redhat.

draft-ietf—ipsecme-ikev2-sa-ts-payloads-opts

IETF-110, IPsecME,
March, 2021

Paul Wouters, RHEL Security

History

- https://tools.ietf.org/html/draft-kampati-ipsecme-ikev2-sa-ts-payloads-opt-02
- Not my draft, work done by Kampti & Bharath of Huawei
  - Reduce bytes sent during IKE/IPsec rekey
- Libreswan is very interested in implementing this
- draft is expired but will be resubmitted this week
- IPR situation was unclear but now resolved
  - Standard IPR claim

Change from regular rekeying

- Negotiate support via Notify in IKE_AUTH
  - N(MINIMAL_REKEY_SUPPORTED)
- During REKEY
  - Omit SA and TS payloads
  - Send N(SA_UNCHANGED) with new SPI
  - Send Nonce / KE as normal if PFS
  - Calculate key from KDF as normal
  - Assume all crypto algos / traffic selector remain identical

Changes needed (according to Paul)

- Remove text about changing cryptographic algorithms
  - This is not allowed in IKEv2
- Remove text for rekey when ACL changed
  - Only way is to delete all SA's and start from scratch
- N(SA_TS_UNCHANGED) must also send old SPI for Child SA
  - This is normally sent inside SA payload
- Clarify PFS