Software-Defined Networking (SDN)-based IPsec Flow Protection

(draft-ietf-i2nsf-sdn-ipsec-flow-protection-**04**)

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

SDN-based IPsec

- **Architecture** for the SDN-based IPsec management to centralize the establishment and management of IPsec security associations
- We have 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
- Host-to-Host and Gateway-to-Gateway
  - Road-warrior is not considered in the current version

YANG model update

- Many changes derived from Paul Wouter's review (see e-mails in the mailing list)
- We have divided the original YANG model 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)

ietf-ipsec-common

- Typedef and grouping common to IKE case and IKE less case:
  - **`typedef integrity-algorithm-t {type ct:mac-algorithm-ref; }`**
    - Reference to netconf-crypto-types yang model
  - **`typedef lifetime-action`** (terminate-clear, terminate-hold, replace)
  - **`typedef ipsec-traffic-direction`**
    - INBOUND and OUTBOUND only
  - **`spd-mark`** has been removed
  - **`grouping lifetime`** (name of leaf nodes changed, now using yang:timestamp type)
  - **`selector-grouping`**: now a traffic selector only allows left and right subnet (instead of a list)
  - **`container processing-info`**: clarified AEAD support

ietf-ipsec-ike (1/2)

- **typedef type-autostartup** (ADD, ON-DEMAND, START)
- **typedef pfs-group** (added)
- **typedef auth-method-type** (pre-shared, eap, digital-signature, null)
- **container auth-method** (eap, pre-shared, digital-signature)
- **import ietf-crypto-types**

```
typedef signature-algorithm-t {
    type ct:signature-algorithm-ref…
```

ietf-ipsec-ike (2/2)

- **grouping ike-proposal** (added)
  - **container ike-sa-lifetime-hard** (added, no action)
  - **container ike-sa-lifetime-soft**
  - **leaf half-open-ike-sa-timer**
  - **leaf half-open-ike-sa-cookie-threshold**
- **container ikev2**
  - **container pad**
  - **list ike-conn-entry** (list of SPD entries)
    - **container list child-sas** (only SPIs for now)

ietf-ipsec-ikeless

- **`container sad-lifetime-hard`** (no action)
- Simplified
  - **`container spd {...}`**
  - **`container sad {...}`**
- Notifications
  - **`sadb_expire`**
  - **`sadb_acquire`**
  - **`sadb_bad-spi`**

Open Questions (1/2)

- **General questions**
  - Should we simplify SPD model? 1 policy with a TS vs 1 SPD with multiple TSs, as RFC4301 assumes
  - "*Is there support for multiple TSi/TSr generating a list of spd's in a single Child SA?*"
  - Should we remove AH support? We are ok removing it
  - "*esp-encap, missing port entry*". **`grouping encap`** already has *sport/dport*. What are we missing?
  - Removing a name associated to a policy? (RFC 4301 specifies a name)
  - Should we include *road-warrior* support or **generate a new I-D**?

Open Questions (2/2)

- **IKE case**
  - SPD is defined inside **`ike-conn-entry`** but PAD is outside. Should we have the SPD at the same level as PAD?
  - SPD entry lifetime. We have a notification **`spdb_expire`** in IKE-less. How about IKE case?
  - We only provide SPIs as state data related with IPsec SAs. Does the Controller need to know anything about the IPsec SAs?
- **IKE-less**
  - Relations between entries in both sides is posible with the traffic selectors→ Should we add a explicit pointer? (i.e. **reqid**)

Next Steps

- We kindly ask the current reviewers whether they are fine with the changes and then…
- We think the document is ready for the WGLC.

Software-Defined Networking (SDN)-based IPsec Flow Protection

(draft-ietf-i2nsf-sdn-ipsec-flow-protection-04)

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