IPSec for BGP Enabled Service over SRv6

https://datatracker.ietf.org/doc/draft-wang-bess-secservice/
Haibo Wang/Linda Dunbar/Cheng Sheng/Hang Shi
Huawei, Futurewei
IETF 119
IPSec over SRv6 Use Case

• Some customers in financial industry build their own backbone network and use SRv6 to orchestrate service.
• Normally, SRv6 domain is considered secure (RFC 8754, RFC 8402, RFC 8986)
• But financial data needs additional security. IPSec is used to encrypt the data end to end in case of any intrusion in the backbone network
• SRH needs to be outside of encryption
Desired Data Plane
BGP Update Message Extension

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-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
New Tunnel-type

• Tunnel Encapsulation Attribute:
  • Tunnel-Type = ESP-Payload
  • IPSec SA Property Sub-TLV reuse draft-ietf-idr-sdwan-edge-discovery-12:
    • IPsec SA Nonce
    • IPSec Public Key
    • IPsec SA Proposal

• Tunnel Encapsulation Attribute:
  • Tunnel-Type = ESP-Payload
  • IPsec SA-ID Sub-TLV (reuse draft-ietf-idr-sdwan-edge-discovery-12)

• Encrypt using ESP then encap into SRv6
Next step

• Similar to Secure EVPN: per route IPSec
• Option 1: merge with Secure EVPN
  • Add a subsection in section 9 to describe encapsulation
  • Add extension of new tunnel type in section 10
• Option 2: Secure EVPN seems not moving forward
  • Ask for WG adoption