Source Address Validation in Inter-domain Networks (Inter-domain SAVNET) Gap Analysis, Problem Statement, and Requirements

Jianping Wu, Dan Li, Lancheng Qin, Mingqing Huang, Nan Geng

Jul 25, 2022

Outline

- Background
- Gap Analysis
- Problem Statement
- Requirement
- Preliminary Idea

Outline

- Background
- Gap Analysis
- Problem Statement
- Requirement
- Preliminary Idea

Existing Inter-domain SAV Mechanisms

- RFC 2827 BCP 38, May 2000
  - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
- RFC 3704 BCP 84, March 2004
  - Ingress Filtering for Multihomed Networks
- RFC 8704 BCP 84, February 2020
  - Enhanced Feasible-Path Unicast Reverse Path Forwarding

Existing Inter-domain SAV Mechanisms

RFC 8704 makes the summary of recommendations for inter-domain SAV

- For directly connected networks
  - ACL-based ingress filtering, RFC 3704, BCP 84
- For directly connected single-homed stub AS
  - Strict uRPF, RFC 3704, BCP 84
- For all other scenarios
  - EFP-uRPF Algorithm B for customer interfaces, RFC 8704, BCP 84
  - Loose uRPF for provider/peer interfaces, RFC 3704, BCP 84

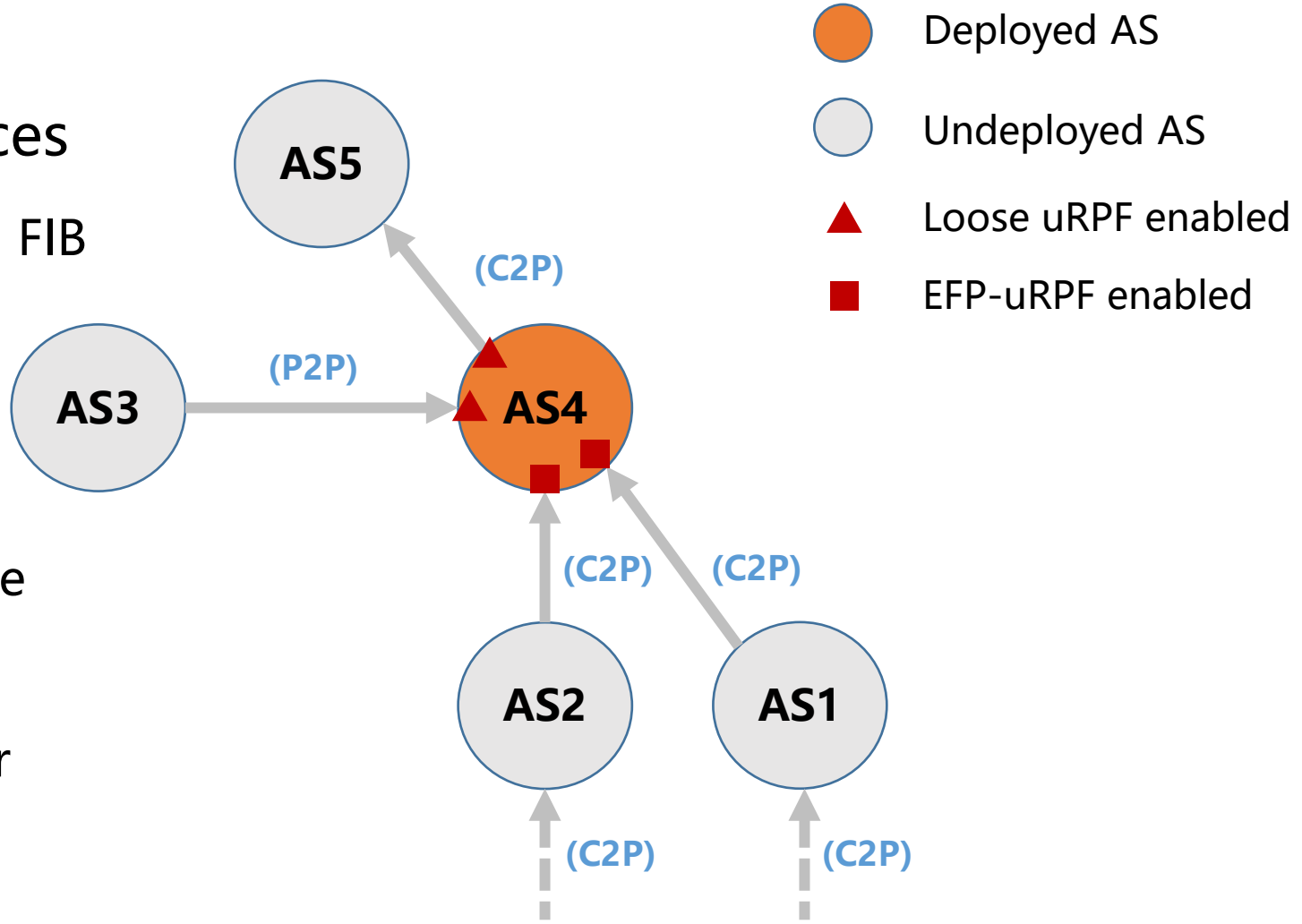
Typical Adoption of Inter-domain SAV

Loose uRPF

- Works on provider/peer interfaces
  - Accepts source addresses existing in FIB

EFP-uRPF

- Works on customer interfaces
  - Algorithm A: each customer interface applies an individual RPF list
  - Algorithm B (preferred): all customer interfaces share a same RPF list



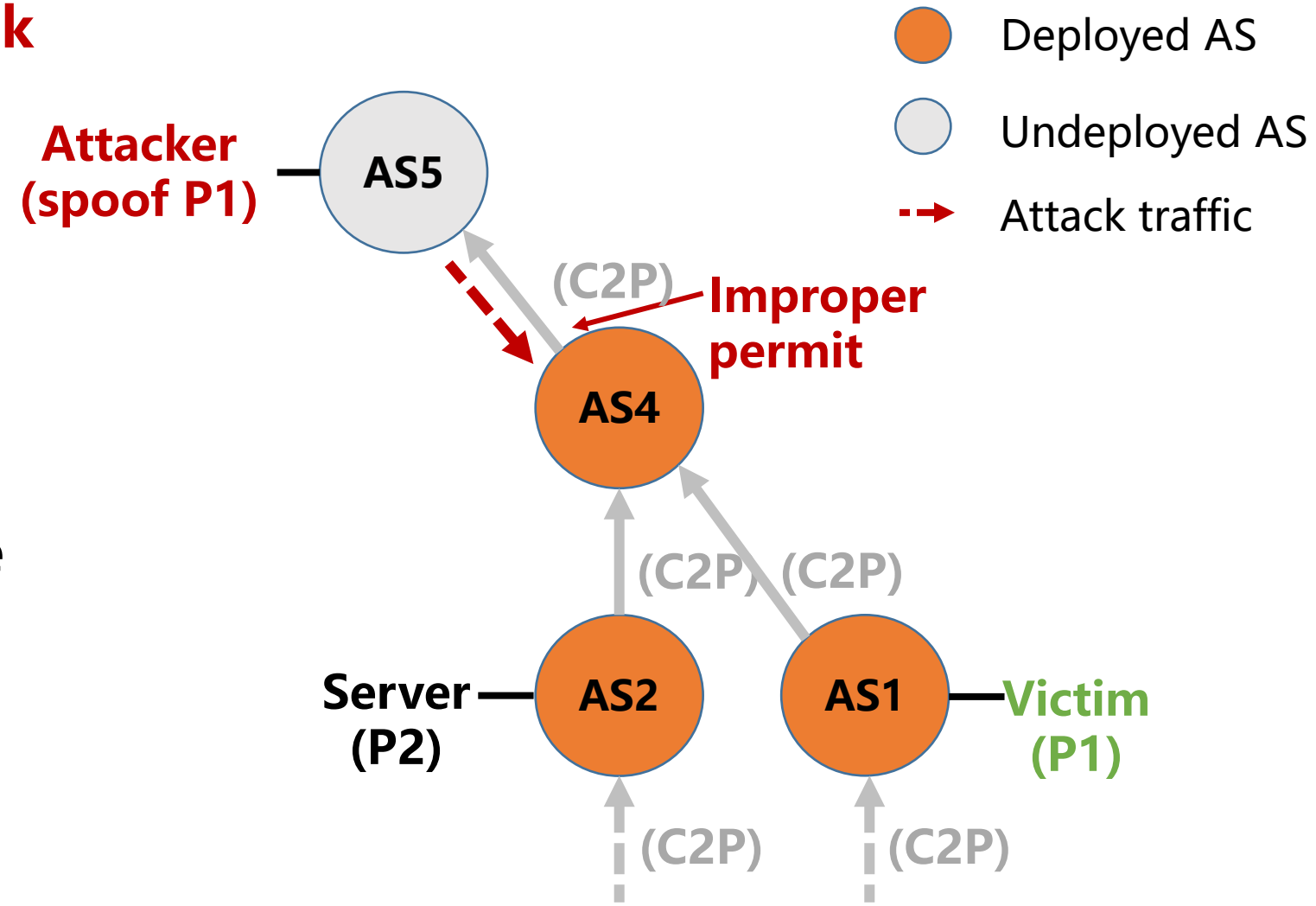
Outline

- Background
- Gap Analysis
- Problem Statement
- Requirement
- Preliminary Idea

Gap #1: Improper Permit

Scenario 1: Reflection attack

- Attacker: AS5
- Reflective server: AS2
- Victim: AS1



Scenario 1: Reflection attack

Behavior

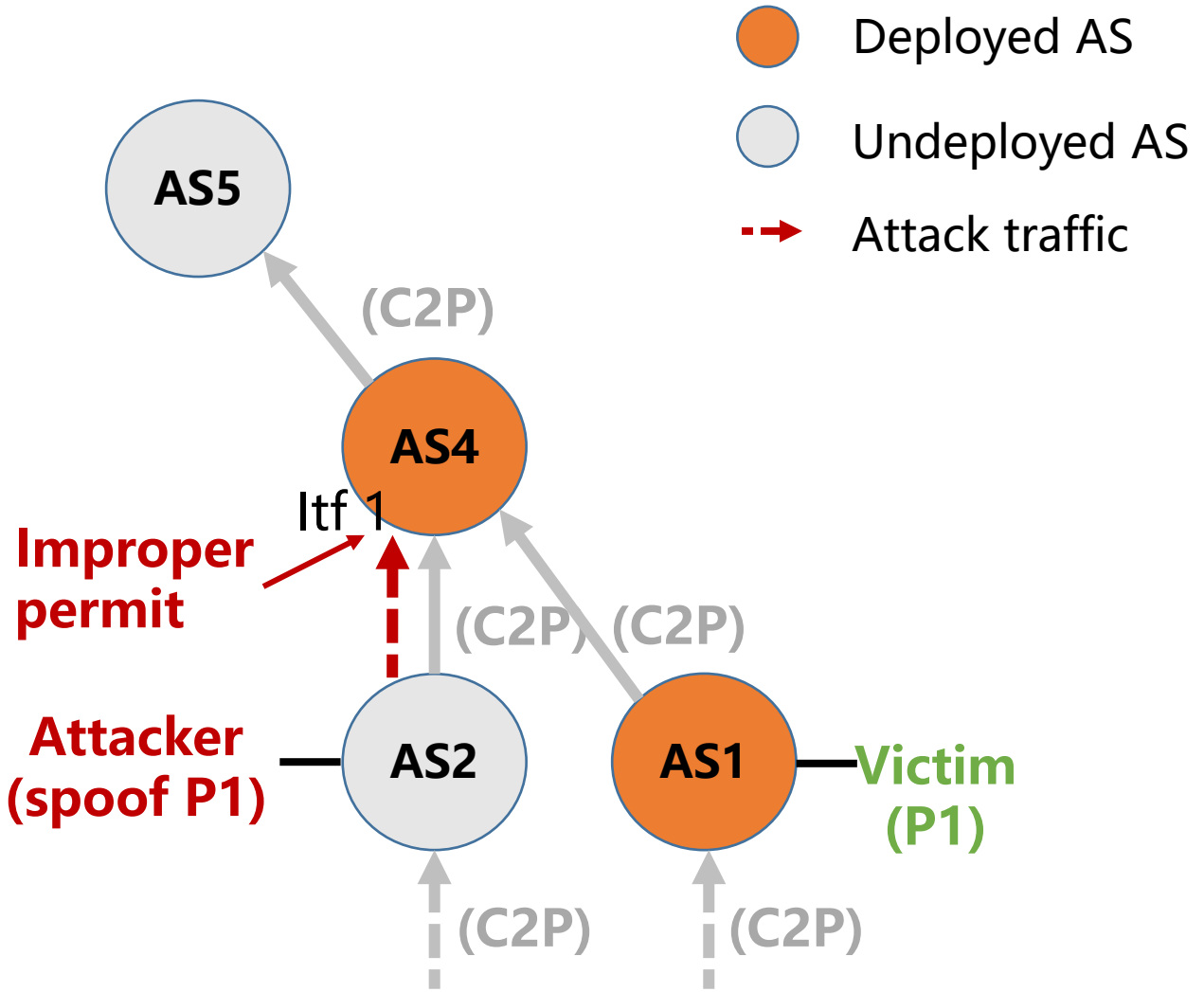
- AS4 **improperly permits** the spoofing traffic from AS5
  - Loose uRPF almost accepts any source address

Gap #1: Improper Permit

- **Scenario 2: Spoofing within the customer cone**

Behavior

- If AS4 runs EFP-uRPF Algorithm A
  - ◆Works well
- If AS4 runs EFP-uRPF Algorithm B
  - ◆**Improper permit** at Itf 1



Scenario 2: Spoofing within a customer cone

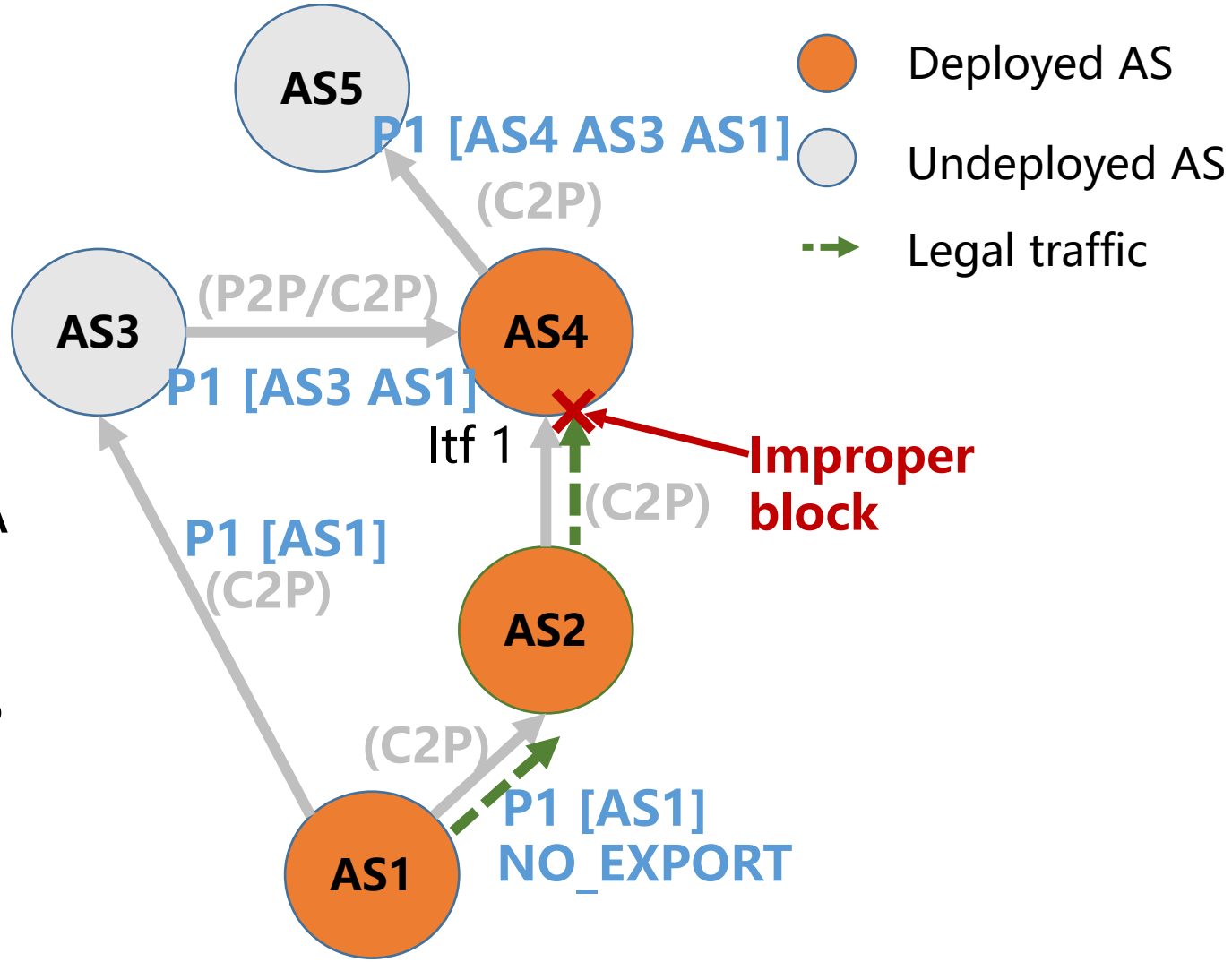
Gap #2: Improper Block

Scenario 3: NO_EXPORT in BGP Advertisement

- Forwarding path from AS1 to AS4: AS1->AS2->AS4

Behavior

- If AS4 runs EFP-uRPF Algorithm A
  - **Improper block** at Itf 1
- If AS4 runs EFP-uRPF Algorithm B
  - If AS3 is customer of AS4: no problem
  - If AS3 is peer of AS4: **improper block** at Itf 1



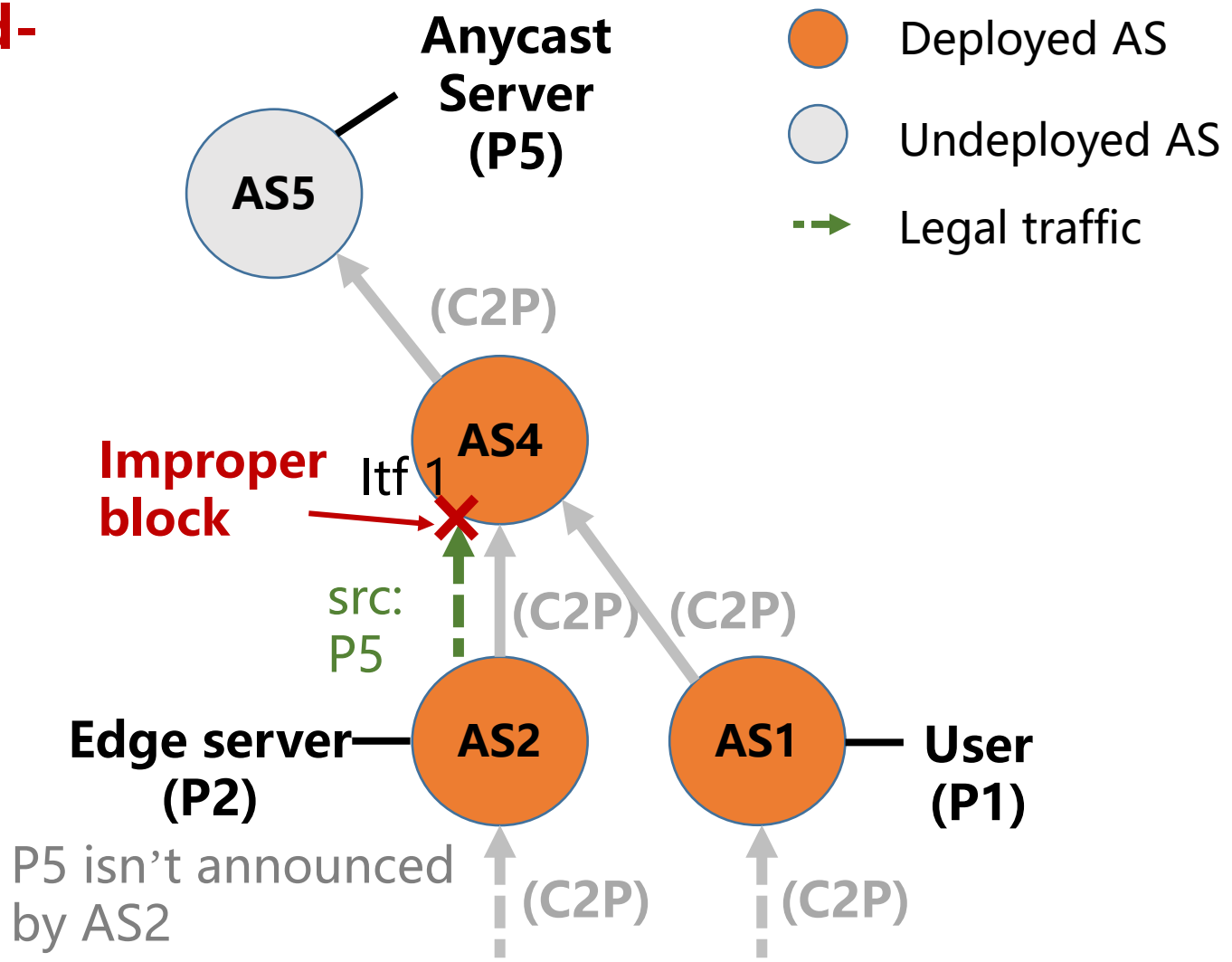
Scenario 3: NO_EXPORT in BGP Advertisement

Gap #2: Improper Block

- **Scenario 4: Anycast/Edge Hybrid--Direct Server Return (DSR)**
  - Request path: AS1->AS4->AS5
  - Tunnel path: AS5->AS4->AS2
  - Response path: AS2->AS4->AS1

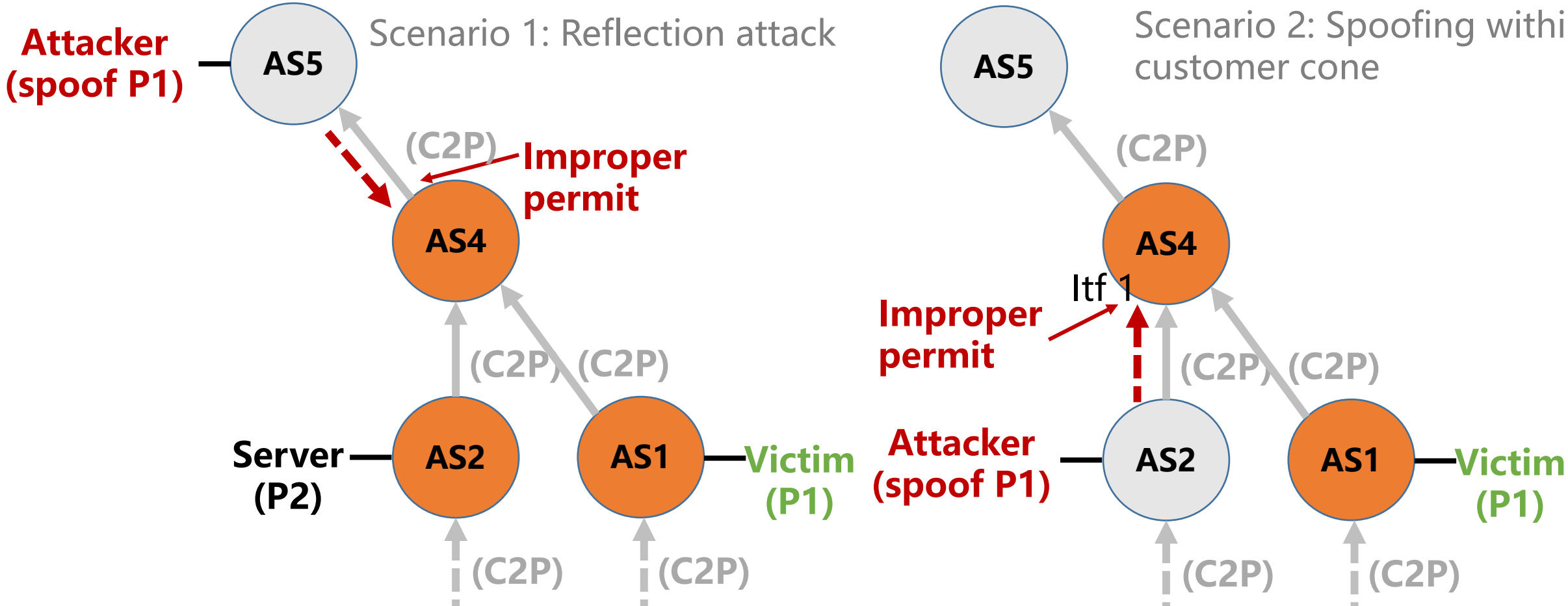
Behavior

- If AS4 runs EFP-uRPF Algorithm A
  - **Improper block** at Itf 1
- If AS4 runs EFP-uRPF Algorithm B
  - **Improper block** at Itf 1



Gap #3: Misaligned Incentive

Behavior: Though AS1 (victim) and AS4 (victim's provider) deploy uRPF, the **attacks succeed**



Outline

- Background
- Gap Analysis
- Problem Statement
- Requirement
- Preliminary Idea

Problem Statement

- Problem #1: Inaccurate validation
  - Behavior gap: improper block or improper permit
  - Reason: conducting SAV based on local RIB which may not match the real data-plane forwarding path from the source
- Problem #2: Misaligned incentive
  - Behavior gap: suffering reflection attack even when SAV mechanisms have been deployed by victim
  - Reason: victim with SAV deployment does not participate in protecting its source addresses from being forged

Outline

- Background
- Gap Analysis
- Problem Statement
- Requirement
- Preliminary Idea

Requirements for New Inter-domain SAV

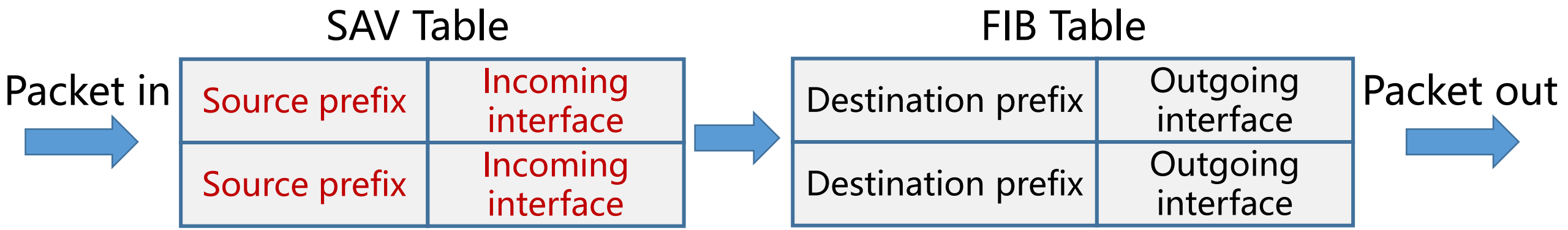
- Requirement #1: SAV mechanisms should discover the real data-plane forwarding path among routers
  - Avoids improper block and reduces improper permit as much as possible
- Requirement #2: SAV mechanisms should provide direct incentives
  - Helps the deployed area mitigate reflection attacks from undeployed area
  - Supports incremental deployment
- Requirement #3: SAV mechanisms should not induce much overhead
  - Avoid data-plane packet modification
  - Limit the number of control-plane protocol messages

Outline

- Background
- Gap Analysis
- Problem Statement
- Requirement
- Preliminary Idea

Preliminary Idea

- SAV table generation
  - Discovering the real data-plane forwarding path among ASes via hop-by-hop prefix notification, and generating SAV tables in routers along the path
    - Each router learns the real incoming interfaces for source addresses of the deployed area
- Data-plane SAV
  - Validating packets received from all directions (provider/peer/customer interfaces) based on local SAV table
  - Protecting source addresses of deployed area from being forged

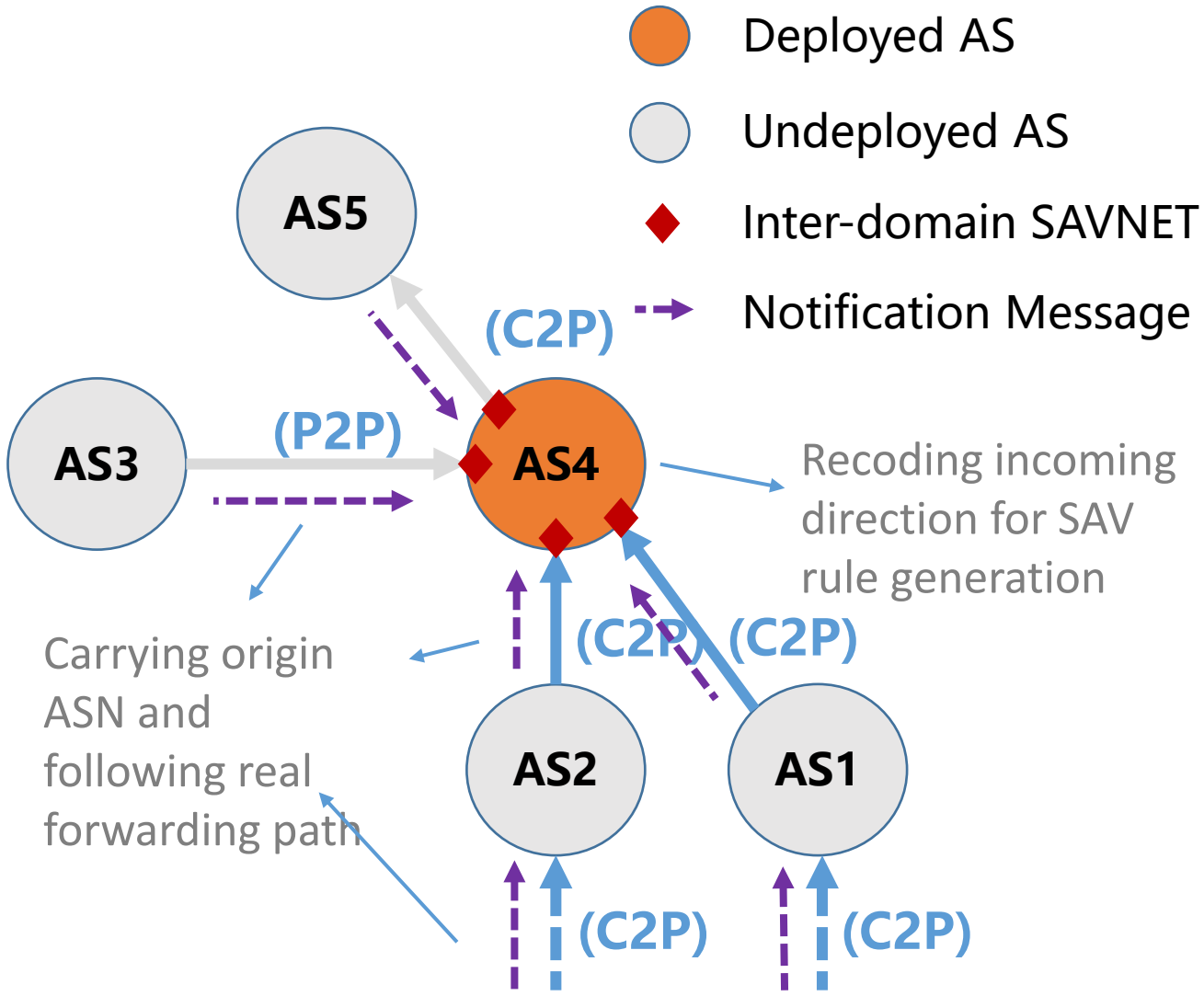


Thanks!

Backup slides

Preliminary Idea: Inter-domain SAVNET

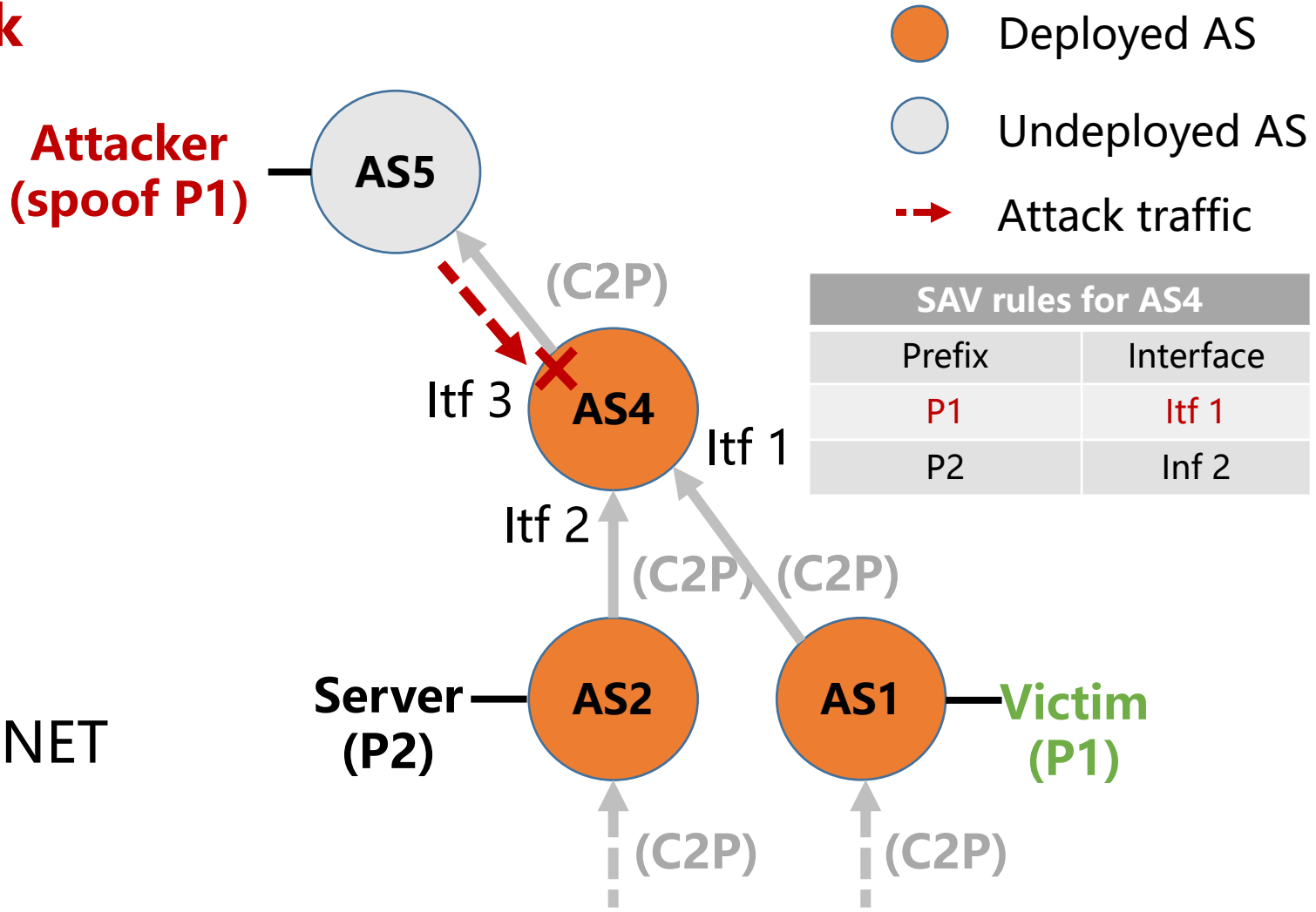
- SAV table generation
  - Each AS notifies its originated prefixes (or represented by ASN) to neighbor ASes based on local AS-path information
  - When receiving a notification message, AS generates SAV rules for the initial AS and continues the notification process to corresponding neighbors, following AS-path information
- Data-plane SAV
  - Validating traffic from both downstream and upstream based on local SAV table



Inter-domain SAVNET: Accurate Validation

Scenario 1: Reflection attack

- Attacker: AS5
- Reflective server: AS2
- Victim: AS1



Scenario 1: Reflection attack

Behavior

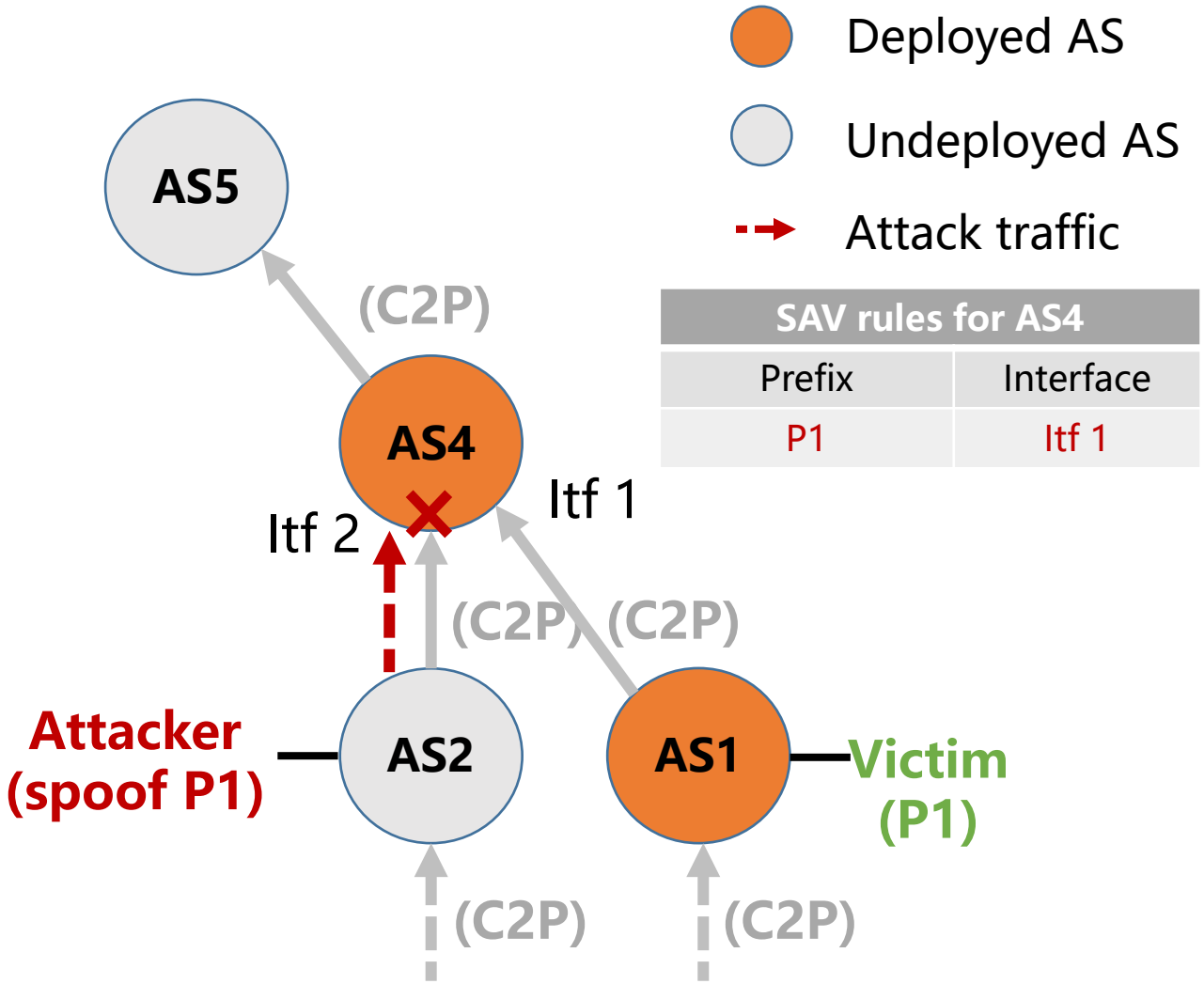
- If AS4 runs loose/EFP uRPF
  - **Improper permit**
- If AS4 runs inter-domain SAVNET
  - **Work best**

Inter-domain SAVNET: Accurate Validation

Scenario 2: Spoofing within the customer cone

Behavior

- If AS4 runs EFP-uRPF Algorithm A
  - ◆No problem
- If AS4 runs EFP-uRPF Algorithm B
  - ◆**Improper permit**
- If AS4 runs inter-domain SAVNET
  - ◆No problem



Scenario 2: Spoofing within a customer cone

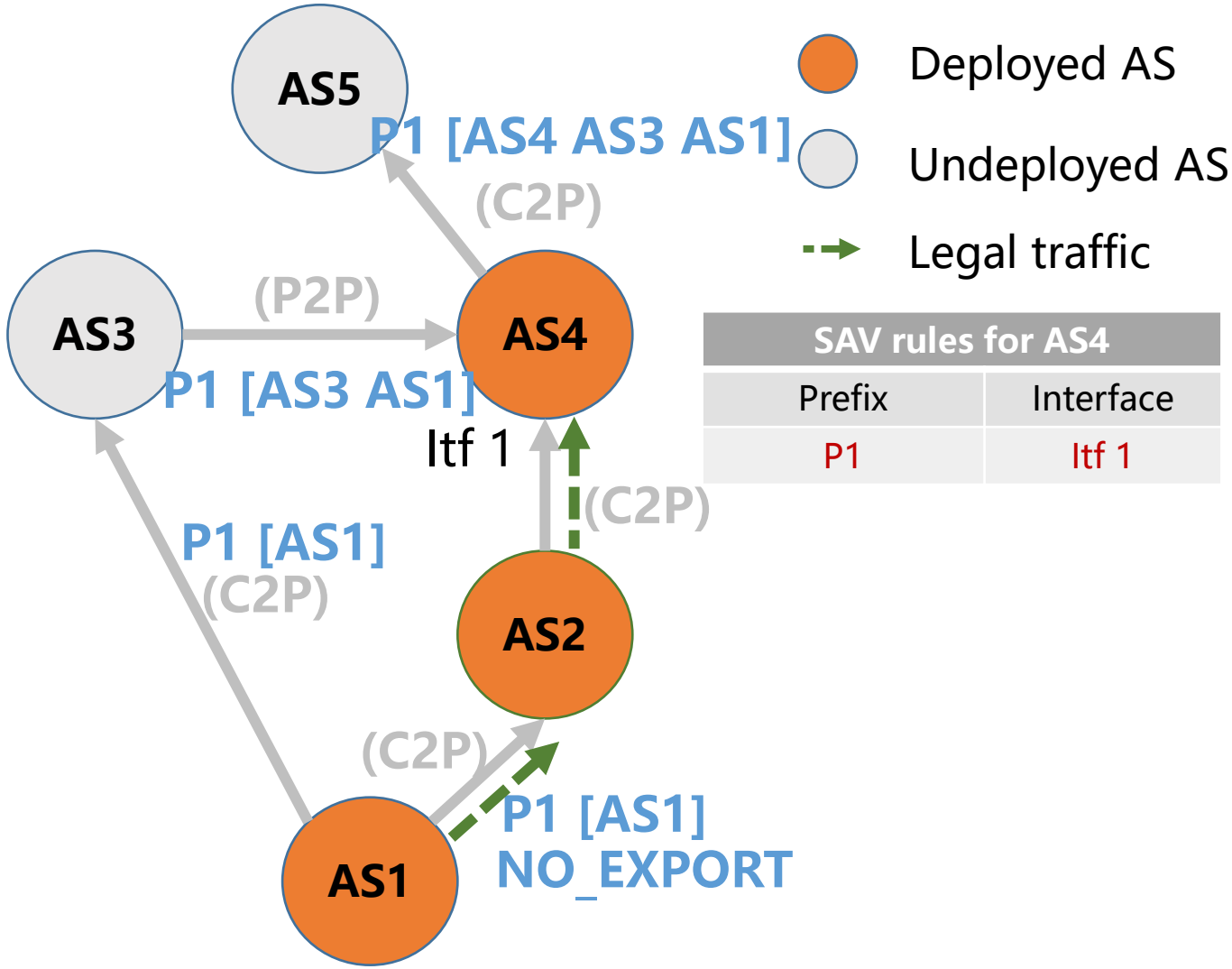
Inter-domain SAVNET: Accurate Validation

Scenario 3: NO_EXPORT in BGP Advertisement

- Forwarding path from AS1 to AS4: AS1->AS2->AS4

Behavior

- If AS4 runs EFP-uRPF
  - **Improper block**
- If AS4 runs inter-domain SAVNET
  - **Work best**



Scenario 3: NO_EXPORT in BGP Advertisement

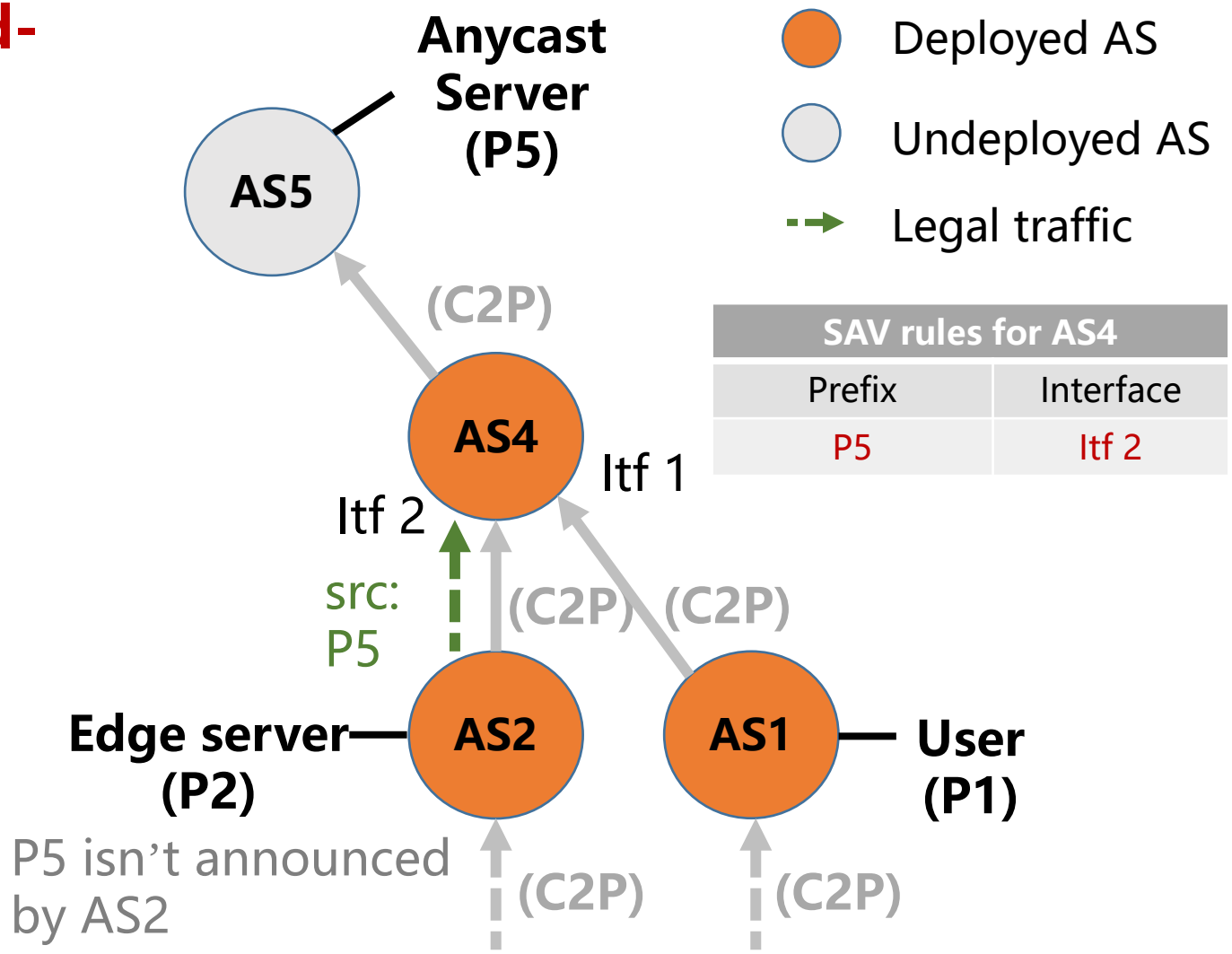
Inter-domain SAVNET: Accurate Validation

Scenario 4: Anycast/Edge Hybrid--Direct Server Return (DSR)

- Request path: AS1->AS4->AS5
- Tunnel path: AS5->AS4->AS2
- Response path: AS2->AS4->AS1

Behavior

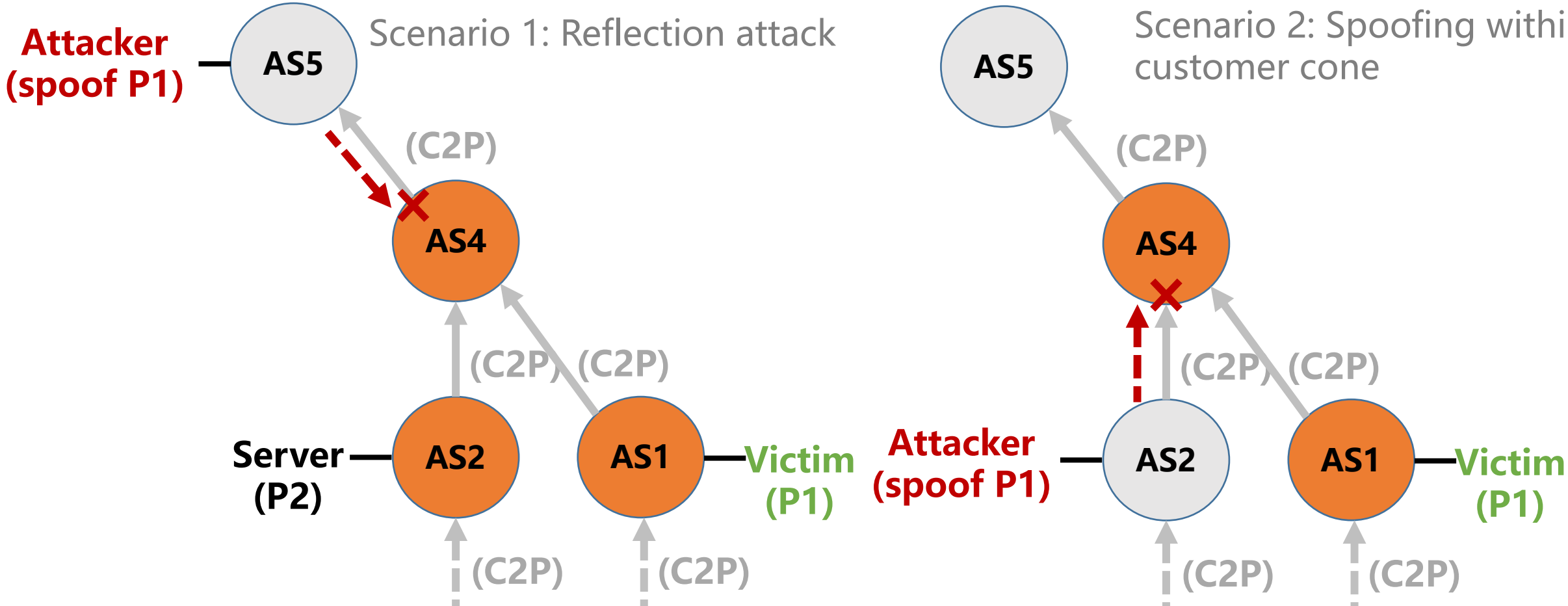
- If AS4 runs EFP-uRPF
  - **Improper block**
- If AS4 runs inter-domain SAVNET
  - **Work best**



Scenario 4: Direct Server Return (DSR)

Inter-domain SAVNET: Aligned Incentive

Behavior: Inter-domain SAVNET protects the source addresses of deployed AS from be forged



Inter-domain SAVNET: Features

- [Correctness:] Routers' SAV tables follow the real forwarding path in the data plane
  - Ensure correct validation even with asymmetric routing
- [Comprehensiveness:] Each AS validates traffic from both downstream and upstream based on local SAV tables
  - If prefixes are not learned in the SAV table, the incoming packet is permitted
  - If prefixes are learned in the SAV table but incoming interface of a packet does not match, the packet is blocked
- [Incentive:] Source prefixes of deployed ASes are protected by all deployed ASes
  - Traffic forging these source prefixes can be blocked as close to the traffic source as possible
  - Mitigate reflective DDoS attack targeting at these source prefixes
- [Cost:] Control-plane protocol extension, without data-plane packet modification
  - BGP is extended to carry the necessary information to build the SAV tables in routers