Software-Defined Networking (SDN)-based IPsec Flow Protection
(draft-abad-i2nsf-sdn-ipsec-flow-protection-00)

Rafael Marín-López
Gabriel López-Millán
(University of Murcia)
Introduction

• IPsec management (e.g. policies) is manually configured in the network devices.
  – This makes the IPsec security association (SA) management difficult
  – generates a lack of flexibility, specially if the number of security policies and SAs to handle is high.

• Software-Defined Networking (SDN) is an architecture that enables users to directly program, orchestrate, control and manage network resources through software

• **SDN-based management of IPsec SAs.**
IPsec: Overview

- IPsec protection: AH and/or ESP.
- IPsec separates protection of the IP packets from the key management procedures.
- IPsec manages three databases:
  - Security Policy Database (SPD)
  - Security Association Database (SAD)
  - Peer Authorization Database (PAD)
- A default key management protocol is the Internet Key Exchange (IKE)
- Proposal: a **centralized security controller** is in charge of **key management procedures** in several flow-based NSF s that implements IPsec.
Case 1: IKE/IPsec in the NSF
Case 2: IPsec (no IKE) in the NSF
Example: NSF-to-NSF


From HQ A: NSF1 IKE/IPsec(SPD/SAD/PAD)  \(\text{NSF2 IKE/IPsec(SPD/SAD/PAD)\rangle}\)  To BO
Abstract Interface

• Applicable to NSF Facing Interface.
• To manage SAD: RFC 2367 (PF_KEYv2)
  – SADB_ADD, SADB_DELETE, SADB_GET, SADB_ACQUIRE, SADB_EXPIRE, SADB_FLUSH, ...
• To manage SPD: extension to PF_KEYv2
  – SADB_X_SPDADD, SADB_X_SPDDELETE, SADB_X_SPDACQUIRE, SADB_X_SPDFLUSH
• Pending: to manage IKE implementation.
Data model

- On-going work.
- It is required to model:
  - SPD
  - SAD
  - PAD
  - IKE
Software-Defined Networking (SDN)-based IPsec Flow Protection
(draft-abad-i2nsf-sdn-ipsec-flow-protection-00)

Rafael Marín-López
Gabriel López-Millán
(University of Murcia)