RPKI Validation

Attacks against the routing system are increasing, and it's not uncommon in today's Internet world to experience prefix hijacking. The IETF has for a while, been woking on an Internet Resource Public Key Infrastructure, to help validate routing (BGP) announcements.

Details on RPKI and how this works is best followed up through the RIR. The RIPE-NCC in particular have excellent resources for you to peruse.

At INX-ZA, we operate three (3) RPKI validators that are made available to the general public for use. These are spread across the country, and are available at:

- https://vc1.inx.net.za
- https://vc2.inx.net.za
- https://vc3.inx.net.za

for you to use manually, or, through the built-in API, to validate your prefixes.

Of course the point of RPKI validation is for your network equipment to do this automatically, so we suggest the following configuration:

RPKI Config

```
router bgp 65001
 bgp rpki server tcp 2001:43F8:1F4:100::40
port 8282 refresh 600
 bgp rpki server tcp 2001:43F8:1F5:100::40
port 8282 refresh 600
 bgp rpki server tcp 2001:43F8:1F3:100::40
port 8282 refresh 600
 bgp rpki server tcp 196.10.52.40 port 8282
refresh 600
 bgp rpki server tcp 196.10.54.40 port 8282
refresh 600
 bgp rpki server tcp 196.10.55.40 port 8282
refresh 600
```

Our recommendations

We recommend that you

- assign a higher local-pref to prefixes that have a Valid ROA
- leave prefixes with Not-Found ROAs untouched
- drop prefix with Invalid ROA

Most operators may be tempted to choose an approach where they set the local-pref of Invalids to something really low (ie. least preferred). The simple problem you're still likely to see is that a more-specific (ie. longer match) route for this, will **still** win in the BGP route selection process, and therefore still leave you to attack.

Dealing with Invalids

Most operators may be tempted to choose an approach where they set the local-pref of Invalids to something really low (ie. least preferred). The simple problem you're still

likely to see is that a more-specific (ie. longer match) route for this, will **still** win in the BGP route selection process, and therefore still leave you to attack.

Should you need assistance with this, please feel free to send a mail to ops [at] inx.net.za