Information Model for Consumer-Facing Interface to Security Controller
(draft-kumar-i2nsf-client-facing-interface-im-05)

IETF 101, London
March 21, 2018

Rakesh Kumar, Anil Lohiya, Dave Qi, Nabil Bitar, Senad Palislamovic, Liang Xia, and Jaehoon (Paul) Jeong [Presenter]
Updates from the Previous Version

• The Previous Version:
  – draft-kumar-i2nsf-client-facing-interface-im-04

• Changes from the Previous Version
  – In Section 3.2, the description of Match-Direction in Condition Sub-Model was corrected.
  – References are updated.
Description Update of Match-Direction in Condition Sub-Model

• Old Text

This field identifies the match criteria used to evaluate whether the specified action needs to be taken or not. This could be either a Policy-Endpoint-Group identifying an Application set or a set of traffic rules.

• New Text

This field identifies whether the match criteria is to be evaluated for both directions or only one direction of the traffic with a default of allowing the other direction for stateful match conditions. This is optional and by default a rule should apply to both directions.
Construction of This Draft

- Information Model (IM) Requirements (draft-ietf-i2nsf-client-facing-interface-req)
  - Derive a detailed information model

- Capability Information Model (draft-ietf-i2nsf-capability)
  - Form the basic structure (ECA model) of the information model through inheritance and extension

- Consumer-Facing Interface Information Model

**Note:** Construction of the Policy IM to be aligned with ECA model for high-level policy
Information Model Design

• Information Model
  – To identify a set of managed objects (resources)
  – To define relationship among these objects
  – To define Consumer-Facing Interface with objects and relationship

• The Corresponding YANG Data Model
  – draft-ietf-i2nsf-consumer-facing-interface-dm-00
Next Steps

• We will refine this draft to
  • Align and Sync with I2NSF capability IM draft: draft-ietf-i2nsf-capability,
  • Extend the IM to accommodate the security policies and threat expression of the open-source security software, such as Suricata, Snort, and STIX (Structured Threat Information Expression), and
  • Proof-of-Concept (POC) of the IM through the implementation of the corresponding YANG Data Model draft: draft-ietf-i2nsf-consumer-facing-interface-dm-00

• Call for WG Adoption
  – Welcome your feedback!