NOKIA

BGP prefix origin validation with RPKI

Greg Hankins
<greg.hankins@nokia.com>
NANOG 67

SR OS support for BGP prefix origin validation with RPKI

- First released in SR OS* 12.0.R4 in July 2014
  - Several enhancements since the initial release
  - Supported for IPv4 and IPv6
  - RPKI servers can be configured in base router (in-band) or management router (out-of-band) contexts
  - Tested with rpki.net
- Standards
  - draft-ietf-sidr-origin-validation-signaling-04, *BGP Prefix Origin Validation State Extended Community*
  - RFC 6810, *The Resource Public Key Infrastructure (RPKI) to Router Protocol*
  - RFC 6811, *Prefix Origin Validation*

* TiMetra → Alcatel → Alcatel-Lucent → Nokia

SR OS support for BGP prefix origin validation with RPKI

- Supported platforms
  - 7450 Ethernet Service Switch (ESS)
  - 7750 Service Router (SR)
  - 7950 Extensible Routing System (XRS)
  - Virtualized Service Router (VSR)
  - Virtualized Mobile Gateway (VMG)
  - Network Services Platform (NSP)
- Product integration
  - 5620 Service Aware Manager (SAM)
  - Accessible via CLI, SNMP, NETCONF/YANG

Configure the RPKI session
Dynamic or static origin validation

```
A:br1-nyc>config>router>origin-validation# info detail
-----------------------------------------------
            rpki-session 192.168.1.1
                description "Test RPKI Server"
                no port
                no local-address
                no connect-retry
                no refresh-time
                no stale-time
                no shutdown
            exit
            static-entry 10.0.0.0/16 upto 24 origin-as 65001 valid
-----------------------------------------------
```

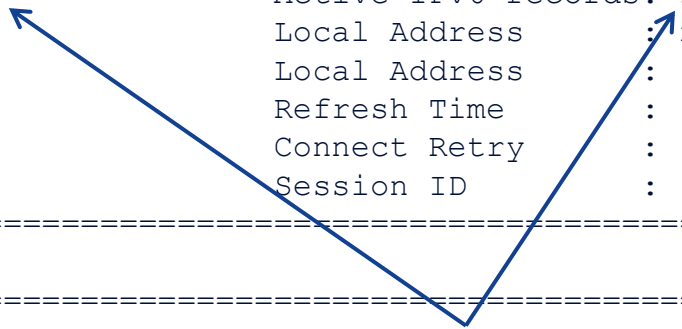
Dynamic RPKI server

Static valid/invalid origin

Show the RPKI session configuration

```
A:br1-nyc# show router origin-validation rpki-session detail

===============================================================================
Rpki Session Information
===============================================================================
IP Address          : 192.168.1.1
-------------------------------------------------------------------------------
Port                : 323                   Oper State          : established
UpTime              : 0d 00:57:41           Flaps               : 0
Active IPv4 records: 17023                  Active IPv6 records: 2515
Admin State         : Up                    Local Address       : n/a
Admin State         : Up                    Local Address       : 192.0.2.2
Hold Time           : 120                   Refresh Time        : 60
Stale Route Time    : 3600                  Connect Retry       : 120
Serial ID           : 41690                 Session ID          : 1452020198
===============================================================================
No. of Rpki-Sessions : 1
===============================================================================
```



Configure origin validation in BGP

```
A:br1-nyc>config>router>bgp# info
----------------------------------------------
            best-path-selection
                compare-origin-validation-state
                origin-invalid-unusable
            exit
            group "EBGP_PEERING"
                enable-origin-validation ipv4 ipv6
            exit
            no shutdown
----------------------------------------------
```

Enable origin validation in path selection: valid < notfound < invalid

Enable if you want to discard routes with an invalid origin

Enable in the BGP peer group for IPv4/IPv6

Configure origin validation in routing policies for IBGP peers
origin-validation-state <valid|notFound|invalid>

```
A:br1-nyc>config>router>policy-options# info
----------------------------------------------
            community "VRP_VALID_COMM" members "ext:4300:0"
            community "VRP_INVALID_COMM" members "ext:4300:2"
            community "VRP_NOT_FOUND_COMM" members "ext:4300:1"
            policy-statement "ORIGIN_POLICY"
                entry 10
                    from
                        origin-validation-state invalid
                    exit
                    action accept
                        community add "VRP_INVALID_COMM"
                        local-preference 90
                    exit
                exit
                entry 20
                    from
                        origin-validation-state notFound
                    exit
                    action accept
                        community add "VRP_NOT_FOUND_COMM"
                        local-preference 100
                    exit
                exit
                entry 30
                    from
                        origin-validation-state valid
                    exit
                    action accept
                        community add "VRP_VALID_COMM"
                        local-preference 110
                    exit
                exit
            exit
```

Origin validation state in routing policies, do different things for each state

Show the origin validation database
VRP (Validated ROA Payload)

```
A:br1-nyc# show router origin-validation database

===============================================================================
Static and Dynamic VRP Database Entries
===============================================================================
Prefix Range [Flags]                                          Origin AS
   Session IP [Flags]
-------------------------------------------------------------------------------
10.0.0.0/16-24 [Static-V]                                     65001
    -
172.16.0.0/12-12 [Dynamic]                                    65002
    192.168.1.1 [B]
-------------------------------------------------------------------------------
No. of Vrp Database Entries: 2
-------------------------------------------------------------------------------
Flags: B = Base instance session
       M = Management instance session
       Static-V = Static-Valid; Static-I = Static-Invalid
===============================================================================
A:br1-nyc# show router origin-validation database summary

===============================================================================
Static and Dynamic VRP Database Summary
===============================================================================
Type                                IPv4 Routes         IPv6 Routes
-------------------------------------------------------------------------------
192.168.1.1-B                       1                   0
Static                              1                   0
===============================================================================
```

Statically configured valid entry

Dynamic entry learned from server

Show the origin validation in BGP

```
*A:DUT>config>router# show router bgp routes 172.16.0.0/12 detail
[...]
Modified Attributes

Network        : 172.16.0.0/12
Route Source   : External
AS-Path        : 65002
Neighbor-AS    : 65002
Orig Validation: Valid
Source Class   : 0                          Dest Class     : 0
[...]
```

Valid, NotFound, Invalid, or
N/A (if not an IPv4 or IPv6 route)

NOKIA

Questions?

