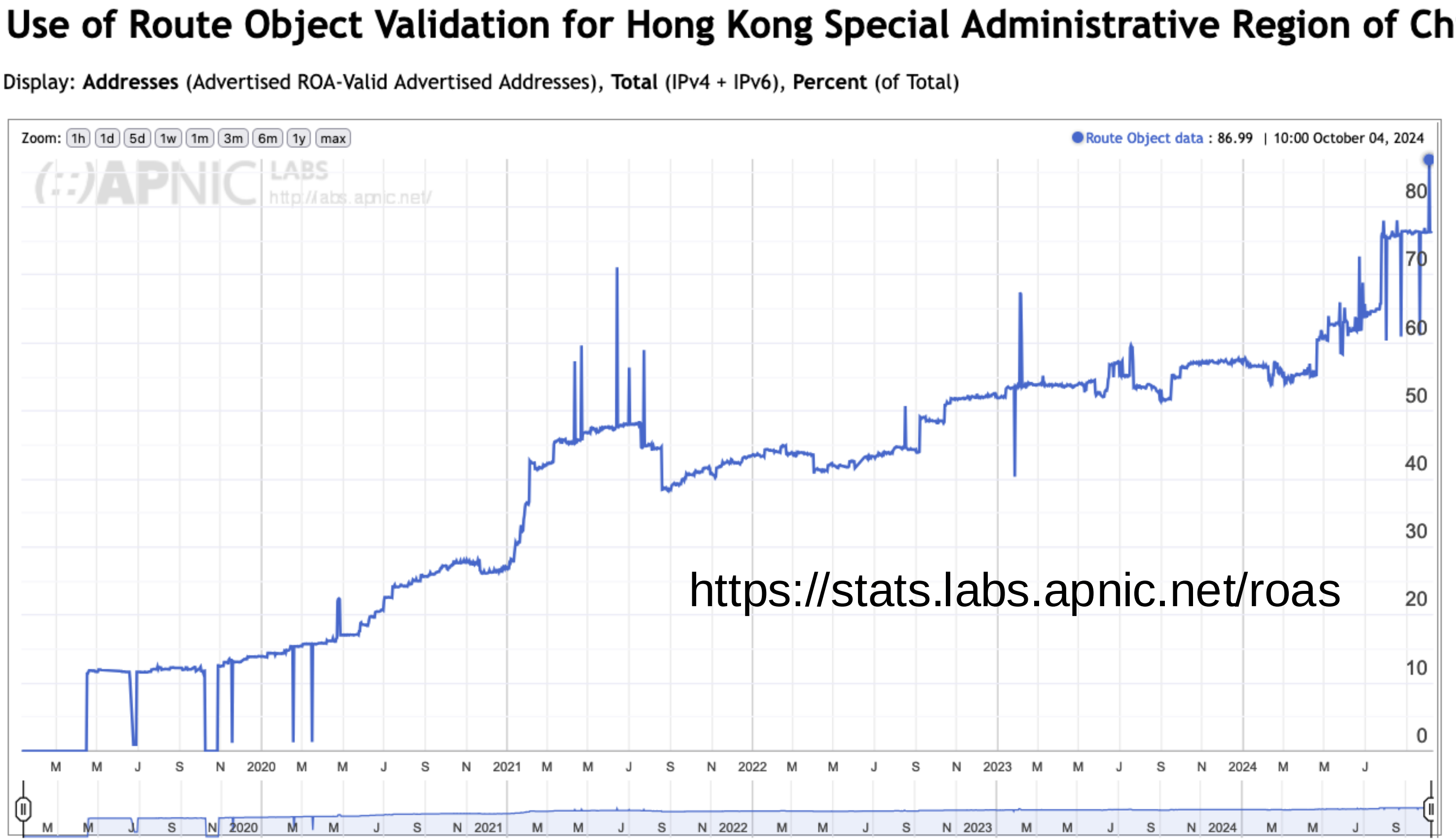
DASH

HKNOG 13.0

Zen Ng – Senior Internet Resource Analyst

1 Nov 2024

IPv4 and IPv6 ROA coverage in Hong Kong



Use of Route Object Validation for Hong Kong Special Administrative Region of China (HK)

Display: **Addresses** (Advertised ROA-Valid Advertised Addresses), **Total** (IPv4 + IPv6), **Percent** (of Total)

Zoom: 1h 1d 5d 1w 1m 3m 6m 1y max

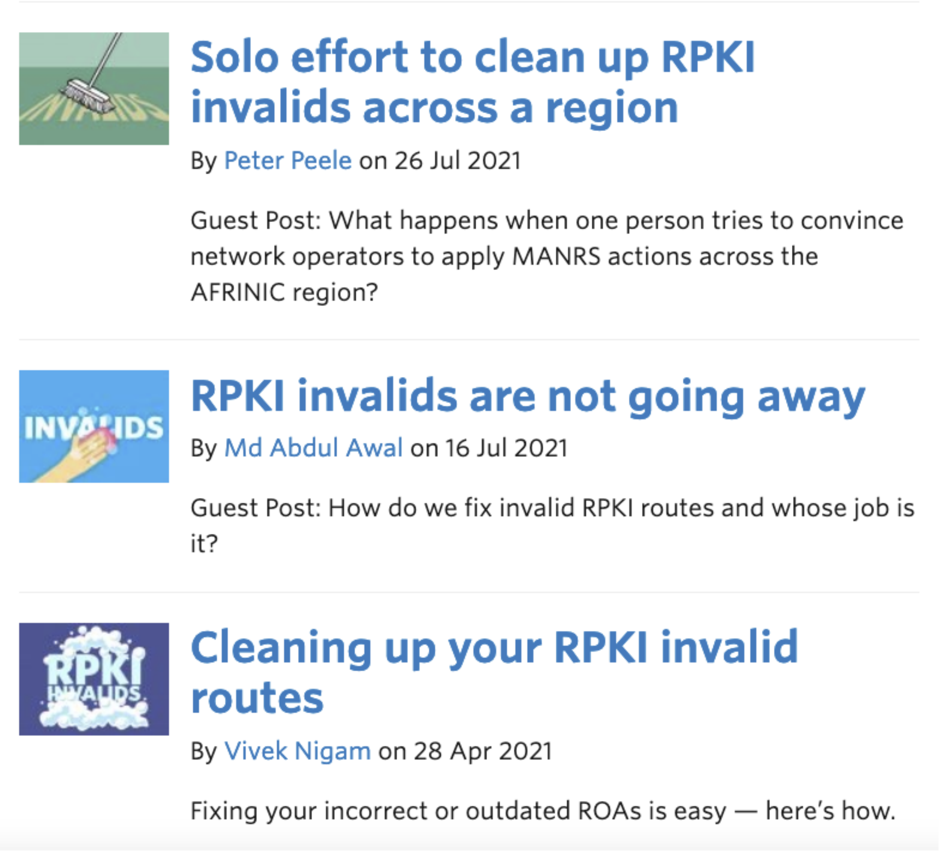
● Route Object data : 86.99 | 10:00 October 04, 2024

(:::)APNIC LABS
http://labs.apnic.net/
80
70
60
50
40
30
20
10
0
M M J S N 2020 M M J S N 2021 M M J S N 2022 M M J S N 2023 M M J S N 2024 M M J
M M J S N 2020 M M J S N 2021 M M J S N 2022 M M J S N 2023 M M J S N 2024 M M J S

86.99%

https://stats.labs.apnic.net/roas

RPKI invalids



Solo effort to clean up RPKI invalids across a region

By Peter Peele on 26 Jul 2021

Guest Post: What happens when one person tries to convince network operators to apply MANRS actions across the AFRINIC region?

RPKI invalids are not going away

By Md Abdul Awal on 16 Jul 2021

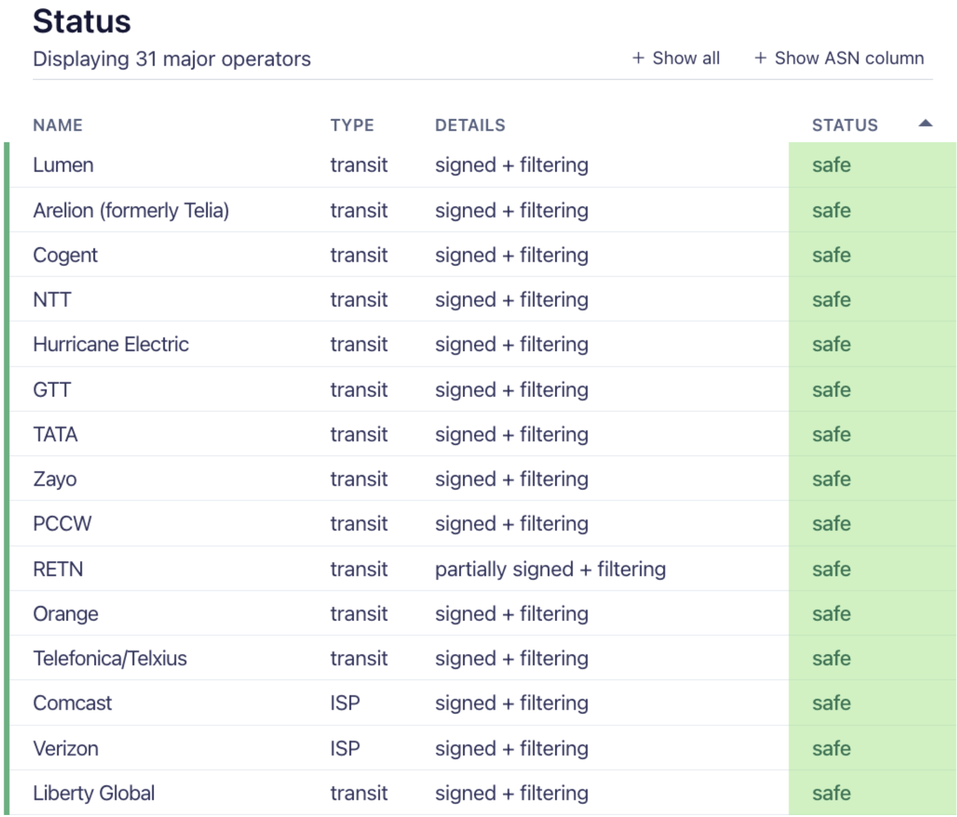
Guest Post: How do we fix invalid RPKI routes and whose job is it?

Cleaning up your RPKI invalid routes

By Vivek Nigam on 28 Apr 2021

Fixing your incorrect or outdated ROAs is easy — here's how.

Route Origin Validation



Status

Displaying 31 major operators

NAME	TYPE	DETAILS	STATUS ▲
Lumen	transit	signed + filtering	safe
Arelion (formerly Telia)	transit	signed + filtering	safe
Cogent	transit	signed + filtering	safe
NTT	transit	signed + filtering	safe
Hurricane Electric	transit	signed + filtering	safe
GTT	transit	signed + filtering	safe
TATA	transit	signed + filtering	safe
Zayo	transit	signed + filtering	safe
PCCW	transit	signed + filtering	safe
RETN	transit	partially signed + filtering	safe
Orange	transit	signed + filtering	safe
Telefonica/Telxius	transit	signed + filtering	safe
Comcast	ISP	signed + filtering	safe
Verizon	ISP	signed + filtering	safe
Liberty Global	transit	signed + filtering	safe

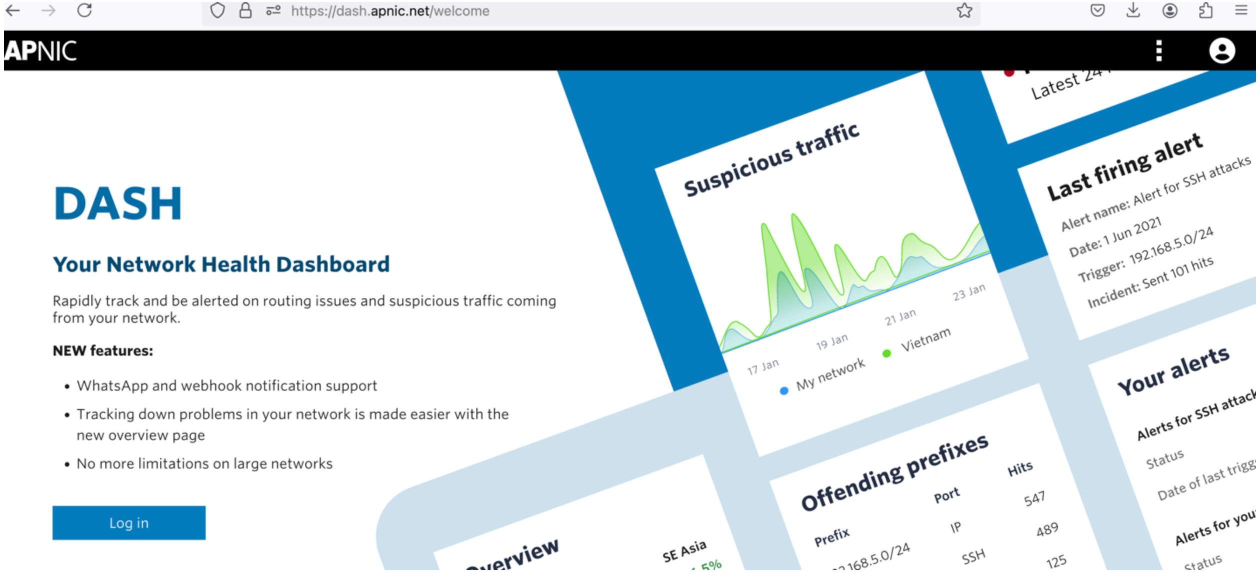
https://isbgpsafeyet.com/

Why DASH is needed?

- ➢ Is putting a padlock on the door enough?? No!
- ➢ Put a CCTV on your front door
- Route Hijacking
- RPKI Invalids
- Fat Finger/ Human Error
- Suspicious traffic

How to access DASH?

- www.dash.apnic.net
- Use same credentials for APNIC login



DASH

Your Network Health Dashboard

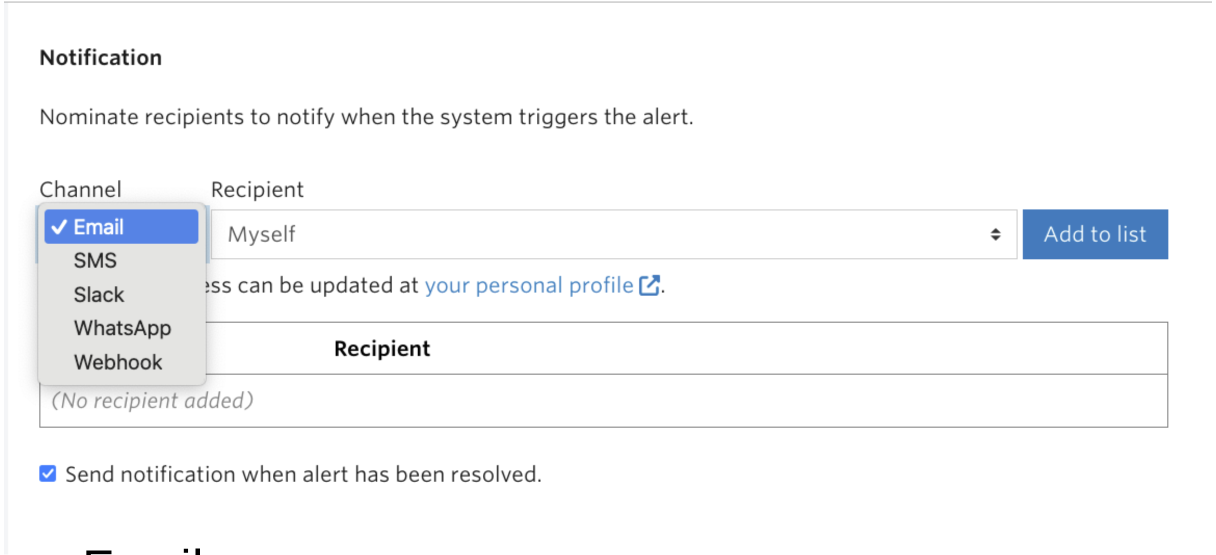
Rapidly track and be alerted on routing issues and suspicious traffic coming from your network.

NEW features:

- WhatsApp and webhook notification support
- Tracking down problems in your network is made easier with the new overview page
- No more limitations on large networks

Log in

How would you like to be notified?



Notification

Nominate recipients to notify when the system triggers the alert.

Channel

✓ Email
SMS
Slack
WhatsApp
Webhook

Recipient

Myself

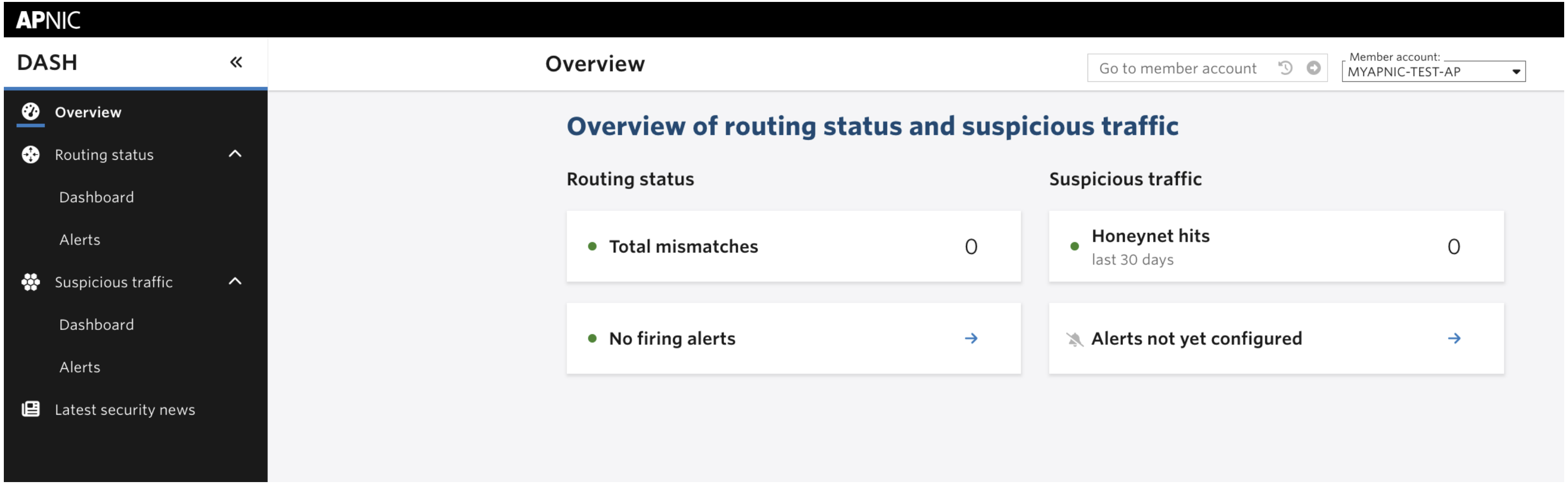
ess can be updated at your personal profile.

	Recipient
(No recipient added)	

☑ Send notification when alert has been resolved.

- Email
- SMS
- Slack
- Whatsapp
- Webhook

Routing status alerts in DASH



APNIC

DASH «

Overview

Go to member account

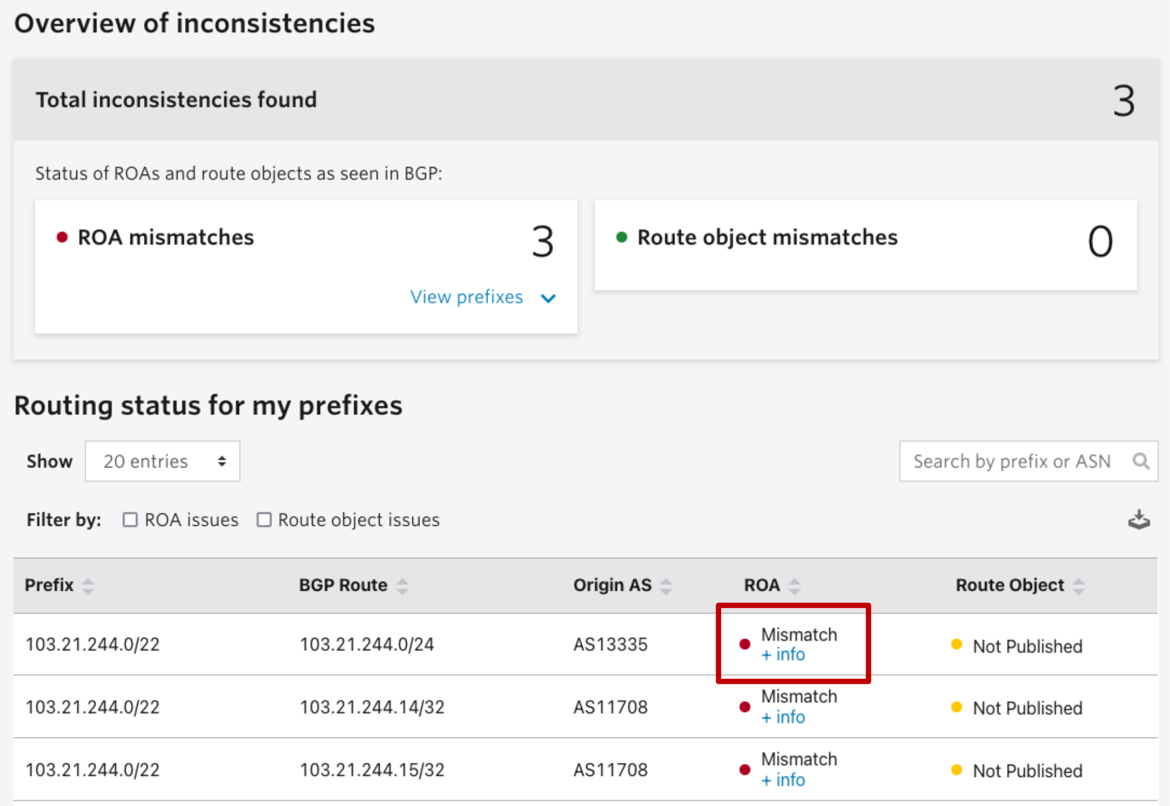
Member account: MYAPNIC-TEST-AP

- Overview
- Routing status
  - Dashboard
  - Alerts
- Suspicious traffic
  - Dashboard
  - Alerts
- Latest security news

Overview of routing status and suspicious traffic

Routing status		Suspicious traffic	
● Total mismatches	0	● Honeynet hits last 30 days	0
● No firing alerts	→	Alerts not yet configured	→

Routing status alerts in DASH



Overview of inconsistencies

Total inconsistencies found 3

Status of ROAs and route objects as seen in BGP:

● ROA mismatches 3

View prefixes ⌄

● Route object mismatches 0

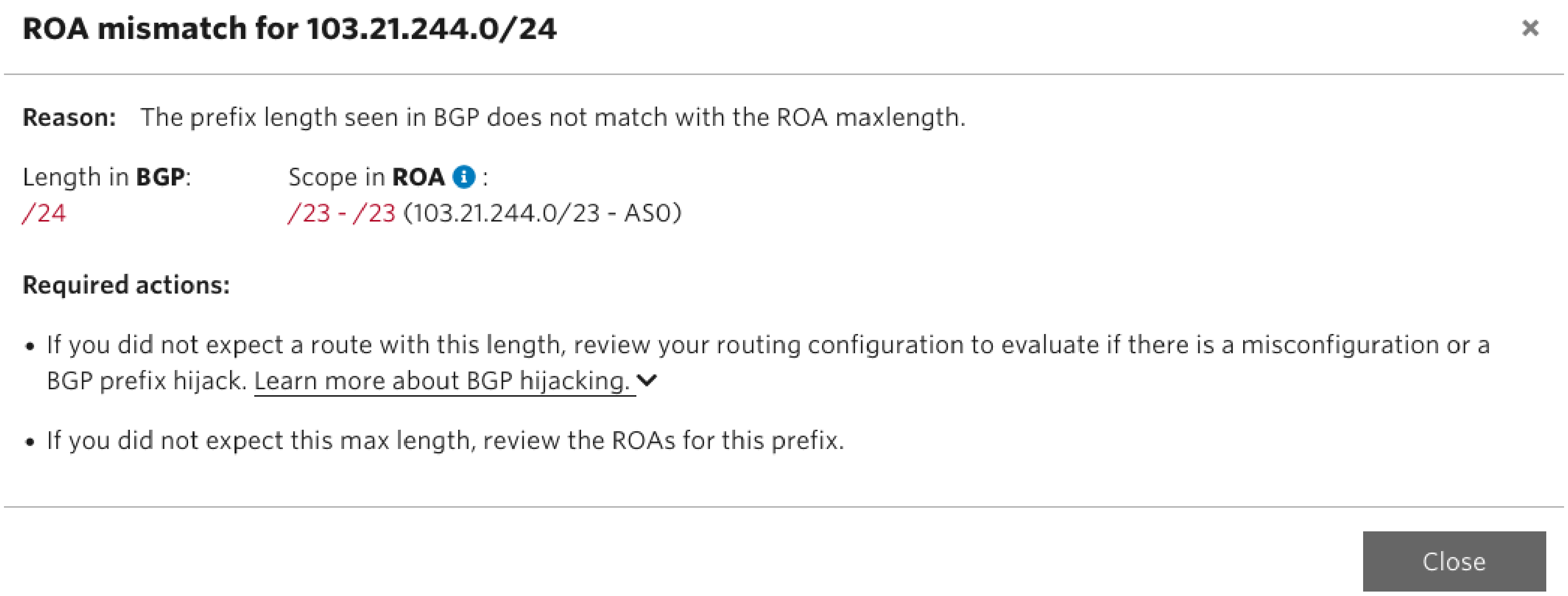
Routing status for my prefixes

Show 20 entries ⬍ | Search by prefix or ASN

Filter by: □ ROA issues □ Route object issues

Prefix	BGP Route	Origin AS	ROA	Route Object
103.21.244.0/22	103.21.244.0/24	AS13335	● Mismatch + info	● Not Published
103.21.244.0/22	103.21.244.14/32	AS11708	● Mismatch + info	● Not Published
103.21.244.0/22	103.21.244.15/32	AS11708	● Mismatch + info	● Not Published

Routing status alerts in DASH



ROA mismatch for 103.21.244.0/24

Reason: The prefix length seen in BGP does not match with the ROA maxlength.

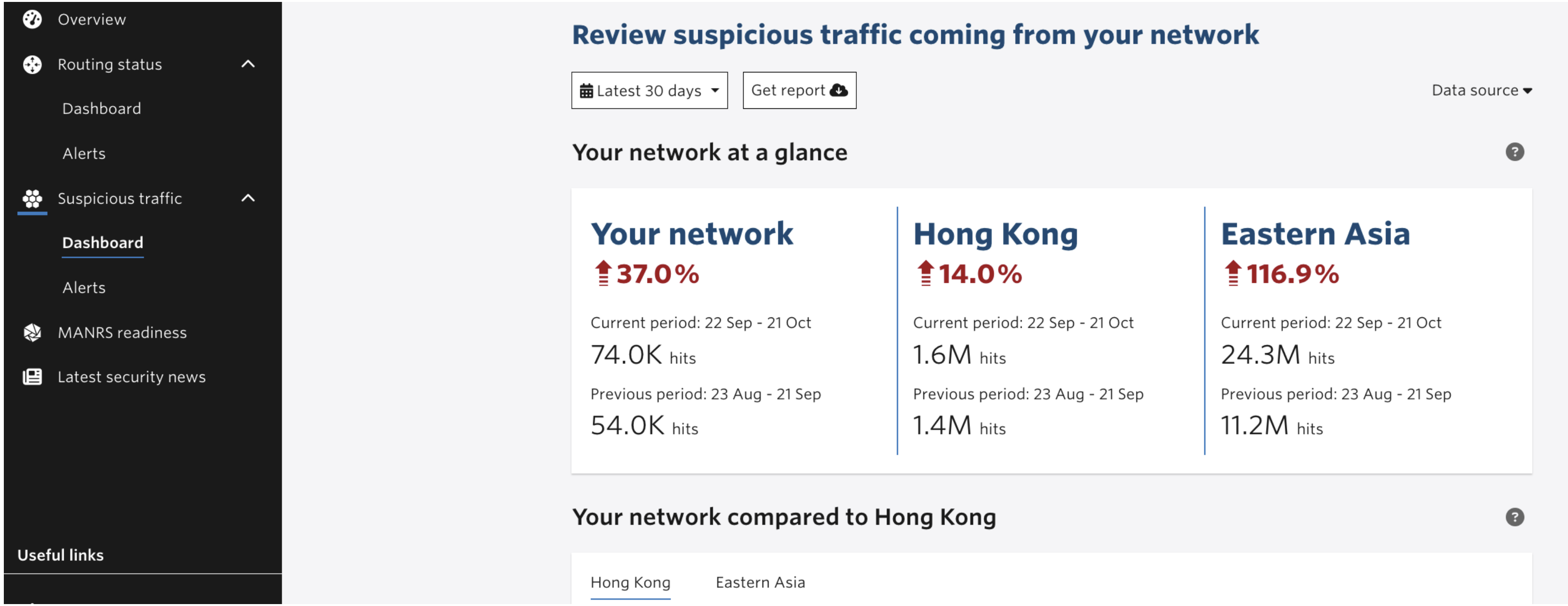
Length in **BGP**: /24

Scope in **ROA** ⓘ : /23 - /23 (103.21.244.0/23 - AS0)

Required actions:

- If you did not expect a route with this length, review your routing configuration to evaluate if there is a misconfiguration or a BGP prefix hijack. Learn more about BGP hijacking.
- If you did not expect this max length, review the ROAs for this prefix.

Suspicious traffic in DASH



Review suspicious traffic coming from your network

Your network at a glance

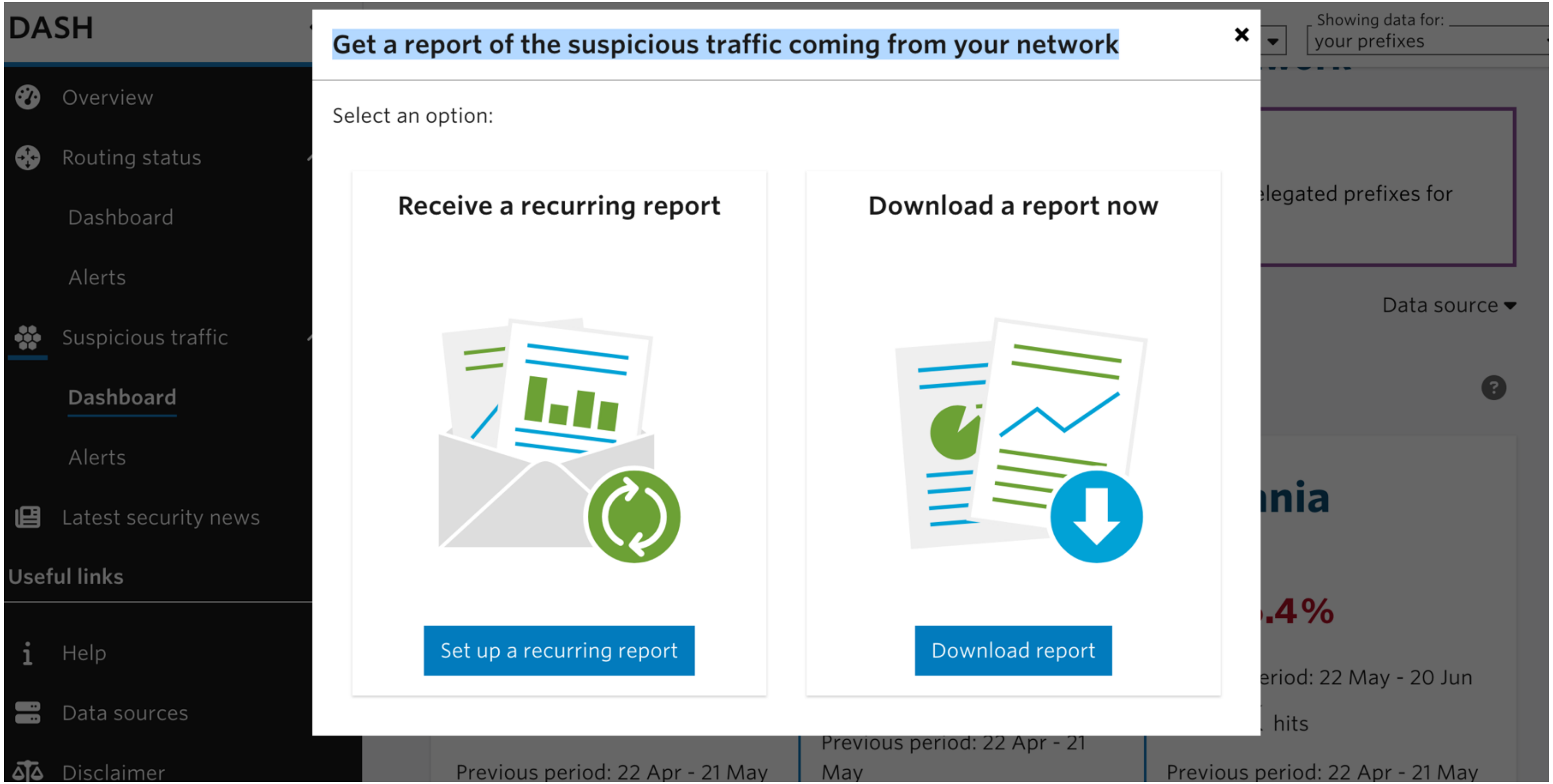
Your network
⬆ 37.0%
Current period: 22 Sep - 21 Oct
74.0K hits
Previous period: 23 Aug - 21 Sep
54.0K hits

Hong Kong
⬆ 14.0%
Current period: 22 Sep - 21 Oct
1.6M hits
Previous period: 23 Aug - 21 Sep
1.4M hits

Eastern Asia
⬆ 116.9%
Current period: 22 Sep - 21 Oct
24.3M hits
Previous period: 23 Aug - 21 Sep
11.2M hits

Your network compared to Hong Kong

Suspicious traffic in DASH



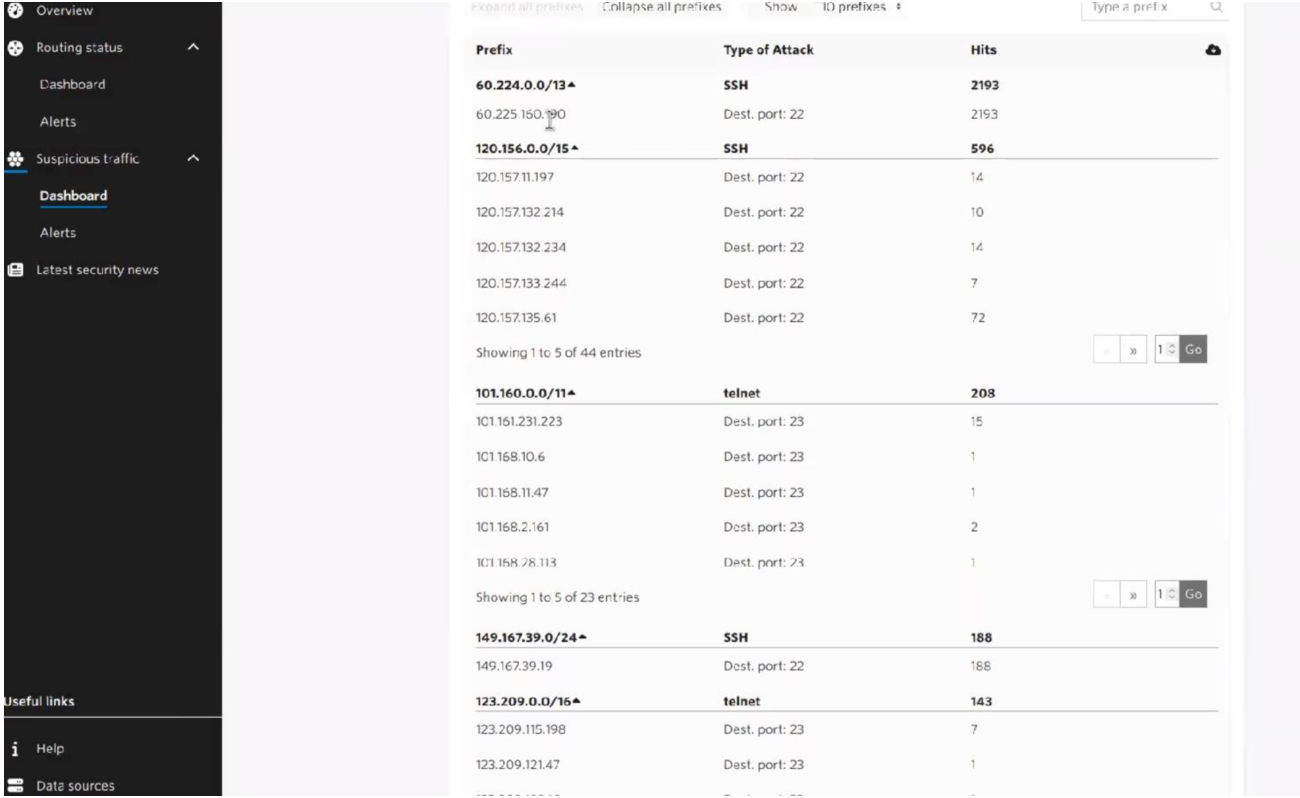
Get a report of the suspicious traffic coming from your network

Select an option:

Receive a recurring report

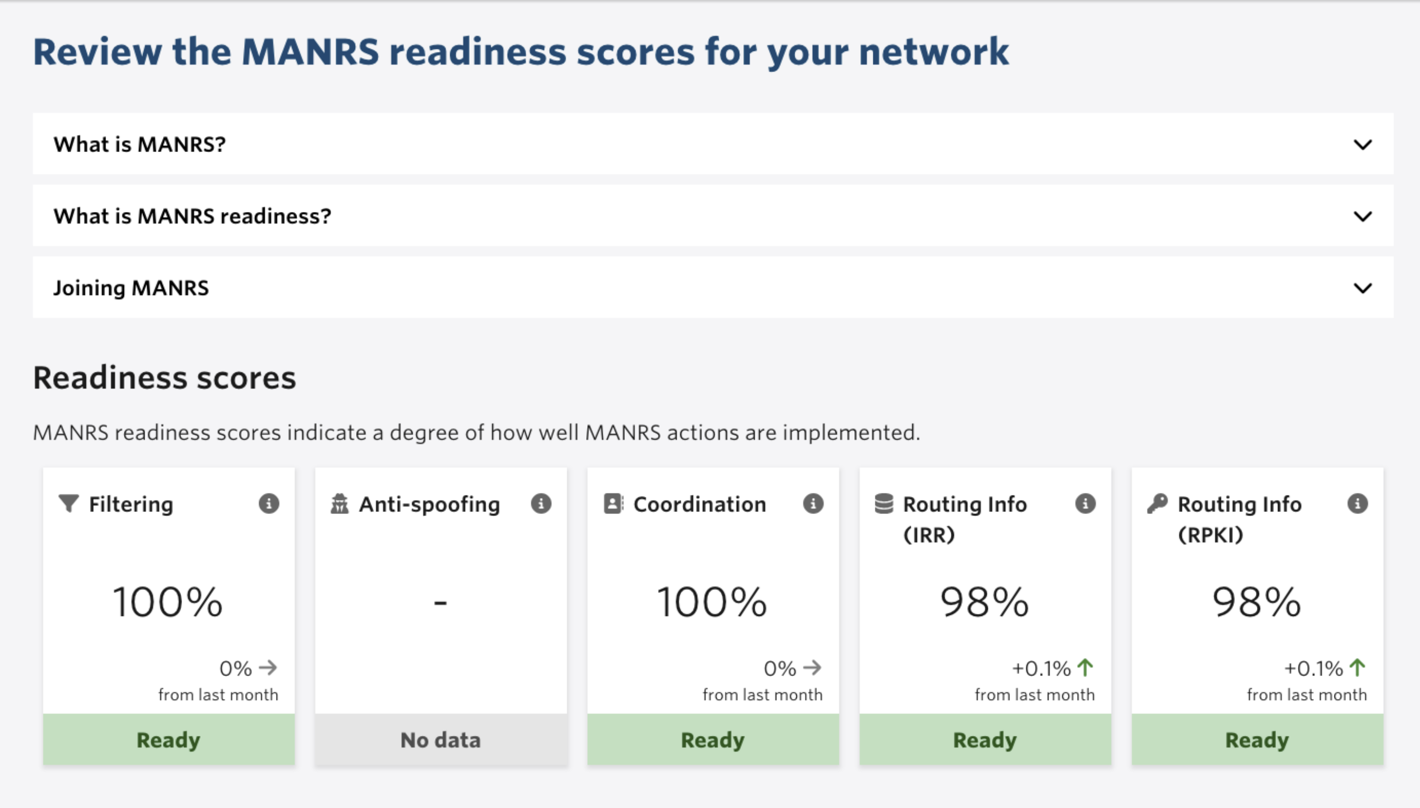
Download a report now

Suspicious traffic in DASH



Prefix	Type of Attack	Hits
60.224.0.0/13▲	**SSH**	**2193**
60.225.160.190	Dest. port: 22	2193
120.156.0.0/15▲	**SSH**	**596**
120.157.11.197	Dest. port: 22	14
120.157.132.214	Dest. port: 22	10
120.157.132.234	Dest. port: 22	14
120.157.133.244	Dest. port: 22	7
120.157.135.61	Dest. port: 22	72
Showing 1 to 5 of 44 entries		
101.160.0.0/11▲	**telnet**	**208**
101.161.231.223	Dest. port: 23	15
101.168.10.6	Dest. port: 23	1
101.168.11.47	Dest. port: 23	1
101.168.2.161	Dest. port: 23	2
101.168.28.113	Dest. port: 23	1
Showing 1 to 5 of 23 entries		
149.167.39.0/24▲	**SSH**	**188**
149.167.39.19	Dest. port: 22	188
123.209.0.0/16▲	**telnet**	**143**
123.209.115.198	Dest. port: 23	7
123.209.121.47	Dest. port: 23	1

MANRS Readiness



Review the MANRS readiness scores for your network

What is MANRS?

What is MANRS readiness?

Joining MANRS

Readiness scores

MANRS readiness scores indicate a degree of how well MANRS actions are implemented.

Filtering

100%

0% →
from last month

Ready

Anti-spoofing

-

No data

Coordination

100%

0% →
from last month

Ready

Routing Info (IRR)

98%

+0.1% ↑
from last month

Ready

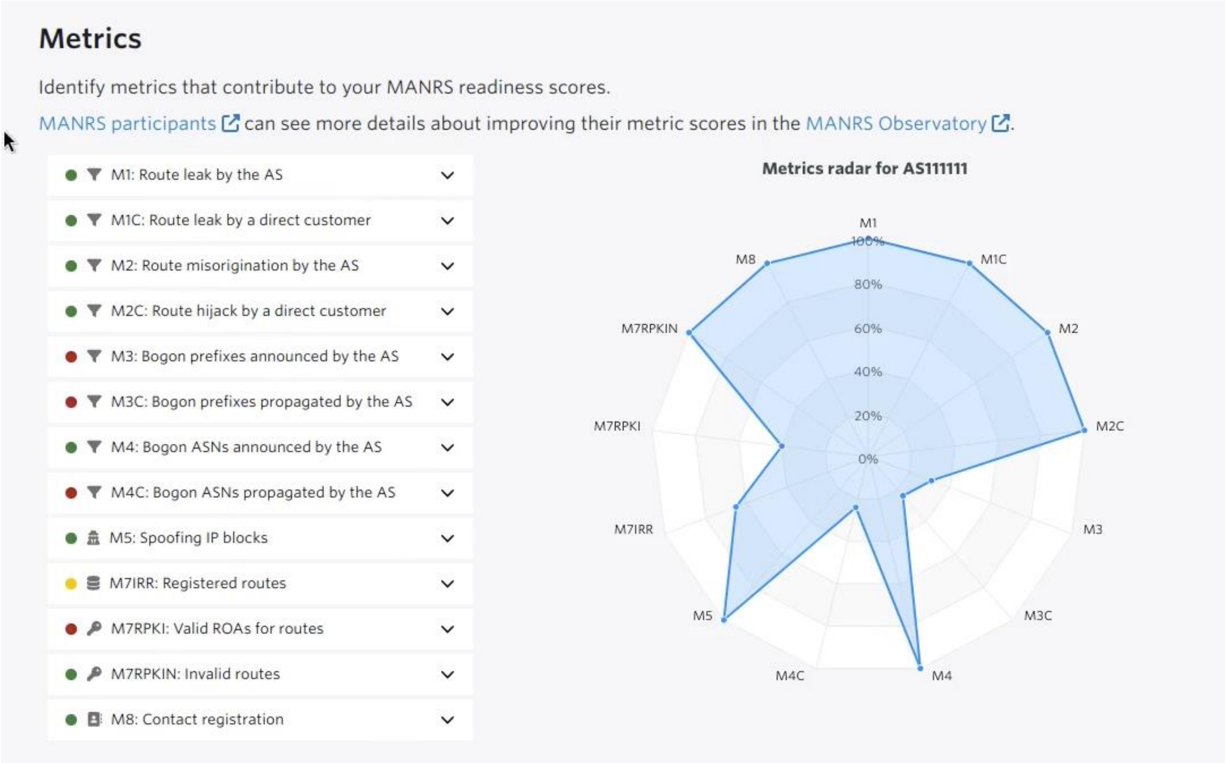
Routing Info (RPKI)

98%

+0.1% ↑
from last month

Ready

MANRS Readiness



Metrics

Identify metrics that contribute to your MANRS readiness scores.

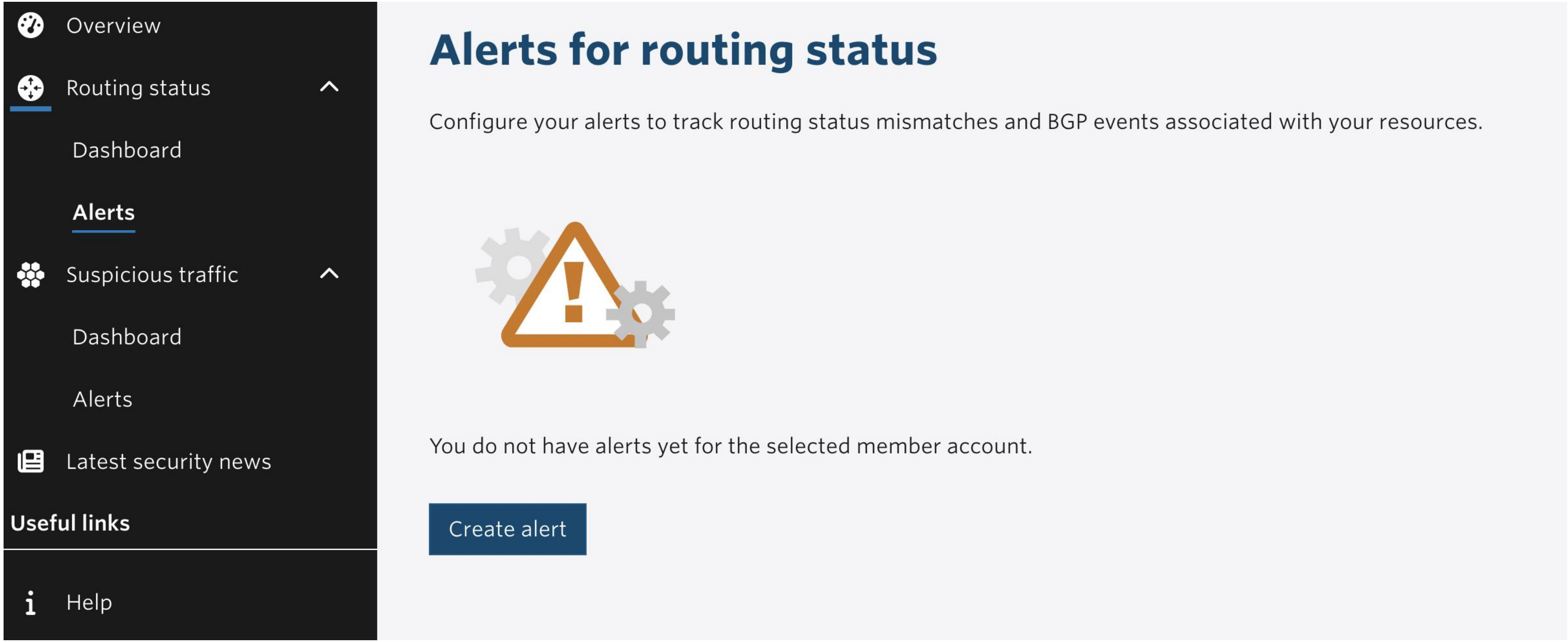
MANRS participants can see more details about improving their metric scores in the MANRS Observatory.

- 🟢 M1: Route leak by the AS
- 🟢 M1C: Route leak by a direct customer
- 🟢 M2: Route misorigination by the AS
- 🟢 M2C: Route hijack by a direct customer
- 🔴 M3: Bogon prefixes announced by the AS
- 🔴 M3C: Bogon prefixes propagated by the AS
- 🟢 M4: Bogon ASNs announced by the AS
- 🔴 M4C: Bogon ASNs propagated by the AS
- 🟢 M5: Spoofing IP blocks
- 🟡 M7IRR: Registered routes
- 🔴 M7RPKI: Valid ROAs for routes
- 🟢 M7RPKIN: Invalid routes
- 🟢 M8: Contact registration

Metrics radar for AS111111

- https://manrs.org/manrs-observatory/measurement-framework/

Use Case: Creating Alerts for routing status

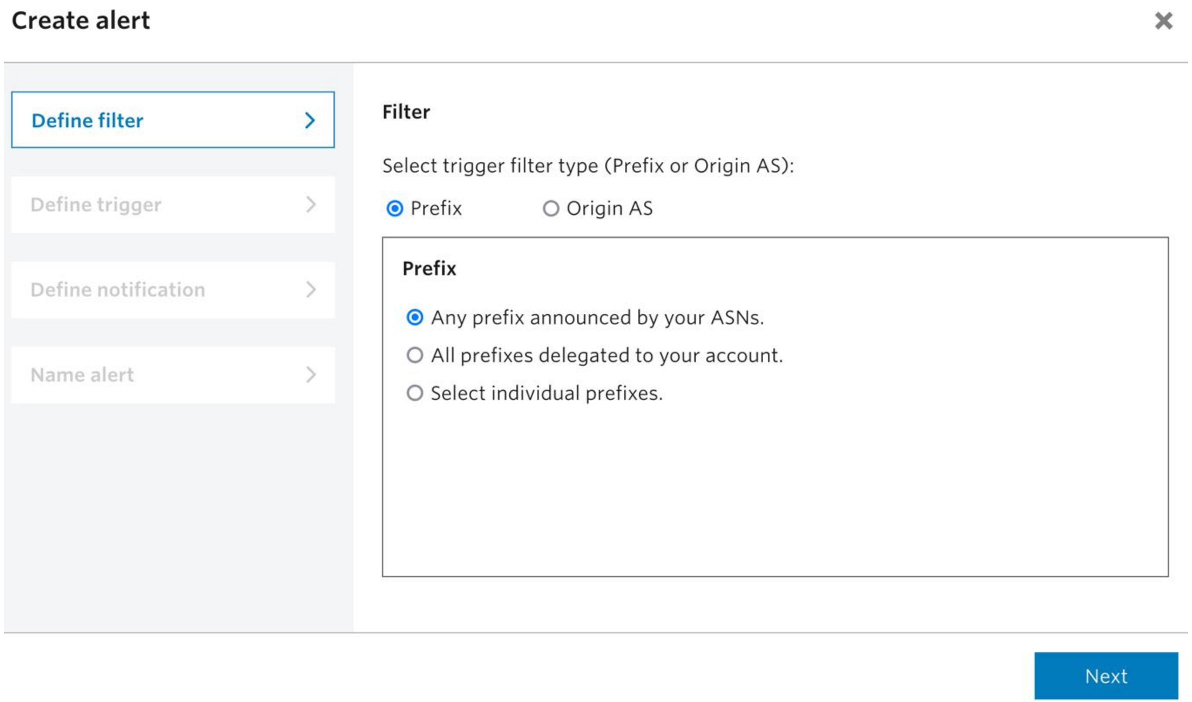


Alerts for routing status

Configure your alerts to track routing status mismatches and BGP events associated with your resources.

You do not have alerts yet for the selected member account.

Use Case: Creating Alerts for routing status



Create alert

Filter

Select trigger filter type (Prefix or Origin AS):

● Prefix ○ Origin AS

Prefix

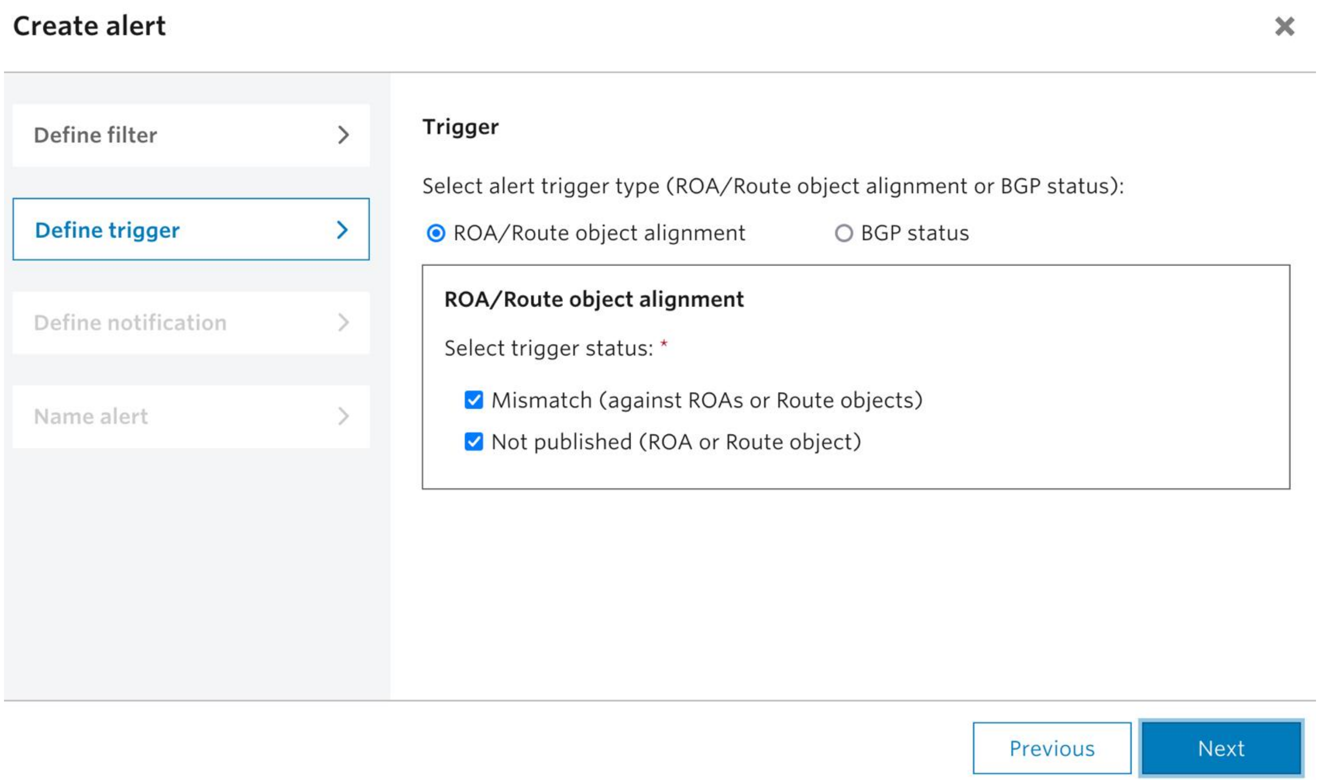
● Any prefix announced by your ASNs.

○ All prefixes delegated to your account.

○ Select individual prefixes.

- Alert for RPKI and IRR that doesn’t match BGP announcement

Use Case: Creating Alerts for routing status



Create alert

Trigger

Select alert trigger type (ROA/Route object alignment or BGP status):

● ROA/Route object alignment ○ BGP status

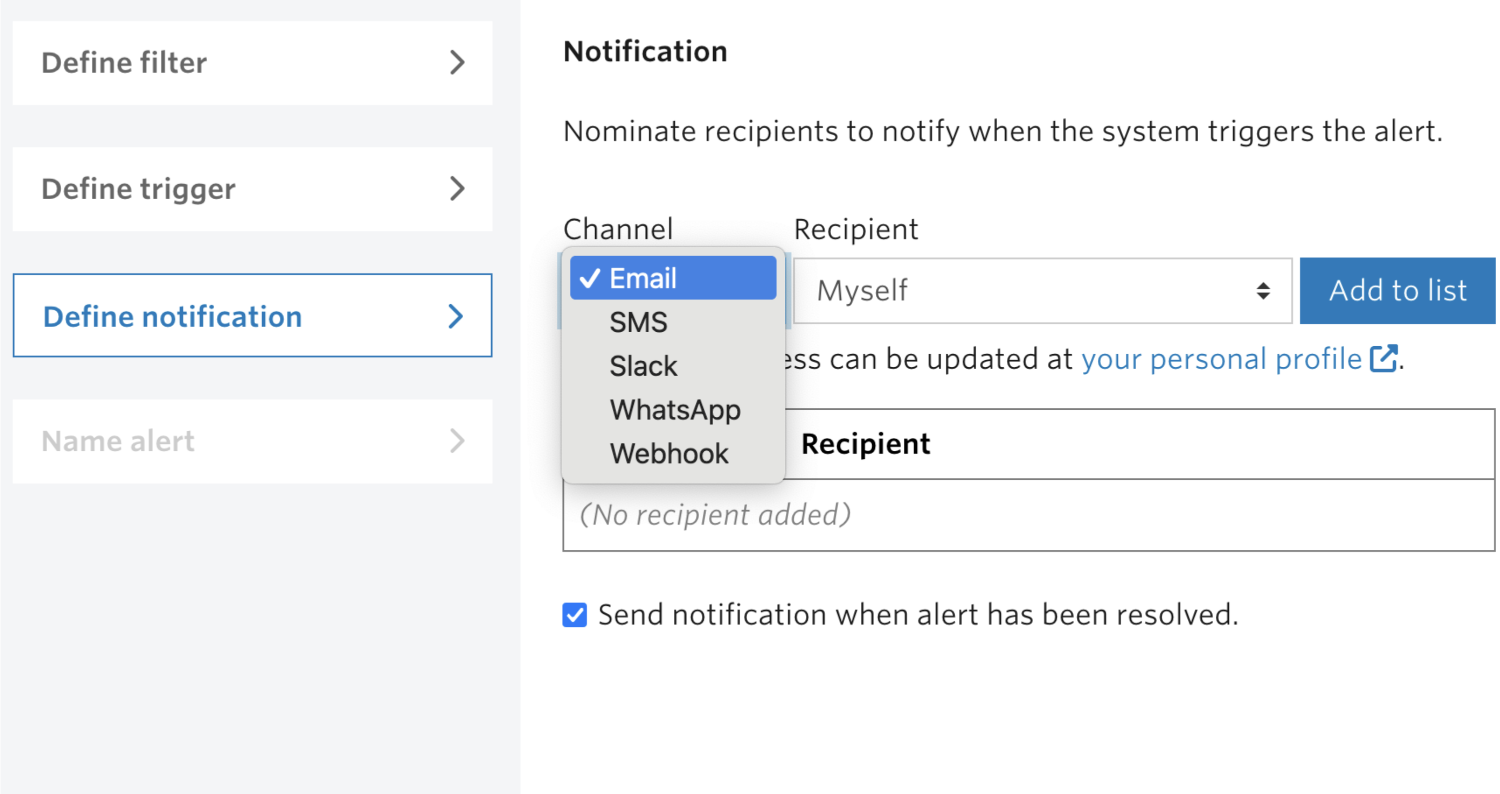
ROA/Route object alignment

Select trigger status: *

☑ Mismatch (against ROAs or Route objects)

☑ Not published (ROA or Route object)

Use Case: Creating Alerts for routing status



Notification

Nominate recipients to notify when the system triggers the alert.

Channel: ✓ Email

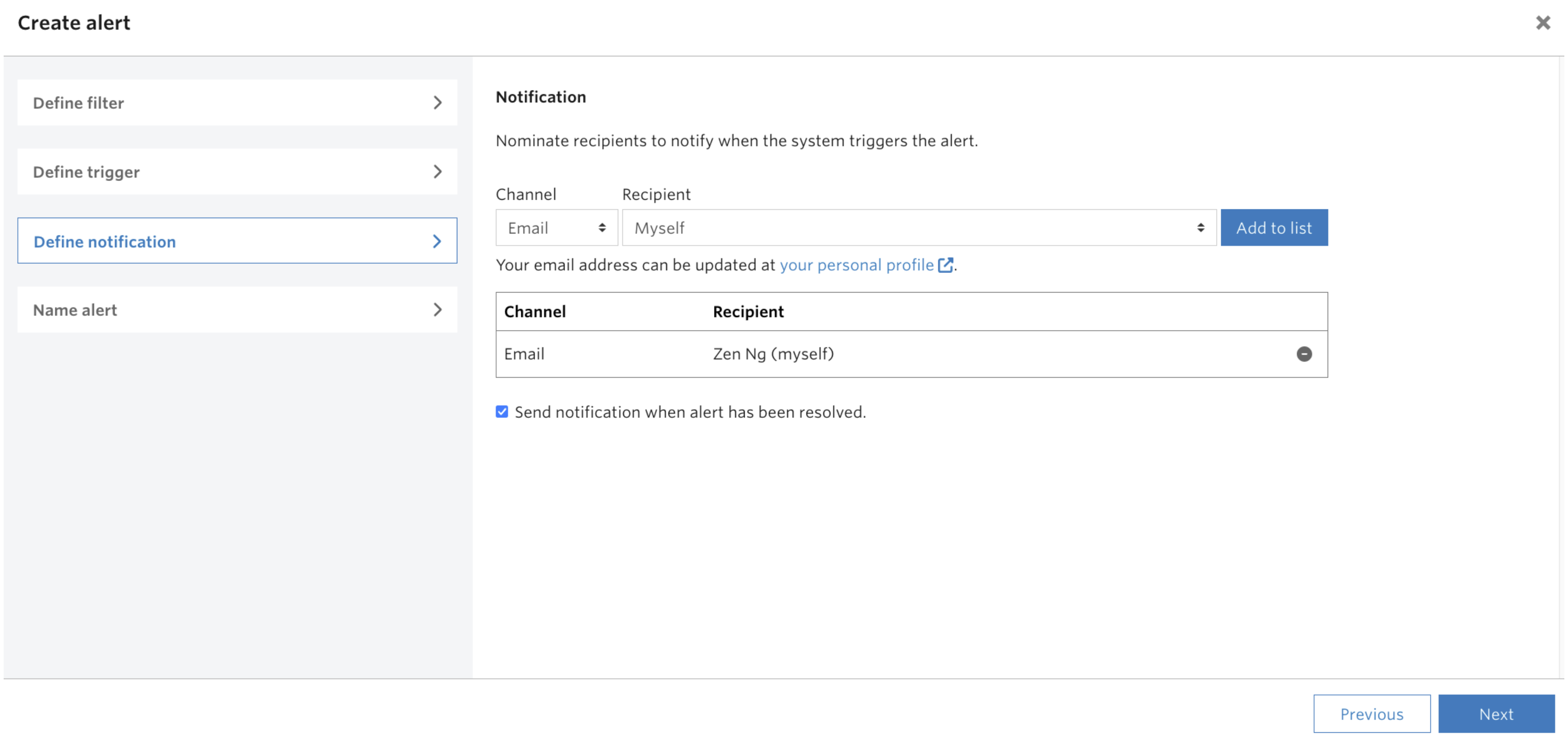
Recipient: Myself

ess can be updated at your personal profile.

	Recipient
(No recipient added)	

☑ Send notification when alert has been resolved.

Use Case: Creating Alerts for routing status



Create alert

Define filter

Define trigger

Define notification

Name alert

Notification

Nominate recipients to notify when the system triggers the alert.

Channel: Email

Recipient: Myself

Add to list

Your email address can be updated at your personal profile.

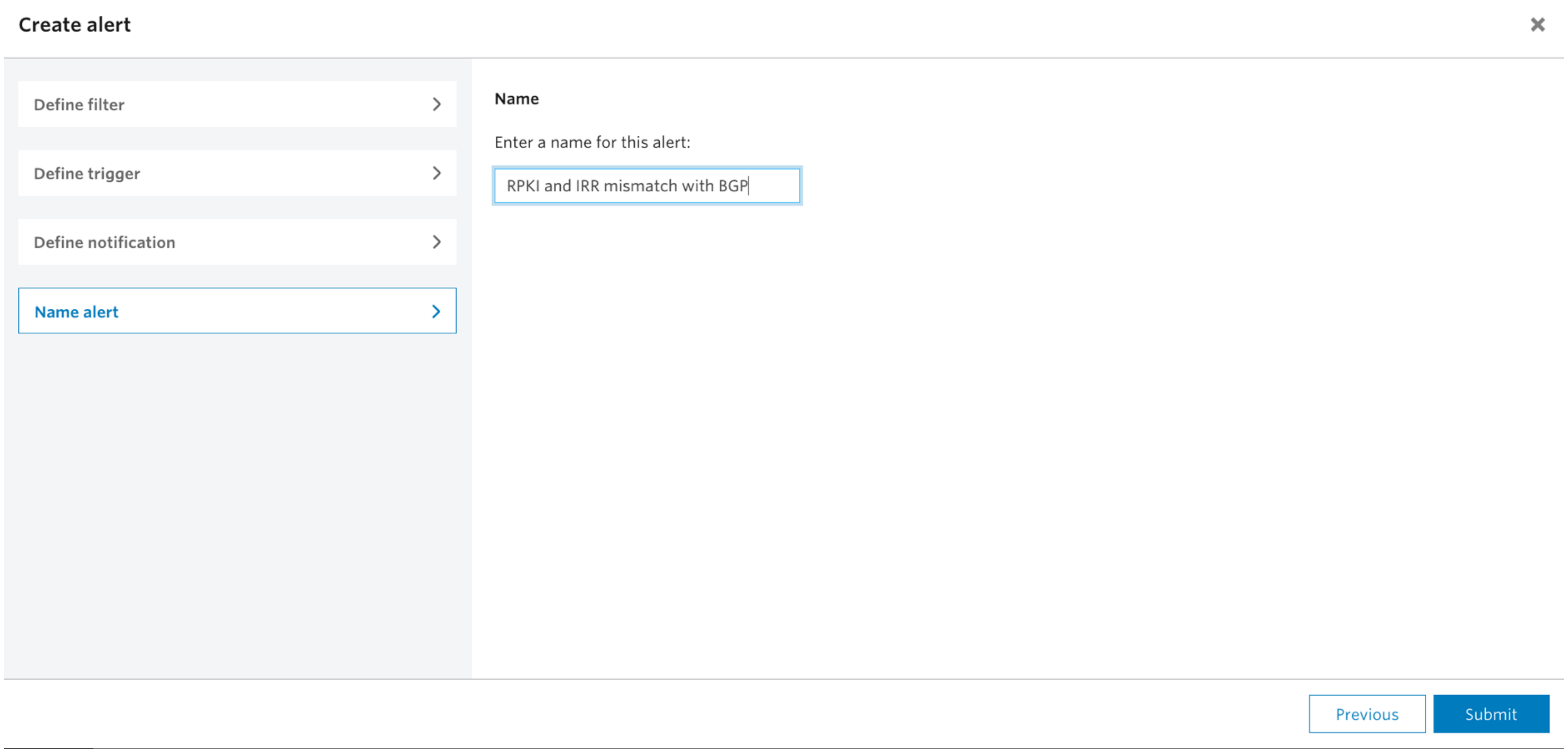
Channel	Recipient
Email	Zen Ng (myself)

☑ Send notification when alert has been resolved.

Previous

Next

Use Case: Creating Alerts for routing status



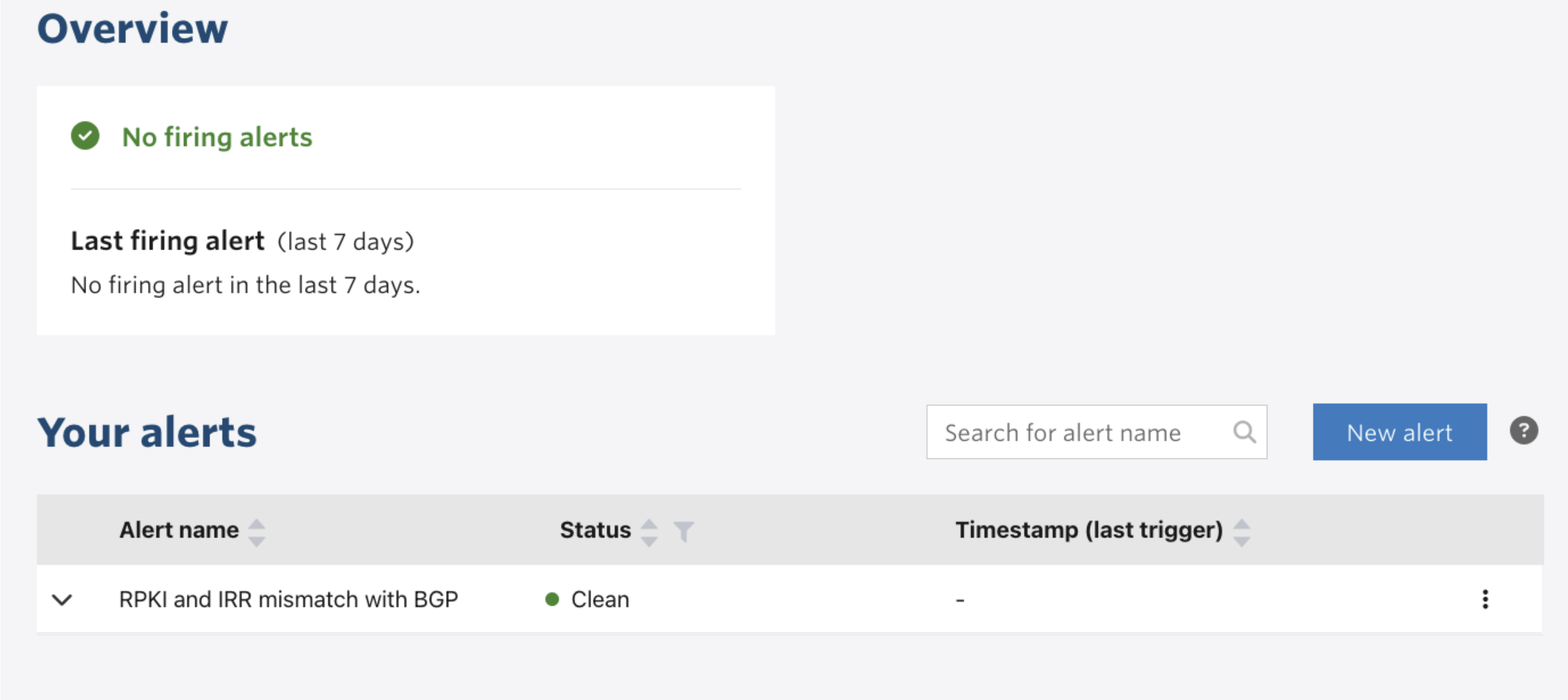
Create alert

Name

Enter a name for this alert:

RPKI and IRR mismatch with BGP

Use Case: Creating Alerts for routing status



Overview

✓ No firing alerts

Last firing alert (last 7 days)

No firing alert in the last 7 days.

Your alerts

	Alert name	Status	Timestamp (last trigger)
∨	RPKI and IRR mismatch with BGP	● Clean	-

Summary: What can you do with DASH?

- Monitor routing issues and suspicious traffic
- Track the status of ROA and IRR Route Objects for your network's BGP announcements.
- Generate reports about suspicious traffic originating from your network, economy and region.
- Evaluate your network's compliance with routing security best practices by checking MANRS readiness scores”
- It is FREE to all APNIC members!

Upcoming DASH improvements

- We will have a feature for BOGONS (RIR undelegated and reserved address)
- Visit dash.apnic.net and start create a stable and safe internet for everyone!

APRICOT 2025 – CfP open now

- The PC is looking for content for the conference and tutorial sessions and Peering Forum
- Deadline for submissions 27 Jan 2025

https://2025.apricot.net/programme/callforpresentations

Thank you!