

Source Prefix Advertisement (SPA) for Inter-domain SAVNET

Nan Geng (Huawei), Lancheng Qin (ZGC Lab), Kotikalapudi Sriram (USA NIST),
Dan Li(Tsinghua University)

July 2025

Improper Block Problems of EFP-uRPF

- [\[I-D.ietf-savnet-inter-domain-problem-statement\]](#) shows that EFP-uRPF [\[RFC8704\]](#) may have improper block problems in the scenarios of
 - a) "hidden source prefixes" in the Direct Server Return (DSR) scenario (see section 4.1.2 of [\[I-D.ietf-savnet-inter-domain-problem-statement\]](#))
 - b) "hidden paths of source prefixes" caused by "Limited Propagation of Prefixes" (see section 4.1.1 of [\[I-D.ietf-savnet-inter-domain-problem-statement\]](#))

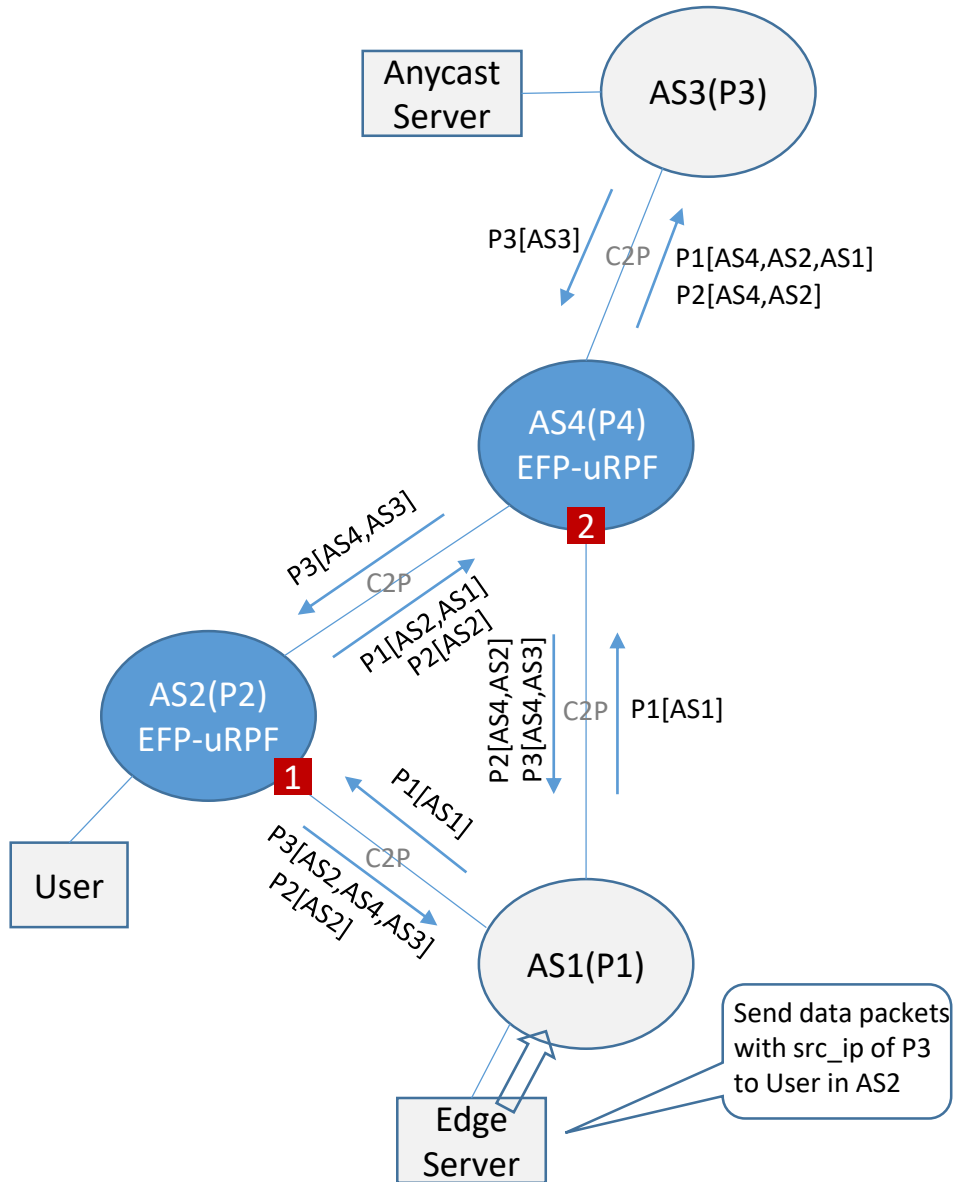
Inter-domain SPA Message

- Inter-domain SPA message is defined, which should include the following items:
 - ◆ Source Prefixes: The source prefixes that the source addresses of the locally originated data packets of Source AS belong to. The updated source prefixes are incremental to the previously announced prefixes.
 - ◆ Source AS Number
 - ◆ AS Path: Same meaning as the AS_PATH attribute in BGP Update.
 - ◆ Update/Withdraw Flag
- SPA can be used for:
 - ◆ Advertising "hidden source prefixes"
 - ◆ Discovering "hidden paths of source prefixes"

Source Prefixes
Source AS Number
AS Path
Update/Withdraw Flag

Inter-domain SPA Message

The DSR Scenario: "Hidden Source Prefixes"



□ BGP Update:

- ◆ AS1, AS2, and AS3 advertises their own routes of P1, P2, and P3.
- ◆ AS1 dose not advertise P3 (anycast server address).

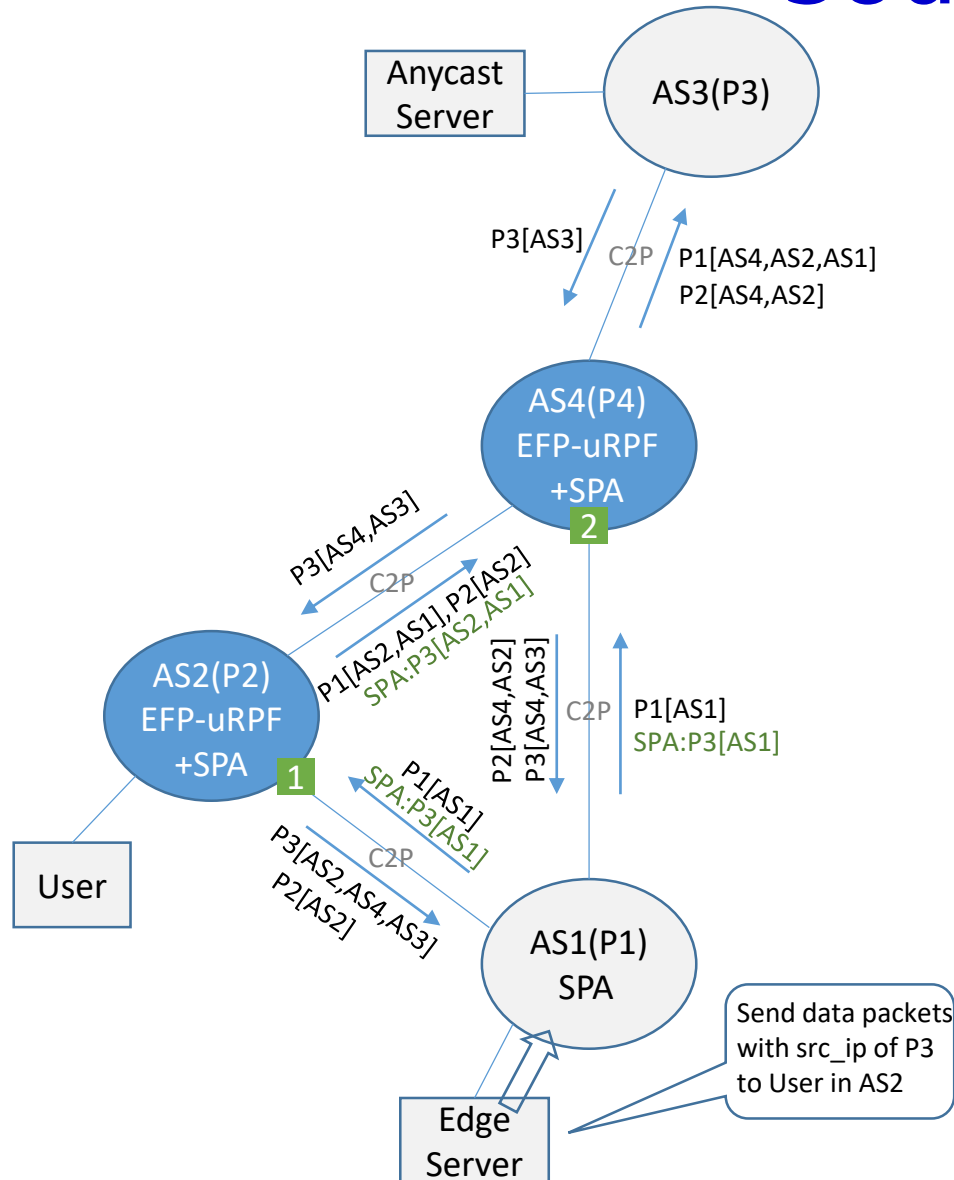
□ EFP-uRPF:

- ◆ If it is enabled at intf1 of AS2, the source prefix allowlist is **[P1]**.
- ◆ If it is enabled at intf2 of AS4, the source prefix allowlist is **[P1]**.

□ Improper block problems:

- ◆ If Edge Server in AS1 sends data packets with src_ip of P3 to User in AS2, the packets will be **improperly blocked** at either intf1 of AS2 or intf2 of AS4.

EFP-uRPF Enhanced by SPA: Advertising "Hidden Source Prefixes"



□ SPA Update:

- ◆ AS1, AS2, and AS4 needs to support SPA function.
- ◆ Besides normal BGP updates, AS1 advertise P3 in SPA messages.

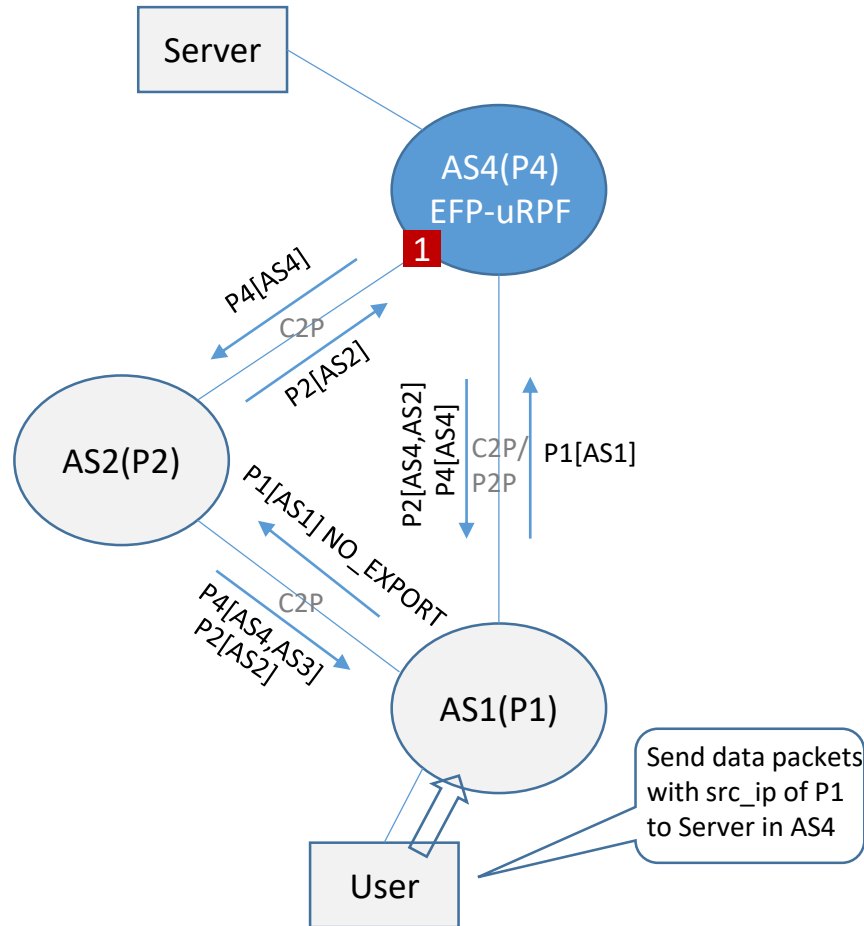
□ EFP-uRPF+SPA:

- ◆ Take a union of the prefixes in the SPA messages and the BGP Update messages for constructing allowlists
- ◆ If it is enabled at intf1 of AS2, the source prefix allowlist is [P1, P3].
- ◆ If it is enabled at intf2 of AS4, the source prefix allowlist is [P1, P3].

□ No improper block problems:

- ◆ If Edge Server in AS1 sends data packets with src_ip of P3 to User in AS2, the packets will be permitted at either intf1 of AS2 or intf2 of AS4.

The NO_EXPORT Scenario: "Hidden Paths of Source Prefixes"



□ BGP Update:

- ◆ AS1, AS2, and AS4 advertises their own routes of P1, P2, and P4.
- ◆ AS1 advertises P1 to AS2 with NO_EXPORT.

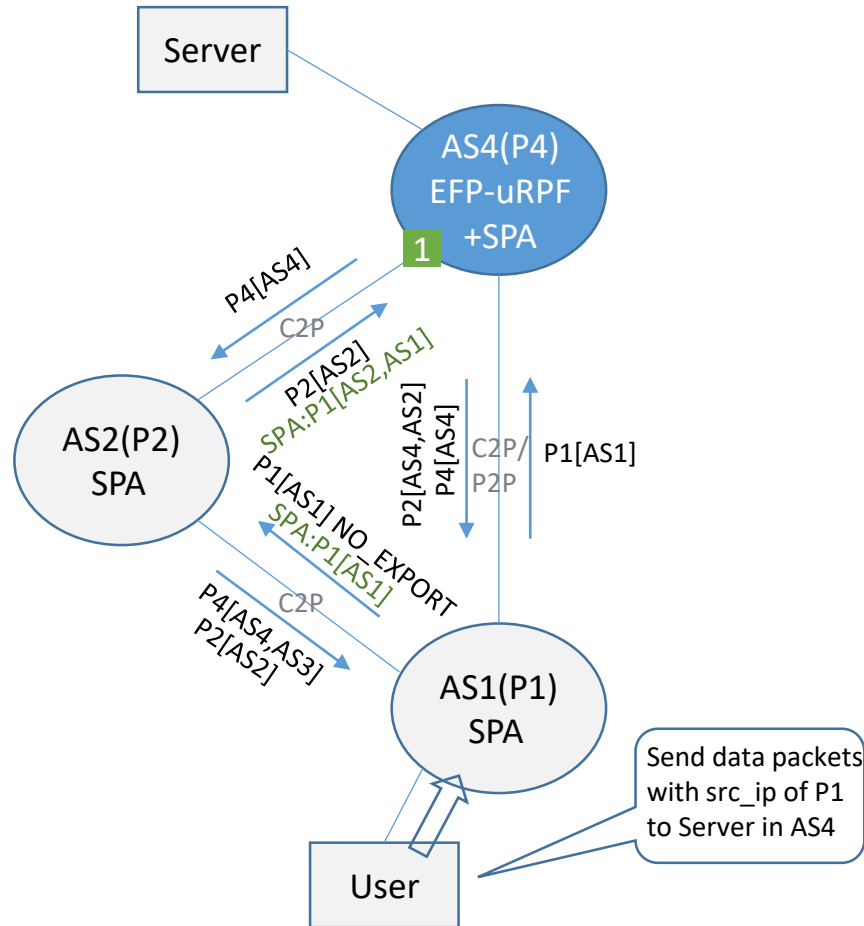
□ EFP-uRPF:

- ◆ If it is enabled at intf1 of AS4, the source prefix allowlist is [P2].

□ Improper block problems:

- ◆ If User in AS1 sends data packets with src_ip of P1 to Server in AS4, the packets will be **improperly blocked** at intf1 of AS4.

EFP-uRPF Enhanced by SPA: Discovering "Hidden Paths of Source Prefixes"



□ SPA Update:

- ◆ AS1, AS2, and AS4 advertises their own routes of P1, P2, and P4.
- ◆ AS1 advertises P1 to AS2 with no NO_EXPORT attached to the SPA message, and AS2 propagates the message to AS4.

□ EFP-uRPF+SPA:

- ◆ Take a union of the prefixes in the SPA messages and the BGP Update messages for constructing allowlists
- ◆ If it is enabled at intf1 of AS4, the source prefix allowlist is [P1, P2].

□ Improper block problems:

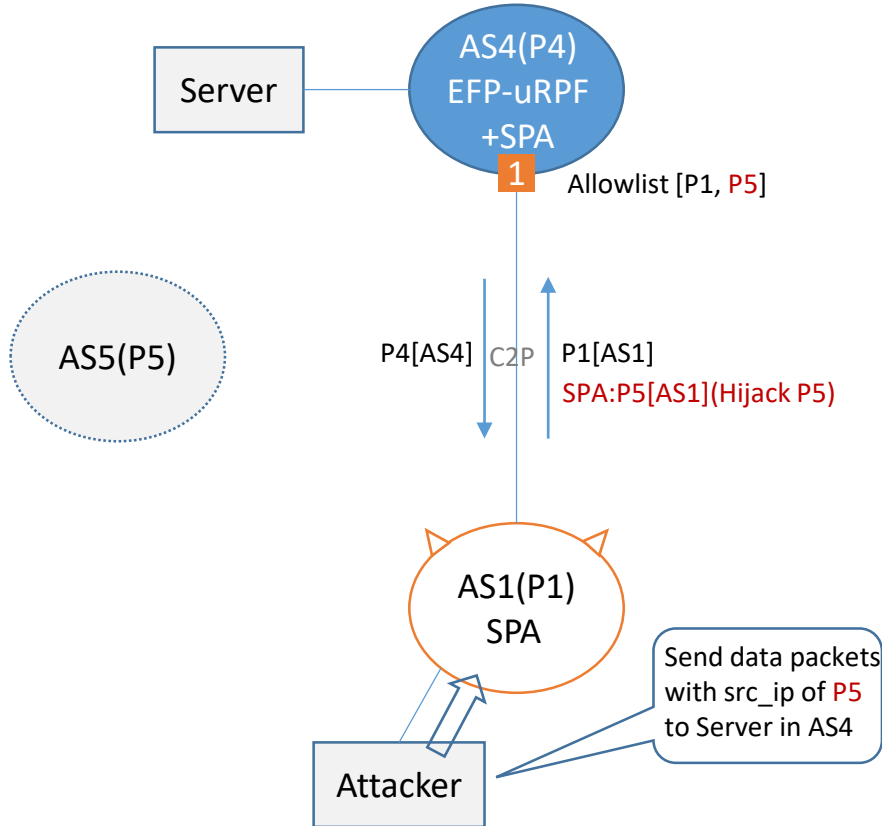
- ◆ If User in AS1 sends data packets with src_ip of P1 to Server in AS4, the packets will be **permitted** at intf1 of AS4.

Convergence Considerations

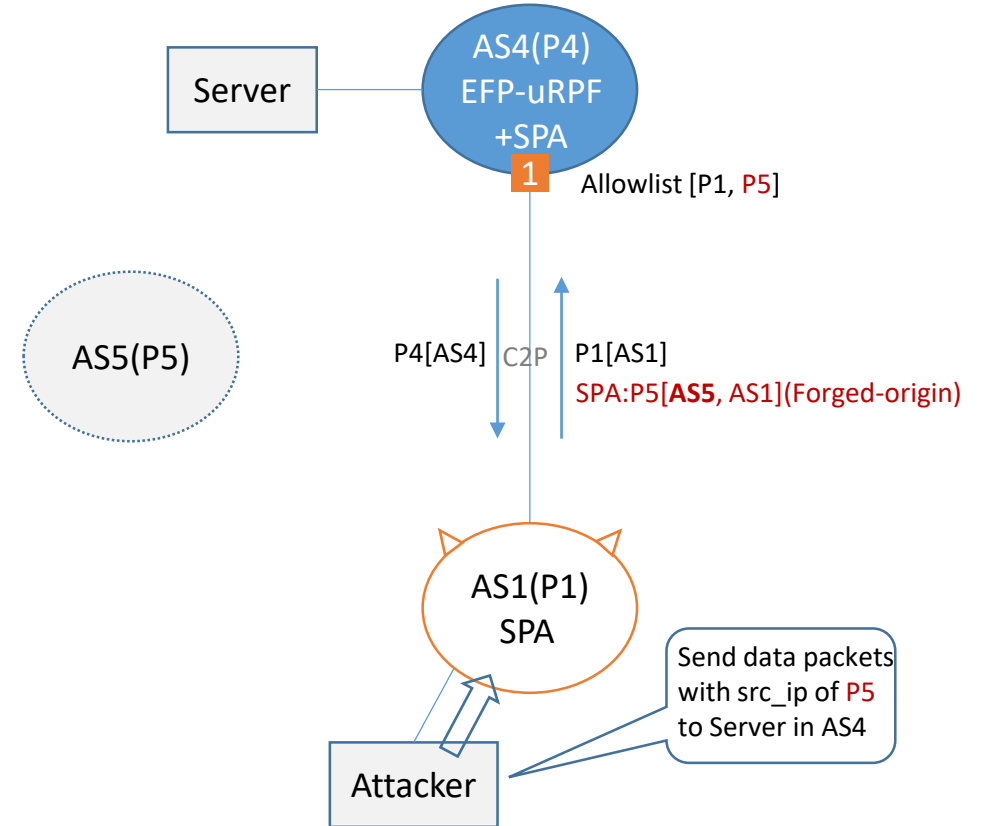
- Validating AS needs to update SAV rules when source prefixes of Source AS or the paths of source prefixes change. The following RECOMMENDED actions will result in more effective re-convergence:
 - ◆ Applying hysteresis in the case of **withdrawal of source prefixes or paths of source prefixes**: During the re-convergence, the SAV source prefix lists will include some withdrawn prefixes for a little longer, and there may exist **improper permitting shortly but no improper blocking**.
 - ◆ **Updating source prefixes or paths of source prefixes** as soon as possible when SPA message is received: During the convergence, any possibility of improper blocking will be minimized or eliminated **if new source prefixes are announced in SPA first and then some delay is allowed before the related services (utilizing the new source prefixes) are activated online**.

Security Considerations

- There are two main threats associated with SPA: prefix hijacking and path hijacking.



In the two cases, AS4 will improperly include P5 in allowlists, which results in improper permitting but no improper blocking.



Prefix hijacking. A malicious AS may send an SPA message which hijacks the source prefixes of a Source AS.

Path hijacking. A malicious AS may send an SPA message which carries a manipulated AS_PATH, which can be a forged-origin attack or a forged-path-segment attack.

Comments are welcome

Thanks!