draft-ietf-bess-secure-01.txt

A. Sajassi (Cisco), A. Banerjee (Cisco), S. Thoria (Cisco), D. Carrel (Cisco), B. Weis (Cisco)

IETF 104, March 2019

Prague

History

- Rev00 was presented in the last IETF (IETF 103) in Bangkok

Solution Overview

- Secure control channel between each PE and the RR (e.g., using existing scheme such as IKv2)
  - Setup BGP session over this secure tunnel
- Use this secured BGP channel for P2MP signaling to establish P2P IPsec SAs for user traffic
  - No need for P2P signaling to establish P2P SA
  - Reducing # of msg exchanges from O(N^2) to O(N)
  - Each PE advertises to other PEs the info needed for establishing P2P SAs

Solution Overview (2)

- When a PE device first comes up and wants to setup an IPsec SA between itself and each of the interested remote PEs, it generates a DH pair for each of its intended IPsec SA using an algorithm defined in the IKEv2 Diffie-Hellman Group Transform IDs [IKEv2-IANA].
- The originating PE distributes DH public value along with a nonce (using IPsec Tunnel TLV in Tunnel Encapsulation Attribute) to other remote PEs via the RR.
- Each receiving PE uses this DH public number and the corresponding nonce in creation of IPsec SA pair to the originating PE

Encapsulations

- Two types of IPSec encapsulations for our applications
  1. IPsec encap in transport mode without outer UDP header
  2. IPsec encap in transport mode with outer UDP header per [RFC3948]
     - Needed for NAT traversal or per flow LB using UDP header

Changes Since Rev00

- Some editorial changes
- Added the requirements for setting up an IPsec tunnel between a pair of ASs between ingress and egress PEs
- Added the new section 3.1 on “Inheritance of Security Policy”
- Modified IPsec Tunnel Attribute sub-TLVs for better optimization

Inheritance of Security Policy

- IPsec tunnels for EVPN & other VPNs can be setup at different level of granularity
- For example, if an IPsec tunnel is needed between a pair of ACs, then IPsec tunnel attribute is carried along with the EVPN route representing each AC
- In the absence of such coloring (e.g., sending IPsec tunnel attribute explicitly along an EVPN route), the route inherits the IPsec tunnel of next level up (of its parent)
- For example, in the absence of Ipsec tunnel attribute for EVPN route representing AC, the AC

Functionality	EVPN	IP-VPN	MVPN	VPLS
per PE	IPv4/v6 route	IPv4/v6 route	IPv4/v6 rte	IPv4/v6
per tenant	IMET (or new)	lpbk (or new)	I-PMSI	N/A
per subnet	IMET	N/A	N/A	VPLS AD
per IP	EVPN RT2/RT5	VPN IP rt	*,G or S,G	N/A
per MAC	EVPN RT2	N/A	N/A	N/A

Min set

Minimum Set

```
ID, [N(INITIAL_CONTACT),] KE, Ni; where

     ID payload is defined in section 3.5 of [RFC7296]
     N (Notify) Payload in section 3.10 of [RFC7296]
     KE (Key Exchange) payload in section 3.4 of [RFC7296]
     Ni (Nonce) payload in section 3.9 of [RFC7296]

KE payload contains the DH public number and also identifies which DH
```

Single Policy

```
ID, [N(INITIAL_CONTACT),SA, KE, Ni

     SA (Security Association) payload in section 3.3 of [RFC7296]
```

Policy List and DH group List

```
ID, [N(INITIAL_CONTACT), [SA], [KE], [Ni]

     [SA] list of IPsec policies (i.e., list of SA payloads)
     [KE] list of KE payloads
```

Base DIM Sub-TLV – min. set

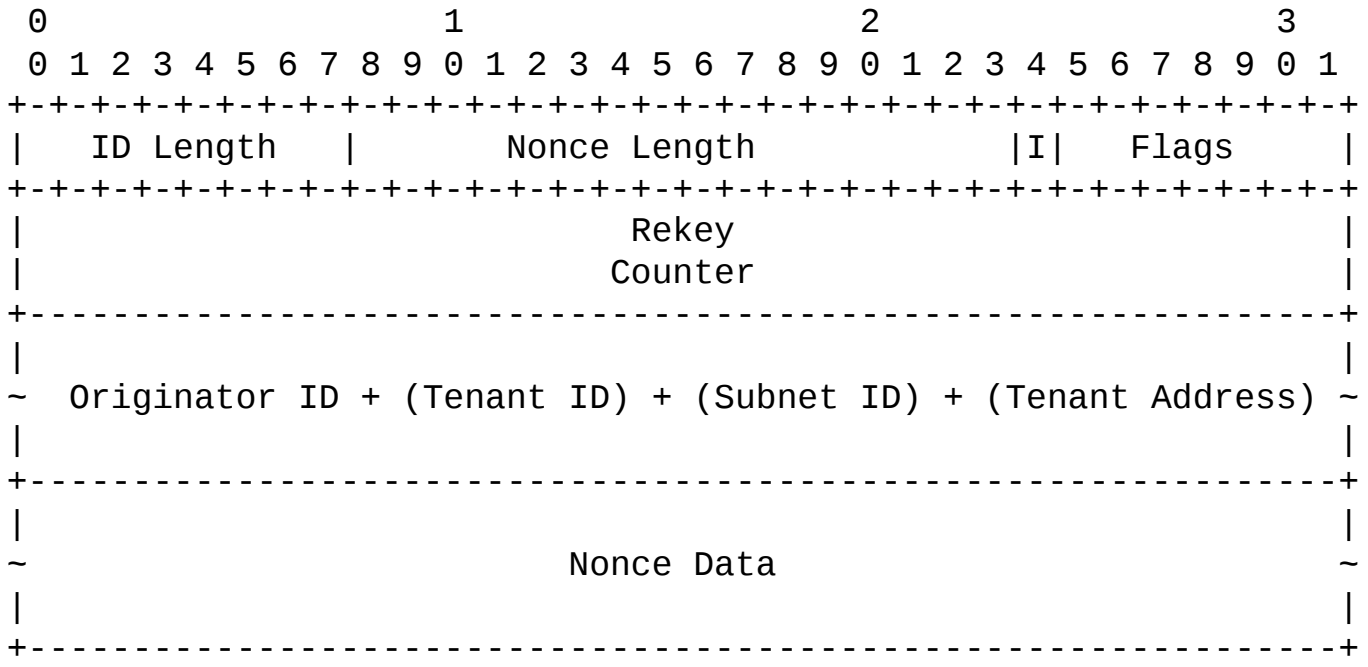

Figure 5: The Base DIM Sub-TLV

Key Exchange Sub-TLV

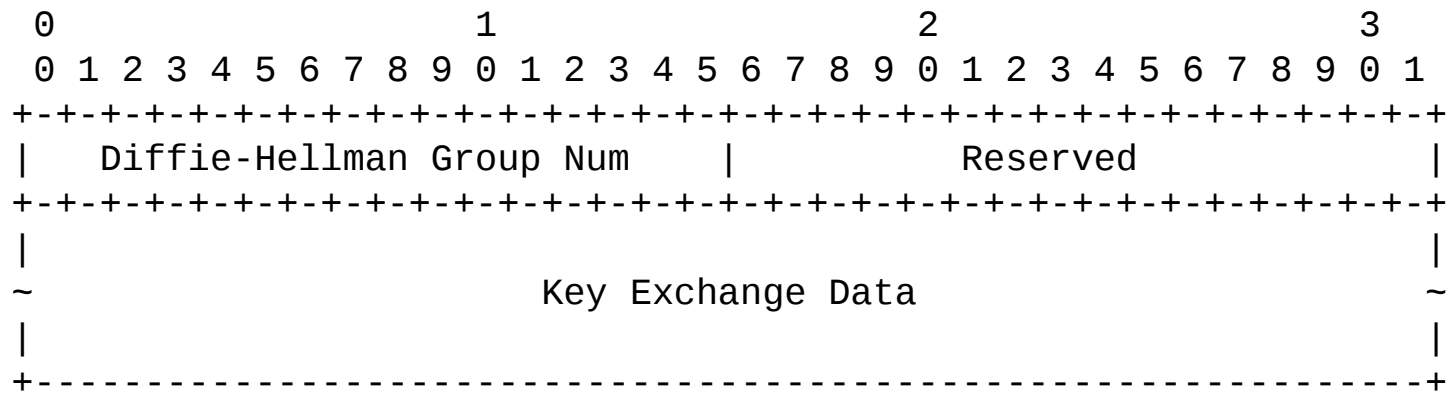

Figure 6: Key Exchange Sub-TLV

SA Proposal Sub-TLV

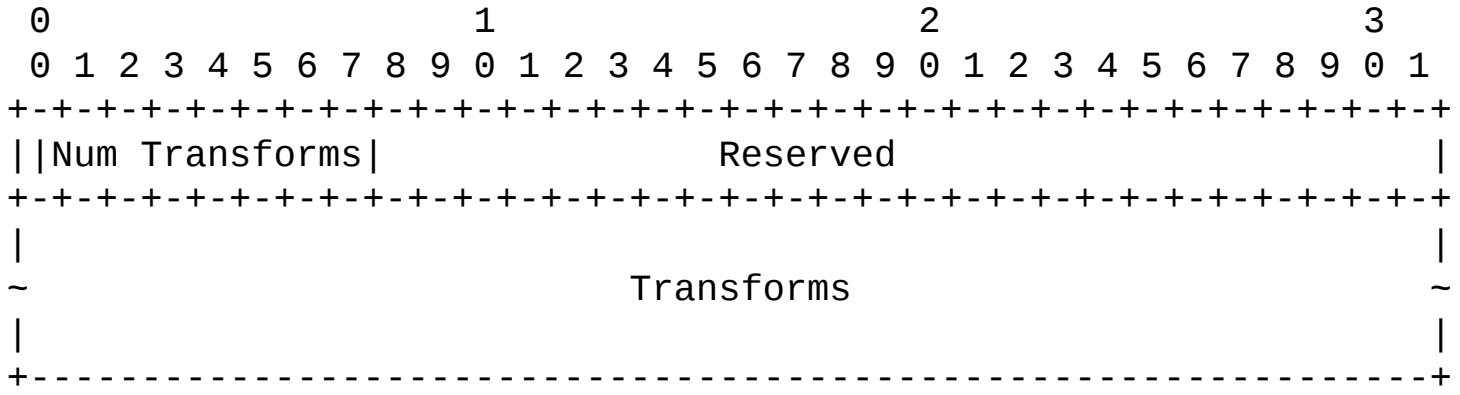

Figure 8: ESP SA Proposals Sub-TLV

Transform Substructure Sub-TLV

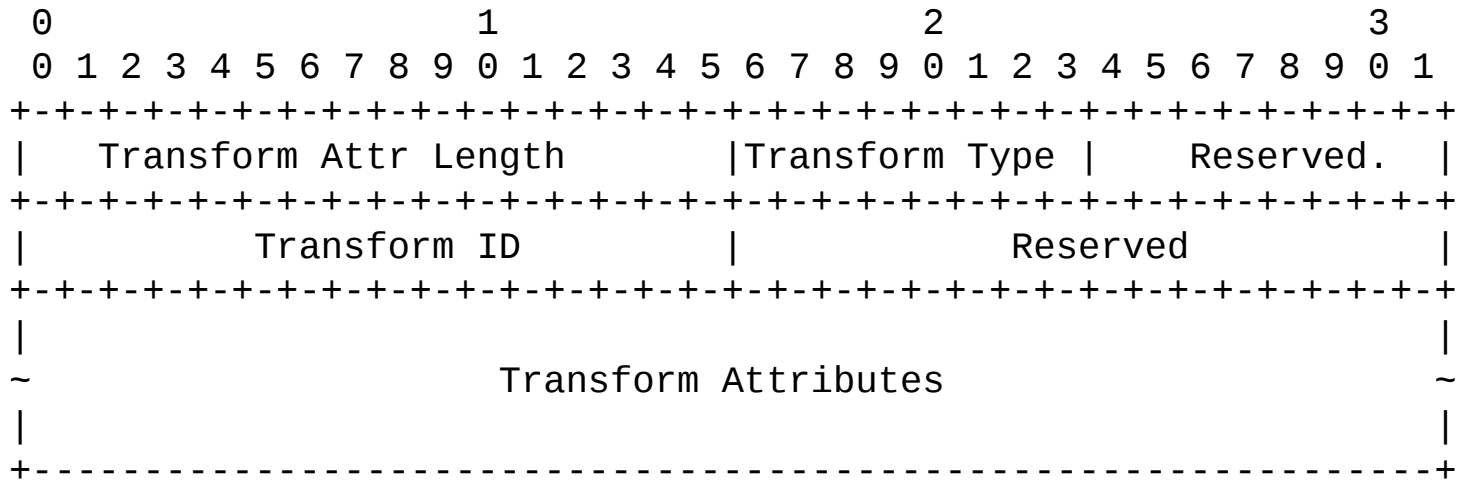

Figure 9: Transform Substructure Sub-TLV

Next Step

- Solicit more input
- Publish Rev02
- Request for WG adoption after Rev02 publication

THANK YOU!