Strengthen your Network Security with APNIC Products and Tools

APNIC Products & Tools

Andre Gelderblom
Product Manager Membership
31/03/2026

Welcome

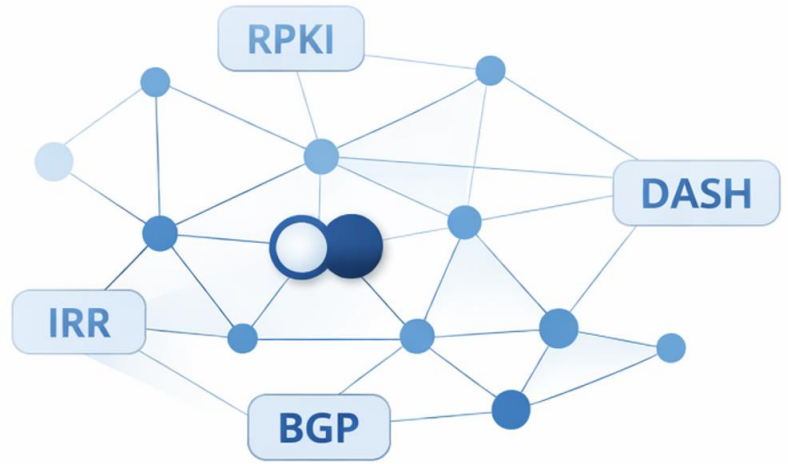
Routing Security – Current and Future Mechanisms

- Routing security uses IRR, RPKI ROAs, and route management today, with future improvements via RPKI ASPAs.

Learn How to Use APNIC DASH

- APNIC DASH visualises BGP security, sends alerts for routing issues and suspicious traffic, and helps assess vulnerabilities and MANRS compliance.

Questions



What's available through APNIC?

APNIC helps strengthen network security with tools and services that can help you.

Learn

Training & support

Learn

Training & support

Connect

Community & knowledge sharing

Connect

Community & knowledge sharing

Operate

Practical tools & services

Operate

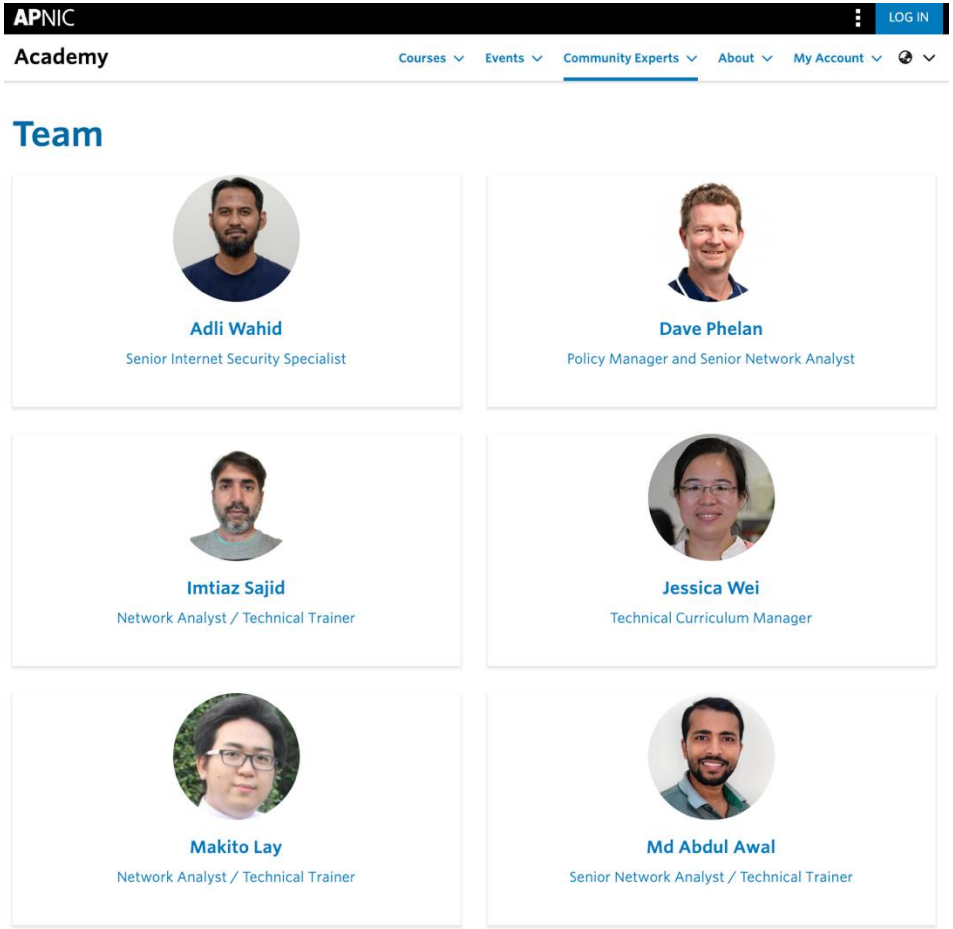
Practical tools & services

Learn

Training, support, and guidance to build capability

APNIC Academy

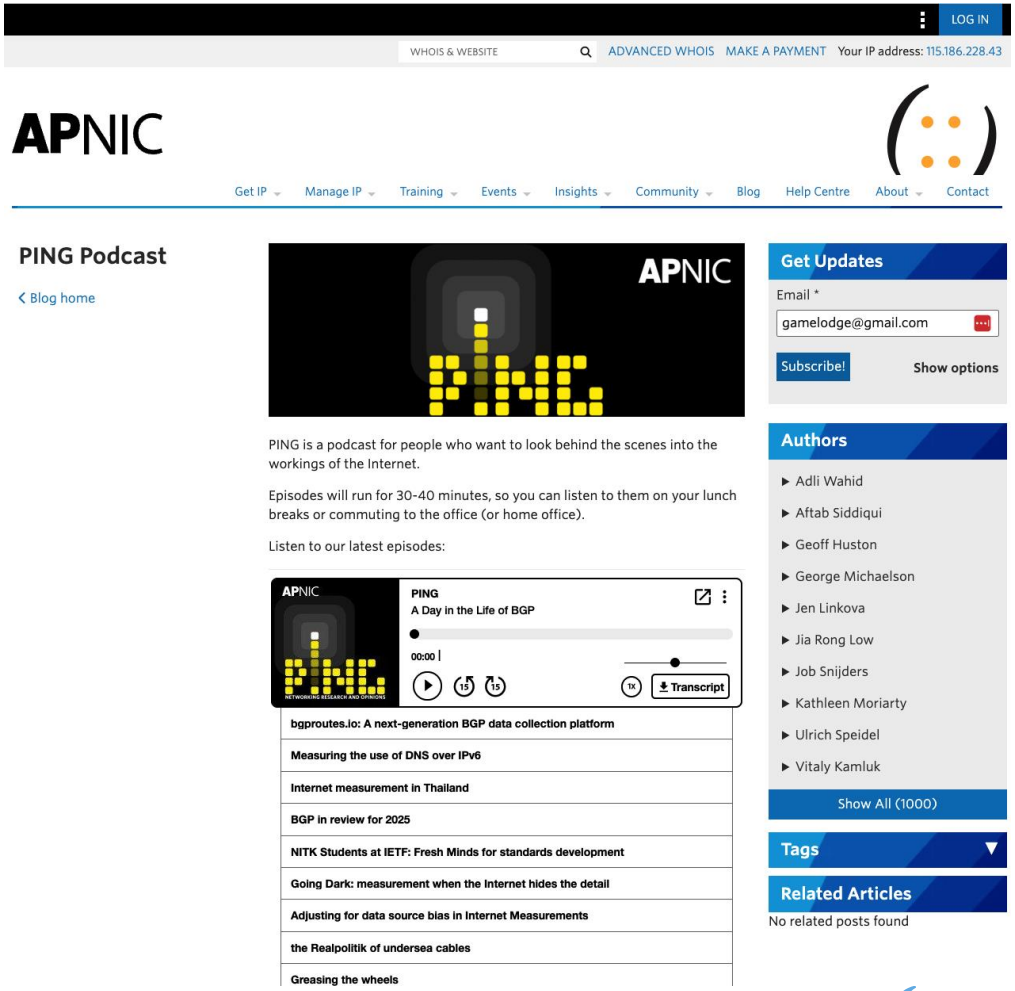
- Online courses
- Virtual labs
- Webinars
- Technical assistance



Connect

Community, discussion, and shared knowledge

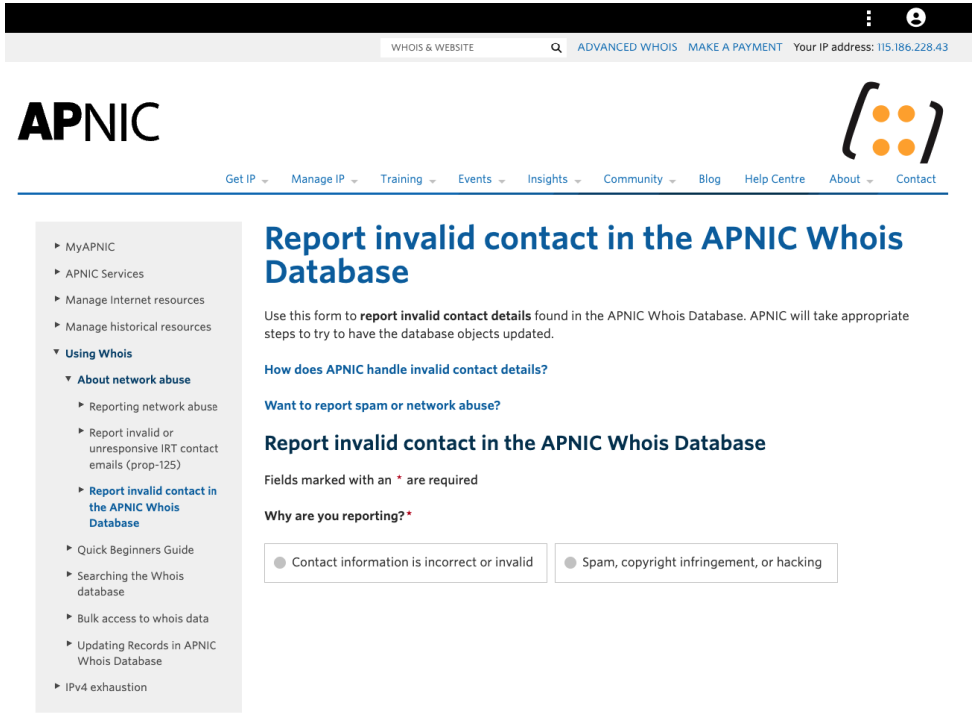
- Mailing lists
- APNIC Blog
- PING podcast



Operate

Tools and services that help Members manage and monitor in practice

- MyAPNIC
- DASH
- Rex
- RDAP
- Report Invalid

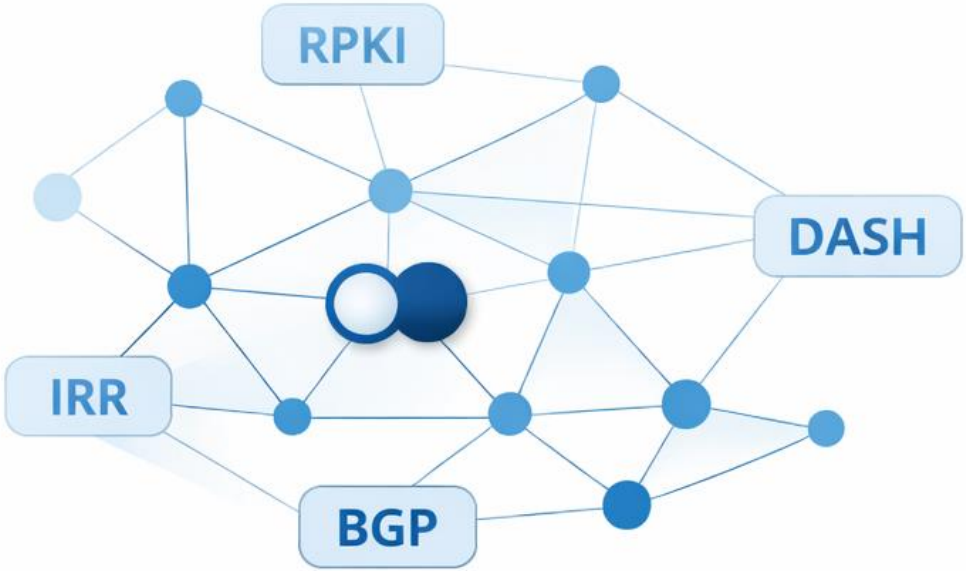


Hands on

Learn

Connect

Operate



Strengthen your Network Security with APNIC Products and Tools

Current and Future Routing Security Mechanisms

Tom Harrison
Product Manager Registry
31/03/2026

Topics

- Current Routing Security Mechanisms
  - Internet Routing Registry (IRR)
    - `route` objects
    - `as-set` objects
  - Resource Public Key Infrastructure (RPKI)
    - Route Origin Authorization (ROA) objects
- Future Routing Security Mechanisms
  - RPKI
    - Autonomous System Provider Authorization (ASPA) objects

Internet Routing Registry (IRR)

- The set of servers that host Routing Policy Specification Language (RPSL, RFC 2622 & 4012) objects
- Two types of server:
  - Authoritative: hosted by RIRs directly
  - Non-authoritative: hosted by third parties
- Current objects and structures mostly in place by the mid-1990s, with the RADb and RIPE servers
- Most clients today rely on the various RIR-hosted servers and/or RADb

IRR `route` objects

- A declaration that the specified origin AS may originate announcements for the specified IP address prefix

```
route:          202.12.29.0/24
descr:          APNIC Network
country:        AU
origin:         AS4608
mnt-by:         MAINT-APNIC-IS-AP
last-modified:  2018-11-20T03:20:12Z
source:         APNIC
```

IRR `route` objects - filtering

```
$ bgpq4 -S APNIC AS4608
no ip prefix-list NN
ip prefix-list NN permit 202.12.29.0/24
ip prefix-list NN permit 203.119.76.0/23
ip prefix-list NN permit 203.119.100.0/22
ip prefix-list NN permit 203.119.104.0/21
ip prefix-list NN permit 203.133.248.0/23
ip prefix-list NN permit 203.133.248.0/24
$
```

IRR `as-set` objects

- A user-defined collection of ASNs
- Often used to document the ASNs that are customers of a given provider

```
as-set:          AS4608:AS-CUSTOMERS
descr:           AS4608 Downstream ASNs
tech-c:          TN433-AP
admin-c:         HM20-AP
mnt-by:          MAINT-APNIC-IS-AP
members:         AS18366,AS18367,AS18368
members:         AS18369,AS18370,AS9545
members:         AS55638,AS131072,AS131074
members:         AS45192,AS7500,AS26415
members:         AS396628,AS25152,AS10906
members:         AS4777
last-modified:   2025-03-18T04:38:17Z
source:          APNIC
```

IRR `as-set` objects - filtering

```
$ bgpq4 -S APNIC AS4608:AS-APNIC
no ip prefix-list NN
ip prefix-list NN permit 103.0.0.0/16
ip prefix-list NN permit 103.0.0.0/24
ip prefix-list NN permit 103.0.1.0/24
ip prefix-list NN permit 103.0.2.0/24
ip prefix-list NN permit 103.0.3.0/24
...
```

Resource Public Key Infrastructure (RPKI)

- A PKI for IP addresses and ASNs
- Operated by the five Regional Internet Registries (RIRs)
- Initial standards finalised in 2012, but services had been offered for some years before that (e.g. 2009 for APNIC)

RPKI Route Origin Authorization (ROA) objects

- Conceptually, very similar to an IRR route object: a declaration that the specified origin AS may originate announcements for the specified IP address prefix
- Differences:
  - Cryptographically-verifiable signed object
  - Supports `max-length` field


```
{
  "type": "roa",
  "ski": "5EC217D57839B2FD634F497BAD3B26896D1A477A",
  "cert_issuer": "/CN=A91DC5BE/serialNumber=...",
  "cert_serial": "3611",
  "aki": "ADA8AED32B15B87E611252D29D1E1D5BDE581646",
  "aia": ".../raiu0ysVuH5hElLSnR4dW95YFkY.cer",
  "sia": ".../DB3F9CA4817B11F0BDC51985C4F9AE02.roa",
  "signing_time": 1772385496,
  "valid_since": 1756102941,
  "valid_until": 1932681600,
  "expires": 1775312187,
  "vrps": [
    { "prefix": "202.12.29.0/24",
      "asid": 4608,
      "maxlen": 24 },
    ...
  ],
  "validation": "OK"
}
```

RPKI ROA objects – filtering (1)

- IRR filtering is based on generating static filter lists, and then configuring the router to use those lists
  - Manual or semi-manual update process
  - Filter list size can cause problems
  - Filters generally either apply or do not apply – binary
- RPKI filtering uses a different model: the router receives the raw RPKI data (via the rpki-rtr protocol), and then performs the validation itself
  - RPKI updates propagate to the router automatically
  - Router is then configured in terms of the validation result: e.g., if validation fails, drop route

RPKI ROA objects – filtering (2)

Operation	Condition	Result
Find all ROAs that have an address range that matches or is larger than that of the announcement	If this set is empty:	
Otherwise: find any ROA that has a max-length that encompasses the address range from the announcement	If no such ROA exists:	
Otherwise:		

MyAPNIC Route Management (1)

Register your routes in MyAPNIC using the tool below. It will automatically create route objects in the APNIC Whois Database with any AS number you have authorized. RPKI ROAs will also be created at the same time, if the ROA option is enabled (changes to RPKI may take around fifteen minutes to propagate, so the ROA status will not be updated until then).

+ Add new

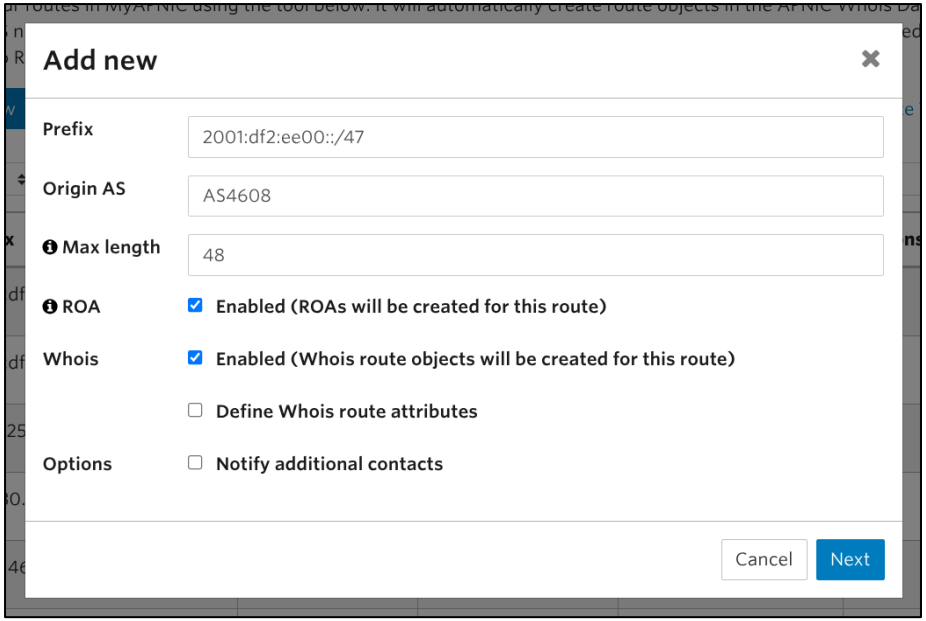
View Route Task Log

Show 10 entries

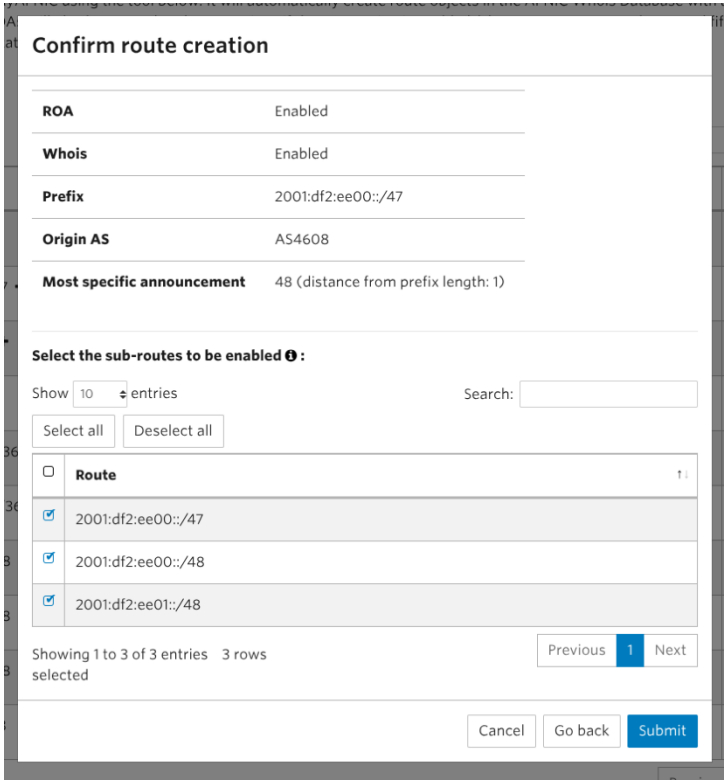
Search:

Prefix	Origin AS	ROA status	Whois status	Actions
2001:df0:a::/48	AS45192	EXISTS	EXISTS	
2001:df2:ee00::/47 +	AS45192	EXISTS	EXISTS	
202.125.96.0/23 +	AS45192	EXISTS	EXISTS	
203.30.127.0/24	AS45192	EXISTS	EXISTS	
2401:4601:1000::/36	AS135533	DISABLED	EXISTS	

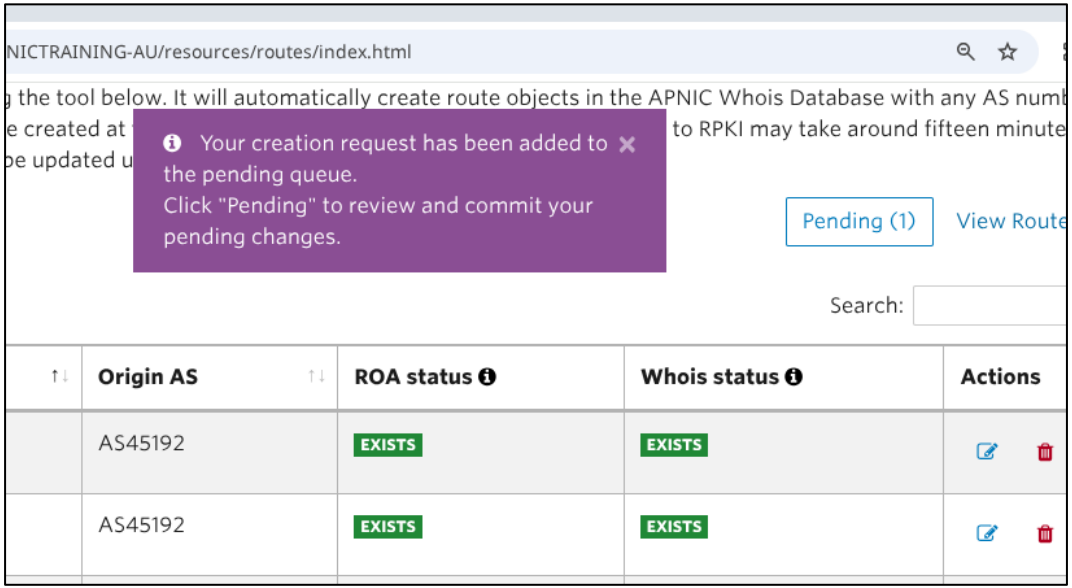
MyAPNIC Route Management (2)



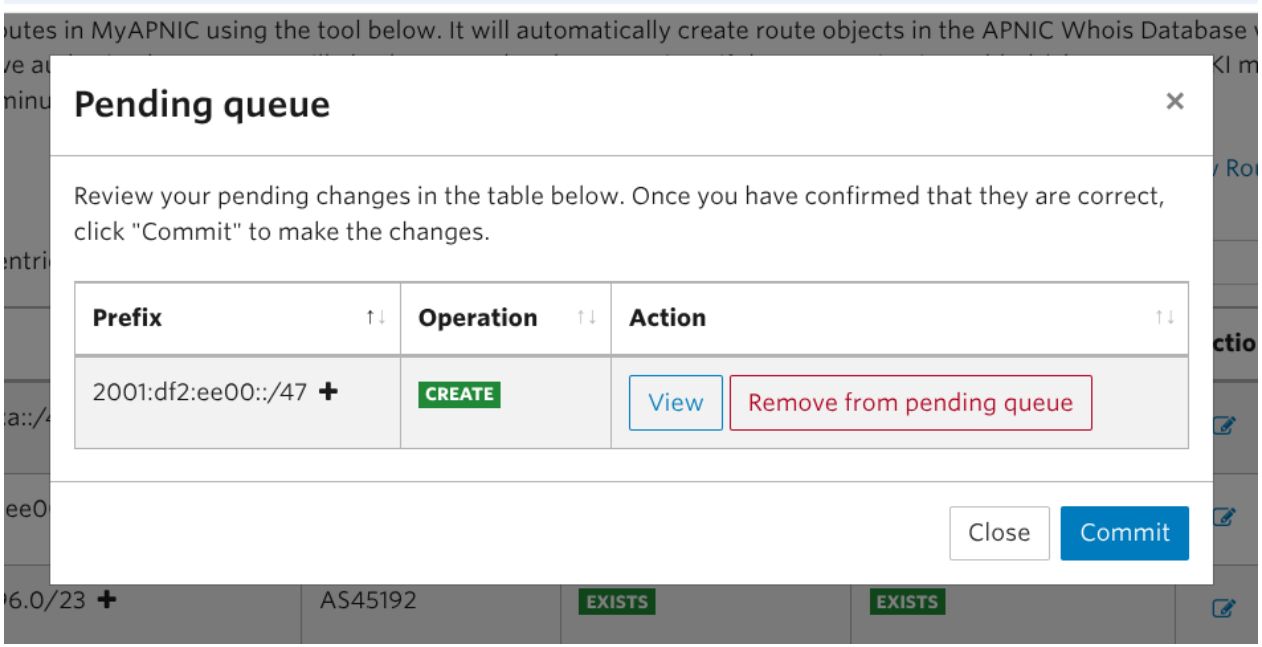
MyAPNIC Route Management (3)



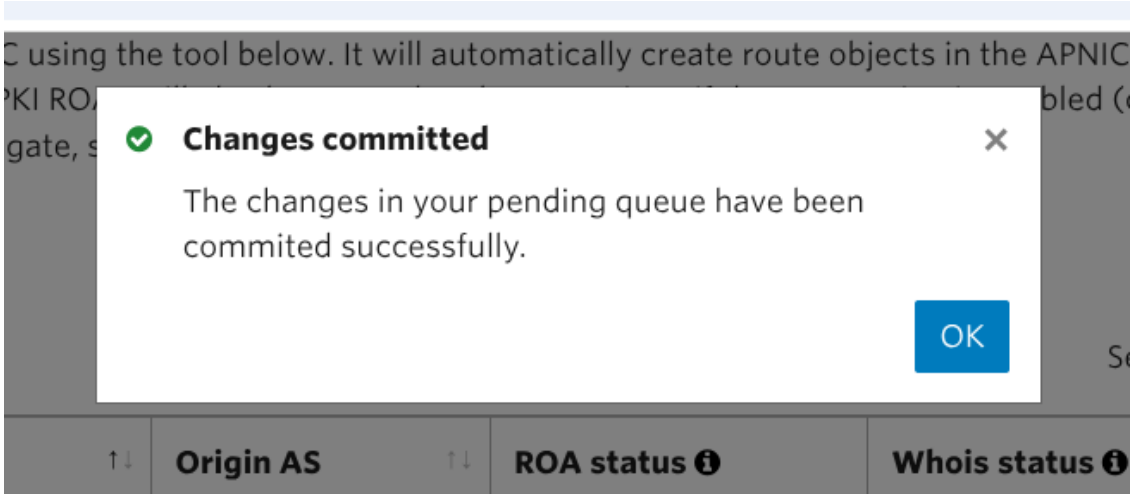
MyAPNIC Route Management (4)



MyAPNIC Route Management (5)



MyAPNIC Route Management (6)



RPKI ASPA objects

- Autonomous System Provider Authorization (ASPA) objects
- A declaration by an ASN holder as to its providers: i.e., those ASNs through which it sends its own announcements, or receives announcements from others
- Currently supported by RIPE and ARIN, with other RIRs following later this year


```
{
  "type": "aspa",
  "ski": "7D18690BD23189FC606BDBB8454CE812A0F7C8DB",
  "aki": "DD8984A82671DD60AA7980ACF2402EF6DA98721C",
  "sia": ".../AS24381.asa",
  "signing_time": 1772229702,
  "valid_since": 1772229402,
  "valid_until": 1803679302,
  "expires": 1774866647,
  "customer_asid": 24381,
  "providers": [
    24322,
    39521,
    44324,
    62553,
    215956
  ],
  "validation": "OK"
}
```

RPKI ASPA objects – upstream filtering

Condition	Result
If AS-path has single entry:	
If AS-path contains hop from provider to customer:	
If AS-path contains hop without ASPA:	
Otherwise, all hops are from customer to provider:	

RPKI ASPA objects – downstream filtering

Condition	Result
If AS-path comprises: • Up-ramp (customers to providers); • Down-ramp (providers to customers); and • Either no hop in the middle, or single lateral hop:	
If AS-path contains valley (hop from provider to customer, then customer to provider):	
Otherwise, unable to determine validity:	

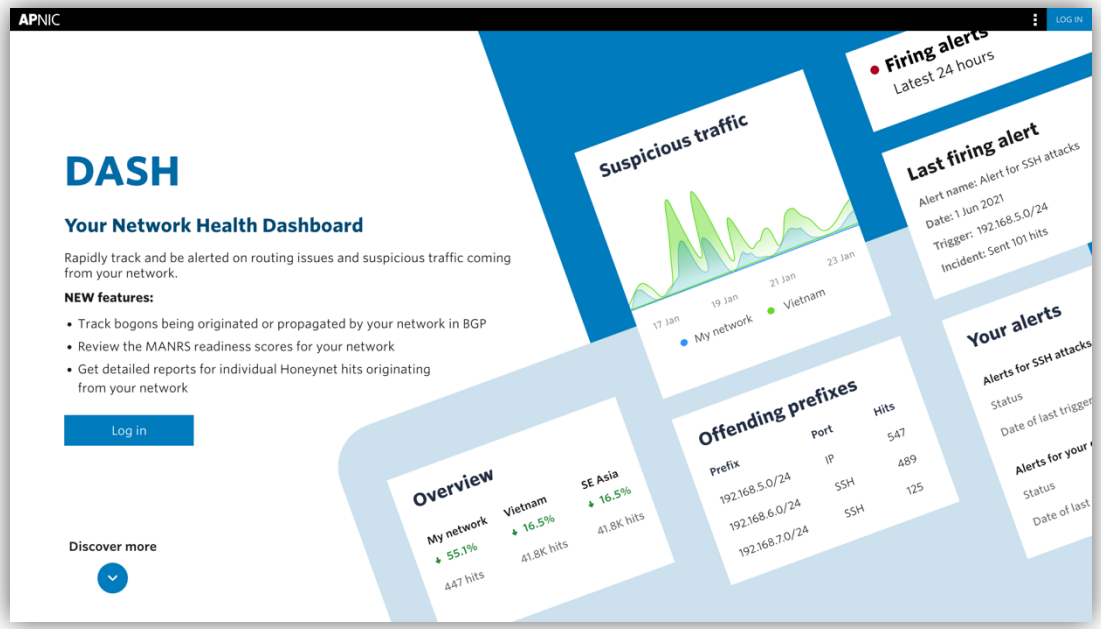
Strengthen your Network Security with APNIC Products and Tools

APNIC DASH

Rafael Cintra
Product Manager Information
31/03/2026

DASH

- APNIC's Network Health Dashboard
- Available to all APNIC Members at dash.apnic.net

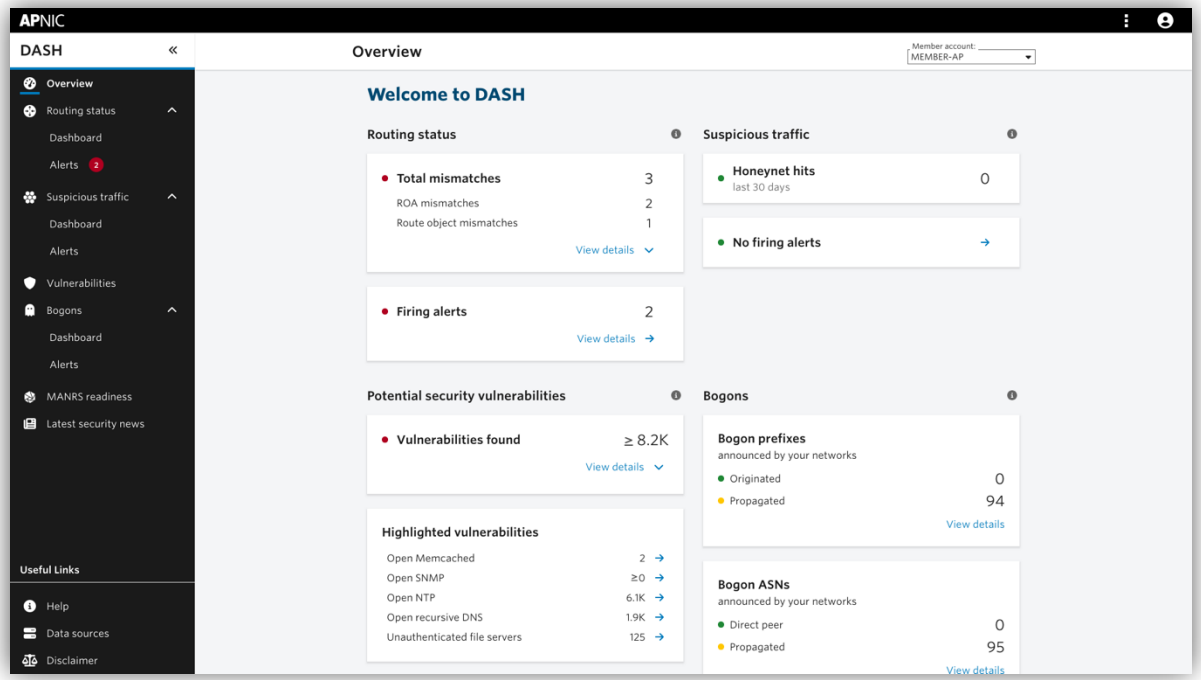


DASH Services

- Current Services
  - Routing status
  - Suspicious traffic
  - Potential security vulnerabilities
  - Bogons
  - MANRS readiness score

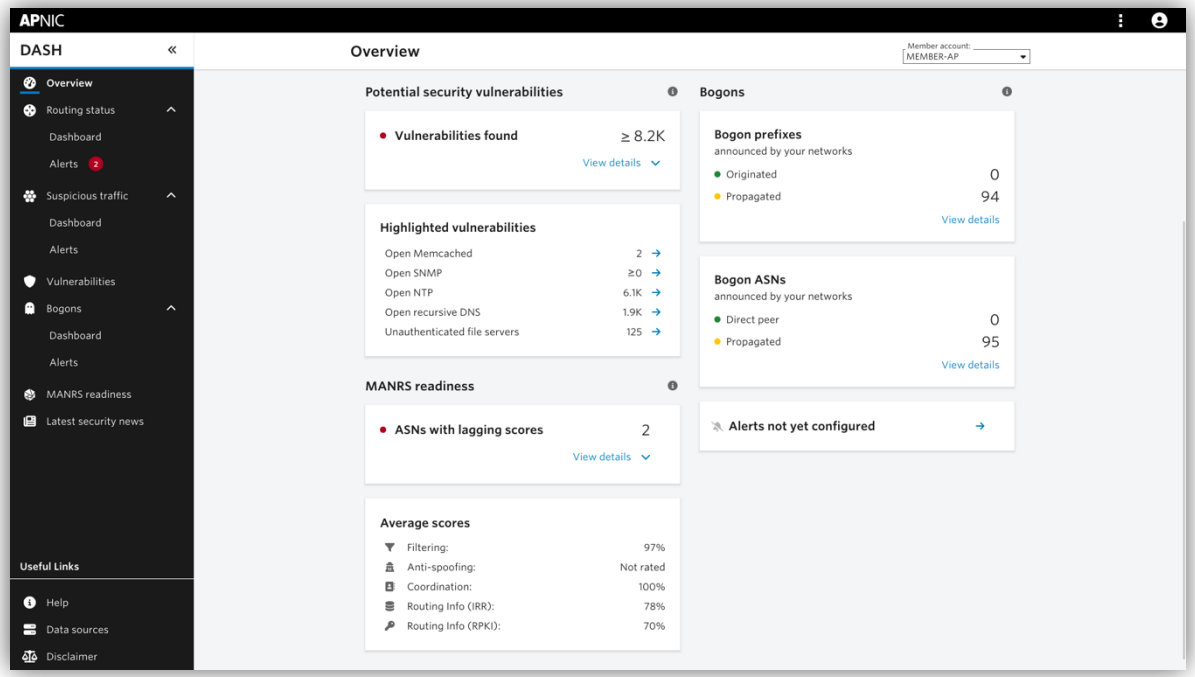
Overview Page

Review the summary of routing status and suspicious traffic issues and alerts.



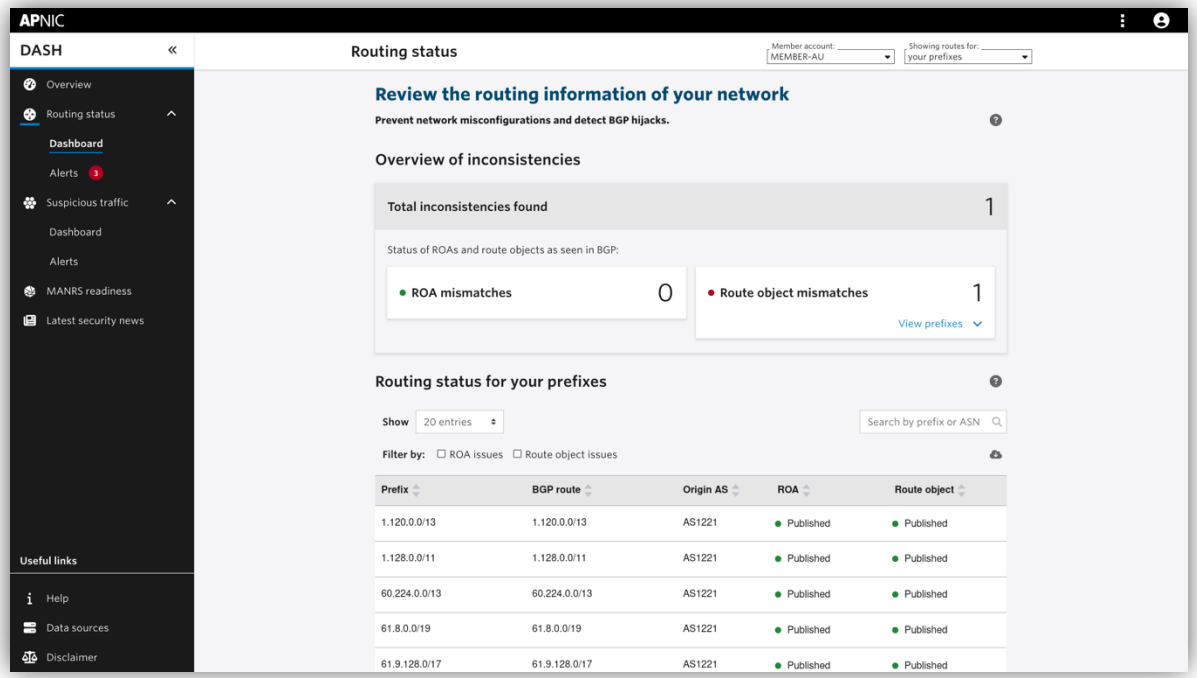
Overview Page

Review the summary of potential security vulnerabilities, Bogons (including alerts) and MANRS readiness scores.

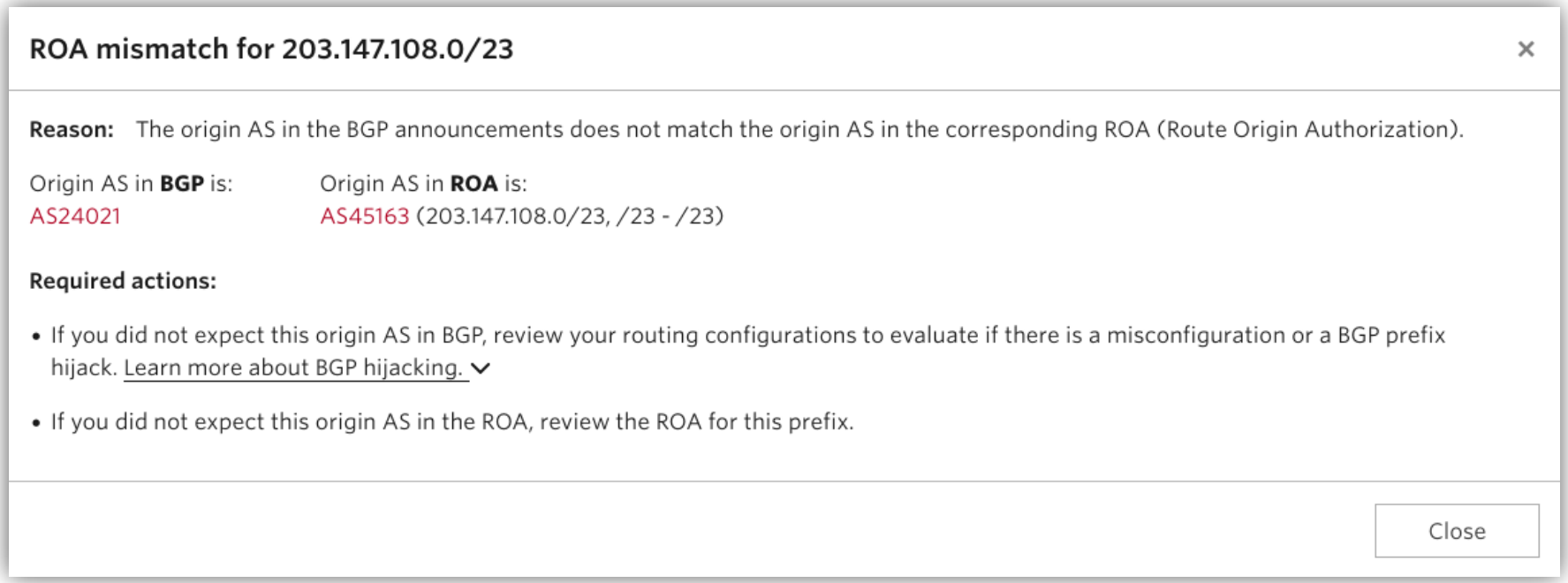


Routing status

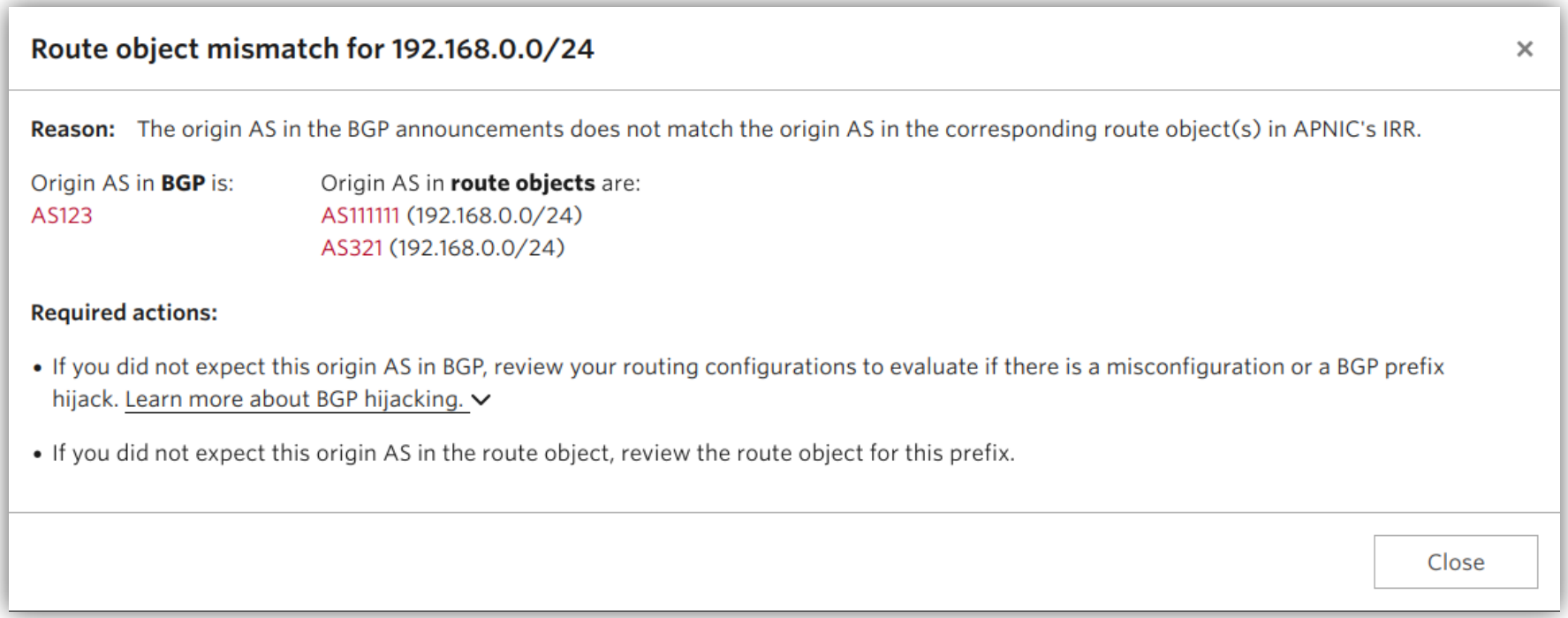
Provides a full picture of all BGP announcements for your network and track inconsistencies against RPKI ROAs and IRR Route Objects.



ROA mismatch example



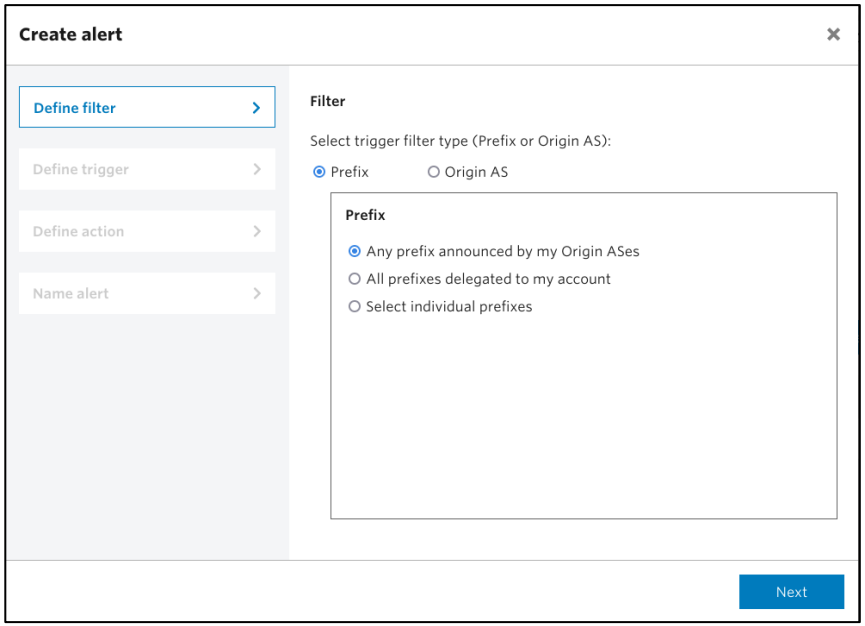
Route object mismatch example

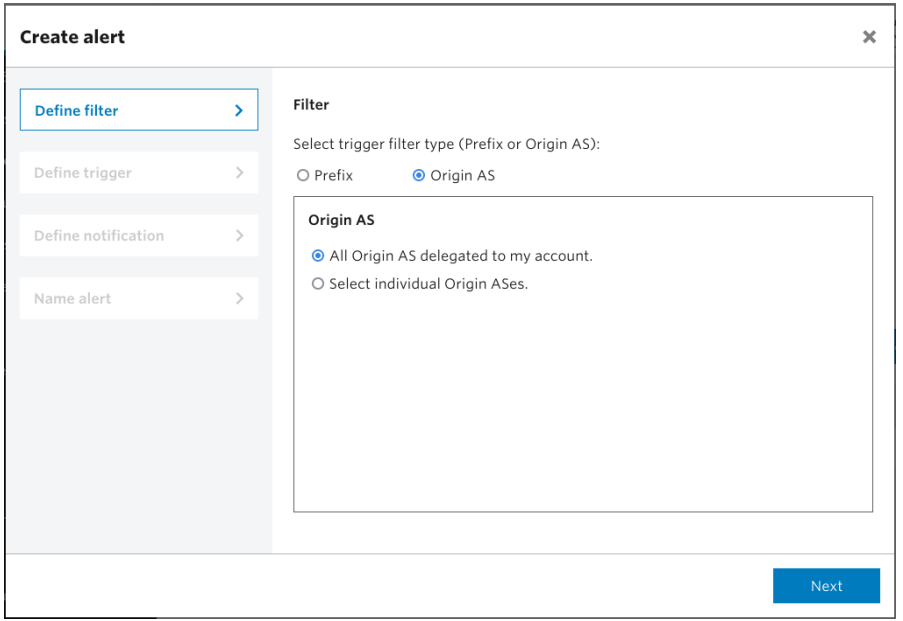


Routing status alerts

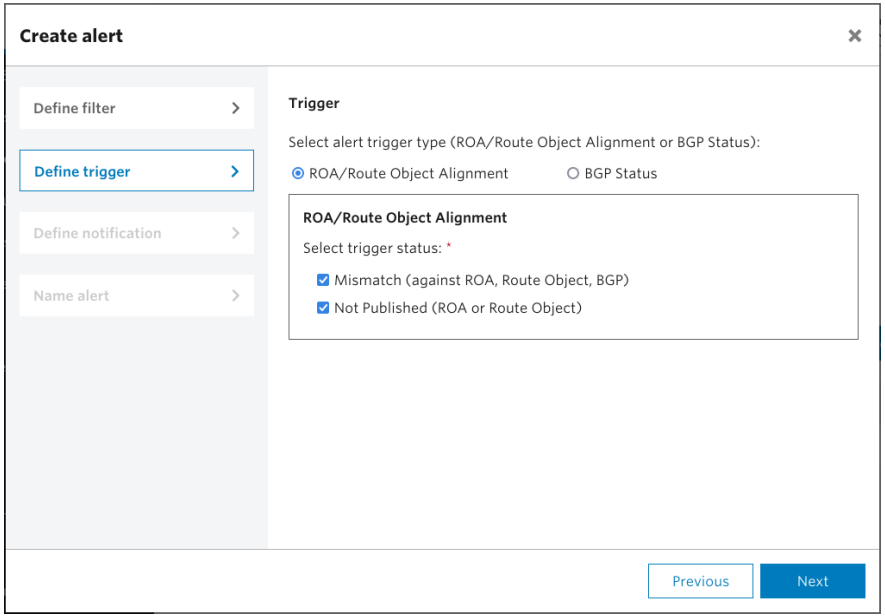
- Receive notifications about misalignments among BGP, RPKI and IRR (e.g. RPKI invalids and missing ROAs and IRR route objects).
- Receive notifications about BGP announcements for unexpected AS origins, detecting potential BGP hijacks.
- Receive notifications about loss of visibility for routes in BGP,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

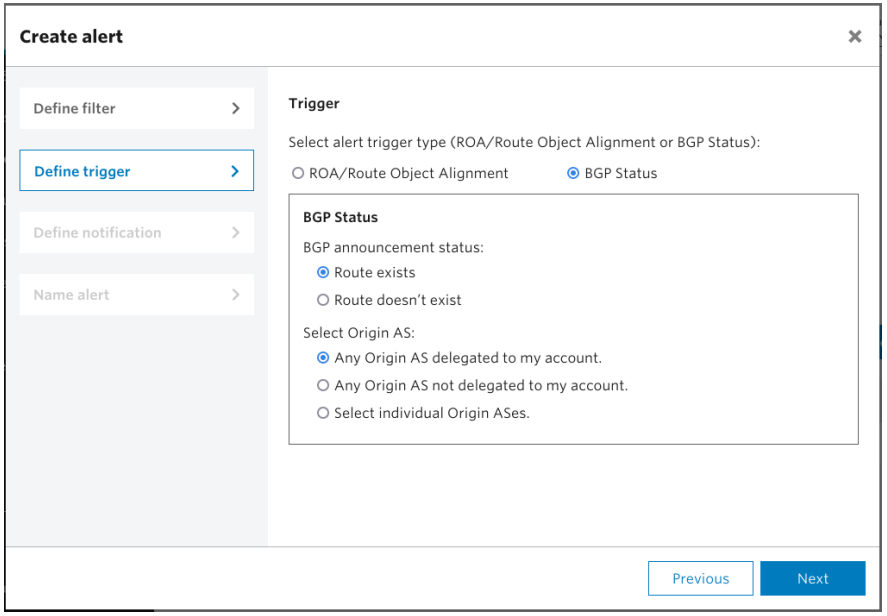
Alert Filters





Alert Triggers





Supported notification options

- Email
- SMS
- Slack
- WhatsApp
- Webhooks
- Discord

Alert Notification Example

- ROA / Route mismatches

Greetings,

This is a routing status alert from DASH.

Your alert *Any RPKI/IRR misalignments or not published* is currently firing.

Timestamp: 18 March 2025 12:07 UTC
Triggering: 10.0.0.0/8, 192.0.2.0/24

New problems:

ROA mismatch (10.0.0.0/8)

Best regards,
APNIC

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

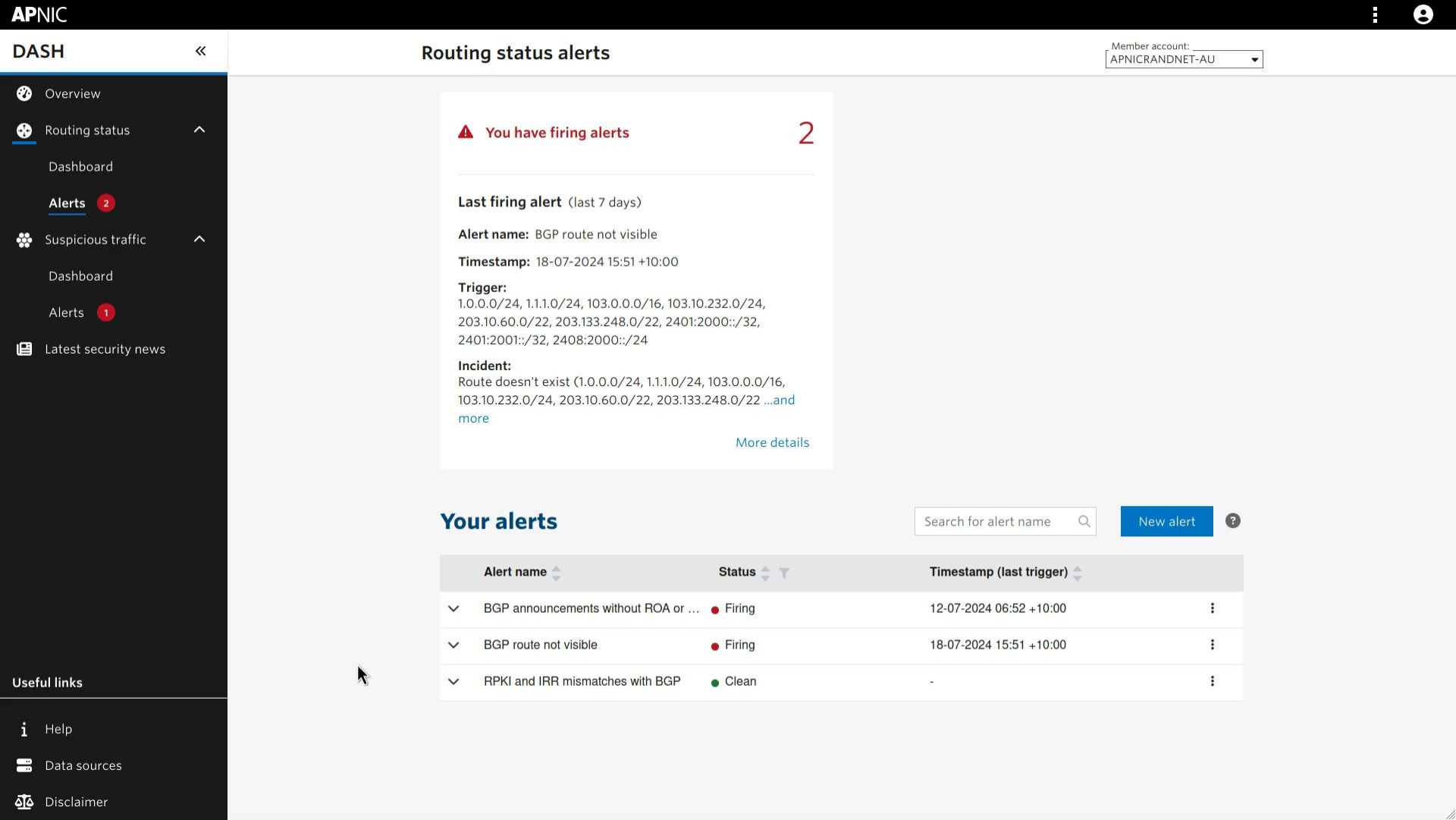
You received this notification because your email address was set as a DASH alert recipient. If you created the alert, you can log into DASH and edit your alert preferences.

Manage your notification preferences or unsubscribe.

Use case 1
Potential BGP hijacks

Potential BGP hijack alert

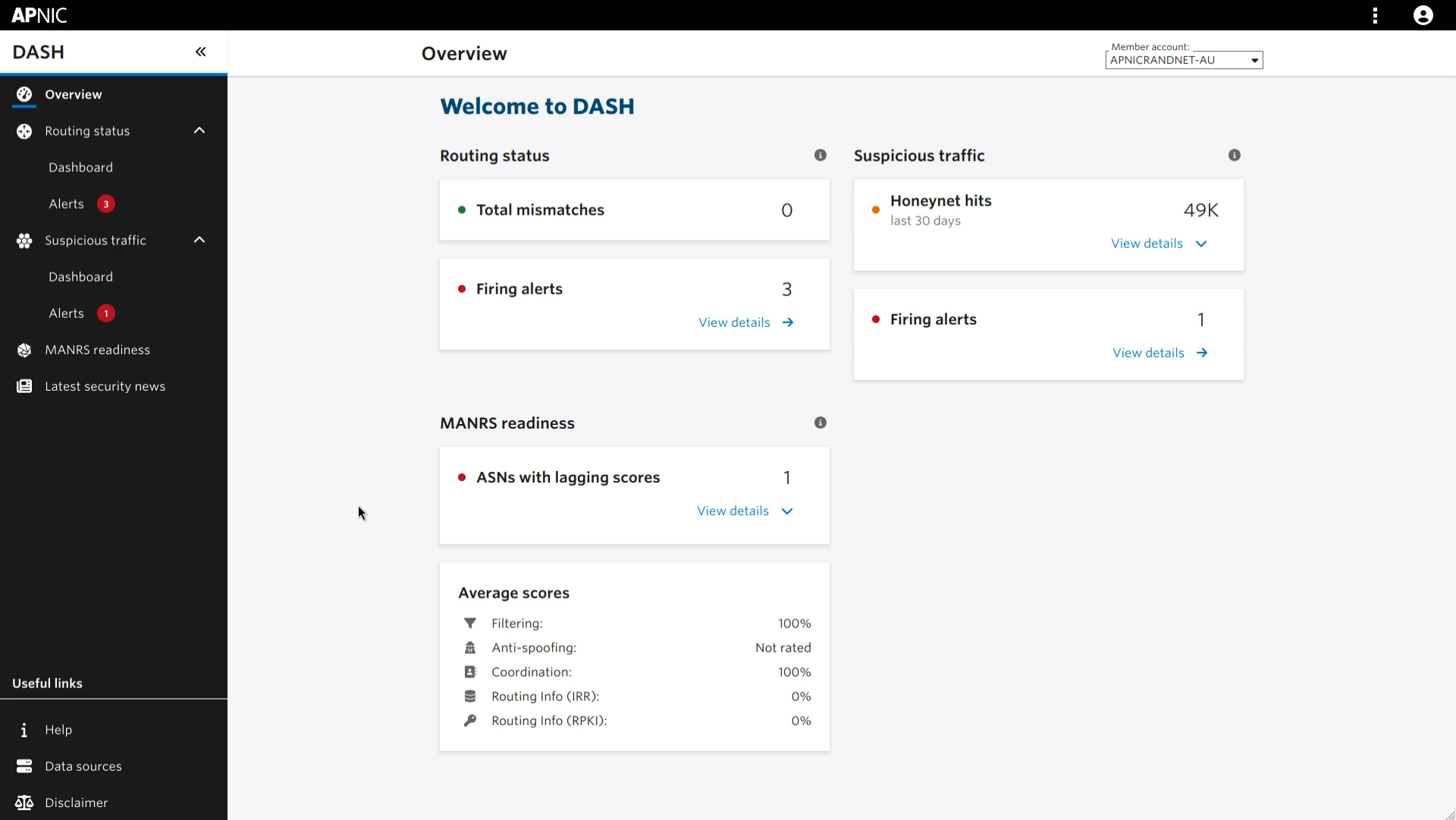
- Filter
  - All prefixes delegated to your account.
- Trigger
  - BGP Status
    - Route exists
    - For any origin AS **not** delegated to your account


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

Use case 2
BGP visibility issues

Route not visible in BGP alert

- Filter
  - Select the route prefix
- Trigger
  - BGP Status
    - Route doesn’t exist
    - Select the AS that should always be originating the prefix


APNIC
DASH
Overview
Member account:
APNICRANDNET-AU
Overview
Routing status
Dashboard
Alerts 3
Suspicious traffic
Dashboard
Alerts 1
MANRS readiness
Latest security news
Useful links
Help
Data sources
Disclaimer
Welcome to DASH
Routing status
Total mismatches 0
Firing alerts 3
View details
Suspicious traffic
Honeynet hits
last 30 days
49K
View details
Firing alerts 1
View details
MANRS readiness
ASNs with lagging scores 1
View details
Average scores
Filtering: 100%
Anti-spoofing: Not rated
Coordination: 100%
Routing Info (IRR): 0%
Routing Info (RPKI): 0%

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 400 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.

APNIC

DASH

Suspicious traffic

Member account: MEMBER-AU

Showing data for: your prefixes

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

Useful links

- Help
- Data sources
- Disclaimer

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

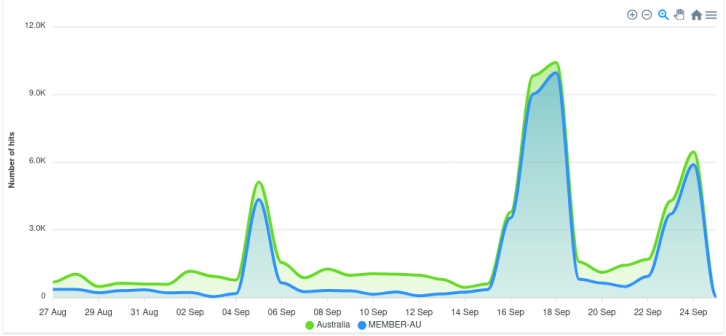
Australia
117.5%
Current period: 27 Aug - 25 Sep
62.1K hits
Previous period: 28 Jul - 26 Aug
28.6K hits

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

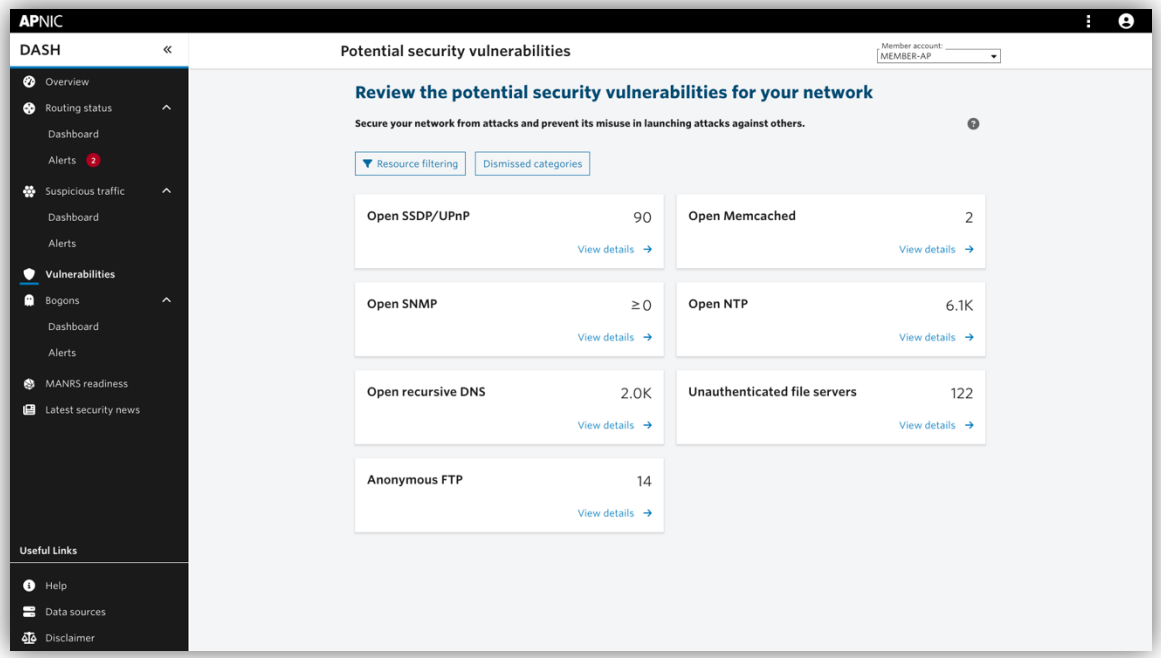
Australia | Oceania

Daily totals of suspicious traffic seen coming from MEMBER-AU compared to Australia

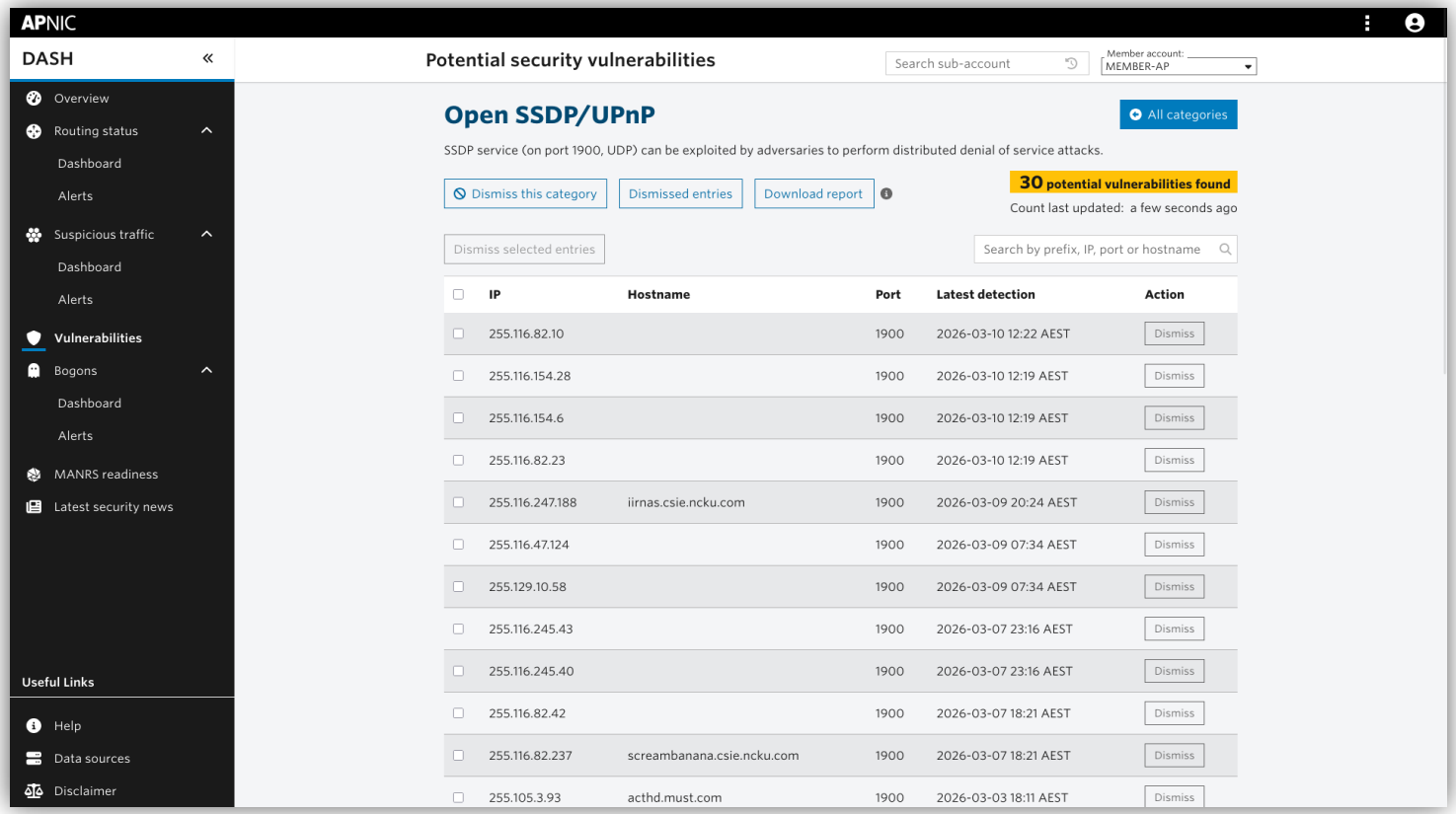


Potential security vulnerabilities

- Uses 3rd party security database: Shodan
- Vulnerabilities list curated by APNIC's security and network experts
- Helps mitigate risks to system integrity and data confidentiality.
- Prevents networked computers from being exploited to amplify DDoS attacks, protecting both our Member's systems and the broader Internet infrastructure.

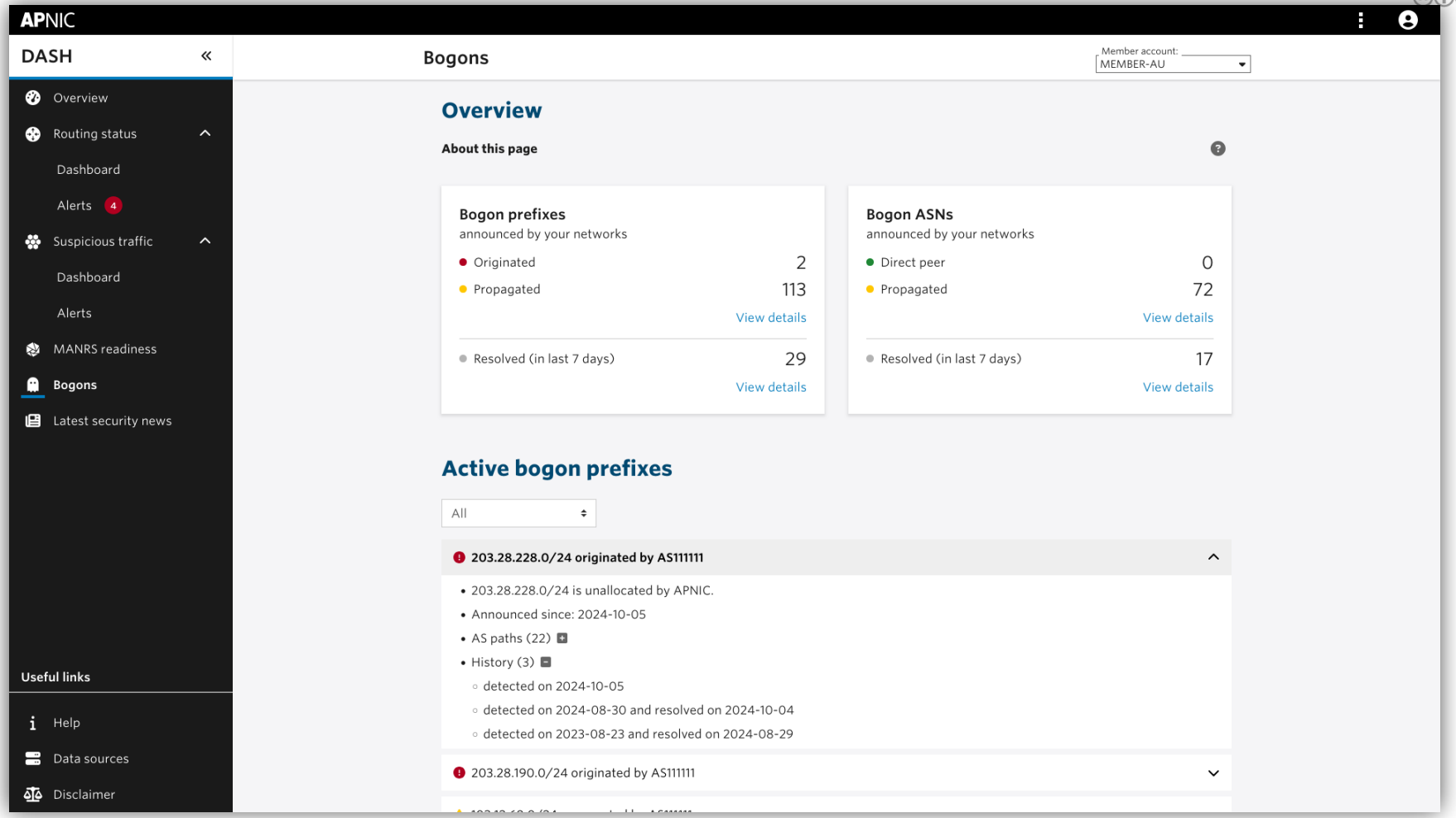


Vulnerabilities details



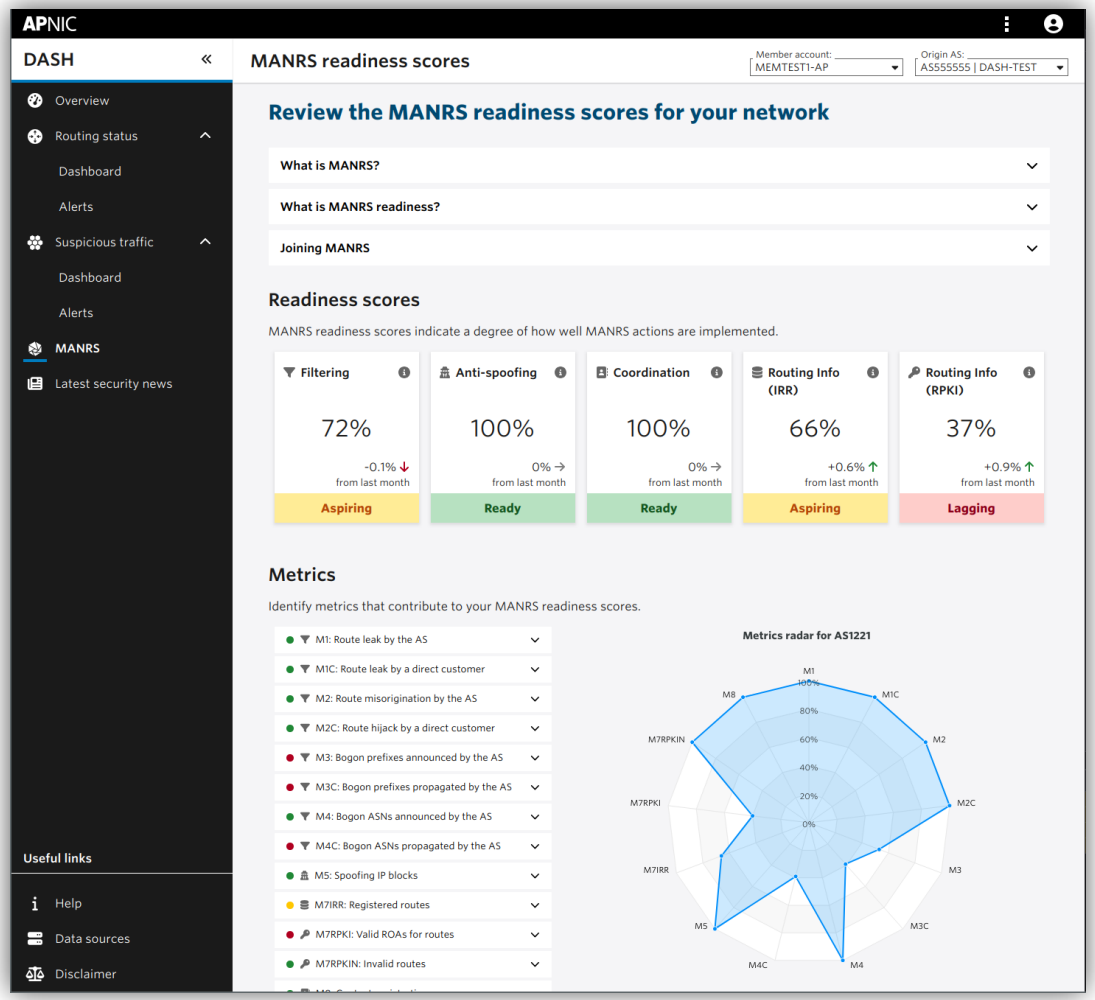
Bogons

- Bogons refer to address space which should not be routed in the public Internet. They are comprised of addresses either not allocated by IANA or RIRs, or by addresses reserved for special use, such as 192.168.0.0/16.
- DASH displays bogons either originated or propagated by your networks in BGP.
- Bogon data is updated daily


APNIC
DASH
Overview
Routing status
Dashboard
Alerts 4
Suspicious traffic
Dashboard
Alerts
MANRS readiness
Bogons
Latest security news
Useful links
Help
Data sources
Disclaimer
Bogons
Member account:
MEMBER-AU
Overview
About this page
Bogon prefixes
announced by your networks
Originated 2
Propagated 113
View details
Resolved (in last 7 days) 29
View details
Bogon ASNs
announced by your networks
Direct peer 0
Propagated 72
View details
Resolved (in last 7 days) 17
View details
Active bogon prefixes
All
203.28.228.0/24 originated by AS111111
203.28.228.0/24 is unallocated by APNIC.
Announced since: 2024-10-05
AS paths (22)
History (3)
detected on 2024-10-05
detected on 2024-08-30 and resolved on 2024-10-04
detected on 2023-08-23 and resolved on 2024-08-29
203.28.190.0/24 originated by AS111111

MANRS readiness

- Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by 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.


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 misoriginated 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%

Strengthen your Network Security with APNIC Products and Tools

Questions