D Dashboard for
A Autonomous
S System
H Health

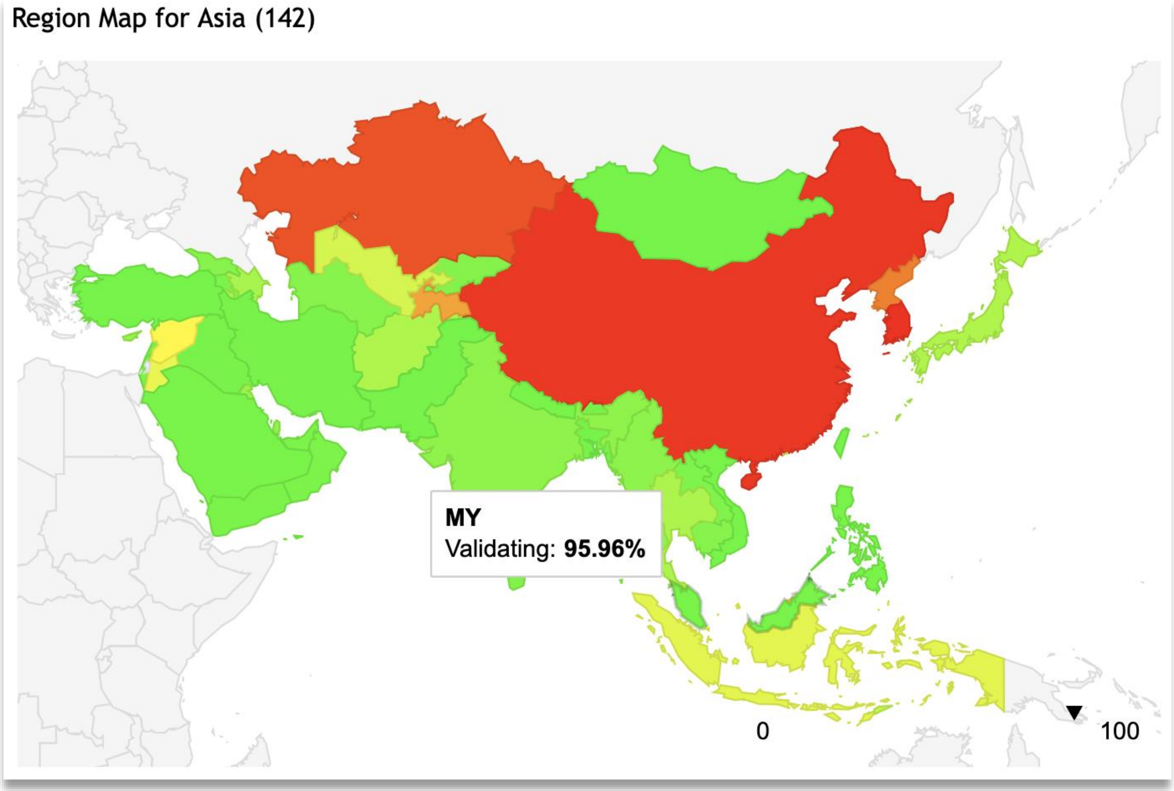
NIR Workshop
APRICOT 2025

Vivek Nigam
APNIC

DASH Services

- Current Services
  - Routing status
  - Suspicious traffic
  - MANRS readiness score
  - Bogons

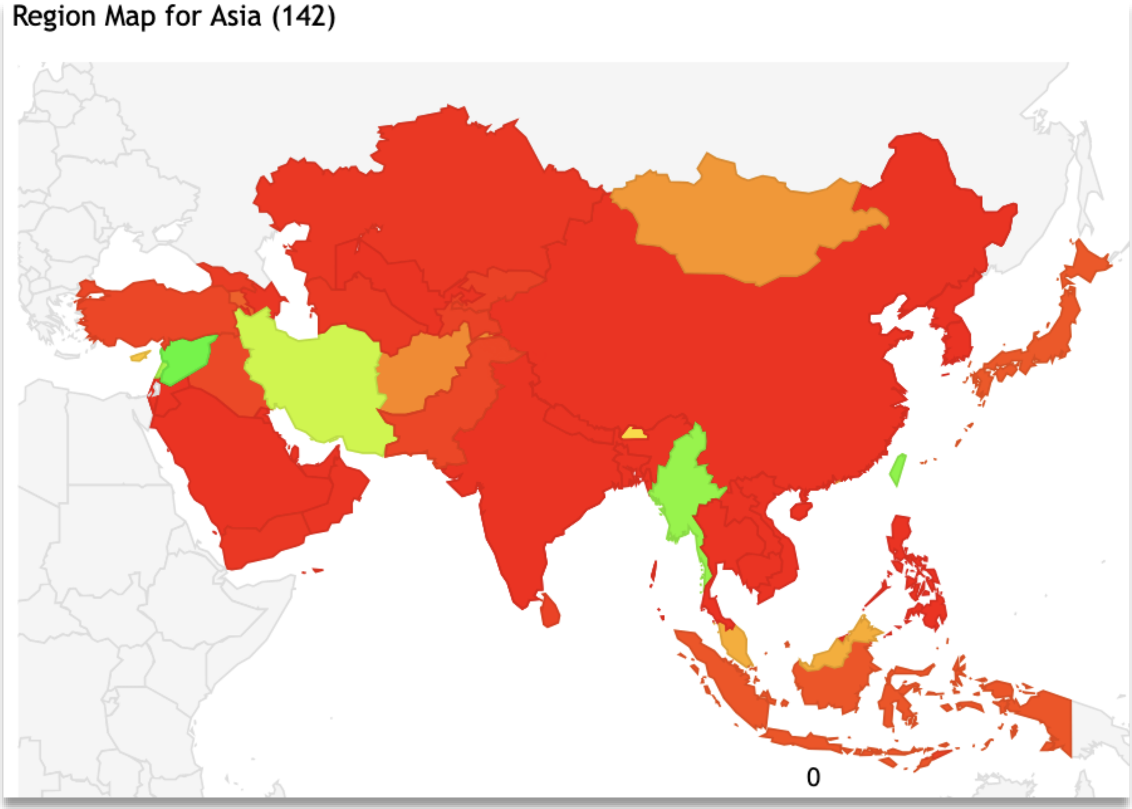
RPKI ROA Uptake



Region Map for Asia (142)

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

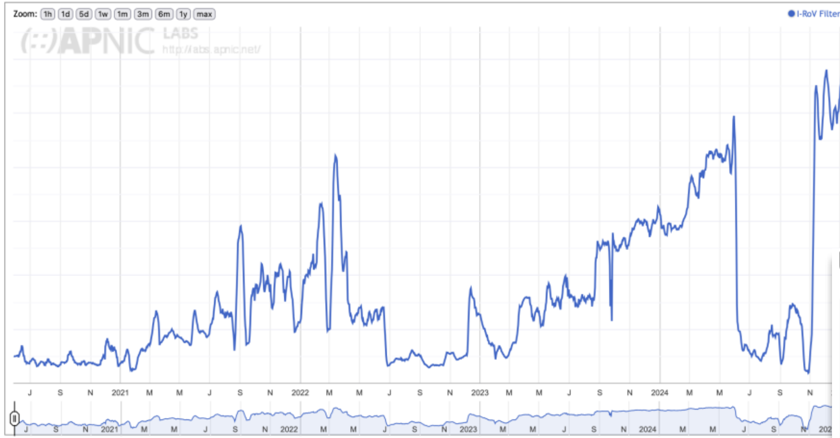
RPKI ROV uptake



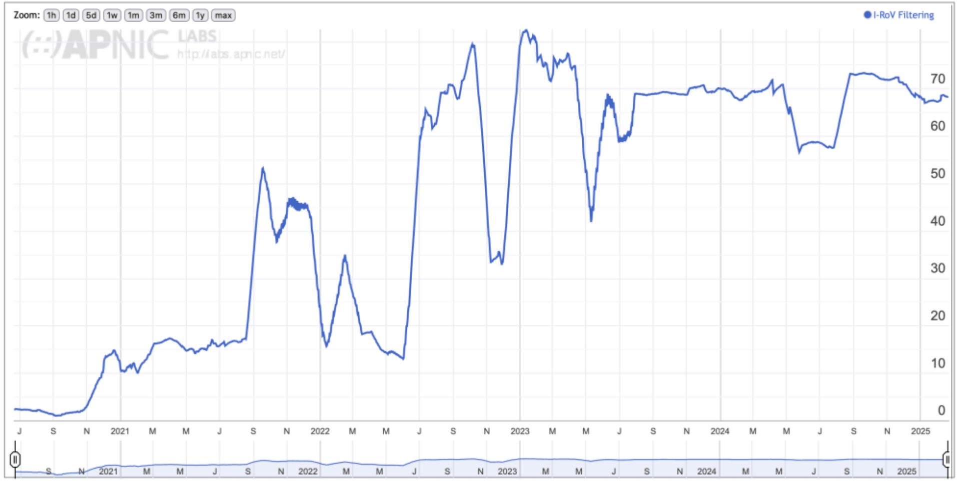
https://stats.labs.apnic.net/rpki

Early adopters of ROV

Use of RPKI Validation for Myanmar (MM)



Use of RPKI Validation for Taiwan (TW)



FAQs

- Visibility of our prefixes became low (29% 189/641) since we have changed the upstream provider, why?

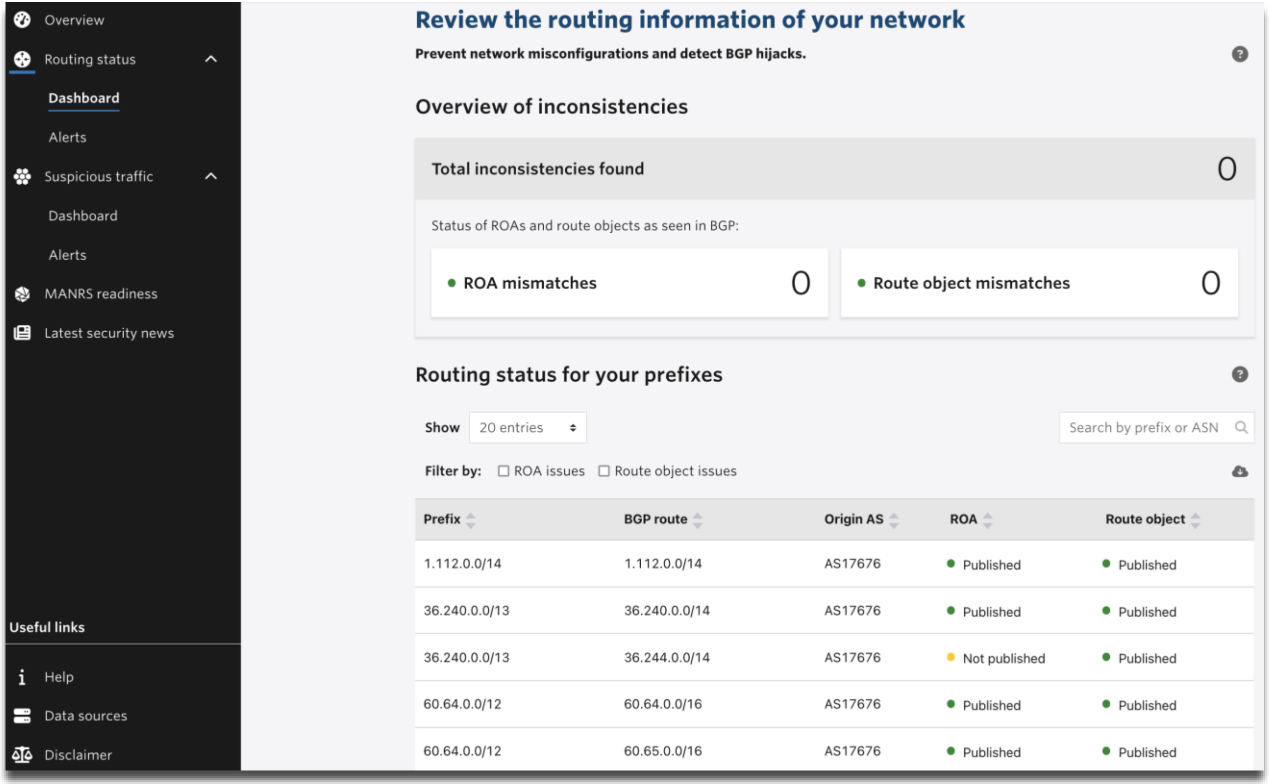
- Why our prefixes show ROA invalid in www.bgp.he.net, how to fix it?

- Our upstream provider sent us an email to create ROA as they are implementing ROV filtering, please support.

- Will there be any issues if I create ROA for my prefixes during peak hours? Do I need to create it overnight?

Routing status

Provides a full picture of all BGP announcements for your network and track inconsistencies against RPKI ROAs and IRR Route Objects.



Review the routing information of your network

Prevent network misconfigurations and detect BGP hijacks.

Overview of inconsistencies

Total inconsistencies found 0

Status of ROAs and route objects as seen in BGP:

● ROA mismatches 0

● Route object mismatches 0

Routing status for your prefixes

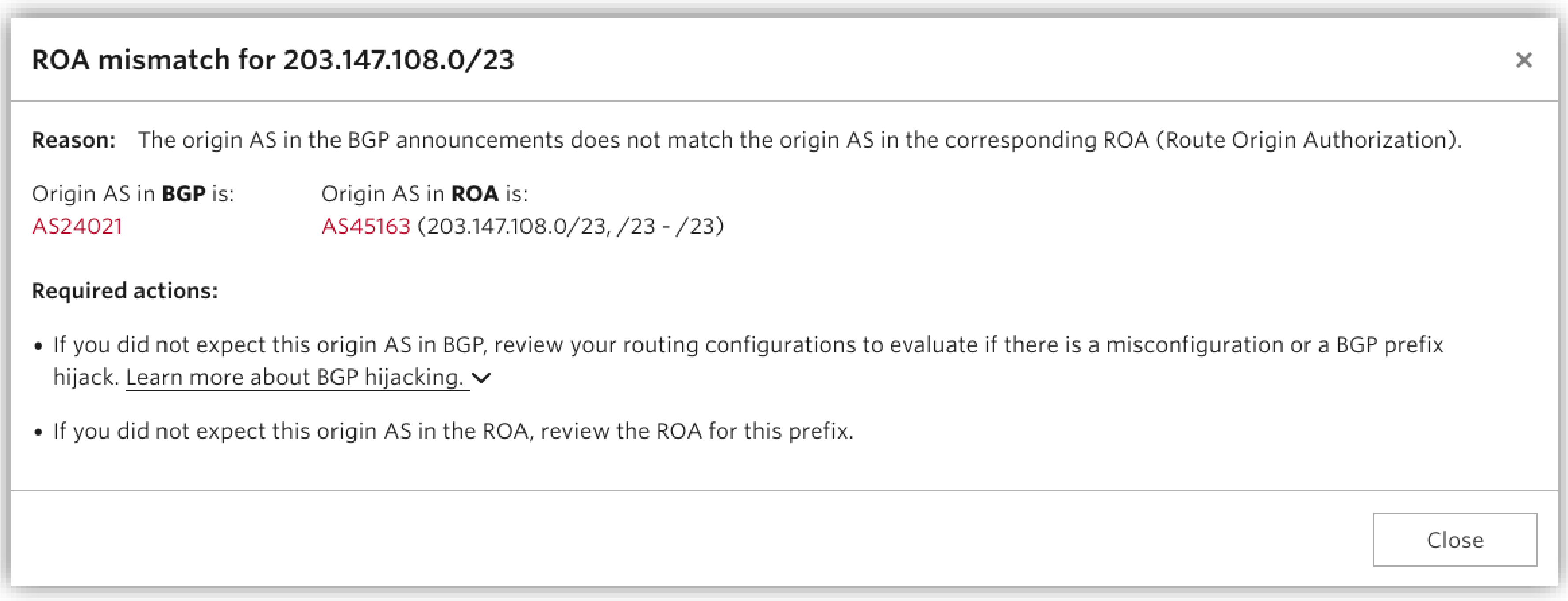
Show 20 entries

Search by prefix or ASN

Filter by: □ ROA issues □ Route object issues

Prefix	BGP route	Origin AS	ROA	Route object
1.112.0.0/14	1.112.0.0/14	AS17676	● Published	● Published
36.240.0.0/13	36.240.0.0/14	AS17676	● Published	● Published
36.240.0.0/13	36.244.0.0/14	AS17676	● Not published	● Published
60.64.0.0/12	60.64.0.0/16	AS17676	● Published	● Published
60.64.0.0/12	60.65.0.0/16	AS17676	● Published	● Published

ROA mismatch example



ROA mismatch for 203.147.108.0/23

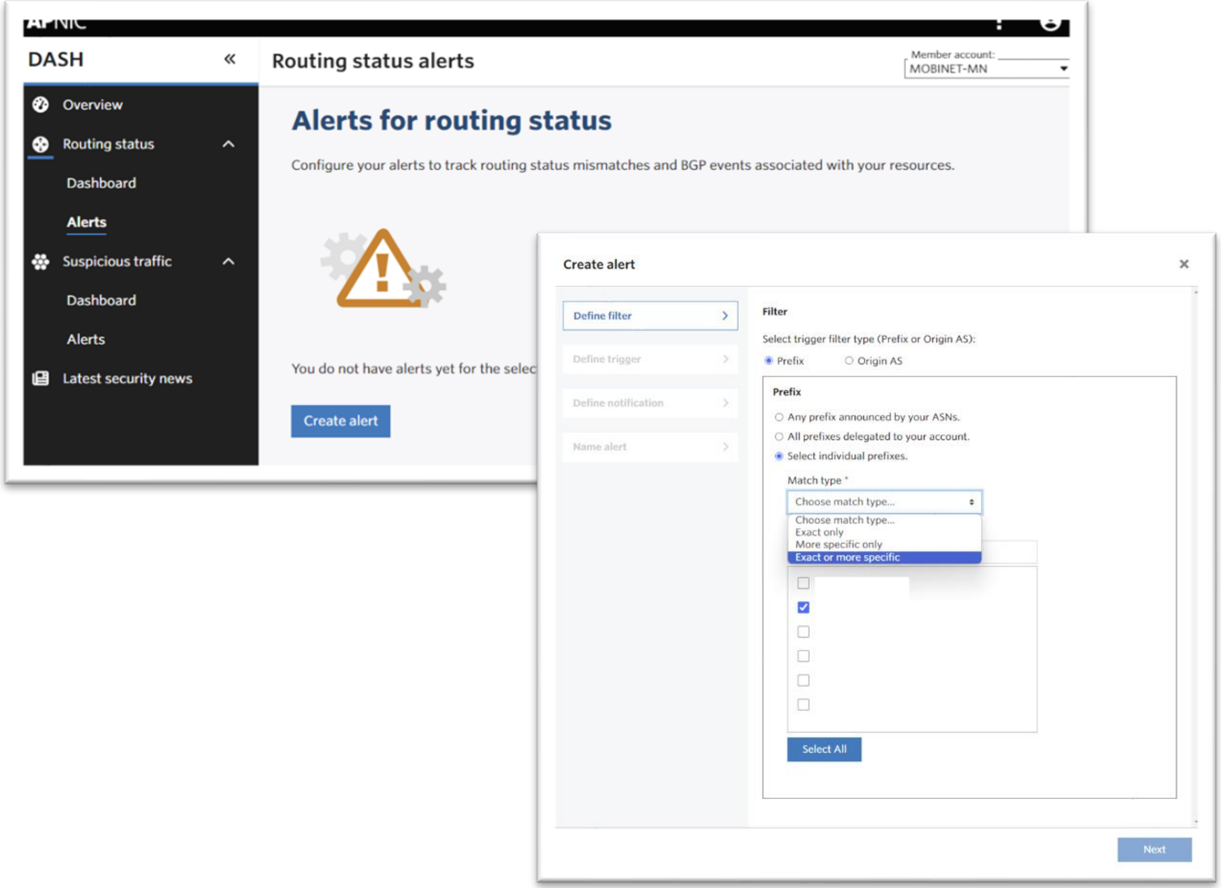
Reason: The origin AS in the BGP announcements does not match the origin AS in the corresponding ROA (Route Origin Authorization).

Origin AS in **BGP** is:	Origin AS in **ROA** is:
AS24021	AS45163 (203.147.108.0/23, /23 - /23)

Required actions:

- If you did not expect this origin AS in BGP, review your routing configurations to evaluate if there is a misconfiguration or a BGP prefix hijack. Learn more about BGP hijacking.
- If you did not expect this origin AS in the ROA, review the ROA for this prefix.

Set up your Routing status alerts



APNIC

DASH «

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

Routing status alerts

Member account: MOBINET-MN

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 selec

Create alert

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.

Match type *

Choose match type...

- Choose match type...
- Exact only
- More specific only
- Exact or more specific

□

☑

□

□

□

□

Select All

Next

Email

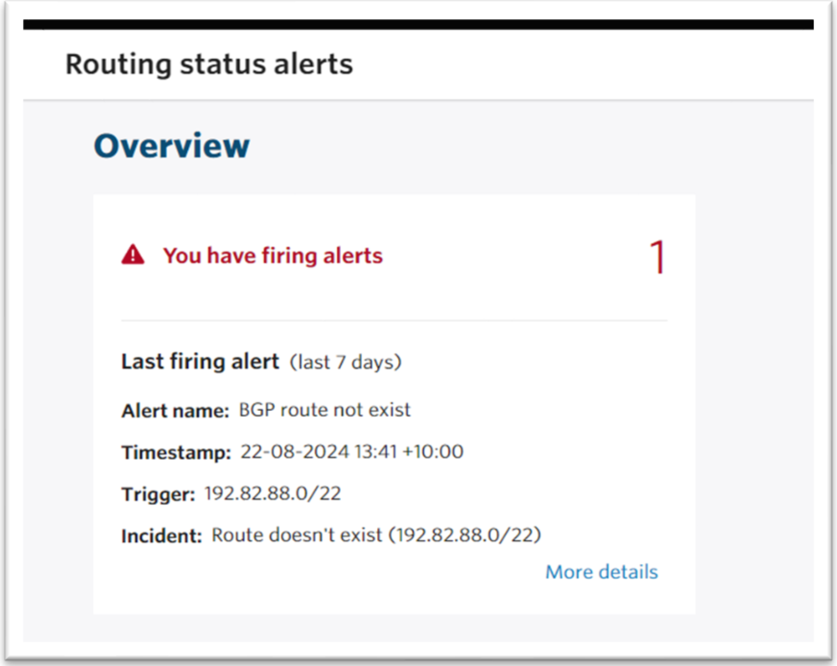
SMS

Slack

WhatsApp

Webhooks

Routing status alert



Routing status alerts

Overview

⚠ You have firing alerts 1

Last firing alert (last 7 days)

Alert name: BGP route not exist

Timestamp: 22-08-2024 13:41 +10:00

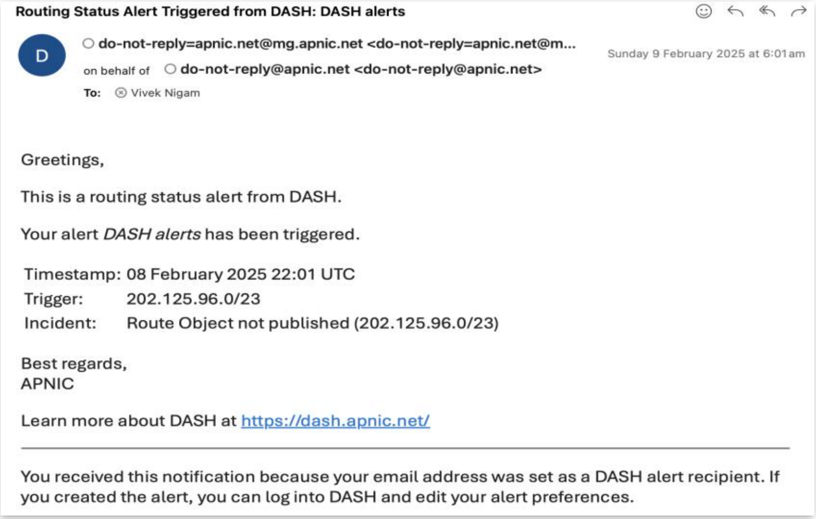
Trigger: 192.82.88.0/22

Incident: Route doesn't exist (192.82.88.0/22)

More details

Type of alerts

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



Routing Status Alert Triggered from DASH: DASH alerts

D ○ do-not-reply=apnic.net@mg.apnic.net <do-not-reply=apnic.net@m...

on behalf of ○ do-not-reply@apnic.net <do-not-reply@apnic.net>

To: Vivek Nigam

Sunday 9 February 2025 at 6:01am

Greetings,

This is a routing status alert from DASH.

Your alert *DASH alerts* has been triggered.

Timestamp: 08 February 2025 22:01 UTC
Trigger: 202.125.96.0/23
Incident: Route Object not published (202.125.96.0/23)

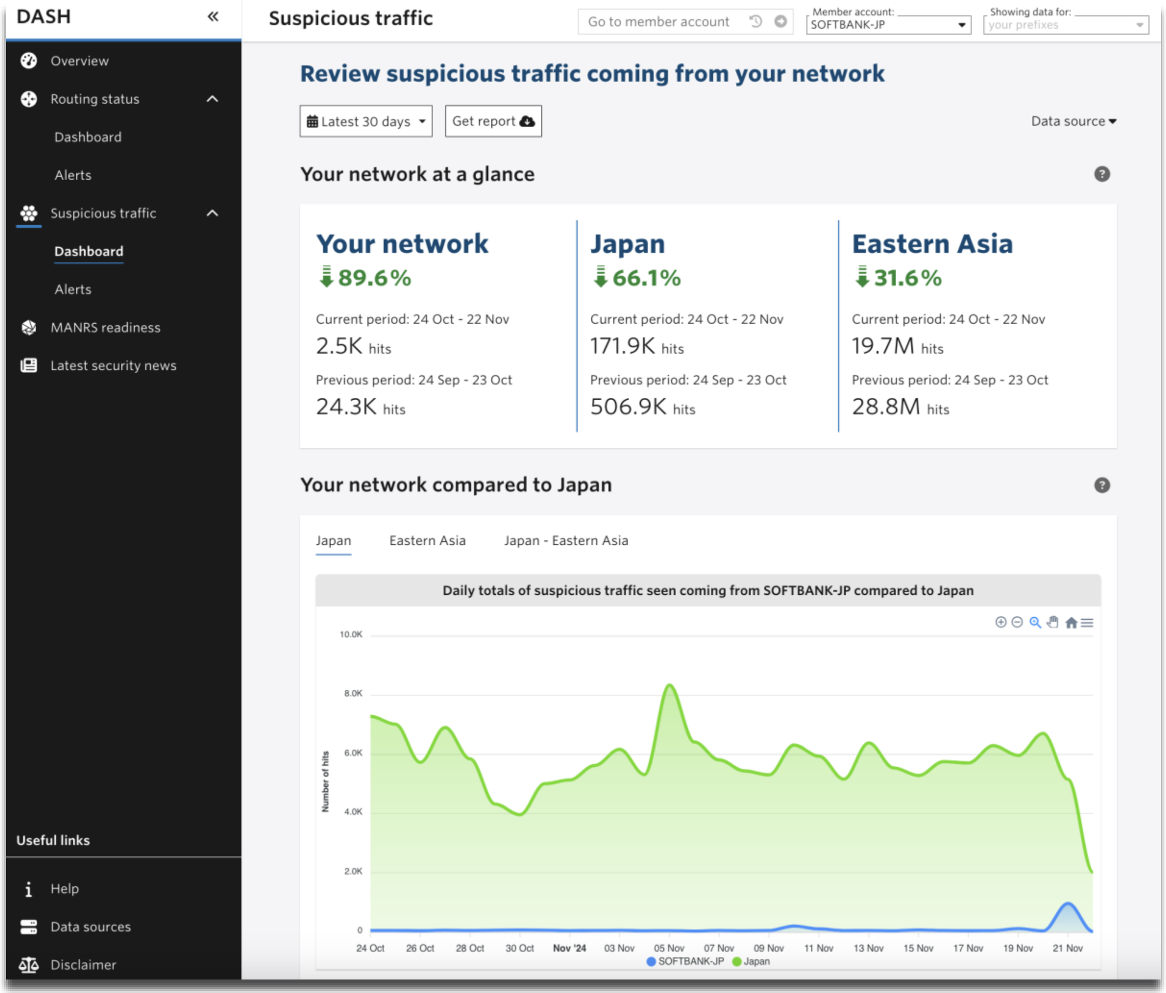
Best regards,
APNIC

Learn more about DASH at https://dash.apnic.net/

You received this notification because your email address was set as a DASH alert recipient. If you created the alert, you can log into DASH and edit your alert preferences.

Suspicious traffic

- Track and be alerted about suspicious traffic originating from your networks.
- Suspicious traffic is detected by APNIC’s Community Honeynet Network, with more than 200 points of data collection mostly in the Asia Pacific region but with nodes in Central and South America, USA and Europe.



Suspicious traffic

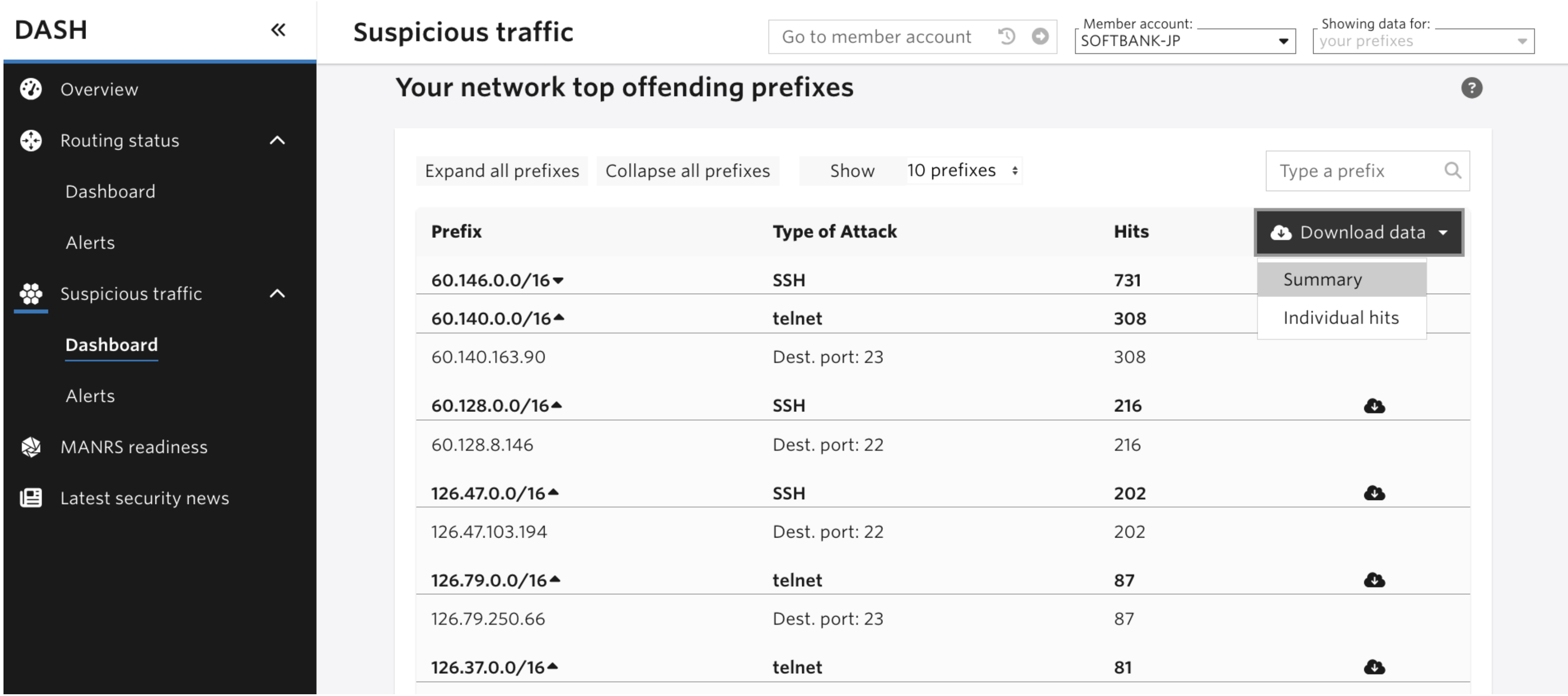
Review suspicious traffic coming from your network

Your network at a glance

Your network	Japan	Eastern Asia
↓89.6%	↓66.1%	↓31.6%
Current period: 24 Oct - 22 Nov	Current period: 24 Oct - 22 Nov	Current period: 24 Oct - 22 Nov
2.5K hits	171.9K hits	19.7M hits
Previous period: 24 Sep - 23 Oct	Previous period: 24 Sep - 23 Oct	Previous period: 24 Sep - 23 Oct
24.3K hits	506.9K hits	28.8M hits

Your network compared to Japan

Daily totals of suspicious traffic seen coming from SOFTBANK-JP compared to Japan



Suspicious traffic

Member account: SOFTBANK-JP

Showing data for: your prefixes

Your network top offending prefixes

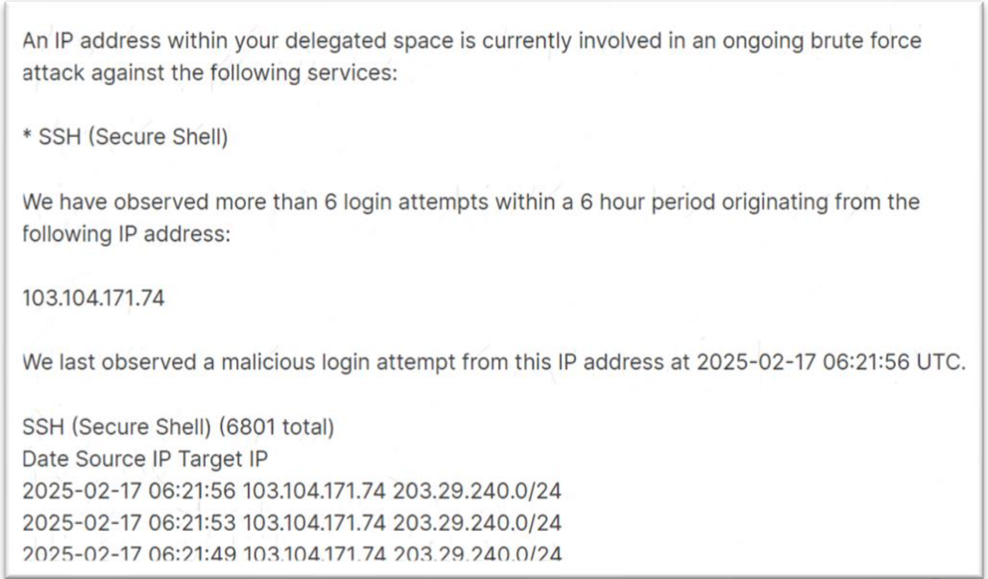
Show 10 prefixes

Prefix	Type of Attack	Hits
60.146.0.0/16▾	**SSH**	**731**
60.140.0.0/16▴	**telnet**	**308**
60.140.163.90	Dest. port: 23	308
60.128.0.0/16▴	**SSH**	**216**
60.128.8.146	Dest. port: 22	216
126.47.0.0/16▴	**SSH**	**202**
126.47.103.194	Dest. port: 22	202
126.79.0.0/16▴	**telnet**	**87**
126.79.250.66	Dest. port: 23	87
126.37.0.0/16▴	**telnet**	**81**

Bogons in Routing table

- There are 179 separate Bogon prefixes announced and 40 Bogon ASNs visible on the internet (APNIC resources only)
- These bogons could be the source of number of attacks, malicious traffics

Member query on Bogon prefixes attempt:



An IP address within your delegated space is currently involved in an ongoing brute force attack against the following services:

* SSH (Secure Shell)

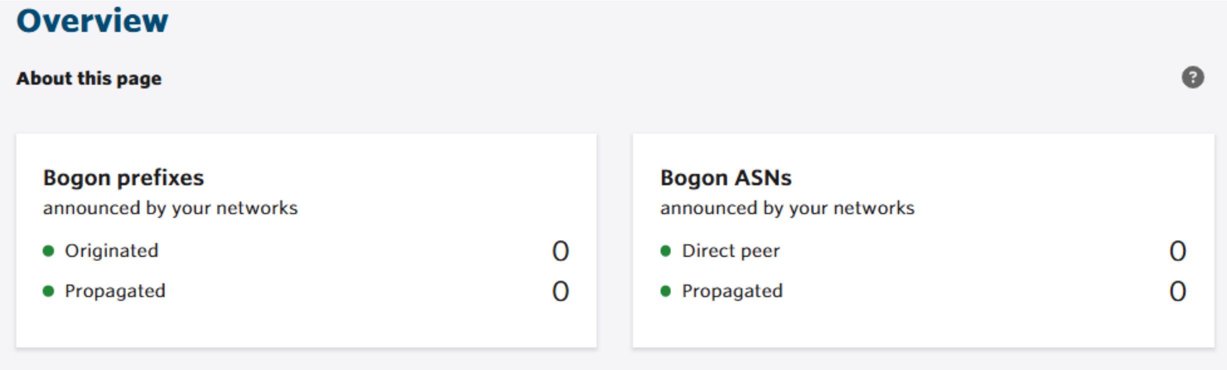
We have observed more than 6 login attempts within a 6 hour period originating from the following IP address:

103.104.171.74

We last observed a malicious login attempt from this IP address at 2025-02-17 06:21:56 UTC.

```
SSH (Secure Shell) (6801 total)
Date Source IP Target IP
2025-02-17 06:21:56 103.104.171.74 203.29.240.0/24
2025-02-17 06:21:53 103.104.171.74 203.29.240.0/24
2025-02-17 06:21:49 103.104.171.74 203.29.240.0/24
```

Bogons in DASH



Overview

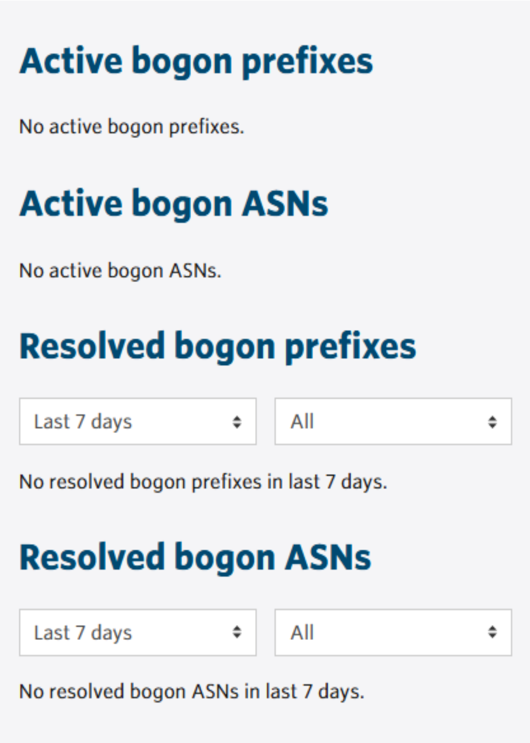
About this page ?

Bogon prefixes
announced by your networks

- ● Originated 0
- ● Propagated 0

Bogon ASNs
announced by your networks

- ● Direct peer 0
- ● Propagated 0



Active bogon prefixes

No active bogon prefixes.

Active bogon ASNs

No active bogon ASNs.

Resolved bogon prefixes

Last 7 days ⇕ | All ⇕

No resolved bogon prefixes in last 7 days.

Resolved bogon ASNs

Last 7 days ⇕ | All ⇕

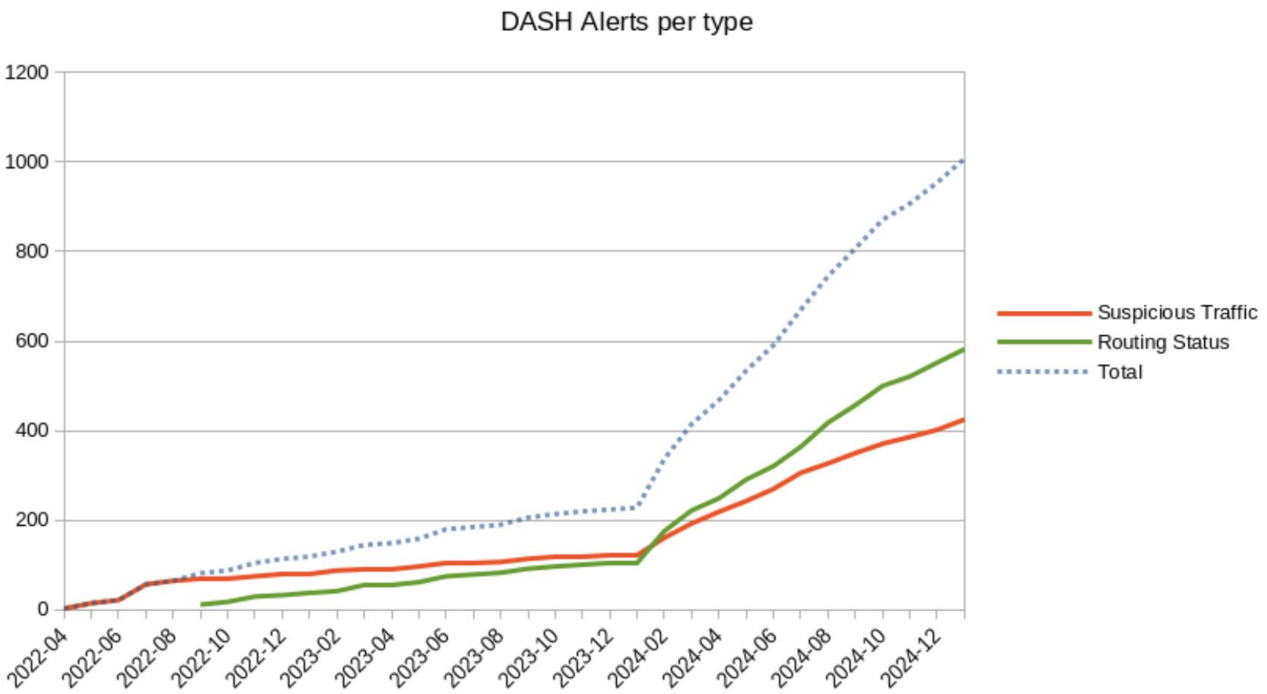
No resolved bogon ASNs in last 7 days.

It demonstrates:

- Whether your ASN is
  - Announcing or propagating Bogon IP address
  - Directly peering or propagating Bogon ASNs

DASH stats

- 1,188 view in the DASH overview page in the last 30 days



Questions?