PCE Working Group
Internet-Draft
Intended status: Standards Track
Expires: 26 January 2026

X. Song
ZTE Corp.
W. Cheng
S. Yue
China Mobile

25 July 2025

Path Computation Element Communication Protocol for Source Address Validation
draft-song-pce-pcep-sav-01

Abstract

This document presents a method of Path Computation Element (PCE) for Source Address Validation (SAV) in networks. It extends Path Computation Element Communication Protocol (PCEP) to support SAV policy distribution and synchronization between PCEP speakers for threat mitigation for source address spoofing.

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 26 January 2026.

Table of Contents

1. Introduction 2
2. Conventions 3
2.1. Requirements Language 3
2.2. Terminology 3
3. PCE for SAV Support 3
3.1. PCE Integration to SANET Architecture 3
3.2. PCE as SAV Policy Controller 4
3.3. Requirements 4
4. PCEP Extenstions 4
4.1. SAV capability advertisement 5
4.2. SAV-POLICY Object 5
4.3. Mechanism for Updates 6
5. IANA Considerations 7
6. Security Considerations 7
7. Acknowledgements 7
8. Normative References 7
9. Informative References 7
Authors' Addresses 9

1. Introduction

Source Address Validation (SAV) is a critical security mechanism designed to mitigate IPv4 and IPv6 source address spoofing attacks by validating the legitimacy of source prefixes against their ingress interfaces. Traditional methods like ACL-based ingress filtering, strict uRPF and loose uRPF mechanisms [RFC3704] have some issues (e.g., high operational overhead, improper block or permit of traffic) as described in [I-D.ietf-savnet-intra-domain-problem-statement] and [I-D.ietf-savnet-inter-domain-problem-statement]. The new inter-domain SAV mechanism is required to have accurate source address validation to avoid improper block and minimize improper permit of traffic, and to support automatic update of SAV rules.

The PCE architecture, defined in [RFC4655], provides centralized control for path computation in networks. This document presents a PCE-based solution for SAVNET to provide dynamic policy enforcement

in networks. By extending the PCEP protocol, PCE can efficiently manage SAV policies, validate source prefixes, and enforce traffic filtering actions to mitigate the threats of source address spoofing.

2. Conventions

2.1. 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.

2.2. Terminology

This document uses the following terms defined in [RFC5440]: PCC, PCE, PCEP Peer, and PCEP speaker.

This document uses the following terms defined in [RFC8051]: stateful PCE.

This document uses the following terms defined in [I-D.ietf-savnet-intra-domain-architecture]: SAV, SAV rule, SAV Information Base.

3. PCE for SAV Support

3.1. PCE Integration to SANET Architecture

SAV Information Base (see [I-D.ietf-savnet-intra-domain-architecture]) that can be a table or data structure in a router which stores SAV-specific information and local routing information. SAV Information Base synchronizes SAV rules to PCE via BGP-LS or NETCONF/YANG interfaces, enabling PCE to compute validation paths. The PCE sends requests to PCC, which receives the SAV rules distributed by PCE and enforces SAV rules on data plane. For example, in an enterprise AS, PCE collects SAV specific routes from edge routers or border routers. It computes that source prefix (for example, 2001:db8:1::/48) is only valid on interfaces connected to the data center subnet. Any traffic with this prefix arriving at an AS border router is dropped unless it originates from the designated interfaces.

The PCE-SAVNET integration proposed here supports both single-PCE and multi-PCE coorperative environments. It is applicable to single-domain and multi-domain AS scenarios, leveraging PCE for cross-domain policy coordination. For example, if the attacker switches the entry

from Eth1/0 of R1 in AS60001 to Eth5/0 of R5 in AS60004, the PCE controller needs to synchronize the SAV rules and enforce policies for source address validation across domains.

3.2. PCE as SAV Policy Controller

The example of process for PCE using PCEP to install SAV policies on edge routers (i.e., PCC role) in inter-domain networks is showed below:

PCE as SAV controller collects SAV-specific information for SAV policy generation of mapping valid interfaces with prefix (e.g., 2001:db8::/32) to have the capability of global SAV policy visibility for single or multiple domains policy enforcement and coordination.

PCE sends PCEP protocol messages (see [RFC8231]) to instal SAV policies, dynamic SAV policy updates.

PCC deploys SAV policies which stores in SAV Information Database for mapping of source address prefix with valid ingress interfaces for ingress traffic filtering.

3.3. Requirements

When the PCE speakers supporting SAV, the PCEP is required to support the following functionalities.

The PCEP MUST support SAV-specific information and local routing information collection for cross-domain coordination and policy enforcement.

The PCEP MUST support SAV capability advertisement in single and multi-domains.

The PCEP MUST support dynamic updates of SAV policies for network changes (e.g., link failures, prefix additions).

The PCEP MUST support backward compatibility with existing SAVNET mechanisms (e.g., BAR-SAV).

The PCEP sessions for SAV MUST be secured against tampering and unauthorized access.

4. PCEP Extenstions

4.1. SAV capability advertisement

The open message is used to establish a PCEP session between PCEP speakers. To support SAV functionality, a new flag is required for SAV capability advertisement which is introduced in this document.

The SAV-CAPABILITY TLV is an optional TLV for use in the OPEN object for SAV capability advertisement. The format for SAV-CAPABILITY TLV refers to figure 9 in [RFC8231]. A new value for Flags field is TBD for the SAV capability advertisement.

4.2. SAV-POLICY Object

To support SAV functions, a new optional SAV object (class=TBD) for SAV information and its related object body formatted as TLV introduced in this document. A SAV-POLICY object is used to carry information of SAV policy within a PCEP update message, which may carry a set of SAV policies delivery and updates.

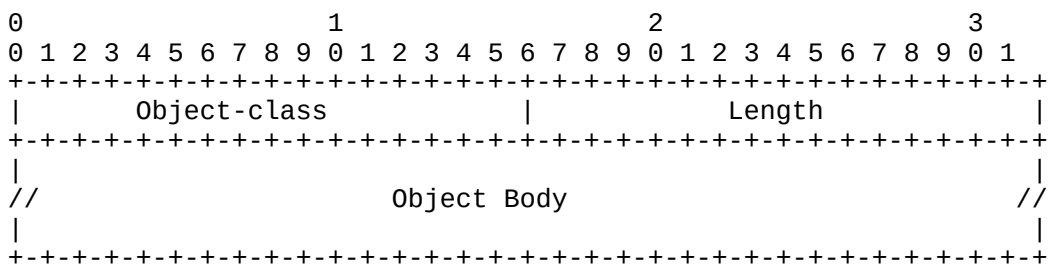

Figure 1: SAV-POLICY Object Format

SAV-POLICY object class value is TBD.

The TLV format for SAV-POLICY object consists of IPv4/IPv6 prefix and incoming-interface list (legitimate or illegitimate interfaces). The information for SAV-POLICY object is carried as TLV format, showed as the following figure:

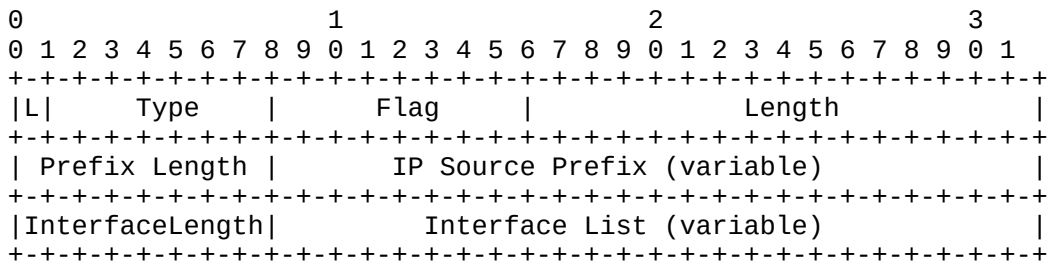

Figure 2: SAV-CAPABILITY TLV Format

The type (8 bits) of the TLV is TBD.

The length field is 16 bits long, indicates the total length of the TLV in octects.

The value contains the following fields:

L: 1 bit long, identifies IP source prefix types, including IPv4 and IPv6 types.

Flag: 8 bits long, identifies the validation modes used in network nodes. The validation modes include 4 modes: interface-based prefix allowlist, interface-based prefix blocklist, prefix-based interface allowlist, prefix-based interface blocklist. By selecting modes in different scenarios, the network can be secured to mitigate spoofing attacks, as introduced in [I-D.ietf-savnet-general-sav-capabilities].

Interface List: contains a list of interfaces. If it is a whitelist, it represents a list of interfaces allowed to access; if it is a blacklist, it represents a list of interfaces not allowed to access. The interface list can be expressed in the form of interface ID, interface name, or index.

IP source prefix: contains the source address prefix information.

4.3. Mechanism for Updates

The PCE needs send PCUpd message for triggering mechanism when PCE makes actively update to the SAV policies, the possible trigger conditions may involve: topology changes (e.g., interface status modified), policy updates (e.g., the new added IP source prefix affiliated interfaces), and attack response from external threats.

5. IANA Considerations

This document requests one new value for SAV capability advertisement, one new value for class of SAV policy object introduced in this document. IANA is requested to allocate TLV values for SAV-CAPABILITY TLV.

6. Security Considerations

Security considerations for PCE are covered in the PCE Architecture [RFC5394], PCEP [RFC5440] and stateful PCE [RFC8231]. PCEP sessions for SAV policy distribution MUST use TLS 1.3 [RFC8346] to prevent tampering. SAVNET security considerations covered in [I-D.ietf-savnet-intra-domain-architecture] and [I-D.ietf-savnet-inter-domain-architecture] are also applicable to the SAVNET procedures through PCEP defined in this document.

7. Acknowledgements

The authors would like to acknowledge Haisheng Wu and Zhenghai Wang for their helpful comments.

8. Normative References

[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>.

[RFC5440] Vasseur, JP., Ed. and JL. Le Roux, Ed., "Path Computation Element (PCE) Communication Protocol (PCEP)", RFC 5440, DOI 10.17487/RFC5440, March 2009, <https://www.rfc-editor.org/info/rfc5440>.

[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>.

[RFC8231] Crabbe, E., Minei, I., Medved, J., and R. Varga, "Path Computation Element Communication Protocol (PCEP) Extensions for Stateful PCE", RFC 8231, DOI 10.17487/RFC8231, September 2017, <https://www.rfc-editor.org/info/rfc8231>.

9. 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-01, 24 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-general-sav-capabilities-01>.

[I-D.ietf-savnet-inter-domain-architecture]
Li, D., Chen, L., Geng, N., Liu, L., and L. Qin, "Inter-domain Source Address Validation (SAVNET) Architecture", Work in Progress, Internet-Draft, draft-ietf-savnet-inter-domain-architecture-01, 3 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-inter-domain-architecture-01>.

[I-D.ietf-savnet-inter-domain-problem-statement]
Li, D., Wu, J., Liu, L., Huang, M., and K. Sriram, "Source Address Validation in Inter-domain Networks Gap Analysis, Problem Statement, and Requirements", Work in Progress, Internet-Draft, draft-ietf-savnet-inter-domain-problem-statement-09, 4 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-inter-domain-problem-statement-09>.

[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-02, 13 April 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-intra-domain-architecture-02>.

[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-17, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-savnet-intra-domain-problem-statement-17>.

[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>.

[RFC4655] Farrel, A., Vasseur, J.-P., and J. Ash, "A Path Computation Element (PCE)-Based Architecture", RFC 4655, DOI 10.17487/RFC4655, August 2006, <https://www.rfc-editor.org/info/rfc4655>.

[RFC5394] Bryskin, I., Papadimitriou, D., Berger, L., and J. Ash, "Policy-Enabled Path Computation Framework", RFC 5394, DOI 10.17487/RFC5394, December 2008, <https://www.rfc-editor.org/info/rfc5394>.

[RFC8051] Zhang, X., Ed. and I. Minei, Ed., "Applicability of a Stateful Path Computation Element (PCE)", RFC 8051, DOI 10.17487/RFC8051, January 2017, <https://www.rfc-editor.org/info/rfc8051>.

[RFC8346] Clemm, A., Medved, J., Varga, R., Liu, X., Ananthakrishnan, H., and N. Bahadur, "A YANG Data Model for Layer 3 Topologies", RFC 8346, DOI 10.17487/RFC8346, March 2018, <https://www.rfc-editor.org/info/rfc8346>.

Authors' Addresses

Xueyan Song
ZTE Corp.
China
Email: song.xueyan2@zte.com.cn

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

Shengna Yue
China Mobile
China
Email: yueshengnan@chinamobile.com