Software-Defined Networking (SDN)-based IPsec Flow Protection
(draft-ietf-i2nsf-sdn-ipsec-flow-protection-05)

Rafael Marín-López
Gabriel López-Millán (Presenter)
(University of Murcia)
Fernando Pereñiguez-García
(University Defense Center)
SDN-based IPsec

• Main changes from v03 to v04
  – Changed the name of the cases
    • Case 1 → **IKE case**: When IKEv2 is in the NSF
    • Case 2 → **IKE-less case**: When the NSF does not implement IKEv2
  – YANG model divided in three parts:
    • **ietf-ipsec-common**
      – Contains common typedef and grouping for both IKE and IKE-less cases.
    • **ietf-ipsec-ike**
      – Contains specific configuration for IKE case (IKE, PAD, SPD)
    • **ietf-ipsec-ikeless**
      – Contains specific configuration for IKE-less case (SPD, SAD)
Changes from v04 to v05 (1/5)

• YANG doctors’ review (Martin’s)
  – Descriptions in model improved
  – Format review

• Paul Wouters’ comments and Tero’s comments
  – Thanks again for your in deep review

• IKE-less notifications (expire, acquire, etc.) have been simplified since most of the information contained in the previous version is already handled by the SC
Changes from v04 to v05 (2/5)

• State data has been simplified.
  – IKE case, most of the information is related with IKE and not with the specific details about IPsec SAs that IKE handles (IKE can abstract this information from the SC)

• Security section improved to discuss about the default IPsec policies that should be in the NSF when it starts before contacting with the SC
  – IPsec policies required to allow traffic SC ↔ NSF

• Subsection 5.3.1 (rekeying process) improved

• New subsection 5.3.4 about NSF discovery by the SC
Changes from v04 to v05 (3/5)

• crypto-algorithms:
  – We have used a simple approach by including an integer and adding text pointing the IANA in reference clause
  – Under discusión in the Netconf WG

typedef encryption-algorithm-type {
    type uint32; \→ //Need to be replaced to uint16
    description
      "The encryption algorithm is specified with a 32-bit number extracted from IANA Registry. The acceptable values MUST follow the requirement levels for encryption algorithms for ESP and IKEv2.";
    reference
      "IANA Registry- Transform Type 1 – Encryption Algorithm Transform IDs. RFC 8221 – Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH) and RFC 8247 - Algorithm Implementation Requirements and Usage Guidance for the Internet Ke Exchange Protocol Version 2 (IKEv2).";
}
Changes from v04 to v05 (4/5)

• We have included three additional Annexes with examples about the usage of YANG models
  – IKE case, tunnel mode (gateway-to-gateway) with X.509 certificate authentication
  – IKE-less case, transport mode (host-to-host) with PSK authentication
  – Notifications: sadb-expire, sadb-acquire, sadb-seq-overflow and sadb-bad-spi
Changes from v04 to v05 (5/5)

• Models validation:
  – pyang --ietf --max-line-length 69 -f tree --lint --lint-ensure-hyphenated-names ietf-ipsec-xxx.yang → OK

• Models installation:
  – sysrepopctl --install --yang=ietf-ipsec-xxx.yang → OK

• Examples validation:
  – yanglint ietf-ipsec-ikeless.yang ikeless-example.xml → OK
  – yanglint ietf-ipsec-ike.yang ike-example.xml → OK
  – yanglint -t notif ietf-ipsec-ikeless.yang notif-ex.xml → OK
Next steps

• Inmediate submission v06 with the last minor changes
• Request publication to IESG
Software-Defined Networking (SDN)-based IPsec Flow Protection
(draft-ietf-i2nsf-sdn-ipsec-flow-protection-05)

Rafael Marín-López
Gabriel López-Millán (Presenter)
(University of Murcia)
Fernando Pereñiguez-García
(University Defense Center)