



VIRT03.DUS01.AS59645.NET

Revisiting BGP Security Best Practices

Tobias Fiebig

Max Planck Institute for Informatics

E-Mail: contact@as59645.net

Phone:

VIRT01.DUS01.AS59645.NET



BCP 194 / RFC 7454

- Running BGP securely
- Published Feb 2015
- The Internet tends to change



© Constanze Dietrich

Example 1: Advertising IXP Prefixes



BCP 194 / RFC 7454

- The IXP SHOULD originate X.Y.0.0/22 and advertise it to its members through an EBGP peering (most likely from its BGP route servers, configured with AS64496).
- The IXP members SHOULD accept the IXP prefix only if it passes the IRR generated filters (see Section 6.1.2.2.1)
- IXP members SHOULD then advertise X.Y.0.0/22 prefix to their downstreams. This announce would pass IRR based filters as it is originated by the IXP.

Example 1: Advertising IXP Prefixes



BCP 194 / RFC 7454

- The IXP SHOULD originate X.Y.0.0/22 and advertise it to its members through an EBGP peering (most likely from its BGP route servers, configured with AS64496).
- The IXP members SHOULD accept the IXP prefix only if it passes the IRR generated filters (see Section 6.1.2.2.1)
- IXP members SHOULD then advertise X.Y.0.0/22 prefix to their downstreams. This announce would pass IRR based filters as it is originated by the IXP.

Reality



Example 2: Prefix filters



- Is:
 - Less than GRT Size for Peers
 - More than GRT Size for Upstreams
 - Nothing for downstreams
- Should:
 - Global thresholds for peers/DS
 - RPKI for all

-bis BCP us part...



- Errata:
 - Not a simple error but practice changed
- -bis
 - Maybe, but might be to much
- New draft?
 - Also maybe
- Certainly: This needs an update!
- Why Opsec? Did BCP194 in the first place.