draft-pwouters-ipsecme-multi-sa-performance

Goal of the draft

- Increase performance of IPsec
  - Setup regular Child SA, signal support in IKE via NOTIFY
  - Additionally, trigger ACQUIREs per CPU
    - Negotiate additional Child SAs with same Traffic Selectors with CPU id in Notify for “pinning”
- Multiple identical Child SAs already possible, but implementations often see these as replacement SAs.

Status

- 00 draft included support for multi CPUs and QoS
- 01 draft removed QoS support, removed SA count negotiation
  - No further changes in 1.5 years – stable code

- Implemented IPsec code for Linux kernel
- Implemented IKEv2 code in strongSwan and Libreswan

Performance numbers

- Using bare metal with Intel i40e cards
- In forwarding mode (gateway to gateway, not host to host)
- Linux 5.x using XFRM

- Using traditional IPsec: 3.5 gbps
- Using 8 per-CPU Child SAs: 27 gbps

Need standardization for per-CPU capability

- Please (re)read draft-pwouters-multi-sa-performance
- If you strongly object to assigning two NOTIFY payloads, please say so on the ipsec list.
- If you like performance, ask chairs for WG adoption call
- Linux kernel code is waiting on this to merge in per-cpu code.
- strongSwan and Libreswan waiting on kernel code before merging