Network Working Group
Internet Draft
Intended status: Informational
Expires: October 24, 2025

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

April 24, 2025

Inter-domain Source Address Validation (SAVNET) OAM
draft-cheng-savnet-inter-domain-oam-01

Abstract

This document is a framework for how Source Address Validation (SAVNET) can be applied to operations and maintenance procedures for Inter-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 October 24, 2025.

Table of Contents

1. Introduction

Source address spoofing is one of the most serious security threats to today's Internet. It serves as a main attack vector for large-

scale Distributed Denial of Service (DDoS) attacks and is commonly used in reflective DDoS attacks. To mitigate source address spoofing, many source address validation (SAV) solutions (e.g., BCP38 [RFC2827] and BCP84 [RFC3704] [RFC8704]) have been proposed. The primary design goal of SAV solutions is avoiding improper block (i.e., blocking legitimate traffic) while maintaining directionality, especially in partial deployment scenarios (see [I-D.ietf-savnet-inter-domain-problem-statement] and [RFC8704]).

To address these issues and guide the design of new inter-domain SAV solutions, [I-D.draft-wu-savnet-inter-domain-architecture] proposes the architecture of inter-domain SAVNET and introduces the use of SAV-specific information in inter-domain networks.

Based on the architecture of inter-domain SAVNET, this document provides a framework and requirements for Inter-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 inter-domain OAM functions.

2. 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.

3. Overview

This document primarily explores the functions that SAV Inter-domain OAM needs to accomplish. As shown in the architecture of Figure 1, the following OAM tasks need to be addressed:

OAM1: Configure for different data sources, including RPKI, Local Routing, IRR Data, BGP Update, and SAV-Specific.

OAM2: Based on the source information from the different data sources in OAM1, provide the functionality to view source information by AS number.

OAM3: Based on the source information from different origins, optimize to generate SAV Rules, and maintain Permit Rules and Block Rules.

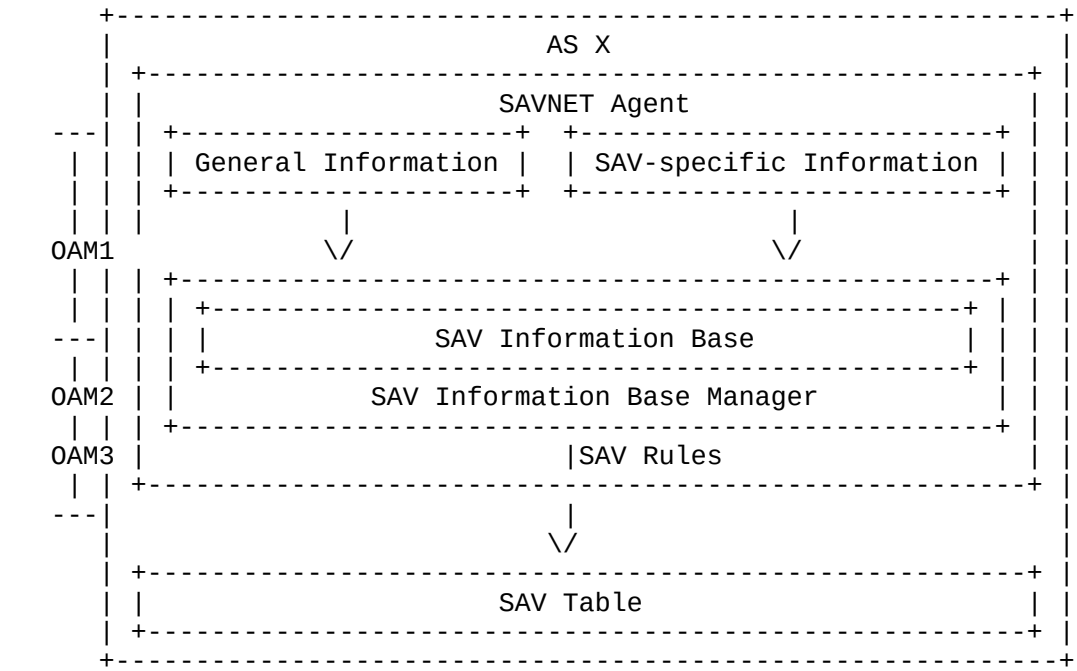

Figure 1

4. Terminology

* ROA: Route Origin Authorization

* ASPA: Autonomous System Provider Authorizations

* IRR: Internet Routing Registry

* Refer to the terms defined in Section 2 of [I-D.draft-wu-savnet-inter-domain-architecture]

5. Fault Management

5.1. 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

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

RPKI Status Monitoring: Monitor BPKI protocol status changes to identify RPKI ROA RPKI ASPA anomalies.

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

5.2. 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 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.

6. Operational and Manageability Considerations

6.1. OAM1: Source information from different origins

For each type of source information, it is necessary to configure whether it is supported. and set the priority for processing this source. Generally, SAV-specific has the highest priority, followed by RPKI ROA Obj. and ASPA Obj, then Local Routing, and finally IRR Data.

6.1.1. Configuration for RPKI

- Enable

Enable the function to obtain prefix origin information via RPKI.

- Priority

The usage priority of prefix origin information obtained through RPKI.

- Capacity

Maximum capacity for prefix origin information via RPKI.

- Cache time

For source information of RPKI, its cache time

6.1.2. Configuration for source information from Local Routing

- Enable

Enable the function to obtain prefix origin information via Local Routing.

- Priority

The usage priority of prefix origin information obtained through Local Routing.

- Capacity

Maximum capacity for prefix origin information via Local Routing.

- Cache time

For source information of Local Routing, its cache time

6.1.3. Configuration for source information IRR Data

- Enable

Enable the function to obtain prefix origin information via IRR Data.

- Priority

The usage priority of prefix origin information obtained through IRR Data.

- Capacity

Maximum capacity for prefix origin information via IRR Data.

- Cache time

For source information of IRR Data, its cache time

6.1.4. Configuration for source information from BGP Update

- Enable

Enable the function to obtain prefix origin information via BGP Update.

- Priority

The usage priority of prefix origin information obtained through BGP Update.

- Capacity

Maximum capacity for prefix origin information via BGP Update.

- Cache time

For source information of BGP Update, its cache time

6.1.5. Configuration for source information from specific

- Enable

Enable the function to obtain prefix origin information via SAV-specific.

- Priority

The usage priority of prefix origin information obtained through SAV-specific.

- Capacity

Maximum capacity for prefix origin information via SAV-specific.

- Cache time

For source information of SAV-specific, its cache time

6.1.6. Notification for Source information

The maximum number of supported information entries for each type of Source Information.

- When cache count exceeds specifications, a notification needs to be sent

- Faults detected by proactive mechanisms.

- Logged security incidents pertaining to the OAM Message Channel.

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

6.1.7. Count for Source information

- Source Information entry Count by type

Count the SAV Source information by source type.

- Source Information entry modify count

Count of Source Information Table Entries Added/Deleted/Modified

6.2. OAM2: SAV Information Base Manager

You can view source information based on prefixes, different source types, and source AS. Each data source’s information corresponds to a different priority level

6.2.1. Organization of Base Manager

- Organization source information Based on Source AS.

- Organization source information based on prefix

- Maintain the inbound AS list and inbound interface list for table entries.

6.2.2. Notification for Base Manager

- Faults detected by proactive mechanisms.

- Logged security incidents pertaining to the OAM Message Channel.

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

6.2.3. Count for Base Manager

- Global Count

Count the SAV Source information by type.

Count the SAV Source information by Source AS.

- Count of Source Information entry modified

Count of Base Manager Entries Added/Deleted/Modified

6.3. OAM3: SAV Rules

6.3.1. Count for SAV Rules

- Global Count

Count the SAV Source information by type.

Count the SAV Source information by Source AS.

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

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

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

- Per Inter-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 inter-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.

- Count of SAV Rule modified

Count of SAV Rule Added/Deleted/Modified

6.3.2. Permit Rules and Block Rules

Based on the actions after matching SAV table entries, there are Permit Rules and Block Rules. The Permit Rule allows traffic matching the prefix and inbound interface entry to pass through, while the Block Rule prevents traffic matching the prefix and inbound interface entry from passing through.

The Permit Rule is used when the inbound interface of the address is precisely known. The Block Rule is applied when the source address is known from some inbound interfaces, with others uncertain, ensuring that the source address does not arrive from specific interfaces where the Block Rule is generated.

6.3.3. Performance

Performance management allows the measurement of the information transfer characteristics of Inter-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 entering the inter-domain from outside the inter-domain.

- Traffic leaving the inter-domain.

- Traffic within the inter-domain.

- Memory occupied by record entries

- Time Spent on Calculating Table Items

The goal is to monitor performance characteristics when the inter-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.

6.4. Security Management

TBD

7. Security Considerations

The security considerations described in [I-D.draft-wu-savnet-inter-domain-architecture] also applies to this document.

8. IANA Considerations

TBD

9. References

9.1. Normative References

[RFC8704] Sriram, K., Montgomery, D., and J. Haas, "Enhanced Feasible-Path Unicast Reverse Path Forwarding", BCP 84, RFC 8704, DOI 10.17487/RFC8704, February 2020, <https://www.rfc-editor.org/info/rfc8704>.

[ietf-savnet-inter-domain-problem-statement] "Source Address Validation in Inter-domain Networks Gap Analysis, Problem Statement, and Requirements", 2024, <https://datatracker.ietf.org/doc/draft-ietf-savnet-inter-domain-problem-statement/>.

[draft-wu-savnet-inter-domain-architecture] D. Li, J. Wu, Tsinghua University, M. Huang, L. Chen, Zhongguancun Laboratory, N. Geng, Huawei, L. Liu, Zhongguancun Laboratory, "Inter-domain Source Address Validation (SAVNET) Architecture", draft-wu-savnet-inter-domain-architecture-11, DOI 10.17487/draft-wu-savnet-inter-domain-architecture-11.txt, February 2025, <https://datatracker.ietf.org/doc/draft-wu-savnet-inter-domain-architecture>.

[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. Informational 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