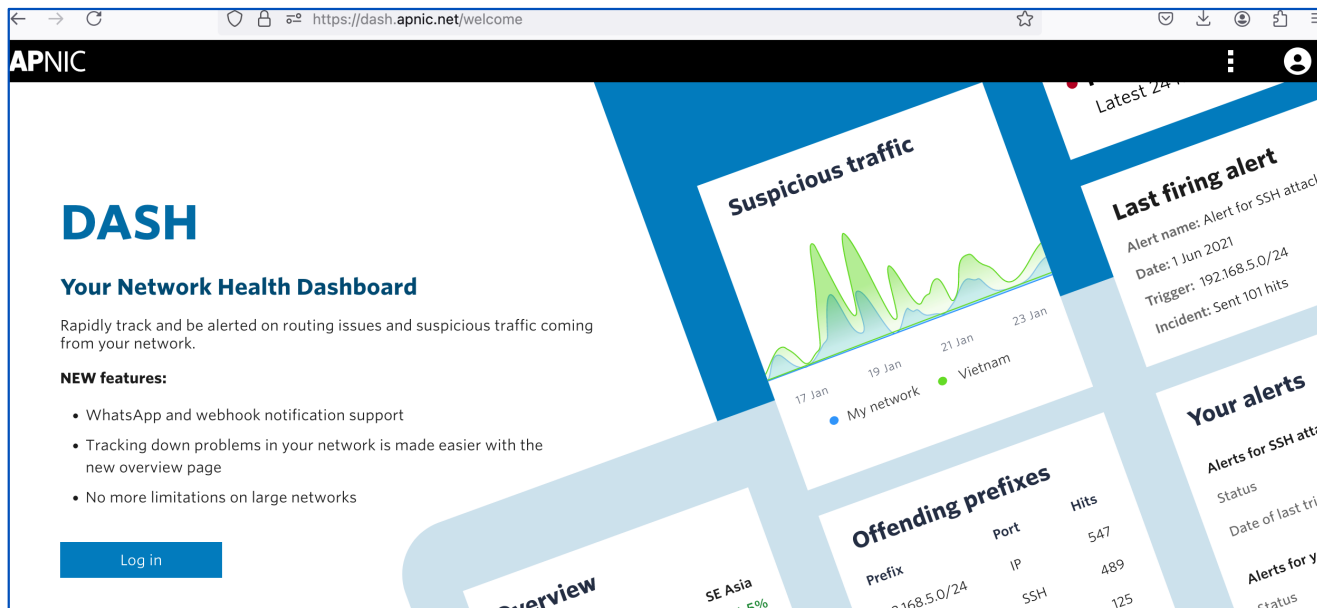


# DASH

PacNOG 34

[jordan.previtera@apnic.net](mailto: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

APNIC

DASH <<

Routing status

Member Account: MEMTEST1-AP

Showing routes for: my prefixes

Dashboard

Routing status

Suspicious traffic

Alerts

What to do

Latest security news

Review the routing information of your network to prevent misconfigurations and detect BGP hijacks.

About this page

Legend

Overview of inconsistencies

Total inconsistencies found 0

Status of ROAs and route objects as seen in BGP:

ROA mismatches 0

Route object mismatches 0

- 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

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

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

**Required actions:**

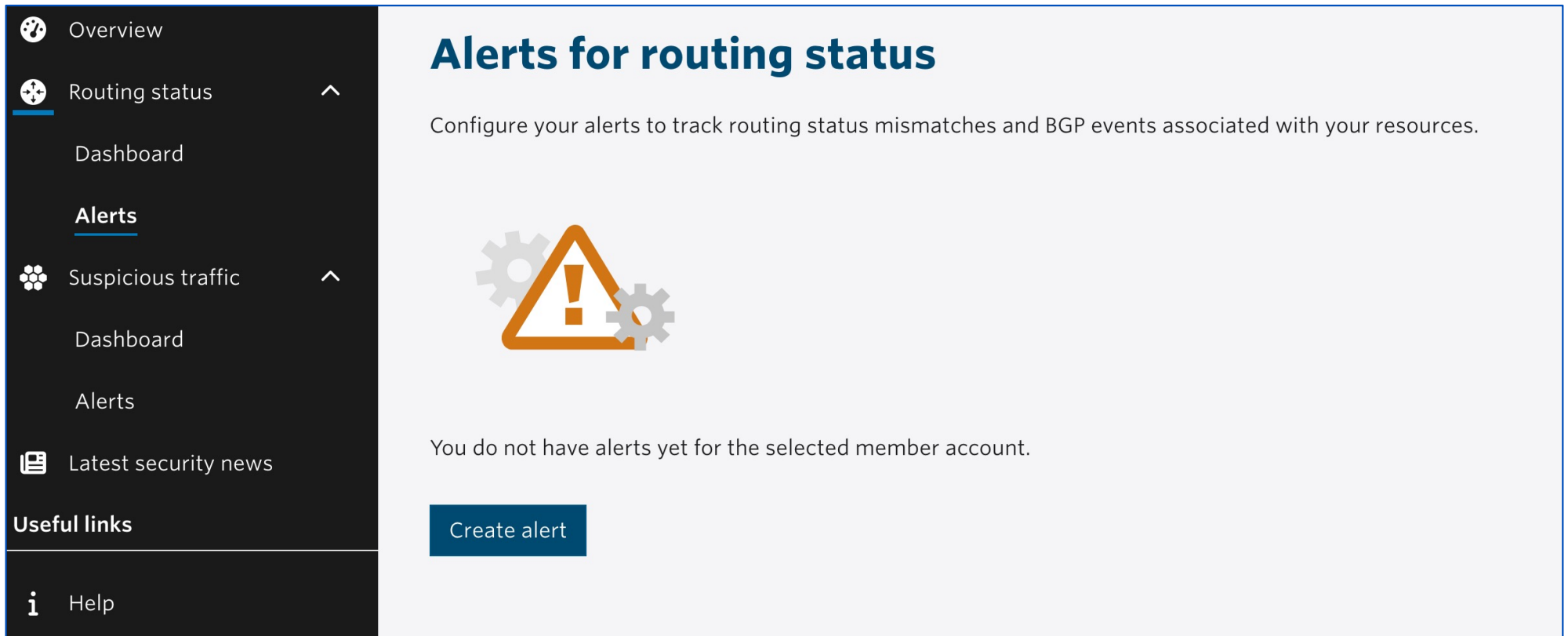
- If you did not expect a route with this length, review your routing configuration to evaluate if there is a misconfiguration or a BGP prefix hijack. [Learn more about BGP hijacking.](#) ▼
- If you did not expect this max length, review the ROAs for this prefix.

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



The screenshot shows the DASH interface for configuring alerts. On the left is a dark sidebar with navigation options: Overview, Routing status (selected), Dashboard, Alerts (selected), Suspicious traffic, Dashboard, Alerts, Latest security news, Useful links, and Help. The main content area has the title "Alerts for routing status" and a sub-header "Configure your alerts to track routing status mismatches and BGP events associated with your resources." Below this is an orange warning triangle icon with a white exclamation mark and two grey gears. The text states "You do not have alerts yet for the selected member account." and a blue "Create alert" button is visible.

**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.

[Create alert](#)

# Alerts creation in DASH

### Create alert ✕

**Define filter** >

**Define trigger** >

**Define notification** >

**Name 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.

**Next**

# Alerts creation in DASH

## Create alert ✕

**Define filter** >

**Define trigger** >

**Define notification** >

**Name alert** >

### Filter

Select trigger filter type (Prefix or Origin AS):

Prefix  Origin AS

#### Origin AS

All origin AS delegated to your account.

Select individual Origin ASNs.

**Next**



# Alerts creation in DASH

## Create alert ✕

**Define filter** >

**Define trigger** >

**Define notification** >

**Name 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.

**Next**

# Alerts creation in DASH

## Create alert ✕

Define filter >

**Define trigger** >

Define notification >

Name 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)

Previous **Next**

# Alerts creation in DASH

## Create alert ✕

Define filter >

**Define trigger** >

Define notification >

Name alert >

### Trigger

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.

Previous **Next**

# Alerts creation in DASH

Define trigger >

**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

# Alerts creation in DASH

Define filter >

Define trigger >

**Define notification >**

Name alert >

## Notification

Nominate recipients to notify when the system triggers the alert.

Channel	Recipient	
<input checked="" type="checkbox"/> Email	Myself	<input type="button" value="Add to list"/>
<input type="checkbox"/> SMS		
<input type="checkbox"/> Slack	Address can be updated at <a href="#">your personal profile</a>	
<input type="checkbox"/> WhatsApp		
<input type="checkbox"/> Webhook		

**Recipient**

(No recipient added)

Send notification when alert has been resolved.

# Alerts creation in DASH

### Create alert

Define filter >

Define trigger >

**Define notification** >

Name alert >

#### Notification

Nominate recipients to notify when the system triggers the alert.

Channel Recipient

Email Myself [Add to list](#)

Your email address can be updated at [your personal profile](#).

Channel	Recipient
Email	Jordan (myself) <a href="#">-</a>

Send notification when alert has been resolved.

[Previous](#) [Next](#)

# Alerts creation in DASH

Define filter >

Define trigger >

Define notification >

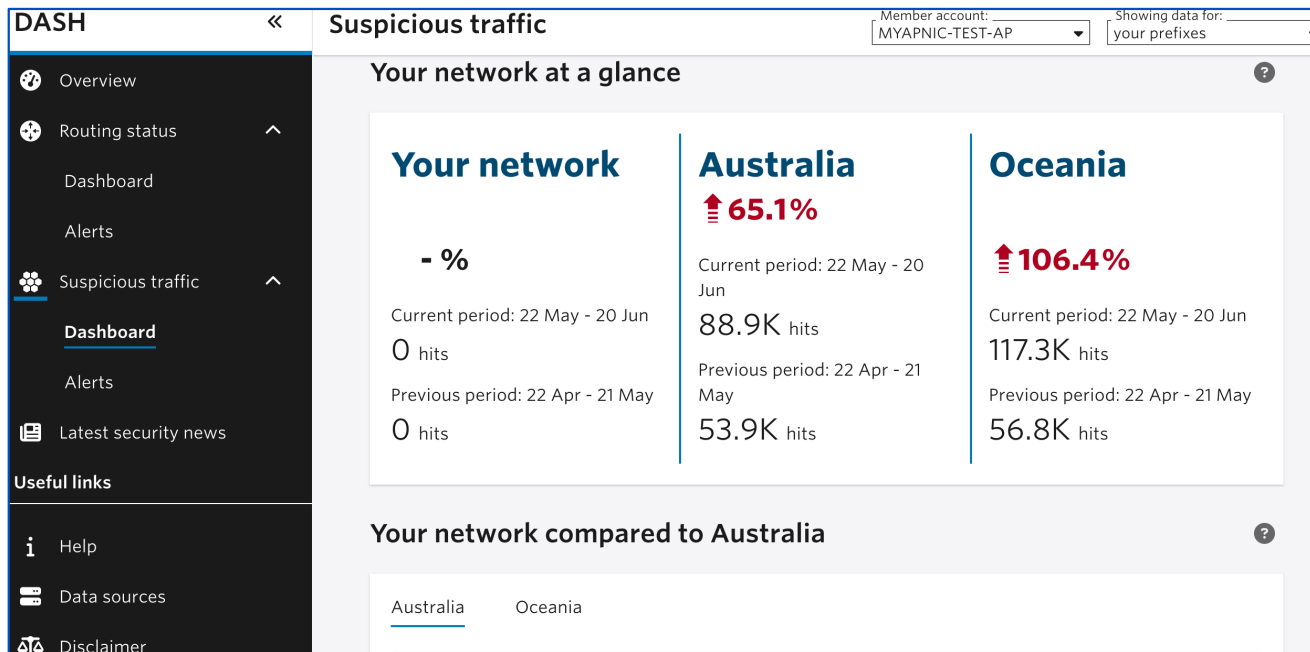
**Name alert >**

**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

The screenshot displays the DASH (Data Analysis and Reporting System) interface. A modal window is open, titled "Get a report of the suspicious traffic coming from your network". The modal offers two options: "Receive a recurring report" and "Download a report now".

**Receive a recurring report**

Select an option:

Receive a recurring report

Download a report now

Set up a recurring report

Download report

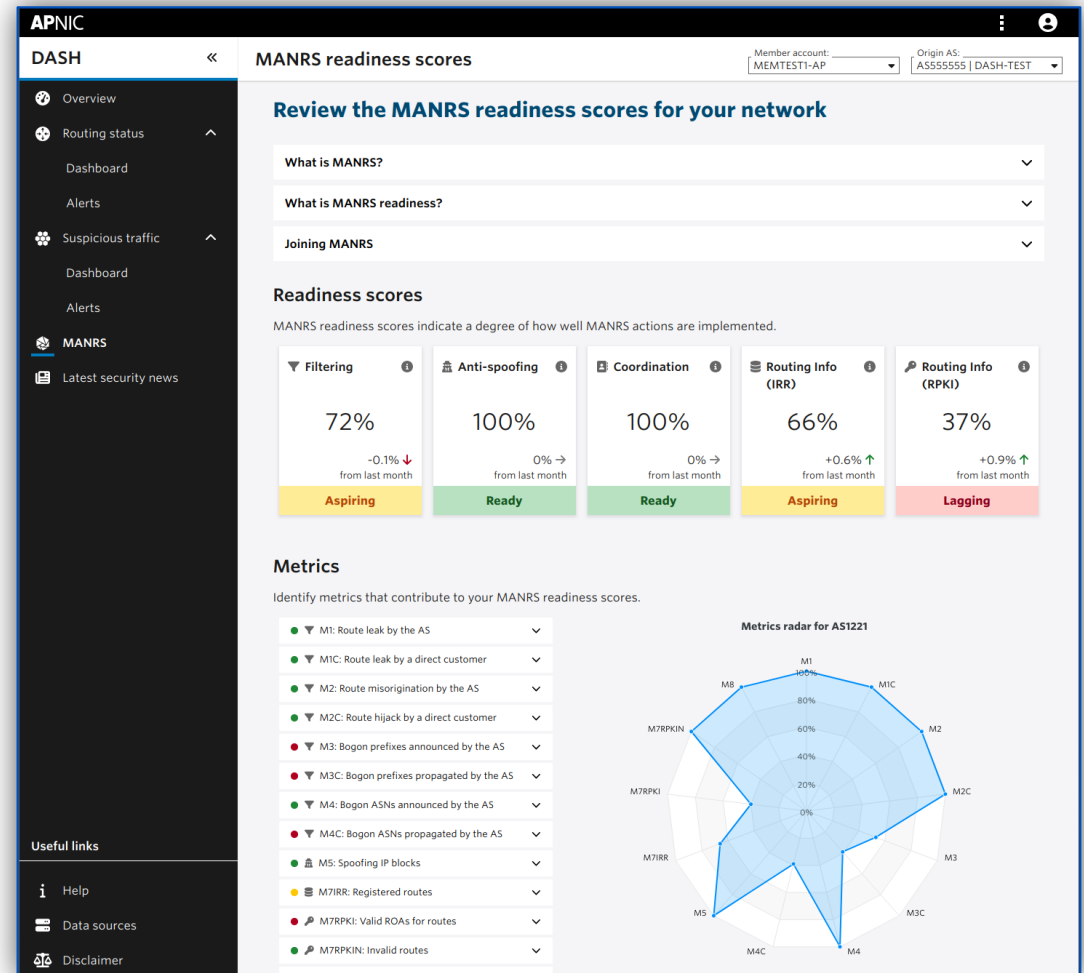
The background interface shows a sidebar with navigation options: Overview, Routing status, Dashboard, Alerts, Suspicious traffic (selected), Latest security news, Useful links, Help, Data sources, and Disclaimer. The main content area shows a chart for "Showing data for: your prefixes" with a "Data source" dropdown and a "Previous period: 22 Apr - 21 May" label.

# Suspicious traffic in DASH

Prefix	Type of Attack	Hits
<b>60.224.0.0/13</b>	<b>SSH</b>	<b>2193</b>
60.225.160.0/20	Dest. port: 22	2153
<b>120.156.0.0/15</b>	<b>SSH</b>	<b>596</b>
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		
<b>101.160.0.0/11</b>	<b>telnet</b>	<b>208</b>
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		
<b>149.167.39.0/24</b>	<b>SSH</b>	<b>188</b>
149.167.39.19	Dest. port: 22	188
<b>123.209.0.0/16</b>	<b>telnet</b>	<b>143</b>
123.209.115.198	Dest. port: 23	7
123.209.121.47	Dest. port: 23	1

# 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!