MANRS

The Mutually Agreed Norms for Routing Security, known as MANRS, is an industry initative supported by the Internet Society to improve routing hygiene on the global Internet.

The MANRS website has full information about what this initiative is all about.

The steps mentioned in this How To Peer section of the Toolbox cover some of the MANRS recommendations. These recommendations are around:

1. Incorrect routing information
2. traffic with spoofed source addresses
3. coordination and collaboration between networks

Route Origin Authorisation and the information contained in the Internet Routing Registry go a long way to helping solve the problem of incorrect routing information appearing on the global internet. Implementation of EBGP filters on all EBGP sessions (as discussed in RFC8212), by default, will also ensure that no operator using BGP will accidentally propagate routes without purposely creating filters to do so.

Traffic with spoofed source addresses can be blocked, at origin, by network operators implementing anti-spoofing filters, as noted in the Packet Filtering section discussing router hardware. Anti-spoofing filters can be even more efficiently implemented by using a technique known as Unicast Reverse Path Forwarding which is implemented in hardware on most access router platforms today.

Coordination and Collaboration between networks is achieved by ensuring that each network has direct contact with their upstream or peer network's Network Operation's Centre (not Customer Support), and keeping contact information in PeeringDB entries and Internet Routing Registry objects up to date.

Back to "What I need to Peer" page

From:
https://bgp4all.com/pfs/ - **Philip Smith's Internet Development Site**

Permanent link:
https://bgp4all.com/pfs/peering-toolbox/manrs?rev=1660823917

Last update: **2022/08/18 11:58**