Cisco's Origin Validation Implementation

Keyur Patel

Arjun Sreekantiah

Nanog 67, June, 2016, Chicago, USA

Code Availability

- CA Toolset

  Freeware (ISC/RPKI.NET)

- Cache Validator Software

  Freeware (ISC/RPKI.NET)

- Router Software

  Origin Validation (RPKI RTR & BGP Modifications) available in Cisco IOS and IOS-XR

  Cisco IOS code available in IOS XE-3.5.0/15.1(3)S

  Cisco IOS platforms targeted ASR1K, 7600, ME3600/ ME3800, ASR 903

  Cisco IOS-XR available in the XR-4.2.1

  Cisco IOS-XR platforms targeted CRS, C12K-XR, ASR9K

IOS Policy and Path Validation State

- Route-maps extended to modify policies based on path validation state
- Effective way of tweaking bestpath selection for IBGP paths
- IOS Route-map example:

```
route-map rpki-map permit 10
   match rpki invalid
set local-preference 50

route-map rpki-map permit 20
   match rpki valid
set local-preference 200
```

IOS Config Commands

```
router bgp 65536
 bgp router-id 192.0.2.1
 bgp log-neighbor-changes
 bgp rpki server tcp 10.0.96.254 port 32000 refresh 120
 neighbor 192.0.2.2 remote-as 64496
 neighbor 194.0.2.2 remote-as 64497
 neighbor 198.61.100.2 remote-as 65539
 neighbor 192.0.3.1 remote-as 65536
 !
 address-family ipv4
  neighbor 192.0.2.2 activate
  neighbor 194.0.2.2 activate
  neighbor 194.0.2.2 route-map rpki in
  neighbor 198.61.100.2 activate
  neighbor 192.0.3.1 activate
  neighbor 192.0.3.1 announce rpki state
exit-address-family
```

IOS Show Commands

```
Router-65536#show ip bgp
BGP table version is 8, local router ID is 192.0.2.1
Status codes: s suppressed, d damped, h history, * valid, > best,
              i - internal, r RIB-failure, S Stale, m multipath,
              b backup-path, f RT-Filter, x best-external,
             a additional-path,
              c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
V*>  192.0.2.128/25   192.0.2.2                0             0 64496 i
I*   192.0.2.129/32   198.61.100.2             0             0 65539 i
N*>  203.0.113.0      198.61.100.2             0             0 65539 i
Router-65536#
```

IOS Records (RPKI) Table


```
Router-65536#show ip bgp rpki table
1 BGP sovc network entries using 88 bytes of memory
1 BGP sovc record entries using 20 bytes of memory

Network                Maxlen  Origin-AS  Source  Neighbor
192.0.2.0/24           26      64496      0       10.0.96.254/32000

Router-65536#
```

IOS Show Commands – Valid Prefix

```
Router-65536#show ip bgp 192.0.2.128
BGP routing table entry for 192.0.2.128/25, version 2
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  64496
    192.0.2.2 from 192.0.2.2 (192.0.2.2)
      Origin IGP, metric 0, localpref 100, valid, external, best
      path 07AEE980 RPKI State valid
Router-65536#
```

IOS Show Commands – Invalid Prefix

```
Router-65536#show ip bgp 192.0.2.129
BGP routing table entry for 192.0.2.129/32, version 6
Paths: (1 available, no best path)
  Not advertised to any peer
  Refresh Epoch 1
  65539
    198.61.100.2 from 198.61.100.2 (198.61.100.2)
      Origin IGP, metric 0, localpref 100, valid, external
      path 07AEE8F0 RPKI State invalid
Router-65536#
```

IOS Show Commands – Incomplete Prefix

```
Router-65536#show ip bgp  203.0.113.0
BGP routing table entry for 203.0.113.0/24, version 8
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
     1
  Refresh Epoch 1
  65539
    198.61.100.2 from 198.61.100.2 (198.61.100.2)
      Origin IGP, metric 0, localpref 100, valid, external,
best
      path 07AEE938 RPKI State not found
Router-65536#
```

IOS-XR Policy and Path Validation State

- RPL extended to modify policies based on path validation state
- Effective way of tweaking bestpath selection for IBGP paths
- IOS-XR RPL example:

```
route-policy rpki
  if validation-state is invalid then
       set local-preference 50
  else if validation-state is valid then
       set local-preference 200
  else
       pass
  endif
end policy
```

IOS-XR Config Commands

```
router bgp 65536
 bgp router-id 192.0.2.1
 rpki cache 10.0.96.254
  transport tcp 32000
  refresh-time 120
 !
 address-family ipv4 unicast
  bgp origin-as validation signal ibgp
 neighbor 194.0.2.2
  remote-as 64437
   address-family ipv4 unicast
    route-policy rpki in
   ...
```

IOS-XR Show Commands

```
IOX#sh bgp origin-as validity
[snip]
 RPKI validation codes: V valid, I invalid, U unknown, d disabled, n
  not-applicable
     Network          Next Hop            Metric LocPrf Weight Path
V*>  192.0.2.128/25   192.0.0.2                0             0 64496 i
I*   192.0.2.129/25   198.61.100.2              0             0 65539 i
U*>  203.0.113.0/24   198.61.100.2              0             0 65539 ?
Processed 3 prefixes, 3 paths
```

IOS-XR Records (RPKI) Table


```
IOX#show bgp rpki table

  Network                Maxlen          Origin-AS          Cache
  67.21.36.0/24          24              3970                 147.28.0.11
  67.21.36.0/24          24              3970               * 198.180.150.1
  91.0.0.0/10            10              3320                 147.28.0.11
  91.0.32.0/20           20              33334444             147.28.0.11
  98.128.0.0/16          16              3130               * 198.180.150.1

* Source cache is down / ROAs are pending removal

 Processed 5 RPKI entries
```

IOS-XR Show Commands – Valid Prefix

```
PE1#show bgp 192.2.0.128/25
Mon May 16 02:07:31.702 PDT
BGP routing table entry for 192.2.0.128/25
Versions:
  Process              bRIB/RIB  SendTblVer
  Speaker                    23          23
Last Modified: May 15 14:22:54.000 for 11:44:38
Paths: (1 available, best #1)
  Advertised to peers (in unique update groups):
    40.0.0.2          50.0.0.2
  Path #1: Received by speaker 0
  64496
    192.0.2.2 from 192.0.2.2 (192.0.2.2)
      Origin IGP, localpref 100, valid, external, best, group-best
      Received Path ID 0, Local Path ID 1, version 23
      Origin-AS validity: valid
```

Cisco's Origin Validation Implementation

- Implementation of RPKI Router Protocol
- BGP changes needed for Origin Validation
- BGP Origin Validation State Extended Community

RPKI Router Protocol Implementation (RPKI RTR)

- Cisco IOS and IOS-XR supports router side implementation of RPKI RTR
- Cisco IOS release supports TCP as a transport
- Cisco IOS-XR release supports TCP & SSHv2 as a transport

BGP Modifications for Origin AS Validation

- Origin AS Validation support for IPv4 and IPv6 AFI
- {origin-as, prefix/min-max} information received via RPKI Router protocol is stored under a separate RPKI table

  Used towards validation of BGP announcements
- Changes to inbound processing of an update message

  Perform Origin Validation and set an appropriate path validation state on a path for a given prefix

  Apply any inbound policies if configured
- BGP Bestpath modified to incorporate path validation state comparison

BGP Modifications & Origin Validation State Extended Community

- Changes to the update generation for IBGP peers

  Outbound policies may use path validation state to manipulate different BGP attributes

  Announce path validation state using a well-known extended community defined in draft-ietf-sidr-origin-validation-signaling-08

Helps avoid re-computation of path validation state on a receiving IBGP speaker
Allows receiving IBGP speaker to compare path validation state of IBGP paths against EBGP paths