

Intra-domain Source Address Validation (SAVNET) Architecture

Presenter: Lancheng Qin

Nov, 2025

WG Discussions Related to SAV Deployment Locations

❑ Deploy SAV at internal interfaces to mitigate source address spoofing by compromised intra-domain routers?

◆ Most WG participants (e.g., Lancheng Qin, Ron Bonica, Tony Li, Mingqing Huang) believe that **problems caused by compromised routers are beyond the scope**

- https://mailarchive.ietf.org/arch/msg/savnet/EzCNyO89I54V0-MZoTnwUpW_WII/
- https://mailarchive.ietf.org/arch/msg/savnet/ZFj4Cj_vQ41FYPsfRVuY5x9KRIA/
- <https://mailarchive.ietf.org/arch/msg/savnet/iLYbsljgbGy1DABR2BEaLyonqco/>
- <https://mailarchive.ietf.org/arch/msg/savnet/i4uzXT17r7Np-qrrfUbDr-ZiPwU/>

❑ Intra-domain SAV deployment locations

◆ The clear conclusion (i.e. WG rough consensus) is that the WG chooses to **focus on edge deployments (i.e., SAV at external interfaces)**

- https://mailarchive.ietf.org/arch/msg/savnet/jGeQ-JMdhT_GvZmVk4pZy0ZMhds/
- https://mailarchive.ietf.org/arch/msg/savnet/KnJG_HY44R4k8VFg-4Y1UhjHmD0/

Main Updates

❑ Added Section 3 (Threat Model)

- ◆ Clearly defines the threat model of intra-domain source address spoofing and specifies the security objectives of intra-domain SAVNET

❑ Added Section 4 (Deployment Scope and Use Cases)

- ◆ Describes the deployment scope of intra-domain SAVNET and presents representative use cases to illustrate where and how the architecture applies

3. Threat Model

4. Deployment Scope and Use Cases

4.1. Use Case 1: Intra-domain SAVNET at External Interfaces Facing Hosts or Non-BGP Customer Networks

4.2. Use Case 2: Intra-domain SAVNET at External Interfaces Facing External ASes

Threat Model

□ Attacker

- ◆ Directly connected hosts
- ◆ Non-BGP customer networks
- ◆ External ASes

□ Attacker Capabilities

- ◆ Attackers may inject packets with spoofed source addresses into the domain, specifically
 - At external interfaces facing hosts or non-BGP customer networks, attackers may attempt to send **packets with source addresses they are not authorized to use**
 - At external interfaces facing external ASes, attackers may attempt to send packets using **internal-use-only source addresses**

□ Assumptions

- ◆ Intra-domain routers are trusted and operate correctly
- ◆ Spoofing traffic originating from a **compromised intra-domain router is out of scope**

Deployment Scope and Use Cases

□ Use Case 1: Intra-domain SAVNET at External Interfaces Facing Hosts or Non-BGP Customer Networks

- ◆ At external interfaces facing directly connected hosts or non-BGP customer networks, intra-domain SAVNET prevents these entities from injecting packets into the domain with source addresses they are not authorized to use

□ Use Case 2: Intra-domain SAVNET at External Interfaces Facing External ASes

- ◆ At external interfaces facing external ASes, intra-domain SAVNET prevents those ASes from injecting packets into the domain that use internal-use-only source addresses

Thanks