Resultados – Seguridad BGP en la Infraestructura de RENATA

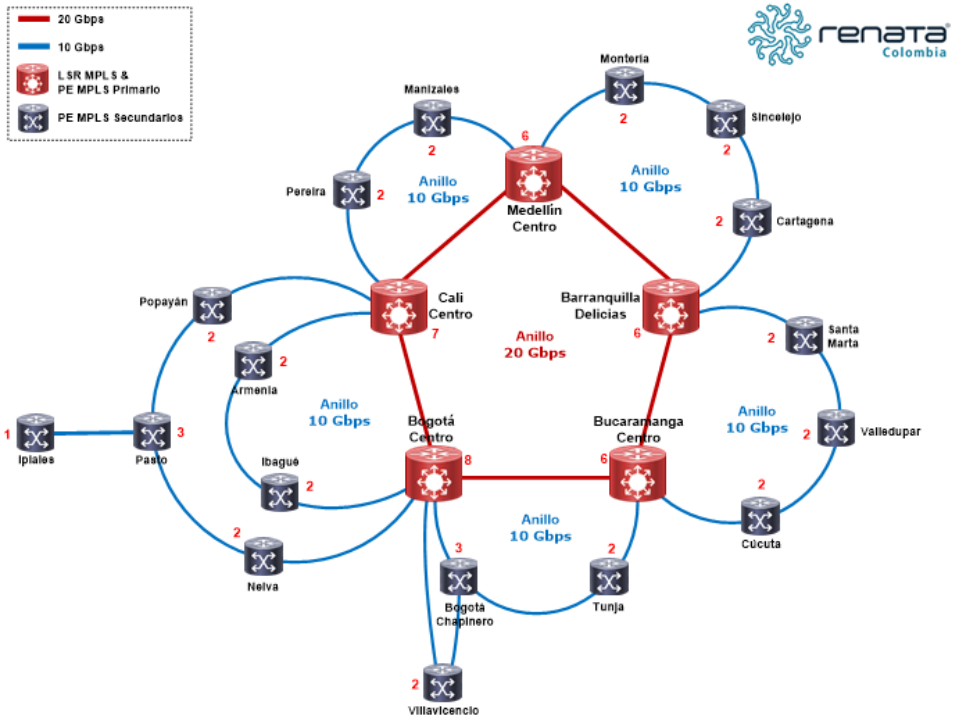
Erika Vega (erika.vega@renata.edu.co)
Coordinadora de Infraestructura y Servicios

renata Colombia

Contenido

Infraestructura de RENATA

- Red de transmisión de 19.000 km de fibra óptica a lo largo del territorio nacional.
- Backbone de 22 nodos, interconectado por lambdas de 100 Gbps.
- Red IP/MPLS basada en equipamiento Alcatel Lucent de última tecnología que soporta 100 Gbps, 200 Gbps, 400 Gbps y 1 Tbit/s.



Puntos de Interconexión

Red académica – CLARA

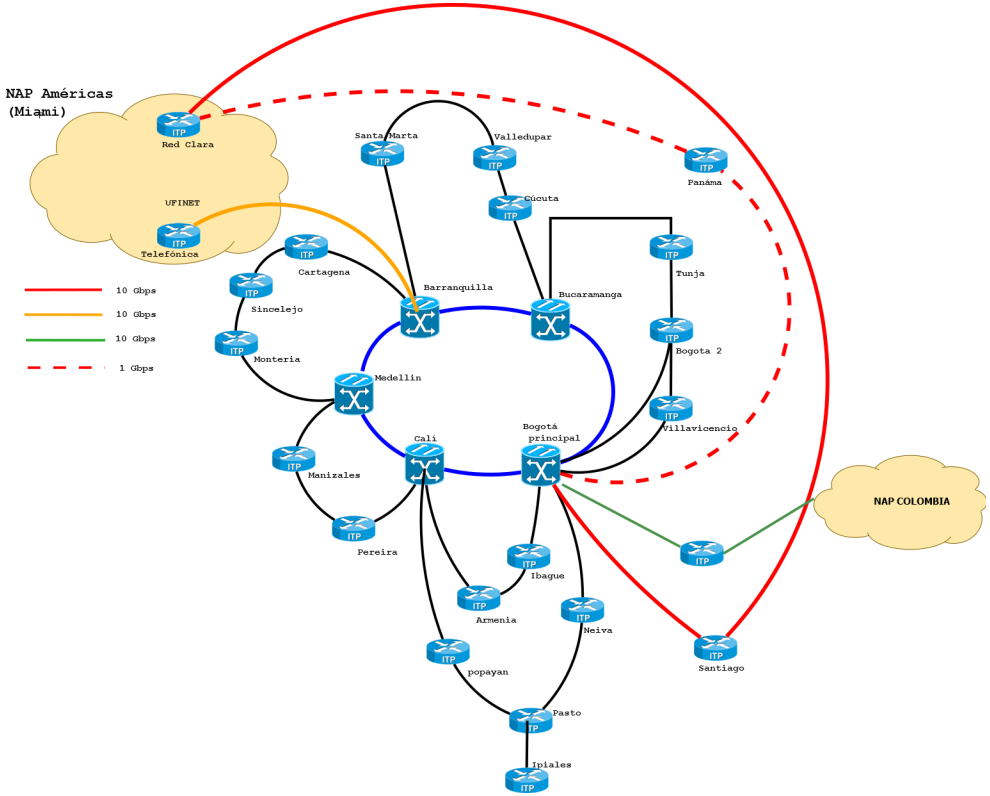
- 1 enlace de 1Gb Panama – Miami.
- 1 enlace de 10 Gb Santiago – Miami.

Acceso Internet

- 1 enlace de 10 Gb.

Salida NAP Colombia

- 1 enlace de 10 Gb.



Acerca del Proyecto

Este proyecto busca realizar validación en el origen de las rutas BGP en el backbone RENATA, que proporciona un servicio de interconexión al Sistema Nacional de Ciencia, Tecnología e Innovación (SNCTI) en Colombia y en todo el mundo.

El foco estará en los grandes puntos de intercambio en el nodo de Bogotá que facilita la conectividad con la Red CLARA y NAP, y en Barranquilla donde se provee conectividad a Internet. La implementación se realizará en el 100 % de los nodos.

Objetivos

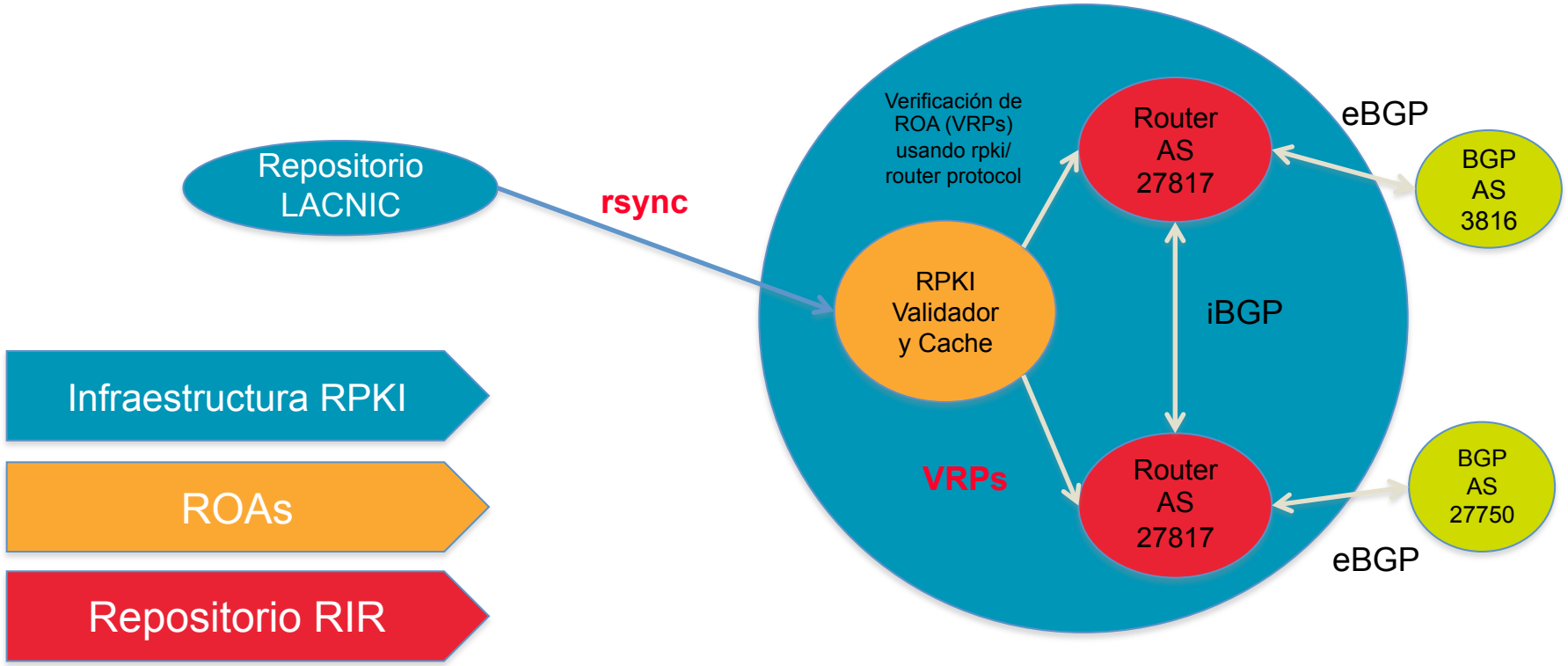
Al realizar la implementación de ésta tecnología a nivel de la red nacional, RENATA busca dar un importante paso hacia el aseguramiento de la infraestructura crítica de internet y las redes académicas además de tener la posibilidad de intercambiar el tráfico local de la red sin necesidad de realizar costosos enlaces internacionales y por último pero no menos importante nutrir a la comunidad académica e investigativa del país de resultados y experiencias de valor al adoptar nuevas prácticas.

Componentes Tecnológico

- El sistema tiene varias partes, tales como: Una infraestructura de clave pública para los recursos de Internet (RPKI), la utilidad de sincronización global (rsync) y los protocolos locales para la validación local en los nodos de enrutamiento de la red.

- Difundir información que se puede verificar independientemente de los paquetes BGP.

Proceso Técnico



Actividades

1. Comunicación y difusión del proyecto.
2. Sensibilización , capacitación y firma de recursos.
3. Pruebas y configuraciones iniciales.
4. Puesta en marcha en producción y correción de configuración.

Comunicación y Difusión

Se construyeron comunicados para ser dirigidos a los coordinadores técnicos de todas las instituciones conectadas a RENATA, en donde se les suministro la siguiente información:

- ¿Qué es RPKI?
- ¿Por qué es importante?
- ¿Por qué RENATA ésta trabajando en su implementación?
- Cuales son las ventajas de su implementación.
- Pasos a seguir para la implementación.

Sensibilización, Capacitación y Firma de Recursos

Como se hizo

Como primera parte , se realizaron dos seminarios teóricos y dos seminarios prácticos en modalidad virtual. Los seminarios contaron con los apoyos de Alvaro Retana, Gerardo Rada y Erika Vega.

Como segunda parte, se llevaron a cabo las capacitaciones presenciales a distintas instituciones conectadas a RENATA y a proveedores de servicios que hacen parte del NAP Colombia. La temática a tratar fue teoría y practica de RPKI, la firma de recursos de la instituciones participantes, la problemática de secuestro de rutas y la activación de la validación de origen en la infraestructura de RENATA.

Sensibilización, Capacitación y Firma de Recursos

Resultados

A un total de 328 profesionales de las distintas instituciones se le dio el proceso de sensibilización en los seminarios de modalidad virtual. En las capacitaciones en modalidad presencial el total de asistentes fue 69 de profesionales.

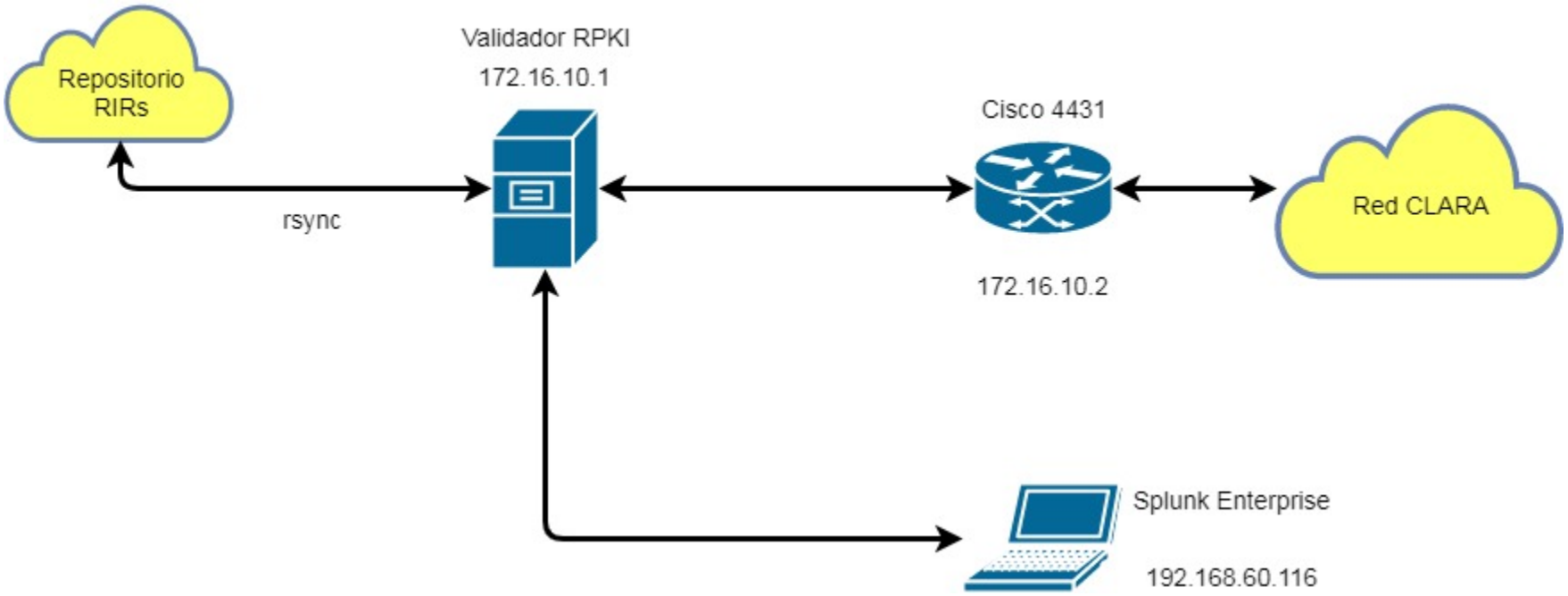
La solicitud para que Telefónica realizará la correspondiente firma de los 1109 recursos de su propiedad. La mayoría de estos 1109 recursos se encontraban en estado **NotFound**, y, posteriormente a la capacitación y entrega del manual para la creación de las ROAs, todos los estados de los 1109 se encuentran ahora es estado **Valid**.

Pruebas y Configuraciones Iniciales

Como se hizo

Se estudiaron los soportes en los dispositivos Cisco y Nokia para la validación de origen. De igual forma , se investigo del soporte al protocolo BMP en ambos dispositivos. Se estableció un escenario de pruebas donde se probaría el funcionamiento y la conectividad del Validador RPKI con el enrutador Cisco 4431. Además, en este escenario se hizo uso de un script que efectuaba la consulta con el Validador RPKI de todos los prefijos que transita por Red CLARA. Los datos obtenidos de dicha consulta fueron indexados en la herramienta de monitoreo llamada Splunk Enterprise, la cual nos suministraba la información de la cantidad de rutas **Valid**, **Invalid** y **NotFound** de una manera fácil de analizar. La instalación fue realizada en un servidor ubicado en las instalaciones de RENATA.

Topología


Repositorio
RIRs
rsync
Validador RPKI
172.16.10.1
Cisco 4431
172.16.10.2
Red CLARA
Splunk Enterprise
192.168.60.116

Pruebas y Configuraciones Iniciales

Resultados

Como resultados del escenario de pruebas, se corroboró el perfecto funcionamiento del Validador RPKI y la conexión establecida entre él y el dispositivo Cisco. Se validaron un total de 28713 prefijos que incluían rutas que tenían como destino Red Clara, NAP Colombia e Internet. Los porcentajes obtenidos se aprecian a continuación:

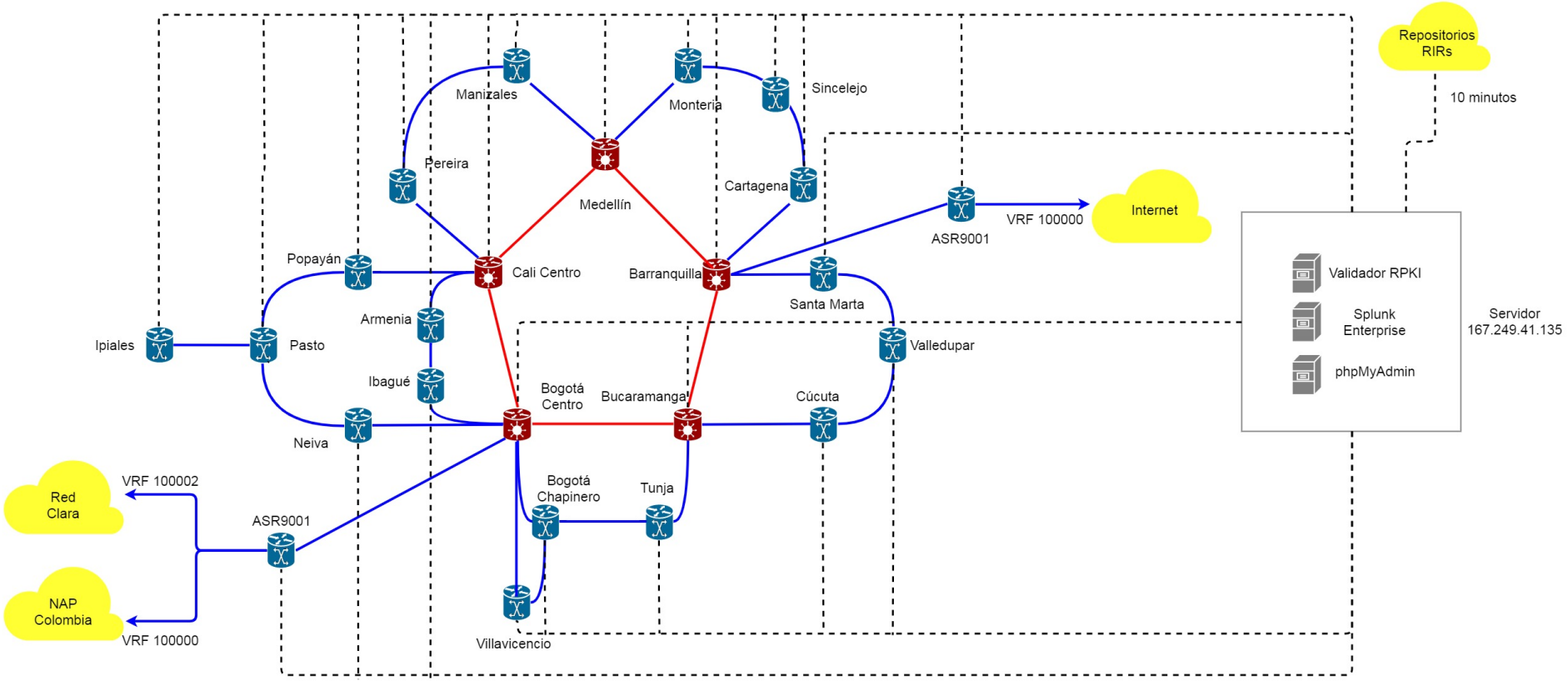
Valid	Invalid	Not Found
28.95%	3.55%	67.50%

Puesta en Marcha a Producción y Corrección de Configuración

Como se hizo

Posterior a los excelentes resultados obtenidos en el escenario de pruebas, se procedió a dar inicio al entorno de producción. Para ello se contrato un servidor alojado en un Virtual Data Center. En este VDC se instalo el servidor una distribución de Ubuntu como sistema operativo, posteriormente, se instalaron los paquetes necesarios para la puesta en marcha del servicio de validación. Los paquetes instalados fueron RIPE NCC RPKI Validator 2.23; como herramienta principal, Splunk Enterprise; como herramienta de monitoreo y reportes, y phpMyAdmin; como un gestor de bases de datos.

Topología


Repositorios RIRs
10 minutos
Manizales
Monteria
Sincelejo
Pereira
Medellín
Cartagena
ASR9001
VRF 100000
Internet
Popayán
Cali Centro
Barranquilla
Santa Marta
Armenia
Ipiales
Pasto
Valledupar
Ibagué
Bogotá Centro
Bucaramanga
Cúcuta
Neiva
Validador RPKI
Splunk Enterprise
phpMyAdmin
Servidor 167.249.41.135
Red Clara
VRF 100002
ASR9001
NAP Colombia
VRF 100000
Bogotá Chapinero
Tunja
Villavicencio

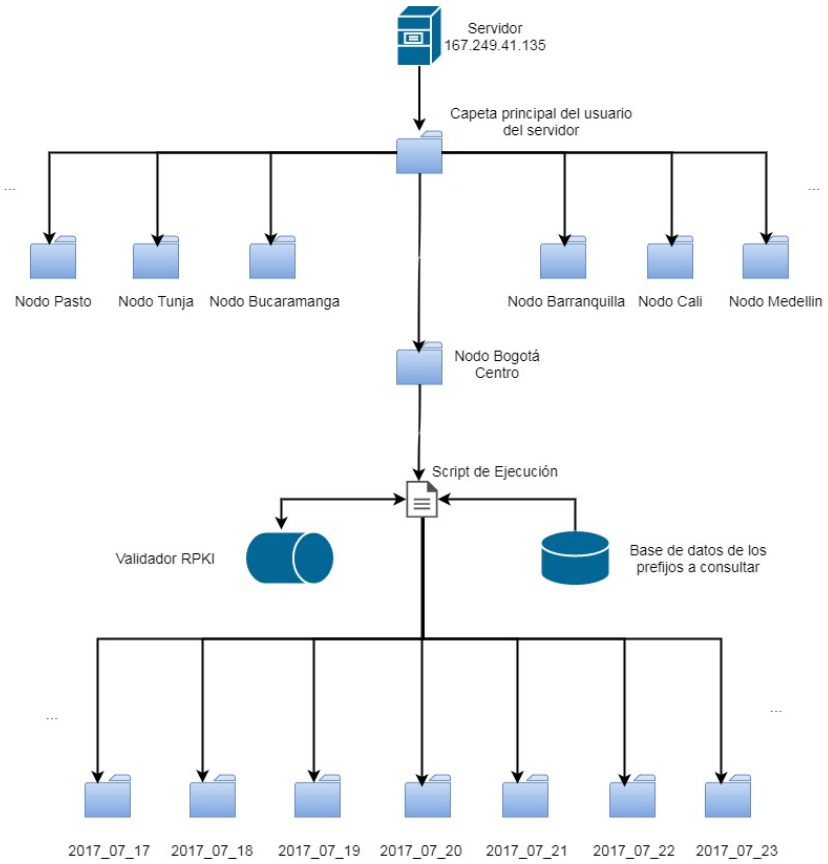
Puesta en Marcha a Producción y Corrección de Configuración

Como se hizo

Con la instalación del Validador RPKI y Splunk Enterprise, se efectuó la conexión entre los enrutadores ASR9001-Bogotá y ALU-Bogotá Centro con el Validador RPKI. Estableciendo entre ellos la comunicación y activando la validación de origen en ambos dispositivos.

Con la comunicación establecida se efectuó la ejecución del script diseñado para relaizar la consulta de los prefijos alojados en las VRFs de los dispositivos. La función del script es realizar una consulta a una base de datos donde están alojados los prefijos que transitan por RENTA y tomar cada prefijo con su respectivo AS y verificar su estado de validez con el Validador RPKI.

Esquema de ejecución del script



Puesta en Marcha a Producción y Corrección de Configuración

Como se hizo

La ejecución de script es de forma automática y los resultados del proceso de ejecución son para monitorear el porcentaje de los estados de validez de las rutas. Las rutas que se analizaron fueron las ubicadas en dos distintas VRFs presentes en los enrutadores de la infraestructura de RENATA. Dichas VRFS conteniente la siguiente cantidad de número de prefijos:

	VRF100000	**VRF100002**
Número de prefijos	14922	17912

Puesta en Marcha a Producción y Corrección de Configuración

Las VRF 100000 es donde están alojados los prefijos que tienen como destino NAP Colombia e Internet. Mientras tanto, la VRF 100002 es donde están alojados los prefijos con destino hacia NAP Colombia.

Fecha	Red Clara			NAP Colombia e Internet		
	Valid	Invalid	NotFound	Valid	Invalid	NotFound
16/08/17	5.828%	1.066%	93.104%	46.134%	2.453%	51.411%
17/08/17	5.828%	1.066%	93.104%	46.141%	2.467%	51.391%
18/08/17	5.828%	1.066%	93.104%	46.148%	2.460%	51.391%
19/08/17	5.828%	1.066%	93.104%	46.154%	2.453%	51.391%

Puesta en Marcha a Producción y Corrección de Configuración

Dato Importante

Se ha efectuado la activación de la validación de origen en los 24 nodos, pero debido a que la información de todas la rutas de BGP se conocen **NO** en el modo Global de BGP sino dentro de las VRF (address-family) fue necesario generar e instalar un parche sobre el sistema operativo de los equipos de la MPLS, logrando así activar la validación dentro del adress- family y así poder validar todas las rutas conocidas dentro de las VRF de la siguiente forma:

Puesta en Marcha a Producción y Corrección de Configuración

Configuración

```
router bgp 27817
rpki server 10.201.1.2
transport tcp port 8282
refresh-time 600
!
vrf 100000
address-family ipv4 unicast
bgp origin-as validation enable
bgp bestpath origin-as use validity
bgp bestpath origin-as allow invalid
```

VALIDACIÓN

```
sh bgp vrf 100000 origin-as validity
```

Puesta en Marcha a Producción y Corrección de Configuración

```
RP/0/RSP0/CPU0:RI-BOG-CEN-1#sh bgp vrf 100000 origin-as validity
Wed Sep 20 15:03:06.831 COL
BGP VRF 100000, state: Active
BGP Route Distinguisher: 27817:100000
VRF ID: 0x60000007
BGP router identifier 10.4.10.25, local AS number 27817
Non-stop routing is enabled
BGP table state: Active
Table ID: 0xe0000016   RD version: 14333781
BGP main routing table version 14333781
BGP NSR Initial initsync version 56445 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, r RIB-failure, S stale, N Nexthop-discard
Origin codes: i - IGP, e - EGP, ? - incomplete
Origin-AS validation codes: V valid, I invalid, N not-found, D disabled
    Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 27817:100000 (default for vrf 100000)
*>i0.0.0.0/0         10.4.10.23                100      0 3816 ?
*>i10.8.0.44/30      10.4.10.6                 100      0 i
*>i10.8.0.48/30      10.4.10.21                100      0 i
*>i10.8.0.72/30      10.4.10.10                100      0 i
*>i10.8.0.76/30      10.4.10.1                 100      0 i
*>i10.8.0.80/30      10.4.10.5                 100      0 i
*>i10.8.0.84/30      10.4.10.3                 100      0 i
*>i10.8.0.88/30      10.4.10.8                 100      0 i
*>i10.8.0.92/30      10.4.10.6                 100      0 i
*>i10.8.0.96/30      10.4.10.14                100      0 i
*>i10.8.0.100/30     10.4.10.5                 100      0 i
*>i10.8.0.112/30     10.4.10.19                100      0 i
*>i10.8.0.116/30     10.4.10.9                 100      0 i
*>i10.8.0.120/30     10.4.10.14                100      0 i
*>i10.8.0.124/30     10.4.10.20                100      0 i
*>i10.8.0.128/30     10.4.10.2                 100      0 i
*>i10.8.0.132/30     10.4.10.19                100      0 i
*>i10.8.0.136/30     10.4.10.1                 100      0 i
*>i10.8.0.152/30     10.4.10.14                100      0 i
*>i10.8.0.160/30     10.4.10.1                 100      0 i
*>i10.8.0.168/30     10.4.10.9                 100      0 i
*>i10.8.0.172/30     10.4.10.4                 100      0 i
*>i10.8.0.176/30     10.4.10.1                 100      0 i
*>i10.8.0.180/30     10.4.10.4                 100      0 i
```

Puesta en Marcha a Producción y Corrección de Configuración

Resultados

Lastimosamente esta configuración solo se pudo realizar en los dos puntos de interconexión debido a que el fabricante de los equipos que se encuentran en la MPLS no ha finalizado el desarrollo del parche necesario para el sistema operativo TiMOS.

Puesta en Marcha a Producción y Corrección de Configuración

Resultados

Se han efectuado reportes diarios desde la puesta en marcha de producción. De estos reportes, se obtuvo información sobre algunos cambios en los porcentajes que respectan a los estados de validez analizados en cada una de las VRFs. Los prefijos que hacen parte de la VRF 100000 (NAP Colombia e Internet) presentan algunos pequeños cambios, aumentando en un pequeño porcentaje de la rutas **Vallid** y disminuyendo las rutas **Invalid** y **NotFound**. No obstante, estos cambios son de un valor realmente irrelevante ya que no es un gran impacto en el resultado final. Sin embargo, estos pequeños cambios no ocurren en la VRF 100002 (Red CLARA). Los porcentajes no han presentado el más mínimo cambio. Esto muestra que sobre estas rutas en donde se debe realizar gran parte del proceso de concientización de la firma de sus correspondientes ROAs.

Reporte VRF 100000

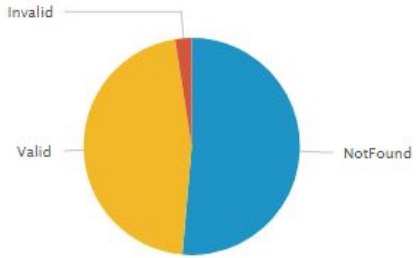
Porcentajes de los anuncios BGP del ALU-BOG - BAR (VRF 100000) - NAP Colombia e Internet comercial

Consultado el 16 de agosto

Estados de Validez	Cantidad de Anuncios	Porcentaje
NotFound	7668	51.411331
Valid	6881	46.134764
Invalid	366	2.453905

Gráfica de los anuncios BGP del ALU-BOG (VRF 100000) - NAP Colombia e Internet comercial

Consultado el 16 de agosto



Reporte VRF 100000

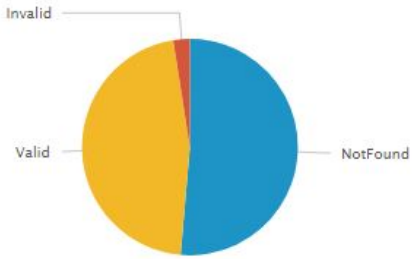
Porcentajes de los anuncios BGP del ALU-BOG - BAR (VRF 100000) - NAP Colombia e Internet comercial

Consultado el 17 de agosto

Estados de Validez	Cantidad de Anuncios	Porcentaje
NotFound	7665	51.391217
Valid	6882	46.141468
Invalid	368	2.467315

Gráfica de los anuncios BGP del ALU-BOG (VRF 100000) - NAP Colombia e Internet comercial

Consultado el 17 de agosto



Reporte VRF 100002

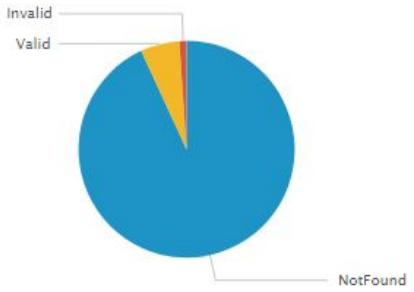
Porcentajes de los anuncios BGP del ASR9001-BOG (VRF 100002) - Red Clara

Consultado el 16 de agosto

Estados de Validez	Cantidad de Anuncios	Porcentaje
NotFound	16676	93.104796
Valid	1044	5.828820
Invalid	191	1.066384

Gráfica de los anuncios BGP del ASR9001-BOG (VRF 100002) - Red Clara

Consultado el 16 de agosto



Reporte VRF 100002

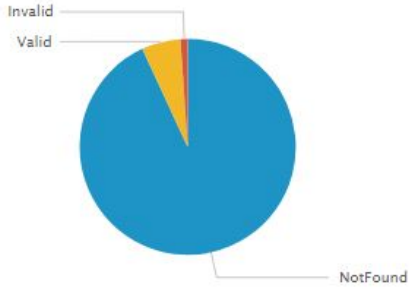
Porcentajes de los anuncios BGP del ASR9001-BOG (VRF 100002) - Red Clara

Consultado el 17 de agosto

Estados de Validez	Cantidad de Anuncios	Porcentaje
NotFound	16676	93.104796
Valid	1044	5.828820
Invalid	191	1.066384

Gráfica de los anuncios BGP del ASR9001-BOG (VRF 100002) - Red Clara

Consultado el 17 de agosto



Impacto e Innovación

- El proyecto propuesto es el primero del mundo en considerar la implementación de la validación de origen a nivel de una red con cobertura nacional.

- Lograr un paso importante hacia la seguridad de la infraestructura crítica de Internet y las redes académicas.

- Proporcionar nuevas prácticas a la comunidad académica y de investigación del país para obtener resultados y valorar experiencias.