Software-Defined Networking (SDN)-based IPsec Flow Protection
(draft-abad-i2nsf-sdn-ipsec-flow-protection-03)

Presenter: Gabriel López-Millán
Rafael Marín-López
(University of Murcia)
SDN-based IPsec: Objectives

- To describe the **architecture** for the SDN-based IPsec management to allow the establishment and management of IPsec security associations from a central point.
- To define (so far) the **NSF facing interfaces** required to manage and monitor the IPsec SAs in the NSF from a Security Controller.
  - YANG models are defined for configuration and state data for IPsec management.
Reminder: Two cases

• Case 1) The NSF implements IKE and the IPsec databases: SPD, SAD, and PAD.
  – The Security Controller is in charge of provisioning the NSF with the required information to IKE, the SPD and the PAD.

• Case 2) The NSF only implements the IPsec databases (no IKE implementation).
  – The Security Controller will provide the required parameters to create valid entries in the SPD and the SAD into the NSF.
  – The NSF will have only support for IPsec while automated key management functionality is moved to the controller.
Update (Changes in 03)

- This drafts focuses on: gateway-to-gateway and host-to-host scenarios.
  - Host-to-gateway (roadwarrior) scenario is TBD.
- Improved Case 1 vs Case 2 discussion following comments received.
- It provides YANG configuration data models
  - Case 1 requires IKEv2, SPD and PAD models
  - Case 2 requires SPD and SAD models
  - A single YANG file to represent both cases
    - part of the models are selectively “activated” depending on YANG features (if-feature)
Update- YANG models

• SPD, SAD, PAD models follow the information gathered from RFC 4301
• IKEv2 model has been obtained from the reading of RFC 7296 and using as reference open source implementations (strongswan, libreswan, …)
• Expert review would be appreciated
Update – Implementation notes

• Proof-of-concept
  – NETCONF: southbound protocol
    • Netopeer implementation
    • YANG model
  – Host-to-host and gw-to-gw
  – Case 1, NSF:
    • Strongswan for the IKE implementation (IKE and PAD)
    • VICI API
  – Case 2, NSF:
    • PF_KEYv2 (RFC 2367) for SAD
    • [I-D.pfkey-spd] for SPD
    • XFRM for SAD and SPD (Linux systems)
YANG Model Trees
Update - SPD model (tree)
Update - SAD model (tree)
Update - PAD model (tree)
Update - IKE model (tree)