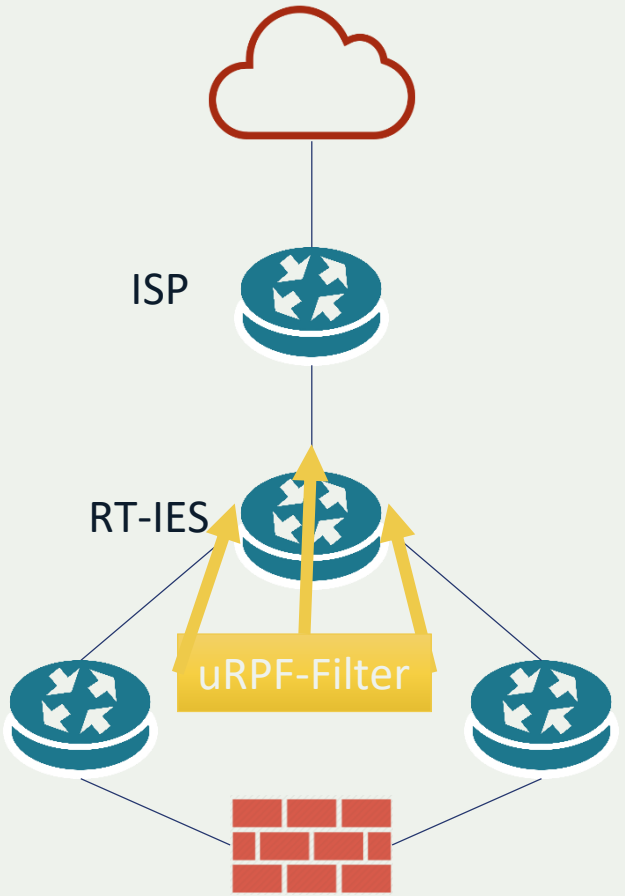
```
/ip firewall filter add action=drop chain=forward comment="spoofed from
AS64501" in-interface=$interface log-prefix="" src-address=!192.0.2.0/24

/ipv6 firewall filter add action=drop chain=forward comment="spoofed from
AS64501" in-interface=$interface log-prefix="" src-
address=!2001:db8:1001::/48
```

uRPF

uRPF


ISP
RT-IES
uRPF-Filter


ISP-1
ISP-2
RT-IES
uRPF-Filter
uRPF-Filter


ISP
RT-IES
uRPF-Filter

uRPF

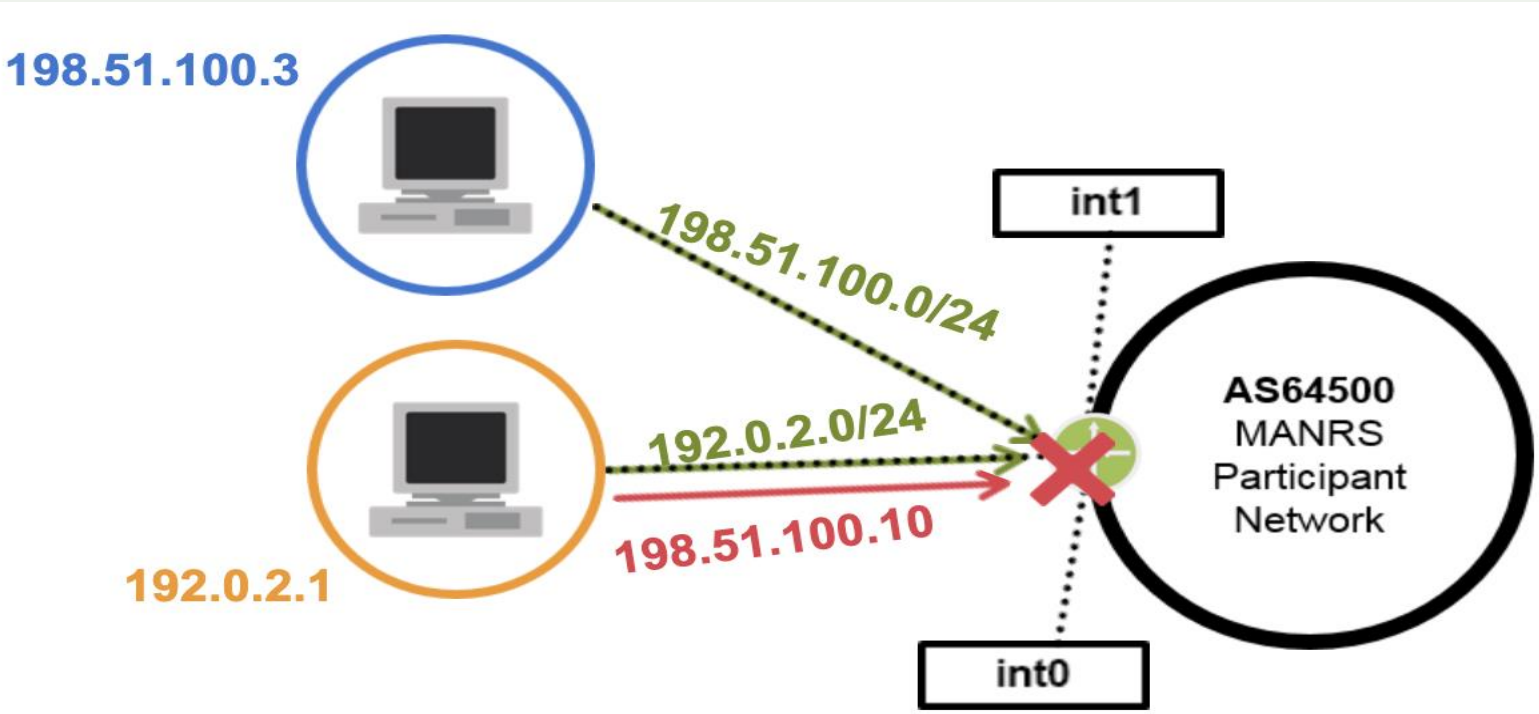
uRPF, según se define en RFC 3704, es una evolución del concepto de que el trafico proveniente de redes no validas conocidas no debería aceptarse en interfaces desde las que nunca deberían haberse originado.

Hay cuatro algoritmos de uRPF:

- **Modo estricto – Strict.** (verificar la IP de origen y la adyacencia).
- **Modo suelto – Loose.** (verificar solo la IP de origen).
- **Ruta factible – Feasible Path.** (verificar la IP de origen con las alternativas de la FIB).
- **Modo VRF** (admitir/denegar la verificación del origen en una tabla independiente de la FIB).

uRPF

Para los clientes con conexión simple (single-homed), se recomienda la implementación del modo uRPF estricto. Para los clientes con conexión múltiple (multi-homed), es mejor usar el modo uRPF factible en su lugar. uRPF suele implementarse en los bordes de las redes donde están conectados los servidores o los clientes.



FIB	
198.51.100.0/24	int1
192.0.2.0/24	int0

Announced network	Incoming pkt source ip
192.0.2.0/24	198.51.100.10 ~~192.0.2.1~~

A FIB record for 198.51.100.10 does not correspond to the incoming interface.

uRPF Cisco

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

uRPF Juniper

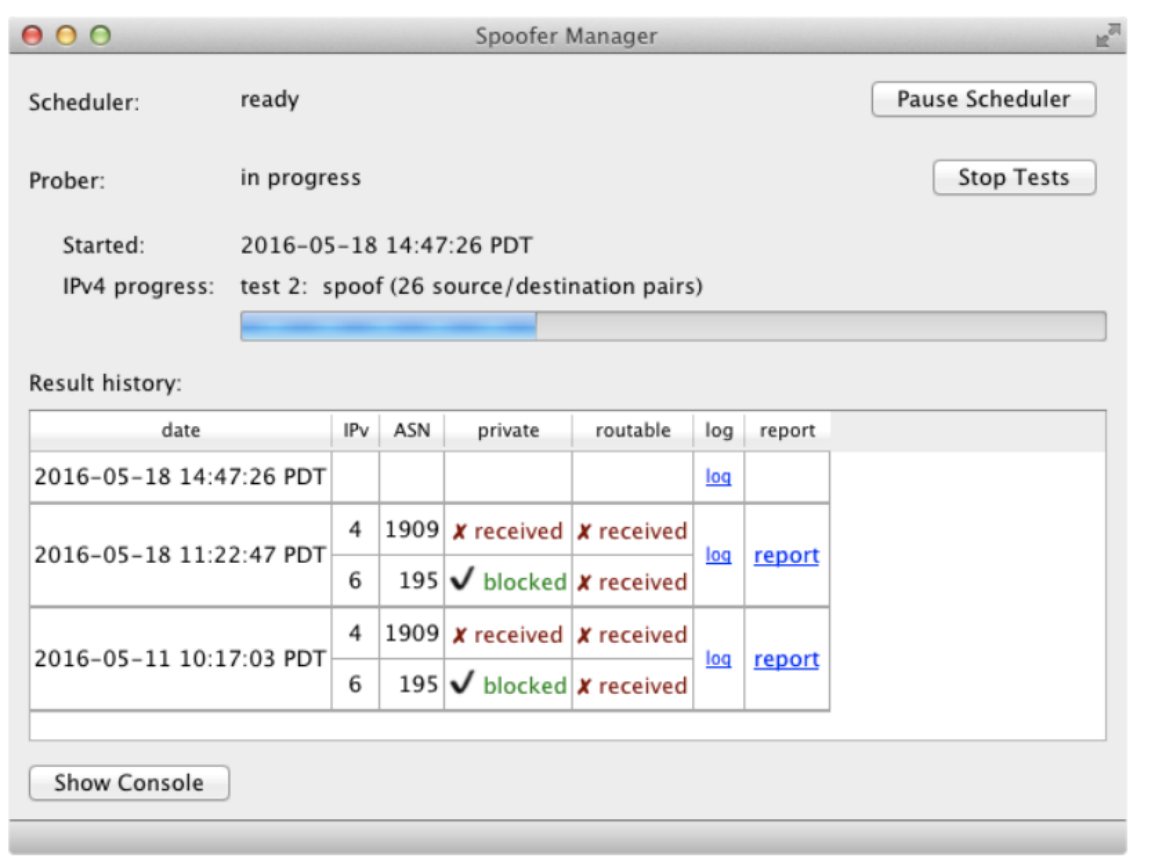
```
family inet {
   rpf-check;
}
family inet6 {
   rpf-check;
}
```

uRPF MikroTik

```
/ip settings set rp-filter=strict
```

Verificación de la protección antisuplantación

Verificación de la protección antisuplantación



Una forma de verificar que su protección antisuplantación funcione es ejecutar un experimento controlado realizando una prueba de suplantador. Sería beneficioso que uno de sus clientes pudiera ejecutar la prueba por usted.

https://www.caida.org/projects/spoofer/

Autoevaluación

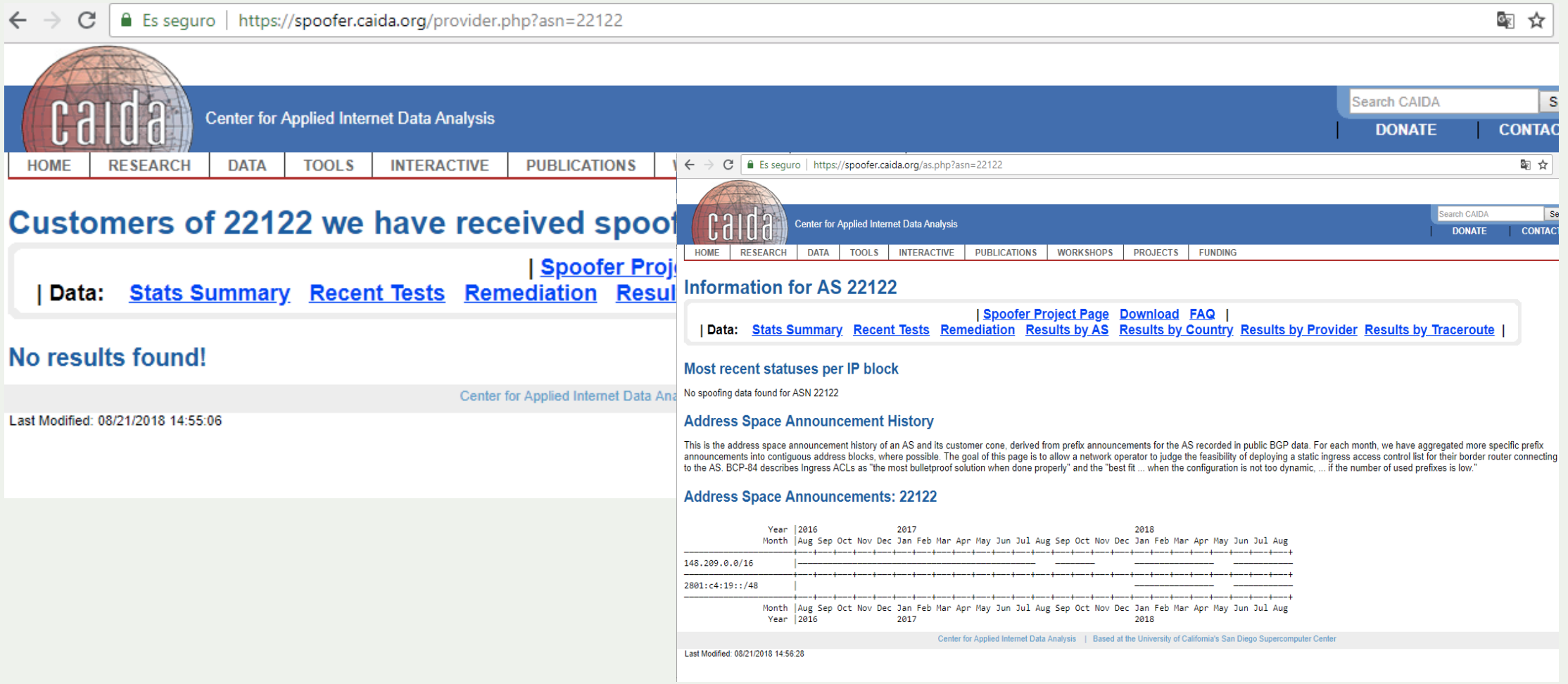
En este momento, iniciemos con los procesos de autoevaluación de nuestros recursos.

- Comprobar que el ASN aplica correctamente ACLs.
- Comprobar que el ASN aplica correctamente uRPF.

Acciones de validación Anti-spoofing

Checar que su ASN no aparezca en la base de datos de Spoofer CAIDA.	
Como proveedor: https://spoofer.caida.org/provider.php?asn=[ASN]	Como ASN: https://spoofer.caida.org/as.php?asn=[ASN]

Acciones de validación Anti-spoofing



Herramientas: Spoofer

Spoofer Manager GUI

Spoofer Scheduler Prober

Scheduler: ready — Pause Scheduler

Prober: next scheduled for 2019-06-15 18:05:14 Hora de verano central (México) (in about 7 days) — Start Tests

Last run: 2019-06-08 16:58:54 Hora de verano central (México)

*** Error: no interface for 192.168.0.10

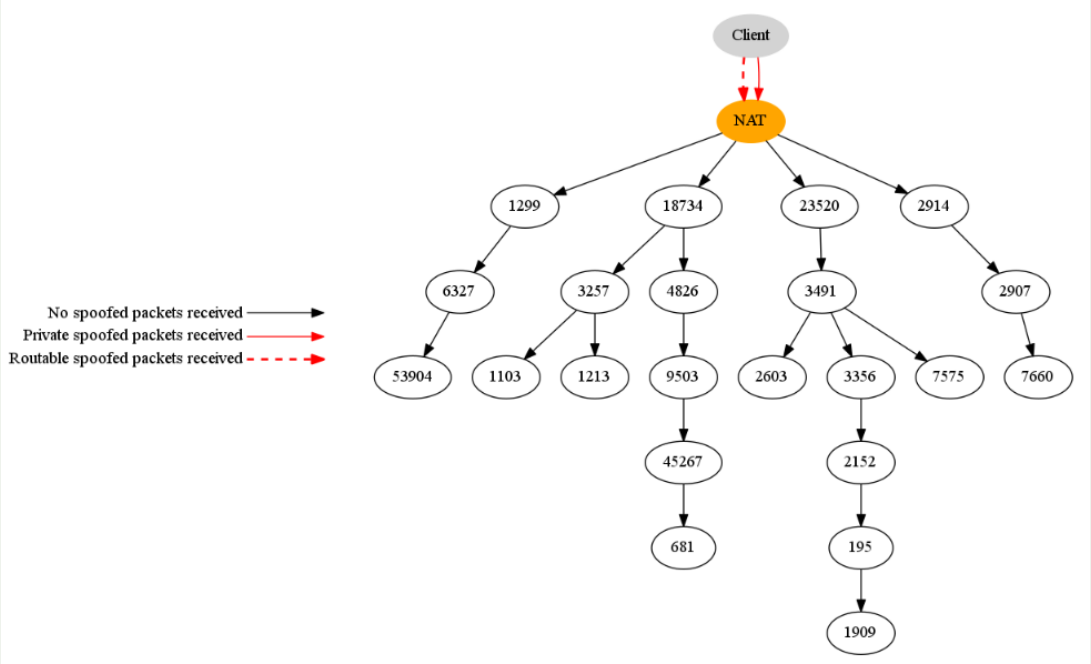
*** Notice: No accessible nonlocal IPv6 interfaces.

*** Notice: Can not test IPv6 spoofing.

Result history: ☑ Hide old blank tests

date	IPv	client address	ASN	outbound private	outbound routable	inbound private	inbound internal	report
2019-06-08 16:58:54	4	177.237.175.32	28545	✔ blocked	✔ blocked			report

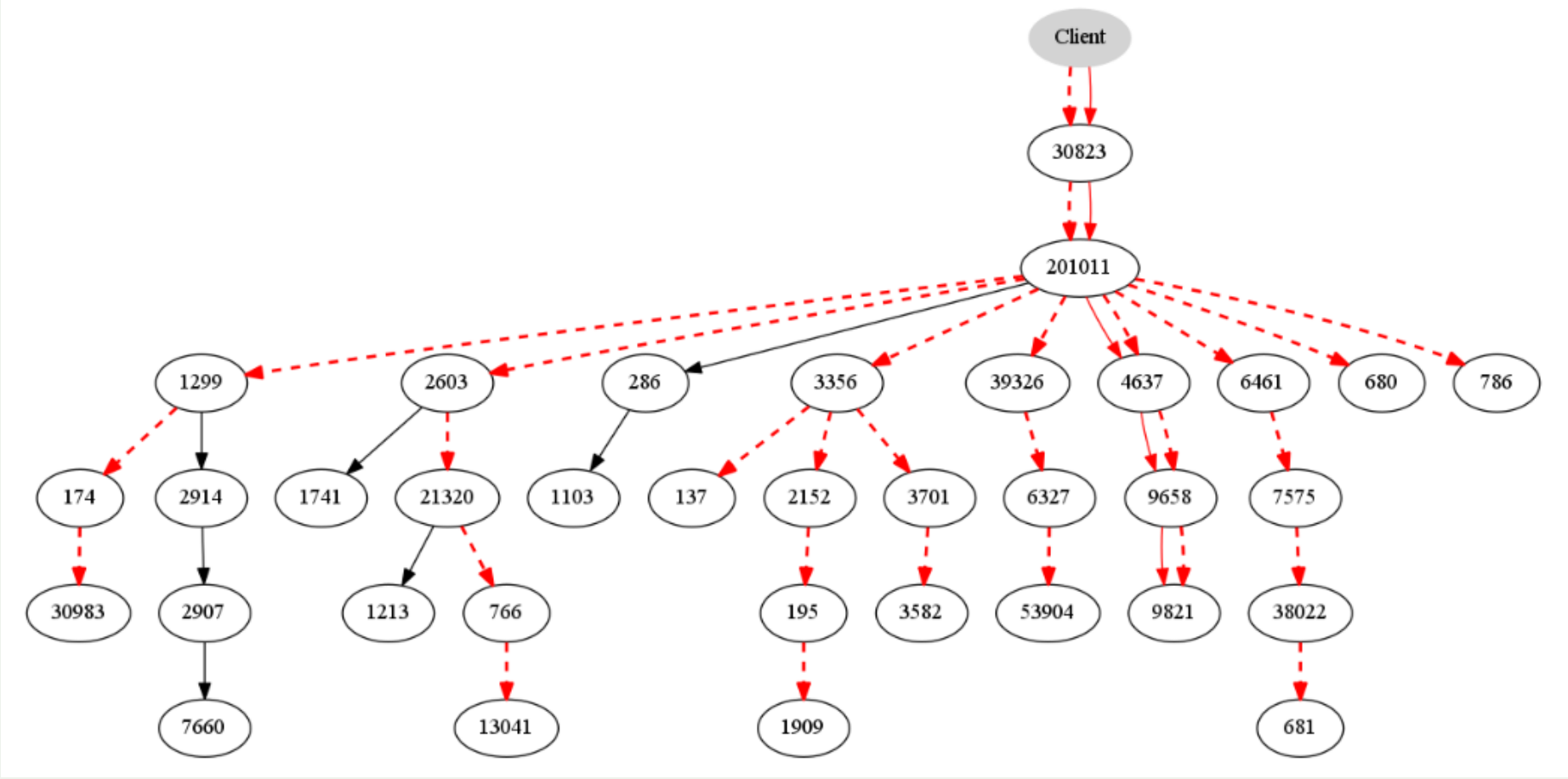
```
>> Ready to test (please allow several minutes to complete).
>> Options:
>>   IPv4: enabled
>>   IPv6: enabled
>>   sharePublic: yes
>>   shareRemedy: yes
>>   enableTLS: yes
>>   multiThreaded: yes
>> Started: 2019-06-08 21:58:54 UTC

dev \Device\NPF_{0E4E4159-758A-4289-9321-25F87FA5F843} (Microsoft)
```



Herramientas: Spoofer

El host (212.114.50.x/24 puede falsificar 16,777,215 direcciones vecinas
(Dentro de tu prefijo /8)

Spoofed source address (anon)	Prefix Length	ASN of spoofed source address	Received
212.114.50.x/24	/31	30823	yes
212.114.50.x/24	/30	30823	yes
212.114.50.x/24	/29	30823	yes
212.114.50.x/24	/28	30823	yes
212.114.50.x/24	/27	30823	yes
212.114.50.x/24	/26	30823	yes
212.114.50.x/24	/25	30823	yes
212.114.50.x/24	/24	30823	yes
212.114.51.x/24	/23	30823	yes
212.114.48.x/24	/22	34549	yes
212.114.54.x/24	/21	198599	yes
212.114.58.x/24	/20	200303	no
212.114.34.x/24	/19	12843	yes
212.114.18.x/24	/18	2118	yes
212.114.114.x/24	/17	12859	yes
212.114.178.x/24	/16	8767	yes
212.115.50.x/24	/15	44050	no
212.112.50.x/24	/14	13189	yes
212.118.50.x/24	/13	25308	yes
212.122.50.x/24	/12	16097	yes
212.98.50.x/24	/11	6730	yes
212.82.50.x/24	/10	9063	yes
212.50.50.x/24	/9	29286	yes
212.242.50.x/24	/8	9158	yes



https://spoofer.caida.org/report.php?sessionid=59431

Referencias

- Recursos: https://stat.ripe.net
- Spoofer: https://www.caida.org/projects/spoofer/
- Configuring ACL Cisco:

  https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html
- Cisco uRPF: https://tools.cisco.com/security/center/resources/unicast_reverse_path_forwarding
- Cisco Guide to Harden Cisco IOS Device: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

Lecturas Recomendadas

RFC 3704: https://datatracker.ietf.org/doc/html/rfc3704

RFC4314: https://datatracker.ietf.org/doc/html/rfc4314

Understanding Unicast Reverse Path Forwarding

- https://www.cisco.com/c/en/us/about/security-center/unicast-reverse-path-forwarding.html

Security Configuration Guide: Unicast Reverse Path Forwarding

- https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_urpf/configuration/xe-3s/sec-data-urpf-xe-3s-book.html

RFC 2267Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing

- https://www.ietf.org/rfc/rfc2267.txt

Dudas o Preguntas

Gracias.

Mauricio Oviedo

Email: mauricio@socium.cr

Emmanuel Serrano

Email: isc.emmanuel.serrano@gmail.com

manrs.org