IPsec Performance of Per-CPU IPsec Security Associations (RFC 9611)

IETF 123 - Hackathon

Saturday 19th + Sunday 20th July

Madrid

I E T F

Our Goal

- **Data centers** protect traffic between machines using IPsec.
- **RFC 9611** was defined to support the negotiation of multiple Child Security Associations (SAs) with the same Traffic Selectors used on different resources, such as CPUs, to improve performance.

```
Internet Engineering Task Force (IETF)                         A. Antony
Request for Comments: 9611                                       secunet
Category: Standards Track                                     T. Brunner
ISSN: 2070-1721                                                 codelabs
                                                             S. Klassert
                                                                 secunet
                                                              P. Wouters
                                                                   Aiven
                                                               July 2024

      Internet Key Exchange Protocol Version 2 (IKEv2) Support for
             Per-Resource Child Security Associations (SAs)

Abstract

   In order to increase the bandwidth of IPsec traffic between peers,
   this document defines one Notify Message Status Types and one Notify
   Message Error Types payload for the Internet Key Exchange Protocol
   Version 2 (IKEv2) to support the negotiation of multiple Child
   Security Associations (SAs) with the same Traffic Selectors used on
   different resources, such as CPUs.
```

[Internet Key Exchange Protocol Version 2 (IKEv2) Support for Per-Resource Child Security Associations (SAs)]

The Testbed

- Big thanks to

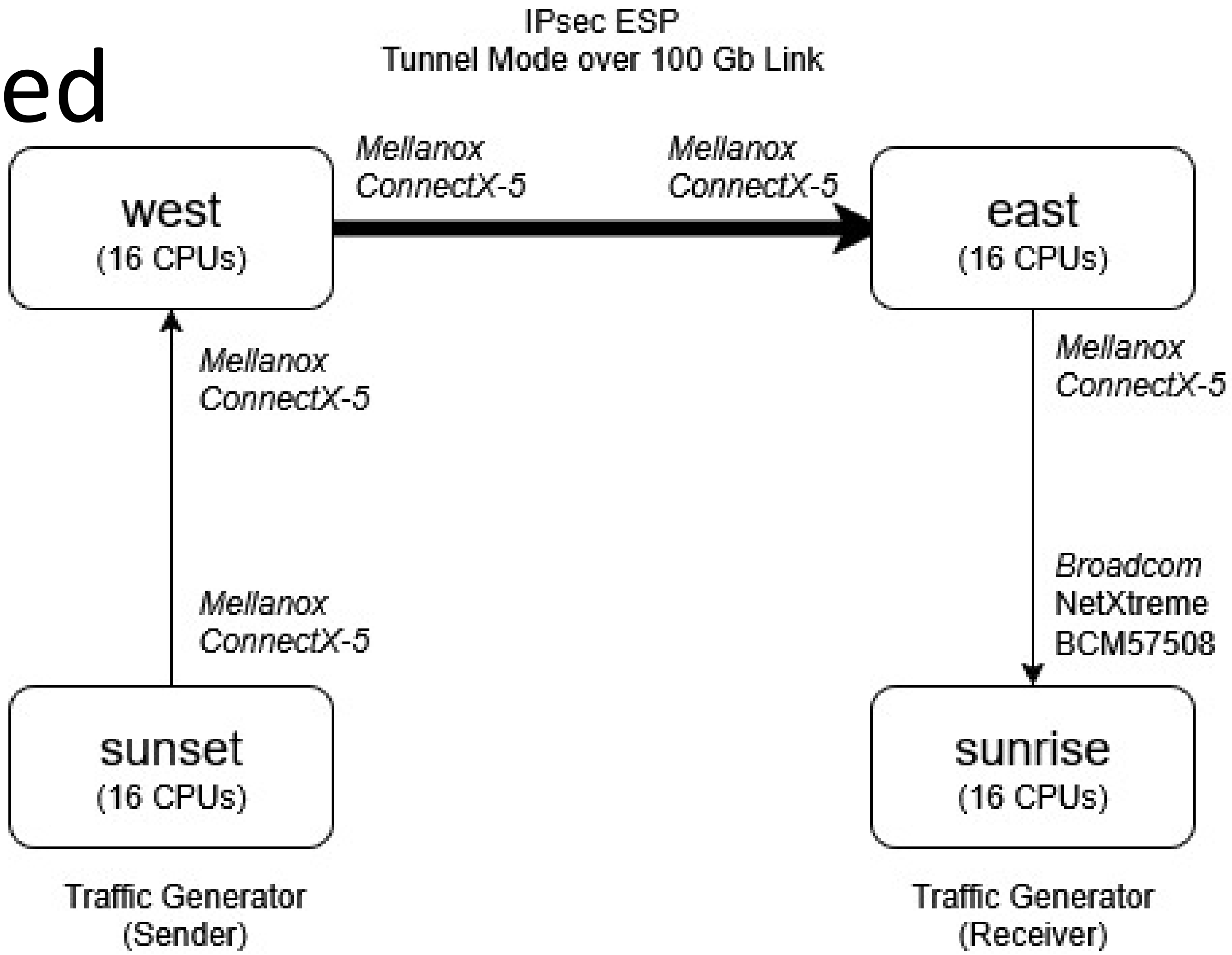
  Paul Wouters

  and

  Tatu Ylonen

  for their

  hardware.



What got done

- Latest Strongswan version with Linux kernel 6.14 using iperf3 & neper. Perf for debugging.
- Testbed configuration with the following tests:
  - Unencrypted traffic (UDP/TCP)
  - Encrypted UDP/TCP traffic without per-CPU feature using a single IPsec SA
  - Encrypted UDP/TCP with per-CPU feature using different number of CPUs.

What we learned

- Per-CPU SAs offer a noticable performance benefit.
- A number of parameters influence the gained benefits and require fine-tuning.
- Pinning tasks to CPUs and configuring Receiver Side Scaling (RSS) and driver config widely affected performance.
- Hardware capabilities like offloading of packets to networking cards vary and require special considerations.
- It took us longer than expected to produce results!
- For the details come to the IPSECME WG meeting.

Our Team

Team members:

- Hannes Tschofenig
- Kai Jansen
- Steffen Klassert
- Tuomo Soini
- Antony Antony
- Tobias Brunner
- Valery Smyslov
- Tero Kivinen
- Christian Hopps
- Simo Soini
- Paul Wouters