I2NSF Security Controller-Facing Interface YANG Data Model for Cross-Domain Security Parameter Exchange

March 30th, 2023

Jeonghyeon (Joshua) Kim, Jaehoon (Paul) Jeong, Patrick Lingga, Susan Hares, and Rafa Marin-Lopez

Email: {jeonghyeon12, pauljeong, patricklink}@skku.edu, shares@ndzh.com, rafa@um.es
Updates of Security Controller-Facing Interface (SFI)

• Updates:

• An update on the Security Controller-Facing Interface information model

• An update on the Security Controller-Facing Interface peer-to-peer use case

• An update on the Security Controller-Facing Interface hierarchical use case
Major Update of Security Controller-Facing Interface (1/3)

- Change of the information model of SFI
Major Update of Security Controller-Facing Interface (2/3)

Old:

3.1.1. Use Case of Peer-to-Peer Security Controllers

Old:

- Addition of NSFs’ capability negotiation process before starting IPsec parameter negotiation

New:

1. Security Policy

New:

- Deliver translated security policy
- Reply OK
- Deliver Translated Security Policy
- Reply OK
- IPsec Parameter Negotiation
- Service Function Chaining with IPsec SAs
Major Update of Security Controller-Facing Interface (3/3)

- Addition of NSFs capability negotiation process before starting IPsec parameter negotiation
Next Step

• This draft introduces the Security Controller-Facing Interface for cross-domain IPsec flow protection.

• It suggests an I2NSF expansion architecture and use cases (i.e., peer-to-peer and hierarchical architectures)

• We will make a YANG data model for SFI before IETF-117 San Francisco.

• How to proceed with its standardization in IETF?
  ✔ Independent Submission or Another WG (e.g., OPSAWG)?