IKEv2 Multi SA

IETF-110, IPsecME,
March, 2021

Paul Wouters, RHEL Security
Resolving limitations

• Give implementation advise on how to handle multiple IPsec SA’s with identical Traffic Selectors


• Install multiple IPsec SA - one per CPU

• Two new NOTIFY payloads for IPsec SA
  • NUM_QUEUES(max)
  • QUEUE_INFO(opaque)
Benchmarks

- pCPU max 22.3 Gbps
- One SA max 3.9 Gbps
- clear text 34.4 Gbps
Changed in -01

- NUM_QUEUES(minimum) – takes one argument instead of two
- Signal CPU identifier send via QUEUE_INFO
  - Does not need to be the actual hardware CPUID
- Readability improvements
RSS for ESP is rarely supported

- RSS usually only supports UDP/TCP port hashing selector
- We want to use UDP encapsulation so RSS for UDP can be used
- But multiple Child SAs would all use the same UDP port
  - We would like Child SAs on different source ports
  - Without affecting IKEv2 channel
  - OS does not always make that easy
  - Can’t negotiate source port, because of NAT
  - How to do NAT port updates?
Suitable as WG item?

- Solves a real world problem (performance)
- We have running code
- We have measured positive results (with specific hardware)
- Solving the UDP source port issue would make this work on all existing (virtual and real) network cards
- Please adopt 😊