Universidad Nacional Autónoma de México

Dirección General de Cómputo y de Tecnologías de la Información

1.Adopción de buenas prácticas MANRS

Probatorio

carlos.altamirano@unam.mx
hugo.rivera@unam.mx

Ciudad Universitaria, 2 de marzo de 2022

1. **Introducción**

La arquitectura de la RedUNAM consiste en un Backbone, integrado por 4 nodos principales ubicados en Ciudad Universitaria y conectado en full-mesh el cual proporciona una conexión redundante e independiente en caso de falla de alguno de estos nodos. Cada uno de estos nodos a su vez tiene un siguiente nivel de comunicación el cuál se le conoce como capa de Distribución, en esta capa se encuentran 4 ruteadores de la marca Cisco, modelos ASR 100X, los cuales interconectan a la RedUNAM a Internet e Internet2.

Esta infraestructura física cuenta con recursos lógicos necesarios para la comunicación a Internet como lo son un número de sistema autónomo (AS, Autonomous System) y prefijos asignados por NIC México tanto de IPv4 como de IPv6.

Para llevar a cabo la interconexión y comunicación a estas redes se requiere de la configuración del protocolo de borde de frontera (***Border Gateway Protocol, BGP***) el cual establece una vecindad (peering) entre el router conectado a RedUNAM y el del Proveedor de Servicio de Internet (ISP), una vez establecida esta comunicación se puede iniciar el anunciamiento y recepción de prefijos de red (segmentos de redes IPv4 o IPv6) entre ambos equipos, cada uno perteneciente a un Sistema Autónomo diferente, para que a su vez el ISP los anuncie a otros proveedores que se interconectan con él para que los prefijos de la RedUNAM (AS278) sean conocidos por todo Internet y el tráfico pueda llegar al destino desde su origen en Internet.

Este intercambio de prefijos entre los diferentes AS es lo que permite la comunicación y construcción de Internet, cada AS es único en Internet y cada prefijo de red que se anuncia en Internet pertenece a uno y sólo un AS, esto para asegurar que el tráfico pueda llegar a su destino y evitar que exista duplicidad de anuncios lo cual pudiera provocar, en caso de existir, que el tráfico no alcance su destino.

Cada uno de los AS tiene registrado un contacto técnico el cual es requerido en caso de presentarse algún incidente hacia su red o que esté originando su red y que afecte a uno o más usuarios de otro AS, a veces estos incidentes son involuntarios, pero en otros casos puede haber incidentes provocados deliberadamente por alguien que tiene interés en afectar las comunicaciones en Internet. Entre estos incidentes se pueden presentar los siguientes:

1. Información de enrutamiento incorrecta.
2. Tráfico con direcciones IP de origen falsificadas.

Cada AS define políticas de enrutamiento, a través de configuraciones en los ruteadores que llevan a cabo el peering de eBGP y a través de estas políticas debe anunciar solamente el número de AS que le ha sido asignado, así como los prefijos IPv4 o IPv6 relacionados a este mismo AS. Esta es la primera y más importante política que debe existir y llevar a cabo el personal que opera y gestiona estos ruteadores y sus configuraciones hacia sus ISP´s.

En caso de que este AS proveedor tenga conectados clientes que a su vez tengan su propio AS y prefijos IP y que quieran utilizar a este AS proveedor como acceso a otras redes o Internet, el AS proveedor deberá verificar que los anuncios de prefijos de sus clientes son correctos, que los prefijos que recibe del AS cliente estén asignados legítimamente por la autoridad competente.

Así como el operador de red de este AS cuida lo que está anunciando hacia los ISP´s con quien tiene conexiones, también debe tener en cuenta establecer políticas de enrutamiento en donde evite que estos ISP´s puedan inyectar prefijos IP no permitidos y con ello evitar que tráfico hacia esas redes no permitidas salga a Internet, utilizando recursos de ancho de banda y generando tráfico que puede afectar a otros usuarios. Actualmente el protocolo BGP tiene opciones para realizar esto pero se requiere de acciones coordinadas para poder definir las redes cuyo origen es inválido o ciertamente no pertenecen a un AS registrado y con ello enviar tráfico a un lugar que está realizando un secuestro de redes con toda intención de beneficiarse de ello o afectar al dueño de esos recursos.

Algunos casos de secuestro de rutas que han afectado a miles o millones de usuarios han sido los de Visa Mastercard en 2017 y Amazon-Google en 2018[1].

Debido a estos y otros casos más que pueden afectar el acceso a diversos sitios de Internet, inclusive los propios de la Universidad, es que se propuso la adopción de la iniciativa para fortalecer la seguridad de Internet a través de la validación de los anuncios de enrutamiento denominada MANRS (Mutually Agreed Norms for Routing Security) .

Iniciativa MANRS

MANRS es una iniciativa comunitaria organizada por Internet Society (ISOC), que tiene como objetivo mejorar la seguridad y la estabilidad del sistema de enrutamiento global. Es una propuesta para que los operadores de red trabajen juntos para crear un nuevo estándar de un enrutamiento más seguro y resistente.

MANRS define 4 y promueve un internet más seguro a través de las siguientes 4 acciones:

1. Filtrado
2. Anti-Spoofing
3. Coordinación
4. Validación

Estas 4 acciones han sido planeadas, diseñadas y configuradas para su operación en la infraestructura de la RedUNAM por miembros del equipo de trabajo del NOC RedUNAM con apoyo del NIC UNAM y patrocinado por la Subdirección de Operación de la Red, así como de la Dirección de Telecomunicaciones de la DGTIC.

A continuación se describen las actividades para lograr llevar a cabo las 4 acciones que propone MANRS.

[1] Consultados el 26 de enero de 2022 en: https://www.icm.es/2021/05/07/que-son-secuestros-de-rutas/

Pruebas de concepto

Antes de implementar las acciones de filtrado, se preparó un escenario de pruebas en la plataforma Cisco Devnet Sandbox. Esta plataforma provee acceso a diferentes ruteadores virtuales para simular la configuración que se pretende aplicar en producción, con ello evitamos que en caso de que se presente algún error o que el diseño de las reglas no sea el adecuado pueda ser rediseñado y modificado para nuevamente aplicarlo, esto no es sencillo hacerlo en ambientes de producción pues podriamos afectar la operación de alguna entiad universitaria o todos un Campus.

1. Acción de Filtrado[2].

Esta acción es necesaria para prevenir la incorrecta propagación de información de ruteo mediante políticas de anuncio y recepción de redes IPv4 e IPv6 a través del protocolo BGP (Border Gateway Protocol). Este protocolo es utilizado para el anuncio y recepción de rutas en internet, al cual se le tienen que aplicar filtros para el aseguramiento de su tráfico. Esta acción se implementó en los ruteadores de internet CU y en los ruteadores de las dependencias foráneas que cuentan con uno o más enlaces de internet local, mediante filtros configurados y aplicados tanto a la entrada como a la salida del tráfico para evitar la propagación y recepción de de rutas falsas que pudieran alterar el comportamiento del tráfico.

MANRS recomienda filtrar anuncios de red tanto de entrada (las redes que recibe el Sistema Autónomo), como de salida que son las redes que se anuncian a los proveedores de internet desde el Sistema Autónomo de la UNAM.

Estas recomendaciones fueron aplicadas en la configuración del protocolo BGP (Border Gateway Protocol) de los ruteadores principales de CU y de los enlaces de internet local de la siguiente manera:

1.1. Filtrado de rutas en BGP IPv4 de entrada y salida en los enlaces principales de CU.

Para esta actividad se tomaron en cuenta las mejores prácticas definidas en el BCP 194 y en el RFC 7454[3] (BGP Operations and Security). En esta Best Practice se recomienda realizar los siguientes filtros:

- Prefijos no ruteables
- Rutas que sean muy específicas
- Rutas que pertenezcan al Sistema Autónomo local

A partir de este documento, se propuso utilizar la siguiente configuración para cumplir con la acción de filtrado en IPv4 en los enlaces de internet en CU, ya que estos ruteadores reciben la tabla completa de BGP por parte de los diferentes proveedores que proporcionan el acceso a Internet al Campus C.U.

[2] https://www.manrs.org/isps/guide/filtering/

[3] https://datatracker.ietf.org/doc/html/rfc7454

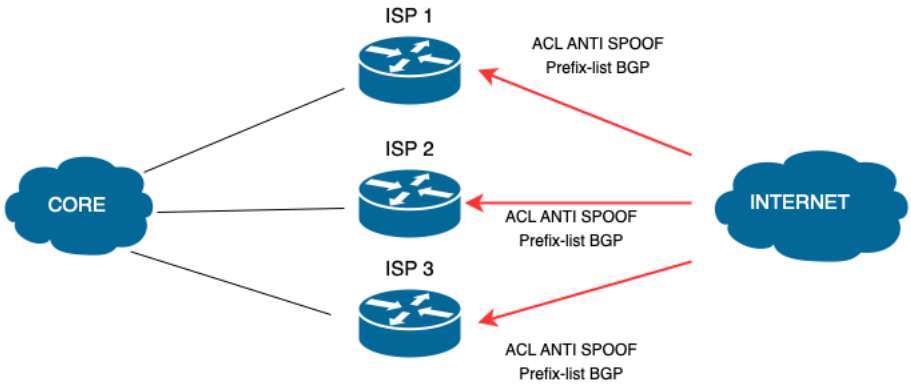
ip prefix-list INVALIDAS_BGP_IN seq 5 deny 0.0.0.0/8 le 32
ip prefix-list INVALIDAS_BGP_IN seq 10 deny 10.0.0.0/8 le 32
ip prefix-list INVALIDAS_BGP_IN seq 15 deny 127.0.0.0/8 le 32
ip prefix-list INVALIDAS_BGP_IN seq 20 deny 169.254.0.0/16 le 32
ip prefix-list INVALIDAS_BGP_IN seq 25 deny 172.16.0.0/12 le 32
ip prefix-list INVALIDAS_BGP_IN seq 30 deny 192.0.2.0/24 le 32
ip prefix-list INVALIDAS_BGP_IN seq 35 deny 192.168.0.0/16 le 32
ip prefix-list INVALIDAS_BGP_IN seq 40 deny 224.0.0.0/3 le 32
ip prefix-list INVALIDAS_BGP_IN seq 45 deny 0.0.0.0/0 ge 25
ip prefix-list INVALIDAS_BGP_IN seq 50 permit 0.0.0.0/0 le 32

Al mismo tiempo, se propuso utilizar la siguiente configuración para cumplir con la acción de filtrado en IPv6 en los enlaces de internet en CU, ya que estos ruteadores reciben la tabla completa de BGP.

ipv6 prefix-list INVALIDAS_IPV6_IN seq 5 deny 3FFE::/16 le 128
ipv6 prefix-list INVALIDAS_IPV6_IN seq 10 deny 2001:DB8::/32 le 128
ipv6 prefix-list INVALIDAS_IPV6_IN seq 15 deny ::/8 le 128
ipv6 prefix-list INVALIDAS_IPV6_IN seq 20 deny FE00::/9 le 128
ipv6 prefix-list INVALIDAS_IPV6_IN seq 25 deny FF00::/8 le 128
ipv6 prefix-list INVALIDAS_IPV6_IN seq 30 deny FC00::/7 le 128
ipv6 prefix-list INVALIDAS_IPV6_IN seq 35 deny FE80::/10 le 128
ipv6 prefix-list INVALIDAS_IPV6_IN seq 40 permit 2000::/3 le 48
ipv6 prefix-list INVALIDAS_IPV6_IN seq 45 deny ::/0 le 128

Primero se configuró el prefix-list la cual por sí sola no hace nada, sino hasta que se aplique su operación en la sesión de eBGP hacia el proveedor correspondiente.

El siguiente diagrama ilustra los filtros aplicados en las interfaces de entrada.



1.2. Filtrado de rutas en BGP IPv4 de entrada y salida en los enlaces de internet local.

Esta configuración sólo se aplicó en los ruteadores de entidades remotas que cuentan con un acceso a Internet local, pues en estos casos no se solicita los ISP´s el envío de la tabla completa de enrutamiento a través del protocolo eBGP.

- Para el tráfico de entrada se aplicó el siguiente filtro para permitir únicamente la ruta por default.

  ip prefix-list DEFAULT_INTERNET_IN seq 5 permit 0.0.0.0/0

  Este *prefix-list* se aplica de entrada a la sesión de eBGP que se tenga con el ISP, con ello nos aseguramos que si el ISP comete un error y nos envía gran cantidad de prefijos, aún así solo permitimos que el router permita el ingreso de la ruta por default (***0.0.0.0/0***) para ser usada por el router en su tabla de enrutamiento.

- Comprobación: Se utilizó el comando "show ip route" para verificar que se recibe la ruta por default.

  B 0.0.0.0/0 [20/0]*

- Para el tráfico de salida se aplicaron los siguientes filtros para permitir las redes locales únicamente.

  ```
  ip prefix-list ENP1_INTERNET_TMX_OUT seq 5 permit prefijo_UNAM
  ```

  Con esta línea de configuración solamente se permite que se anuncie el o los segmentos de red asignados por NIC UNAM a la dependencia remota. Este *prefix-list* puede estar conformada por tantas líneas como segmentos de redes tenga asignada la entidad universitaria simplemente haya que ir agregando las líneas diferenciándose con un número de secuencia (*seq*).

  ```
  ip as-path access-list 5 permit ^$
  ```

  Con esta línea de as-path se configura la política de enrutamiento que permite solamente el envío de prefijos (anuncios de red) que inicie y finalice con el sistema autónomo que se esta configurando localmente, en este caso solamente el AS278 de la UNAM. Esta política se puede aplicar ya sea para anuncios de entrada o salida en la sesión de eBGP que se tenga con el ISP, en este caso se aplica para los anuncios de salida, pues solo permitiremos prefijos originados por el AS278 de la UNAM.

- Comprobación: Se utilizó el comando "*show ip bgp neighbor x.x.x.x advertised routes*" para verificar que se anuncian sólo las redes deseadas.

1.3. Filtrado de rutas en BGP IPv6 de entrada y salida en los enlaces de internet local.

Al igual que en IPv4, también se aplicó esta política en para los anuncios de prefijos en IPv6.

- Para el tráfico de entrada se aplicó el siguiente filtro para permitir únicamente la ruta por default.

```
ipv6 prefix-list DEFAULT_INTERNET_IN seq 5 permit ::/0
```

- Comprobación: Se utilizó el comando "show ipv6 route" para verificar que se recibe la ruta por default.

```
B   ::/0 [20/0]
```

- Para el tráfico de salida se aplicaron los siguientes filtros para permitir las redes locales únicamente.

```
ipv6 prefix-list INTERNET_OUT seq 5 permit prefijo_ipv6_UNAM
ip as-path access-list 5 permit ^$
```

- Comprobación: Se utilizó el comando "`show ip bgp ipv6 unicast neighbor x.x.x.x` advertised routes" para verificar que se anuncian sólo las redes deseadas.

La siguiente tabla muestra la cantidad de interfaces configuradas en toda la RedUNAM

	Routers Internet CU	Routers Internet Local
Routers configurados	5	67
Interfaces de internet configuradas	5	94

1. Acción Anti-spoofing

Esta acción es útil para prevenir tráfico con direcciones IP falsificadas que pudieran ocasionar daño en la infraestructura de una red. Se basa principalmente en filtrar direcciones IP que son usadas con fines de pruebas o que están reservadas por el organismo que las administra. Estas direcciones IP están documentadas en el RFC 8190[4].

[4] https://www.rfc-editor.org/info/rfc8190

Para completar esta acción, MANRS recomienda utilizar filtros de entrada y utilizar la arquitectura "Unicast Reverse Path Forwarding" (uRPF) que consiste en utilizar la "Forwarding Information Base" de cada dispositivo de red para decidir si el paquete es reenviado o filtrado.

En el caso de la RedUNAM, se implementaron las listas de acceso en los enlaces de internet en CU y en los enlaces de internet local. La arquitectura *uRPF* fue implementada en los enlaces LAN de las dependencias remotas fuera de CU, con el objetivo de evitar que direccionamientos no asignados a las redes LAN puedan tratar de comunicarse a través de la infraestructura de RedUNAM hacia otros servicios dentro de la RedUNAM o a Internet.

De acuerdo al RFC 8190, esta es la lista de acceso que fue configurada y aplicada en los enrutadores de RedUNAM.

Configuración y aplicación de lista de acceso (ACL)

FLTROS ANTI-SPOOF IPV4

```
ip access-list extended ANTI-SPOOF
 deny   ip 0.0.0.0 0.255.255.255 any
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 127.0.0.0 0.255.255.255 any
 deny   ip 169.254.0.0 0.0.255.255 any
 deny   ip 172.16.0.0 0.15.255.255 any
 deny   ip 192.0.0.0 0.0.0.255 any
 deny   ip 192.0.2.0 0.0.0.255 any
 deny   ip 192.88.99.0 0.0.0.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
 deny   ip 192.18.0.0 0.1.255.255 any
 deny   ip 192.51.100.0 0.0.0.255 any
 deny   ip 203.0.113.0 0.0.0.255 any
 deny   ip 224.0.0.0 15.255.255.255 any
 deny   ip 240.0.0.0 15.255.255.255 any
 deny   ip host 255.255.255.255 any
 permit ip any any
```

Una vez configurada, esta lista de acceso debe ser aplicada en el puerto de interconexión al proveedor de internet. El siguiente comando muestra un ejemplo de esta configuración:

```
interface TenGigabitEthernet0/0/1.13
    description INTERFACE a INTERNET LOCAL
    ip access-group ANTI-SPOOF in
    ipv6 traffic-filter ANTI-SPOOF_IPv6 in
```

Comando de verificación. Con el siguiente comando podemos observar la cantidad de paquetes que se están filtrando en ese puerto en específico.

```
#show access-lists ANTI-SPOOF
Extended IP access list ANTI-SPOOF
10 deny ip 0.0.0.0 0.255.255.255 any (540919 matches)
20 deny ip 10.0.0.0 0.255.255.255 any (9319845 matches)
```

Configuración y aplicación de uRPF. A continuación se muestra la configuración de uRPF aplicada en cada LAN, para ipv4 e IPv6.

```
interface GigabitEthernet0/0/3
description INTERFAZ de la RED LAN de la ENTIDAD
ip verify unicast source reachable-via rx
ipv6 verify unicast source reachable-via rx
```

Comandos de verificación. El siguiente comando sirve para verificar la operación de la arquitectura uRPF.

```
#show ip int GigabitEthernet0/0/3 | section IP verify source
IP verify source reachable-via RX
   5258299 verification drops
   0 suppressed verification drops
   9 verification drop-rate
```

La siguiente tabla muestra algunos números de las configuraciones realizadas.

	Internet CU	Internet Local	Red LAN
Routers configurados	5	67	120
Filtros configurados	5	94	120

2. Acción de coordinación

Esta acción facilita la comunicación global entre operadores de red mediante la publicación de datos de contacto, esto apoya a que mejore la comunicación y coordinación entre operadores de redes, procurando la reducción de tiempos en la atención de incidentes mediante la comunicación oportuna entre los administradores de la red.

En esta acción se realizó lo siguiente:

- **Registro en el sitio PeeringDB.** MANRS recomienda el registro de los datos de contactos técnicos para facilitar la comunicación con las diferentes organizaciones alrededor del mundo para contar con un medio de comunicación en caso de incidentes de seguridad.

- **Registro de datos en Lacnic**. El área del Centro de Información de RedUNAM (NIC UNAM) mantiene actualizado este registro con los datos técnicos y administrativos de la UNAM. Estos datos se pueden consultar en el IRR de la región www.lacnic.net y directamente en los siguientes enlaces:

  https://query.milacnic.lacnic.net/search?id=278
  https://query.milacnic.lacnic.net/irr

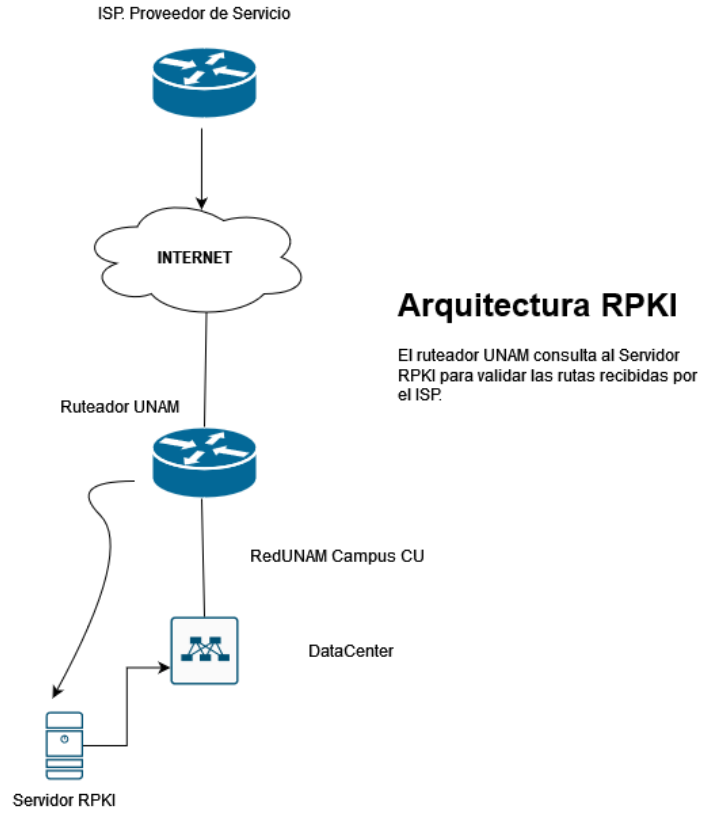
3. Acción de validación

Esta acción facilita la validación de información de ruteo a nivel global mediante el protocolo RPKI. Para cumplir con esta acción, se realizó lo siguiente:

- **Instalación y configuración de servidor RPKI (Resource Public Key Infrastructure).** RPKI es un método criptográfico para firmar registros que asocian un anuncio de prefijo con BGP con el número de Sistema Autónomo (AS) de origen correcto. RPKI se define en RFC6480[5].
- **Configuración del protocolo RPKI en los ruteadores del Campus de Ciudad Universitaria que proveen el acceso a internet**. Sólo se configuró en estos ruteadores debido a que son los únicos que reciben la tabla completa de enrutamiento de Internet por parte de los ISPs.

- **Actualización de los Route Origin Authorization (ROA)** por parte del NIC UNAM en el sitio web de LACNIC. Estos ROA (Route Origin Attestations) son objetos firmados digitalmente que describen una asociación entre un conjunto de prefijos (IPv4 o IPv6) y el sistema autónomo autorizado a originar esos prefijos en anuncios BGP.

Diagrama de funcionamiento



[5] https://www.rfc-editor.org/info/rfc6480

El servidor RPKI instalado en la RedUNAM se comunica con otros servidores del sistema de gestión RPKI para traer y validar criptográficamente los certificados y ROAs de los repositorios. Con esto se validan que los prefijos IPv4 e IPv6 pertenecen a los AS a los que dicen están registrados.

Los ruteadores que intercambian la información de enrutamiento a través del protocolo BGP, se comunican con el servidor RPKI local para validar esa información para validar que los anuncios que recibe por parte de su vecino sean válidas para utilizarlas dentro de su tabla de enrutamiento.

Comandos de configuración

Instalación del validador FORT.

1. **Descarga de paquete de instalación**
   `wget https://github.com/NICMx/FORT-validator/releases/download/1.5.3/fort-1.5.3-1.el8.x86_64.rpm`

El archivo de configuración estará en /etc/fort

2. **Instalación**

   ```
   rpm -i fort-1.5.3-1.el8.x86_64.rpm
   ```

   Si se trata de una actualización, ejecutar:
   ```
   rpm -U fort-1.5.3-1.el8.x86_64.rpm
   ```

3. **Configuración de archivos TAL**.
   Esto permitirá sincronizar la base de datos de prefijos para validar.

   ```
   fort --init-tals --tal=/etc/fort/tal
   ```

4. **Iniciar el proceso de Fort.**

   ```
   # systemctl start fort
   # systemctl status  fort
   # fort.service - FORT RPKI validator
   ```

Después de esto, aparecerá un log con lo siguiente:

First validation cycle has begun, wait until the next notification to connect your router(s)

Después de 10 minutos aparecerá lo siguiente:

First validation cycle has begun, wait until the next notification to connect your router(s)

Después de este mensaje ya será posible configurar el ruteador.

5. **En el ruteador de Campus UNAM**

   ```
   router bgp 278
   bgp rpki server tcp ip_router port 323 refresh 600
   ```

Comandos de verificación

```
#show ip bgp rpki tables
```

Mostrará todas las rutas que se reciben

```
#show ip bgp rpki servers
```

Mostrará la tabla de ruteo con las redes válidas e inválidas.

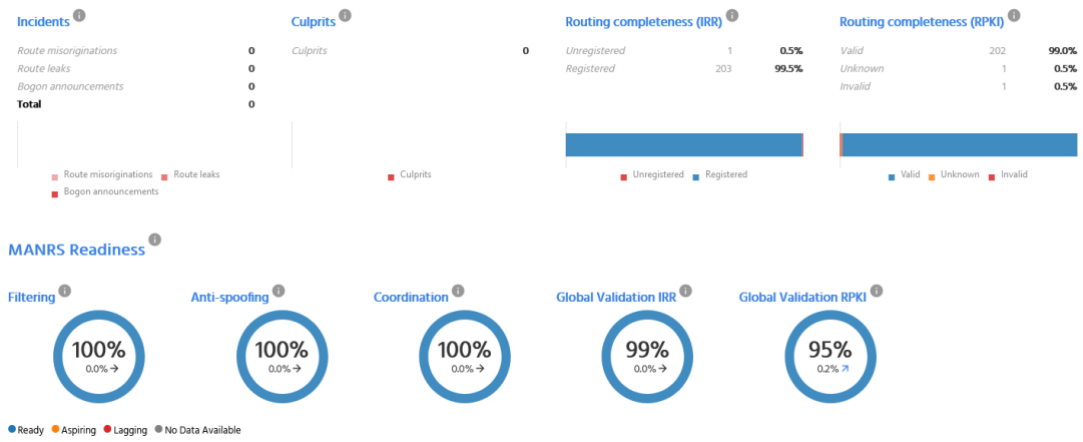
Comandos de *troubleshooting*

```
#no bgp rpki server tcp ip_router port 323 refresh 600
#clear ip bgp rpki
# systemctl stop fort
```

5. Observatorio MANRS

En el observatorio MANRS (https://observatory.manrs.org/), se puede ver el avance del cumplimiento de cada una de las acciones implementadas. El objetivo es llegar al cumplimiento del 100% de cada una de ellas y mantenerlas en ese estado durante la operación del día a día y en caso de algún requerimiento nuevo de las acciones a cumplir.

La siguiente gráfica, muestra el estado actual que la RedUNAM lleva en el cumplimiento de las 4 acciones de MANRS. Podemos observar que hay tareas pendientes en la acción de validación, las cuales ya estamos en proceso de solucionar para llegar al 100%.



Conclusión

Con la implementación de estas acciones, la UNAM colabora en el objetivo de conseguir un internet más seguro. El reto es mantener el cumplimiento de las mismas mediante una correcta operación de la arquitectura de RPKI y de la continua actualización de las reglas de filtrado y antispoofing.

Una de los beneficios a nivel personal es que el Lic. Carlos Alberto Vicente Altamirano ha sido invitado a diversos foros relacionados a MANRS para promover el programa y las experiencias de este proyecto.

Siendo la UNAM la Institución de Educación Superior Pública más grande e importante de México es necesario que difundamos la adopción de estas prácticas en beneficio de un internet más seguro para todos, por lo que podríamos difundir esta adopción con nuestros diferentes ISP´s para que adopten estas prácticas y juntos nos beneficiemos de estas mejoras.

Lecciones Aprendidas

- En un principio fue difícil encontrar cómo llevar a cabo estas configuraciones en los ruteadores y en el validador porque no existe mucha documentación. Tuvimos que buscar otras fuentes de documentación aparte de las oficiales, para llevar a cabo las configuraciones requeridas.

- Aprendimos que debemos aprovechar la experiencia de otros colegas por lo que acudimos directamente con los desarrolladores del validador para aclarar algunas dudas y nos acercamos a los foros de LACNIC y MANRS para recibir capacitación.

- La definición técnica de las configuraciones y los procedimientos para agregarlas a cada uno de los ruteadores facilitó la implementación en cada uno de los ruteadores que integran la RedUNAM.

- La organización de la información relacionada a cada uno de los ruteadores facilitó tanto la implementación como el control y seguimiento de cada unas de las acciones adoptadas pues dio visibilidad a cómo se desarrolló el proyecto hasta su finalización.

- El trabajo en equipo y colaborativo de los integrantes del NOC RedUNAM y diversas áreas de la Dirección de Telecomunicaciones fueron factor clave para el logro del objetivo.

- La definición de un área en específico como responsable de llevar a cabo el proyecto es clave, pues dio facilidades para la asignación de responsabilidades y actividades, la comunicación a nivel Dirección de Telecomunicaciones es importante para dar visibilidad a las iniciativas y proyectos que se tienen, con el objetivo de participar o colaborar con información, conocimientos o recursos que puedan ser útiles.

- Este proyecto llegó a su finalización exitosa, pero no hay que olvidar que se encuentra en operación y como tal deben definirse procesos de gestión y operación para mantener estas prácticas de MANRS actualizadas de acuerdo a las necesidades que surjan en el día a día.

Referencias.

Acción de filtrado en MANRS.
https://www.manrs.org/isps/guide/filtering/

RFC 8190. Direcciones IP reservadas.
https://datatracker.ietf.org/doc/html/rfc8190

Acción AntiSpoofing en MANRS
https://www.manrs.org/isps/guide/antispoofing/

Información validador FORT
https://fortproject.net/en/validator

Plataforma Cisco Devnet Sandbox
https://developer.cisco.com/site/sandbox/

Observatorio MANRS
https://observatory.manrs.org/#/overview

Integrantes del proyecto:

Lic. Carlos Alberto Vicente Altamirano
NOC RedUNAM
Coordinación de proyecto
Configuración de filtros y listas de acceso
Elaboración del reporte
Pruebas de validación FORT-Ruteadores
Configuración del servidor FORT

Ing. Lourdes Jiménez Ramírez
NOC RedUNAM
Configuración de buenas prácticas
Análisis de información de los RFC.

Marcial Martínez Quinto
NOC RedUNAM
Configuración de filtros y listas de acceso
Elaboración de plantilla de configuración

Lic. Alejandro Cruz
NIC UNAM
Instalación de servidor RPKI (FORT)
Registro de ROA´s
Registro PeeringDB

Mtro. Hugo Rivera Martínez
NOC RedUNAM
Supervisión del proyecto
Elaboración, colaboración y revisión del reporte