BGP RPKI met XR7 Cisco 8000 Whitepaper begrijpen

Inhoud

Inleiding

Dit document beschrijft de RPKI-functie (border Gateway Protocol) (BGP) voor Resource Public Key Infrastructure (RPKI) op het Cisco IOS® XR-platform.

Achtergrondinformatie

Voorwoord

Dit document bespreekt de BGP RPKI-functie en hoe deze BGP met routers beschermt tegen valse/kwaadaardige BGP-prefixupdates.

Reikwijdte

Dit document gebruikt Cisco 8000 met XR 7.3.1 release voor demonstratie. BGP RPKI is echter een platformonafhankelijke functie en de concepten die in dit document worden besproken, zijn van toepassing op andere Cisco-platforms (met Cisco IOS, Cisco IOS-XE .) met geschikte equivalente CLI-conversies. Dit document heeft geen betrekking op de procedure voor het toevoegen van routeoorsprongvergunningen (Route Origin Authorisations, ROA's) aan regionale internetregisters.

Voorwaarden

De lezer heeft kennis van het BGP-protocol nodig.

Vrijwaring

De in dit document gebruikte IP-adressen (Internet Protocol) zijn niet bedoeld als werkelijk adres. Om het even welke voorbeelden, output van de bevelvertoning, en cijfers inbegrepen in het document worden getoond voor illustratieve slechts doeleinden. Elk gebruik van actuele IP-adressen in illustratieve inhoud is onbedoeld en toevallig.

BGP-problemen als gevolg van slechte prefixadvertenties

BGP fungeert als de ruggengraat van het internetverkeer. Ook al is het de belangrijkste component van internet core, het heeft niet de mogelijkheid om te verifiëren of de indringende BGP-aankondiging afkomstig is van een geautoriseerd autonoom systeem of niet.

Deze beperking van BGP maakt het een gemakkelijke kandidaat voor verschillende soorten aanvallen. Een veelvoorkomende aanval wordt ‘route hijack’ genoemd. Deze aanval kan worden gebruikt om:

- Steal IP’s om spamresultaten te verzenden in IP wordt afgewezen en dus denial of service.
- Spion op verkeer om gevoelige informatie zoals wachtwoorden te verkrijgen.
- Verstoringen als gevolg van onjuiste configuraties door de beheerder.
- Beletten dat er verkeer wordt geleverd door valse servers op te zetten die ontkenning van de service veroorzaken.

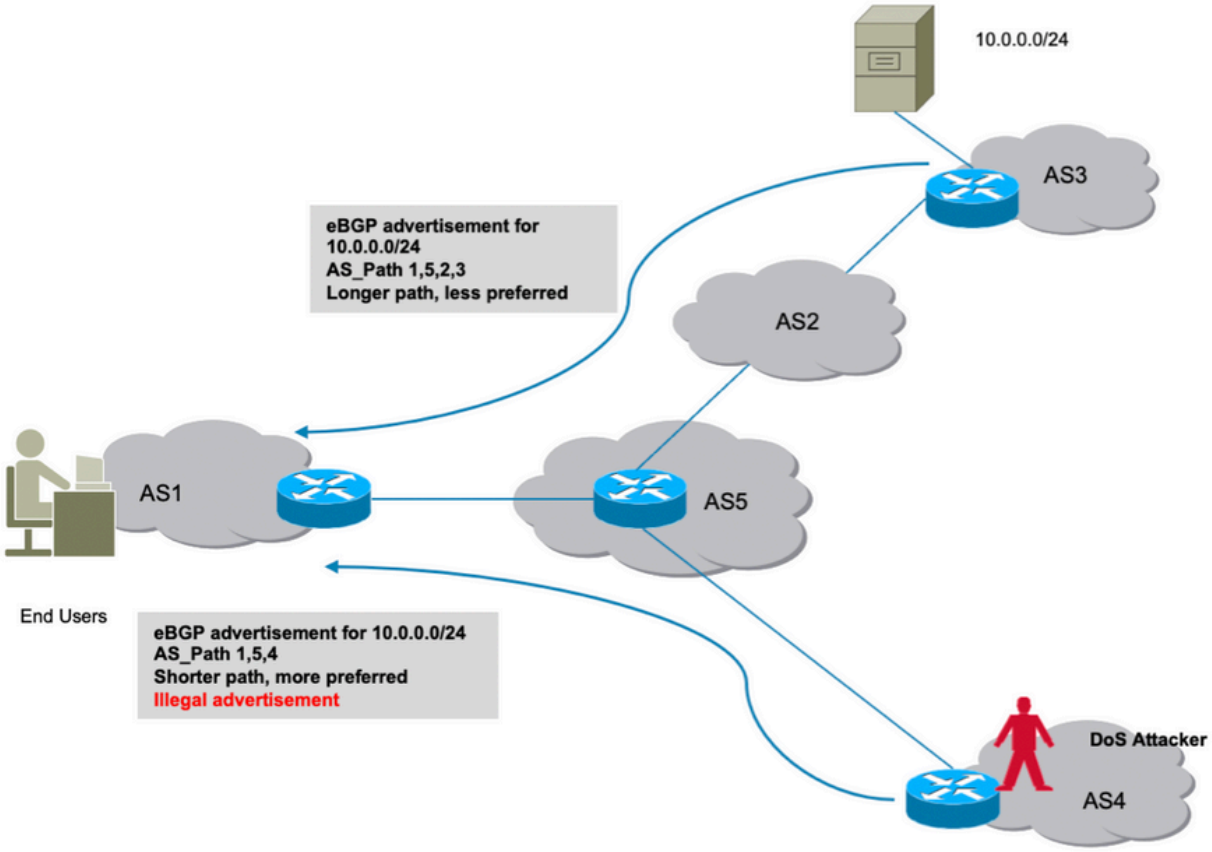
Denial of Service-aanval (algemeen bekend als DoS) is een kwaadaardige poging om het normale

verkeer naar een router, switch, server enzovoort te onderbreken. Er zijn verschillende DoS-aanvallen en er worden hier maar weinig besproken.

Routehijacking

Neem het scenario dat hier getoond wordt. Autonomous System 3 (AS3) stuurt juridische BGP-advertenties voor het voorvoegsel 10.0.0.0/24. Door het ontwerp van BGP is er niets in BGP dat een aanvaller ervan zou weerhouden hetzelfde voorvoegsel op het internet te adverteren.

Zoals getoond, adverteert de aanvaller in AS4 het zelfde prefix 10.0.0.0/24. BGP best path algoritme geeft de voorkeur aan een pad met kortere AS_Path. AS_Path 1,5,4 wint over een langer pad via AS 1,5,2,3. Daarom zal het verkeer van de cliënten nu aan het milieu van de aanvaller worden opnieuw gericht en kan zwart holed zijn die in ontkenning van de dienst aan eindcliënten voortvloeit.

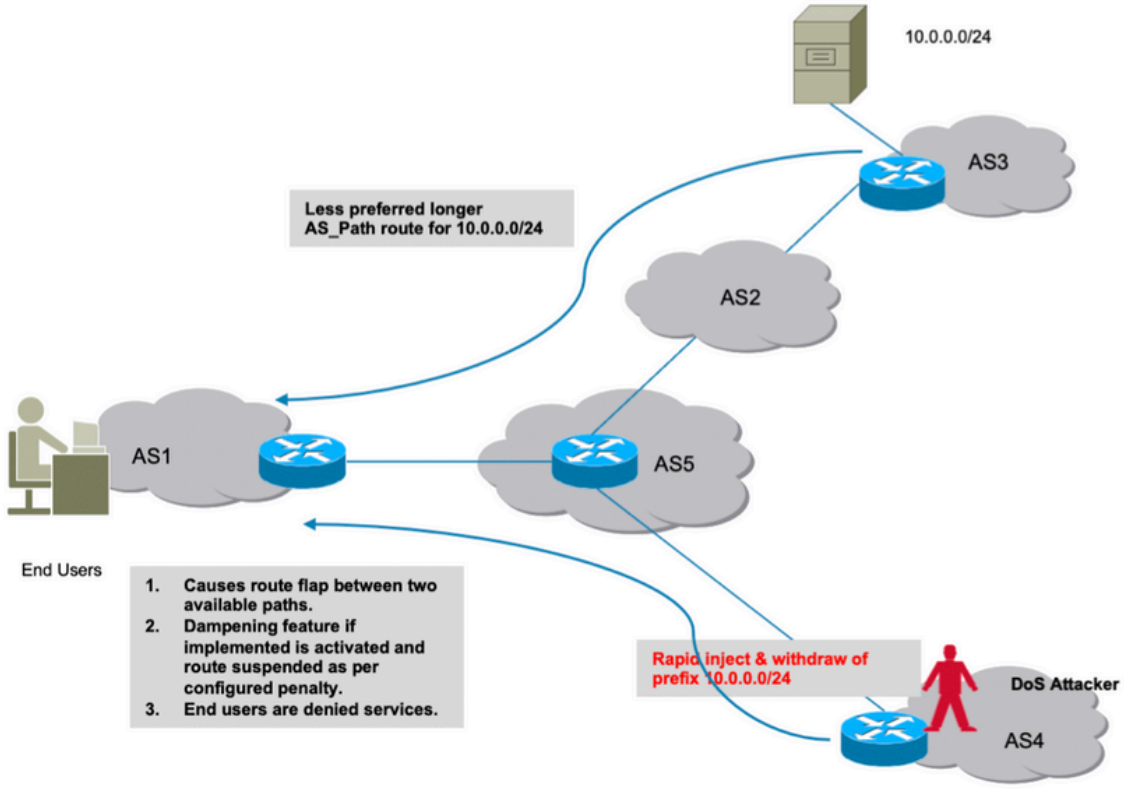


Routehijack

Verslechtering van systeemprestaties

In deze paragraaf wordt een andere manier besproken waarop diensten kunnen worden geweigerd. Als de BGP-routedempende functie van Cisco is geconfigureerd, kan deze worden benut als de hacker snelle routeflaps introduceert in het netwerk die een constante karnton veroorzaken.

De demping optie zal boetes opleggen aan de legitieme route en zal het niet beschikbaar maken voor het echte verkeer. Bovendien zal dit soort onethisch geïnduceerde flaps druk uitoefenen op de resources van de router zoals CPU, geheugen enzovoort.

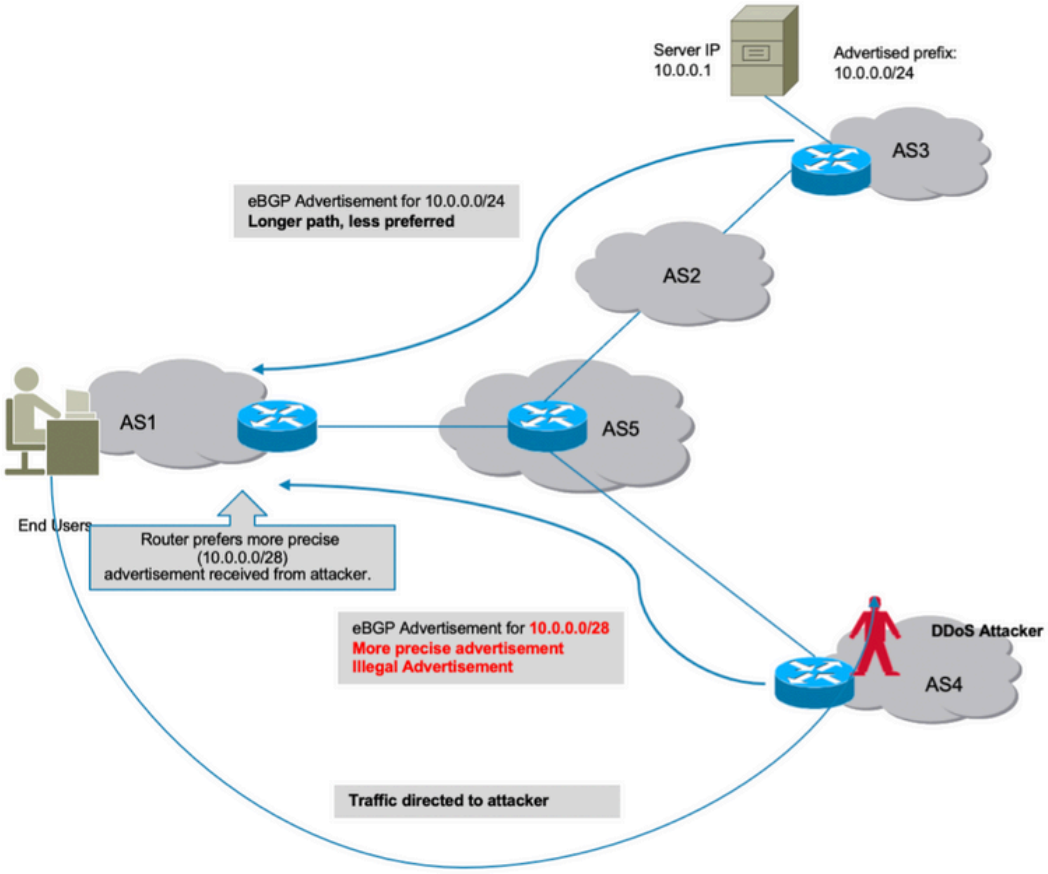


Routebeperking

Hijacking van het subprefix

Zoals besproken in de vorige sectie, hoe een aanvaller een prefix illegaal kan voortbrengen en een verstoring van verkeer veroorzaken. Helaas is een verstoring niet de enige reden tot zorg. In dergelijke aanvallen kunnen feitelijke gegevens worden gecompromitteerd, waarbij een aanvaller ontvangen gegevens kan scannen voor onethisch gebruik.

Evenzo zou het kapen van een route kunnen gebeuren door het illegaal adverteren van een preciezere route. BGP geeft de voorkeur aan prefixes die een langere match zijn en dit gedrag kan verkeerd worden uitgebuit zoals getoond in de afbeelding.



Hijack van subprefix

Alle aanvallen die worden besproken vloeien voort uit het feit dat BGP niet kon identificeren of de oorsprong AS van deze kwaadwillig geadverteerde prefixes geldig was of niet. Om dit op te lossen is een ‘ware’ en ‘vertrouwde’ bron van gegevens nodig die een router in zijn database kan bewaren. Vervolgens bij elke ontvangst van een nieuwe advertentie, wordt de router nu in staat om de AS-oorspronginformatie van het prefix die van BGP-peer wordt ontvangen, te verifiëren met zijn lokale databaseinformatie van de validator.

Aldus, kan de router de goede reclame van de slechte (illegale) degenen onderscheiden en het vermogen om alle eerder besproken aanvallen te vermijden wordt inherent toegevoegd op de router. BGP RPKI biedt de benodigde betrouwbare informatiebron.

RPKI

RPKI maakt gebruik van een repository die ROA’s bevat. Een ROA bevat informatie over het prefix en het bijbehorende BGP AS-nummer. De vergunning van de routeoorsprong is een cryptografisch ondertekende verklaring.

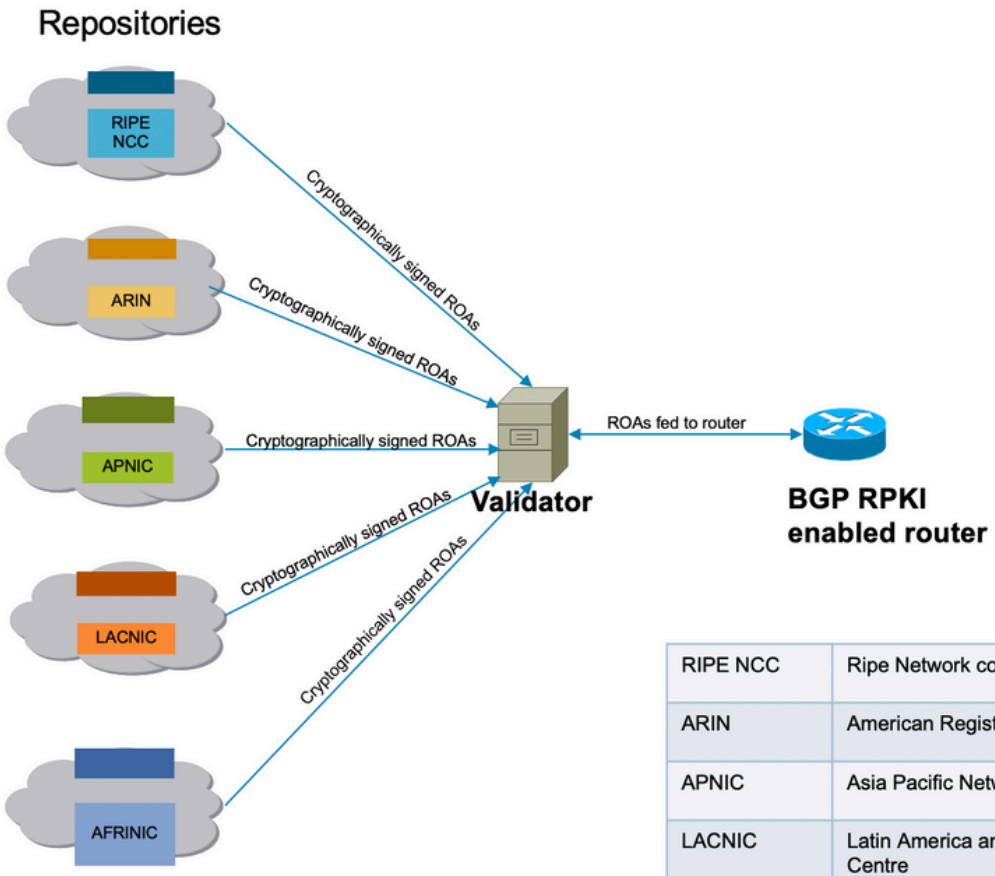
De 5 Regionale Internet Registries (RIR's) zijn de vertrouwensankers van de RPKI. Internet Assigned Numbers Authority (IANA) is de top van de boom die IP-prefixes uitdeelt. De RIR's volgen in de hiërarchie. Ze wijzen subprefixes toe aan Local Internet Registries (LIR's) en Large Internet Service Provider (ISP). Ze tekenen een certificaat voor deze prefixes. Het volgende niveau wijst subprefixes van deze toe en gebruikt de certificaten van hierboven om hun eigen certificaten te ondertekenen om hun eigen toewijzingen te certificeren. Zij gebruiken doorgaans hun eigen publicatiepunten om de certificaten en ROA's te hosten. Elk certificaat vermeldt de

publicatiepunten van de kindercertificaten die het ondertekent. Aldus, vormt RPKI een boom van certificaten die de boom van IP adrestoewijzingen weerspiegelt. De RPKI-validateurs die eigendom zijn van de vertrouwende partijen verzamelen alle publicatiepunten om bijgewerkte certificaten en ROA's (en CRL's en manifesten) te vinden. Ze beginnen bij de trust ankers en volgen de links naar de publicatiepunten van de kindcertificaten.

ROA's worden in de gegevensbank ingevoerd via RIR's, maar hetzelfde kan worden gedaan via andere registers (nationaal of lokaal). Deze verantwoordelijkheid kan ook worden gedelegeerd aan ISP's, met passend toezicht en verificatie door RIR's.

Op dit moment zijn er vijf ROA-repositories die worden beheerd door RIPE NCE, ARIN, APNIC, LACNIC en AFRINIC.

Een validator aanwezig in het netwerk communiceert met deze repositories en downloadt een vertrouwde ROA database om zijn cache te bouwen. Dit is een samengevoegde kopie van de RPKI, die periodiek direct of indirect van de mondiale RPKI wordt gehaald/vernieuwd. Validator geeft deze informatie vervolgens door aan de routers zodat ze de inkomende BGP-aankondigingen kunnen vergelijken met de RPKI-tabel om een veilig besluit te kunnen nemen.



RIPE NCC	Ripe Network coordination center
ARIN	American Registry for Internet Numbers
APNIC	Asia Pacific Network Information Centre
LACNIC	Latin America and Caribbean Network Information Centre
AFRINIC	African Network Information Centre

RPKI-infrastructuurconnectiviteit

Validator

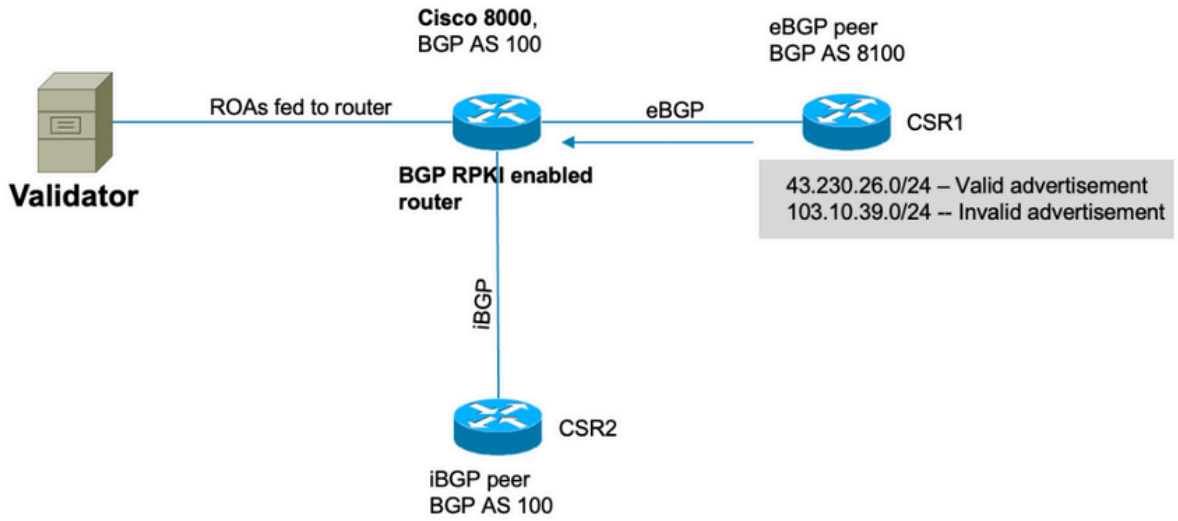
Deze demonstratie maakt gebruik van de RIPE-validator. De validator zal communiceren met de router door een TCP sessie te starten. In deze demonstratie luistert de validator naar zijn IP 192.168.122.120 en poort 3323.

```
routinator server --rtr 192.168.122.120:3323 --refresh=900
```

IANA heeft haven 3323 voor deze mededeling gespecificeerd. De verversen timer definieert het tijdsinterval waarna de lokale repository gesynchroniseerd en bijgewerkt zal worden om bij te blijven.

BGP RPKI-demonstratie

Topologie



Topologie

> **Opmerking**: Deze demonstratie gebruikt willekeurig Public AS-nummer en prefixes gewoon om BGP RPKI-mechanica uit te leggen. Publieke IP's worden gebruikt vanwege RPKI is voornamelijk bedoeld voor openbare prefixbescherming en alle ROA's die op RIR's zijn gemaakt, zijn openbare prefixes. Tot slot heeft geen van de acties, configuraties, enz. die in dit document worden beschreven, enige invloed op deze openbare IP's en AS's.

Configureren

```
router bgp 100

bgp router-id 10.1.1.1

rpki server 192.168.122.120

transport tcp port 3323

refresh-time 900
```

```
address-family ipv4 unicast
 !
 neighbor 10.0.12.2
 remote-as 8100
 address-family ipv4 unicast
  route-policy Pass in
  route-policy Pass out
 !
 !
 neighbor 10.0.13.3
 remote-as 100
 address-family ipv4 unicast
 !
 !
// ‘Pass’ is a permit all route-policy.
```

BGP RPKI-sessie

De router zet een TCP sessie met een validator (IP: 192.168.122.120, poort 3323) om het ROA cache te downloaden naar het geheugen van de router.

```
RP/0/RP0/CPU0:Cisco8000#show bgp rpki server 192.168.122.120
Wed Jan 20 22:54:15.763 UTC

RPKI Cache-Server 192.168.122.120
 Transport: TCP port 3323
 Bind source: (not configured)
 Connect state: ESTAB
 Conn attempts: 1
 Total byte RX: 4428792
 Total byte TX: 1400
 Last reset
   Timest: Jan 20 05:59:58 (16:54:17 ago)
   Reason: protocol error
```

ROA-downloads op router

Validator voert de informatie ROA aan de router in. Deze cache wordt periodiek ververst om de mogelijkheid van de router met verouderde informatie te minimaliseren. In deze demonstratie is een vernieuwende tijd van 900 seconden ingesteld. Zoals hier getoond, heeft Cisco 8000 router 172632 IPv4 en 28350 IPv6 ROA's gedownload van de validator.

```
RP/0/RP0/CPU0:Cisco8000#show bgp rpki server summary

Wed Jan 20 23:01:59.432 UTC

Hostname/Address        Transport       State           Time                ROAs (IPv4/IPv6)

192.168.122.120         TCP:3323        ESTAB           17:00:21        172632/28350

RP/0/RP0/CPU0:Cisco8000#show bgp rpki table ipv4

Wed Jan 20 23:09:26.899 UTC

>>>Snipped output<<<

 Network               Maxlen      Origin-AS         Server

 10.0.0.0/24            24              13335             192.168.122.120

 10.0.4.0/22            22              38803             192.168.122.120

 10.0.4.0/24            24              38803             192.168.122.120

 10.0.5.0/24            24              38803             192.168.122.120

 10.0.6.0/24            24              38803             192.168.122.120

 10.0.7.0/24            24              38803             192.168.122.120

 10.1.1.0/24            24              13335             192.168.122.120

 10.1.4.0/22            22              4134              192.168.122.120

 10.1.16.0/20           20              4134              192.168.122.120

 10.2.9.0/24            24              4134              192.168.122.120

 10.2.10.0/24           24              4134              192.168.122.120

 10.2.11.0/24           24              4134              192.168.122.120

 10.2.12.0/22           22              4134              192.168.122.120

 10.3.0.0/16            16              4134              192.168.122.120

 10.6.0.0/22            24              9583              192.168.122.120
```

Verifiëren

Deze sectie toont aan hoe BGP RPKI in actie en hoe het de router verhindert verkeerde/illegale

reclame.

Oorsprong-als-geldigheid inschakelen

Standaard haalt de router ROA's uit de validator, maar begint deze pas te gebruiken als de router hiervoor is geconfigureerd. Hierdoor worden deze voorvoegsels gemarkeerd als "D" of uitgeschakeld.

```
RP/0/RP0/CPU0:Cisco8000#show bgp origin-as validity

Wed Jan 20 23:27:37.268 UTC

BGP router identifier 10.1.1.1, local AS number 100

BGP generic scan interval 60 secs

Non-stop routing is enabled

BGP table state: Active

Table ID: 0xe0000000   RD version: 30

BGP main routing table version 30

BGP NSR Initial initsync version 2 (Reached)

BGP NSR/ISSU Sync-Group versions 0/0

BGP scan interval 60 secs


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

D*> 203.0.113.0/24     10.0.12.2                0             0 8100 ?

D*> 203.0.113.1/24     10.0.12.2                0             0 8100 ?

D*> 192.168.122.1/32   10.0.12.2                0             0 8100 ?
```

Activeer deze opdracht voor de betreffende adresfamilie om de router in te schakelen voor de controle van de geldigheid als-oorsprong.

```
router bgp 100

 address-family ipv4 unicast

 bgp origin-as validation enable

 !
```

Wanneer u dit bevel activeert, veroorzaakt het de router om de prefixes te scannen huidig in zijn

BGP- lijst tegen de ROA informatie die van validator wordt ontvangen en één van de drie staten wordt toegewezen aan prefixes.

```
RP/0/RP0/CPU0:Cisco8000#show bgp origin-as validity

Thu Jan 21 00:04:58.136 UTC

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

V*> 203.0.113.0/24     10.0.12.2                0             0 8100 ?

I*  203.0.113.1/24     10.0.12.2                0             0 8100 ?

N*> 192.168.122.1/32   10.0.12.2                0             0 8100 ?
```

Om de router in staat te stellen om de informatie over de prefixvalidatiestatus te gebruiken bij het berekenen van het beste pad, is deze opdracht nodig. Dit is standaard niet ingeschakeld omdat het u de mogelijkheid biedt om de validiteitsinformatie niet te gebruiken voor de beste padberekening, maar wel om deze te gebruiken in routebeleid dat later in dit document wordt besproken.

```
router bgp 100

 address-family ipv4 unicast

 bgp bestpath origin-as use validity

 !
```

Status Prefix-geldigheid

Er zijn drie toestanden waarin een voorvoegsel kan worden gevonden.

```
RP/0/RP0/CPU0:Cisco8000#show bgp origin-as validity

Thu Jan 21 00:04:58.136 UTC



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
```

```
V*> 203.0.113.0/24     10.0.12.2               0             0 8100 ?

I*  203.0.113.1/24     10.0.12.2               0             0 8100 ?

N*> 192.168.122.1/32   10.0.12.2               0             0 8100 ?
```

- Ongeldig - Geeft aan dat het prefix aan een van de volgende twee voorwaarden voldoet: 1. Het komt overeen met een of meer **Route Origin Authorisations** (ROAs), maar er is geen ROA match waar de oorsprong AS overeenkomt met de oorsprong AS op de AS-PATH. 2. Het komt overeen met een of meer ROA's op de in de ROA gespecificeerde minimumlengte, maar voor alle ROA's waar het overeenkomt met de minimumlengte, is het langer dan de gespecificeerde maximumlengte. Oorsprong AS is niet van belang voor voorwaarde #2.
- Geldig - Geeft het prefix en het AS-paar aan die in de RPKI-cachetabel staan.
- Niet gevonden - Geeft aan dat het prefix niet bestaat uit de geldige of ongeldige prefixes.

In deze sectie worden elk prefix en de status in detail besproken.

1. 203.0.113.0/24 - Geldig

eBGP-peer in AS 8100 heeft deze route gegenereerd en geadverteerd naar Cisco 8000 knooppunt. Aangezien de oorsprong AS (8100) overeenkomt met de oorsprong AS in ROA (ontvangen van validator), wordt deze prefix gemarkeerd als geldig en geïnstalleerd in de routertabel.

```
RP/0/RP0/CPU0:Cisco8000#show bgp rpki table | in "203.0.113.0|Max"

Thu Jan 21 00:21:26.026 UTC

 Network               Maxlen          Origin-AS         Server

 203.0.113.0/24                24       8100              192.168.122.120
```

De route is geïnstalleerd in de BGP-tabel.

```
RP/0/RP0/CPU0:Cisco8000#show bgp 203.0.113.0/24

Thu Jan 21 05:30:13.858 UTC

BGP routing table entry for 203.0.113.0/24

Versions:

 Process           bRIB/RIB  SendTblVer

 Speaker                 31          31

Last Modified: Jan 21 00:03:33.344 for 05:26:40

Paths: (1 available, best #1)

 Not advertised to any peer

 Path #1: Received by speaker 0

 Not advertised to any peer

 8100
```

```
   10.0.12.2 from 10.0.12.2 (192.168.122.105)

     Origin incomplete, metric 0, localpref 100, valid, external, best, group-best

     Received Path ID 0, Local Path ID 1, version 31

     Origin-AS validity: valid
```

Aangezien dit de beste BGP-prefix is en ook geldig per RPKI, wordt deze met succes geïnstalleerd in de routeringstabel.

```
RP/0/RP0/CPU0:Cisco8000#show route 203.0.113.0/24

Thu Jan 21 00:29:43.667 UTC



Routing entry for 203.0.113.0/24

 Known via "bgp 100", distance 20, metric 0

 Tag 8100, type external

 Installed Jan 21 00:03:33.731 for 00:26:10

 Routing Descriptor Blocks

   10.0.12.2, from 10.0.12.2, BGP external

     Route metric is 0

 No advertising protos.
```

2. 203.0.113.1/24 - Ongeldig

Dit prefix is ongeldig omdat er een conflict is in de oorsprong AS informatie in ROA en de oorsprong-als informatie die via BGP bericht van eBGP peer wordt ontvangen. 203.0.113.1/24 wordt ontvangen via BGP met oorsprong AS 8100.

```
RP/0/RP0/CPU0:Cisco8000#show bgp origin-as validity invalid

Thu Jan 21 00:34:38.171 UTC

BGP router identifier 10.1.1.1, local AS number 100

BGP generic scan interval 60 secs

Non-stop routing is enabled

BGP table state: Active

Table ID: 0xe0000000   RD version: 33

BGP main routing table version 33

BGP NSR Initial initsync version 2 (Reached)

BGP NSR/ISSU Sync-Group versions 0/0
```

```
BGP scan interval 60 secs


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

  Network            Next Hop            Metric LocPrf Weight Path

*  203.0.113.1/24     10.0.12.2                0             0 8100 ?
```

Het ROA dat van de validator is ontvangen, laat echter zien dat dit voorvoegsel tot AS 10021 behoort.

```
RP/0/RP0/CPU0:Cisco8000#show bgp rpki table 203.0.113.1/24 max 24

Thu Jan 21 00:37:05.615 UTC


RPKI ROA entry for 203.0.113.1/24-24

 Origin-AS: 10021 from 192.168.122.120

Version: 124211
```

Aangezien de AS oorspronginformatie in de ontvangen BGP aankondiging (AS 8100) niet overeenkwam met de daadwerkelijke AS oorsprong die in ROA (AS 10021) werd ontvangen, is het prefix gemarkeerd als Ongeldig en is niet geïnstalleerd in de routeringstabel.

```
RP/0/RP0/CPU0:Cisco8000#show bgp 203.0.113.1/24

Thu Jan 21 05:37:26.714 UTC

BGP routing table entry for 203.0.113.1/24

Versions:

 Process           bRIB/RIB  SendTblVer

 Speaker                 32          32

Last Modified: Jan 21 00:03:33.344 for 05:33:53

Paths: (1 available, no best path)

 Not advertised to any peer

 Path #1: Received by speaker 0

 Not advertised to any peer

 8100

   10.0.12.2 from 10.0.12.2 (192.168.122.105)

     Origin incomplete, metric 0, localpref 100, valid, external

     Received Path ID 0, Local Path ID 0, version 0

     Origin-AS validity: invalid
```

Bit is een 192.168.122.1/32 niet gevonden aanwezig in het ROA cache. BGP meldde dit voorvoegsel als ‘Niet gevonden’.

```
RP/0/RP0/CPU0:Cisco8000#show bgp 192.168.122.1/32

Thu Jan 21 05:44:39.861 UTC

BGP routing table entry for 192.168.122.1/32

Versions:

 Process           bRIB/RIB  SendTblVer

 Speaker                 33          33

Last Modified: Jan 21 00:03:33.344 for 05:41:06

Paths: (1 available, best #1)

 Not advertised to any peer

 Path #1: Received by speaker 0

 Not advertised to any peer

 8100

   10.0.12.2 from 10.0.12.2 (192.168.122.105)

     Origin incomplete, metric 0, localpref 100, valid, external, best, group-best

     Received Path ID 0, Local Path ID 1, version 33

     Origin-AS validity: not-found
```

Aangezien RPKI nog steeds wordt aangenomen, worden 'niet-gevonden' prefixes geïnstalleerd in de routeringstabel. Anders zal BGP ertoe bewegen deze legitieme prefixes te negeren die niet zijn geregistreerd in de RPKI database.

Ongeldig prefix toestaan

Hoewel dit niet wordt aanbevolen, geeft de software wel een knop om ongeldige prefixes toe te staan om deel te nemen aan het beste padberekeningsalgoritme.

```
router bgp 100

 address-family ipv4 unicast

 bgp bestpath origin-as allow invalid

 !
```

Met deze configuratie, beschouwt de router ongeldige prefixes voor beste wegberekening terwijl Dit duidelijk als "ongeldig". Deze uitvoer toont '203.0.113.1/24' als het beste pad.

```
RP/0/RP0/CPU0:Cisco8000#show bgp

Thu Jan 21 06:21:34.294 UTC

BGP router identifier 10.1.1.1, local AS number 100
```

```
BGP generic scan interval 60 secs

Non-stop routing is enabled

BGP table state: Active

Table ID: 0xe0000000   RD version: 34

BGP main routing table version 34

BGP NSR Initial initsync version 2 (Reached)

BGP NSR/ISSU Sync-Group versions 0/0

BGP scan interval 60 secs



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

  Network            Next Hop            Metric LocPrf Weight Path

*> 203.0.113.0/24     10.0.12.2                0             0 8100 ?

*> 203.0.113.1/24     10.0.12.2                0             0 8100 ?

*> 192.168.122.1/32   10.0.12.2                0             0 8100 ?
```

Zoals in deze output wordt getoond, wordt het prefix gemarkeerd als best ondanks gehouden ongeldig.

```
RP/0/RP0/CPU0:Cisco8000#show bgp 203.0.113.1/24

Thu Jan 21 06:23:26.994 UTC

BGP routing table entry for 203.0.113.1/24

Versions:

 Process           bRIB/RIB  SendTblVer

 Speaker                 34          34

Last Modified: Jan 21 06:05:31.344 for 00:17:55

Paths: (1 available, best #1)

 Not advertised to any peer

 Path #1: Received by speaker 0

 Not advertised to any peer

 8100

   10.0.12.2 from 10.0.12.2 (192.168.122.105)

     Origin incomplete, metric 0, localpref 100, valid, external, best, group-best
```

```
    Received Path ID 0, Local Path ID 1, version 34

    Origin-AS validity: invalid
```

Opgemerkt moet worden dat een router nog steeds een ongeldig voorvoegsel als laatste optie behandelt en altijd de voorkeur geeft aan een geldig voorvoegsel boven een ongeldig voorvoegsel als dit beschikbaar is.

Handmatige ROA-configuratie op router

Als om de een of andere reden een ROA voor een bepaald prefix nog niet is gemaakt, ontvangen of vertraagd, kan een handmatige ROA worden geconfigureerd op de router. Bijvoorbeeld, het prefix ‘192.168.122.1/32’ wordt gemarkeerd als ‘Niet gevonden’ zoals hier wordt getoond.

```
RP/0/RP0/CPU0:Cisco8000#show bgp origin-as validity

Thu Jan 21 06:36:31.041 UTC

BGP router identifier 10.1.1.1, local AS number 100

BGP generic scan interval 60 secs

Non-stop routing is enabled

BGP table state: Active

Table ID: 0xe0000000   RD version: 34

BGP main routing table version 34

BGP NSR Initial initsync version 2 (Reached)

BGP NSR/ISSU Sync-Group versions 0/0

BGP scan interval 60 secs



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

V*> 203.0.113.0/24     10.0.12.2                0             0 8100 ?

I*> 203.0.113.1/24     10.0.12.2                0             0 8100 ?

N*> 192.168.122.1/32   10.0.12.2                0             0 8100 ?
```

Een handmatige ROA kan worden geconfigureerd zoals hier wordt getoond. Dit commando associeert het prefix ‘192.168.122.1/32’ met AS 8100.

```
router bgp 100

 rpki route 192.168.122.1/32 max 32 origin 8100
```

Bij deze configuratie verandert de status van het prefix van "N" in "V".

```
RP/0/RP0/CPU0:Cisco8000#show bgp origin-as validity

Thu Jan 21 06:36:34.151 UTC

BGP router identifier 10.1.1.1, local AS number 100

BGP generic scan interval 60 secs

Non-stop routing is enabled

BGP table state: Active

Table ID: 0xe0000000   RD version: 35

BGP main routing table version 35

BGP NSR Initial initsync version 2 (Reached)



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

V*> 203.0.113.0/24     10.0.12.2                0             0 8100 ?

I*> 203.0.113.1/24     10.0.12.2                0             0 8100 ?

V*> 192.168.122.1/32   10.0.12.2                0             0 8100 ?
```

Routebeleid en status van prefix-validatie

De staatsresultaat van het prefix kan worden gebruikt om routebeleid te maken. Deze staten kunnen in een matchverklaring worden gebruikt en de beheerder gewenste acties kan worden gevoerd. Dit voorbeeld past alle prefixes met een ongeldige staat aan en stelt een gewichtswaarde van 12345 voor hen in.

```
route-policy Invalid

 if validation-state is invalid then

   set weight 12345

 endif

end-policy
```

```
!



router bgp 100
 remote-as 8100
 address-family ipv4 unicast
  route-policy Invalid in
 !
 !
!
```

Deze output toont een ongeldig prefix toegepast gewicht van 12345.

```
RP/0/RP0/CPU0:Cisco8000#show bgp 203.0.113.1/24
Thu Jan 21 06:57:33.816 UTC
BGP routing table entry for 203.0.113.1/24
Versions:
 Process           bRIB/RIB  SendTblVer
 Speaker                 38          38
Last Modified: Jan 21 06:54:04.344 for 00:03:29
Paths: (1 available, best #1)
 Not advertised to any peer
 Path #1: Received by speaker 0
 Not advertised to any peer
 8100
   10.0.12.2 from 10.0.12.2 (192.168.122.105)
     Origin incomplete, metric 0, localpref 100, weight 12345, valid, external, best, group-best
     Received Path ID 0, Local Path ID 1, version 38
     Origin-AS validity: invalid
```

Informatie over validatie van voorvoegsel delen via uitgebreide community

Omdat BGP-router de prefix-validatiestatus ook kan delen met andere routers (zonder lokaal cache van validator) via BGP-uitgebreide community. Dit bespaart de overheadkosten van elke router in het netwerk met een sessie met de validator en het downloaden van alle ROA's.

Dit wordt mogelijk gemaakt door de BGP uitgebreide gemeenschap.

Met deze opdracht kan de router informatie over prefixvalidatie delen met iBGP-peers.

```
router bgp 100

 address-family ipv4 unicast

 bgp origin-as validation signal ibgp
```

Zodra Cisco 8000 router is geconfigureerd zoals aangegeven, sluiten BGP-updates voor peers informatie voor prefixvalidatie in. In dit geval is de buurrouter iBGP een IOS-XE router.

```
csr2#show ip bgp 203.0.113.1/24

BGP routing table entry for 203.0.113.1/24, version 14

Paths: (1 available, best #1, table default)

 Not advertised to any peer

 Refresh Epoch 1

 8100

   10.0.12.2 from 10.0.13.1 (10.1.1.1)

     Origin IGP, metric 0, localpref 100, valid, internal, best

     Extended Community: 0x4300:0:2

     rx pathid: 0, tx pathid: 0x0

     Updated on Jan 21 2021 18:16:56 UTC
```

Deze uitgebreide community-mapping kan worden begrepen met het gebruik van 0x4300 0x000 (4 bytes die de status aangeven).

De vier bytes die op staat wijzen worden behandeld als een niet ondertekend geheel met 32 bits die één van de waarden hebben:

- 0 - geldig
- 1 - Niet gevonden
- 2 - Ongeldig

Prefix 203.0.113.1/24's community is 0x4300:0:2, wat overeenkomt met het 'Ongeldige' prefix. Op deze manier kan de csr2 router, ondanks dat er geen lokaal cachegeheugen beschikbaar is, nog steeds beslissingen nemen op basis van prefix-validatiestatus.

De validatiestatus van de prefix kan nu worden gebruikt om aan te passen in een routekaart of in het BGP-algoritme voor het beste pad.

Aanbevelingen voor BGP RPKI-implementatie

Goede praktijken voor ROA Creation

Dit zijn enkele aanbevelingen gebaseerd op onbereikbare netwerken waargenomen op RPKI-Observatory. Het RPKI-observatorium analyseert meerdere aspecten van het gebruikte RPKI-landschap.

- Als er voor een prefix een ROA is gemaakt, wordt het aanbevolen om dat prefix aan te kondigen in BGP. Bij gebrek daaraan kan iemand het aankondigen door gewoon te doen alsof ASN in dat ROA zit en het voorvoegsel te gebruiken.
- Als ROA is gemaakt met een maxlen groter dan de prefixlengte, dan is het gelijk aan het maken van ROA's voor alle mogelijke prefixes onder het originele prefix tot aan het maxlen. Het is sterk aanbevolen om al die prefixes in BGP aan te kondigen.
- Als een ROA is gemaakt voor een prefix en de prefixeigenaar een subprefix van het originele prefix aankondigt, dan maakt de ROA dat subprefix ongeldig. Een ROA voor het subprefix of het maximum van het oorspronkelijke ROA moet worden uitgebreid tot het subprefix.
- Als een organisatie een prefix bezit, maar van plan is dit niet aan te kondigen in BGP, dan moet er een ROA voor het prefix voor AS0 gecreëerd worden. Dit maakt elke aankondiging van het prefix ongeldig omdat AS0 niet in een AS-pad kan verschijnen.
- Als er meerdere ASN's zijn die hetzelfde prefix hebben, dan moeten ROA's voor dat prefix gemaakt worden voor elk van de ASN's. Bijgevolg, als een router meerdere ROA's heeft voor hetzelfde prefix, zal een BGP-advertentie die een van hen aanpast geldig zijn. Meervoudige ROA's voor hetzelfde prefix botsen niet met elkaar.
- Indien "A" een prefix voor zijn klant "B" heeft en namens "B" een ROA voor dat prefix creëert, dan moet "A" voor "B" ASN aan de aankondiging voorafgaan of moet "B" het prefix zelf laten ontstaan.

Prestatie-impact van RPKI op XR BGP-routers

Effect van ROA Update op CPU met routebeleid

Wanneer ROAs wordt bijgewerkt en als de router een lokaal ingangsroute-beleid voor een buur heeft die een "bevestiging-staat is" bevat, dan wordt het belangrijk om de status van prefixes opnieuw te valideren die op nieuwe bijgewerkte ROAs wordt gebaseerd. Dit wordt bereikt door de router die een BGP REFresh-verzoek naar zijn peer verzendt.

Wanneer BGP-buren dit bericht ontvangen zoals wordt getoond, verzenden buren hun prefixes opnieuw en kan het inkomende routebeleid de inkomende prefixes opnieuw valideren.

```
Jan 22 18:28:41.360: BGP: 10.0.12.1 rcv message type 5, length (excl. header) 4

Jan 22 18:28:41.360: BGP: 10.0.12.1 rcvd REFRESH_REQ for afi/safi: 1/1, refresh code is 0
```

Het probleem wordt nog groter wanneer veel buren zich tegelijkertijd vernieuwen wanneer ROA's worden bijgewerkt. Als buurland inkomende route-beleid complex zijn en veel verwerking vereisen, dan hoge CPU resultaten voor een paar minuten na een ROA update. Deze REFresh berichten komen niet voor als het buurland inkomende route-beleid geen "bevestiging-staat"bevel bevat is.

Als "soft-reConfiguration inbound altijd" is geconfigureerd voor een buur, dan worden er geen BGP REFresh-berichten verzonden, maar wordt hetzelfde routebeleid nog steeds uitgevoerd met dezelfde snelheid en kan hetzelfde CPU-gebruik worden verwacht.

Om de in punt 6.2.2 uiteengezette redenen wordt aanbevolen de voorkeur te geven aan de "bgp bestpath origine-as use validity"-benadering boven het configureren van een routebeleid.

CPU-impact door ROA Update minimaliseren

De beste manier om het hier uiteengezette probleem te vermijden is om **bestpath oorsprong-als gebruiksgeldigheid** zonder **validatie-staat** te gebruiken **is** in het beleid.

```
router bgp 100

 address-family ipv4 unicast

 bgp bestpath origin-as use validity

 !
```

Deze opdracht houdt een ontvangen ongeldige route op router maar voorkomt dat het een best-path wordt. Het zal niet worden geïnstalleerd of verder geadverteerd. Het is zo goed als het te laten vallen. Als met de volgende ROA-update deze geldig wordt, is geen VERNIEUWING vereist en komt deze automatisch in aanmerking voor het beste pad zonder dat beleidsuitvoering nodig is.

Als de gebruiker liever ‘ongeldige’ prefixes toestaat en deze niet gebruikt, dan gebruikt u naast de **bestpath origine-als gebruiksgeldigheid** de configuratie **best path origine-als ongeldig toestaan**.

In dit geval, wanneer een ROA verandert, wordt het beste pad automatisch bijgewerkt zonder dat er een REFresh-bericht nodig is. Om de-preferentie uit te schakelen, betekent een route dat tijdens de BGP-routeselectie het ongeldige RPKI-pad minder de voorkeur geniet dan enig ander pad naar dezelfde bestemming. Het is vergelijkbaar met het toekennen van het gewicht of lokale voorkeur minder dan 0.

Het aantal RPKI-invaliden is relatief klein en blijft in de tabel staan, maar heeft geen significant effect op de middelen.

> **Opmerking**: als u "bestpath-oorsprong-als-gebruiksgeldigheid" wilt gebruiken, moeten alle paden van een route, inclusief de IBGP-paden, de juiste RPKI-geldigheid hebben. Zo niet, dan kan het testen van de validatiestatus in routebeleid nog steeds gebruikt worden.

IBGP-routes worden niet gevalideerd door de router tegen de ROA-database. IBGP-routes verkrijgen een RPKI-geldigheid uit de uitgebreide RPKI-community. Als de IBGP-route wordt ontvangen zonder deze uitgebreide community, wordt de validatiestatus ingesteld op not-found.

BGP RPKI-geheugenvoetafdruk

Elk ROA verbruikt geheugen voor de index en de gegevens. Als twee ROA's voor hetzelfde IP-prefix zijn, maar verschillende max_len hebben of worden ontvangen van verschillende RPKI-servers, dan delen ze dezelfde index maar hebben ze afzonderlijke gegevens. Geheugenvereisten kunnen variëren omdat de geheugen-overhead niet constant is. Een overbudget van 10% wordt aanbevolen. Voor 64-bits platforms is meer geheugen nodig voor elk geheugenobject dan voor 32-bits platforms. IOS-XR geheugengebruik in bytes voor een indexobject en een gegevensobject is in de tabel opgenomen. Enkele meestal constante overheadkosten zijn inbegrepen in de getallen.

	32-bits platform (bytes)	64-bits platform (bytes)
IPv4-index	74	111
IPv6-index	86	125
gegevens	34	53

Deze sectie neemt twee scenario's om te verklaren hoe ROAs geheugen verbruiken.

Scenario 1. Drie RPKI-servers geconfigureerd op router

Neem een router met 3 RPKI-servers, die elk 200.000 IPv4 ROA's en 20.000 IPv6 ROA's op een 64-bits routeprocessor leveren, en die dit geheugen nodig hebben:

20000 * (125 + 3*53) + 200000 * (111 + 3*53) bytes = 59,68 miljoen bytes

Tijdens het berekenen van het geheugen, ROA voor hetzelfde prefix van drie verschillende validators gedeeld dezelfde indexwaarde.

Scenario 2. Enkelvoudige RPKI-servers geconfigureerd op router

BGP-procesgeheugen zonder ROA's:

```
RP/0/RP0/CPU0:Cisco8000#show processes memory detail location 0/RP0/CPU0 | in $

Fri Jan 22 17:19:57.945 UTC

JID        Text       Data       Stack      Dynamic    Dyn-Limit  Shm-Tot    Phy-Tot
 Process

1069           2M        71M       132K        25M      7447M        50M        74M        bgp


RP/0/RP0/CPU0:Cisco8000#show bgp rpki server summary

Fri Jan 22 17:12:09.073 UTC

Hostname/Address    Transport     State         Time          ROAs (IPv4/IPv6)

192.168.122.120     TCP:3323      NONE          00:00:25      N/A
```

BGP-proces neemt 25 MB geheugen in beslag zonder ROA's.

BGP-procesgeheugen met ROA:

```
RP/0/RP0/CPU0:Cisco8000#show bgp rpki server summary

Fri Jan 22 17:23:46.769 UTC

Hostname/Address    Transport     State         Time          ROAs (IPv4/IPv6)

192.168.122.120     TCP:3323      ESTAB         00:02:42      172796/28411
```

```
RP/0/RP0/CPU0:Cisco8000#show processes memory detail location 0/RP0/CPU0 | in $

Fri Jan 22 17:24:14.659 UTC

JID        Text       Data       Stack      Dynamic    Dyn-Limit  Shm-Tot    Phy-Tot     Process

1069          2M        99M       132K        53M      7447M        50M       102M       bgp
```

BGP-proces neemt 25 MB geheugen in beslag zonder ROA's.

BGP-procesgeheugen met ROA:

```
RP/0/RP0/CPU0:Cisco8000#show bgp rpki server summary

Fri Jan 22 17:23:46.769 UTC

Hostname/Address    Transport     State         Time          ROAs (IPv4/IPv6)

192.168.122.120     TCP:3323      ESTAB         00:02:42      172796/28411

RP/0/RP0/CPU0:Cisco8000#show processes memory detail location 0/RP0/CPU0 | in $

Fri Jan 22 17:24:14.659 UTC

JID        Text       Data       Stack      Dynamic    Dyn-Limit  Shm-Tot    Phy-Tot     Process

1069          2M        99M       132K        53M      7447M        50M       102M       bgp
```

Cisco 800 router draait 64-bits OS. Het ontving 172796 IPv4 ROA en 28411 ROA.

Geheugen (bytes) = 172,796 x [111 (index) + 53 (gegevens)] + 28411 x [125 (index) + 53 (gegevens)].

Deze berekeningen geven ~27 MB wat ongeveer de toename is die hierboven op het geheugen van de router is opgemerkt.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.