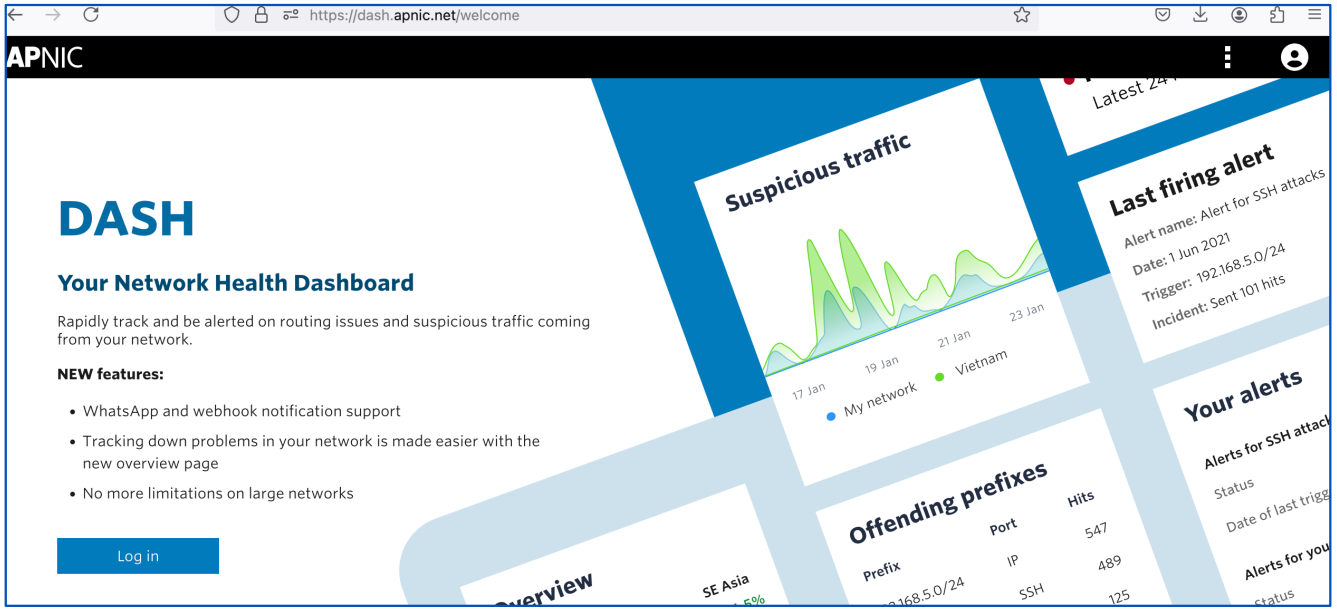
DASH

PacNOG 34

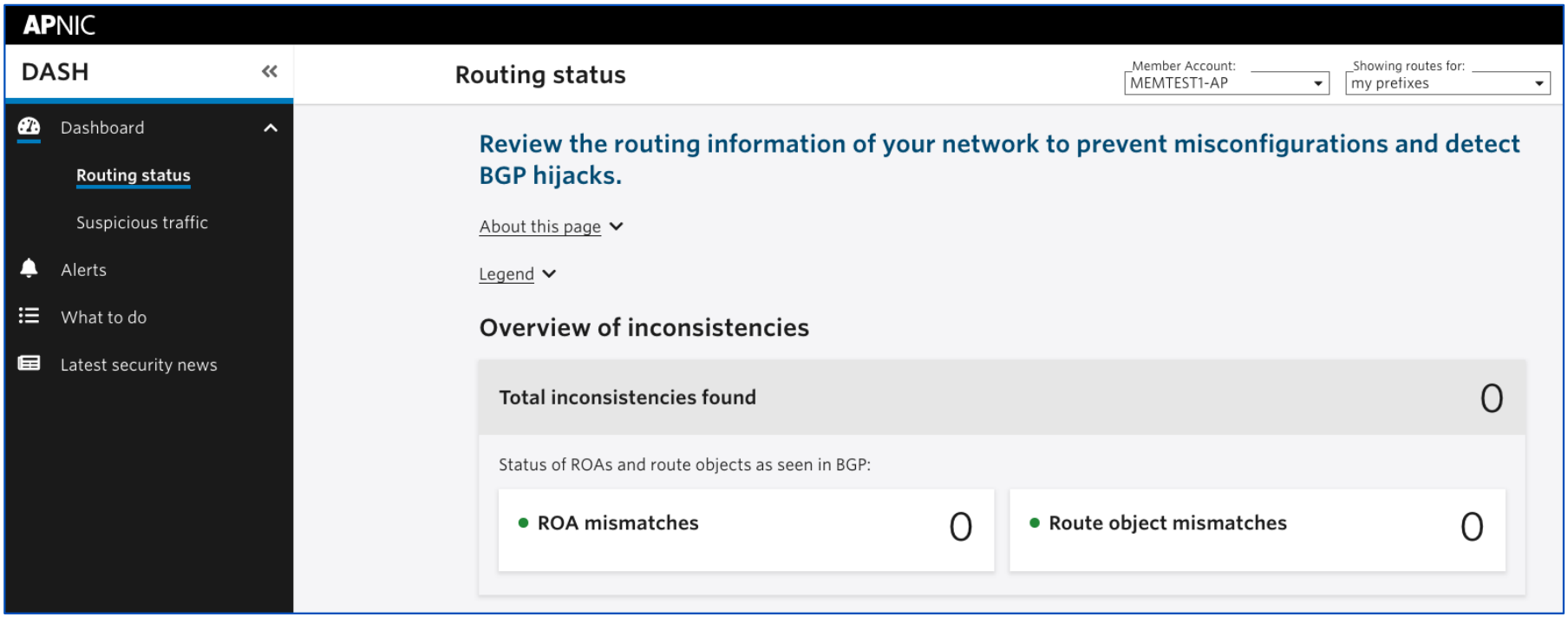
jordan.previtera@apnic.net

Improved DASH interface



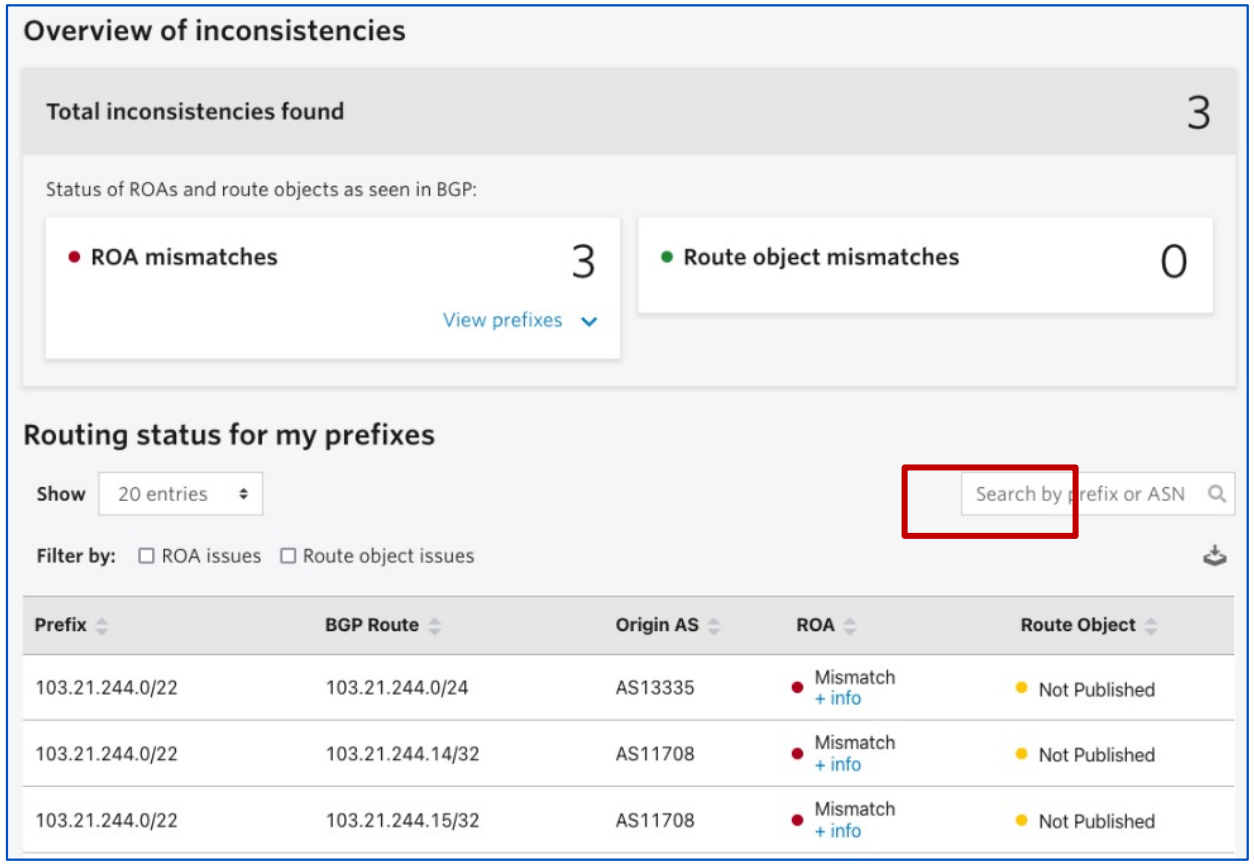
- An online portal for APNIC Members who can login through MyAPNIC or dash.apnic.net
- Implemented for suspicious traffic alerts
- Rapidly track and be alerted on routing issues and suspicious traffic on your network
- Compare your organization against your economy or sub-region
- Generate reports for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



- If you are using ROAS and some of them have caused RPKI invalids this is what it will look like
- Shows 3 mismatches for ROAS
- They are routing it as a /24 using origin AS13335 but the ROA created does not match this announcement
- This account intentionally set up this invalid for measuring purposes to see which networks accept this announcement

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**:	Scope in **ROA** :
/24	/23 - /23 (103.21.244.0/23 - AS0)

Required actions:

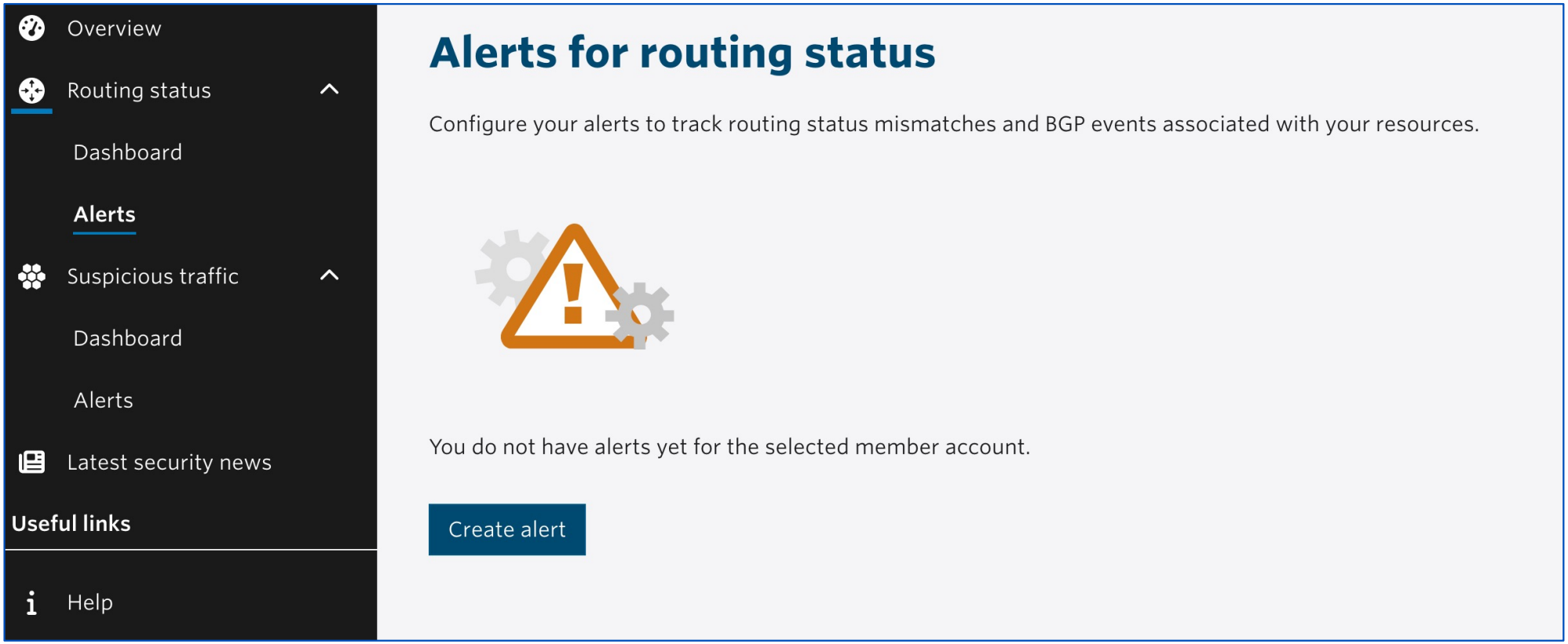
- If you did not expect a route with this length, review your routing configuration to evaluate if there is a misconfiguration or a BGP prefix hijack. Learn more about BGP hijacking.
- If you did not expect this max length, review the ROAs for this prefix.

Close

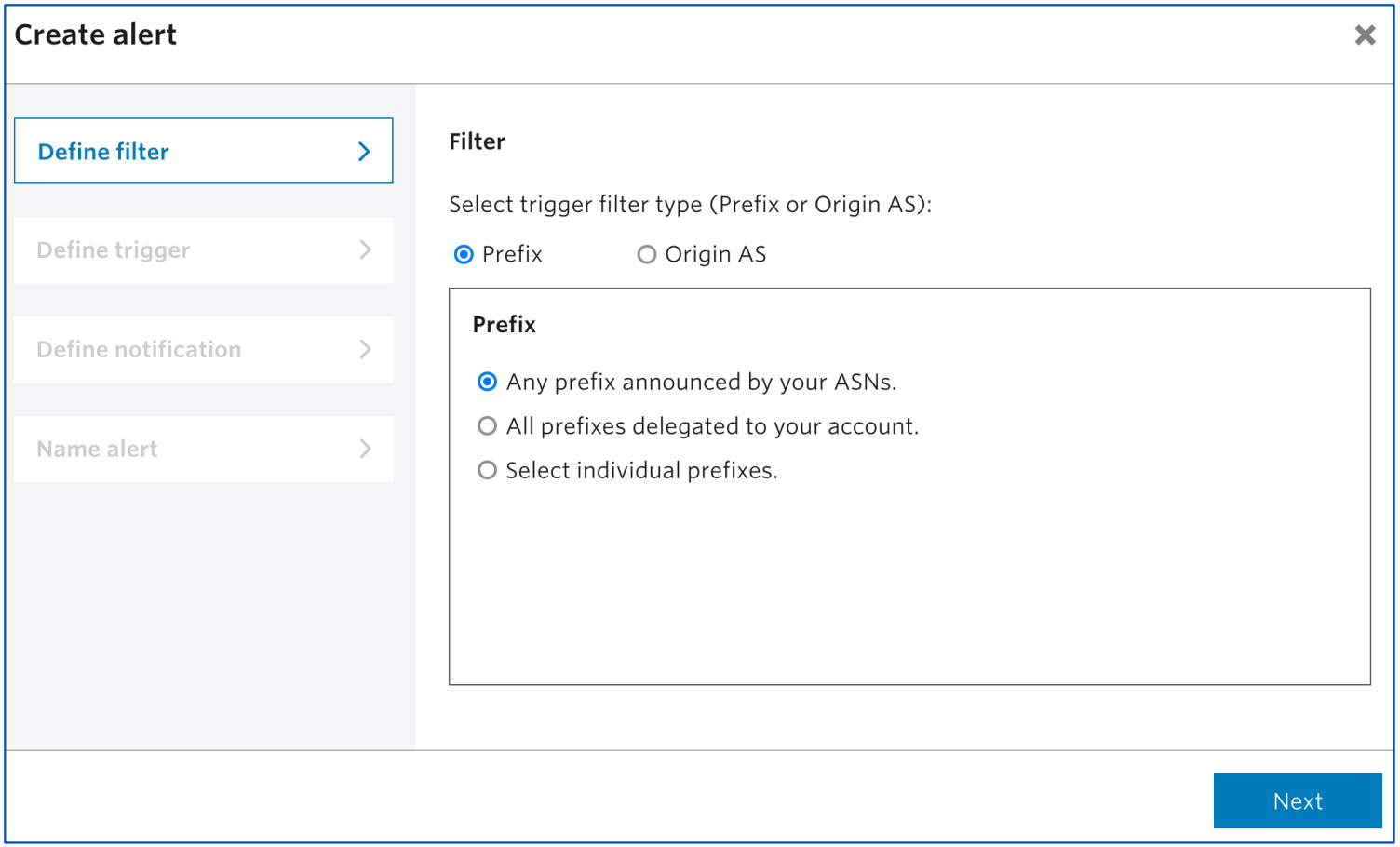
What are the types of alerts for this?

- BGP route not exist
- RPKI/ROA mismatch with BGP prefix length in BGP vs ROA record
- BGP hijacking

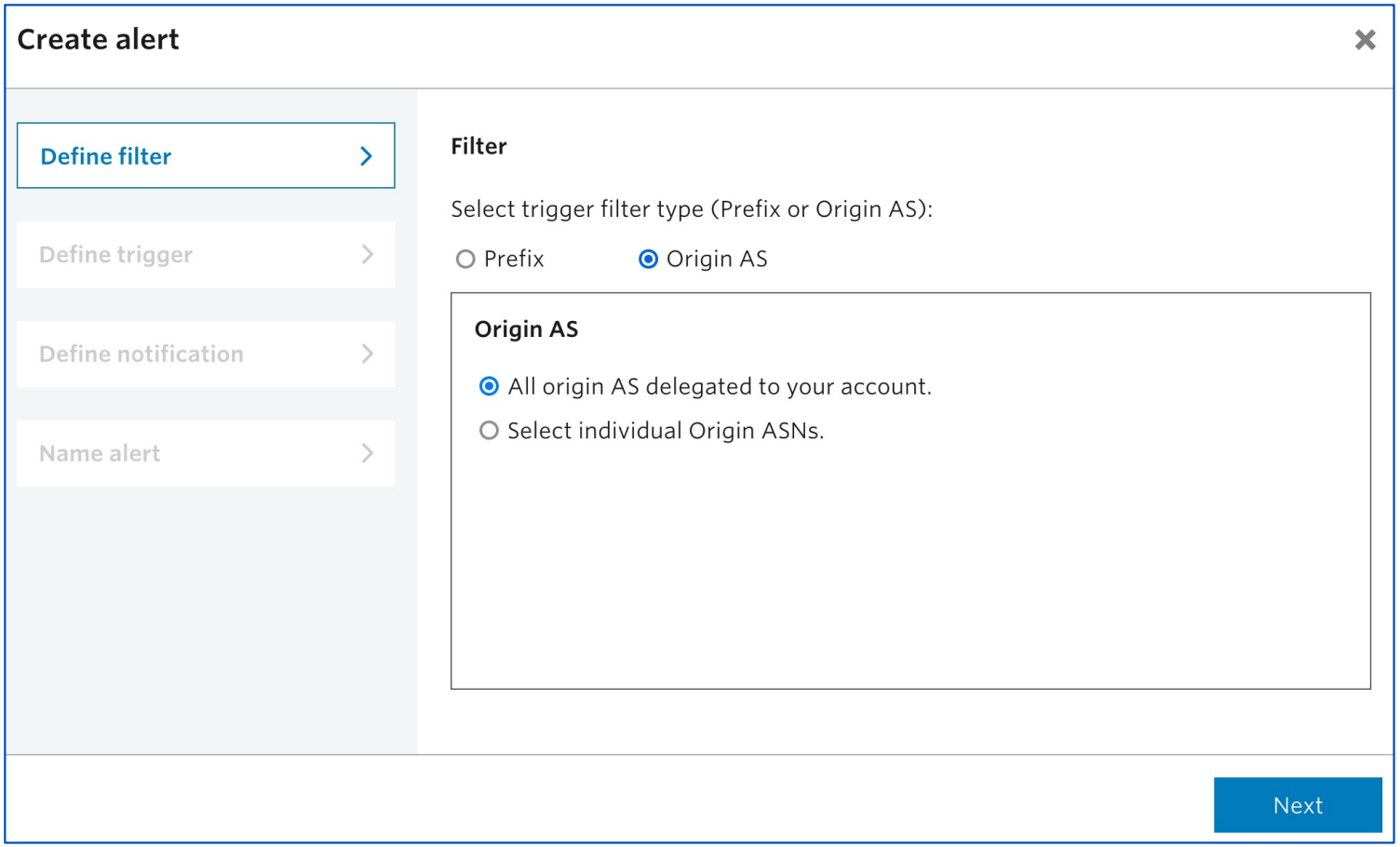
Alerts for routing status in DASH



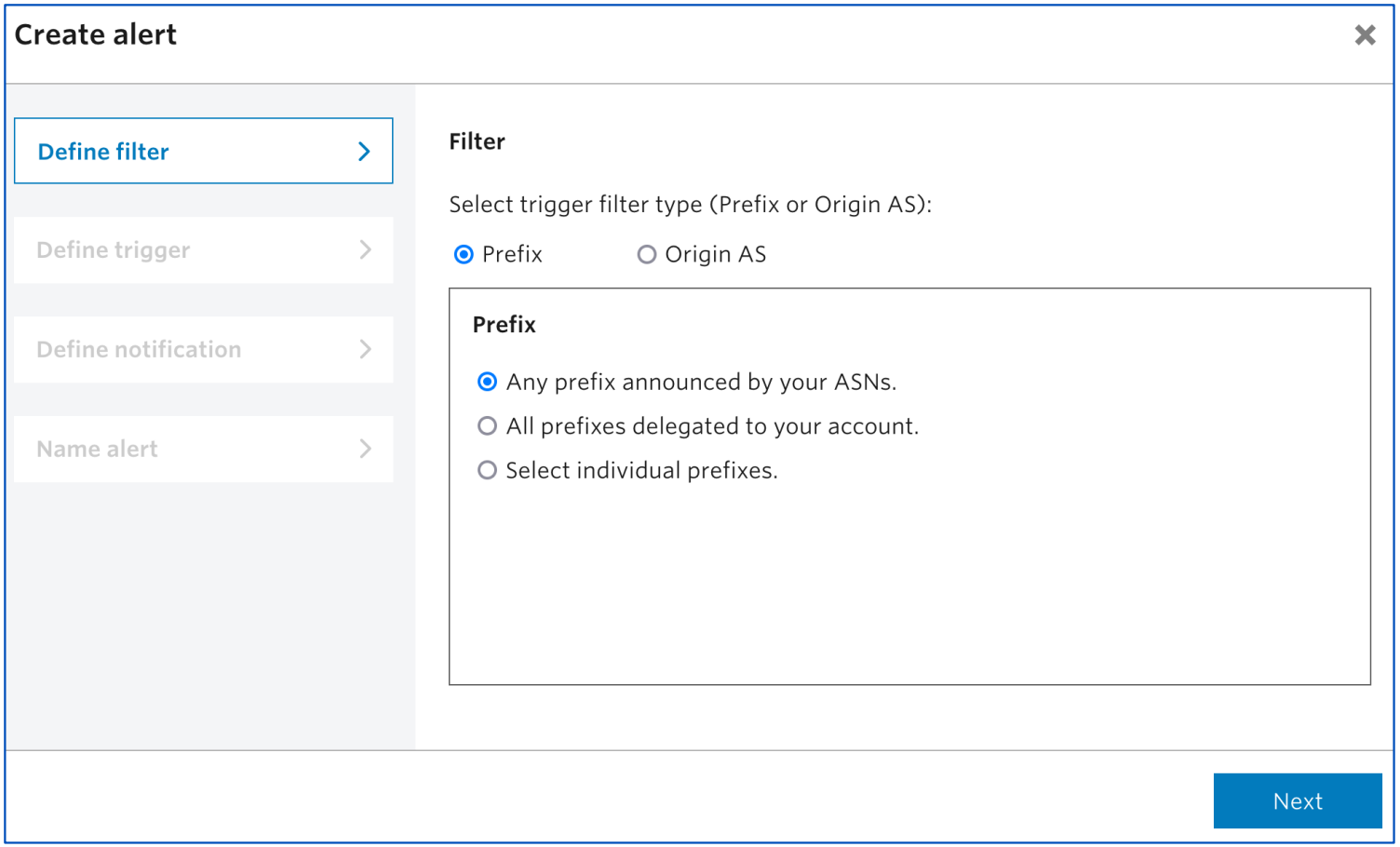
Alerts creation in DASH



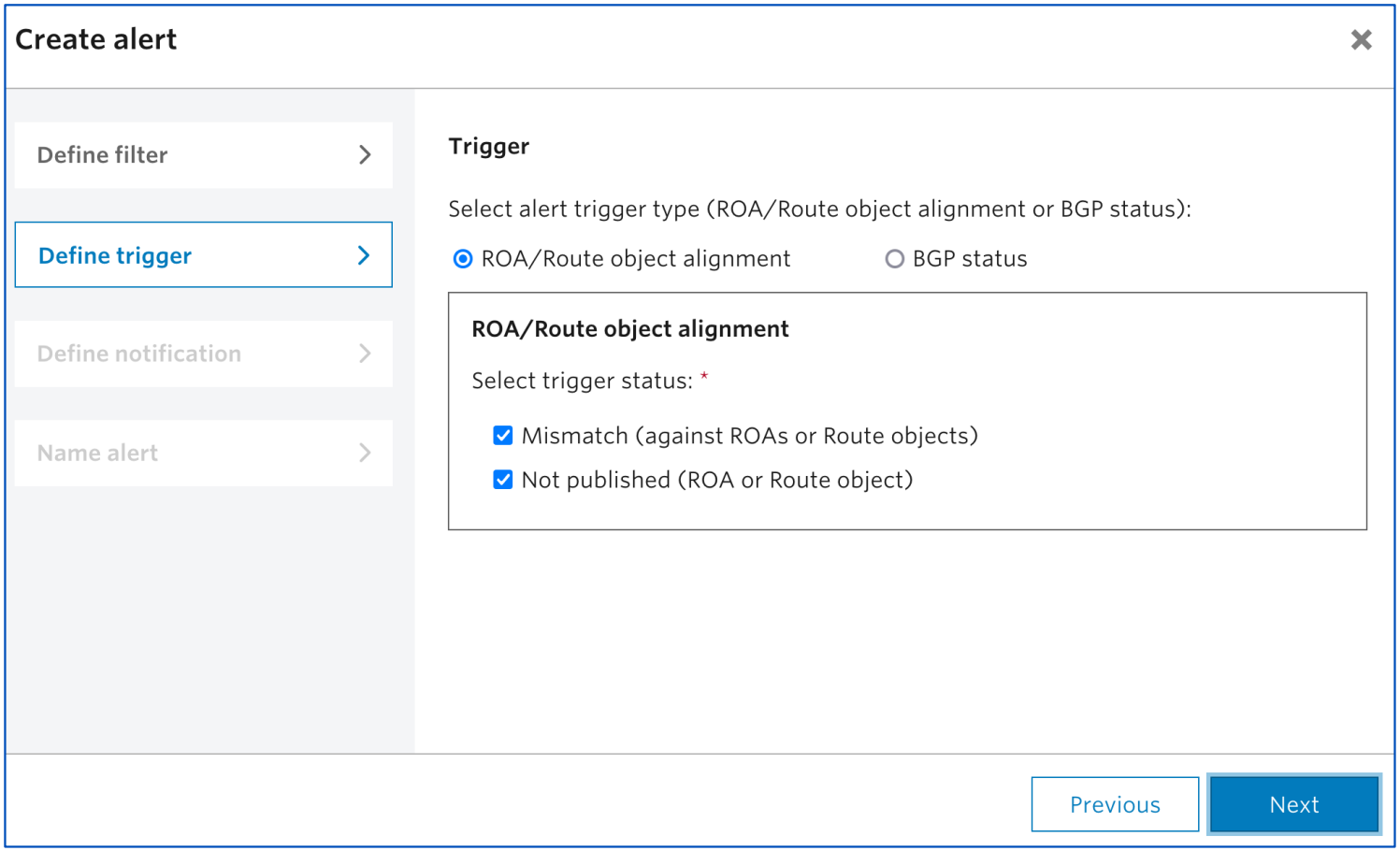
Alerts creation in DASH



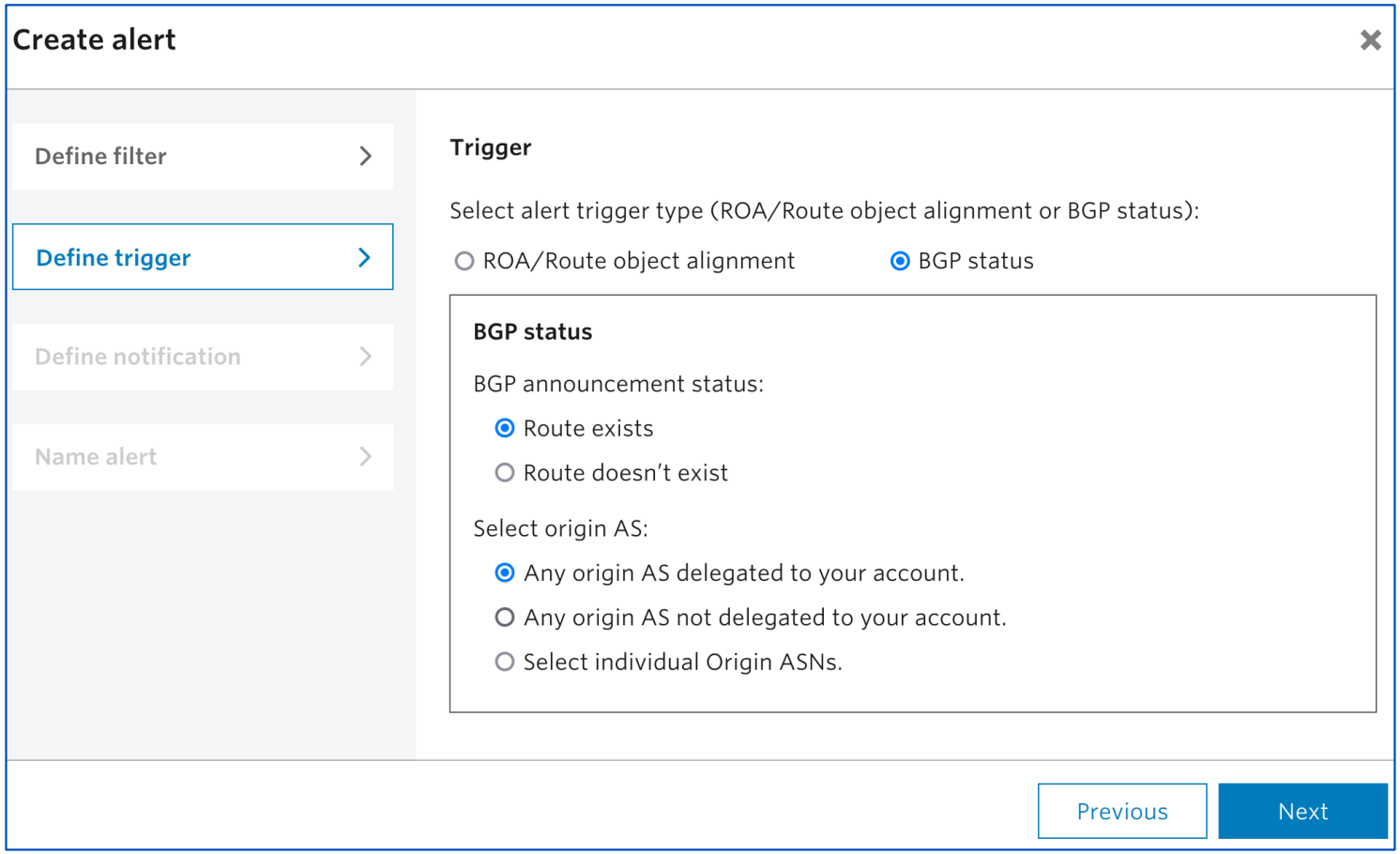
Alerts creation in DASH



Alerts creation in DASH



Alerts creation in DASH



Alerts creation in DASH

Define filter

Define trigger

Define notification

Name alert

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

- ○ ROA/Route object alignment
- ◉ BGP status

BGP status

BGP announcement status:

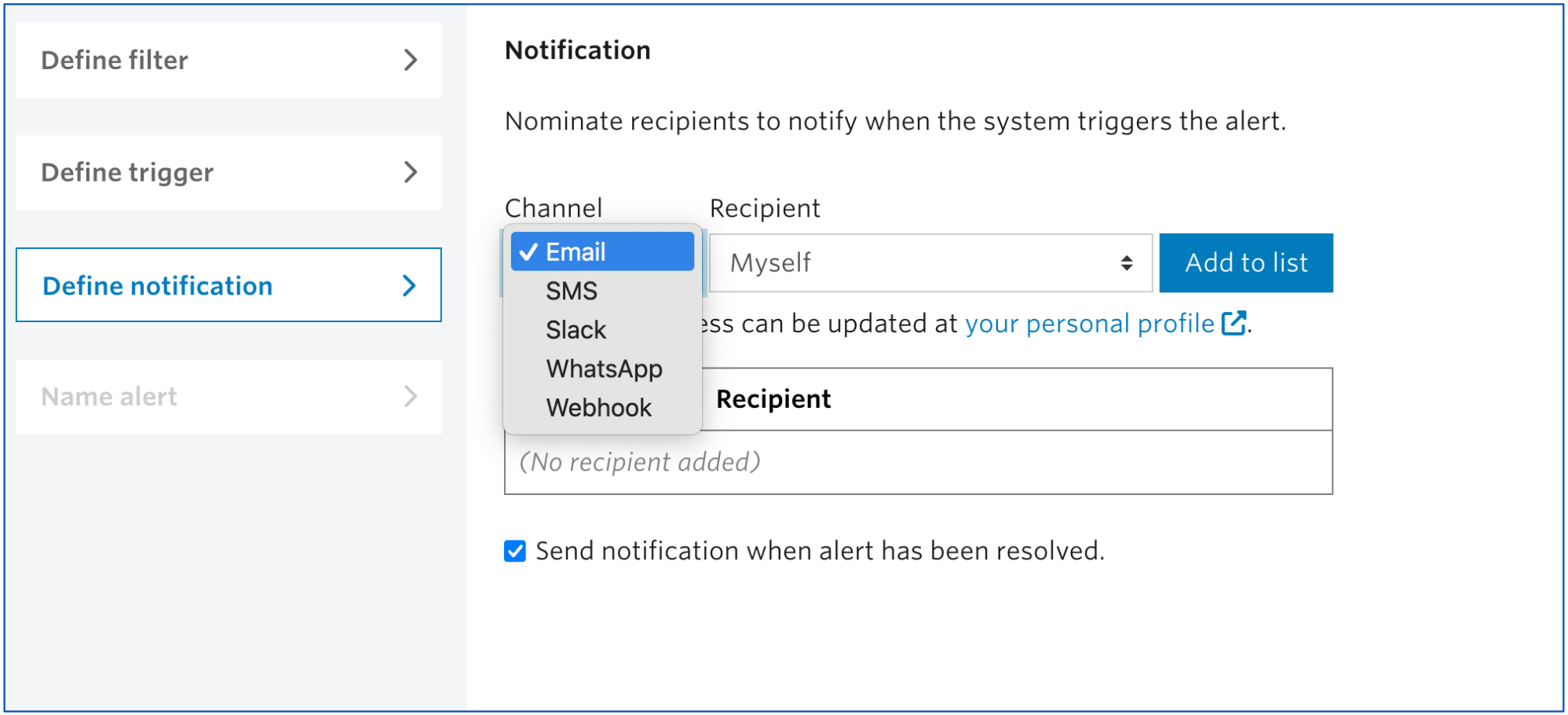
- ◉ Route exists
- ○ Route doesn't exist

Select origin AS:

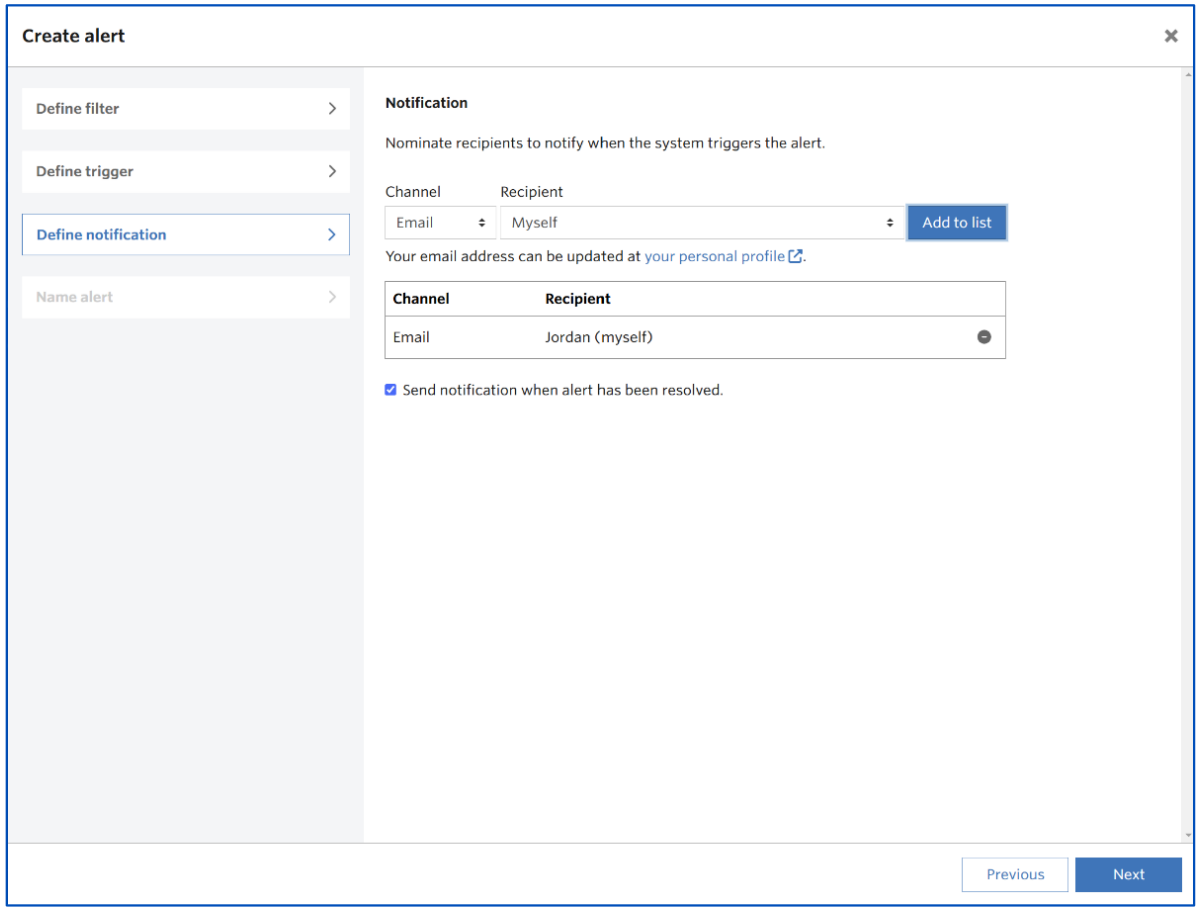
- ○ Any origin AS delegated to your account.
- ○ Any origin AS not delegated to your account.
- ◉ Select individual Origin ASNs.

460 Add

Alerts creation in DASH



Alerts creation in DASH



Alerts creation in DASH

Define filter >

Define trigger >

Define notification >

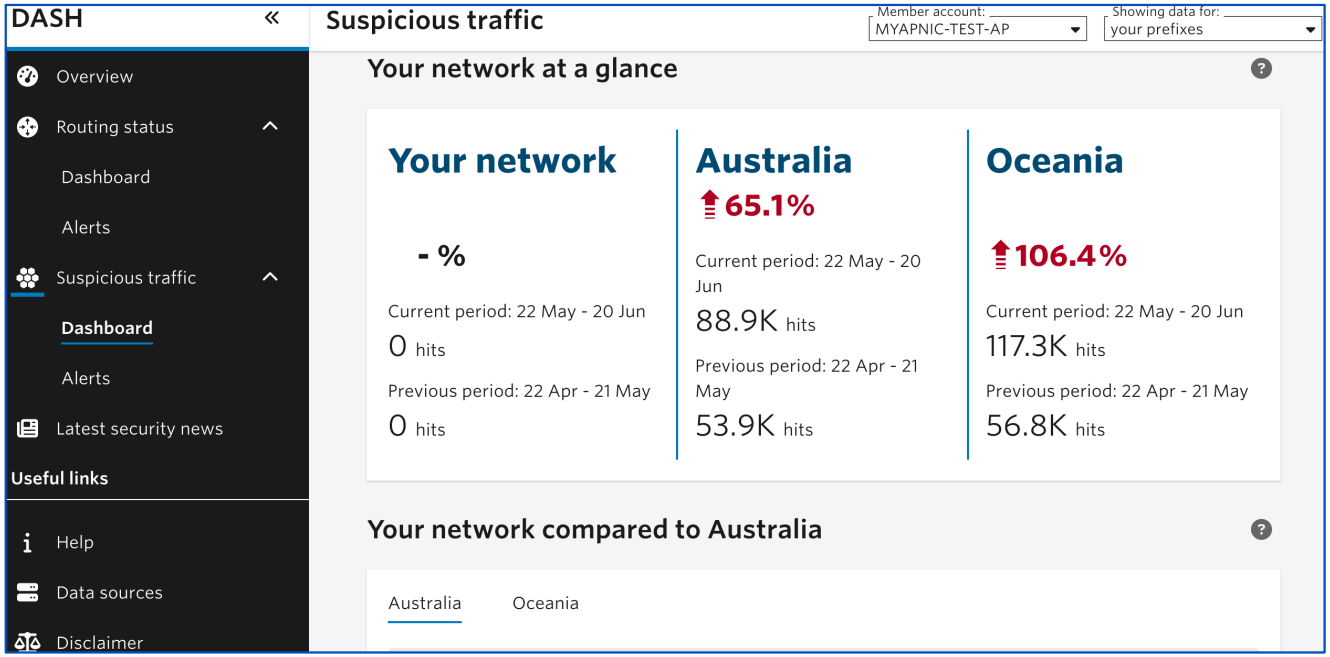
Name alert >

Name

Enter a name for this alert:

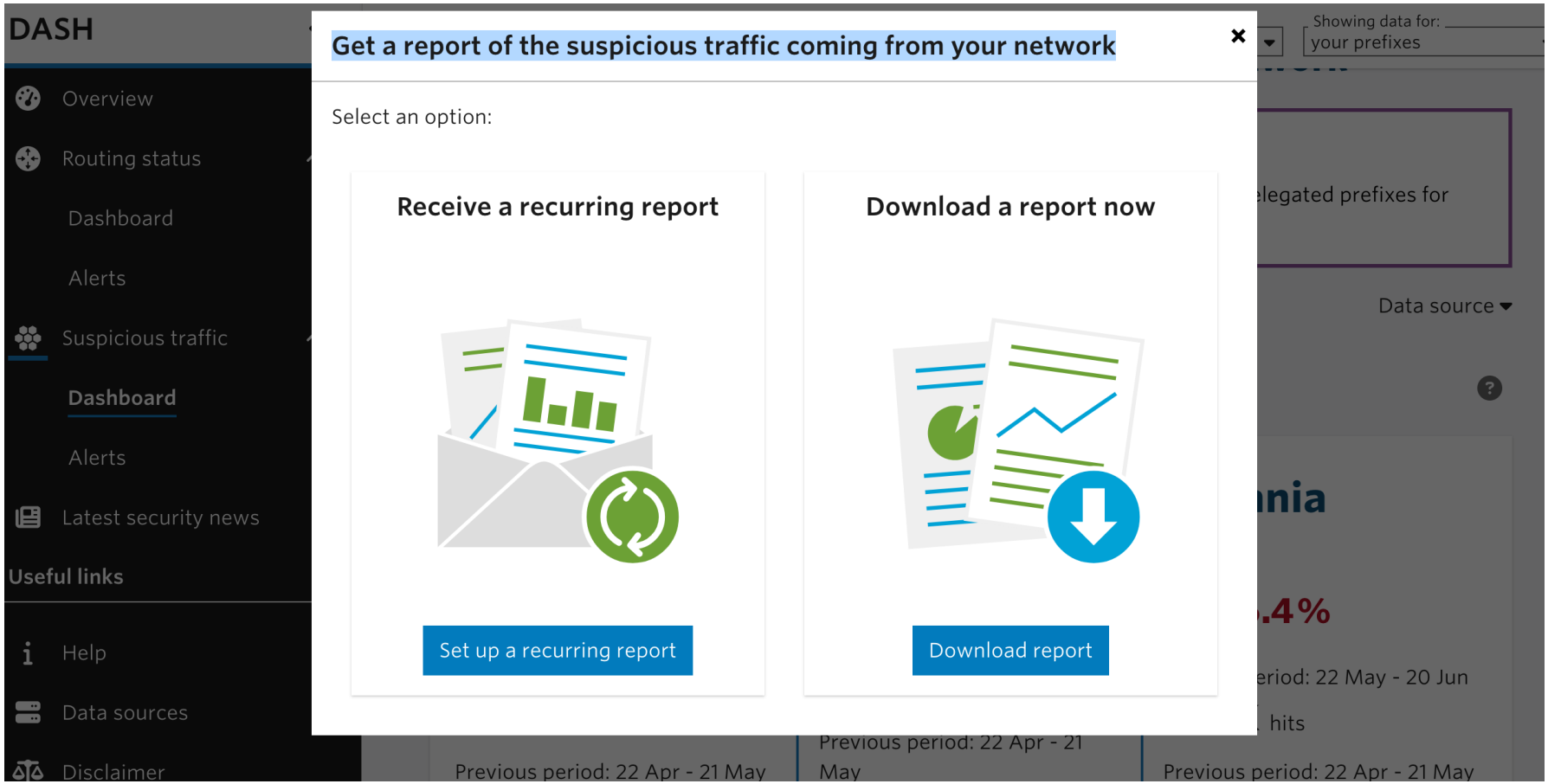
An alert name is required.

Suspicious traffic in DASH

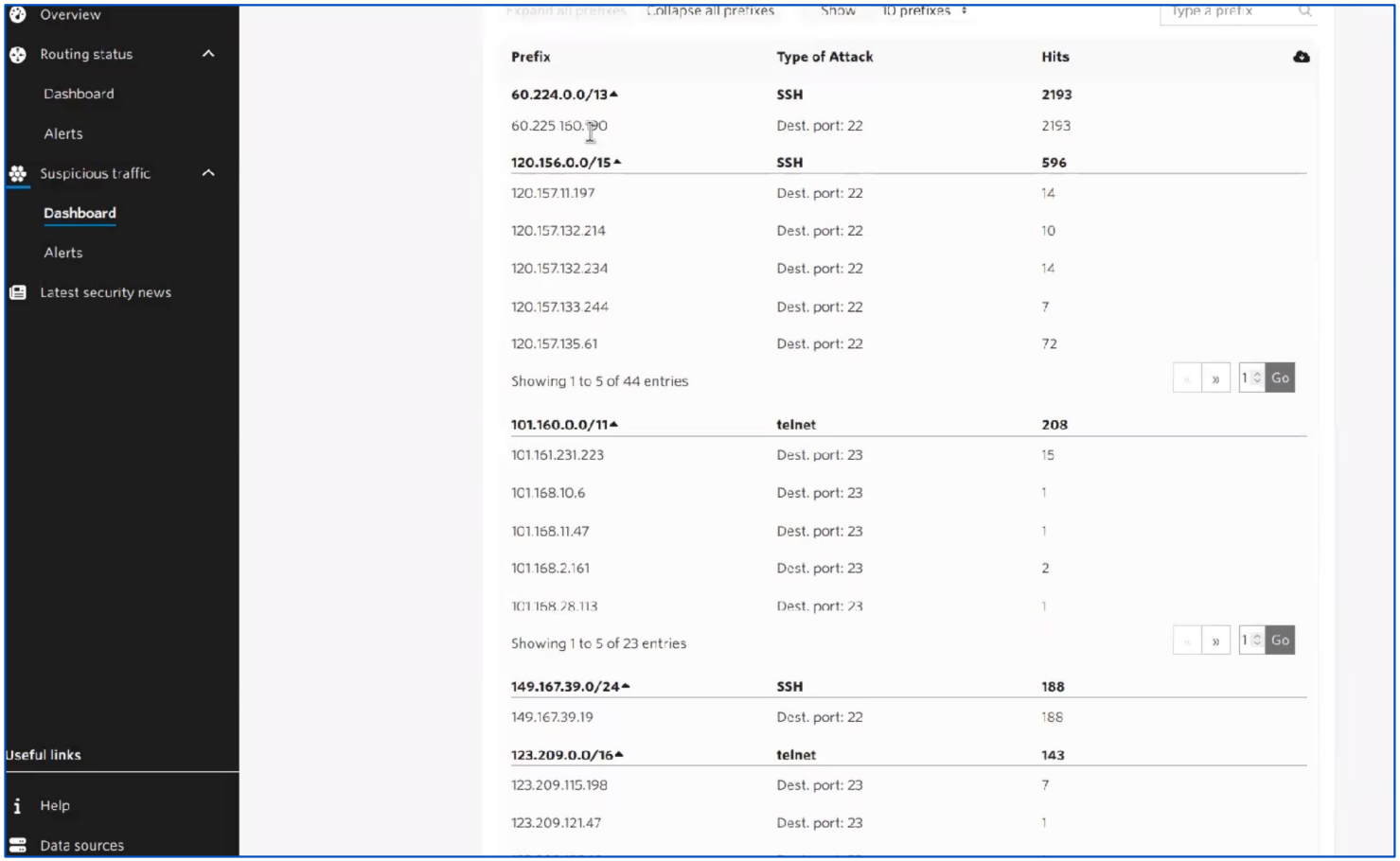


- Suspicious traffic was the original feature in DASH
- Honeynet is a network of honeypots and these sensors are spread across the Internet
- They are not announcing their IP
- These honeypots sit there and as soon as another machine tries to access it, it gets what we call hits - that someone is trying to invade the sensor
- The data from this helps your organization act and investigate why the suspicious traffic is coming from those machines and can also compare your activity against your economies and regions

Suspicious traffic in DASH

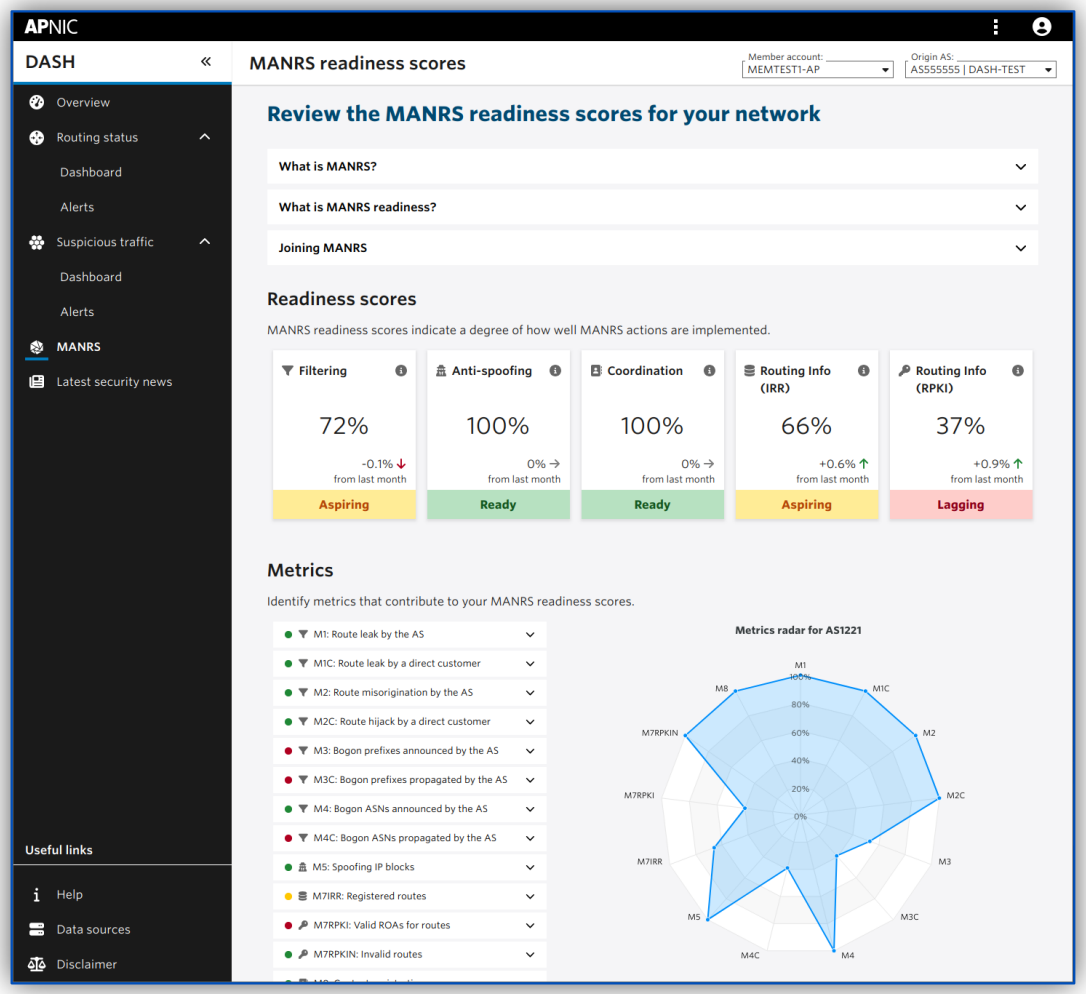


Suspicious traffic in DASH



MANRS readiness

- Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Global Cyber Alliance to reduce the most common routing threats
- Now ready to use in DASH



Thank you!