

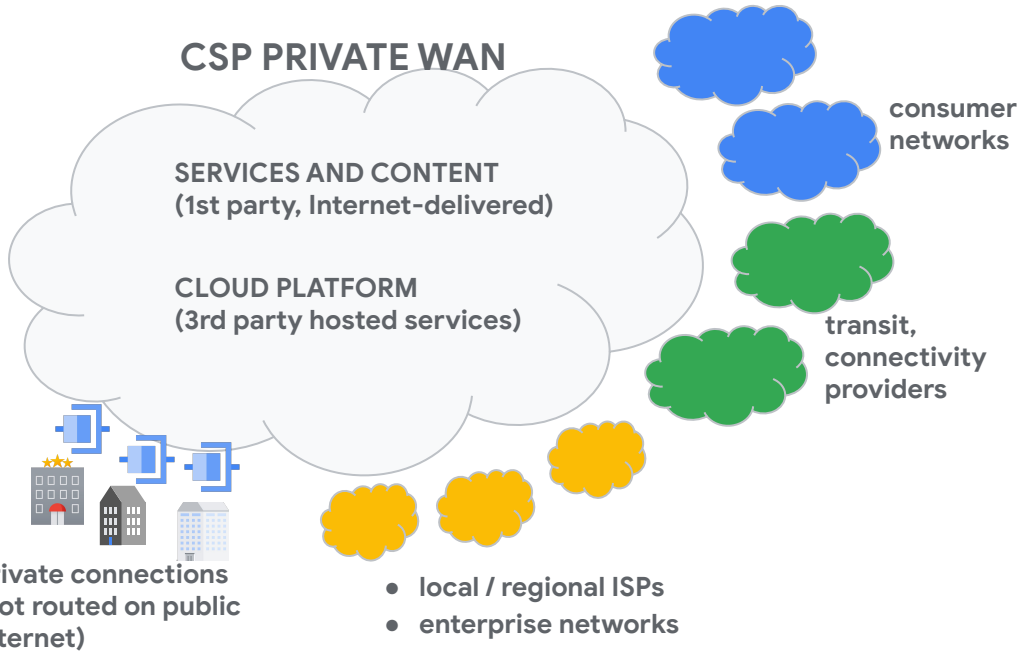
# BGP routing security: Cloud/Content providers

Anees Shaikh

*Google Global Networking*

July 2023 BGP Security Workshop

# Cloud Service Provider (CSP) networks



CSP networks are private “stub” networks with some unique characteristics

- large peering surface – independent reachability to significant portion of the Internet<sup>1</sup>
- global presence – peering in private facilities and public IXPs
- varying network architectures (e.g., differences in reliance on transit provider networks)

<sup>1</sup>Cloud Provider Connectivity in the Flat Internet, *ACM Internet Measurement Conference 2020*

# Protection for multiple types of routes

Cloud providers need to protect traffic against multiple kinds of routing disruptions

- *routes to CSP services and content* (reachability from users)
  - enable route validation by *other* networks (RPKI OV, IRR filtering, peer locks, ...)
  - monitor for hijacks in other networks (aim for proactive mitigation)
- *routes to reach users of CSP services and content* (return path to users)
  - validate received routes (filtering based on IRR and RPKI)
  - facilitate / encourage route registrations to enable wider filtering and limit propagation
- *routes to third-party services / content* (used by Cloud customers)
  - same techniques as above to validate received routes
- *third-party owned routes announced from the CSP* (e.g., BYOIP)
  - validate route ownership (e.g., by requiring creation of ROAs)
  - enable route validation and propagation by external networks

Not all routes are equal – how to prioritize?

- evaluate impact on traffic volume associated with routes
- routes associated with critical services or high-value customers

# Helping peers debug and improve their routing data

| Prefix ↑   | IRR                               | RPKI                   | Other Problems | Received by | Origin | Previous hops |
|------------|-----------------------------------|------------------------|----------------|-------------|--------|---------------|
| [REDACTED] | No Route Object <a href="#">🔗</a> | Good <a href="#">🔗</a> |                | Peering     | yes    | [REDACTED]    |
| [REDACTED] | No Route Object <a href="#">🔗</a> | Good <a href="#">🔗</a> |                | Peering     | yes    | [REDACTED]    |
| [REDACTED] | No Route Object <a href="#">🔗</a> | Good <a href="#">🔗</a> |                | Peering     | yes    | [REDACTED]    |
| [REDACTED] | No Route Object <a href="#">🔗</a> | Good <a href="#">🔗</a> |                | Peering     | yes    | [REDACTED]    |

Example: Google ISP portal  
(available to all networks that peer with Google)

Portal allows filtering by problem area (e.g., IRR or RPKI records)

Detail pane highlights specific problems and shows underlying IRR data

- route objects
- AS-SET objects
- peeringDB entries

BGP Prefixes → [REDACTED]

IRR Filtering Details ⓘ RPKI Filtering Details ⓘ

**IRR for [REDACTED] has a problem.** IRR SOURCE DETAILS

**IRR Route Objects**

**Route Object not found in IRR**  
We do not see a Route or Route6 record for this prefix in our IRR sources.

Peer: [REDACTED]  
peeringsdb.com/asn/[REDACTED]

- ✓ AS-SET found in PeeringDB
- ✓ PeeringDB AS-SET is valid

IRR AS-SET Records

[REDACTED]

# CSP routing security (partial) wishlist

## More networks registering routes in public databases (enable filtering)

- simplify RPKI ROA management (e.g., standardize across RIRs)
  - can we do better when we get to ASPA registrations?
- further enablement for legacy IP space to be registered in RPKI
- apply common filtering standards (e.g., for IRR-based filtering)

## Close gaps with major networks performing route validation (limit / eliminate propagation)

- steps to encourage remaining Tier-1/transit networks to filter on all links
  - good progress with RPKI OV in many large networks, but big gaps remaining (globally)
- public / managed filtering infrastructure (e.g., hosted RP systems)
  - enable networks with fewer resources to apply route validation
- remove remaining legal / process hurdles
- engage global govt. agencies to further encourage filtering deployment

## Expand coverage and visibility from route monitoring and incident reporting services

- public projects (RouteViews, RIS, GRIP, ...) and commercial services
- more focus on supporting and expanding public routing visibility and reporting projects

## BGP-related threats are getting more sophisticated – accelerate deployment of next set of protections

- path validation: ASPA? BGPsec? (today we have AS-SETs and peer locks)
- address vulnerabilities in legacy processes (LOAs, IRR authentication, ...)