Policy Computing Element Communication Protocol for Source Address Validation

draft-song-pce-pcep-sav-00

Xueyan Song	ZTE Corp.
Weiqiang Cheng	CMCC.
Shengnan Yue	CMCC.

IETF 123 Meeting, July 2025

Overview

- SAV (Source Address Validation)
  - 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.
- PCEP for SAV
  - PCE provides a centralized control architecture for path computation in networks.
  - PCE as SAV controller has the visibility of global SAV policy across network domains.
  - PCEP communicated between PCEP speakers can be extended to support SAV policy management, source address validation and traffic filtering enforcement.

PCE for SAV Support

- **Topology collection**
  - Obtain link and node status.
  - Collect topology information and construct global network vision.
- **Path computation**
  - Compute the valid incoming interface list based on the AS affiliation and topology constraints.
  - Generate SAV policies based on the source prefixes, prefix path and incoming interfaces.
- **Policy delivery**
  - Dynamically delivery SAV policies to edge/border nodes (PCC) of network through PCEP protocol.
- **Action & Feedback**
  - Execute filtering actions and report policies implement status.
  - Re-compute path and adjust filtering policies to reflect network topology updates or abnormal traffic detection.

PCEP Extension-1/2

- **SAV Capability TLV**
  - An optional TLV for use in the OPEN object for SAV capability advertisement.
  - A new value for Flag in the "STATEFUL-PCE-CAPABILITY" TLV Flag Field, the description of the flag is SAV-CAPABILITY, reference RFC8231.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Type=16         |            Length=4           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             Flags                           |U|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

PCEP Extension-2/2

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Object-class           |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
//                         Object Body                         //
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|L|     Type    |      Flag     |             Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Prefix Length |       IP Source Prefix (variable)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|InterfaceLength|        Interface List (variable)              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

SAV Capability Object

- Optional object for SAV information advertisement
- Class value is TBD

SAV Capability Object body

- L: 1 bit, identifies IPv4 and IPv6 types
- Type: 7 bits, is TBD
- Flag: 8 bits, identifies the validation modes used in network nodes.
- Interface List: variable length, contains a list of interfaces.
- IP source prefix: variable length, contains the source address prefix information.

Next Steps

- Keep following the progress of SAVNET WG and make corresponding updates.
- Improve the processing procedures and encapsulation methods of PCEP extension.
- Welcome reviews, comments and collaborations.

Thank you!