DASH

Your Network Health Dashboard

Pubudu Jayasinghe

APNIC services

Ever been blacklisted ?

Hijacked ? ROAs done, time to ROV

Is BGP safe yet? *No.*

Border Gateway Protocol (BGP) is the postal service of the Internet. It's responsible for looking at all of the available paths that data could travel and picking the best route.

Unfortunately, it isn't secure, and there have been some major Internet disruptions as a result. But fortunately there is a way to make it secure.

ISPs and other major Internet players (Sprint and others) would need to implement a certification system, called RPKI.

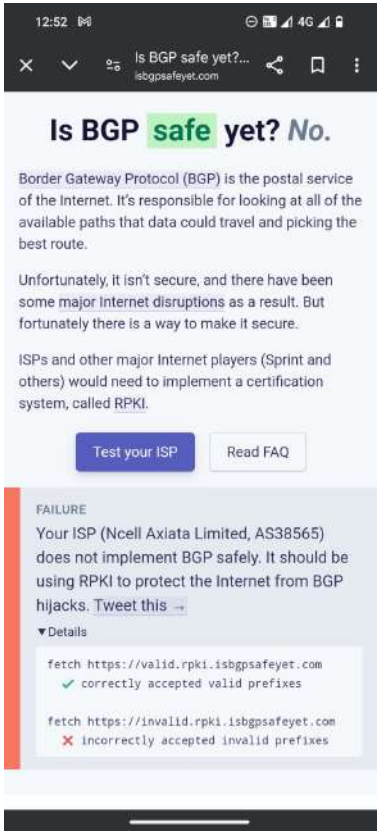
Test your ISP | Read FAQ

FAILURE

Your ISP (Websurfer Nepal Communication System Pvt. Ltd., AS24550) does not implement BGP safely. It should be using RPKI to protect the Internet from BGP hijacks. Tweet this →

▸ Details

isbgpsafeyet.com



Border Gateway Protocol (BGP) is the postal service of the Internet. It's responsible for looking at all of the available paths that data could travel and picking the best route.

Unfortunately, it isn't secure, and there have been some major Internet disruptions as a result. But fortunately there is a way to make it secure.

ISPs and other major Internet players (Sprint and others) would need to implement a certification system, called RPKI.

Test your ISP Read FAQ

SUCCESS

You are using Cloudflare WARP, which implements BGP safely.

▶ Details

Who are safe ?

Status

Displaying 31 major operators + Show all + Show ASN colu

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
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
Vodafone	transit	signed + filtering peers only	partially safe
Telstra International	transit	signed	partially safe
AT&T	ISP	signed + filtering peers only	partially safe
Google	cloud	signed	partially safe
DigitalOcean	cloud	filtering peers only	partially safe
Sparkle	transit	started	unsafe
PJSC RosTelecom	transit		unsafe
TransTelecom	transit		unsafe
SingTel	transit		unsafe
M247	cloud		unsafe

isbgpsafeyet.com

DASH

- Health Dashboard for your network
- Available to all APNIC Members

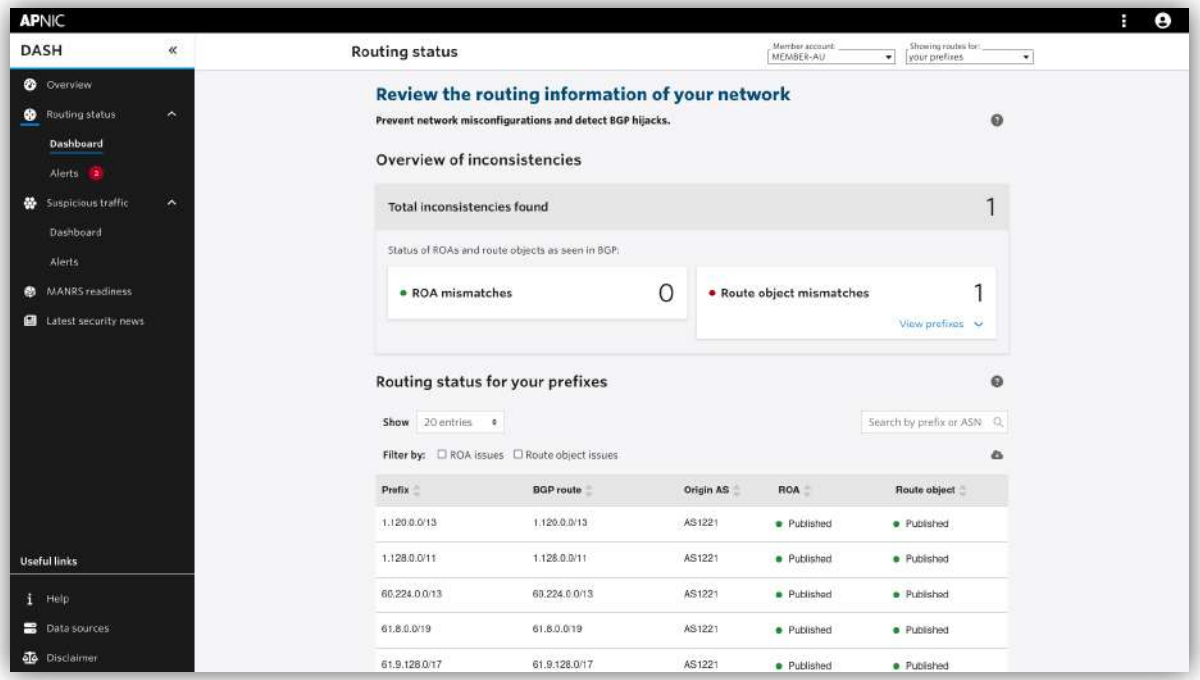
dash.apnic.net

DASH Services

- Current Services
  - Routing status
  - Suspicious traffic
  - MANRS readiness score
- Under implementation
  - Bogons (planned release: December 2024)

Routing status

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



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).

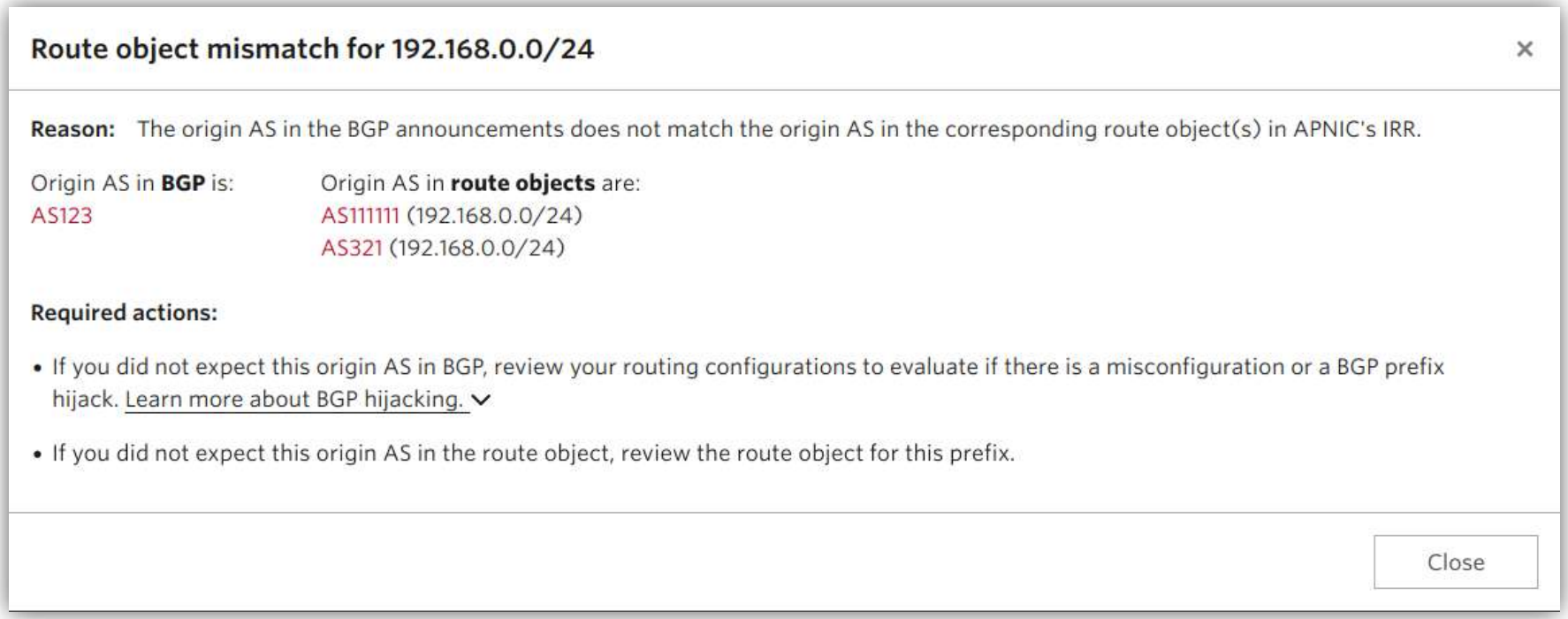
Origin AS in **BGP** is:	Origin AS in **ROA** is:
AS24021	AS45163 (203.147.108.0/23, /23 - /23)

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.

Close

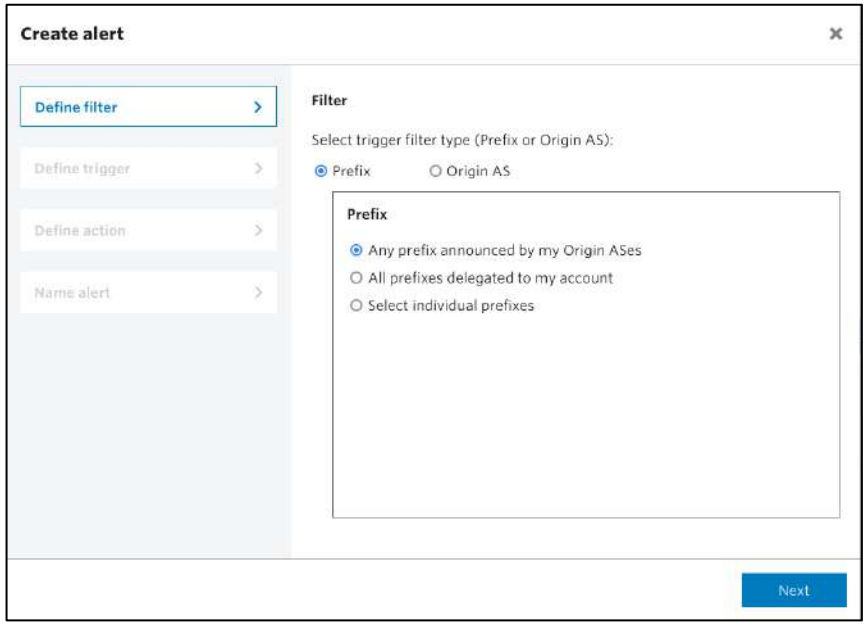
Route object mismatch example

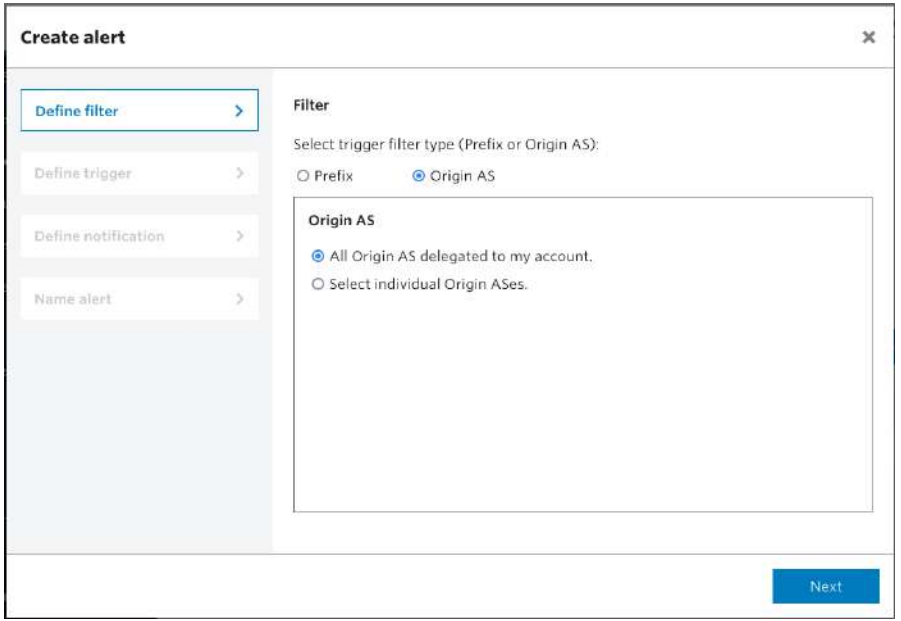


Routing status alerts

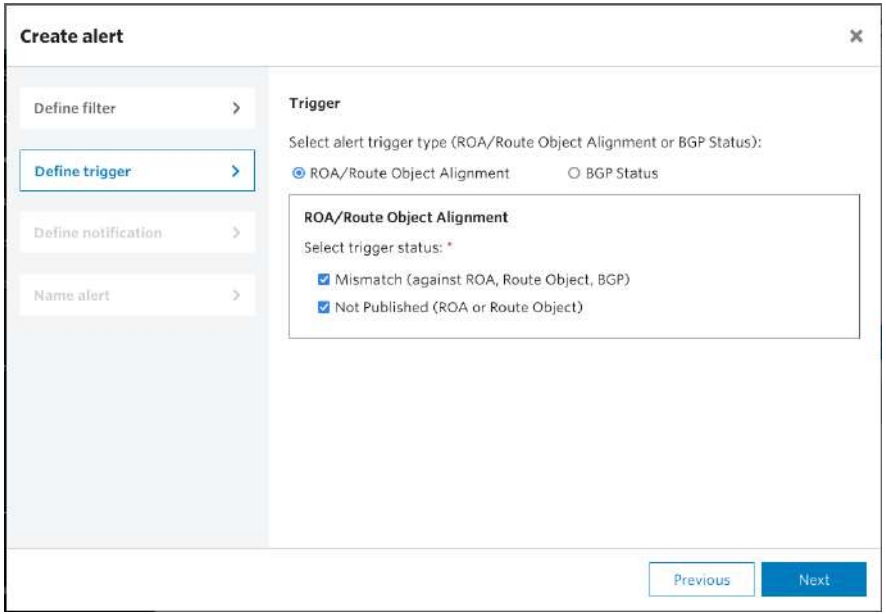
- Receive notifications about misalignments among BGP, RPKI and IRR (e.g. RPKI invalids and missing ROAs and IRR route objects).
- Receive notifications about BGP announcements for unexpected AS origins, detecting potential BGP hijacks.
- Receive notifications about loss of visibility for routes in BGP, detecting potential network issues or misconfigurations.

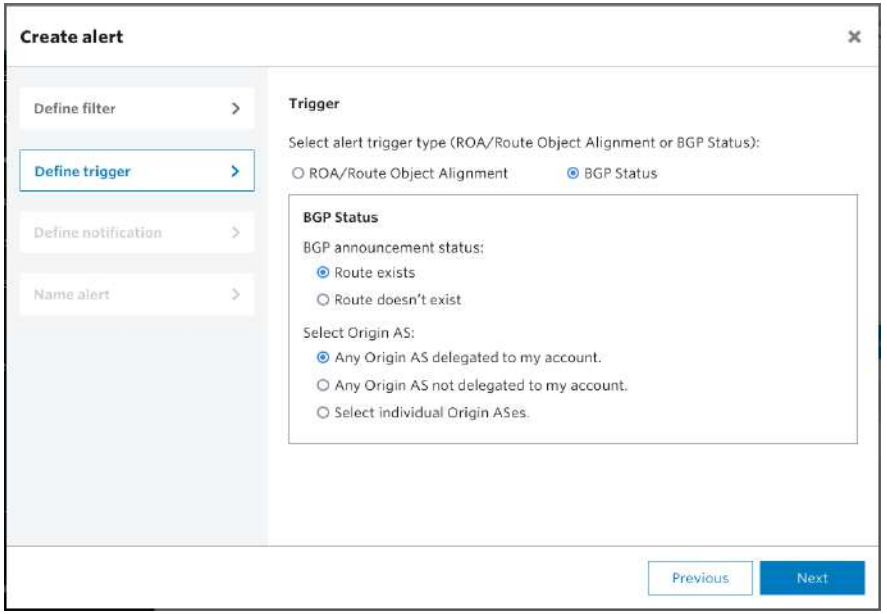
Alert Filters – “What”

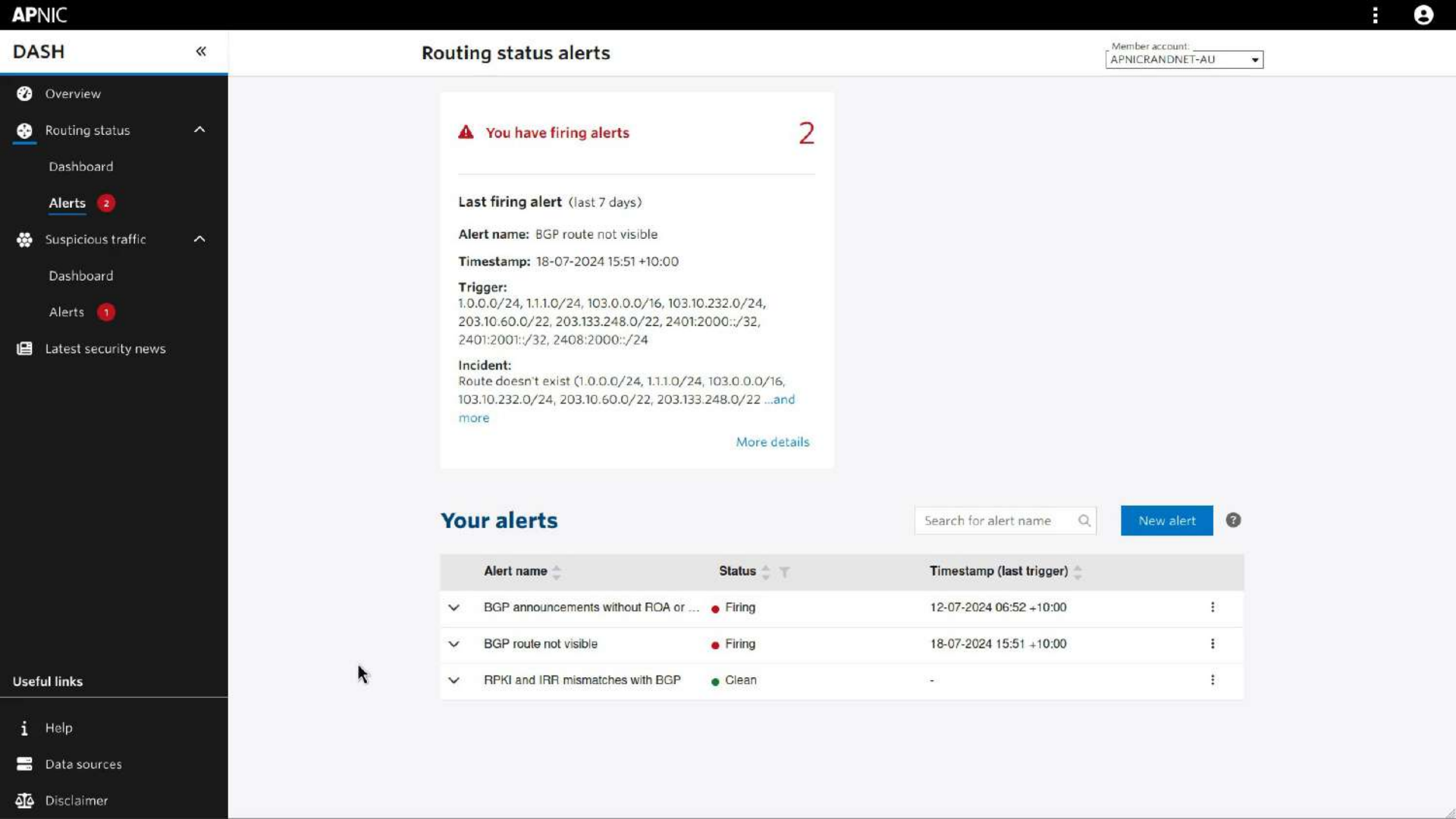




Alert Triggers – “When”






APNIC
DASH
Routing status alerts
Member account:
APNICRANDNET-AU
Overview
Routing status
Dashboard
Alerts 2
Suspicious traffic
Dashboard
Alerts 1
Latest security news
You have firing alerts 2
Last firing alert (last 7 days)
Alert name: BGP route not visible
Timestamp: 18-07-2024 15:51 +10:00
Trigger:
1.0.0.0/24, 1.1.1.0/24, 103.0.0.0/16, 103.10.232.0/24, 203.10.60.0/22, 203.133.248.0/22, 2401:2000::/32, 2401:2001::/32, 2408:2000::/24
Incident:
Route doesn't exist (1.0.0.0/24, 1.1.1.0/24, 103.0.0.0/16, 103.10.232.0/24, 203.10.60.0/22, 203.133.248.0/22 ...and more
More details
Your alerts
Search for alert name
New alert
Alert name
Status
Timestamp (last trigger)
BGP announcements without ROA or ... Firing 12-07-2024 06:52 +10:00
BGP route not visible Firing 18-07-2024 15:51 +10:00
RPKI and IRR mismatches with BGP Clean -
Useful links
Help
Data sources
Disclaimer

Alert Notification Example

- ROA / Route mismatches

Greetings,

This is a routing status alert from DASH.

Your alert *RPKI/IRR misalignments* has been triggered.

Timestamp: 02 May 2023 15:15 UTC
Trigger: 10.0.0.0/8, 192.0.2.0/24
Incident: ROA mismatch (10.0.0.0/8), Route Object mismatch (192.0.2.0/24)

Best regards,
APNIC

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

You received this notification because you set up an alert in DASH. If you wish to edit your alert preferences or stop receiving it, please log in to DASH and edit the alert preferences or cancel it.

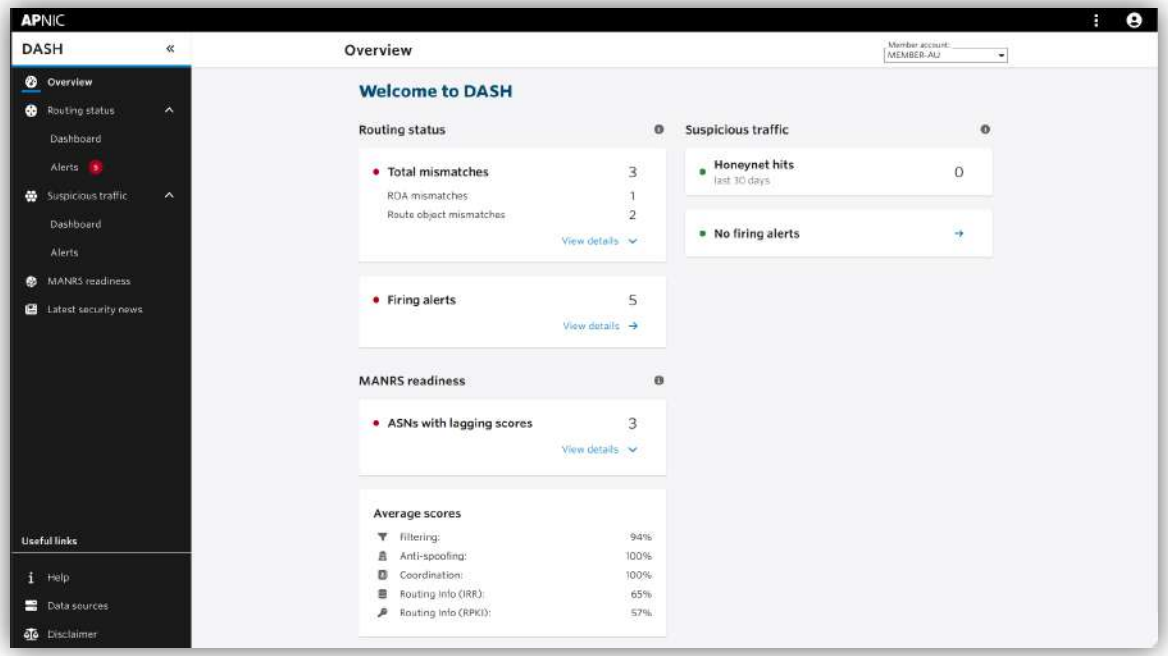
Manage your notification preferences or unsubscribe.

Supported notification options

- Email
- SMS
- Slack
- WhatsApp
- Webhooks

Suspicious Traffic

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



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.
- Alerts
  - Receive notifications about detected suspicious traffic originated by your networks.

What is a Honey pot ?

In computer security terms, a cyber honeypot works in a similar way, baiting a trap for hackers. It's a sacrificial computer system that’s intended to attract cyberattacks, like a decoy. It mimics a target for hackers, and uses their intrusion attempts to gain information about cybercriminals and the way they are operating or to distract them from other targets.

Source : kaspersky

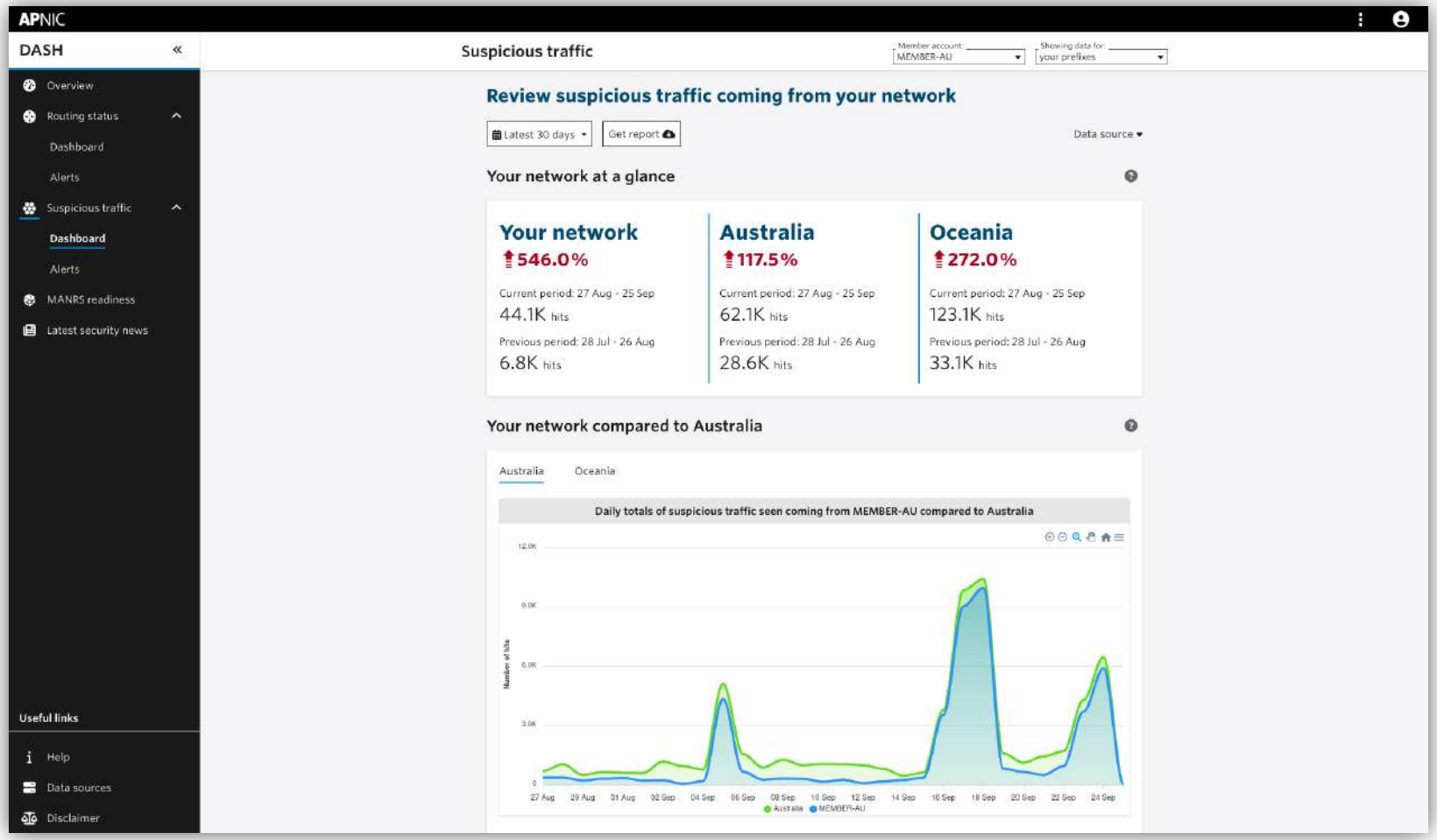
Suspicious traffic; does it matter ?

- Your network reputation
- Getting blacklisted
- Legal consequences and compliance issues
- Complaints (IRT)
- Poor user experience

2.2 Unauthorized Access in Computer Materials

Any person who, with the intention to access any program, information, or data on a computer, uses the computer without the authorization of the owner or the responsible person, or even with authorization, engages in acts contrary to the authorization, shall be liable to the following punishment:

- Fine: Not exceeding Two Hundred Thousand Rupees
- Imprisonment: Not exceeding three years

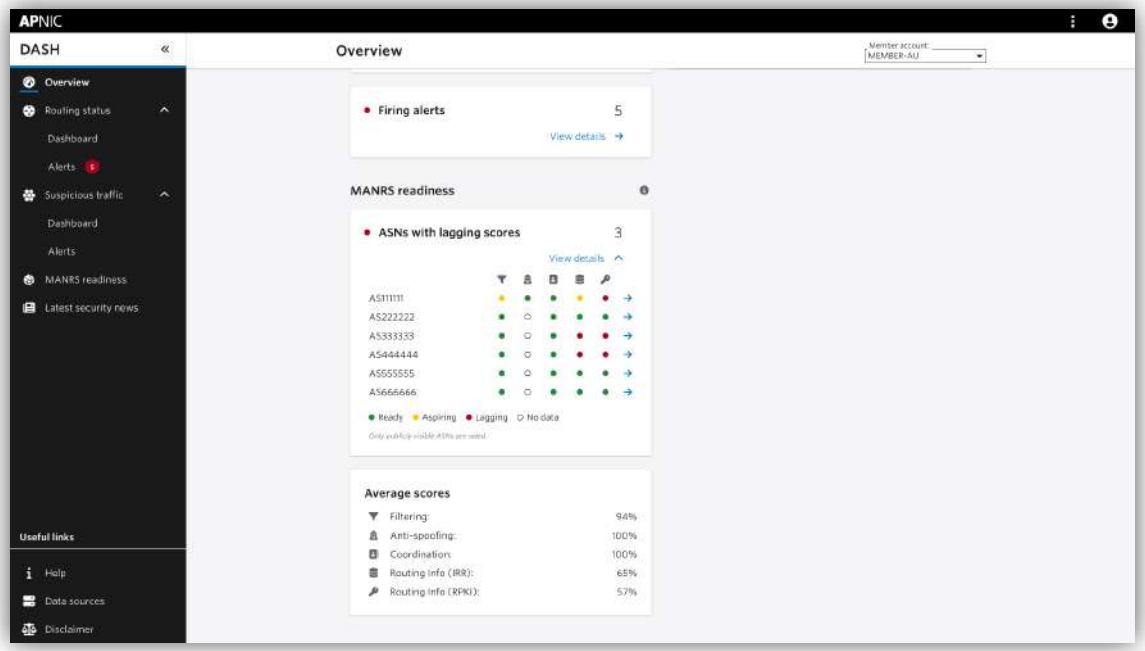

APNIC
DASH
Overview
Routing status
Dashboard
Alerts
Suspicious traffic
Dashboard
Alerts
MANRS readiness
Latest security news
Useful links
Help
Data sources
Disclaimer
Suspicious traffic
Member account:
MEMBER-AU
Showing data for:
your prefixes
Review suspicious traffic coming from your network
Latest 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
Number of hits
12.0K
9.0K
6.0K
3.0K
0
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

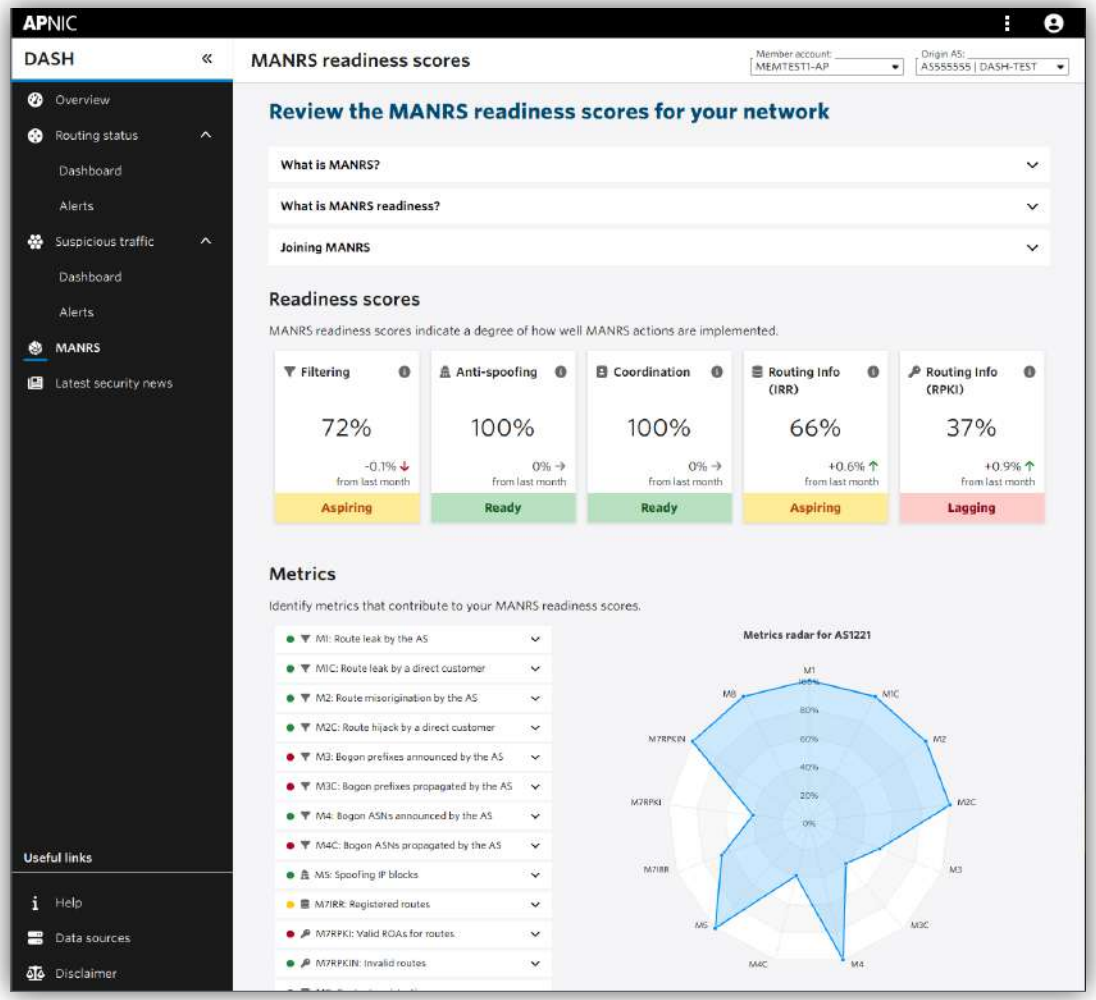
MANRS readiness

- Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Global Cyber Alliance.
- MANRS readiness indicates a degree of how well MANRS Actions are implemented. It is calculated using a set of metrics for each Action, computed from different data sources.
- We want to encourage APNIC Members to join the MANRS program and implement routing security best practices.

MANRS score

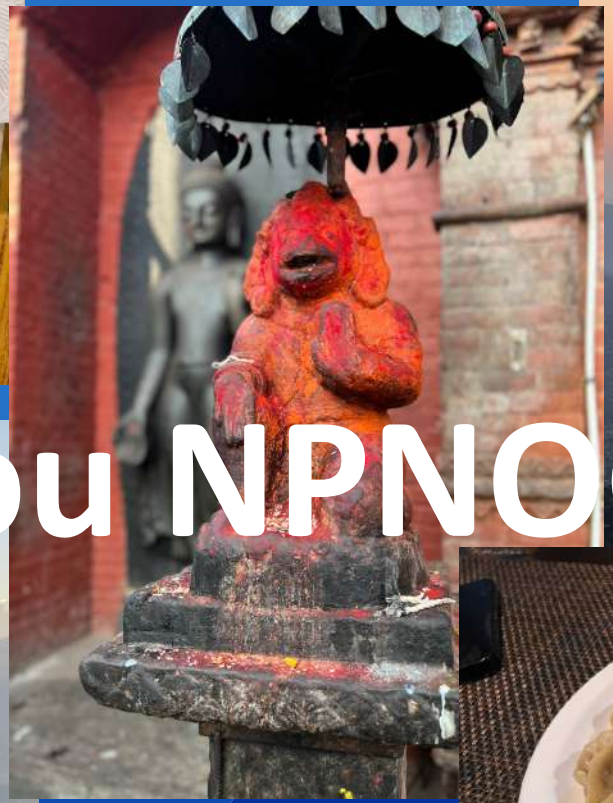
Check your network's conformance to security best practices by reviewing your MANRS readiness score.

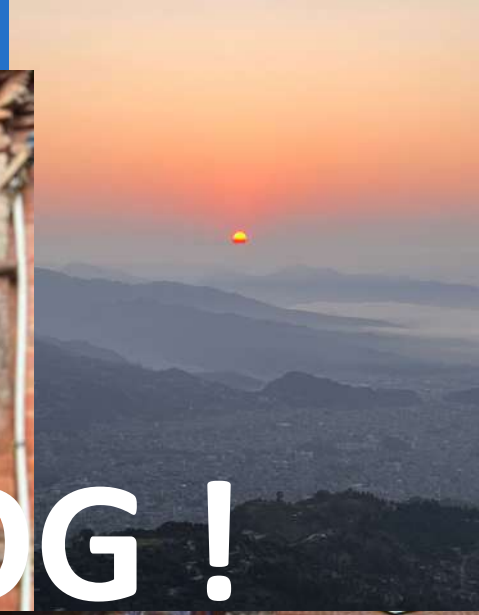



APNIC
DASH
MANRS readiness scores
Member account:
MEMTEST1-AP
Origin AS:
AS555555 | DASH-TEST
Overview
Routing status
Dashboard
Alerts
Suspicious traffic
Dashboard
Alerts
MANRS
Latest security news
Useful links
Help
Data sources
Disclaimer
Review the MANRS readiness scores for your network
What is MANRS?
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
80%
60%
40%
20%
0%

Feedback for APNIC developers ?

Need a demo ?





Thank you NPNOG !