



# THE IMPOSSIBLE MANNERS

Hanna Kreitem

[KREITEM@ISOC.ORG](mailto:KREITEM@ISOC.ORG)

# Why Does MANRS Matter?



# Quick Overview of MANRS

Border Gateway Protocol (BGP) is based entirely on trust between networks.

Prone to Prefix and Route Hijacks, Route Leaks, and IP Spoofing.

Mutually Agreed Norms for Routing Security (MANRS) offers crucial fixes to reduce the most common routing threats. Relies on collective responsibility to ensure a globally robust and secure routing infrastructure.

MANRS Programs defines the minimum steps networks, CDNs, vendors, and IXPs should take to ensure the security and resilience of the Internet's global routing system.

# MANRS Programs and Actions

Network Operators	CDN and Cloud Providers	IXP	Vendor
Action1: Filtering *	Filtering	Filtering	Provide solutions for the implementation of specific MANRS Actions by other participants
Action 2: Anti-spoofing	Anti-spoofing	Promotion	Promote MANRS through training and technical content
Action 3: Coordination *	Coordination	Protect the peering platform	Commit to ongoing MANRS activities
Action 4: Global Validation *	Global Validation	Coordination	
	Promotion	Tools	
	Tools		



# Conforming with MANRS

Or is MANRS impossible to conform with?



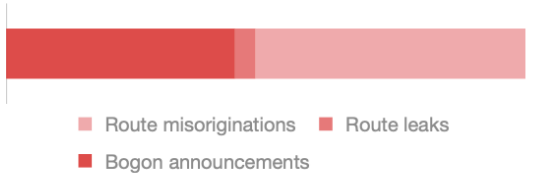
# MANRS Readiness, Global

## State of Routing Security

Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

### Incidents i

Route misoriginations	939
Route leaks	71
Bogon announcements	794
<b>Total</b>	<b>1,804</b>



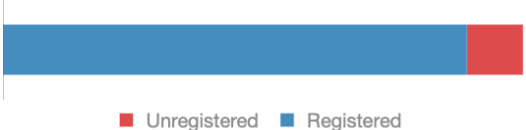
### Culprits i

Culprits	1,236
----------	-------



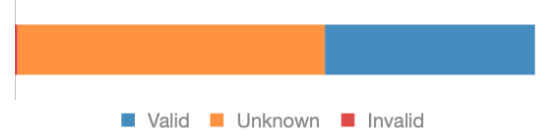
### Routing completeness (IRR) i

Unregistered	122,277	10.8%
Registered	1,008,528	89.2%



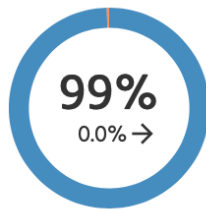
### Routing completeness (RPKI) i

Valid	456,387	40.4%
Unknown	668,526	59.1%
Invalid	5,892	0.5%

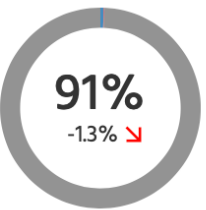


## MANRS Readiness i

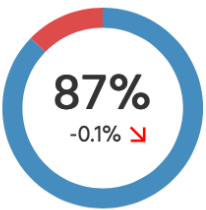
### Filtering i



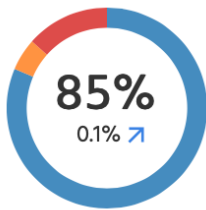
### Anti-spoofing i



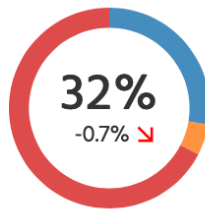
### Coordination i



### Global Validation IRR i



### Global Validation RPKI i



● Ready ● Aspiring ● Lagging ● No Data Available

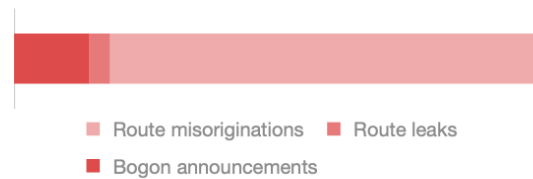
# MANRS Readiness, Middle East

## State of Routing Security

Number of incidents, networks involved and quality of published routing information in the IRR and RPKI in the selected region and time period

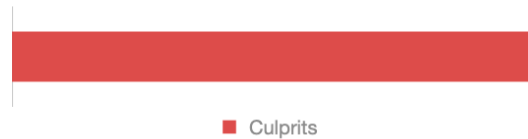
### Incidents i

Route misoriginations	62
Route leaks	3
Bogon announcements	11
<b>Total</b>	<b>76</b>



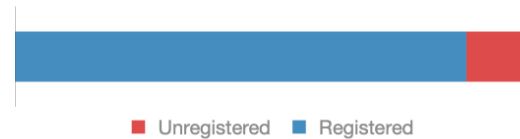
### Culprits i

Culprits	46
----------	----



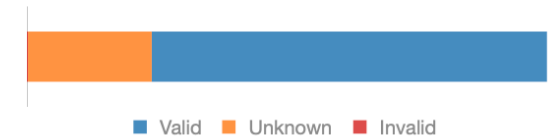
### Routing completeness (IRR) i

Unregistered	7,814	13.2%
Registered	51,553	86.8%



### Routing completeness (RPKI) i

Valid	45,105	76.0%
Unknown	14,110	23.8%
Invalid	152	0.2%

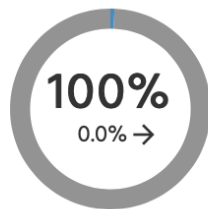


## MANRS Readiness i

### Filtering i



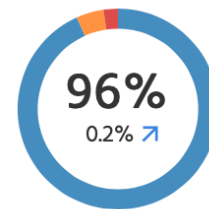
### Anti-spoofing i



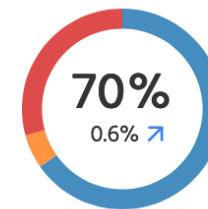
### Coordination i



### Global Validation IRR i



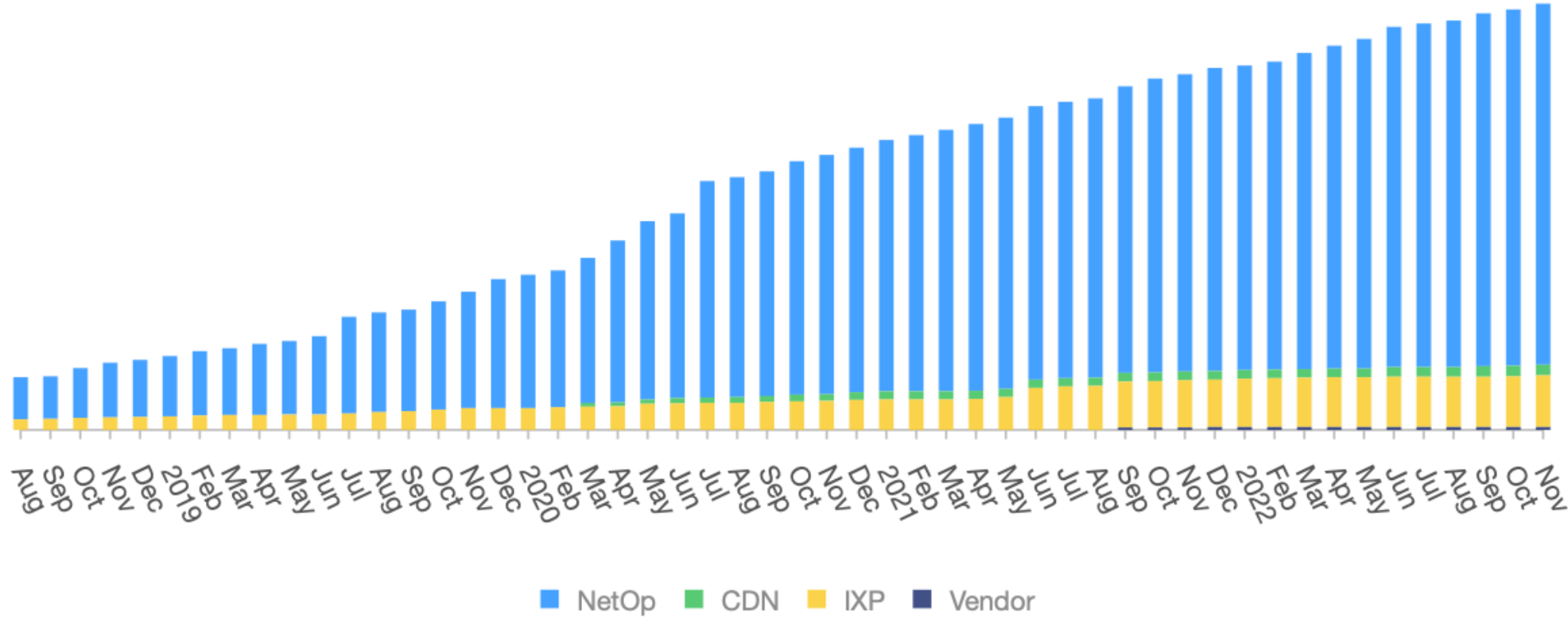
### Global Validation RPKI i



● Ready ● Aspiring ● Lagging ● No Data Available

# MANRS Participants Global

Participants by program by month



Network Operators	747
CDN and Cloud Providers	22
IXP	107
Vendors	6
<b>November 2022</b>	





# MANRS Participants ME

Network Operators	18
CDN and Cloud Providers	-
IXP	3 (UAE-IX, SAIX, DE-CIX IST)
Vendors	-
November 2022	



# What does it take to become a MANRS participant?



**TIME**



**KNOW-HOW**



**ACCESS TO RESOURCES**

# MANRS Actions and Implementation (NetOps)

## Action 1, Filtering

Preventing propagation of incorrect routing information.

There are several ways to build these filters:

1. Use Internet Routing Registries (IRRs) and require the customers to register route objects
2. Use Resource Public Key Infrastructure (RPKI) and require the customers to create Route Origin Authorizations (ROAs)
3. Use an internal database with the information provided as part of the provisioning process This document will only focus on the first two cases, since case 3 is proprietary.

More details and sample configurations available at the MANRS Implementation Guide:

<https://www.manrs.org/netops/guide/>



# MANRS Actions and Implementation (NetOps)

## Action 2, Anti-spoofing

Preventing traffic with spoofed source IP addresses

Network operator implements a system that enables source address validation for at least single-homed stub customer networks, their own end-users and infrastructure. Network operator implements anti-spoofing filtering to prevent packets with incorrect source IP address from entering and leaving the network.

For most smaller and simpler network architectures the easiest way to prevent spoofing is by using Unicast RPF (uRPF) in Strict Mode.

More details and sample configurations available at the MANRS Implementation Guide:

<https://www.manrs.org/netops/guide/>



# MANRS Actions and Implementation (NetOps)

## Action 3, Coordination

Facilitating global operational communication and coordination between network operators

- At a minimum, a network operator should register and maintain 24/7 contact information in at least one of RADB, AfriNIC, APNIC, ARIN, LACNIC and RIPE, and also on their public website.

More details and sample configurations available at the MANRS Implementation Guide:

<https://www.manrs.org/netops/guide/>



# MANRS Actions and Implementation (NetOps)

## Action 4, Global Validation

Facilitating validation of routing information on a global scale.

- Network operator is able to communicate to their adjacent networks which announcements are correct;
- Network operator has publicly documented routing policy, ASNs and prefixes that are intended to be advertised to external parties.

route/route6 objects registered in one of the IRR databases; and ROAs published in the RPKI system

More details and sample configurations available at the MANRS Implementation Guide:

<https://www.manrs.org/netops/guide/>



## MANRS Network Operator Application

Fields marked with an asterisk (\*) are required.

The form can be filled out either in English, or in your native language.

1 Operator Information 2 MANRS Actions 3 Consent & Review

Organization Name \*

Organization Website \*

Areas Served \*

Select the countries where your organization is based and/or provides services. We use ISO 3166-1 Alpha-2 country codes.

AS Number(s) of Your Networks \*

Add each AS Number on its own line by using the "+" key.

Organization Logo

Upload a .jpg or .png version of your company's logo, suitable for display on a white background in 400x400 pixels. This image will be published with your listing if your application is accepted.

Choose File no file selected

# Common Issues When Joining MANRS

1. Applying
2. Anti-spoofing data
3. For the region: Action 3

We usually aim to respond to your application within 2-3 days, can take up to a week.

Advanced Search

Internet Society **Gold Sponsor**

Exchange ID	ASN	Speed
IX Australia (Sydney NSW)	141384	10G
218.100.53.78	2001:77a:11:4:2:2848:0:1	
25Pse	141384	1G
185.1.224.234	2001:77b:11e:234	

Private Peering Facilities

Facility ID	ASN	Country	City
Equinix SY4 - Sydney	141384	Australia	Sydney
NTT Zurich 1 Data Center (ZRH-1)	141384	Switzerland	Römlang
141384			

Website: <http://www.internetsociety.org>

AS-set/route-set: RIPE::AS-ISOC

Route Server URL:

Looking Glass URL:

Network Type: Non-Profit

IPv4 Prefixes: 3

IPv6 Prefixes: 3

Traffic Levels: 20-100Mbps

Traffic Ratios: Balanced

Geographic Scope: Global

Protocols Supported:  Unicast IPv4  Multicast  IPv6  Never via route servers

Last Updated: 2022-07-27T05:35:43Z

Public Peering Info Updated: 2022-03-30T16:44:39

Peering Facility Info Updated: 2021-08-24T13:23:52

Contact Info Updated: 2021-08-24T13:05:38

Notes:

RIR Status: ok

RIR Status Updated: 2022-07-27T05:29:57

Routing Policy Information

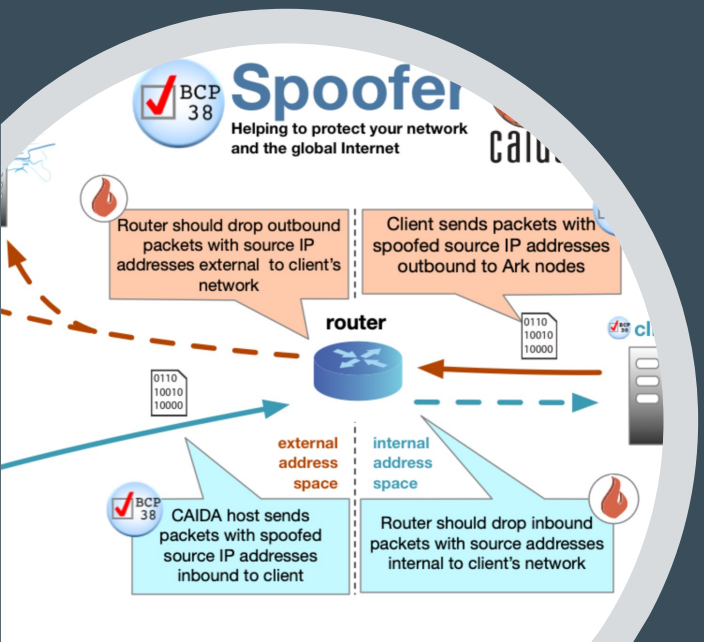
Routing Policy: <http://www.internetsociety.org>

Policy: Open

Conditions: Not Required

Prefix List: No

AS Path: Not Required



Next?

Implement the actions and apply to  
become a participant





# Thank you.

Hanna Kreitem

KREITEM@ISOC.ORG

LEARN MORE:

<https://www.manrs.org>

FOLLOW US:



/RoutingMANRS

manrs.org