

IDR Secure VPN discussions

A. Sajassi (Cisco), D. Carrel (Cisco)

IETF 105, July 2019

Montreal

Customer Requirements for Signaling

- Single signaling mechanism based on BGP
- Similar requirements have been asked before for other solutions:
 - Multicast VPN: BGP signaling instead of PIM
 - L2VPN: BGP signaling instead of targeted LDP
- Some Customers are now asking for not only BGP-based signaling but a single AFI/SAFI (EVPN)
- Customers now want the same thing when enabling VPN services with IPsec tunnels

Key Exchange Protocol

- Edge devices have a single BGP session to RR (signaling controller)
- Key exchange uses secure/authenticated BGP signaling channel already established between Edge device and RR
- DH based key exchange done through controller
 - Peers send their DH public values and nonce to controller
 - Controller sends list of all public values to all other peers
 - All peers calculate a unique pairwise secret for each other peer

Key Exchange Protocol – Cont.

- Re-key synchronization allows frequent re-keying with forward secrecy
- RR provides optimized distribution of keys
- Simultaneous re-key synchronization regardless of path delays

Singling Scale Example

- In IKE you need to send at least 6 message between two peers
- With 10K peers, we'll have 600,000,000 messages network wide per hour
- With RR, every peer sends a single message to RR
- RR can aggregate before sending
 - $20K * N$; where re-key-interval/agg-interval
 - $20K * (60/5) = 100K$

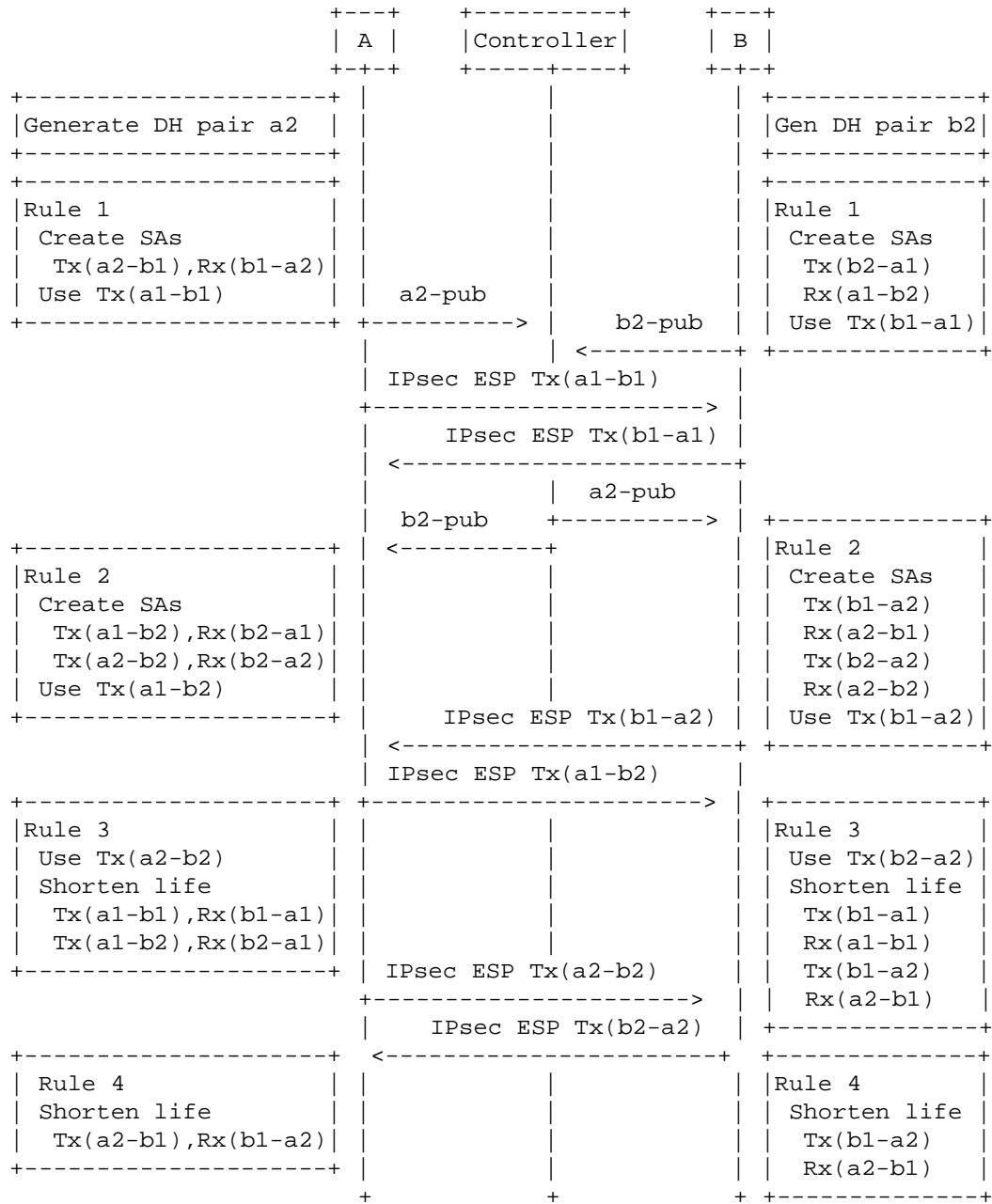


Figure 4: Simultaneous IPsec Device Rekey Protocol Flow