BGP operations and security
draft-jdurand-bgp-security-01.txt

Jerome Durand

Gert Doering

Ivan Pepelnjak

Goal

- Describe BGP security best practices for the Internet
- Synthesis of many existing pieces available (Cymru, RIPE, many IETF docs, some well known pages…)
- More and more small AS'es with little knowledge about rules to follow
  - Help them build easily rules that work
- Have consistent rules across the Internet
- IPv4 and IPv6
  - Maybe a good idea to drive a bit IPv6 deployments with good BGP security policy

What is covered in the doc

- Session security (TTL, MD5, IPsec)
- Address filtering
  - Filters definition: special addresses, IANA not allocated, SIDR, IRR filters, IXP prefixes, prefixes too specific, default route…
  - Where to apply these filters
- BGP route flap dampening
- Maximum prefixes per peering
- AS Path filtering
- Community scrubbing

Changes between -01 and -00

- Add normative reference for RFC5082 in former section 3.2
  - ➔ TTL
- "Non routable" changed in title of former section 4.1.1
  - ➔ Prefixes that MUST not be routed by definition
- Correction of typo for IPv4 loopback prefix in former section 4.1.1.1
- Added shared transition space 100.64.0.0/10 in former section 4.1.1.1
- Clarification that 2002::/16 6to4 prefix can cross network boundaries in former section 4.1.1.2
- Rationale of 2000::/3 explained in former section 4.1.1.2
  - ➔ In order to build simplified prefix filters
- Added 3FFE::/16 prefix forgotten initially in the simplified list of prefixes that MUST not be routed by definition in former section 4.1.1.2
- Warn that filters for prefixes not allocated by IANA must only be done if regular refresh is guaranteed, with some words about the IPv4 experience, in former section 4.1.2.1

Changes between -01 and -00

- Replace RIR database with IRR. A definition of IRR is added in former section 4.1.2.2
- Remove any reference to anti-spoofing in former section 4.1.4
  - ➔ Not anti-spoofing as not dataplane!
- Clarification for IXP LAN prefix and pMTUd problem in former section 4.1.5
  - ➔ Using long discussions outcomes on RIPE ML
- "Autonomous filters" typo (instead of Autonomous systems) corrected in the former section 4.2
- Removal of an example for manual address validation in former section 4.2.2.1
- RFC5735 obsoletes RFC3300
- Ingress/Egress replaced by Inbound/Outbound in all the document

Conclusion

- Great feedback received so far!
  - Lot of support and many contributions received
  - Last IETF meeting many people agreed the initiative was worth continuing

➔Time for WG adoption

➔Questions ?