

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



MANRS

Mutually Agreed Norms for Routing Security

Every day dozens of incidents affect the routing system. These incidents are global in scale, with one operator's routing problems cascading to impact others.

MANRS provides crucial fixes to eliminate the most common routing threats, outlining four simple but concrete actions that network operators should take.

Filtering

Prevent propagation of incorrect routing information.

Anti-spoofing

Prevent traffic with spoofed source IP addresses.

Coordination

Facilitate global operational communication and coordination between network operators.

Global Validation

Facilitate validation of routing information on a global scale.

For more information, visit www.manrs.org

We are in this together.

MANRS requires collaboration among participants and shared responsibility for the global Internet routing system.

Joining MANRS means joining a community of security-minded organizations committed to making the global routing infrastructure more robust and secure.

Implementing the MANRS actions:

- Signals an organization's security-forward posture
- Improves routing security: Mitigates routing incidents, helping networks identify and address problems with customers or peers
- Improves operational efficiency with better and cleaner peering communication pathways
- Provides granular insight for troubleshooting



Join the MANRS community.

For more information, visit www.manrs.org