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

```
                      +---+    +----------+     +---+
                      | A |    |Controller|     | B |
                      +-+-+    +-----+----+     +-+-+
+---------------------+ |            |            | +--------------+
|Generate DH pair a2  | |            |            | |Gen DH pair b2|
+---------------------+ |            |            | +--------------+
+---------------------+ |            |            | +--------------+
|Rule 1               | |            |            | |Rule 1        |
| Create SAs          | |            |            | | Create SAs   |
|  Tx(a2-b1),Rx(b1-a2)| |            |            | |  Tx(b2-a1)   |
| Use Tx(a1-b1)       | |  a2-pub    |            | |  Rx(a1-b2)   |
+---------------------+ +----------> |    b2-pub  | | Use Tx(b1-a1)|
                        |            | <----------+ +--------------+
                        | IPsec ESP Tx(a1-b1)     |
                        +----------------------> |
                        |     IPsec ESP Tx(b1-a1) |
                        | <-----------------------+
                        |            |  a2-pub    |
                        |  b2-pub    +----------> | +--------------+
+---------------------+ | <----------+            | |Rule 2        |
|Rule 2               | |            |            | | Create SAs   |
| Create SAs          | |            |            | |  Tx(b1-a2)   |
|  Tx(a1-b2),Rx(b2-a1)| |            |            | |  Rx(a2-b1)   |
|  Tx(a2-b2),Rx(b2-a2)| |            |            | |  Tx(b2-a2)   |
| Use Tx(a1-b2)       | |            |            | |  Rx(a2-b2)   |
+---------------------+ |     IPsec ESP Tx(b1-a2) | | Use Tx(b1-a2)|
                        | <-----------------------+ +--------------+
                        | IPsec ESP Tx(a1-b2)     |
+---------------------+ +----------------------> | +--------------+
|Rule 3               | |            |            | |Rule 3        |
| Use Tx(a2-b2)       | |            |            | | Use Tx(b2-a2)|
| Shorten life        | |            |            | | Shorten life |
|  Tx(a1-b1),Rx(b1-a1)| |            |            | |  Tx(b1-a1)   |
|  Tx(a1-b2),Rx(b2-a1)| |            |            | |  Rx(a1-b1)   |
+---------------------+ | IPsec ESP Tx(a2-b2)     | |  Tx(b1-a2)   |
                        +---------------------->  | |  Rx(a2-b1)   |
                        |    IPsec ESP Tx(b2-a2)  | +--------------+
+---------------------+  <----------------------+  +--------------+
| Rule 4              | |            |            | |Rule 4        |
| Shorten life        | |            |            | | Shorten life |
|  Tx(a2-b1),Rx(b1-a2)| |            |            | |  Tx(b1-a2)   |
+---------------------+ |            |            | |  Rx(a2-b1)   |
                        +            +            + +--------------+
```

Figure 4: Simultaneous IPsec Device Rekey Protocol Flow