SID as Source Address in SRv6

draft-yang-spring-sid-as-source-address-01

Feng Yang (China Mobile) (Presenter)

Changwang Lin (New H3C Technologies)

IETF-116

Requirements

- **Using SRv6 SID as source address**

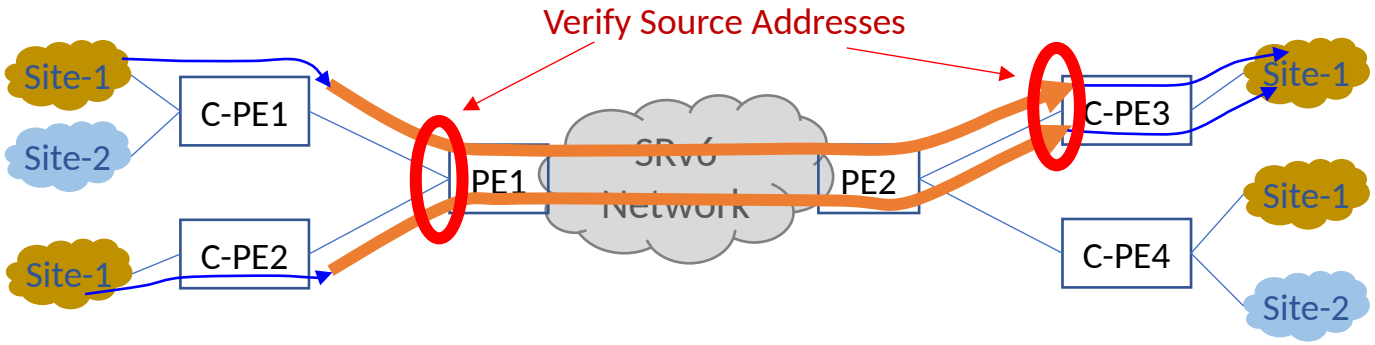
For L2 VPN VPWS, L2 VPN VPLS and L3 IPv4/IPv6 VPN Service , the user traffic towards SRv6 network will be encapsulated in SRv6 tunnel. The source address of the SRv6 packet should be assigned using the local VPN SID of the PE(C-PE) device.

- **Verify source address**
  - On **the SRv6 tunnel 2nd hop node**, to prevent SRv6 tunnel source address fraud.

  Use the inbound interface and source address as keys to lookup the Source Address Verification Rules.
  - On **the SRv6 Tunnel egress node**, to prevent SRv6 tunnel egress SID fraud.

  Access authorization is granted to all source L2 or L3 SRv6 service SIDs on egress node.

  After receiving an SRv6 packet, look up the SRv6 Source Verification Table based on the source address of packet, and check whether the source site allows access to local site.



Use Cases

Use Case1: Pass through SR-aware Stateful Firewall

- **Problem:**
  - The dest address of SRv6 tunnel is VPN-SID, while src address usually uses the loopback address. Bidirectional flows are using 2 different pairs of src&dest address. Traffic will be dropped by FW sitting in middle of tunnel
- **Proposal:**
  - By using VPN SID as source address, bidirectional flows have single pair of src&dest address.

Use Case2&3: VPN isolation enforcement for SRv6 overlay & underlay VPN services

- **Problem:**
  - With falsified dest VPN SID, one can reach any VPNs at will.
- **Proposal:**
  - Using VPN SID as src address, enable src verification on tail of SRv6 tunnel before doing VPN forwarding.
  1. Src Verification Table contains src VPN sid for access control, packet will be dropped on src address lookup failure.
  2. Src Verification Table can be filled up by advertising VPN SID as BGP prefix SID associated with RT attribute.

Considerations about ICMPv6 Messages

Ping Echo Reply and ICMP error messages may use SRv6 SID as destination address.

RFC 8986 4.1.1

Allowing the processing of specific Upper-Layer header types is useful for Operations, Administration, and Maintenance (OAM). As an example, an operator might permit pinging of SIDs. To do this, they may enable local configuration to allow Upper-Layer header type 58 (ICMPv6).

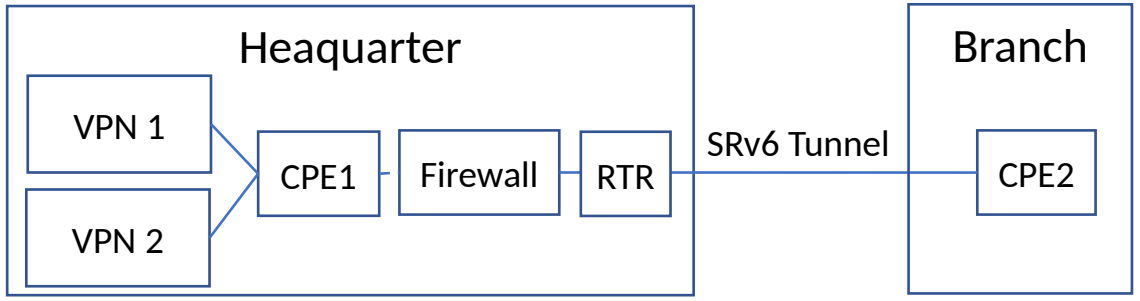
It is RECOMMENDED that an implementation of local configuration only allows Upper-Layer header processing of types that do not result in the packet being forwarded (e.g., ICMPv6).

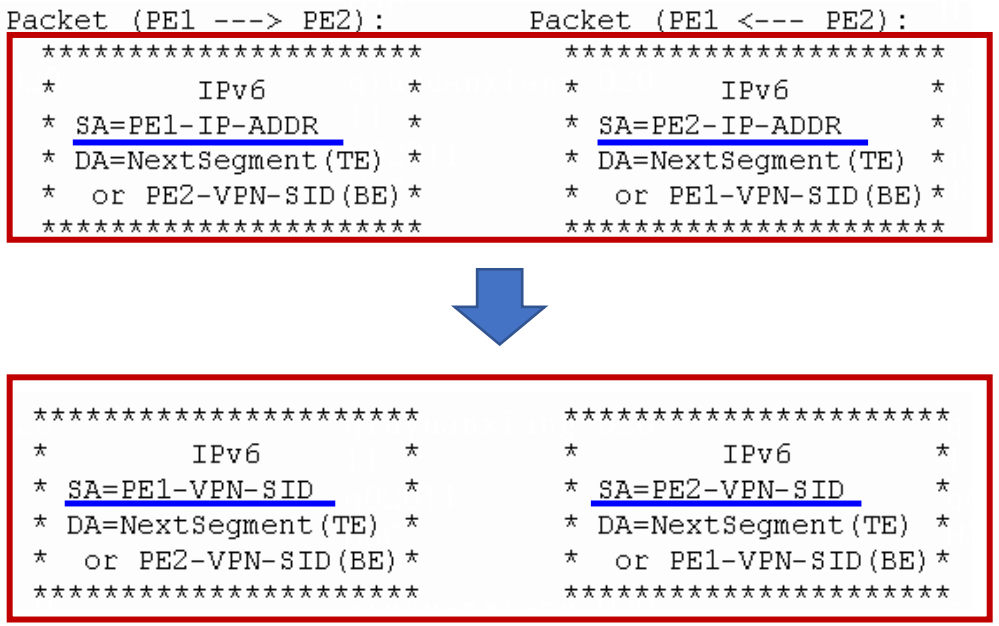
Next Steps

- Any questions or comments are Welcomed
- Seeking for feedback

Use Case 1

In SRv6 Network with SR-aware Stateful Firewall, use service SID as source address.





- **Current problem**

The destination of the outer IPv6 header is the VPN-SID of the egress CPE1. The source address usually uses the loopback address.

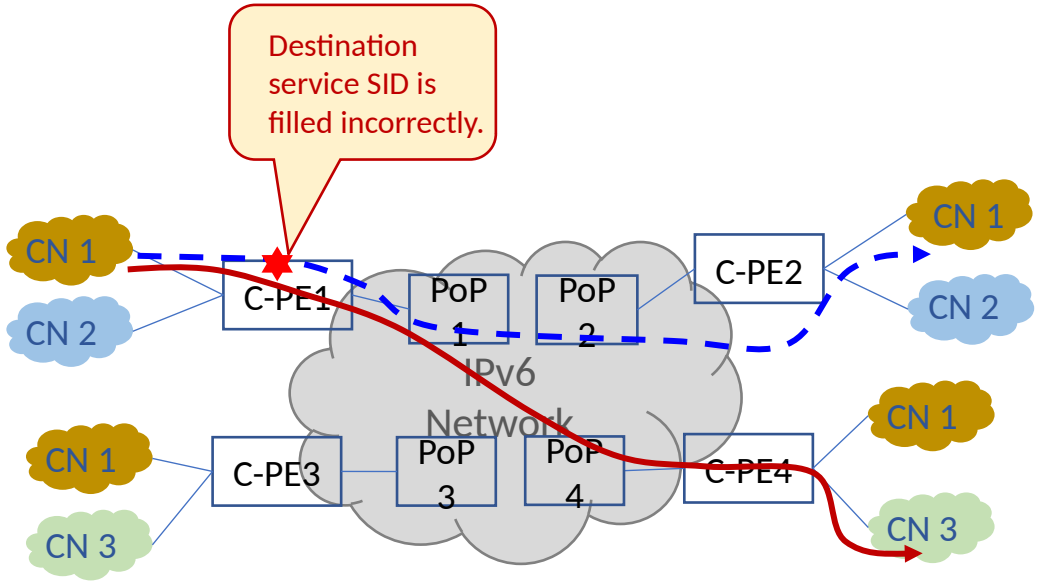
So, it is difficult for a stateful firewall to establish the association relationship between the bidirectional traffic flows.

- **Proposal**

When CPE1 receives the packet from CPE2, it checks which L3 VPN service it belongs to, and uses the VPN SID associated with that L3 VPN service as the source address when encapsulating the outer IPv6 header with the optional SRH.

Use Case 2

VPN isolation enforcement for SRv6 SDWAN network by source address verification.



- **Current problem**

When someone manipulate the SRH, he/she can reach any VPNs without authorized.

For example, the destination address of the traffic from CN1 of C-PE1 to CN1 of C-PE2 is misconfigured or tampered with as the service SID of CN3 of C-PE4. The traffic can be send to C-PE4.

- **Proposal**

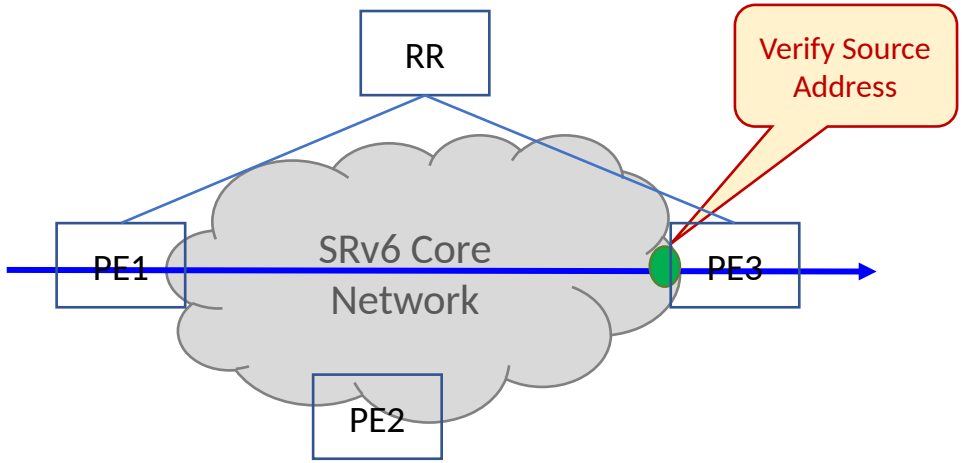
Enable SRv6 Source Verification on C-PE4.

1. Configure SRv6 Source Verification entries on C-PE4, and specify which user sites from which C-PE can communicate with it.
2. After receiving SRv6 packet, based on the source address, C-PE4 check the SRv6 packet for authorized access. If the SRv6 packet passes check, it will forward the SRv6 packet; otherwise, discard it.

Use Case 3

VPN isolation enforcement mechanism needed within SRv6 domain.
--RFC 5920 identified potential attack inside trusted domain: compromised software within the trust domain, malign person with access to any LSR in the trust domain

The SRv6 source verification function can be enabled on the PE of the tenant network connecting to the SRv6 core network.
When the traffic is pass through the SRv6 core network, the received traffic can be verified.



SRv6 Source Verification Table

- **What is the content?**
  - **Source service address**, which is encapsulated as the outer source IPv6 address of the packet, used to identify the service of the source client network.
    - L2 SRv6 Service SID: End.DX2 or End.DT2U
    - L3 SRv6 Service SID: End.DT46, End.DT4, End.DT6, End.DX4, or End.DX6

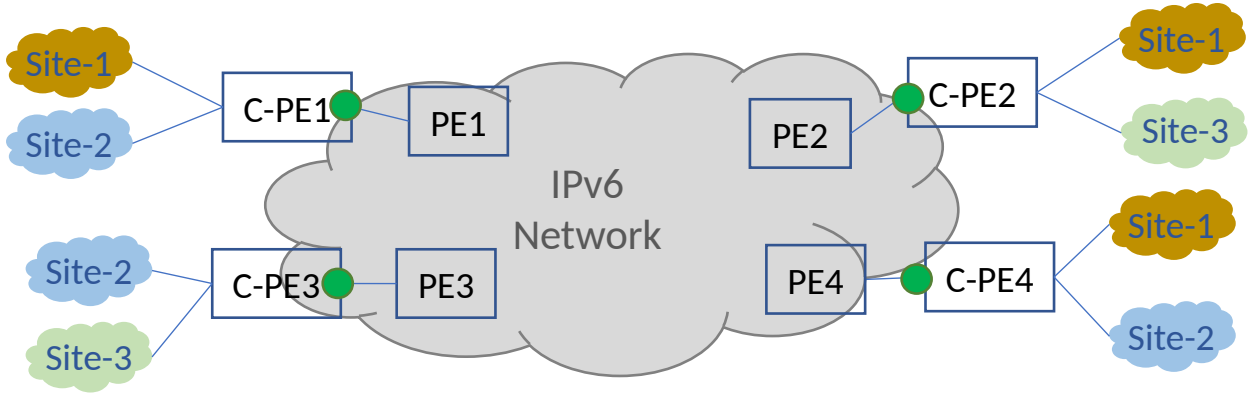
- **How to create ?**
  1. Manual static configuration on the SRv6 egress node.
  2. Dynamic creation after learning the service address of source site through BGP.

  When the L3VPN/L2VPN route with the remote L3VPN/L2VPN service SID is inserted into the local VPN table, the relationship between the local L3VPN/L2VPN service SID and the remote L3VPN/L2VPN service SID is recorded, and a dynamic source address Verification table in local VPN table is generated.

  Every L2/L3 VPN service has a source verification table.

Configuration Example

Configuration of source verification in SRv6 SDWAN Network



1) Configure VPN SID

```
VPN SID on C-PE1:
   CN1:
      vpn-instance 1 end-dt4 100::100
   CN2:
      vpn-instance 2 end-dt4 100::200
VPN SID on C-PE2:
   CN1:
      vpn-instance 1 end-dt4 200::100
   CN3:
      vpn-instance 3 end-dt4 200::300
VPN SID on C-PE3:
   CN2:
      vpn-instance 2 end-dt4 300::200
   CN3:
      vpn-instance 3 end-dt4 300::300
VPN SID on C-PE4:
   CN1:
      vpn-instance 1 end-dt4 400::100
   CN2:
      vpn-instance 3 end-dt4 400::200
```

2) Configure source address verification entries

```
Source address verification table on C-PE1:
      vpn-instance 1:
          Trusted-source-address 200::100
          Trusted-source-address 400::100
      Vpn-instance 2:
          Trusted-source-address 300::200
          Trusted-source-address 400::200
Source address verification table on C-PE2:
      Vpn-instance 1:
          Trusted-source-address 100::100
          Trusted-source-address 400::100
      Vpn-instance 3:
          Trusted-source-address 300::300
```