MANRS

Content Delivery Network (CDN) and Cloud Programme

Routing security is vital to the future and stability of the Internet.

Mutually Agreed Norms for Routing Security (MANRS), a global initiative supported by the Internet Society, provides crucial fixes to reduce the most common threats to the Internet's routing system.

Originally designed for network operators, the initiative has expanded over the years to also address the unique needs and concerns of Internet Exchange Points (IXPs) and now CDNs and cloud providers.

The global routing system is under constant threat: attacks like route hijacks, route leaks, IP address spoofs, and other harmful activities can lead to denial of service, traffic inspection, lost revenue, reputational damage, and more. These incidents are global in scale, with one network's routing problems cascading to impact others.

CDNs and cloud providers typically exchange traffic with thousands of other networks so data can flow efficiently around the world. This makes them large hubs of the Internet interconnection infrastructure. Their participation in MANRS amplifies the positive effect they have on routing security, and the routing hygiene of networks they peer with.

According to industry estimates, over half of all web traffic is served over CDNs, and their use continues to grow to meet Internet users' growing appetite for media content, such as video, music, gaming, and software downloads. CDNs are therefore in a unique position to help to secure the global Internet.

We are inviting CDNs and cloud providers around the world to join the programme.

- Create a secure network peering environment, preventing potential attacks at their border
- Encourage better routing hygiene from your peering partners
- Signal organization security-forward posture
- Demonstrate responsible behaviour
- Improve operational efficiency for peering interconnections, minimizing incidents and providing more granular insight for troubleshooting

Join us in protecting the Internet ecosystem.

For more information, visit manrs.org/cdn-cloud-providers/
or contact us at manrs@isoc.org

Protect the core.

By joining, CDN and cloud providers support and commit to the baseline of routing security defined by a set of six security-enhancing actions, of which five are mandatory to implement.

1 Prevent propagation of incorrect routing information

Ensure correctness of own announcements. Ensure correctness of announcements of their peers (non-transit) by implementing explicit (whitelist) filtering with prefix granularity.

2 Prevent traffic of illegitimate source IP addresses

Implement anti-spoofing controls to prevent packets with illegitimate source IP address from leaving the network (egress filters).

3 Facilitate global operational communication and coordination

Maintain globally accessible and up-to-date contact information in PeeringDB and relevant RIR databases.

4 Facilitate validation of routing information on a global scale

Publicly document ASNs and prefixes that are intended to be advertised to external parties. Two main types of repositories are IRRs and RPKI. The requirement is to publish this information in at least one type of the repository (there may be more than one appropriate IRR); a recommendation is to maintain in both.

5 Encourage MANRS adoption

Actively encourage MANRS adoption among their peers.

6 Provide monitoring and debugging tools to peering partners (optional)

Provide a mechanism to inform peering partners if their announcements did not meet the requirements of the peering policy of the CDN and cloud provider.

We are inviting CDNs and cloud providers around the world to join the programme. Join us in protecting the Internet ecosystem.

manrs.org/cdn-cloud-providers/
manrs@isoc.org