simple VPN solution using Multi-point SA

draft-yamaya-ipsecme-mpsa-01

Arifumi Yamaya, Ken Ueki, Tomoki Murai

Furukawa Network Solution Corp.

Takafumi Ohya

NTT West Corp.

Tomohiro Yamagata

KDDI Corporation

Motivation

- Low-cost VPN solution for a large scale VPN service, that requires
  - Full Mesh topology
  - Many communications simultaneously
  - Low-cost CPE
  - Minimum configuration at CPE
  - Peer address resolution (can be done with other existing protocol, such as BGP)
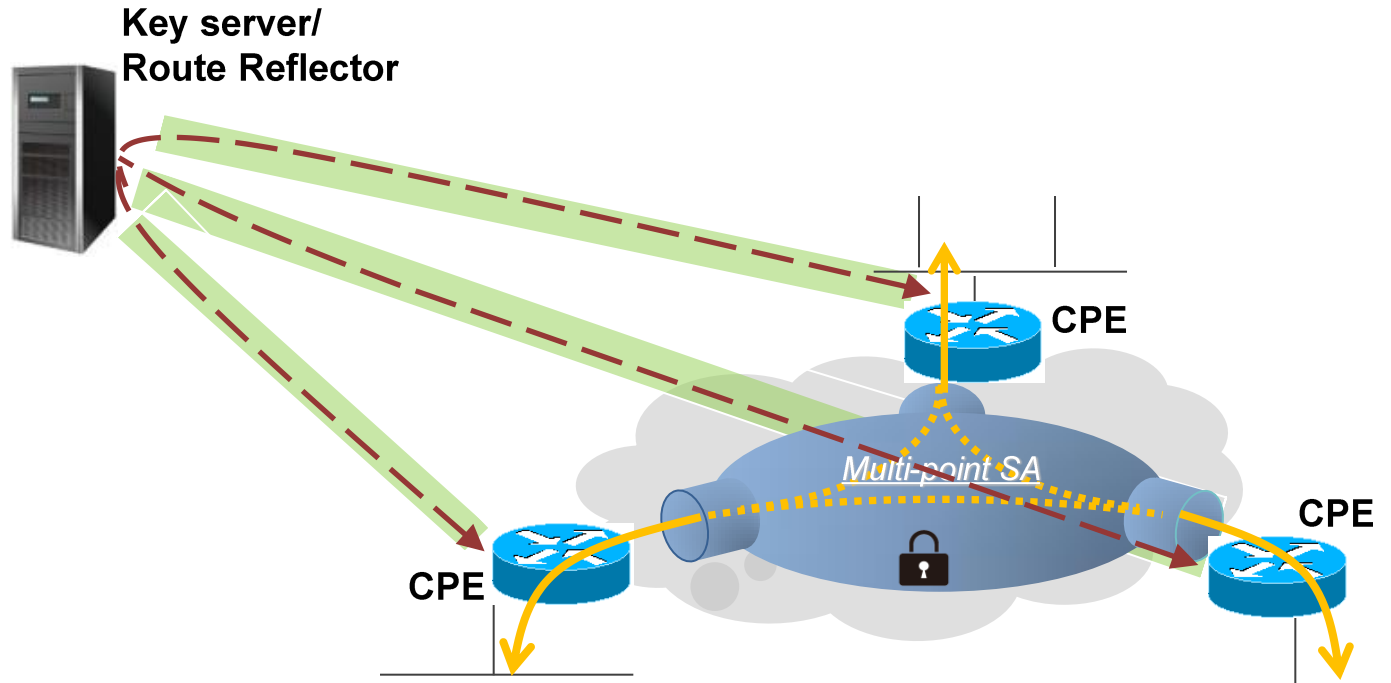
Use case

- Large scale VPN service for enterprises provided by a ISP/carrier
  - Many branch-to-branch communications
  - Real-time traffic
- Control/Data plane separation
  - Control plane in could
  - Low-cost CPE as a concentrator of Data plane

Solution
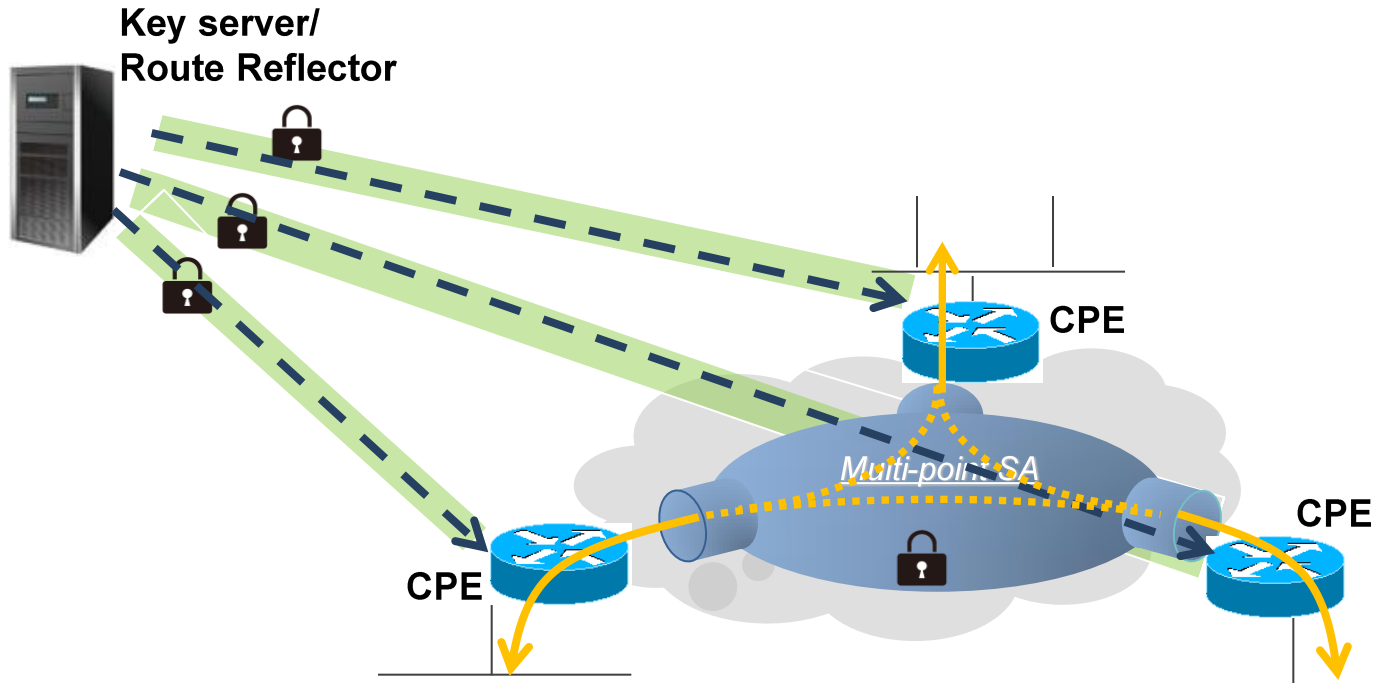
- Multi-point SA is introduced for meshed tunnel network. CPE communicates others with single mpSA
- Key distribution method is implemented to IKEv2

Peer address resolution by BGP

Key server/
Route Reflector

CPE

CPE

CPE

Multi-point SA

- RFC5565 is used for routing on meshed tunnel network. CPEs advertise
  - Route information for route-based VPN
  - Tunnel destination for peer address discovery

Next steps

- Update text
  - Security Considerations
  - Shared SA Pros/Cons
  - Use cases
- Comments and Suggestions are welcome