Network Working Group
Internet Draft
Intended status: Informational
Expires: August 15, 2025

W. Cheng
China Mobile
D. Li
Tsinghua University
C. Lin
New H3C Technologies
S. Yue
China Mobile

February 15, 2025

Intra-domain Source Address Validation (SAVNET) OAM
draft-cheng-savnet-intra-domain-oam-01

Abstract

This document is a framework for how Source Address Validation (SAVNET) can be applied to operations and maintenance procedures for Intra-domain network. The document is structured to outline how Operations and Management (OAM) functionality can be used to assist in fault, configuration, accounting, performance, and security management, commonly known by the acronym FCAPS.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on August 15, 2025.

Table of Contents

1. Introduction

The purpose of intra-domain SAV is to prevent outgoing data packets from an intra-domain subnet (e.g., a host network or a customer network) from forging source addresses of other intra-domain subnets or other ASes, and to prevent incoming data packets from external ASes from forging source addresses of the local AS. To achieve this, intra-domain SAV should focus on SAV on host-facing routers, customer-facing routers, and AS border routers (see [I-D.ietf-savnet-intra-domain-architecture]). Specifically, host-facing or customer-facing routers should block data packets from the connected host or customer network that contain a spoofed source IP address not belonging to that network. AS border routers should block data

packets from other ASes that contain a spoofed source IP address belonging to the local AS.

However, existing intra-domain SAV solutions (e.g., BCP38 [RFC2827] and BCP84 [RFC3704]) have issues like high operational overhead or inaccurate validation (see [I-D.ietf-savnet-intra-domain-problem-statement]). ACL-based ingress filtering requires manual operations to configure and update the SAV rules, while uRPF-based solutions might improperly block legitimate data packets in scenarios of routing asymmetry. To address these issues and guide the design of new intra-domain SAV solutions, [I-D.ietf-savnet-intra-domain-architecture] proposes the architecture of intra-domain SAVNET and introduces the use of SAV-specific information in intra-domain networks.

Following the intra-domain SAVNET architecture, [I-D. draft-cheng-savnet-intra-domain-sav-igp] and [I-D. draft-cheng-savnet-intra-domain-sav-bgp] propose an intra-domain SAV solution. Based on these intra-domain SAV solutions, this document provides a framework and requirements for Intra-domain SAVNET Operations, Administration, and Maintenance (OAM). The approach of this document is to outline the functionality, potential mechanisms to provide the functions, and the required applicability of intra-domain OAM functions.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Terminology

SAV Rule: The rule in a router that describes the mapping relationship between a source address (prefix) and the valid incoming interface(s). It is used by a router to make SAV decisions and is inferred from the SAV Information Base.

Host-facing Router: An intra-domain router of an AS which is connected to an intra-domain host network (i.e., a layer-2 network).
Customer-facing Router: An intra-domain router of an AS which is connected to an intra-domain customer network running the routing protocol (i.e., a layer-3 network).

3. Fault Management

3.1. Fault Detection

- Real-time Monitoring

  Network Monitoring Systems: Use protocols like SNMP, NetFlow, sFlow, etc., to monitor network traffic and device status in real-time, quickly identifying anomalies through monitoring data.

  Log Analysis: Automated log collection and analysis to detect abnormal logs or device error messages.

  Performance Monitoring: Monitor network performance metrics (such as latency, packet loss rate, jitter, etc.) to identify potential issues.

- Alert System

  Threshold Alerts: Set threshold values to automatically trigger alerts when performance metrics exceed preset ranges.

  Pattern Recognition: Detect abnormal traffic patterns or behaviors using machine learning and pattern recognition techniques.

- Automated Diagnostic Tools

  Self-check Tools: Use built-in self-check tools to perform regular checks on SAVNET configurations to detect configuration errors or inconsistencies.

  Fault Diagnostic System: Utilize intelligent fault diagnostic systems to quickly identify and locate faults.

- Routing Protocol Analysis

  IGP/BGP Status Monitoring: Monitor IGP/BGP protocol status changes to identify routing table anomalies.

  SAVNET Table Validation: Regularly validate SAV table entries to avoid faults caused by incorrect configurations.

3.2. Fault Isolation

- Interface Level

Disable Interface: If the fault comes from a specific network interface, you can temporarily disable that interface to prevent the spread of abnormal traffic.

Adjust Traffic Path: Modify the routing policy to reroute traffic around the faulty interface.

- Routing Level

Adjust Routing Table: Modify the IGP/BGP routing table to avoid routing traffic through the faulty node or path.

Withdraw Route Advertisements: Withdraw route advertisements for the faulty path in BGP, preventing other routers from forwarding traffic to the fault path.

- Device Level

Isolate Faulty Device: Temporarily isolate the faulty device from the network and activate backup devices.

Device Restart: If the fault is due to a temporary issue with the device, try restarting the device to restore it to normal operation.

4. Operational and Manageability Considerations

4.1. OAM Configuration

Routers may be configured to enable intra-domain SAVNET functions via the device Command Line Interface (CLI) or through one of the defined management protocols, such as the Network Configuration Protocol (NETCONF) [RFC6241]. The following is a non-exhaustive list of configuration parameters that apply to Intra-domain SAVNET.

4.1.1. Base Parameters

- Global Configuration

Enable SAVNET function.

SAV mode, SAV table capacity, SAV sources priority.

- Interface Configuration

Control for SAVNET (function enable/disable), SAV mode.

4.1.2. Static SAV Parameters

- Static SAV rules configuration in the SAV table.

  SAV entries: "Source prefix" and "Incoming interface," including IPv4 and IPv6 SAV rules.

- Capacity of the SAV table and upper limitation of IPv4 or IPv6 SAV rules.

4.1.3. IGP SAV Parameters

- Enable SAVNET function under address families in the IGP.

- Enable the IGP to calculate SAVNET interfaces.

- IGP control to advertise SAVNET source address filtering function.

- IGP control to filter SAVNET table entry generation.

4.1.4. BGP SAV Parameters

- Enable BGP prefix iteration function.

- BGP control to advertise SAVNET source address filtering function.

- BGP control to filter SAVNET table entry generation.

4.2. OAM Notifications

Intra-domain SAVNET OAM mechanisms should trigger notifications to alert operators to certain conditions. Such conditions include but are not limited to:

- Faults detected by proactive mechanisms.

- Reception of event-driven defect indications.

- Logged security incidents pertaining to the OAM Message Channel.

- Protocol errors (for example, as caused by misconfiguration).

Notifications generated by OAM mechanisms may be via YANG, Syslog messages, or any other standard management protocol that supports asynchronous notifications.

5. Accounting

5.1. Requirements

For intra-domain SAVNET, the following statistical functionalities are required:

- Interface-based Statistics: Collect statistics at the interface level for traffic where the source address fails the intra-domain source address validation. Record the five-tuple information of the flows.

- Interface-based Statistics: Collect statistics at the interface level for traffic where the source address passes the intra-domain source address validation. Record the five-tuple information of the flows.

- Interface-based Statistics: Collect statistics at the interface level for traffic where the source address is not found in the intra-domain SAVNET table. Record the five-tuple information of the flows.

- Per Intra-domain SAVNET Table Entry Statistics: Collect statistics for each table entry on the number of passes and drops, recording the five-tuple information of the flows.

- Global Statistics: Collect global statistics for intra-domain source address checks, including the number of passes, drops, lookups not found, and blacklist hits. This aids in overall operational management.

- Blacklist Statistics: Collect statistics for traffic where the source address hits the blacklist. Record the five-tuple information of the flows.

5.2. Location of Accounting

For host-facing or customer-facing routers, interface-level statistics should be monitored. For intra-domain boundary routers, blacklist statistics are the focus. Other table-based statistics and global statistics should be monitored on all intra-domain routers.

6. Performance Management

Performance management allows the measurement of the information transfer characteristics of Intra-domain SAVNET, which can then be compared against an SLA. This falls into two categories: latency (including jitter as a variation in latency) and information loss.

Perform performance measurements for traffic from different sources:

- Traffic coming from host-facing or customer-facing routers.

- Traffic entering the intra-domain from outside the intra-domain.

- Traffic leaving the intra-domain.

- Traffic within the intra-domain.

The goal is to monitor performance characteristics when the intra-domain SAVNET function is enabled. The network operator can extract performance monitoring metrics based on whether one-way or two-way performance monitoring functions are performed:

- For one-way performance monitoring functions, the metrics will be available at the target router.

- For two-way performance monitoring functions, all metrics will be available at the source router, while a subset will be available at the target router. Specifically, metrics for both the direction from source to target and from target to source will be available at the source router. Metrics for the direction from source to target will be available at the target router.

7. Security Management

TBD

8. Security Considerations

This document describes a framework for Intra-domain SAVNET Operations and Management. It does not introduce any new security concerns.

The security considerations described in

[I-D.ietf-savnet-intra-domain-problem-statement] and

[I-D.ietf-savnet-intra-domain-architecture] also applies to this document.

9. References

9.1. Normative References

[I-D.ietf-savnet-intra-domain-problem-statement] Li, D., Wu, J., Qin, L., Huang, M., and N. Geng, "Source Address Validation in Intra-domain Networks Gap Analysis,Problem Statement, and Requirements", Work in Progress,Internet-Draft, draft-ietf-savnet-intra-domain-problem-statement-03, 13 February 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-intra-domain-problem-statement-03>.

[I-D.ietf-savnet-intra-domain-architecture]Li, D., Wu, J., Qin, L., Geng, N., and L. Chen, "Intra-domain Source Address Validation (SAVNET) Architecture",Work in Progress, Internet-Draft, draft-ietf-savnet-intra-domain-architecture-00, 12 April 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-intra-domain-architecture-00>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

9.2. Informative References

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, DOI 10.17487/RFC2827, May 2000, <https://www.rfc-editor.org/info/rfc2827>.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, DOI 10.17487/RFC3704, March 2004, <https://www.rfc-editor.org/info/rfc3704>.

Authors' Addresses

Weiqiang Cheng
China Mobile
China
Email: chengweiqiang@chinamobile.com

Dan Li
Tsinghua University
Beijing
China
Email: tolidan@tsinghua.edu.cn

Changwang Lin
New H3C Technologies
China
Email: linchangwang.04414@h3c.com

Shengnan Yue
China Mobile
China
yueshengnan@chinamobile.com