Muslina Devi Nurhemdi
muslina.nurhemdi@tm.com.my

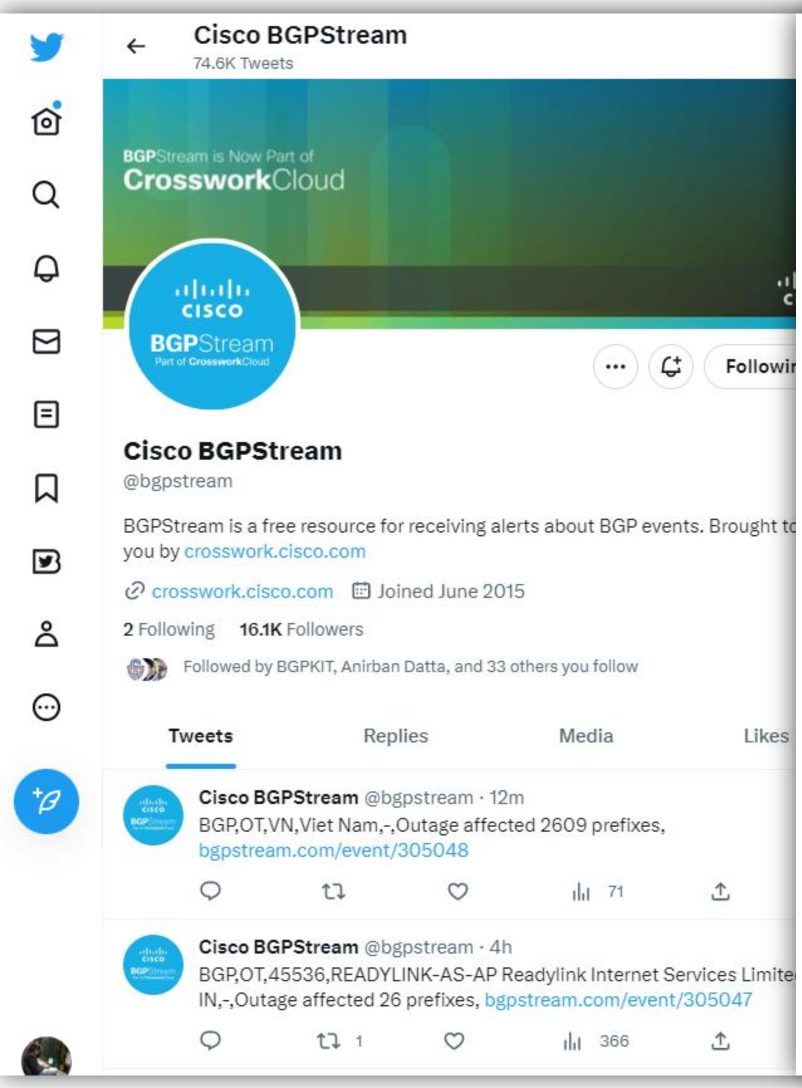
Telekom Malaysia RPKI Deployment

Problem Statement: Route Hijacking in TM’s Network Infrastructure Before RPKI Deployment

Background:
Route hijacking, a form of BGP attack, occurs when a malicious or misconfigured network announces IP prefixes it does not own. This misleads other networks into directing traffic through unintended paths, potentially leading to data interception, service disruption, or denial of service.

	Sample Case - Impacted	Sample Case - Not Impacted
When	5 Feb 2021	2 Apr 2022
What	Campana hijacked Twitter route and advertise to internet	SPT Vietnam hijack route Akamai in TM network.
How it happened and mitigation work	TM saw the best route to Twitter is via Campana. TM sent traffic user to Campana and being blackhole. Manually rejected routes at peering sites with Campana.	Akamai had registered ROA, mentioning the prefix only valid to be advertised by Akamai and TM. Telstra, which already have validator, saw the IP as invalid route, because at that time Akamai already register ROA. Hence, no effect to TM user accessing Akamai in MY.

YOUR NEXT IS NOW TM



Cisco BGPStream
74.6K Tweets

BGPStream is Now Part of CrossworkCloud

Cisco BGPStream
@bgpstream

BGPStream is a free resource for receiving alerts about BGP events. Brought to you by crosswork.cisco.com

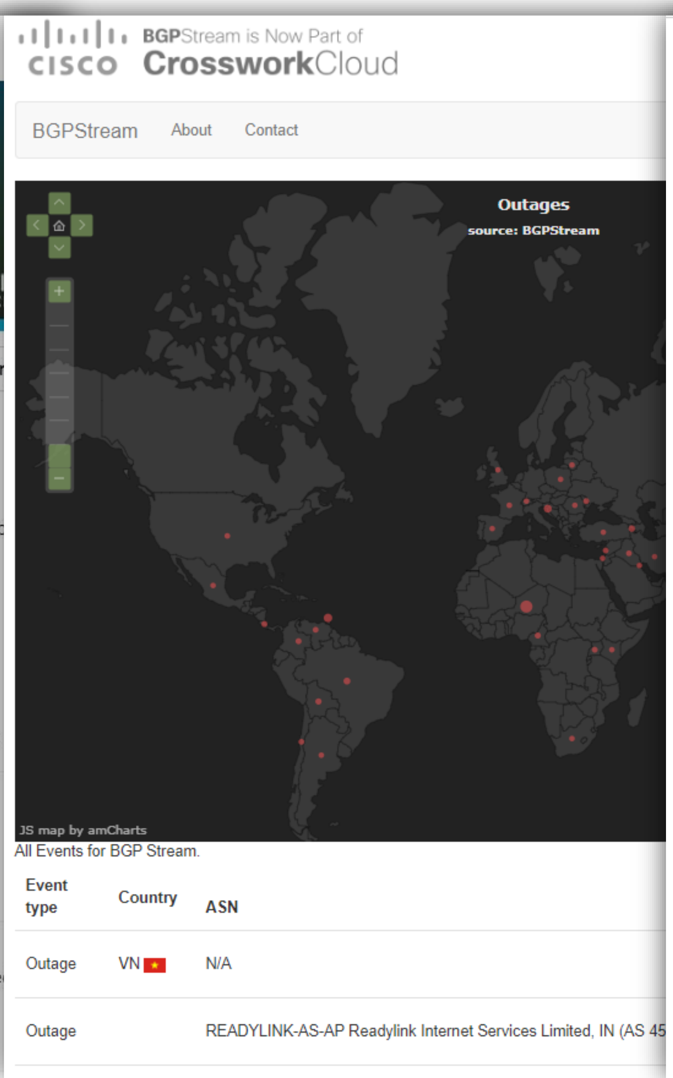
crosswork.cisco.com Joined June 2015

2 Following 16.1K Followers

Followed by BGPKIT, Anirban Datta, and 33 others you follow

Cisco BGPStream @bgpstream · 12m
BGP,OT,VN,Viet Nam,-,Outage affected 2609 prefixes, bgpstream.com/event/305048

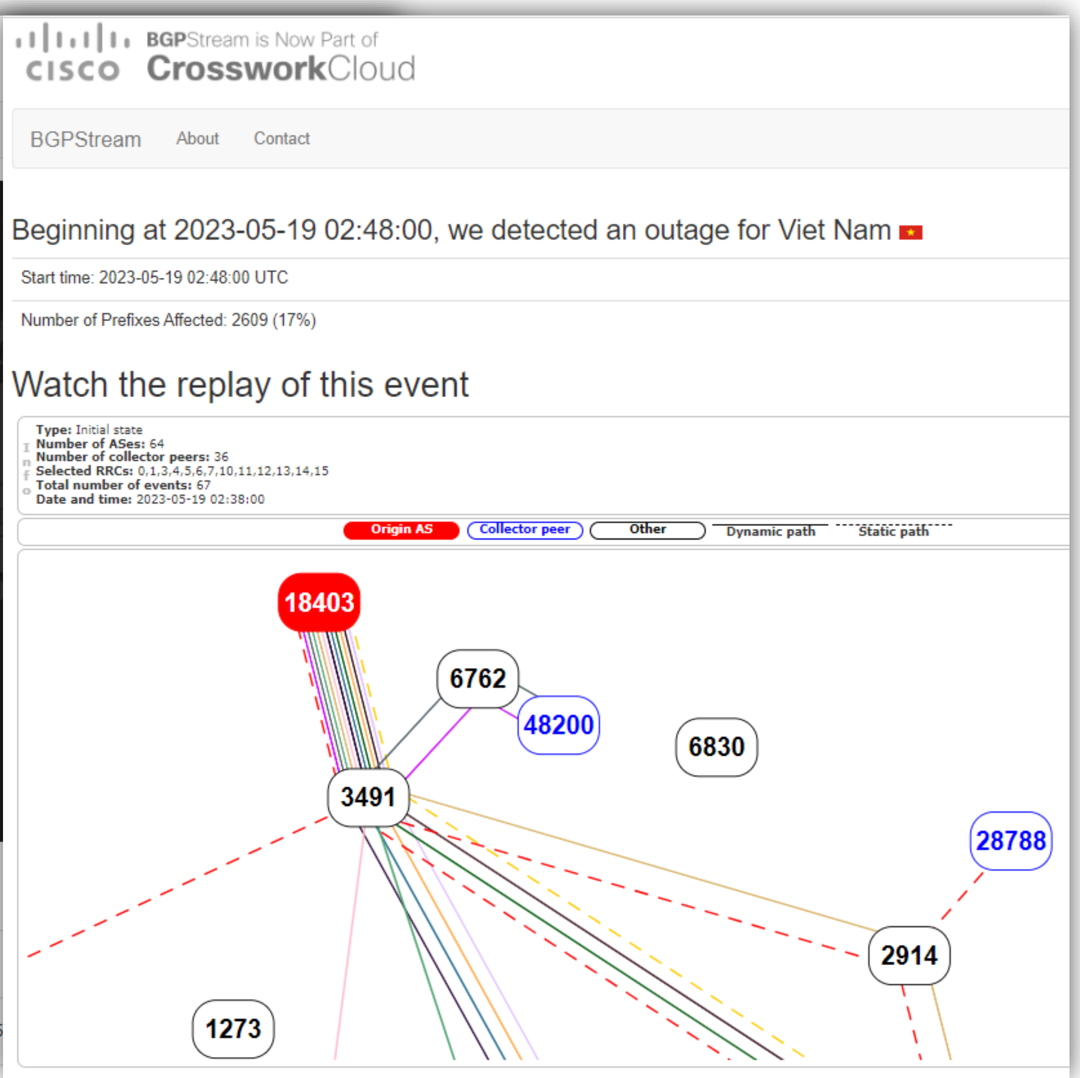
Cisco BGPStream @bgpstream · 4h
BGP,OT,45536,READYLINK-AS-AP Readylink Internet Services Limite IN,-,Outage affected 26 prefixes, bgpstream.com/event/305047



BGPStream is Now Part of CrossworkCloud

All Events for BGP Stream.

Event type	Country	ASN
Outage	VN	N/A
Outage		READYLINK-AS-AP Readylink Internet Services Limited, IN (AS 45



BGPStream is Now Part of CrossworkCloud

Beginning at 2023-05-19 02:48:00, we detected an outage for Viet Nam

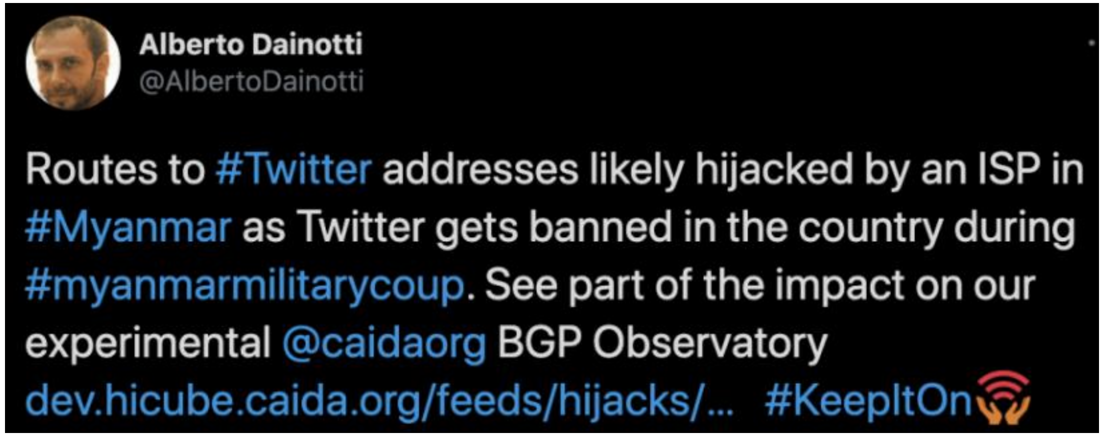
Start time: 2023-05-19 02:48:00 UTC

Number of Prefixes Affected: 2609 (17%)

Watch the replay of this event

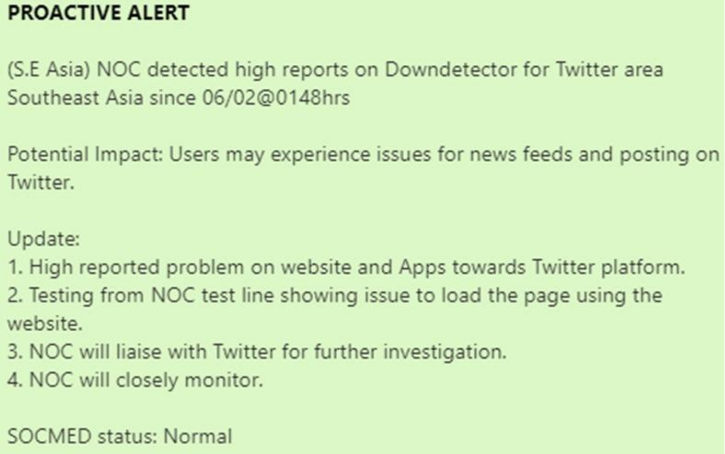
Type: Initial state
Number of ASes: 64
Number of collector peers: 36
Selected RRCs: 0,1,3,4,5,6,7,10,11,12,13,14,15
Total number of events: 67
Date and time: 2023-05-19 02:38:00

Route Hijack Incidents Worldwide



Alberto Dainotti
@AlbertoDainotti

Routes to #Twitter addresses likely hijacked by an ISP in #Myanmar as Twitter gets banned in the country during #myanmarmilitarycoup. See part of the impact on our experimental @caidaorg BGP Observatory dev.hicube.caida.org/feeds/hijacks/... #KeepItOn



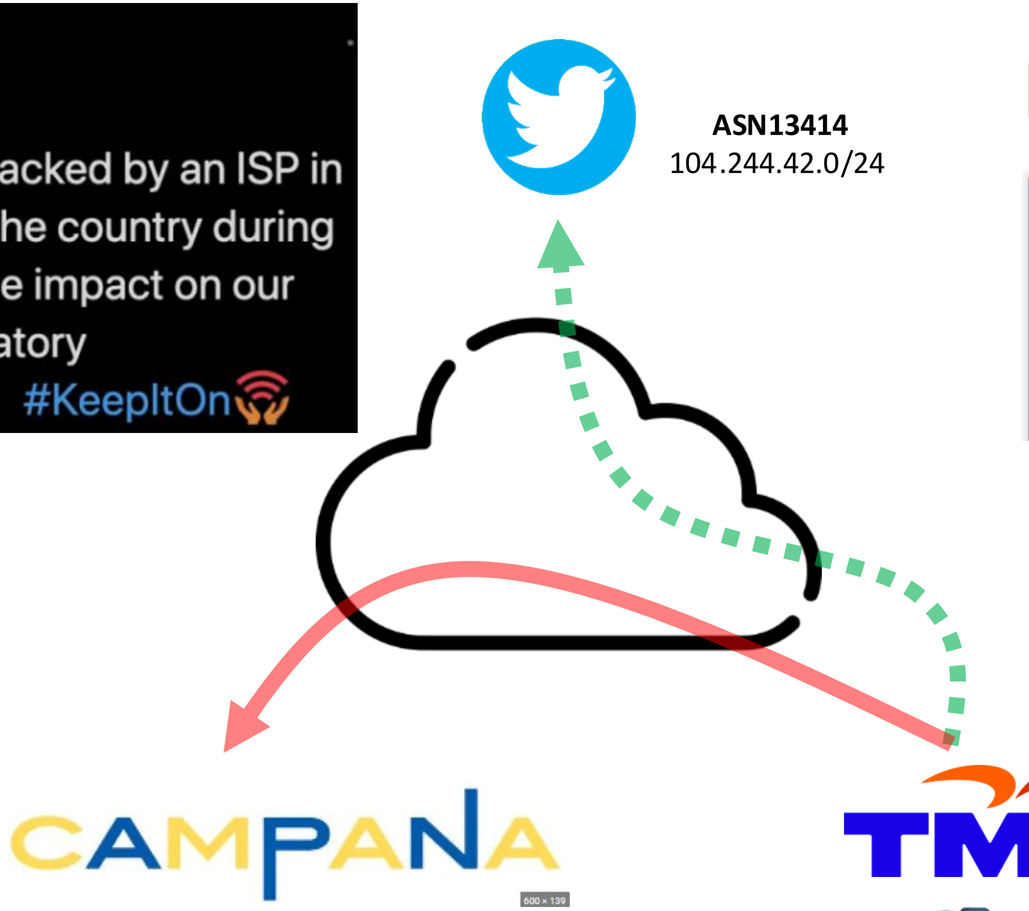
PROACTIVE ALERT

(S.E Asia) NOC detected high reports on Downdetector for Twitter area Southeast Asia since 06/02@0148hrs

Potential Impact: Users may experience issues for news feeds and posting on Twitter.

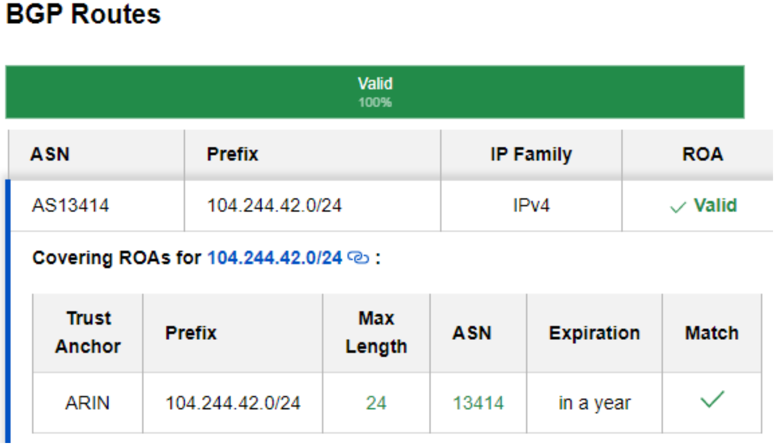
Update:
1. High reported problem on website and Apps towards Twitter platform.
2. Testing from NOC test line showing issue to load the page using the website.
3. NOC will liaise with Twitter for further investigation.
4. NOC will closely monitor.

SOCMED status: Normal



ASN13414
104.244.42.0/24

ASN8342
104.244.42.0/24



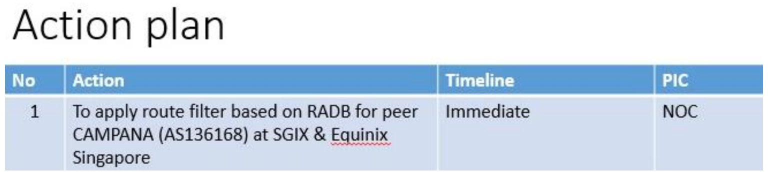
BGP Routes

Valid
100%

ASN	Prefix	IP Family	ROA
AS13414	104.244.42.0/24	IPv4	✓ Valid

Covering ROAs for 104.244.42.0/24 :

Trust Anchor	Prefix	Max Length	ASN	Expiration	Match
ARIN	104.244.42.0/24	24	13414	in a year	✓



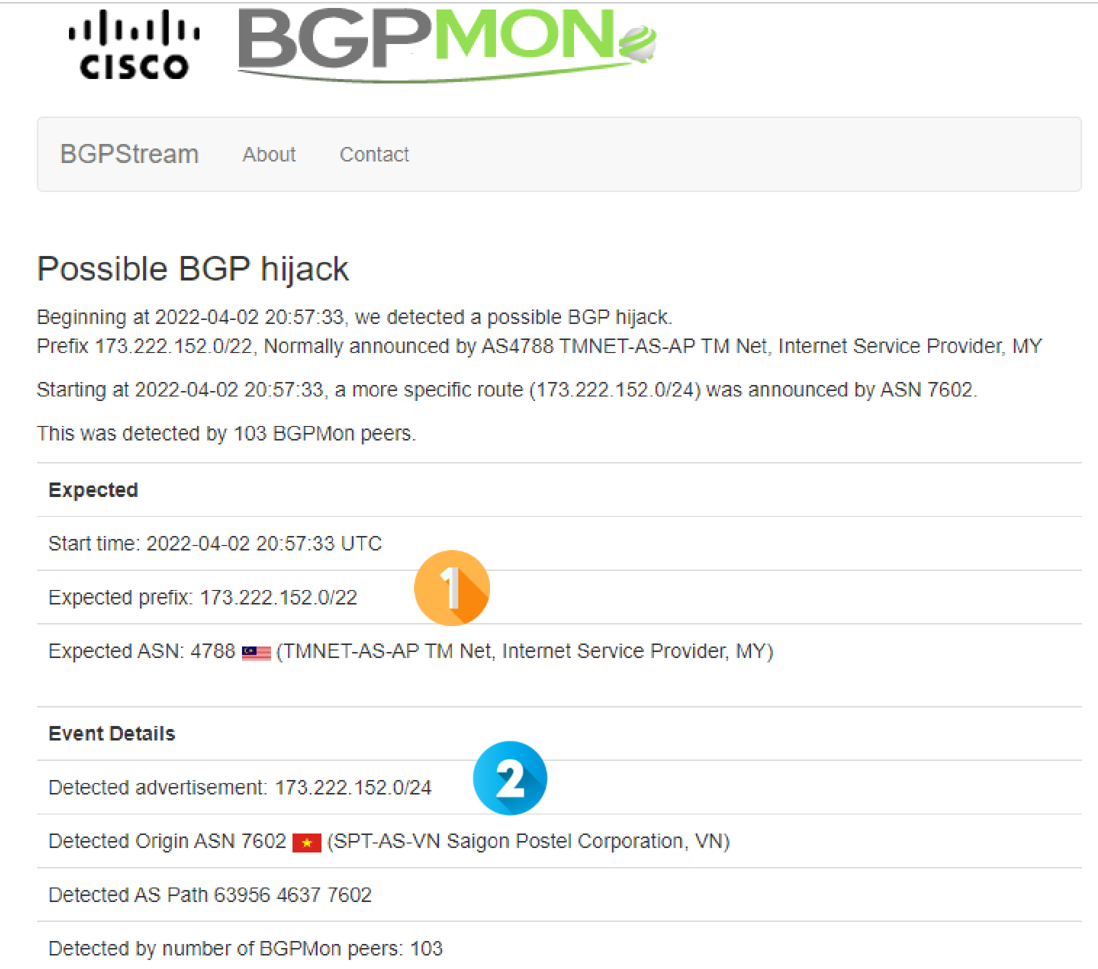
Action plan

No	Action	Timeline	PIC
1	To apply route filter based on RADB for peer CAMPANA (AS136168) at SGIX & Equinix Singapore	Immediate	NOC

Source: https://www.manrs.org/2021/02/did-someone-try-to-hijack-twitter-yes/

Route Hijack Impacted TM Users
5 Feb 2021

YOUR NEXT IS NOW TM



BGPStream About Contact

Possible BGP hijack

Beginning at 2022-04-02 20:57:33, we detected a possible BGP hijack.
Prefix 173.222.152.0/22, Normally announced by AS4788 TMNET-AS-AP TM Net, Internet Service Provider, MY

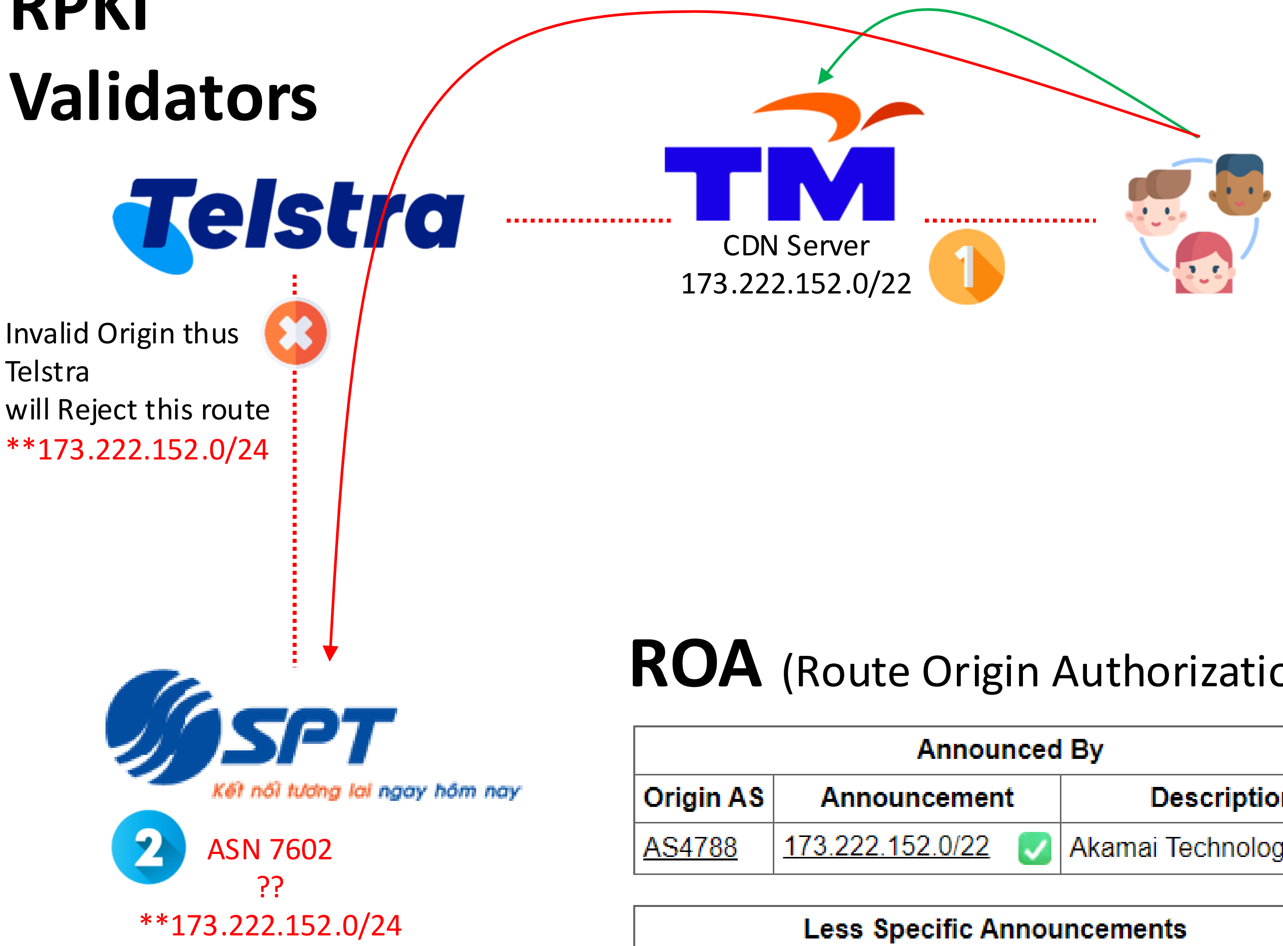
Starting at 2022-04-02 20:57:33, a more specific route (173.222.152.0/24) was announced by ASN 7602.

This was detected by 103 BGPMon peers.

Expected
Start time: 2022-04-02 20:57:33 UTC
Expected prefix: 173.222.152.0/22
Expected ASN: 4788 (TMNET-AS-AP TM Net, Internet Service Provider, MY)

Event Details
Detected advertisement: 173.222.152.0/24
Detected Origin ASN 7602 (SPT-AS-VN Saigon Postel Corporation, VN)
Detected AS Path 63956 4637 7602
Detected by number of BGPMon peers: 103

RPKI Validators



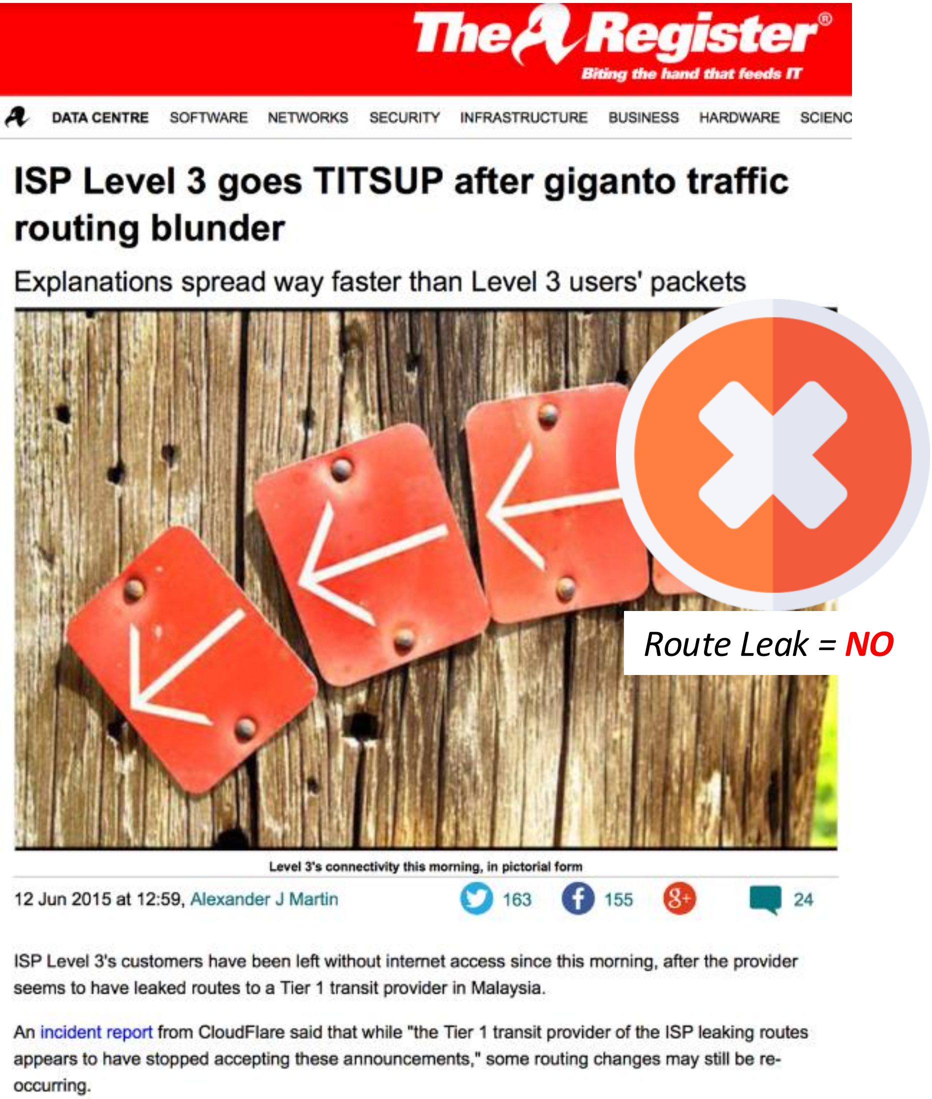
ROA (Route Origin Authorization)

Announced By		
Origin AS	Announcement	Description
AS4788	173.222.152.0/22 ✓	Akamai Technologies, Inc.

Less Specific Announcements		
Origin AS	Announcement	Description
AS20940	173.222.0.0/15 ✓	Akamai Technologies, Inc.

How RPKI Protect From Route Hijack 2 Apr 2022

YOUR
NEXT
IS NOW



ISP Level 3 goes TITSUP after giganto traffic routing blunder

Explanations spread way faster than Level 3 users' packets

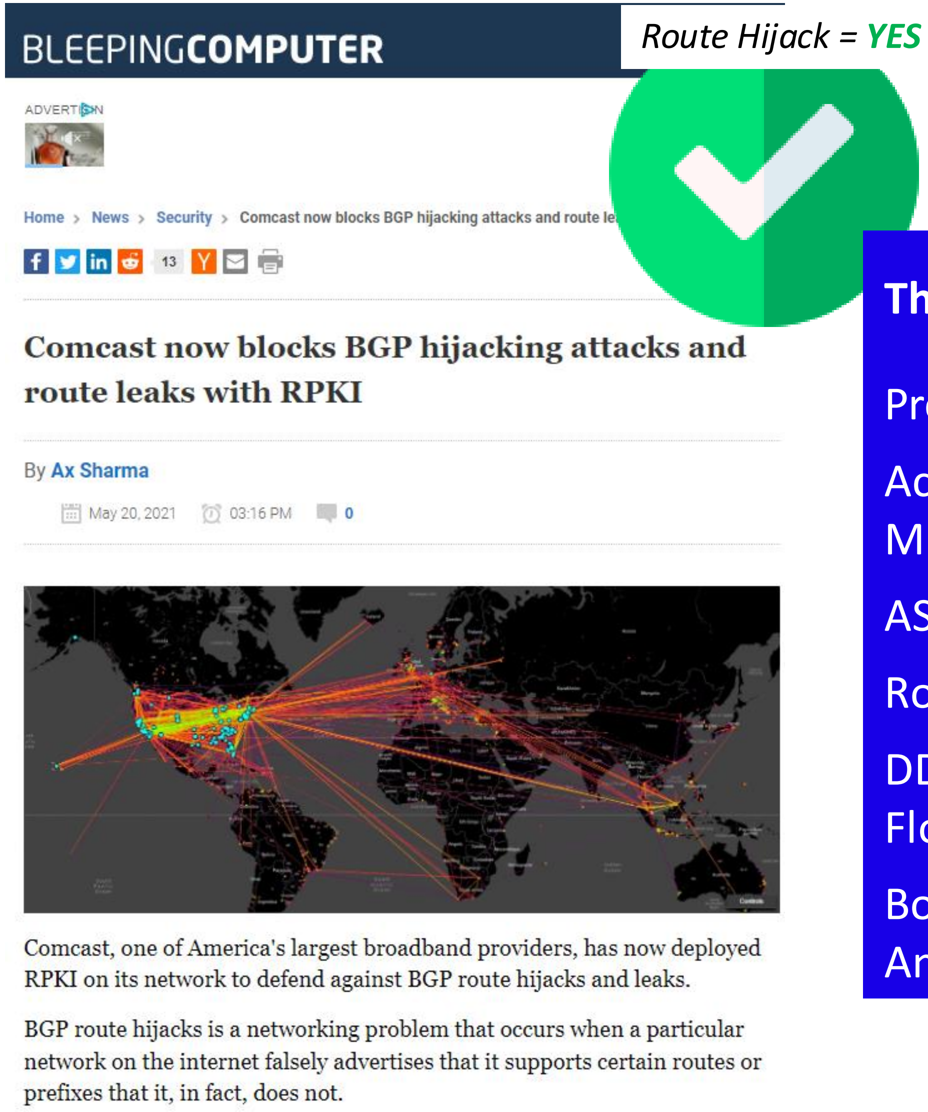
Level 3's connectivity this morning, in pictorial form

12 Jun 2015 at 12:59, Alexander J Martin

ISP Level 3's customers have been left without internet access since this morning, after the provider seems to have leaked routes to a Tier 1 transit provider in Malaysia.

An incident report from CloudFlare said that while "the Tier 1 transit provider of the ISP leaking routes appears to have stopped accepting these announcements," some routing changes may still be re-occurring.

Route Leak = ***NO***



BLEEPINGCOMPUTER
ADVERTISEMENT
Home › News › Security › Comcast now blocks BGP hijacking attacks and route le
13

Route Hijack = ***YES***

Comcast now blocks BGP hijacking attacks and route leaks with RPKI

By Ax Sharma

May 20, 2021 03:16 PM 0

Comcast, one of America's largest broadband providers, has now deployed RPKI on its network to defend against BGP route hijacks and leaks.

BGP route hijacks is a networking problem that occurs when a particular network on the internet falsely advertises that it supports certain routes or prefixes that it, in fact, does not.

Threat Type	RPKI Protection
Prefix Hijacking	✓ Yes
Accidental Route Misconfigurations	✓ Yes
AS Path Hijacking	✗ No
Route Leaks	✗ No
DDoS / Traffic Flooding	✗ No
Bogon IP Announcements	✗ No

What RPKI Able vs Unable to Protect

Why TM pursue to update ROA and deploy RPKI Validator

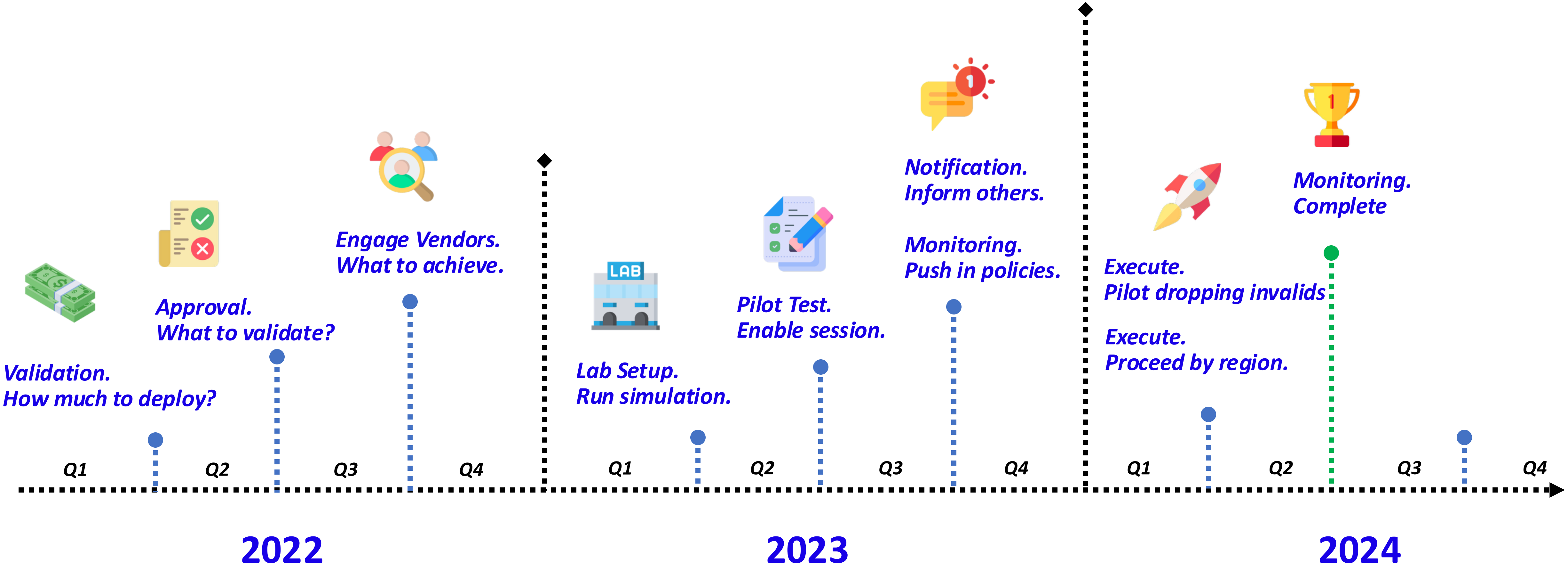
To build more secure/safe and reliable network in protecting our customer

To prevent BGP route hijacking from attacker or fat finger (misconfiguration)

Join the industries in the global initiative to reduce the route hijack incidents

YOUR
NEXT
IS NOW

Timeline Deployment



Validation.
How much to deploy?

Approval.
What to validate?

Engage Vendors.
What to achieve.

Lab Setup.
Run simulation.

Pilot Test.
Enable session.

Notification.
Inform others.

Monitoring.
Push in policies.

Execute.
Pilot dropping invalids

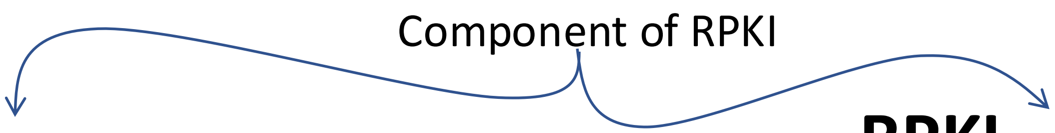
Execute.
Proceed by region.

Monitoring.
Complete

YOUR
NEXT
IS NOW

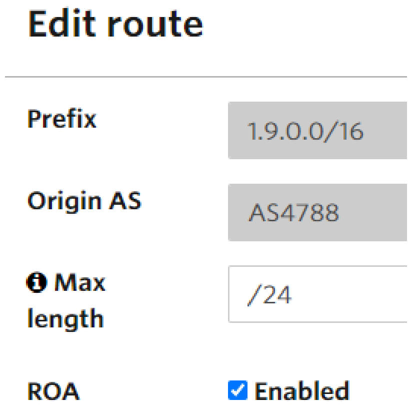
TM

RPKI (Resource Public Key infrastructure) also known as **Resource Certification** is a **Framework** to improved the routing security in the **Internet** introduced by the **Internet Society**



Component of RPKI

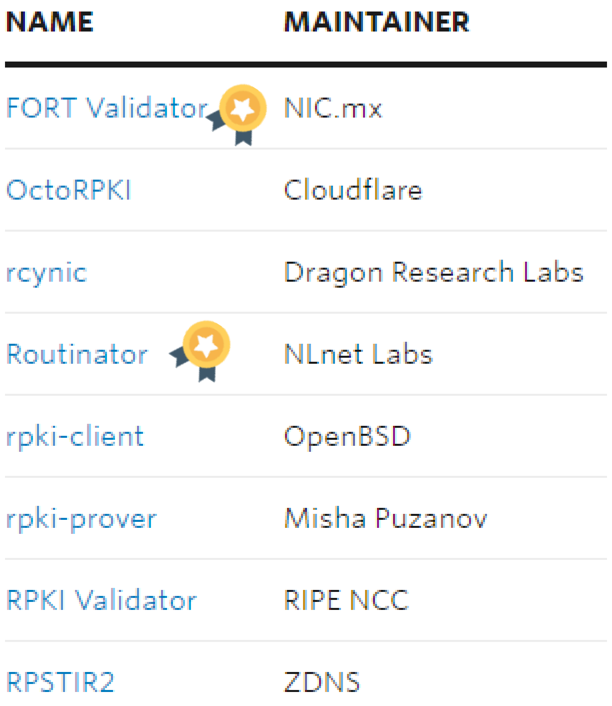
ROA (Route Origin Authorization)



Edit route

Prefix	1.9.0.0/16
Origin AS	AS4788
Max length	/24
ROA	☑ Enabled

RPKI Validators



NAME	MAINTAINER
FORT Validator	NIC.mx
OctoRPKI	Cloudflare
rcynic	Dragon Research Labs
Routinator	NLnet Labs
rpki-client	OpenBSD
rpki-prover	Misha Puzanov
RPKI Validator	RIPE NCC
RPSTIR2	ZDNS

What is RPKI?

What is RPKI?

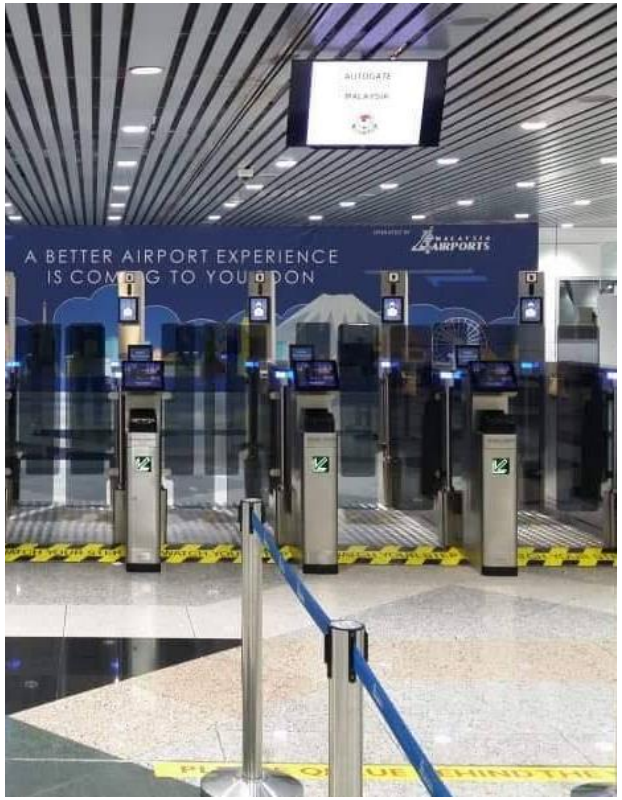
RPKI (Resource Public Key infrastructure) also known as **Resource Certification** is a **Framework** to improved the routing security in the **Internet** introduced by the **Internet Society**

Component of RPKI

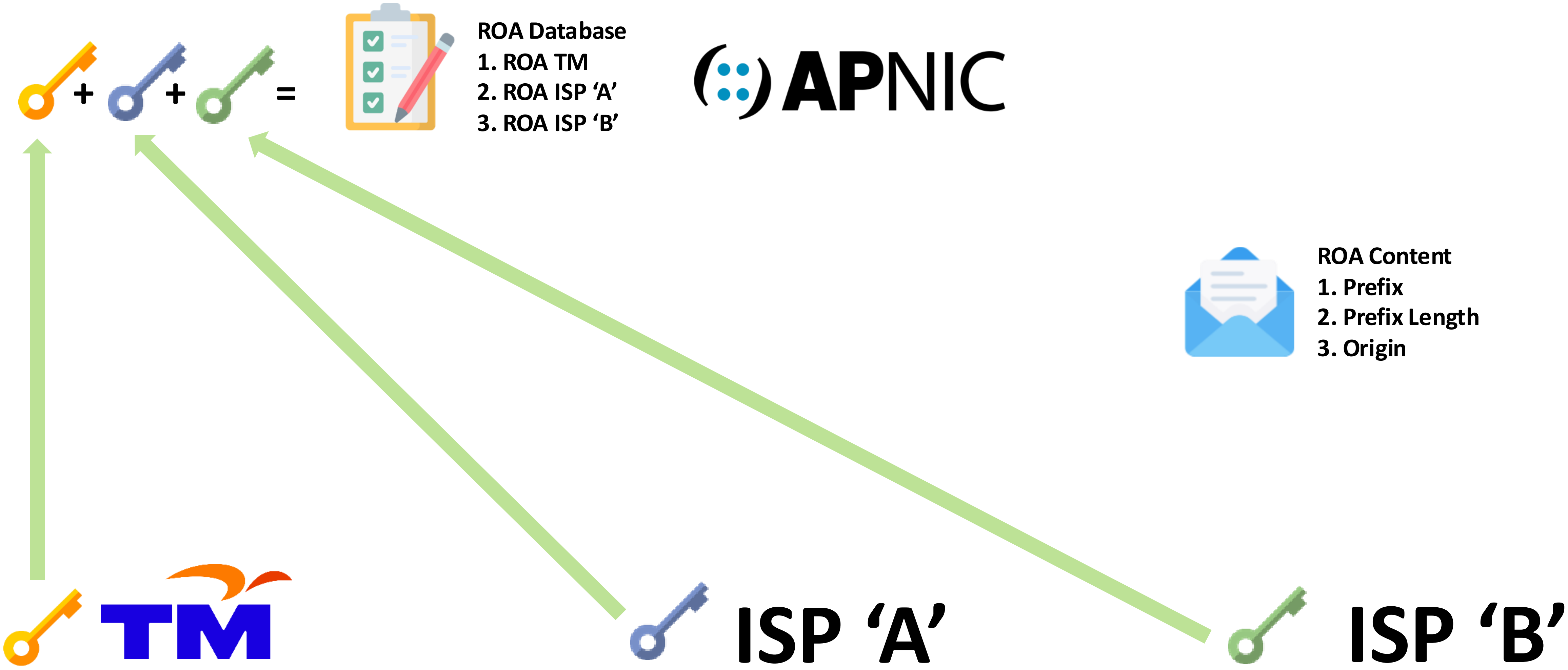
ROA (Route Origin Authorization)

Source: https://media.thevibes.com/images/uploads/covers/_large/passport-travel-BERNAMA.jpg

RPKI Validators



Source: https://www.facebook.com/imigresen/photos/

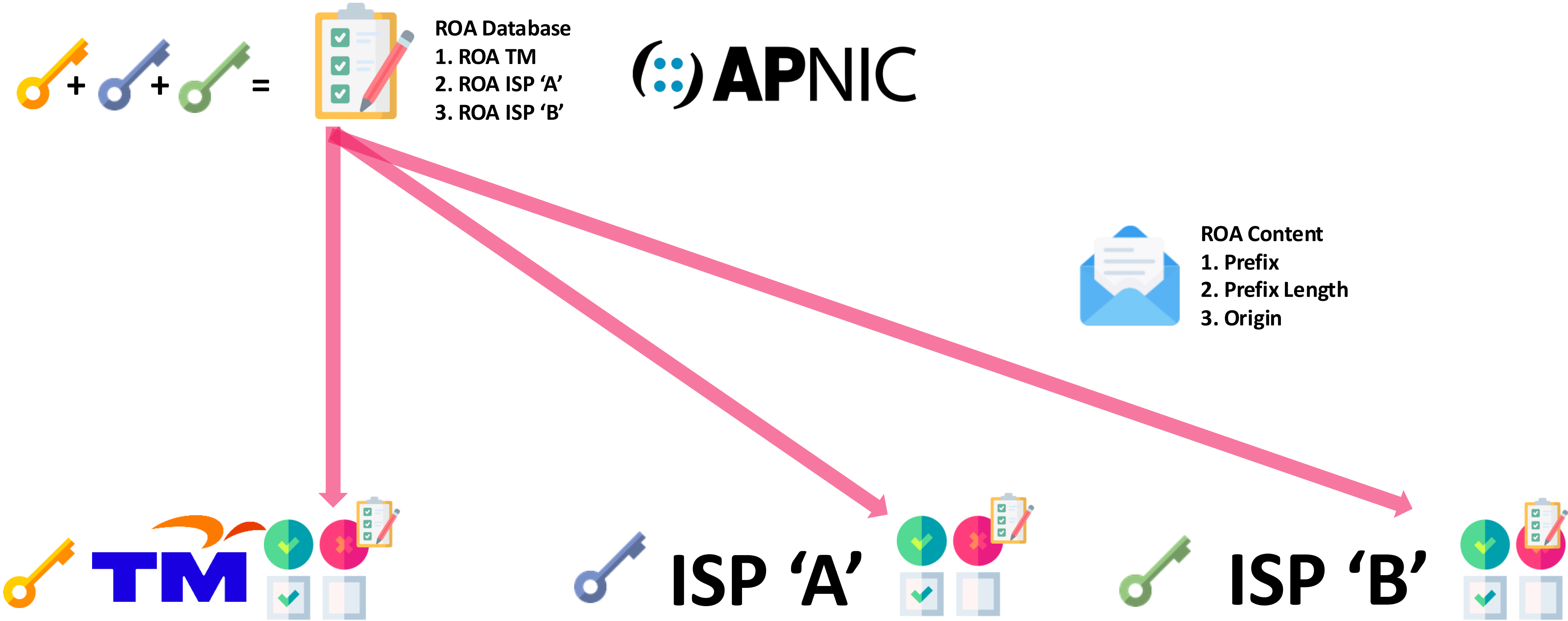


ROA Database
1. ROA TM
2. ROA ISP ‘A’
3. ROA ISP ‘B’

ROA Content
1. Prefix
2. Prefix Length
3. Origin

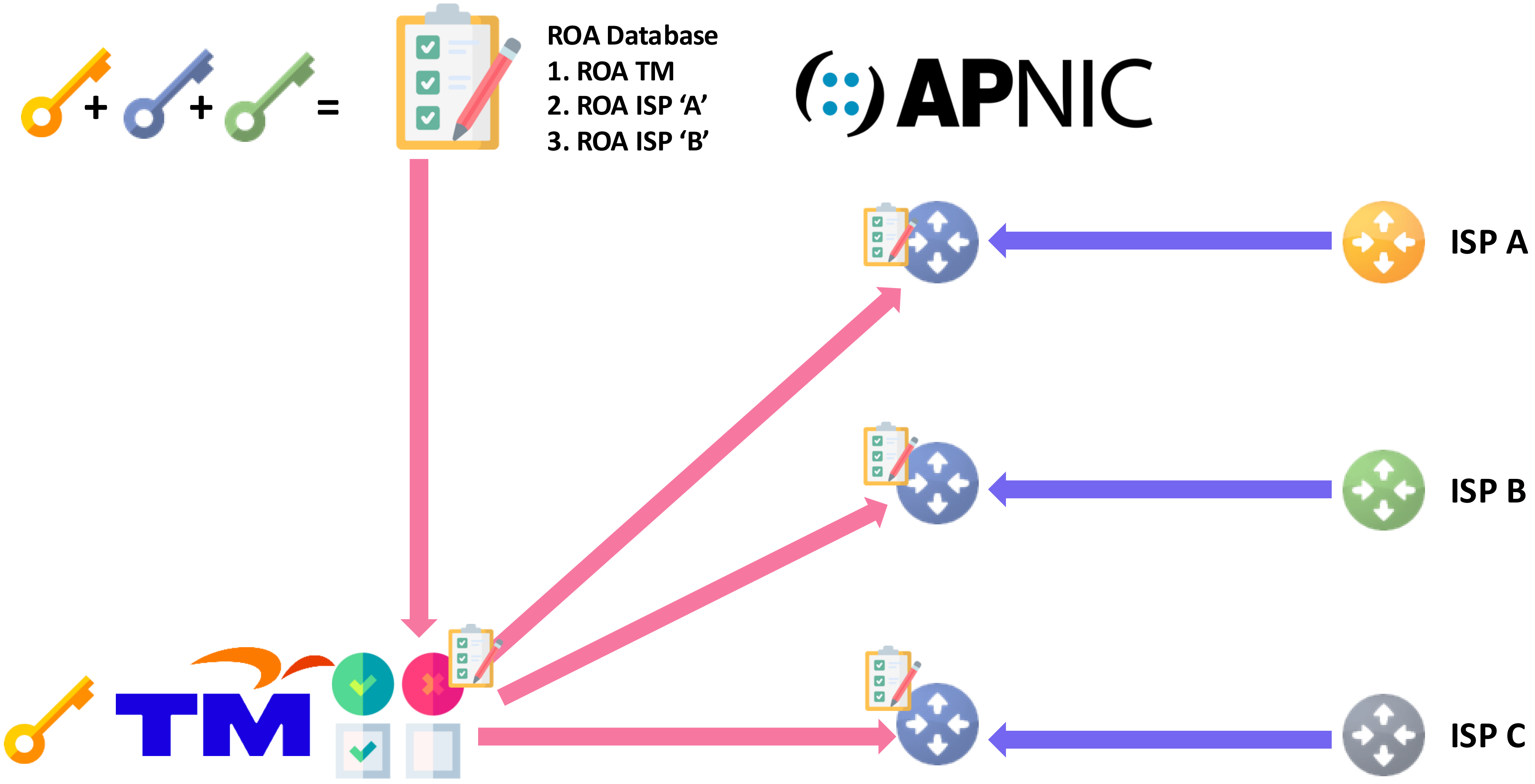
RPKI Logical Flow - Register ROA

RPKI Logical Flow - Validator



ROA Database
1. ROA TM
2. ROA ISP ‘A’
3. ROA ISP ‘B’

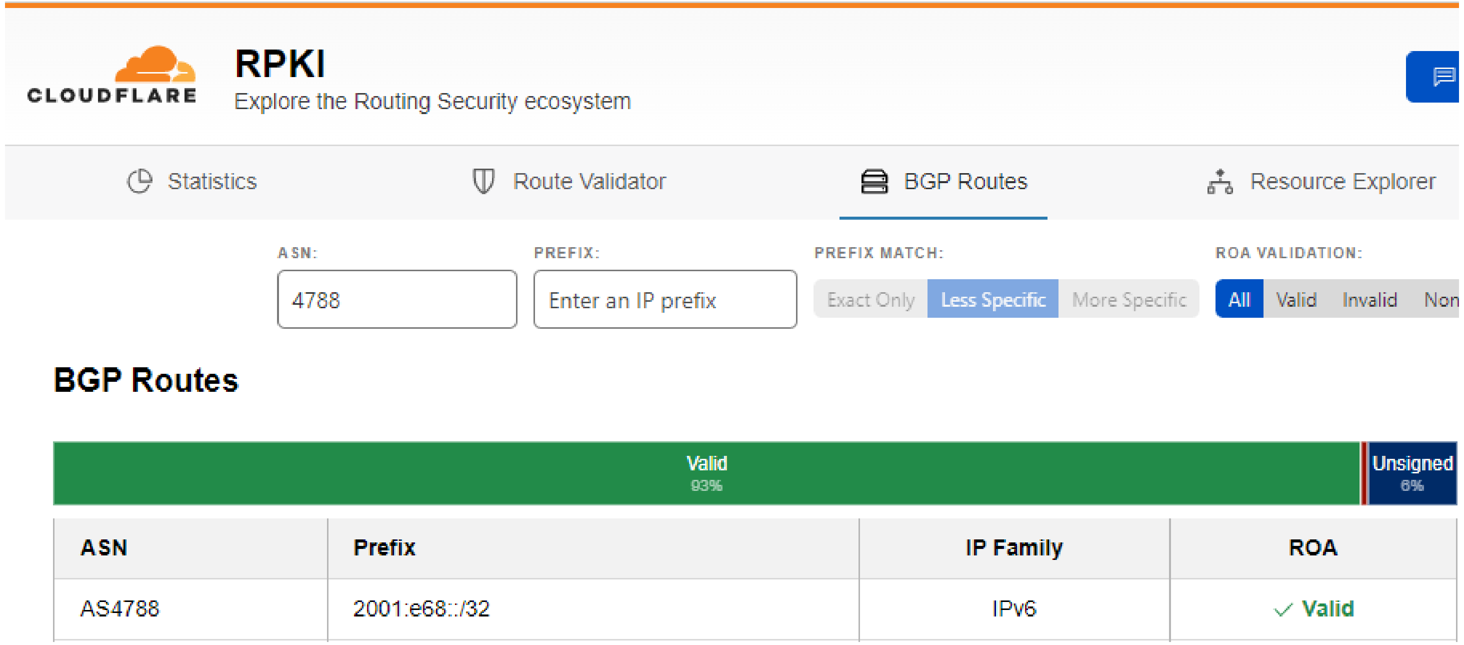
ROA Content
1. Prefix
2. Prefix Length
3. Origin



ROA Database
1. ROA TM
2. ROA ISP ‘A’
3. ROA ISP ‘B’

RPKI Logical Flow - Router/PE

YOUR NEXT IS NOW TM



CLOUDFLARE

RPKI

Explore the Routing Security ecosystem

Statistics | Route Validator | BGP Routes | Resource Explorer

ASN: 4788

PREFIX: Enter an IP prefix

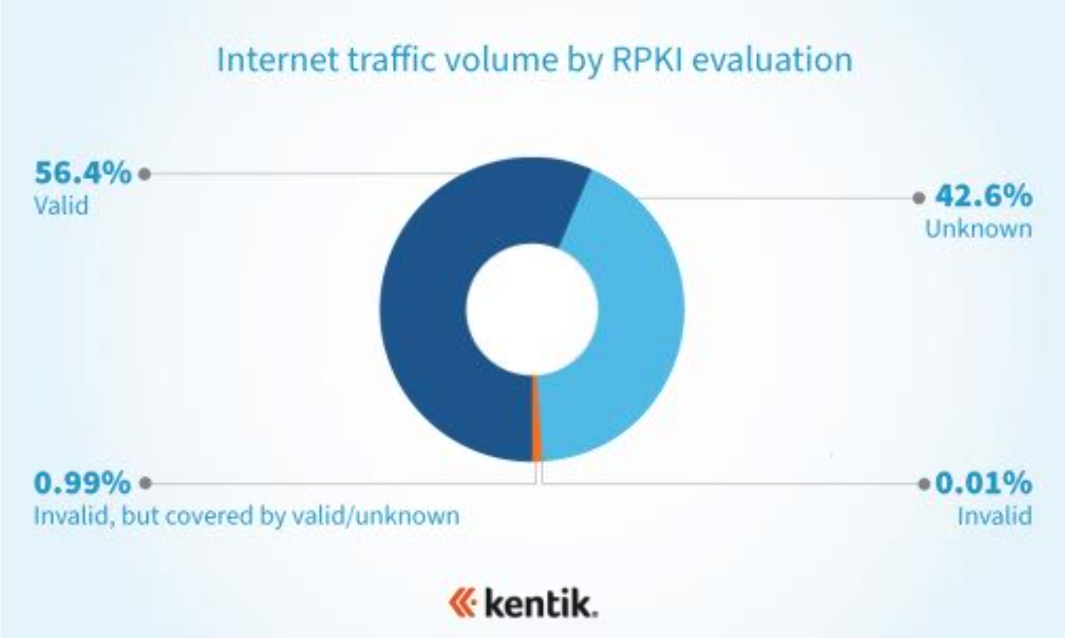
PREFIX MATCH: Exact Only | Less Specific | More Specific

ROA VALIDATION: All | Valid | Invalid | Non

BGP Routes

Valid 93% | Unsigned 6%

ASN	Prefix	IP Family	ROA
AS4788	2001:e68::/32	IPv6	✓ Valid



TM 99%

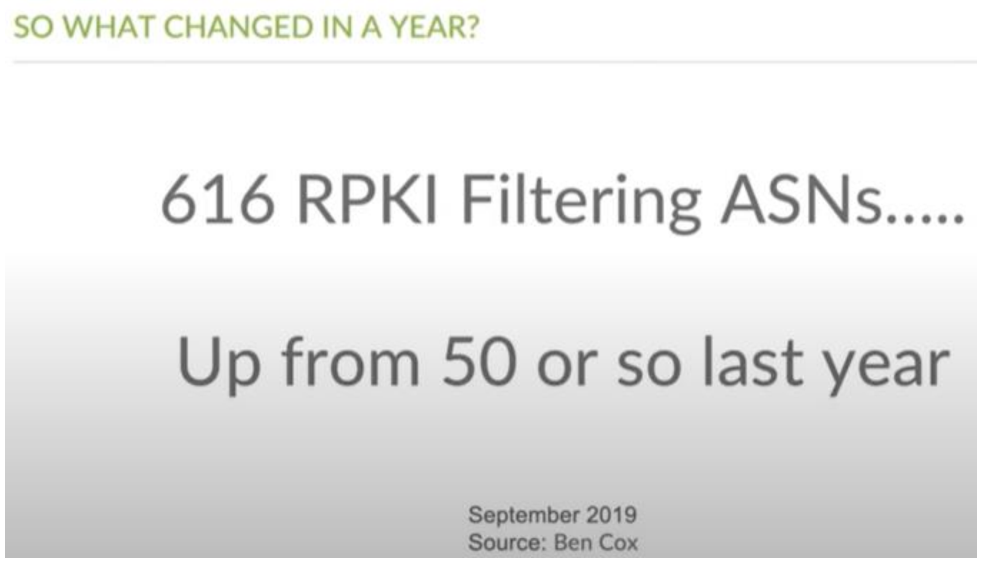
Global ROA Takeup

Source: https://www.kentik.com/blog/author/job-snijders/

ROA Route Origin Authorization

YOUR NEXT IS NOW TM

Current Global RPKI “Take-up”

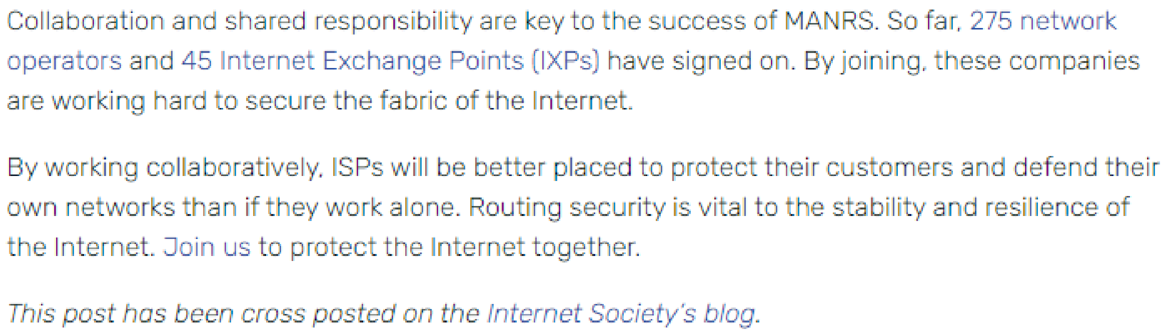


SO WHAT CHANGED IN A YEAR?

616 RPKI Filtering ASNs…..

Up from 50 or so last year

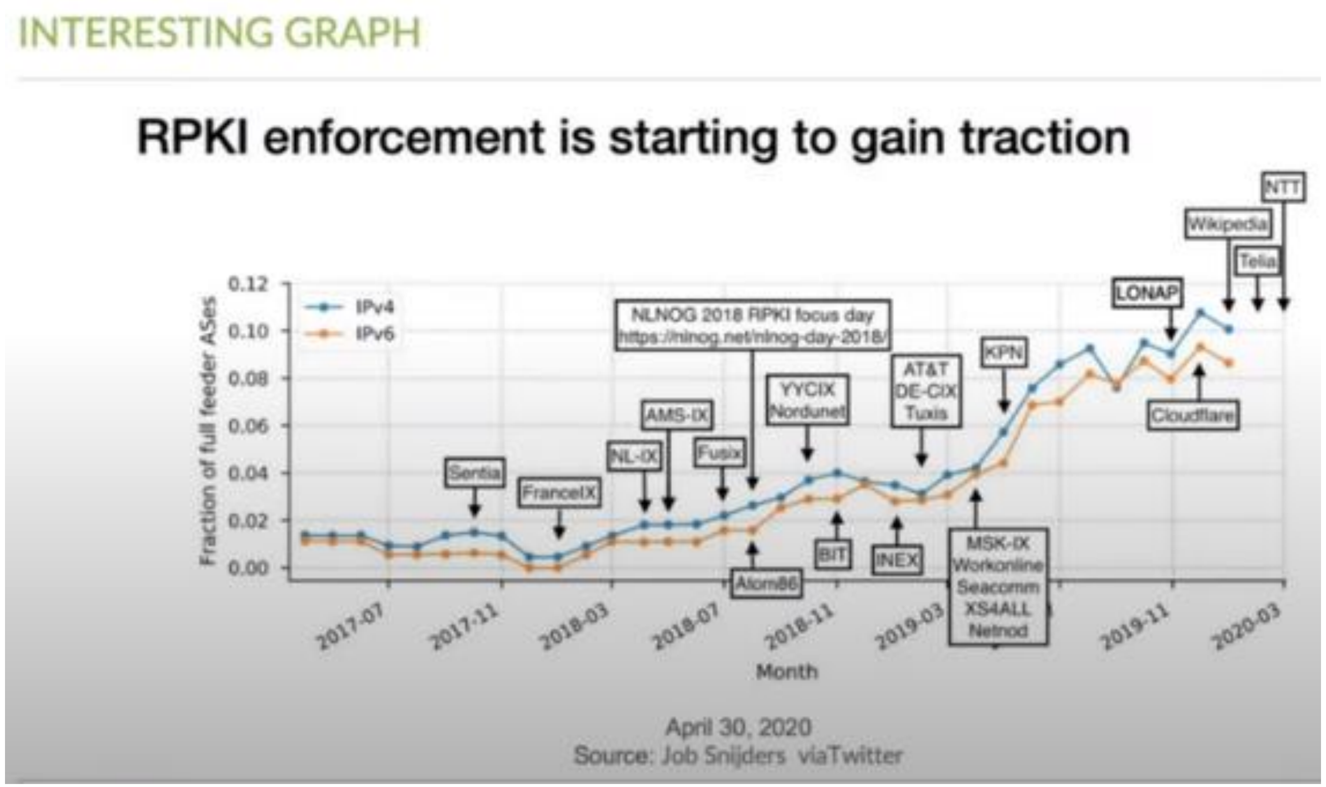
September 2019
Source: Ben Cox



Collaboration and shared responsibility are key to the success of MANRS. So far, 275 network operators and 45 Internet Exchange Points (IXPs) have signed on. By joining, these companies are working hard to secure the fabric of the Internet.

By working collaboratively, ISPs will be better placed to protect their customers and defend their own networks than if they work alone. Routing security is vital to the stability and resilience of the Internet. Join us to protect the Internet together.

This post has been cross posted on the Internet Society’s blog.



INTERESTING GRAPH

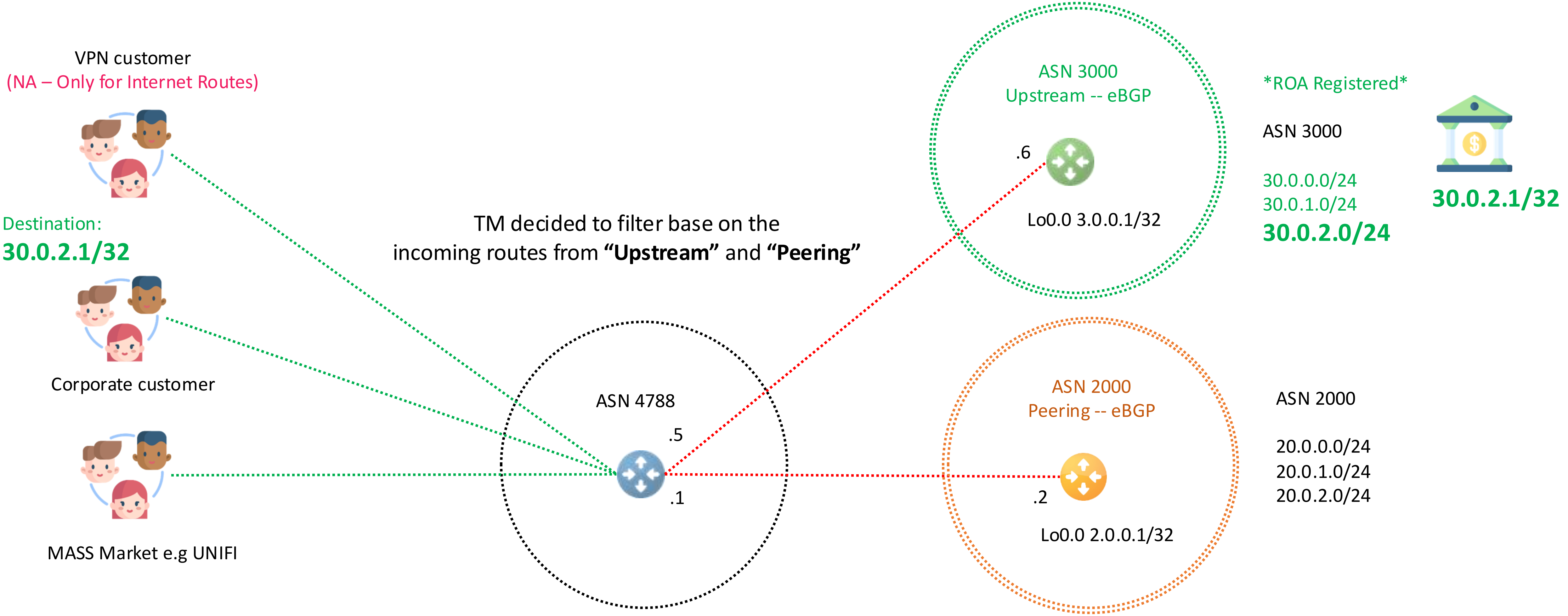
RPKI enforcement is starting to gain traction

April 30, 2020
Source: Job Snijders viaTwitter

Source: https://www.manrs.org/2020/01/isps-should-strongly-consider-manrs-to-fight-cybercrime-wef-report/

Source: https://www.manrs.org/netops/participants/

How the "Protection Mechanism" help to drop "Invalid" routes



VPN customer

(NA – Only for Internet Routes)

Destination:

30.0.2.1/32

Corporate customer

MASS Market e.g UNIFI

TM decided to filter base on the incoming routes from **"Upstream"** and **"Peering"**

ASN 4788

.5

.1

ASN 3000

Upstream -- eBGP

.6

Lo0.0 3.0.0.1/32

ASN 2000

Peering -- eBGP

.2

Lo0.0 2.0.0.1/32

ROA Registered

ASN 3000

30.0.0.0/24

30.0.1.0/24

30.0.2.0/24

30.0.2.1/32

ASN 2000

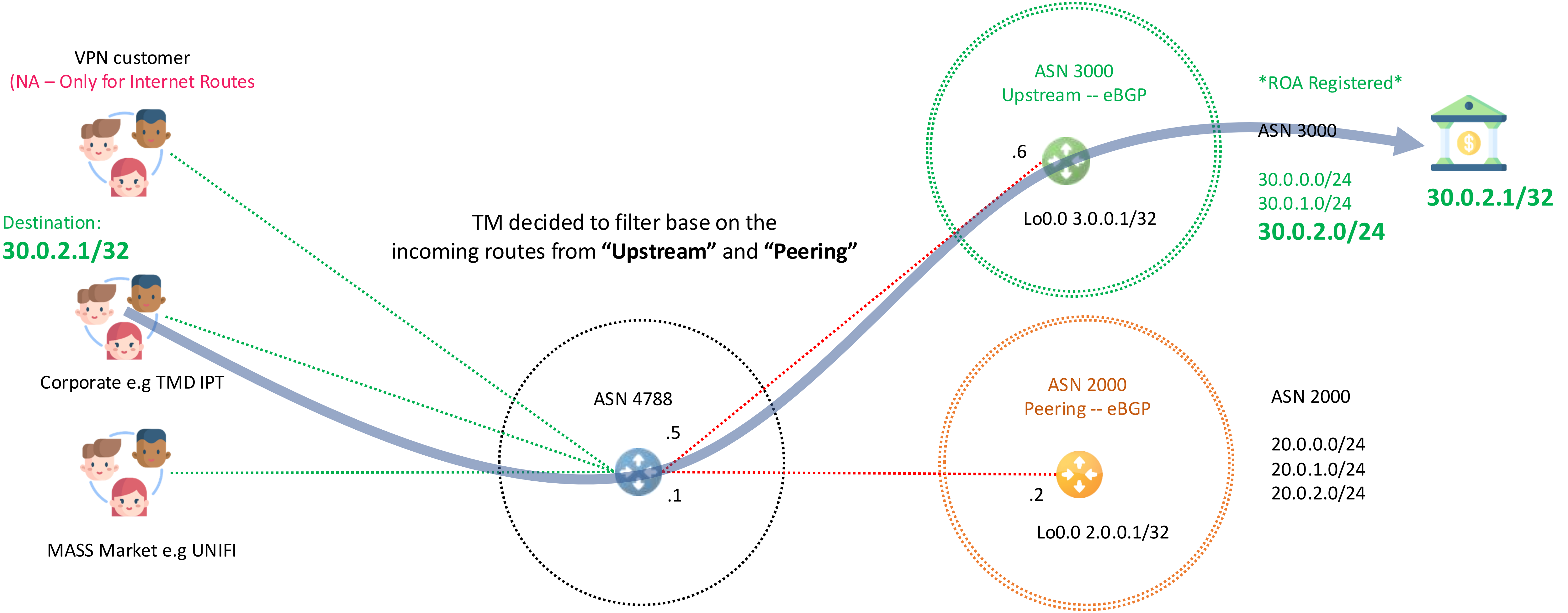
20.0.0.0/24

20.0.1.0/24

20.0.2.0/24

YOUR NEXT IS NOW

TM



VPN customer
(NA – Only for Internet Routes

Destination:
30.0.2.1/32

Corporate e.g TMD IPT

MASS Market e.g UNIFI

TM decided to filter base on the incoming routes from **“Upstream”** and **“Peering”**

ASN 4788
.5
.1

ASN 3000
Upstream -- eBGP
.6
Lo0.0 3.0.0.1/32

ASN 2000
Peering -- eBGP
.2
Lo0.0 2.0.0.1/32

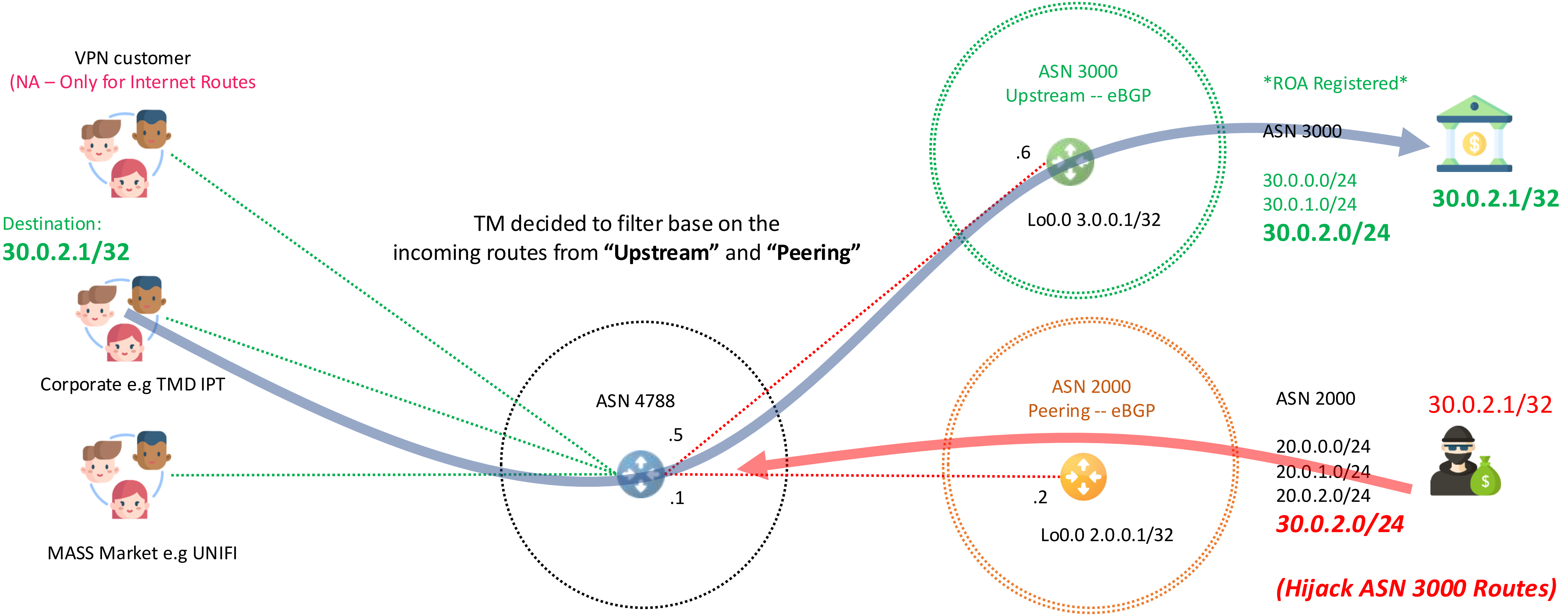
ROA Registered
ASN 3000
30.0.0.0/24
30.0.1.0/24
30.0.2.0/24

30.0.2.1/32

ASN 2000
20.0.0.0/24
20.0.1.0/24
20.0.2.0/24

How the “Protection Mechanism” help to drop “Invalid” routes

YOUR NEXT IS NOW TM



VPN customer

(NA – Only for Internet Routes

Destination:

30.0.2.1/32

Corporate e.g TMD IPT

MASS Market e.g UNIFI

TM decided to filter base on the
incoming routes from **“Upstream”** and **“Peering”**

ASN 4788

.5

.1

ASN 3000
Upstream -- eBGP

.6

Lo0.0 3.0.0.1/32

ROA Registered

ASN 3000

30.0.0.0/24
30.0.1.0/24
30.0.2.0/24

30.0.2.1/32

ASN 2000
Peering -- eBGP

.2

Lo0.0 2.0.0.1/32

ASN 2000

30.0.2.1/32

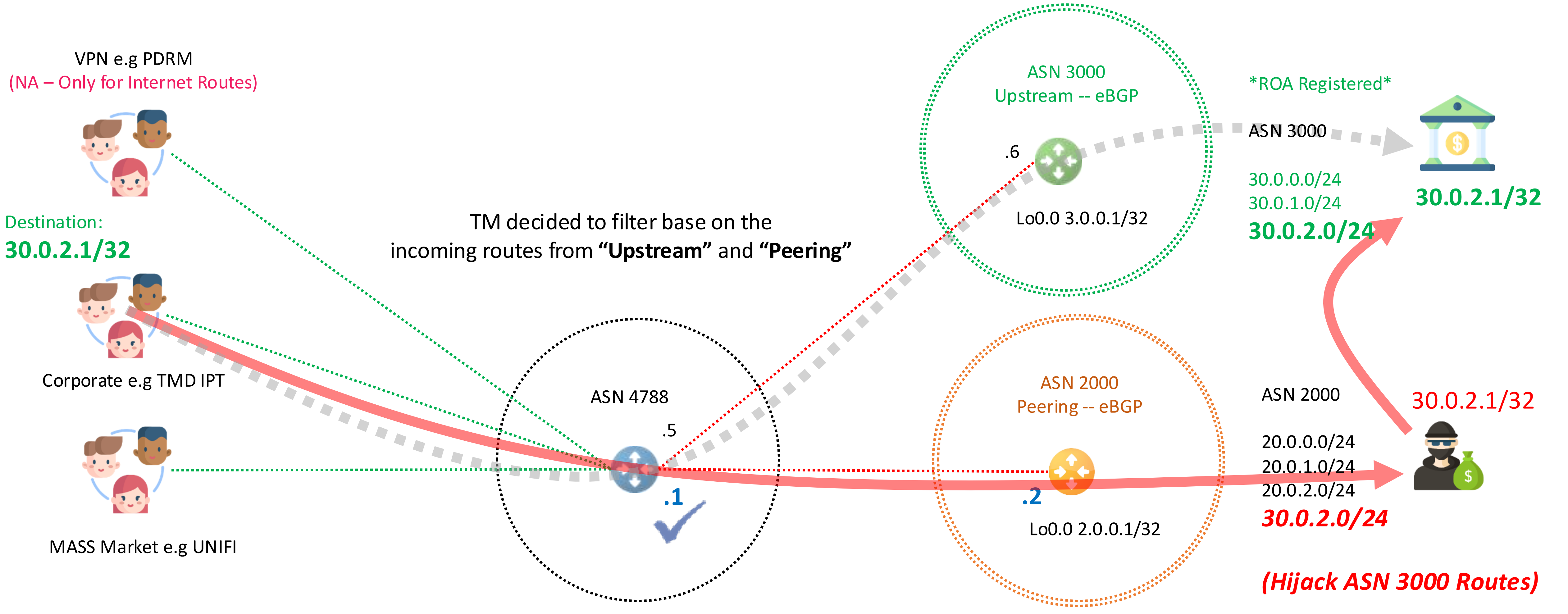
20.0.0.0/24
20.0.1.0/24
20.0.2.0/24
30.0.2.0/24

(Hijack ASN 3000 Routes)

How the “Protection Mechanism” help to drop “Invalid” routes

YOUR
NEXT
IS NOW

TM



VPN e.g PDRM

(NA – Only for Internet Routes)

Destination:

30.0.2.1/32

Corporate e.g TMD IPT

MASS Market e.g UNIFI

TM decided to filter base on the incoming routes from **“Upstream”** and **“Peering”**

ASN 4788

.5

.1

ASN 3000

Upstream -- eBGP

.6

Lo0.0 3.0.0.1/32

ROA Registered

ASN 3000

30.0.0.0/24

30.0.1.0/24

30.0.2.0/24

30.0.2.1/32

ASN 2000

Peering -- eBGP

.2

Lo0.0 2.0.0.1/32

ASN 2000

20.0.0.0/24

20.0.1.0/24

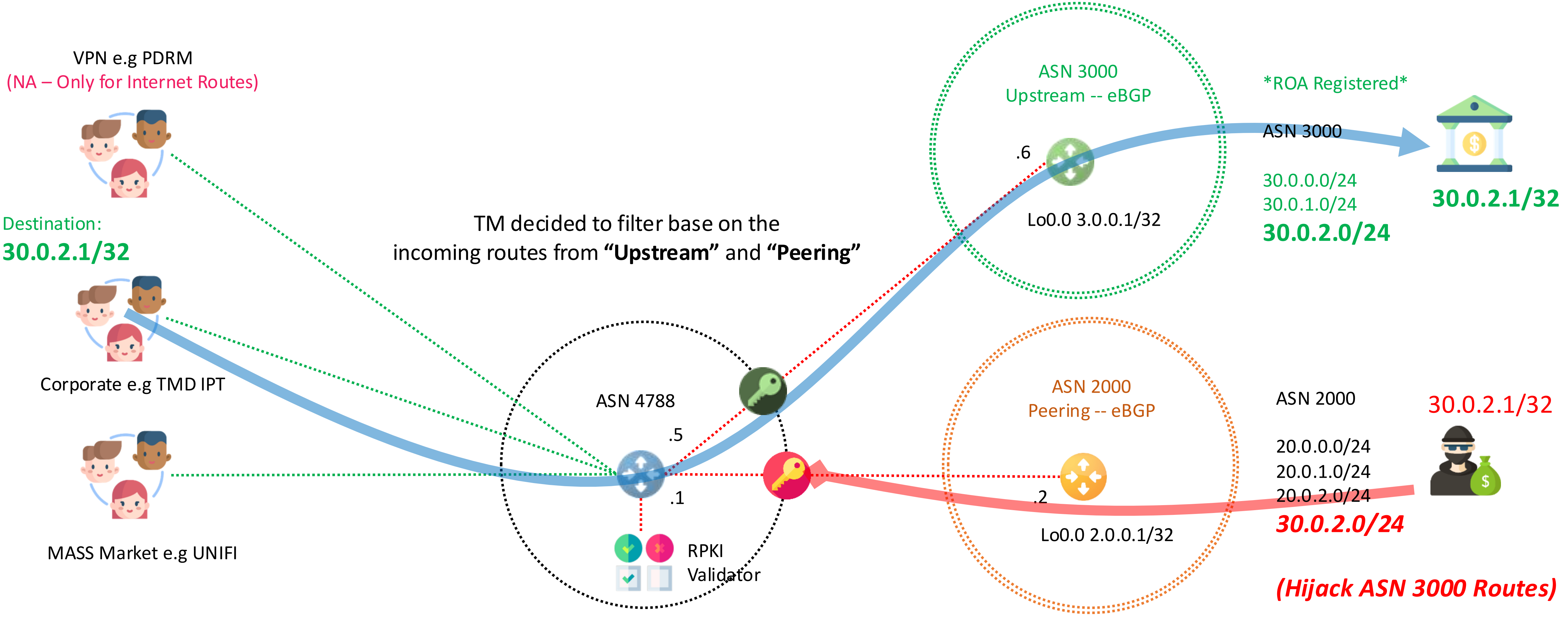
20.0.2.0/24

30.0.2.0/24

30.0.2.1/32

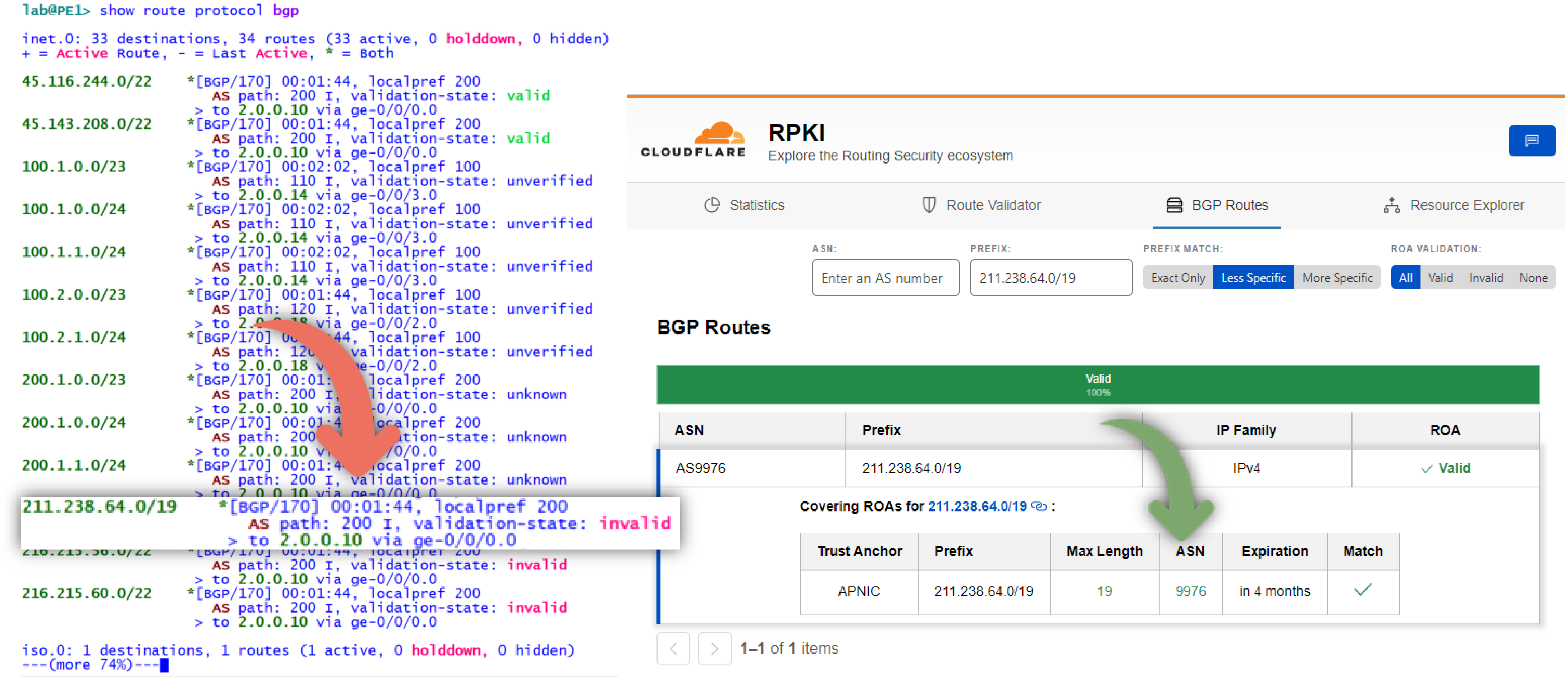
(Hijack ASN 3000 Routes)

How the “Protection Mechanism” help to drop “Invalid” routes



How the "Protection Mechanism" help to drop "Invalid" routes

YOUR NEXT IS NOW TM



```
lab@PE1> show route protocol bgp

inet.0: 33 destinations, 34 routes (33 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

45.116.244.0/22    *[BGP/170] 00:01:44, localpref 200
                      AS path: 200 I, validation-state: valid
                    > to 2.0.0.10 via ge-0/0/0.0
45.143.208.0/22    *[BGP/170] 00:01:44, localpref 200
                      AS path: 200 I, validation-state: valid
                    > to 2.0.0.10 via ge-0/0/0.0
100.1.0.0/23       *[BGP/170] 00:02:02, localpref 100
                      AS path: 110 I, validation-state: unverified
                    > to 2.0.0.14 via ge-0/0/3.0
100.1.0.0/24       *[BGP/170] 00:02:02, localpref 100
                      AS path: 110 I, validation-state: unverified
                    > to 2.0.0.14 via ge-0/0/3.0
100.1.1.0/24       *[BGP/170] 00:02:02, localpref 100
                      AS path: 110 I, validation-state: unverified
                    > to 2.0.0.14 via ge-0/0/3.0
100.2.0.0/23       *[BGP/170] 00:01:44, localpref 100
                      AS path: 120 I, validation-state: unverified
                    > to 2.0.0.18 via ge-0/0/2.0
100.2.1.0/24       *[BGP/170] 00:01:44, localpref 100
                      AS path: 120 I, validation-state: unverified
                    > to 2.0.0.18 via ge-0/0/2.0
200.1.0.0/23       *[BGP/170] 00:01:44, localpref 200
                      AS path: 200 I, validation-state: unknown
                    > to 2.0.0.10 via ge-0/0/0.0
200.1.0.0/24       *[BGP/170] 00:01:44, localpref 200
                      AS path: 200 I, validation-state: unknown
                    > to 2.0.0.10 via ge-0/0/0.0
200.1.1.0/24       *[BGP/170] 00:01:44, localpref 200
                      AS path: 200 I, validation-state: unknown
                    > to 2.0.0.10 via ge-0/0/0.0
211.238.64.0/19    *[BGP/170] 00:01:44, localpref 200
                      AS path: 200 I, validation-state: invalid
                    > to 2.0.0.10 via ge-0/0/0.0
216.215.56.0/22    *[BGP/170] 00:01:44, localpref 200
                      AS path: 200 I, validation-state: invalid
                    > to 2.0.0.10 via ge-0/0/0.0
216.215.60.0/22    *[BGP/170] 00:01:44, localpref 200
                      AS path: 200 I, validation-state: invalid
                    > to 2.0.0.10 via ge-0/0/0.0

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
---(more 74%)---
```

CLOUDFLARE

RPKI

Explore the Routing Security ecosystem

ASN: Enter an AS number

PREFIX: 211.238.64.0/19

PREFIX MATCH: Exact Only | **Less Specific** | More Specific

ROA VALIDATION: **All** | Valid | Invalid | None

BGP Routes

Valid
100%

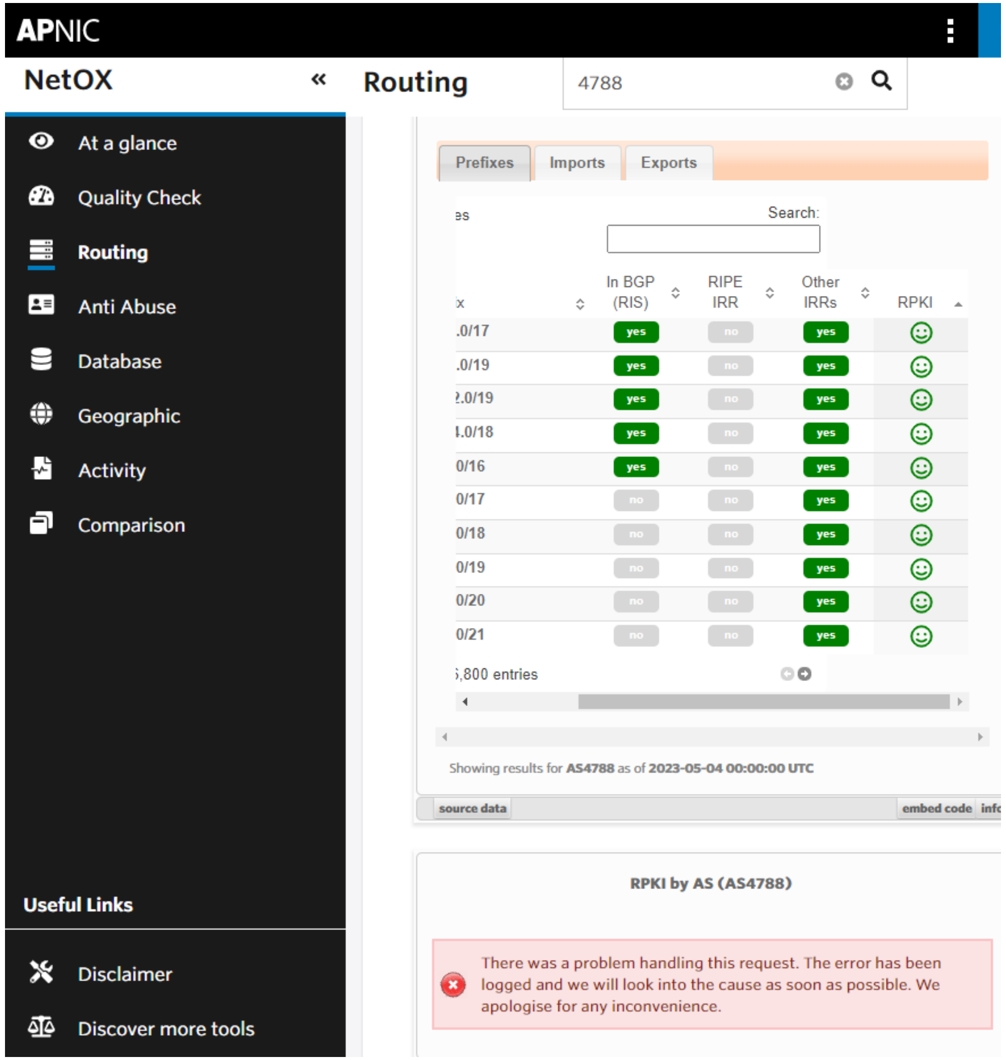
ASN	Prefix	IP Family	ROA
AS9976	211.238.64.0/19	IPv4	✓ Valid

Covering ROAs for 211.238.64.0/19 :

Trust Anchor	Prefix	Max Length	ASN	Expiration	Match
APNIC	211.238.64.0/19	19	9976	in 4 months	✓

1–1 of 1 items

Routing Table View



Routing

4788

Search:

x	In BGP (RIS)	RIPE IRR	Other IRRs	RPKI
.0/17	yes	no	yes	☺
.0/19	yes	no	yes	☺
2.0/19	yes	no	yes	☺
4.0/18	yes	no	yes	☺
0/16	yes	no	yes	☺
0/17	no	no	yes	☺
0/18	no	no	yes	☺
0/19	no	no	yes	☺
0/20	no	no	yes	☺
0/21	no	no	yes	☺

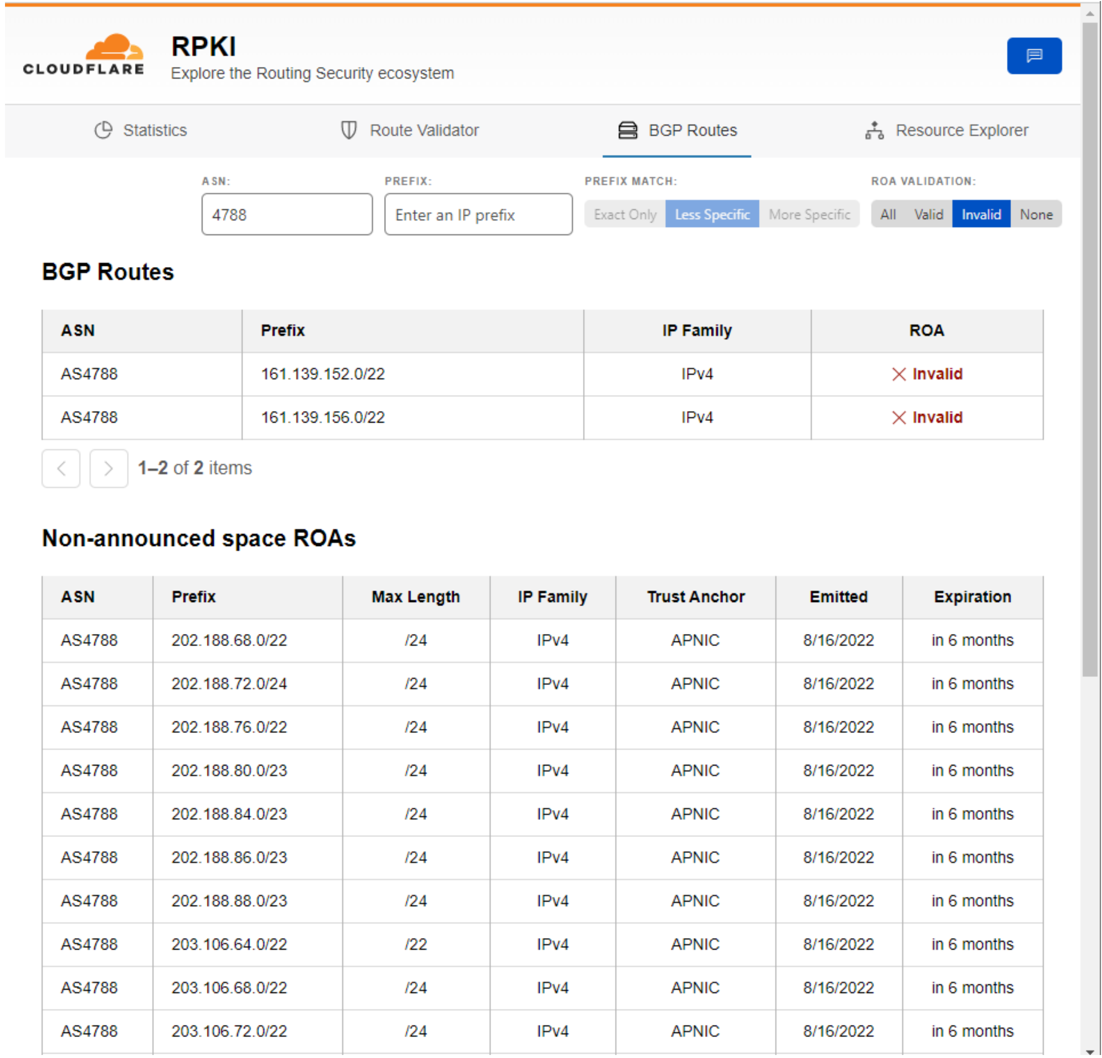
5,800 entries

Showing results for **AS4788** as of **2023-05-04 00:00:00 UTC**

RPKI by AS (AS4788)

There was a problem handling this request. The error has been logged and we will look into the cause as soon as possible. We apologise for any inconvenience.

Source: https://netox.apnic.net/apnic-routing/AS4788



RPKI

Explore the Routing Security ecosystem

ASN: 4788

PREFIX: Enter an IP prefix

PREFIX MATCH: Exact Only | **Less Specific** | More Specific

ROA VALIDATION: All | Valid | **Invalid** | None

BGP Routes

ASN	Prefix	IP Family	ROA
AS4788	161.139.152.0/22	IPv4	✕ Invalid
AS4788	161.139.156.0/22	IPv4	✕ Invalid

1–2 of 2 items

Non-announced space ROAs

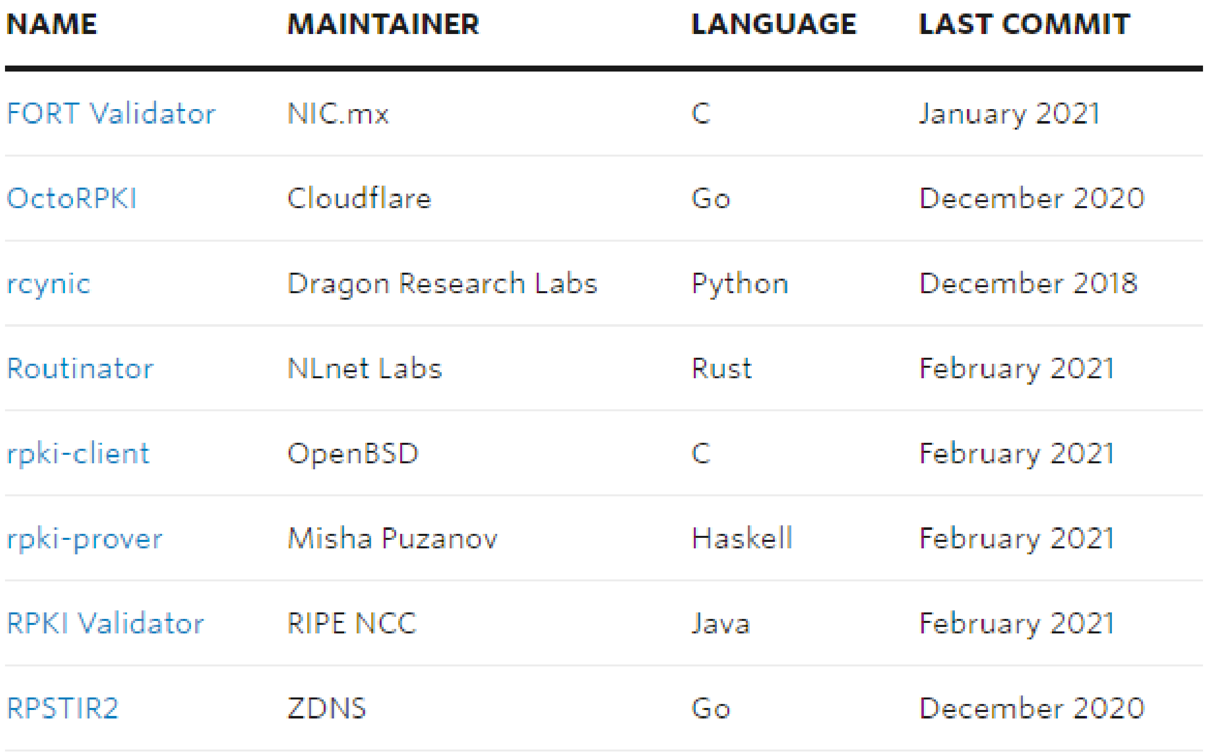
ASN	Prefix	Max Length	IP Family	Trust Anchor	Emitted	Expiration
AS4788	202.188.68.0/22	/24	IPv4	APNIC	8/16/2022	in 6 months
AS4788	202.188.72.0/24	/24	IPv4	APNIC	8/16/2022	in 6 months
AS4788	202.188.76.0/22	/24	IPv4	APNIC	8/16/2022	in 6 months
AS4788	202.188.80.0/23	/24	IPv4	APNIC	8/16/2022	in 6 months
AS4788	202.188.84.0/23	/24	IPv4	APNIC	8/16/2022	in 6 months
AS4788	202.188.86.0/23	/24	IPv4	APNIC	8/16/2022	in 6 months
AS4788	202.188.88.0/23	/24	IPv4	APNIC	8/16/2022	in 6 months
AS4788	203.106.64.0/22	/22	IPv4	APNIC	8/16/2022	in 6 months
AS4788	203.106.68.0/22	/24	IPv4	APNIC	8/16/2022	in 6 months
AS4788	203.106.72.0/22	/24	IPv4	APNIC	8/16/2022	in 6 months

Source: https://rpki.cloudflare.com/?view=bgp&validateRoute=9986_&asn=4788&validState=Invalic

Validate ROA status

Validators

did you notice a fw there? remember at the airport..there are police officers as well right? to protect is not a single entity task ..



NAME	MAINTAINER	LANGUAGE	LAST COMMIT
FORT Validator	NIC.mx	C	January 2021
OctoRPKI	Cloudflare	Go	December 2020
rcynic	Dragon Research Labs	Python	December 2018
Routinator	NLnet Labs	Rust	February 2021
rpki-client	OpenBSD	C	February 2021
rpki-prover	Misha Puzanov	Haskell	February 2021
RPKI Validator	RIPE NCC	Java	February 2021
RPSTIR2	ZDNS	Go	December 2020

Source: https://blog.apnic.net/2021/02/17/ripes-rpki-validator-is-being-phased-out-so-what-are-the-other-options/

validador FORT

TM Validators

VM

RedHat

RAM - 8GB

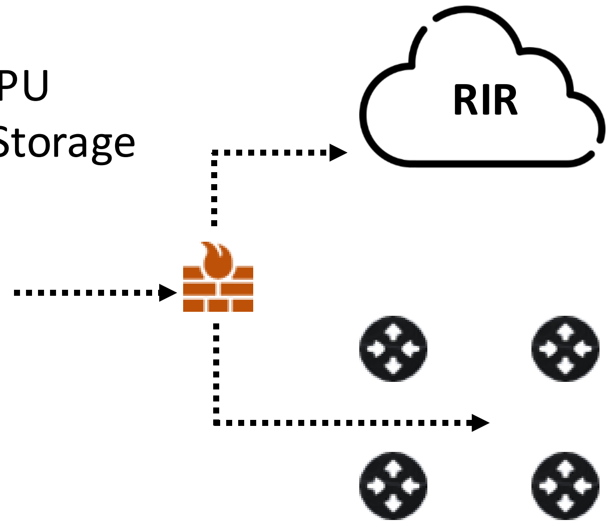
vCPUs - 2 vCPU

Disk - 50GB Storage

2 gateway;

1 to Internet

1 to Infra



Challenges in RPKI Deployment

New setup - Awareness

Firmware - For a certain vendors,
only latest version are able to support RPKI config.

Multi vendors - Meaning to say that you will
have multiple way of executing and configuring the syntax

Which timer - Which value to use. E.g keeping the database upon validator failure?

	Vendor A	Vendor B	Vendor C	Vendor D
1. Dual peer validator	OK	OK	OK	OK
2. BGP route status	OK	OK	OK	OK
3. Drop Invalid	OK	OK	OK	OK
4. Add comm for Unknown route	OK	OK	OK	OK
5. Modify local pref for Unknown route	OK	OK	OK	OK
6. Whitelist	OK	NA	NA	OK
7. Validator 1 down	OK	OK	OK	OK
8. Validator 2 down while 1 still down	OK	OK	OK	OK
9. Validator up at the same time	OK	OK	OK	OK
10. Route status when both validator fail	OK	OK	OK	OK

What TM validates prior to deployment

YOUR NEXT IS NOW TM

	Vendor A	Vendor B	Vendor C	Vendor D	TM Node
refresh-time (s)	300 (5m)	300 (5m)	1800 (30m)	300 (5m)	600 (10m)
hold-time (s)	600 (10m)	600 (10m)	1800x3 (90m) **Fix**	600 (10m)	1200 (20m)
record-lifetime (s)	3600 (60m)	= hold-time	3600 (60m)	3600 (60m)	3600 (60m)
preference (s)	NA	1..10 < best	NA	1..200 > best	
white-list invalid	YES	NA	NA	YES	

hold-time	Time after which the session is declared down. (10..3600 seconds)
Port	Port number to connect (1..65535)
Preference	Preference for session establishment (1..255)
record-lifetime	Lifetime of route validation records (60..604800 seconds)
refresh-time	Interval between keep alive packet transmissions (1..1800 seconds)

Vendor Timers RTR Preference

Best Practice Summary

No	Item	Detail
1	**Start with ROA Management**	• **Create ROAs** for your prefixes to specify which ASNs are authorized to originate them. • Use the **minimal-specific ROA** model to avoid inadvertent invalids. E.g., avoid overlapping or overly specific ROAs unless necessary. • Regularly **review and update ROAs**—especially during IP transfers, reassignments, or peering changes.
2	**Monitor Route Validity**	• Use tools like RIPEstat, BGPalerter, or RPKI Dashboard tools to monitor validity and alerts. • Analyze **invalid announcements** and assess whether they are due to misconfigurations or malicious activity.
3	**Rely on Trusted RPKI Validators**	• Deploy well-supported validators like: Routinator (NLnet Labs) OctoRPKI (Cloudflare) rpki-client (OpenBSD) • Ensure validator software is **updated regularly** for security and reliability.
4	**Implement RPKI Route Origin Validation in BGP**	• Use routers that support **RPKI origin validation** (e.g., Juniper, Cisco, Arista, etc.). • Apply **policy controls** based on validation states: **Valid**: Accept and prefer **Invalid**: Reject or deprioritize **Unknown**: Treat as normal (until broader coverage is achieved)
5	**Gradual Rollout**	• **Monitor first**, then **enforce**: Start with logging-only mode for RPKI origin validation. • Run dual logging (RPKI and traditional filters) to compare results. • Move to enforcement once you're confident in coverage and policy correctness.

No	Item	Detail
1	**Avoid Overlapping ROAs**	• Overlapping or conflicting ROAs can cause valid routes to be marked **invalid** unintentionally. • Example: ROAs that don't cover more-specific subnets or misalign with prefix lengths can break routing
2	**Operational Complexity Increases with ROA Granularity**	• The more fine-grained your ROAs (e.g., per /24 vs per /16), the harder it is to maintain accuracy. • Automate ROA creation and expiration tracking when possible.
3	**Coordination is Key**	• Misalignments between upstreams and downstreams (e.g., if one party uses outdated ROAs) can cause **reachability issues**. • Maintain **clear communication** between all parties in the routing chain.
4	**Partial Adoption Limits Effectiveness**	• Many routes are still in "Not Found" (Unknown) status because of partial RPKI adoption • Origin validation only works well when a **critical mass** of ASNs participates
5	**Invalid ≠ Malicious**	• Many invalids are due to: ○ Forgotten or stale ROAs ○ Typos ○ IP address changes not reflected in ROAs • Avoid overreacting to invalids—**investigate first**.
6	**RPKI Trust Anchor Management is Critical**	• Monitor trust anchors (APNIC, ARIN, RIPE, LACNIC, AFRINIC) and ensure your validator has **up-to-date TALs** (Trust Anchor Locators). • Use **multiple redundant validators** in production.

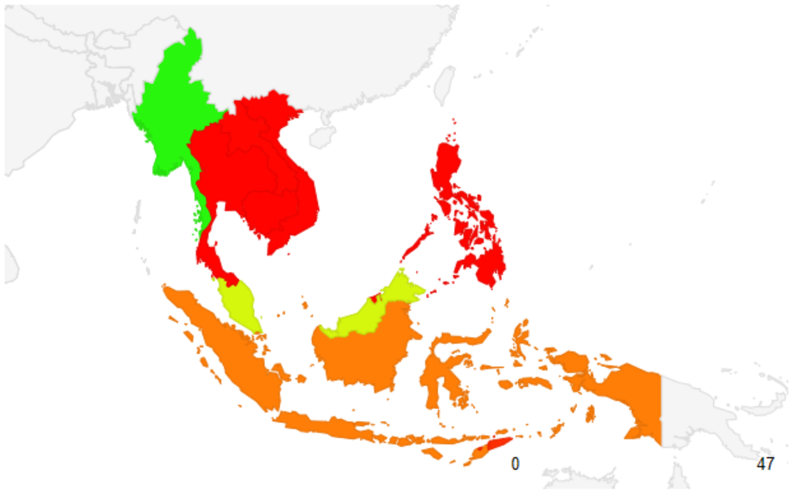
Lessons Learned from Operational Deployment

YOUR NEXT IS NOW

TM

Region Map for South-Eastern Asia (035)

Feb 2025



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

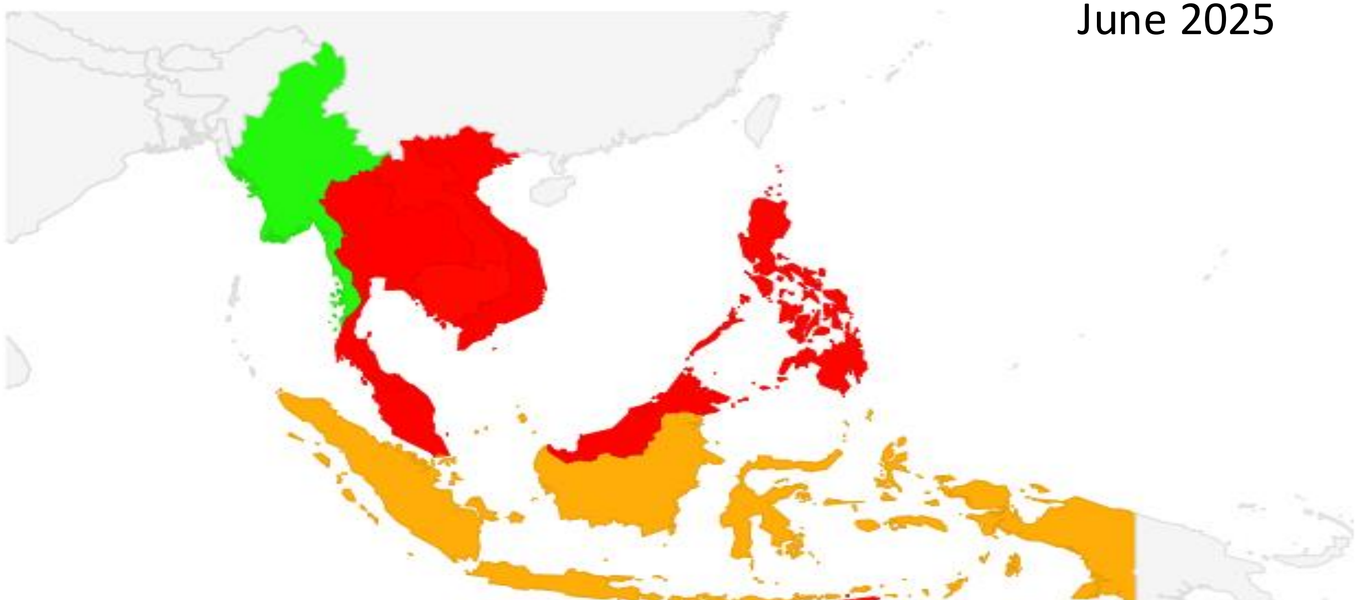
Code	Region	RPKI Validates	Samples	Weight	Weighted Samples	V4 Validates	V4 Count	V6 Validates	V6 Count
XA	World	21.73%	10,646,193	1	10,646,193	22.56%	10,646,193	26.16%	4,161,596
XD	Asia	5.81%	5,178,352	1.16	6,018,408	6.39%	5,178,352	4.49%	2,274,729

Code	Region	RPKI Validates	Samples	Weight	Weighted Samples	V4 Validates	V4 Count	V6 Validates
XU	South-Eastern Asia, Asia	9.11%	1,473,669	0.61	905,664	9.29%	1,473,669	7.49%

ASN	AS Name	RPKI Validates	Samples	V4 Validates	V4Count	V6 V
AS4788	TTSSB-MY TM TECHNOLOGY SERVICES SDN. BHD.	99.66%	31,915	99.66%	31,915	
AS9534	MAXIS-AS1-AP Binariang Berhad	0.12%	26,883	0.62%	26,883	
AS4818	DIGIIX-AP DiGi Telecommunications Sdn. Bhd.	0.14%	20,750	0.48%	20,750	
AS10030	CELCOMNET-AP Celcom Axiata Berhad	0.28%	17,783	0.77%	17,783	

Region Map for South-Eastern Asia (035)

June 2025



Telekom Malaysia's phased RPKI deployment revealed interoperability issues among different router vendors. For instance, one vendor's PE router triggered unnecessary route refresh messages upon receiving updated ROA data, leading to increased CPU consumption on route reflectors. Such vendor-specific quirks necessitated custom configurations and patches, underscoring the complexities of multi-vendor RPKI implementations.

Additionally, the presence of **multi-vendor devices with EOS (End of Support**) nodes has limited Telekom Malaysia’s ability to expand its RPKI deployment.

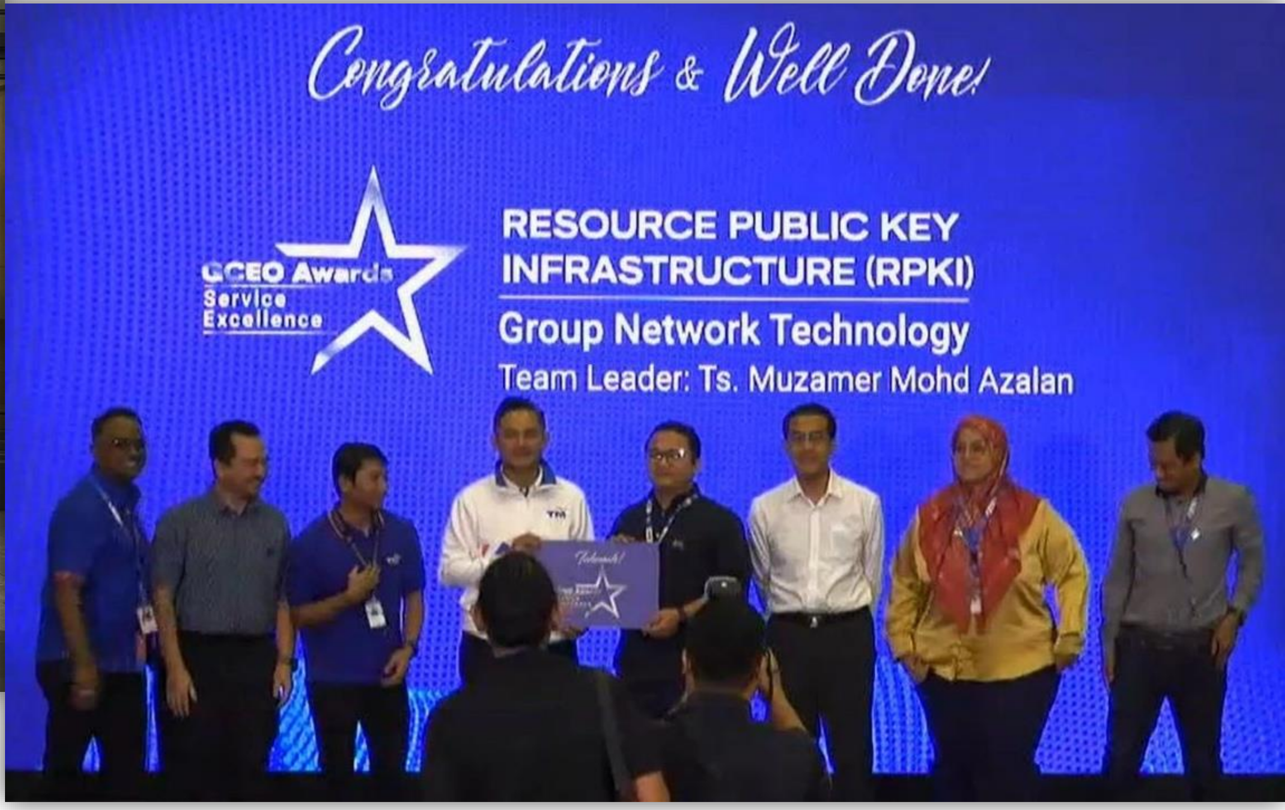
Success Stories that eventually required more action to sustain

YOUR NEXT IS NOW TM

What`s Next?

Initiative	Purpose
Expand ROA Coverage	• Ensure **100% ROA coverage** for all routed prefixes, including sub-allocations and customer downstreams. • Introduce **ROA automation** via APIs (e.g., ARIN, RIPE) to reduce manual overhead and errors.
Enable RPKI Validation Across All Networks	• Enforce **origin validation** on all BGP edge routers (IXPs, upstreams, customer-facing). • To revisit 2 routers that need to OS upgrade to enable RPKI adoption. • To revisit vendor x RPKI implementation.
RPKI Resiliency	• Deploy **multiple redundant validators** in geographically diverse PoPs. • Build in **validator health monitoring and failover** using BGP communities or policy triggers

YOUR NEXT IS NOW | TM


Congratulations & Well Done!
GCEO Awards
Service Excellence
RESOURCE PUBLIC KEY INFRASTRUCTURE (RPKI)
Group Network Technology
Team Leader: Ts. Muzamer Mohd Azalan

The Ceremony

My Words...

Implementing RPKI has not been without its challenges. The team encountered a steep learning curve, particularly in understanding and deploying components such as validators, ROAs, and the RTR protocol.

Despite these hurdles, your perseverance and commitment have been truly commendable. I would like to extend my heartfelt congratulations to the entire team for your outstanding work and for being pioneers in RPKI implementation here in Malaysia. Your efforts are a significant milestone in strengthening the security and integrity of our national internet infrastructure.

I strongly encourage all ISPs to take the next step and begin their RPKI journey. Yes, there will be challenges. Yes, the learning curve is real. But as we've seen, the benefits far outweigh the initial investment. By deploying RPKI, you are not just protecting your network—you are contributing to a more secure, resilient internet for everyone.

YOUR
NEXT
IS NOW
TM

Thank You

YOUR NEXT IS NOW TM