MANRS

Mutually Agreed Norms for Routing Security

Why Routing Security is a Task for Computer Security Incident Response Teams

INFORMATION FOR CSIRTS

Over the last 12 months, around 2,500 significant attacks have occurred on the global Internet transport and routing systems. These incidents, called 'route hijacks' and 'route leaks,' can:

- Strain infrastructure
- Result in dropped traffic
- Allow unauthorized traffic inspection
- Lead to Denial of Service (DoS) attacks

As a Computer Security Incident Response Team (CSIRT) member, you develop security awareness and mitigation measures for your end users. Routing is a crucial element of critical national and international infrastructure and supply chains, yet most CSIRTs don't include routing security as part of infrastructure security within their service portfolios.

While CSIRTs generally don't run networks, you possess specialized knowledge of attacks and threats and mitigation, resolution strategies, and industry contacts. That puts you uniquely positioned to recommend best practices for securing systems, networks, critical data and assets, and other incident prevention.

We encourage you to work with others to improve global routing security, while taking a holistic view of the Internet security ecosystem. This is where MANRS comes in.

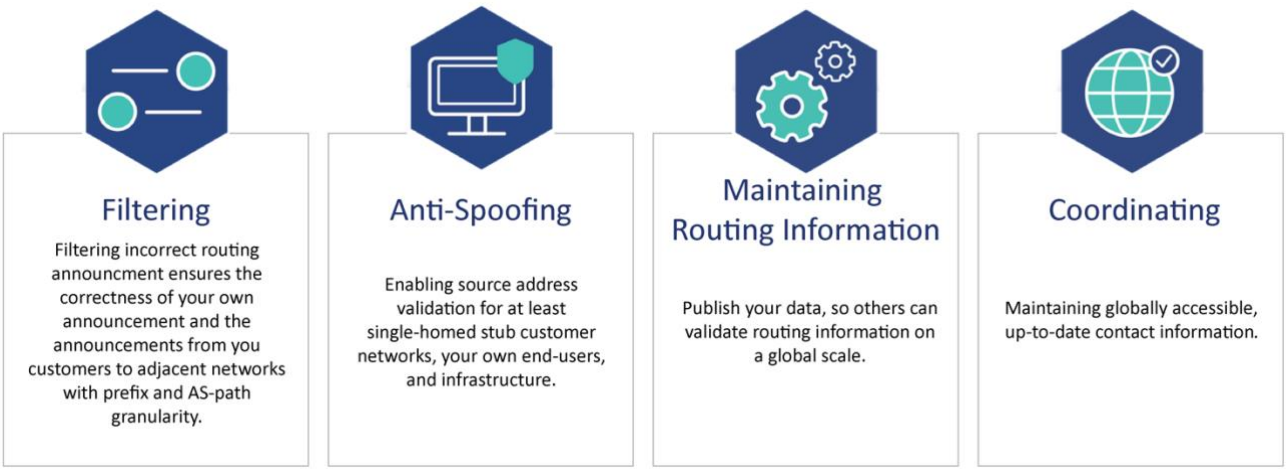
What is MANRS?

An industry-led initiative, Mutually Agreed Norms for Routing Security (MANRS), establishes a set of specific actions for networks to take based on their role in the Internet ecosystem. MANRS builds a community of security-minded organizations that meet MANRS conformance and transparency requirements. More than 1,000 networks are already MANRS participants, including network operators, content providers, and Internet exchange points (IXPs).

Securing routing information is a shared responsibility. Each network must implement basic routing security techniques on its own network and monitor its network neighbors to allow only legitimate traffic. Unfortunately, the level of awareness and the business case for implementing routing security measures is often not strong enough.

Mutually Agreed Norms for Routing Security (MANRS)

By choosing service providers that comply with MANRS actions, organizations can improve their network and encourage other providers to improve their infrastructure and supply chain security.



How Can MANRS Help?

MANRS can support CSIRT communities in the following areas:

- Raising awareness of routing security issues within your communities
- Encouraging other CSIRTs to add routing security incident monitoring and incident handling to their service portfolios
- Encouraging CSIRTs to adopt the MANRS Observatory monitoring tool to provide situational awareness of routing security
- Extending the reach of the MANRS initiative within CSIRT constituencies, as well as into national critical infrastructure initiatives
- Holding practical routing security workshops or co-developing a routing security curriculum in the context of training the trainers and/or network forensics capacity-building programs
- Adding routing security to network security auditing programs

CSIRTs can help explain the criticality of routing security and promote MANRS actions to improve the security of the routing system by:

- Encouraging their parent organizations or constituents to take routing security issues more seriously
- Raising awareness with governments of how routing security issues can affect critical infrastructure
- Advocating the adoption of routing security recommendations (such as NIST standards)

Given the significant impact of routing incidents on critical networks, we must prioritize protecting and improving our network infrastructure.

FIND OUT MORE AT MANRS.ORG