Cleaning up your RPKI invalids

Jordan Previtera
Internet Resource Analyst
APNIC

What is RPKI?

A robust security framework for verifying the association between **resource holders** and their **Internet number resources**.

Route Origin Authorization

What is contained in a ROA?

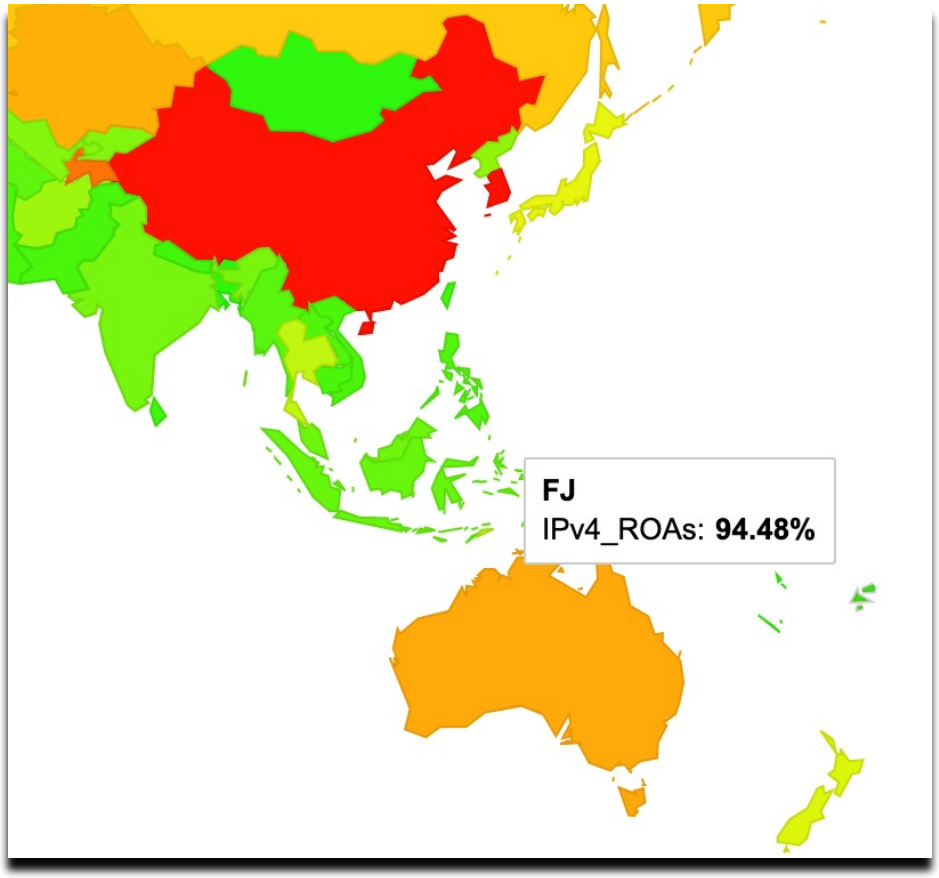
- The AS number you have authorized
- The prefix that is being originated from it
- The most specific prefix (maximum length) that the AS may announce

"For example: “ISP 4 permits AS65551 to originate a route for the prefix 198.51.100.0/24"

Route Origin Validation

- Valid
  - The prefix (prefix length) and AS pair found in the database
- Invalid
  - Prefix is found, but origin-AS is wrong, OR
  - The prefix length is longer than the maximum length

ROA uptake



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

Route Origin Validation

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
Vodafone	transit	signed + filtering	safe
RETN	transit	partially signed + filtering	safe
Orange	transit	signed + filtering	safe
Telstra International	transit	signed + filtering	safe
Telefonica/Telxius	transit	signed + filtering	safe
Comcast	ISP	signed + filtering	safe
AT&T	ISP	signed + filtering	safe
Verizon	ISP	signed + filtering	safe
Liberty Global	transit	signed + filtering	safe
Cloudflare	cloud	signed + filtering	safe
Microsoft	cloud	signed + filtering	safe
Amazon	cloud	signed + filtering	safe
Netflix	cloud	signed + filtering	safe
Wikimedia Foundation	cloud	signed + filtering	safe
Scaleway	cloud	signed + filtering	safe
Google	cloud	signed	partially safe
DigitalOcean	cloud	filtering peers only	partially safe

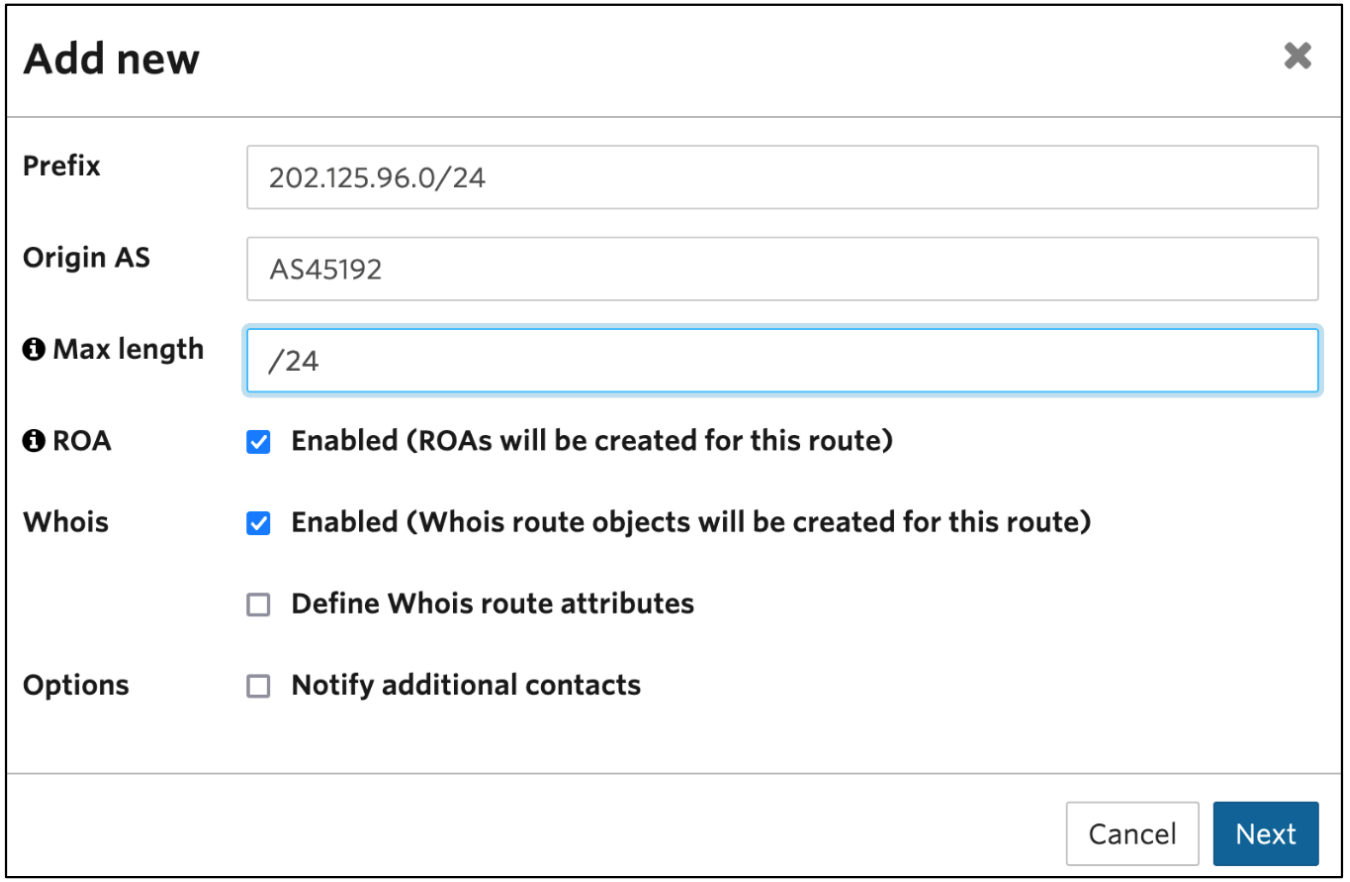
https://isbgpsafeyet.com/

RPKI invalids

Validation result	IPv4 count
Invalid origin ASN	126
Invalid origin ASN and Max Length	42
Invalid Max Length	860

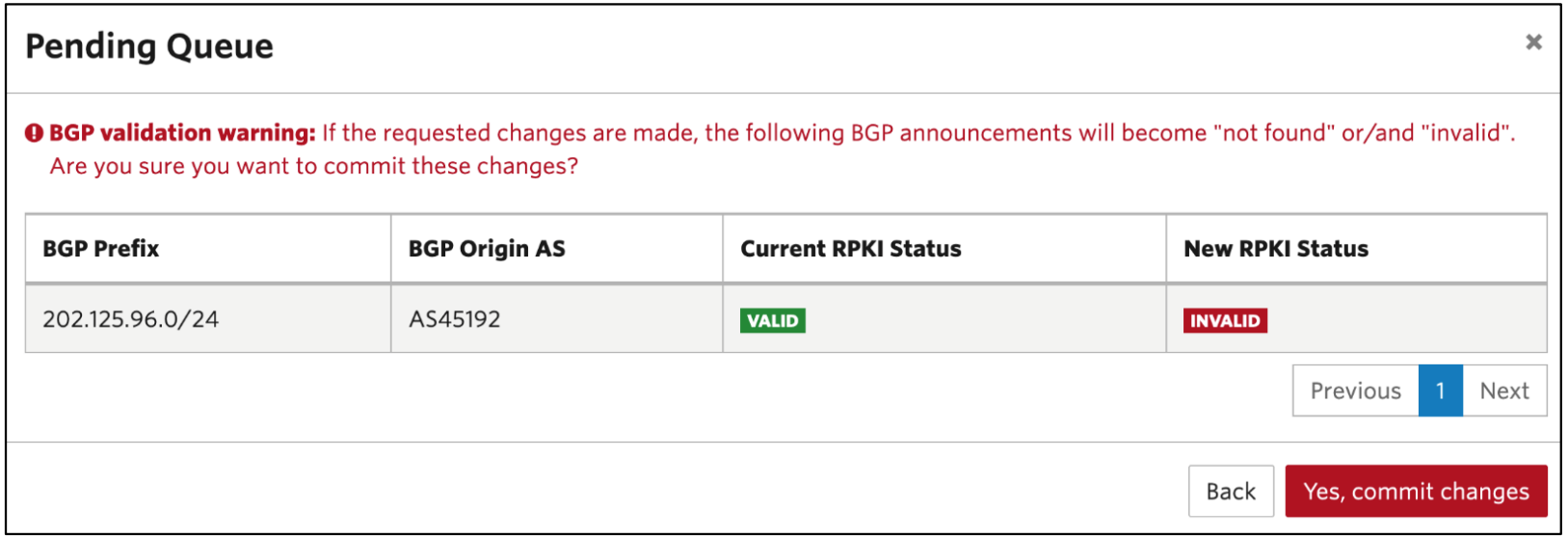
Routeviews collector SG and Routunator

ROA Prevalidation

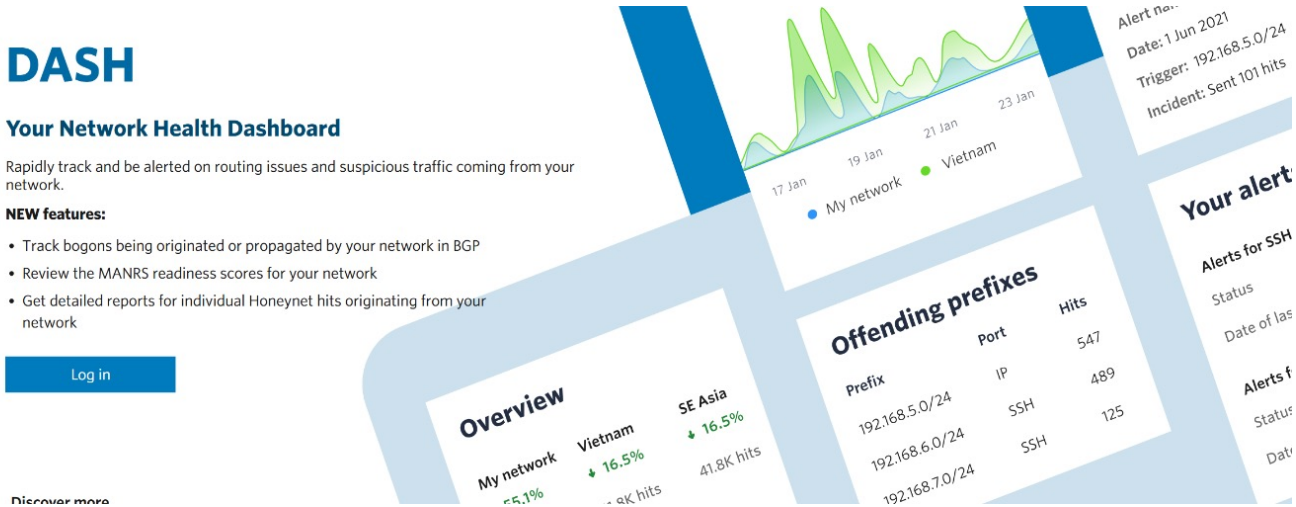


ROA Prevalidation

- Validate changes submitted via MyAPNIC to ensure that they won’t cause problems in BGP
- Allows Members to override if necessary

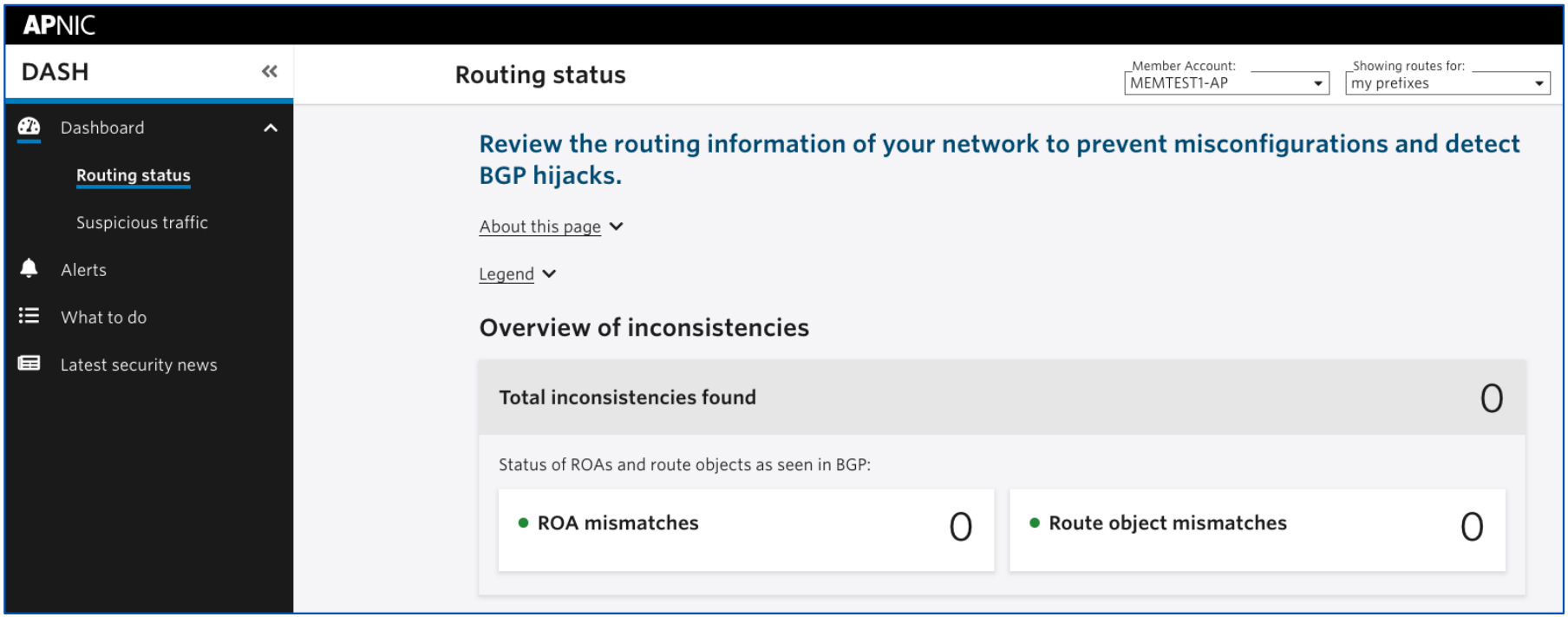


Improved DASH interface



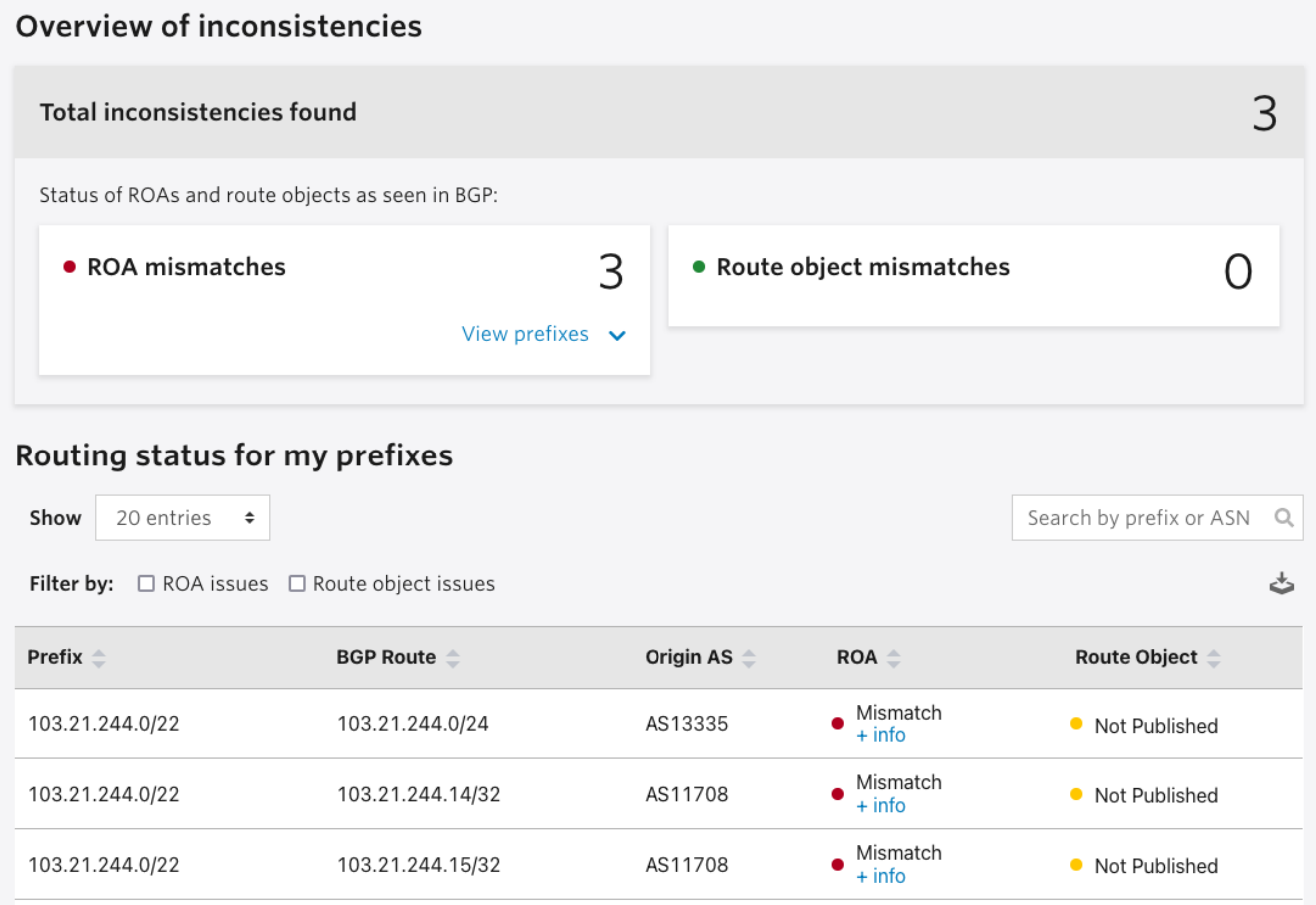
- An online portal for APNIC Members who can login through MyAPNIC or dash.apnic.net
- Implemented for suspicious traffic alerts
- Rapidly track and be alerted on routing issues and suspicious traffic on your network
- Compare your organization against your economy or sub-region
- Generate reports for informed decision-making
- Available for all APNIC Members

Routing status alerts in DASH



- RPKI ROA mismatches will show on this screen
- Could be for all your prefixes or the announcements you have from your ASN
- DASH will compare these against RPKI and IRR to find misalignments between these
- For this example, none of the prefixes associated with this account have any ROA mismatches or route object mismatches

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

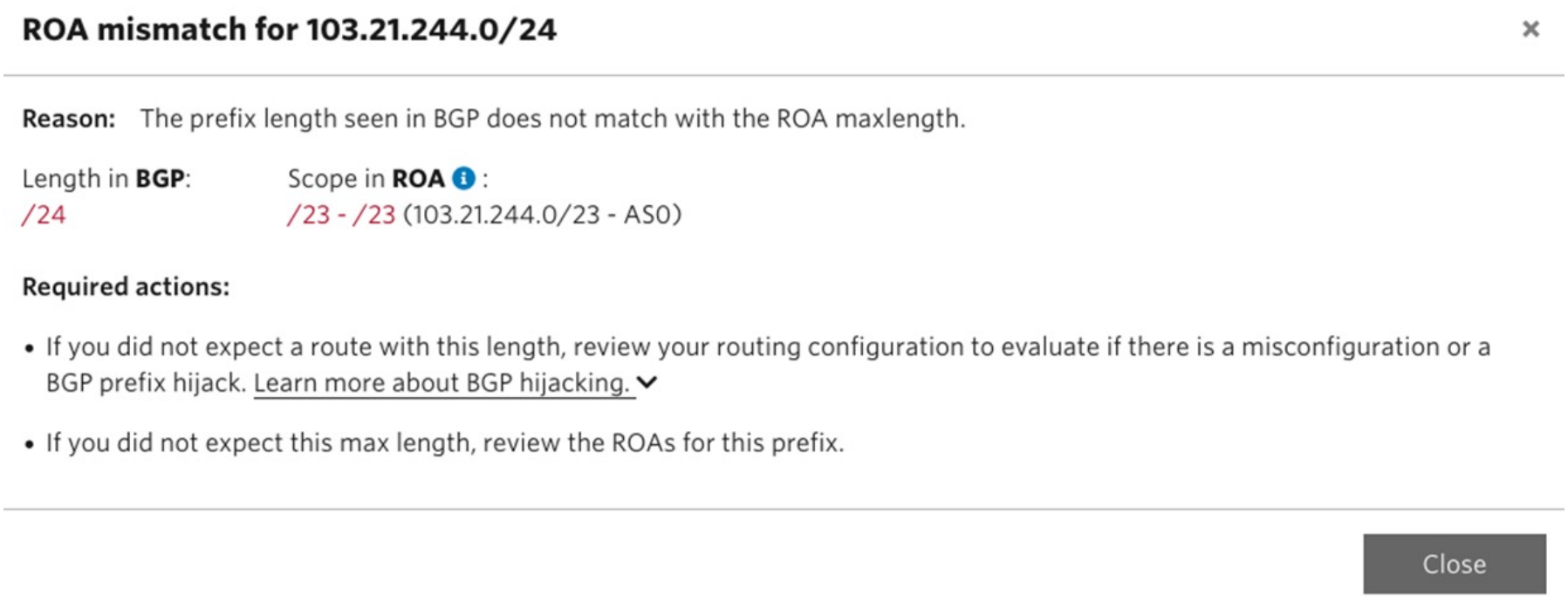
Show 20 entries — Search by prefix or ASN

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

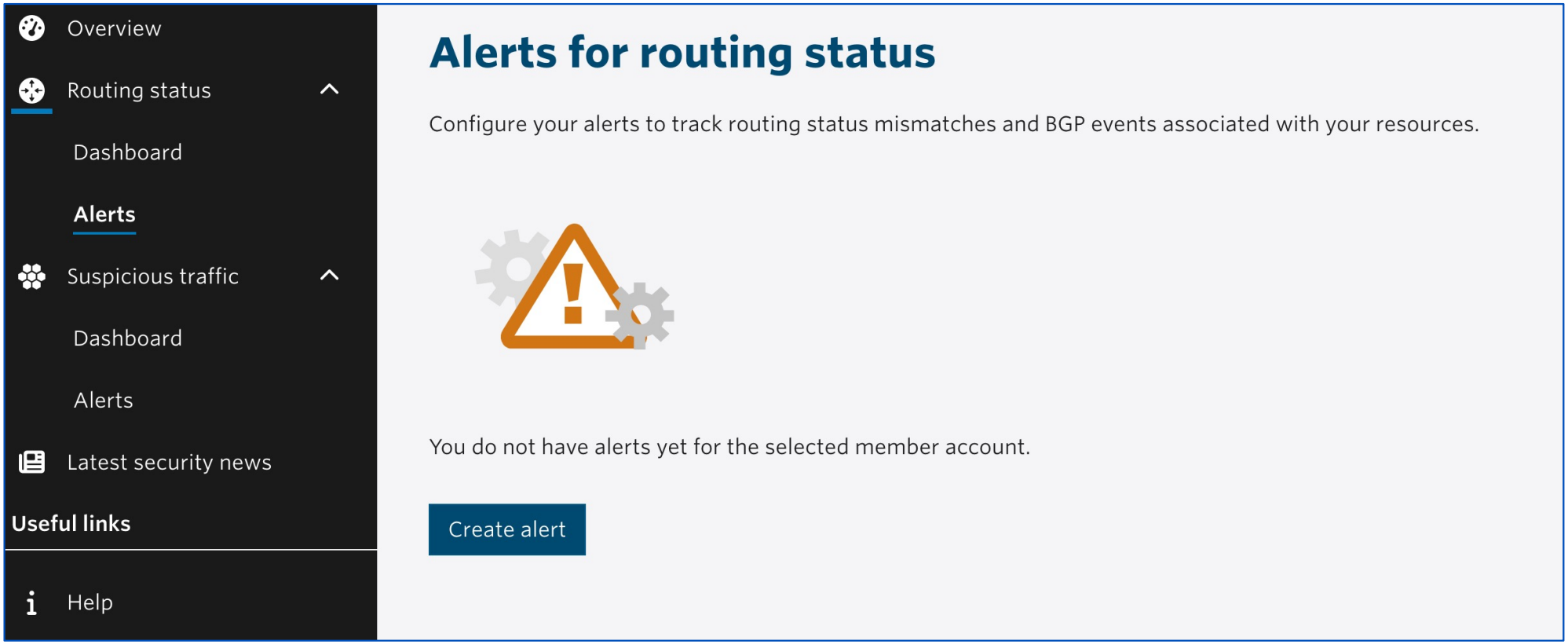
https://dash.apnic.net/

Routing status alerts in DASH

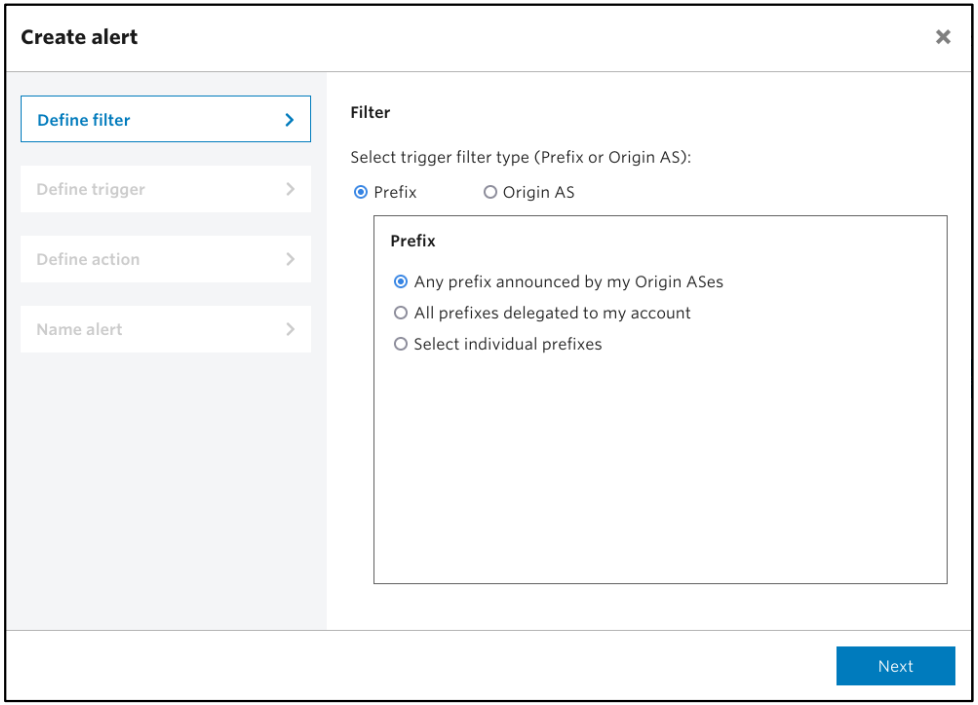


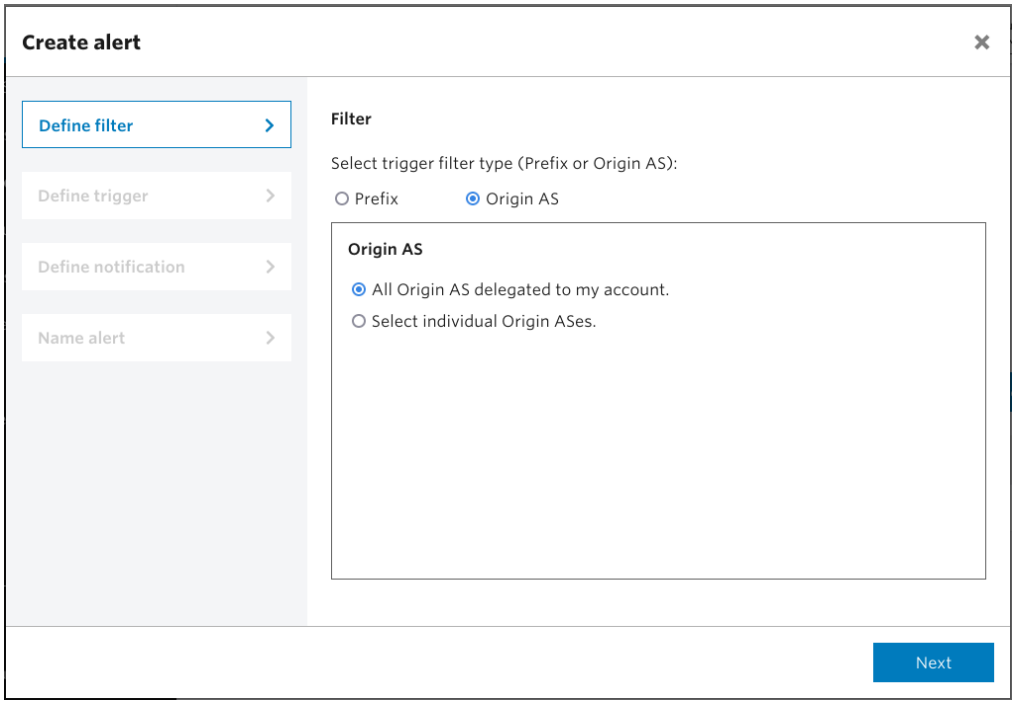
https://dash.apnic.net/

Alerts for routing status in DASH

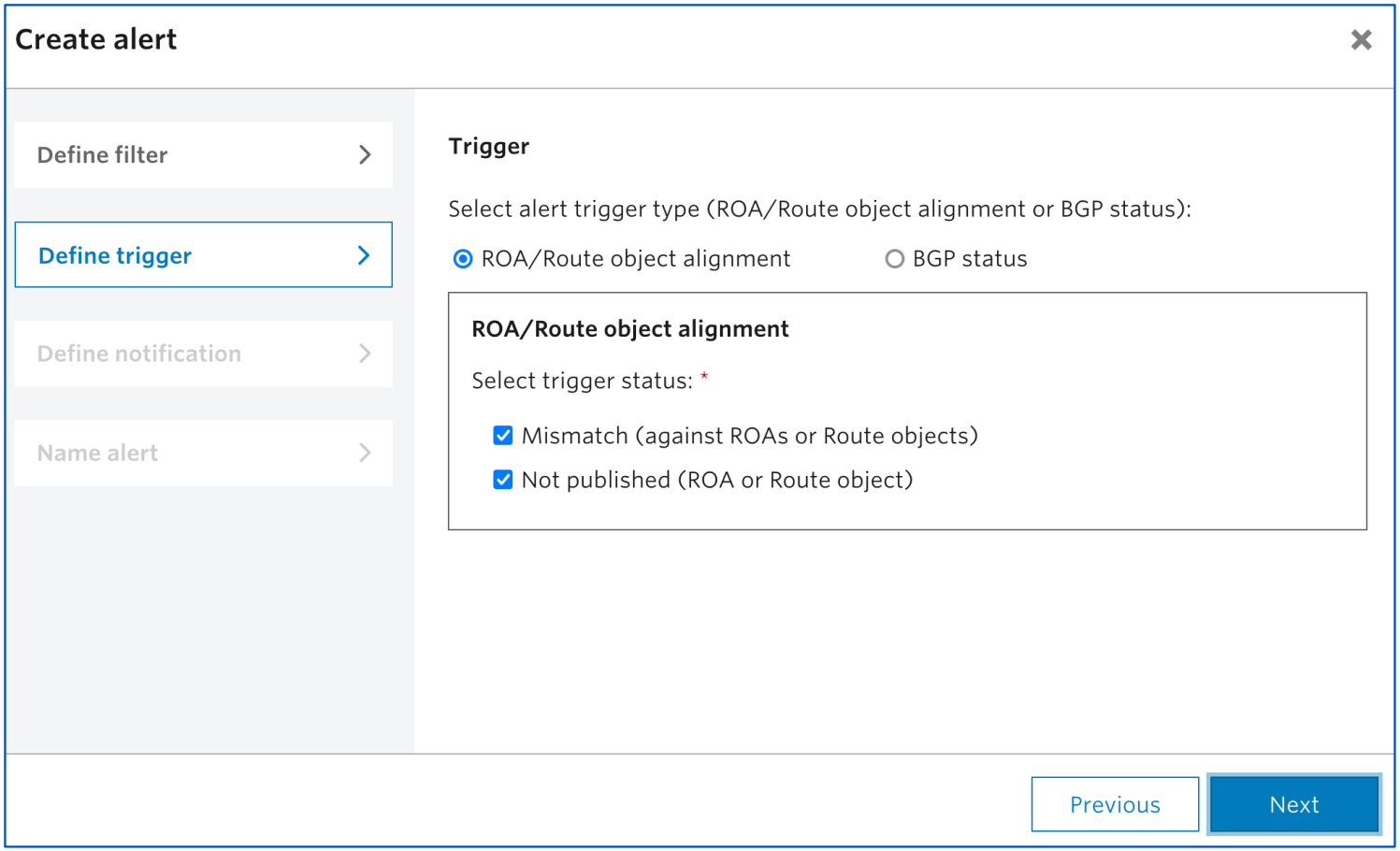


ROA alert filters in DASH

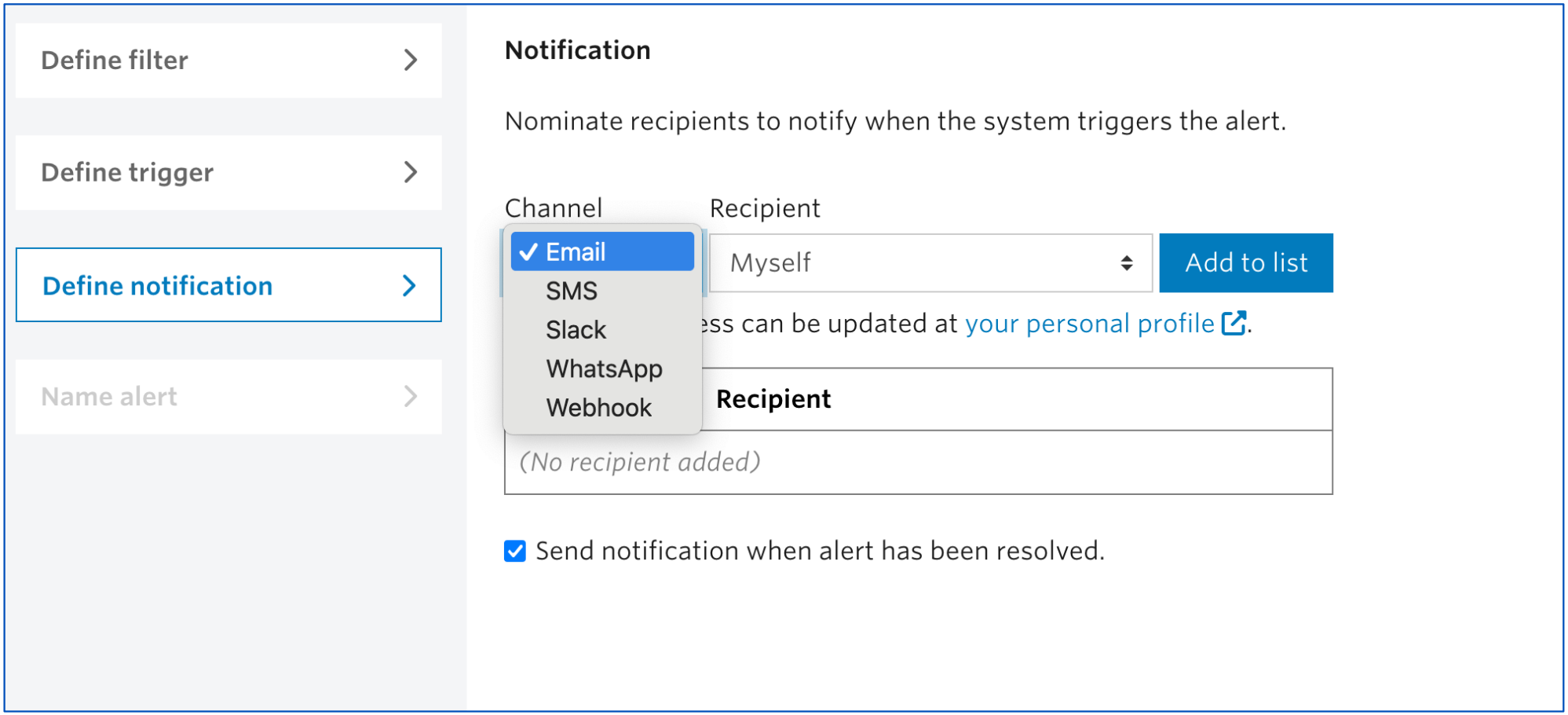




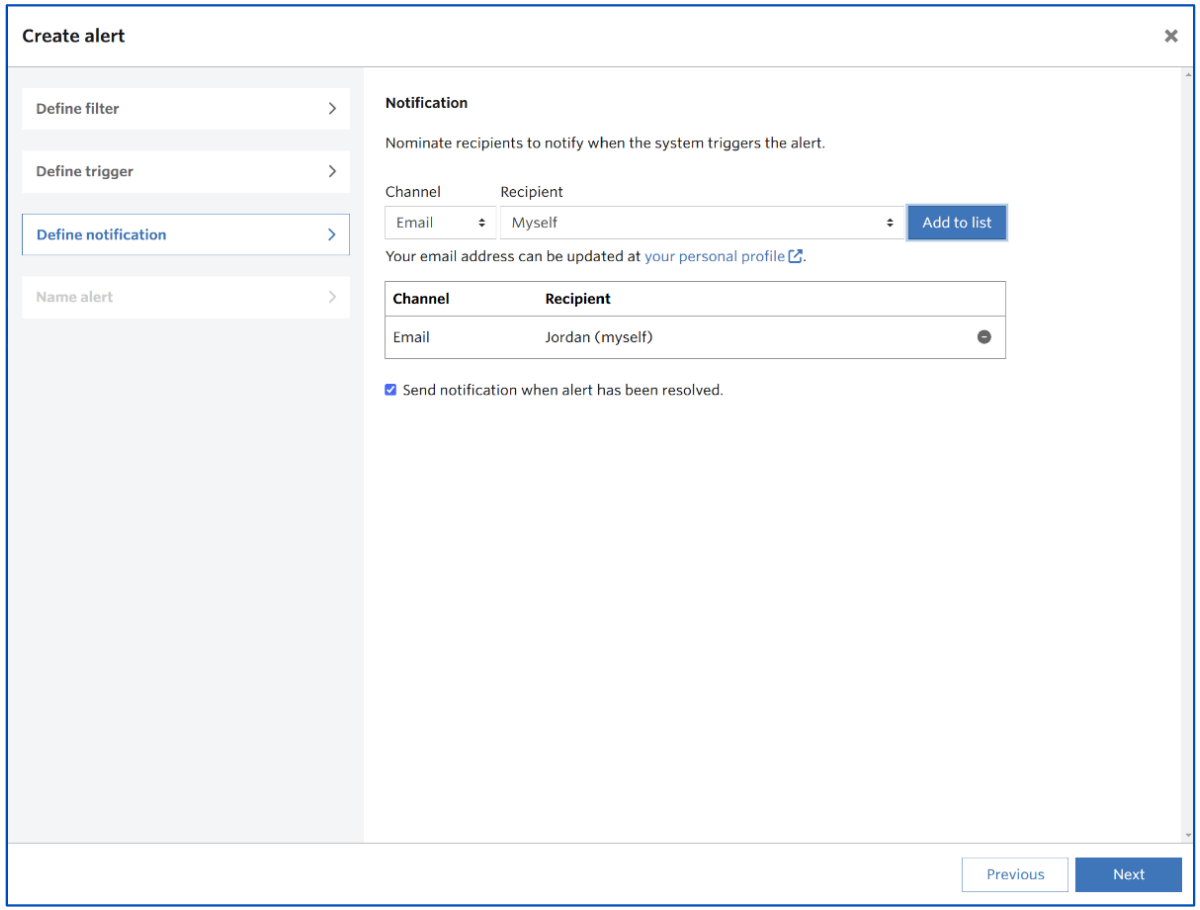
Alerts creation in DASH



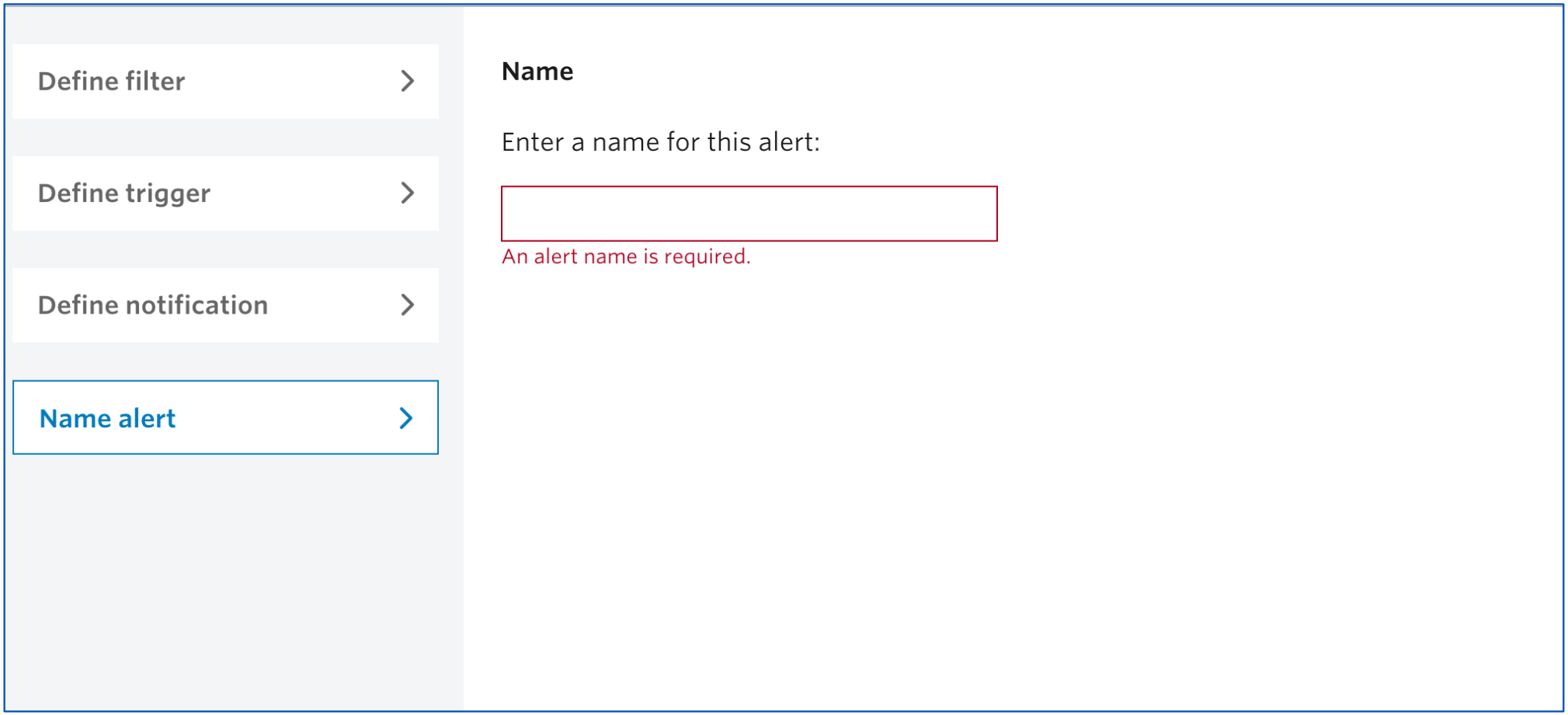
Alerts creation in DASH

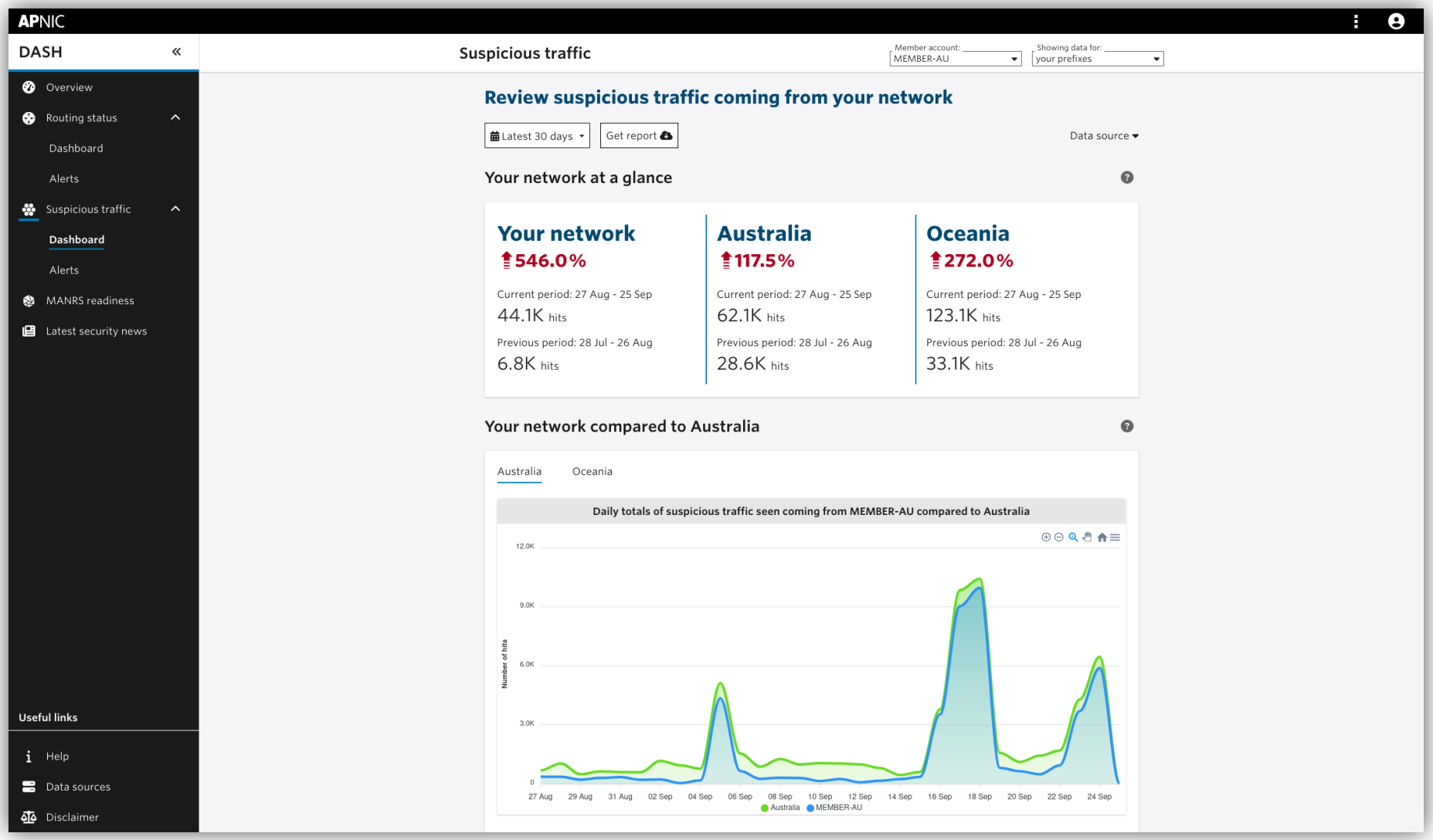


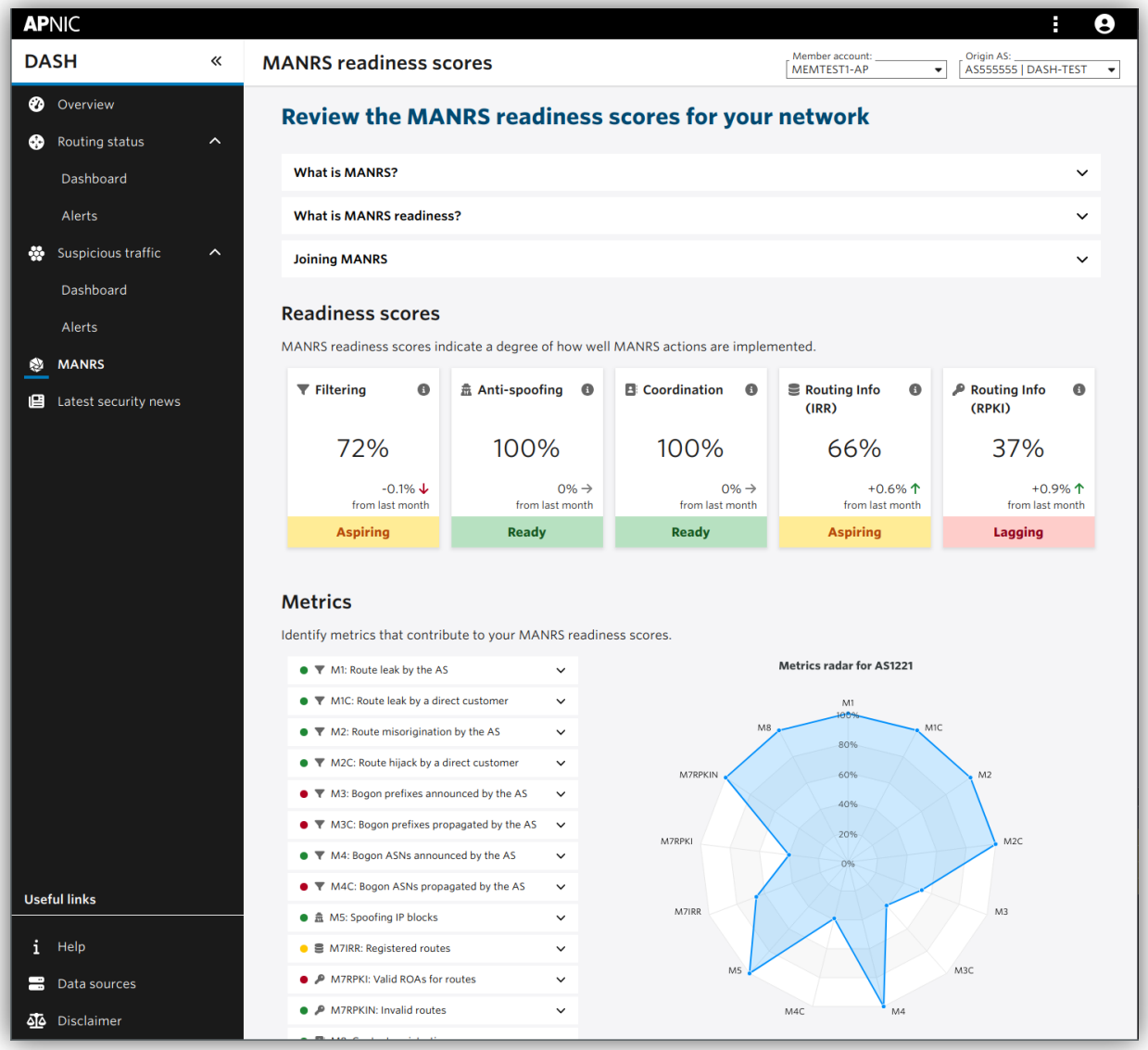
Alerts creation in DASH



Alerts creation in DASH




APNIC
DASH
Overview
Routing status
Dashboard
Alerts
Suspicious traffic
Dashboard
Alerts
MANRS readiness
Latest security news
Useful links
Help
Data sources
Disclaimer
Suspicious traffic
Member account:
MEMBER-AU
Showing data for:
your prefixes
Review suspicious traffic coming from your network
Latest 30 days
Get report
Data source
Your network at a glance
Your network
546.0%
Current period: 27 Aug - 25 Sep
44.1K hits
Previous period: 28 Jul - 26 Aug
6.8K hits
Australia
117.5%
Current period: 27 Aug - 25 Sep
62.1K hits
Previous period: 28 Jul - 26 Aug
28.6K hits
Oceania
272.0%
Current period: 27 Aug - 25 Sep
123.1K hits
Previous period: 28 Jul - 26 Aug
33.1K hits
Your network compared to Australia
Australia
Oceania
Daily totals of suspicious traffic seen coming from MEMBER-AU compared to Australia
12.0K
9.0K
6.0K
3.0K
0
Number of hits
27 Aug
29 Aug
31 Aug
02 Sep
04 Sep
06 Sep
08 Sep
10 Sep
12 Sep
14 Sep
16 Sep
18 Sep
20 Sep
22 Sep
24 Sep
Australia
MEMBER-AU


APNIC
DASH
MANRS readiness scores
Member account:
MEMTEST1-AP
Origin AS:
AS555555 | DASH-TEST
Overview
Routing status
Dashboard
Alerts
Suspicious traffic
Dashboard
Alerts
MANRS
Latest security news
Useful links
Help
Data sources
Disclaimer
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
72%
-0.1% ↓
from last month
Aspiring
Anti-spoofing
100%
0% →
from last month
Ready
Coordination
100%
0% →
from last month
Ready
Routing Info (IRR)
66%
+0.6% ↑
from last month
Aspiring
Routing Info (RPKI)
37%
+0.9% ↑
from last month
Lagging
Metrics
Identify metrics that contribute to your MANRS readiness scores.
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
Metrics radar for AS1221
M1
M1C
M2
M2C
M3
M3C
M4
M4C
M5
M7IRR
M7RPKI
M7RPKIN
M8
100%
80%
60%
40%
20%
0%

Thank you!