opsawg
Internet-Draft
Intended status: Standards Track
Expires: 26 April 2026

Q. Cao
M. Huang
Zhongguancun Laboratory
B. Claise
Everything OPS
T. Zhou
Huawei

23 October 2025

Export of Source Address Validation (SAV) Information in IPFIX
draft-cao-opsawg-ipfix-sav-00

Abstract

This document specifies the IP Flow Information Export Information Elements to export the context and outcome of Source Address Validation enforcement data. These SAV-specific Information Elements provide detailed insight into why packets are identified as spoofed by capturing the specific SAV rules that triggered validation decisions. This operational visibility is essential for network operators to verify SAV effectiveness, audit rule correctness, and analyze source address spoofing events.

Table of Contents

1. Introduction

Source Address Validation (SAV) serves as a fundamental defense mechanism against IP source address spoofing. Despite its critical role in network security, current SAV implementations lack operational visibility, making it difficult to answer essential operational questions:

* How many packets are identified as spoofed and dropped by SAV?

* Which interfaces receive spoofed packets and which source prefixes are targeted?

* Which specific SAV rules trigger the enforcement actions?

* Are SAV rules functioning as intended or potentially misconfigured?

This document introduces a set of SAV-specific IP Flow Information Export (IPFIX) Information Elements (IEs) that enable detailed reporting of Source Address Validation enforcement actions. These elements align with the SAV concepts and operational models defined in [I-D.ietf-savnet-general-sav-capabilities], and provide traffic observations that can be operationally correlated with the SAV configuration and state information available via the YANG data model [I-D.li-savnet-sav-yang].

2. Terminology

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.

This document makes use of the terms defined in [RFC7011], and [I-D.ietf-savnet-general-sav-capabilities].

The following terms are used as defined in [RFC7011]:

* IPFIX

* IPFIX Information Elements

* Template

* Template Record

* Data Record

* Data Set

* Exporter

* Collector

The following terms are used as defined in [I-D.ietf-savnet-general-sav-capabilities]

* SAV rule

* Validation mode

3. SAV Overview and IPFIX Export Requirements

This section outlines the operational requirements for SAV telemetry export using IPFIX, based on the generalized SAV architectural framework defined in [I-D.ietf-savnet-general-sav-capabilities].

The SAV framework establishes four canonical validation modes that model validation policies:

* *Interface-based prefix allowlist (Mode 1):* Validates that a source prefix is explicitly permitted on the incoming interface.

* *Interface-based prefix blocklist (Mode 2):* Validates that a source prefix is not explicitly blocked on the incoming interface.

* *Prefix-based interface allowlist (Mode 3):* Validates that a packet is received on an interface explicitly permitted for its source prefix.

* *Prefix-based interface blocklist (Mode 4):* Validates that a packet is not received on an interface explicitly blocked for its source prefix.

These modes can be applied independently or in combination on a router, following a defined validation procedure (Section 2 of [I-D.ietf-savnet-general-sav-capabilities]). Furthermore, when identifying a packet as spoofed, a range of traffic handling policies (e.g. discard, rate-limit, redirect) can be applied.

However, the generalized SAV model requires corresponding operational visibility capabilities. Without integrated telemetry, operators face significant challenges in:

* Operational Verification: Confirming SAV is actively and correctly enforcing policies

* Root-Cause Analysis: Determining why specific packets were deemed invalid

* Threat Intelligence: Quantifying spoofing attempts and analyzing attack patterns

To address these limitations, IPFIX [RFC7011] and [RFC7012] provides a vendor-neutral protocol for SAV telemetry. The exported data must provide insight into:

* The validation outcome and specific reason for the decision

* The identity and type of SAV rule or rule set that influenced the decision

* The configured rule content that was evaluated during validation

* The enforcement action applied to spoofed packets

The following section defines the IPFIX IEs that meet these requirements.

4. IPFIX SAV Information Elements

This section defines the IEs used for SAV telemetry. These IEs have been specified in accordance with the guidelines in [RFC7013].

4.1. Design Rationale

The SAV IPFIX IEs are designed to provide detailed visibility into SAV enforcement actions, enabling network operators and automation systems to monitor and troubleshoot SAV operations effectively. The design follows these principles:

* *Scope*. The SAV-specific IEs are used to report the outcome and context of SAV processing for data plane traffic observations. Interface, device or network-level SAV configuration is out of scope for these IEs and is covered by the SAVNET YANG data model.

* *Conceptual Alignment*. The elements align with the validation modes and rule types defined in [I-D.ietf-savnet-general-sav-capabilities], ensuring consistency with the architectural SAV concepts.

* *Semantic Correlation*. The IPFIX encoding preserves the semantic relationships defined in [I-D.li-savnet-sav-yang], which enables correlation between IPFIX Data Record in data-plane and YANG configuration/state data in control-plane comprehensive analysis.

* *Structured Encoding*. The savMatchedContentList is encoded as a subTemplateList to represent the multi-field tuples of SAV rules. The structure of subTemplateList was chosen because it can encapsulate heterogeneous fields (e.g., prefix, length, interface) within a single list element. The list semantics (allOf, exactlyOneOf) directly encode the SAV validation logic (e.g., matching all rules in an allowlist vs. exactly one in a blocklist) into the data structure.

4.2. savRuleType (unsigned8)

The savRuleType element classifies the rule as either an allowlist or a blocklist. The values correspond to the check type concepts in the SAV architecture:

* A value of 0 (allowlist) indicates the packet was validated against an allowlist.

* A value of 1 (blocklist) indicates the packet was validated against a blocklist.

4.3. savTargetType (unsigned8)

The savTargetType element specifies the lookup key used by the SAV rule. It may be used in conjunction with savRuleType to fully define the validation mode applied.

* A value of 0 (interface-based) indicates the rule is indexed by an interface (e.g., "on interface X, what prefixes are allowed/ blocked?").

* A value of 1 (prefix-based) indicates the rule is indexed by a source prefix (e.g., "for prefix Y, which interfaces are allowed/ blocked?").

4.4. savMatchedContentList (subTemplateList)

The savMatchedContentList element carries the content of the rules that were relevant to the validation decision, encoded as a subTemplateList according to [RFC6313]. Each element in the list represents a complete SAV rule tuple. The content and semantics of the list are defined by the savRuleType:

* *For Allowlist non-matches (savRuleType=0)*: The savMatchedContentList consists of the set of all rule tuples from the consulted SAV allowlist at the time of the packet's processing. The subTemplateList semantic SHOULD be allOf (0x03), indicating that the packet was validated against all these rules and did not match any of them.

* *For Blocklist matches (savRuleType=1)*: The savMatchedContentList contains the first rule tuple that matched the packet from the SAV blocklist. The subTemplateList semantic SHOULD be exactlyOneOf (0x01), indicating that the packet matched this specific rule.

Semantic Interpretation of Standard Information Elements: When standard IPFIX IEs (such as ingressInterface, sourceIPv4Prefix,sourceIPv4PrefixLength or their IPv6 equivalents) are used within the subTemplateList of savMatchedContentList, they represent values from the SAV rule configuration, rather than from the actual packet being validated. This contextual distinction is critical for correct interpretation:

* *In the parent Data Record*: These IEs describe attributes of the actual spoofed packets that were validated by SAV.

* *Within savMatchedContentList*: These same IEs describe the configured SAV rule parameters that were evaluated during validation.

This approach ensures clear semantic distinction by reusing existing IEs, without requiring definition of new elements for SAV rule parameters.

4.5. savPolicyAction (unsigned8)

The savPolicyAction indicates the action applied to packets identified as spoofed. The action taken is a matter of local policy. This element reports the outcome.

5. Use Cases

The SAV-specific IPFIX IEs defined in this document enable network operators to answer critical operational questions that are currently unaddressable without telemetry for SAV:

SAV Effectiveness Monitoring: Use savRuleType (TBD1), savTargetType (TBD2), savPolicyAction (TBD4) and standard IPFIX counters, to quantify spoofing attempt volumes, analyze their distribution across different validation modes, and identify applied enforcement actions (discard, rate-limit, redirect) to spoofed traffic.

Rule-Level Attribution and Troubleshooting: UsesavMatchedContentList (TBD3) to determine the specific SAV rule configuration that triggered enforcement decisions , including the exact rule parameters (interfaces, prefixes) evaluated during validation, whether for allowlist failures or blocklist matches.

Forensic Analysis and Compliance: Correlate SAV Data Records with packet-level details using selectionSequenceId for incident investigation and gather evidence to support external trust initiatives and regulatory compliance reporting.

6. Operational Considerations

While this document defines new IPFIX IEs using standard IPFIX mechanisms, implementors should consider:

* *Exporter Implementation:* Exporters MUST properly encode the subTemplateList structure for savMatchedContentList and ensure semantic consistency between savRuleType and list contents. Exporters MUST also define the sub-templates (e.g., 901-904) used in savMatchedContentList prior to exporting Data Records that use them.

* *Collector Processing:* Collectors MUST be capable of parsing subTemplateList structure and understanding the context-dependent semantics of standard IEs within savMatchedContentList. Collectors MUST associate the sub-templates with the main template for correct interpretation.

7. Open Issues

The mappings between the SAV YANG data model and IPFIX IEs are considered based on the common foundation of the general SAV capabilities document [I-D.ietf-savnet-general-sav-capabilities]. The operational correlation is demonstrated in Table 1, which defines the values for the designed IEs mapped from the corresponding [I-D.li-savnet-sav-yang] SAV Management YANG Module.

YANG Elements	IPFIX IEs
sav-check-type sav:sav-allow-list sav:sav-block-list	savRuleType 0 (allowlist) 1 (blocklist)
sav-mode sav:sav-im sav:sav-cm	savTargetType 0 (interface-based) 1 (prefix-based)
SAV Rules attributes source-prefix incoming-interface	savMatchedContentList sourceIPv4Prefix/sourceIPv6Prefix ingressInterface

Table 1: Mappings between SAV YANG Data Model and IPFIX Information Elements

The savPolicyAction element carries real-time SAV decisions applied to spoofed packets. It does not directly map to YANG configuration node.

The code points for these IEs are maintained by IANA in the corresponding subregistries of the IPFIX registry. Future additions or changes are managed via Expert Review as described in IANA Considerations (Section 9).

8. Security Considerations

There are no additional security considerations regarding allocation of these new IPFIX IEs compared to [RFC7012]. Other security considerations described in [I-D.ietf-savnet-general-sav-capabilities] apply to this document.

9. IANA Considerations

This document requests IANA to create four new IEs under the "IPFIX Information Elements" registry [RFC7012] available at [IANA-IPFIX].

Element ID	Name
TBD1	savRuleType
TBD2	savTargetType
TBD3	savMatchedContentList
TBD4	savPolicyAction

9.1. savRuleType

* *ElementID*: TBD1
* *Name*: savRuleType
* *Abstract Data Type*: unsigned8
* *Data Type Semantics*: identifier
* *Description*: Identifies the validation rule type triggered during SAV enforcement.
* *Reference*: This document, savRuleType (Section 4.2)

9.2. savTargetType

* *ElementID*: TBD2
* *Name*: savTargetType
* *Abstract Data Type*: unsigned8
* *Data Type Semantics*: identifier
* *Description*: Specifies the entity type against which validation was performed.
* *Reference*: This document, savTargetType (Section 4.3)

9.3. savMatchedContentList

* *ElementID*: TBD3
* *Name*: savMatchedContentList
* *Abstract Data Type*: subTemplateList
* *Data Type Semantics*: list
* *Description*: The content of the SAV rules relevant to the validation decision.
* *Reference*: This document, savMatchedContentList (Section 4.4)

9.4. savPolicyAction

* *ElementID*: TBD4
* *Name*: savPolicyAction
* *Abstract Data Type*: unsigned8
* *Data Type Semantics*: identifier
* *Description*: Action applied to packets identified as spoofed.
* *Reference*: This document, savPolicyAction (Section 4.5)

Additionally, IANA is requested to create new subregistries under the IPFIX IEs registries. The subregistries contain values for the savRuleType, savTargetType and savPolicyAction IEs. The allocation policy is Expert Review [RFC8126]. Experts should consult the SAVNET architecture [I-D.ietf-savnet-general-sav-capabilities] to ensure new values are consistent with SAV validation concepts and operational models.

9.5. IPFIX savRuleType (TBD1) Subregistry

* *Reference*: [I-D.ietf-savnet-general-sav-capabilities], Section 2 (Validation Modes)
* *Allocation Policy*: Expert Review [RFC8126]
* *Expert Guidance*: Experts should ensure that new values are consistent with the SAV architecture concepts defined in [I-D.ietf-savnet-general-sav-capabilities], particularly the validation modes and rule types (allowlist or blocklist).

Initial values:

Value	Name	Description
0	allowlist	The packet was validated against an allowlist
1	blocklist	The packet was validated against an blocklist

9.6. IPFIX savTargetType (TBD2) Subregistry

* *Reference*: [I-D.ietf-savnet-general-sav-capabilities], Section 2 (Validation Modes)

* *Allocation Policy*: Expert Review [RFC8126]

* *Expert Guidance*: Experts should consult [I-D.ietf-savnet-general-sav-capabilities] to ensure new values align with the defined target types (interface-based or prefix-based).

Initial values:

Value	Name	Description
0	interface-based	The rule is indexed by an interface
1	prefix-based	The rule is indexed by a prefix

9.7. IPFIX savPolicyAction (TBD4) Subregistry

* *Reference*: [I-D.ietf-savnet-general-sav-capabilities], Section 4 (Traffic Handling Policies)

* *Allocation Policy*: Expert Review [RFC8126]

* *Expert Guidance*: Experts should ensure that new actions are consistent with the SAV traffic handling policies defined in [I-D.ietf-savnet-general-sav-capabilities].

Initial values:

Value	Name	Description
0	permit	The packet was allowed to proceed (monitoring only)
1	discard	Packet was discarded or dropped
2	rate-limit	Traffic was subjected to rate limiting
3	redirect	Packet was redirected to alternative destination
4-255	unassigned	Reserved for future assignment

10. References

10.1. Normative References

[I-D.li-savnet-sav-yang]
Li, D., Liu, L., Lin, C., Wu, J., Wu, T., and W. Cheng, "YANG Data Model for Intra-domain and Inter-domain Source Address Validation (SAVNET)", Work in Progress, Internet-Draft, draft-li-savnet-sav-yang-07, 9 October 2025, <https://datatracker.ietf.org/doc/html/draft-li-savnet-sav-yang-07>.

[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>.

[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>.

[RFC7011] Claise, B., Ed., Trammell, B., Ed., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, DOI 10.17487/RFC7011, September 2013, <https://www.rfc-editor.org/info/rfc7011>.

[RFC7012] Claise, B., Ed. and B. Trammell, Ed., "Information Model for IP Flow Information Export (IPFIX)", RFC 7012, DOI 10.17487/RFC7012, September 2013, <https://www.rfc-editor.org/info/rfc7012>.

[RFC7013] Trammell, B. and B. Claise, "Guidelines for Authors and Reviewers of IP Flow Information Export (IPFIX) Information Elements", BCP 184, RFC 7013, DOI 10.17487/RFC7013, September 2013, <https://www.rfc-editor.org/info/rfc7013>.

[RFC6313] Claise, B., Dhandapani, G., Aitken, P., and S. Yates, "Export of Structured Data in IP Flow Information Export (IPFIX)", RFC 6313, DOI 10.17487/RFC6313, July 2011, <https://www.rfc-editor.org/info/rfc6313>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

10.2. Informative References

[I-D.ietf-savnet-general-sav-capabilities]
Huang, M., Cheng, W., Li, D., Geng, N., and L. Chen, "General Source Address Validation Capabilities", Work in Progress, Internet-Draft, draft-ietf-savnet-general-sav-capabilities-02, 10 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-general-sav-capabilities-02>.

[I-D.ietf-savnet-inter-domain-problem-statement]
Li, D., Qin, L., Liu, L., Huang, M., and K. Sriram, "Gap Analysis, Problem Statement, and Requirements for Inter-Domain SAV", Work in Progress, Internet-Draft, draft-ietf-savnet-inter-domain-problem-statement-12, 20 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-inter-domain-problem-statement-12>.

[IANA-IPFIX]
"IP Flow Information Export (IPFIX) Entities", n.d., <https://www.iana.org/assignments/ipfix/ipfix.xhtml>.

Appendix A. IPFIX Encoding Examples

This appendix provides encoding examples for the SAV-specific IPFIX IEs defined in this document.

A.1. Template Record and Data Record with Sub-Template List

This example demonstrates the encoding for two observed SAV enforcement events representing different validation scenarios and address families as shown in Table 2.

Event	Source Address	Interface	Rule Type	Target Type	Policy Action
1	192.0.2.100	5001	Allowlist	Interface	Rate-limit
2	2001:db8::1	5001	Blocklist	Prefix	Discard

Table 2: Two Observed SAV Validation Events

The first event represents an IPv4 allowlist non-match event where a packet from source 192.0.2.100 arriving on interface 5001 failed to match any source prefixes configured in the interface-based allowlist. The second event represents an IPv6 blocklist match event where a packet from source 2001:db8::1 was received on interface 5001, which matched a prefix-based blocklist rule.

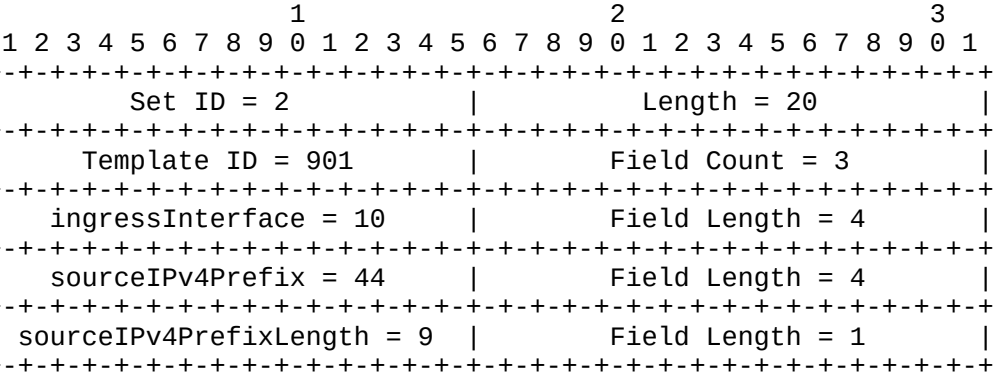
A.1.1. Sub-Template Definitions

The following sub-templates are defined for use within the savMatchedContentList element to encode different types of SAV rule mappings based on address family and validation target type. The savMatchedContentList element is encoded as a subTemplateList according to [RFC6313].

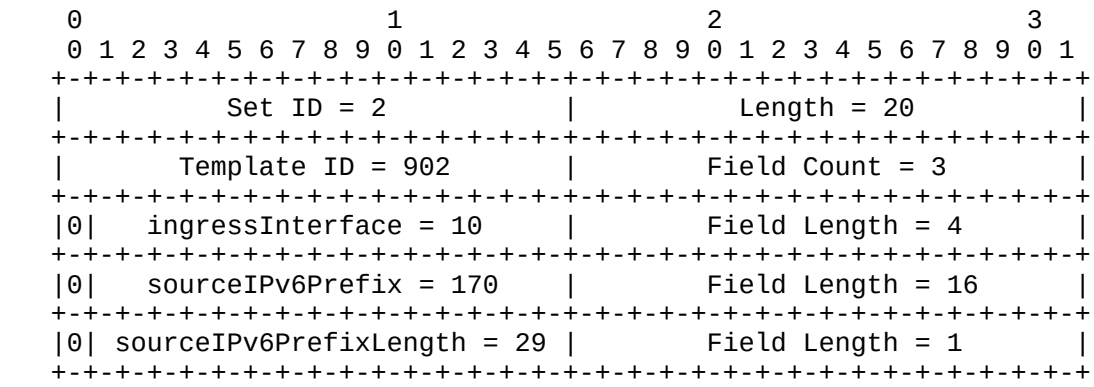
The template IDs used in these examples are exemplary and chosen arbitrarily. In actual implementations, exporters MUST assign unique template IDs within the IPFIX session for these sub-templates.

* *Sub-Template 901: IPv4 Interface-to-Prefix Mapping*

This sub-template is used when savTargetType=0(interface-based validation mode) for IPv4 traffic. It contains the mapping from an interface to source IPv4 prefixes as defined in the SAV rule configuration. It can be used for both blocklist and allowlist.

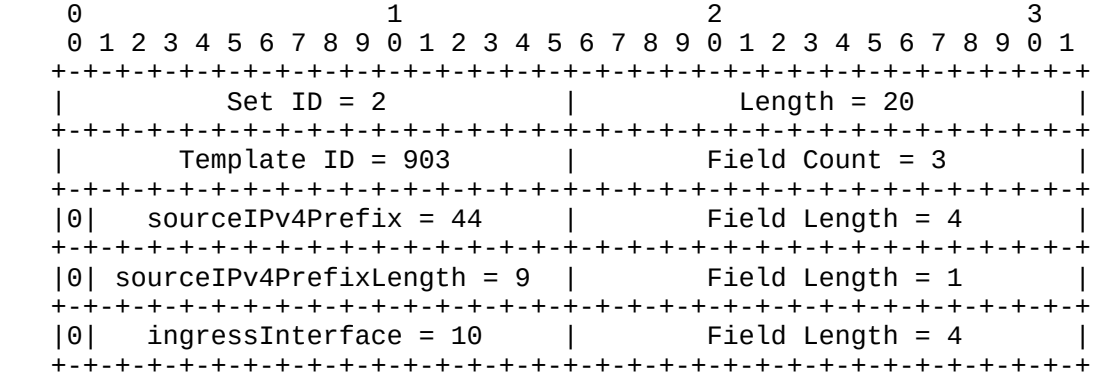


* *Sub-Template 902: IPv6 Interface-to-Prefix Mapping* This sub-template is the IPv6 equivalent of Sub-Template 901, used for interface-based validation with IPv6 traffic.



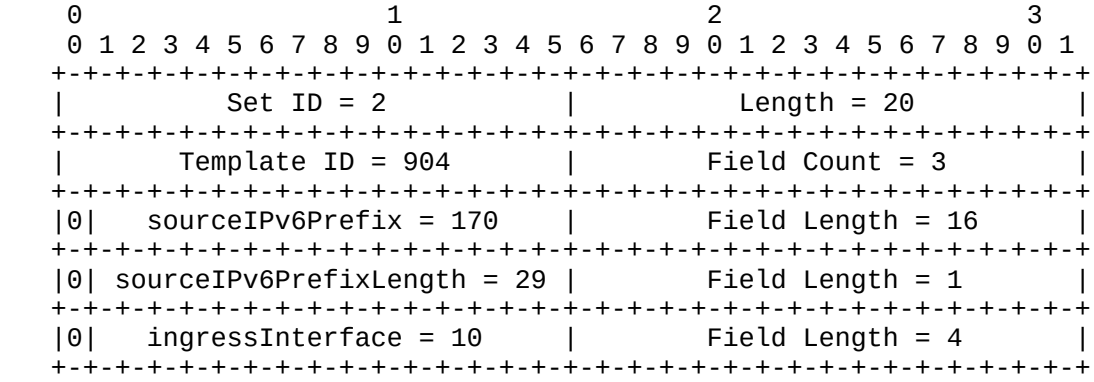
* *Sub-Template 903: IPv4 Prefix-to-Interface Mapping*

This sub-template is used when savTargetType=1(prefix-based validation mode) for IPv4 traffic. It contains the mapping from a source IPv4 prefixes to interface as defined in the SAV rule configuration. It can be used for both blocklist and allowlist.



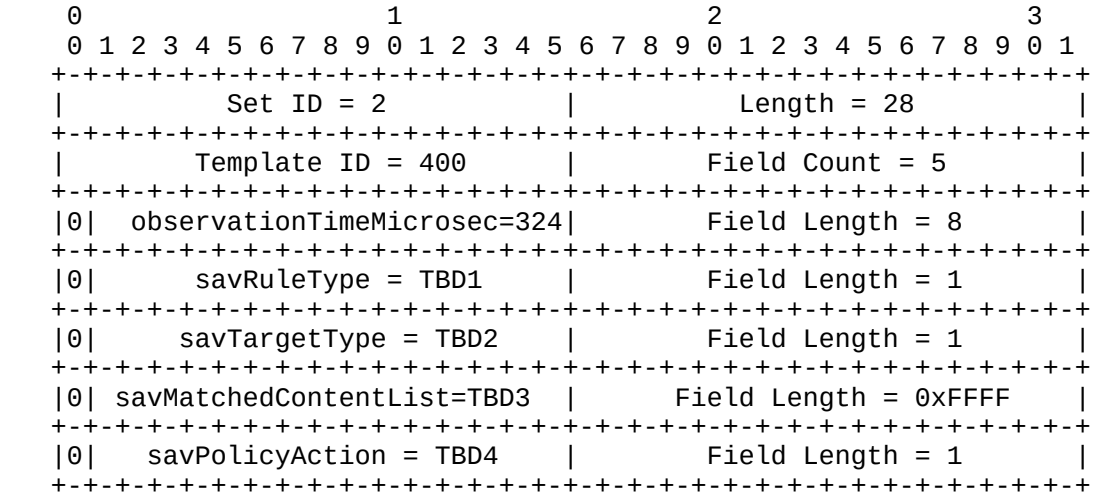
* *Sub-Template 904: IPv6 Prefix-to-Interface Mapping*

This sub-template is the IPv6 equivalent of Sub-Template 903, used for prefix-based validation with IPv6 traffic.



A.1.2. Main Template Record

The main Template Record (ID 400) contains fields for exporting detailed SAV enforcement information including the validation outcome and the specific rule content that triggered the action. The template incorporates the savMatchedContentList element as a variable-length subTemplateList to carry the relevant SAV rule contents using the appropriate sub-templates defined above.



A.1.3. Data Set Example

The following Data Set contains two Data Records that represent the two SAV validation scenarios in Table 2. The savMatchedContentList element for the first record encodes the complete set of allowed prefixes using Sub-Template 901 with the allOf semantic (0x03). The allowlist includes three sav rules. The savMatchedContentList element for the second record encodes the specific blocked interface using Sub-Template 904 with the exactlyOneOf semantic (0x01), indicating the packet matched this particular rule.


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Set ID = 400
Length = 88
observationTimeMicrosec =
0x5D2F0A0000000000
savRuleType=0
savTargetType=0
255
List Length
= 33
semantic=(allOf)
Template ID = 901
ingressInterface[0] = 5001
sourceIPv4Prefix[0] = 198.51.100.0
sourceIPv4PrfLen[0]=24
ingressInterface[1] =
5001
sourceIPv4Prefix[1] =
203.0.113.0
sourceIPv4PrfLen[1]=24
ingressInterface[2] =
5001
sourceIPv4Prefix[2] =
192.10.2.0
sourceIPv4PrfLen[2]=24
savPolicyAction=2
observationTimeMicrosec =
0x5D2F0A0000000001
savRuleType=1
savTargetType=1
255
List Length
= 27
semantic=exactlyOneOf
Template ID = 904
sourceIPv6Prefix[0]
sourceIPv6PrfLen[0]=32
ingressInterface[0] =
5001
savPolicyAction=1
padding

Authors' Addresses

Qian Cao
Zhongguancun Laboratory
Beijing
China
Email: caoqian@zgclab.edu.cn

Mingqing Huang
Zhongguancun Laboratory
Beijing
China
Email: huangmq@mail.zgclab.edu.cn

Benoit Claise
Everything OPS
Belgium
Email: benoit@everything-ops.net

Tianran Zhou
Huawei
Beijing
China
Email: zhoutianran@huawei.com