Synchronization of IKEv2 windows between IKEv2 Peers

Kalyani Garigipati
(Cisco Systems)

Agenda

- **Problem Statement**
- **Solutions**

Problem Statement

- IKEv2 windowing mandates that the sender window does not move until the oldest message sent from one peer to another is acknowledged.
- Loss of even a single packet leads to repeated retransmissions followed by an IKE SA teardown if the retransmissions are unacknowledged.
- De-synchronization of windows between sender and receiver of IKEv2 messages can happen, more so in high availability topologies.
- Recovery from window de-synchronization is not possible in HA topologies since stand by device does not have the actual message Id range

Problem Statement (Contd)

- In case of HA, the message window needs to be updated from the active to the standby. Ideally the updating should happen after each packet is sent or received.

- Periodic synchronization of IKEv2 message window (rather than per-packet) is more desirable to make the HA updates less chatty.

- However, this can lead to message window de-synchronization between the new active device and the peer.

Solution 1 - Periodic or more relaxed updates.

- Relax the message window requirement and accept packets below and above the current window within configurable limits.

- Possible Impact
  - Violation of the IKEv2 RFC
  - Can lead to replay attacks, where older – previously sent packets are replayed.

Solution 2 – New Window-Sync Exchange between Peers.

- Introduction of a new exchange type that allows two peers to exchange and synchronize window state between peers.
- Window-sync exchange gets triggered when a device detects that it is out of sync with it's peer.
- Window-sync exchange is a request-response, where each peer declares it's send and receive windows and eventually both peers synchronize to the higher message-id.
- Rough draft was earlier proposed in ietf with the problem statement
- New Draft to be published soon with changes as proposed here …