ESP Protected Services over SRv6

https://datatracker.ietf.org/doc/draft-wdh-srv6ops-secservice/

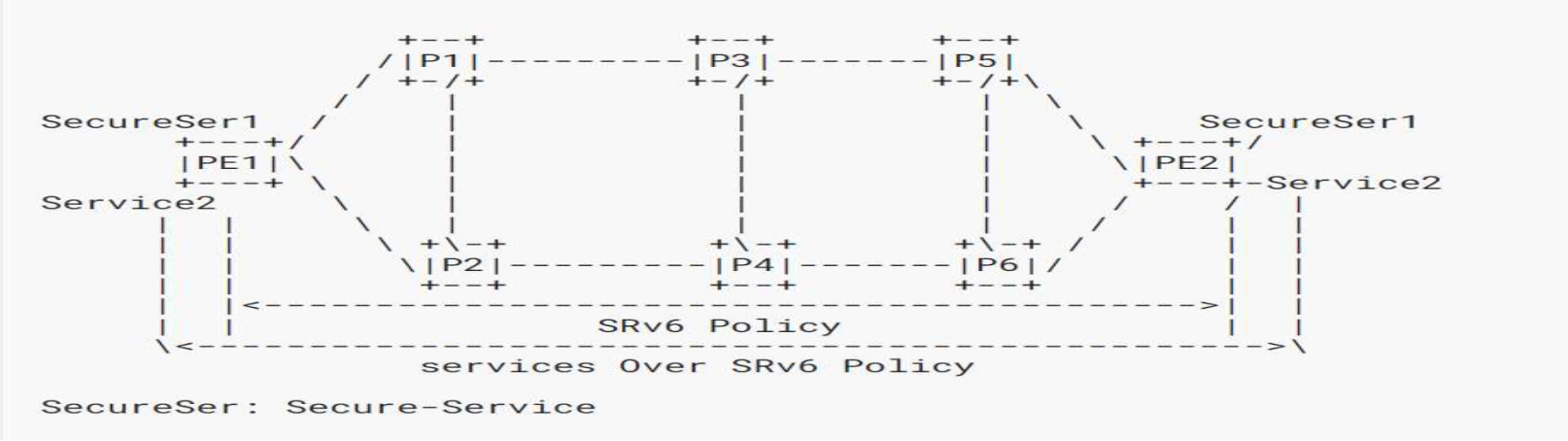
Haibo Wang/**Linda Dunbar**/Jun Li/Yao Yang

IETF 125

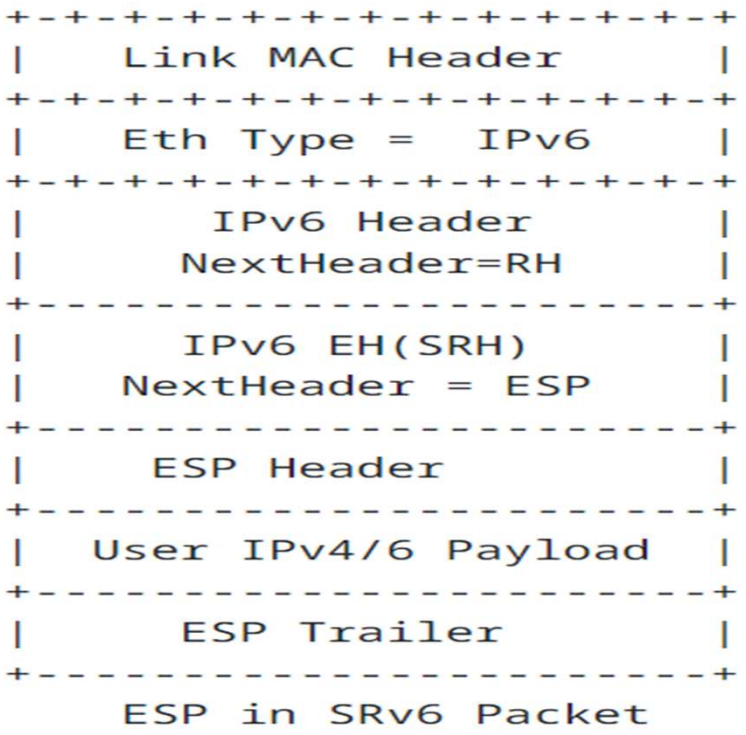
Shen Zhen

Use Case

- **Some financial data require additional security.**
  - IPsec ESP used for those selective services
- **SRH needs to be outside of encryption for traversing through SRv6 domain**



Desired Data Plane

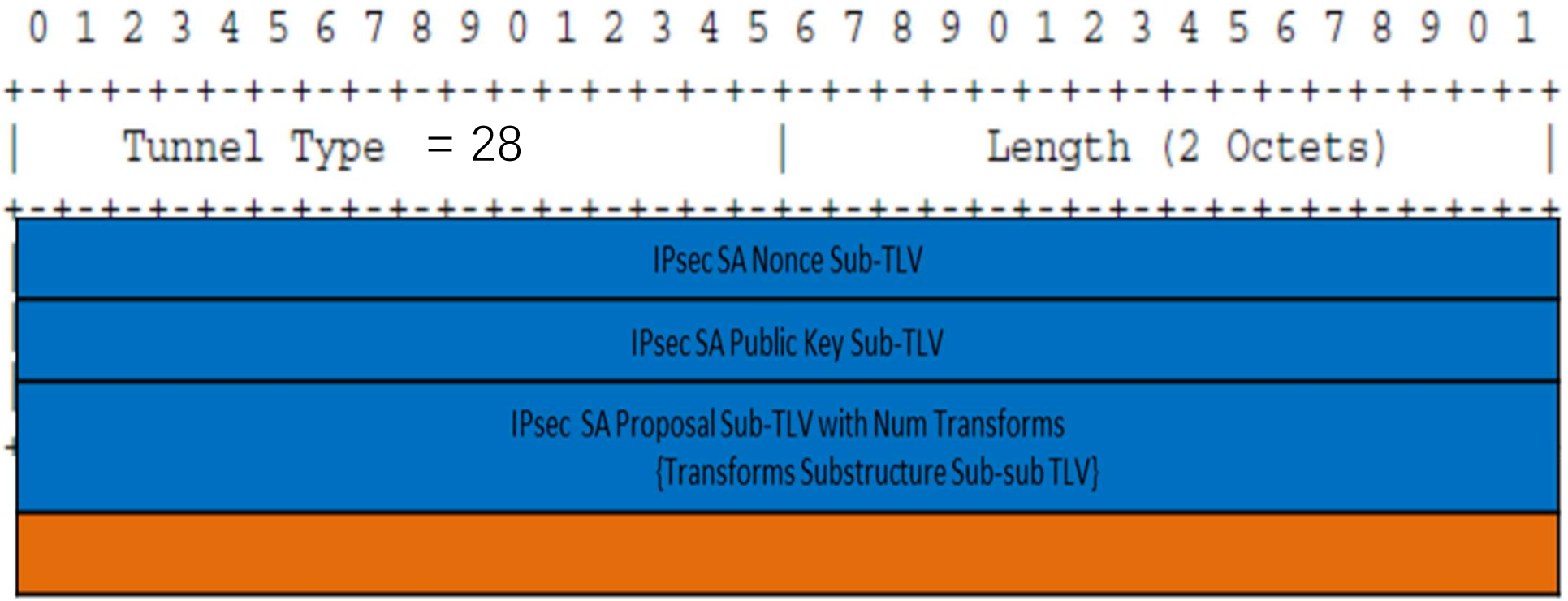


ESP in SRv6 Packet

New Tunnel-type

- Tunnel Encapsulation Attribute:
  - Tunnel-Type: ESP-Protected-Payload = 28
  - IPSec SA Property Sub-TLV reuse draft-ietf-idr-sdwan-edge-discovery:
    - IPsec SA Nonce
    - IPSec Public Key
    - IPsec SA Proposal

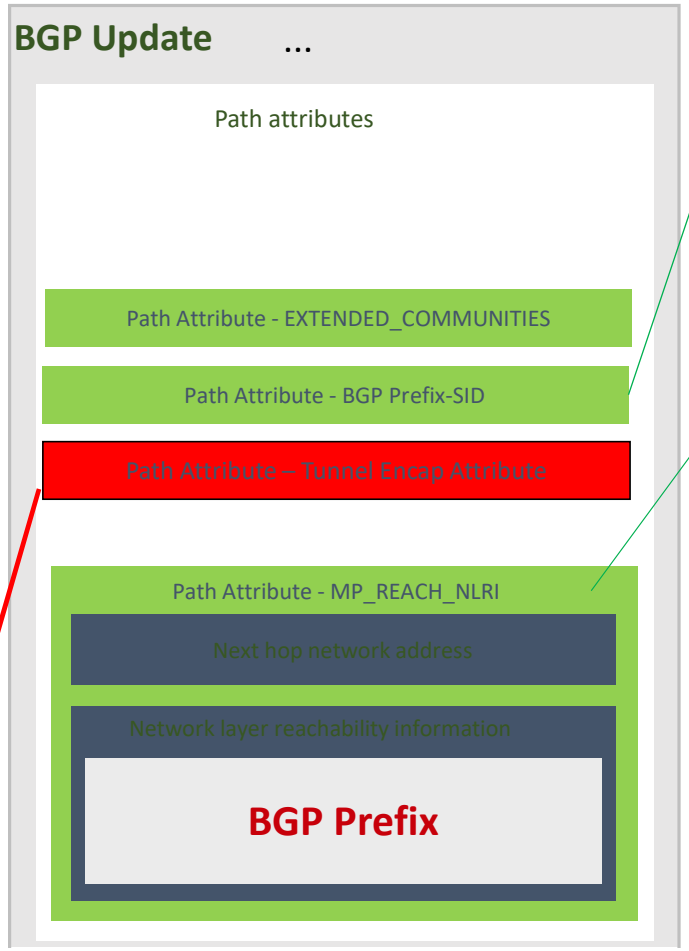
Tunnel Encap Attribute



BGP Update

Border Gateway Protocol - UPDATE Message
Marker: ffffffffffffffffffffffffffffffff
Path Attribute - EXTENDED_COMMUNITIES
Flags: 0xc0, Optional, Transitive, Complete
Type Code: EXTENDED_COMMUNITIES (16)
Length: 8
Carried extended communities: (1 community)
Route Target: 1:1 [Transitive 2-Octet AS-Specific]
Type: Transitive 2-Octet AS-Specific (0x00)
Subtype (AS2): Route Target (0x02)
2-Octet AS: 1
4-Octet AN: 1

Tunnel Encap Attribute:
Tunnel-type= ESP-Protected-Payload
Tunnel egress endpoint = 2001:DB8:3::3/128
IPsec SubTLVs



Path Attribute - BGP Prefix-SID
Flags: 0xd0, Optional, Transitive, Extended-Length, Complete
Type Code: BGP Prefix-SID (40)
Length: 22
BGP Prefix-SID TLV type: 4
End.DT4: 2001:DB8:130::200

Path Attribute - MP_REACH_NLRI
Flags: 0x90, Optional, Extended-Length, Non-transitive, Complete
1... .... = Optional: Set
.0.. .... = Transitive: Not set
..0. .... = Partial: Not set
...1 .... = Extended-Length: Set
.... 0000 = Unused: 0x0
Type Code: MP_REACH_NLRI (14)
Length: 45
Address family identifier (AFI): **IPv4 (1)**
Subsequent address family identifier (SAFI): **Labeled VPN Unicast (128)**
Next hop network address (24 bytes)
Next Hop: Empty Label Stack RD=0:0 IPv6=**2001:DB8:3::3**
Number of Subnetwork points of attachment (SNPA): 0
Network layer reachability information (16 bytes)
BGP Prefix
Prefix Length: 120
Label Stack: 3 (bottom)
Route Distinguisher: **200:1**
MP Reach NLRI IPv4 prefix: **22.22.22.22**

Process Illustration

1) PE1 adds a Tunnel-Encapsulation Attribute to the routes based on local policies. The Tunnel-Type parameter is ESP-Protected-Payload. Advertises the route to PE2 through RRs
   - PE1 obtains IPSec related parameters by configuration, from its management system, or via negotiation, including IPsec SA encryption algorithms, keying material, nonce, and security policies, etc..
   - PE1 obtains the VPN route and carries tunnel information, such as the VPN SID and Color Extended Community, based on the local policy.
2) Upon receiving the route advertised by PE1, PE2 performs IPsec key negotiation based on the ESP-Protected-Payload Tunnel-Encapsulation Attribute carried in the route.
   - Based on the VPN ID and color, PE2 associates the route with the SRv6 tunnel.
3) When PE2 receives the CE-side traffic that matches the route advertised by PE1. PE2 performs IPsec encryption based on the indicated IPSec sub-TLVs advertised by PE1, encapsulates the traffic into an SRv6 tunnel based on the indicated tunnel information, and sends the traffic to PE1 along the tunnel information.
4) After receiving the traffic from PE2, PE1 finds the corresponding VRF based on the SRv6 tunnel information and decrypts the packets to obtain the original user packet payload. Forwards traffic to the CE based on the user packet header.

Next step

- Need more reviews