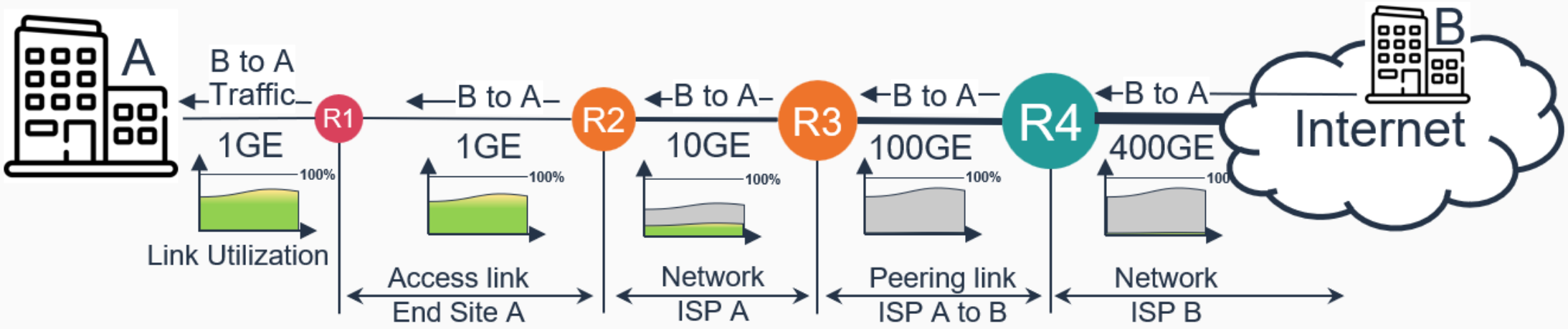
Source-Selective BGP (SSB)

draft-braet-idr-source-selective-bgp-framework &
draft-braet-idr-bgp-source-selective-attr

Kamiel Braet – Liberty Global
IETF 126 Vienna
July 2026

Internet DDoS challenge 1/4

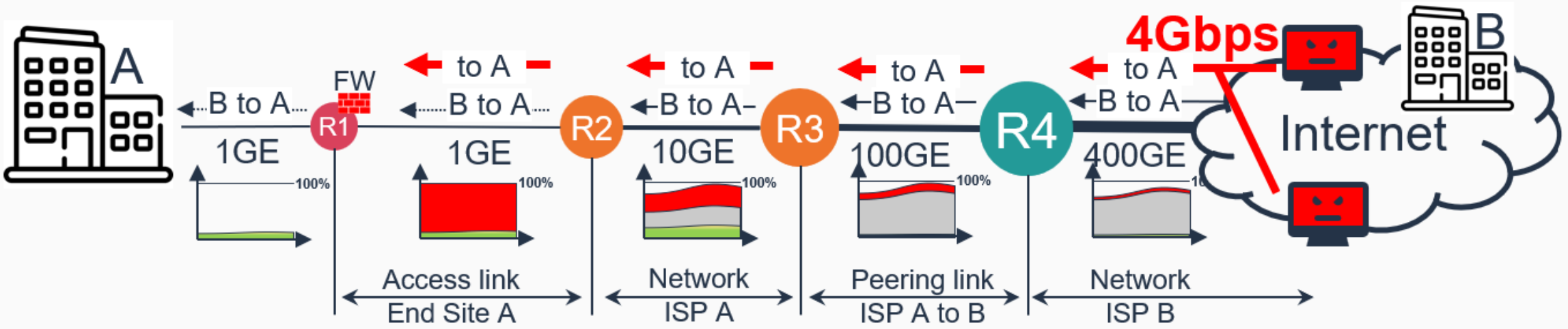


- End Site A has a 1GE access link to the Internet.
- End Site A uses this connection to receive traffic from Remote End Site B.
- Incoming traffic at End Site A arrives at an uncongested 1GE link with a utilization of less than 80%.
- Upstream ISP A & B links have increased capacity and shared usage with other End Sites. On these shared links the End Site A traffic is just a fraction of the total capacity.

Internet DDoS challenge 2/4

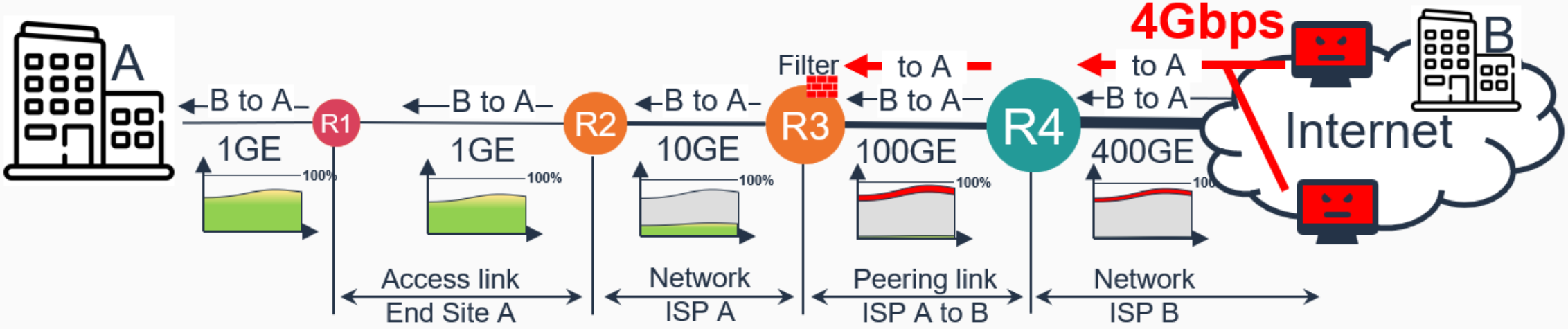
- 4Gbps DDoS attack is initiated to IP address space of End Site A.
- 400GE and 100GE connections can easily carry additional traffic, while the 10GE metro network link starts to drop some traffic and the 1GE is overloaded several times over.
- 1GE access link to End Site A is forced to start tail dropping >90% of legitimate traffic from B.

Internet DDoS challenge 3/4



- End Site A decides to start filtering out the unwanted DDoS traffic.
- As a result, the DDoS traffic no longer reaches the internal IT infrastructure, but End Site B traffic is still dropped due to the congested 1GE access link from ISP A.
- This still means that End Site A has effectively lost all Internet connectivity.

Internet DDoS challenge 4/4



- ISP A detects the DDoS attack and starts to filter out the unwanted DDoS traffic.
- As a result, the DDoS traffic no longer reaches ISP A network, which effectively reestablishes the Internet service of End Site A.
- This is because the 100GE peering link has the needed available capacity to absorb the 4 Gbps DDoS attack. **But what if the Attacker decides to increase the volume to 100Gbps?**

DDoS Mitigation Problem statement

- **The Scale Challenge**: Terabit-level volumetric DDoS attacks can only be absorbed by massive transit networks serving tens of millions of subscribers.
- **The Operational Goal**: How can these large networks dynamically leverage their massive edge capacity to protect hundreds of thousands of individual customer services?
- **The Engineering Constraints**:
  - **Data Plane**: Must utilize existing, deployed routing hardware (no expensive ASIC upgrades).
  - **Control Plane**: Must scale to hundreds of thousands of precise rules without destabilizing BGP or exhausting TCAM.
  - **Visibility**: Must support architectural openness and standard routing visibility to facilitate cross-domain troubleshooting.

Source-Selective BGP components

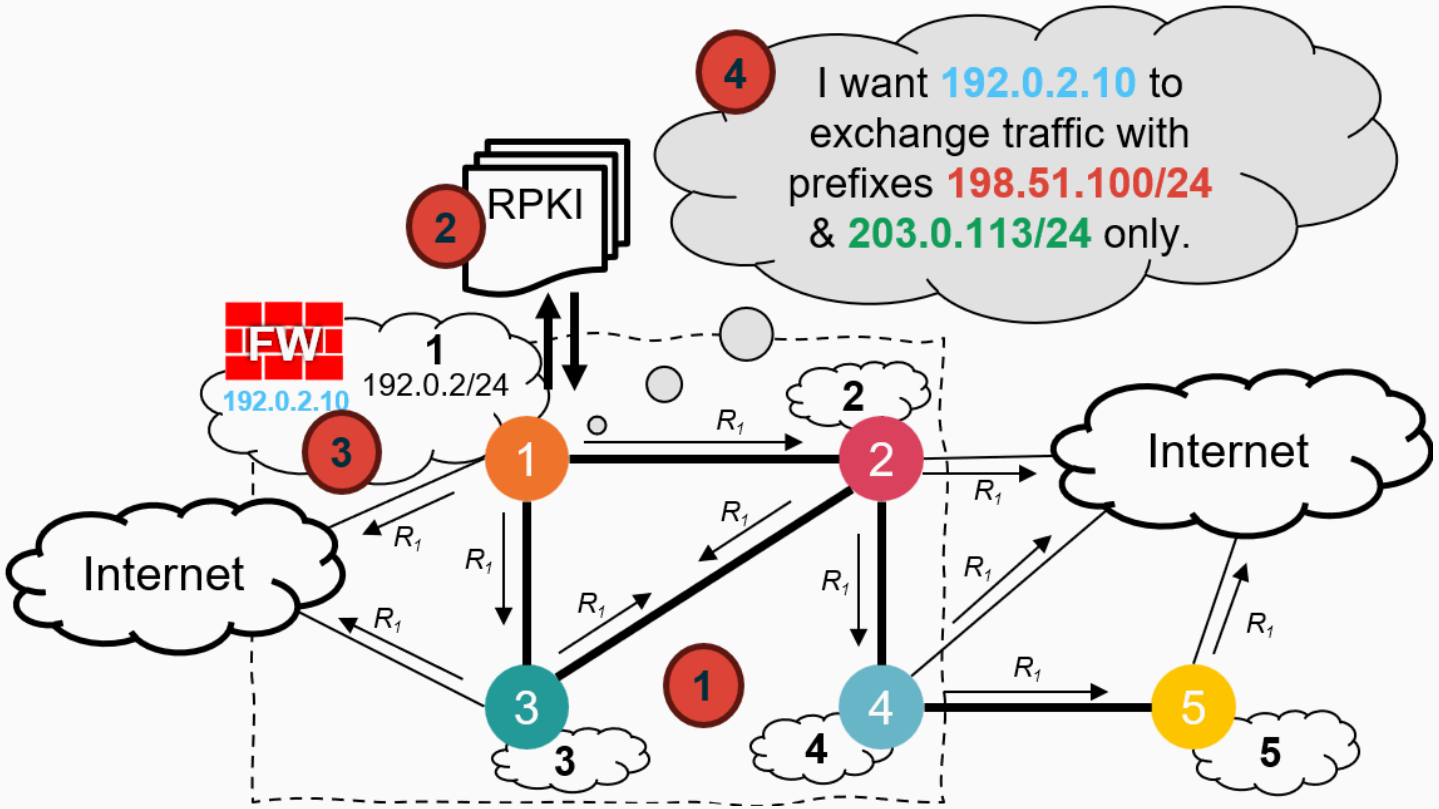
- BGP Attribute **SOURCE_SELECTIVE** containing RPKI object references:

```
▾ Path Attribute – SOURCE_SELECTIVE
  ▾ SA-ID: 2001:db8:2016.1f00::/56
      SA Type: Source Prefix Authorization IPv6 (SPA-IPv6)
      Length: 9
      Prefix Length: 56
      Protected Prefix: 2001:db8:2016.1f00::
  ▾ SA-ID: 2001:db8:2016.1f01::/56
      SA Type: Source Prefix Authorization IPv6 (SPA-IPv6)
      Length: 9
      Prefix Length: 56
      Protected Prefix: 2001:db8:2016.1f01::
```

- RPKI **Source Prefix Authorization** (SPA) profile type containing:
  - Protected Prefix (Ownership RPKI validated)
  - Authorized Source Prefixes

```
Border Gateway Protocol - UPDATE Message
  Marker: ffffffffffffffffffffffffffffffff
  Length: 85
  Type: UPDATE Message (2)
  Withdrawn Routes Length: 0
  Total Path Attribute Length: 62
▾ Path attributes
  › Path Attribute - ORIGIN: INCOMPLETE
  › Path Attribute - AS_PATH: empty
  › Path Attribute - MULTI_EXIT_DISC: 1
  › Path Attribute - LOCAL_PREF: 100
  ▾ Path Attribute - MP_REACH_NLRI
    › Flags: 0x80, Optional, Non-transitive, Complete
      Type Code: MP_REACH_NLRI (14)
      Length: 38
      Address family identifier (AFI): IPv6 (2)
      Subsequent address family identifier (SAFI): Unicast (1)
    › Next hop: 2001:db8:2018:1ff::15
      Number of Subnetwork points of attachment (SNPA): 0
    ▾ Network Layer Reachability Information (NLRI)
      ▾ 2001:db8:2016::/48
          MP Reach NLRI prefix length: 48
          MP Reach NLRI IPv6 prefix: 2001:db8:2016::
▾ Path Attribute – SOURCE_SELECTIVE
  ▾ SA-ID: 2001:db8:2016.1f00::/56
      SA Type: Source Prefix Authorization IPv6 (SPA-IPv6)
      Length: 9
      Prefix Length: 56
      Protected Prefix: 2001:db8:2016.1f00::
  ▾ SA-ID: 2001:db8:2016.1f01::/56
      SA Type: Source Prefix Authorization IPv6 (SPA-IPv6)
      Length: 9
      Prefix Length: 56
      Protected Prefix: 2001:db8:2016.1f01::
```

Source-Selective BGP applied 1/2

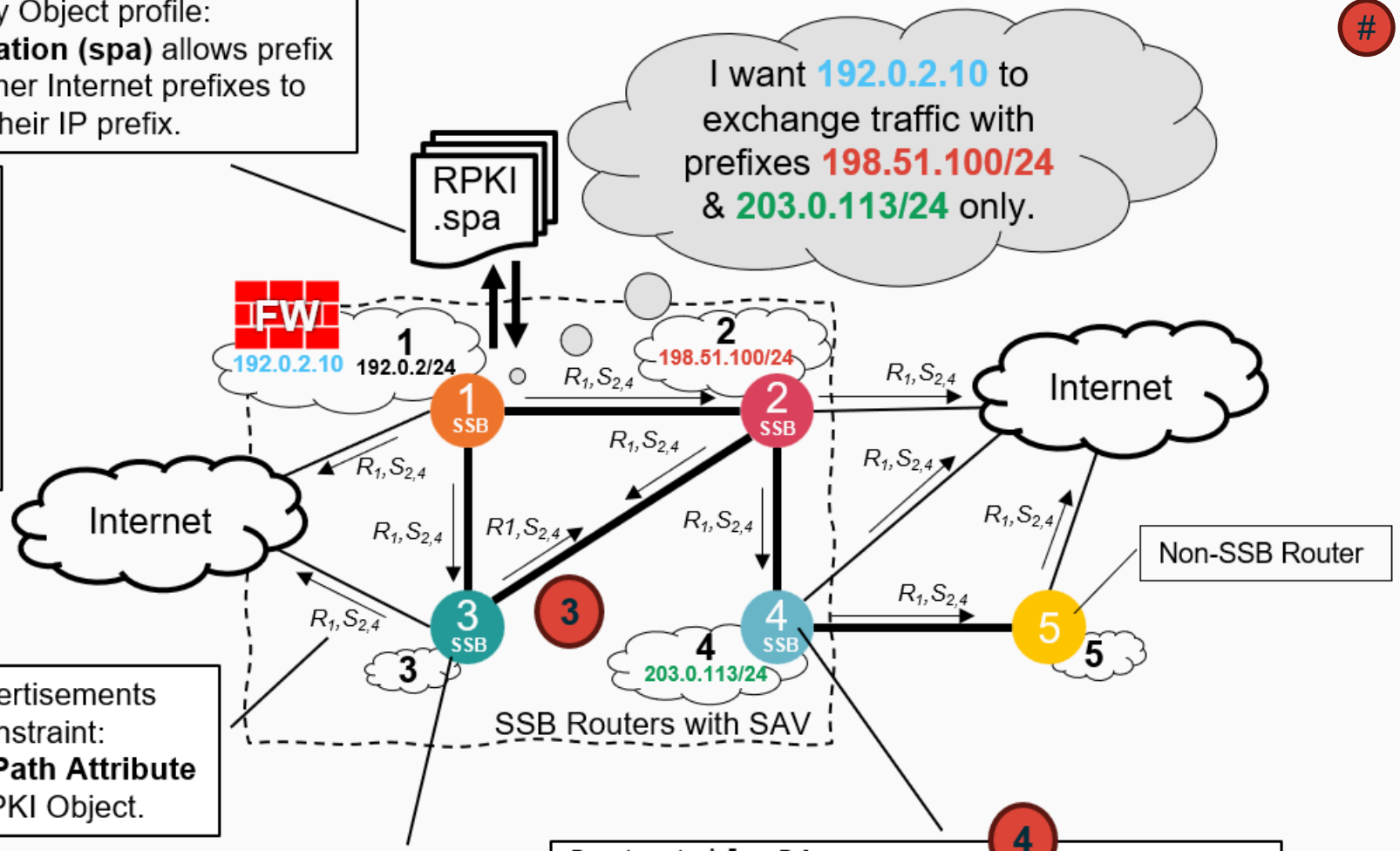


Source-Selective BGP applied 2/2

RPKI Repository Object profile:
Source Prefix Authorization (spa) allows prefix holders to authorize other Internet prefixes to send data to their IP prefix.

1

```
RPKI SPA Object:
 Protected Prefix:
  192.0.2.10/32
 Source Prefixes:
  198.51.100/24,
  203.0.113/24
 Policy type:
  allow
```



2

SSB Reachability advertisements include Source constraint:
SOURCE_SELECTIVE Path Attribute referring to a SPA RPKI Object.

Received SSB advertisements create route entries with Allowlist IP Packet forwarding constraints. SSB advertisement might be limited by policy to SSB routers only.

4

```
Route table R4:
 192.0.2.10/32 via R2; from AllowList-1
Allowlists R4 (implicit deny all):
 AllowList-1 198.51.100/24, 203.0.113/24
```

- Callout Points

Source-Selective BGP is NOT

- SSB does not define a Source Address Validation data-plane mechanism. Instead, is heavily relies on it.
- Fundamental destination-based routing remains unchanged; parsing attributes is entirely down to local operator policy.
- It does not mandate universal packet-filtering behaviours.

Mailing List Feedback Overview

- Path MTU discovery relies on **Packetization Layer Path MTU Discovery**
- Suitable for **Tier-1 networks** with Terabit DDoS absorption capabilities:
  - SSB is intended for environments whereby a single ISP must be able to serve 100s of thousands of protected prefixes with **millions of source prefixes** using standard ISP router forwarding hardware without capacity penalty.
  - Leverages **standard BGP update stability** to protect 100s of thousands of organizations from Terabit-level attacks.
- ISP can realistically only offer SSB for source prefixes in its own validated **Customer Cone** with rigorous SAV applied.
  - As a second stage SSB can be deployed across trusted SAV islands.
- SSB allows for stable **publicly visible Source Authorization policy activation**, while maintaining the open visibility needed for cross-domain troubleshooting and route validation.

The author would like to thank Robert Raszuk and Maria Matejka for their valuable feedback regarding the BGP SOURCE_SELECTIVE attribute specification.

Request for feedback

- **Attribute Optimization:**
  - Is the proposed format for carrying multiple RPKI SPA object references within the SOURCE_SELECTIVE attribute optimal?
  - Are there specific constraints regarding update sizing when a protected prefix references many distinct SPA objects?
- **Deployment & Integration:**
  - Are the operational interactions between SSB and SAVNET architectures sufficiently aligned?
  - Are there edge-case scenarios within the "SAV Island" or "Customer Cone" trust models that need additional documentation?
- **Next Steps for the Drafts:**
  - Seeking additional reviewers, operators, and co-authors to help refine the specifications.
  - Target is to collect feedback from this meeting and publish a comprehensive -01 update.