IETF-116

Guidelines for Security Policy Translation in Interface to Network Security Functions

draft-yang-i2nsf-security-policy-translation-14

March 30th, 2023

Jaehoon (Paul) Jeong and **Patrick Lingga**
Sungkyunkwan University
Email: {pauljeong, patricklink}@skku.edu

I E T F

Security Policy Translation Draft

- Within I2NSF Framework, the high-level and low-level security policies are specified by YANG data model [RFC7950] with the delivery using either NETCONF [RFC6241] or RESTCONF [RFC8040].

- The **translation from a high-level** security policy to the corresponding **low-level** security policy will be able to rapidly elevate I2NSF in real-world deployment.

- A rule in a high-level policy can **include a broad target object** (e.g., firewall and web filter).

- This document provides a **guideline** that shows the **relationship and mapping between** the **Consumer-Facing Interface** and **NSF-Facing Interface** YANG data models.

Updates of Security Policy Translation Draft (1/4)

- This version updates the YANG data model and mapping information to follow the latest Consumer-Facing Interface YANG data model.

OLD Data Model:

```
|   +--rw anti-virus
|   |  +--rw exception-files*   string
```

NEW Data Model:

```
|   +--rw anti-virus
|   |  +--rw profile*               string
|   |  +--rw exception-files*       string
```

NEW Guideline:

```
 #anti-virus-condition mapping
   /ietf-i2nsf-cons-facing-interface/i2nsf-cfi-policy/rules/condition
   /anti-virus/profile
     -> mapping: /ietf-i2nsf-nsf-facing-interface/i2nsf-security-policy
                 /rules/condition/anti-virus/profile

   /ietf-i2nsf-cons-facing-interface/i2nsf-cfi-policy/rules/condition
   /anti-virus/exception-files
     -> mapping: /ietf-i2nsf-nsf-facing-interface/i2nsf-security-policy
                 /rules/condition/anti-virus/exception-files
```

Updates of Security Policy Translation Draft (2/4)

OLD Data Model:

```
+--rw geographic-location
   +--rw source*
    -> /i2nsf-cfi-policy/endpoint-groups/location-group/name
   +--rw destination*
    -> /i2nsf-cfi-policy/endpoint-groups/location-group/name
```

NEW Data Model:

```
+--rw geographic-location
   +--rw source
   |  +--rw country? -> /endpoint-groups/location-group/country
   |  +--rw region?  -> /endpoint-groups/location-group/region
   |  +--rw city?    -> /endpoint-groups/location-group/city
   +--rw destination
      +--rw country? -> /endpoint-groups/location-group/country
      +--rw region?  -> /endpoint-groups/location-group/region
      +--rw city?    -> /endpoint-groups/location-group/city
```

NEW Guideline:

```
#geographic-location mapping
/ietf-i2nsf-cons-facing-interface/i2nsf-cfi-policy/rules/condition
/context/geographic-location/source
/("country" and "region" and "city")
  -> reference: /ietf-i2nsf-cons-facing-interface/endpoint-groups
                /location-group/("country" and "region" and "city")
    -> extract: /ietf-i2nsf-cons-facing-interface/endpoint-groups
                /location-group/range-ipv4-address
                /("start" and "end")
      -> mapping: /ietf-i2nsf-nsf-facing-interface
                  /i2nsf-security-policy/rules/condition/ipv4
                  /("source-ipv4-network" or "source-ipv4-range")
    -> extract: /ietf-i2nsf-cons-facing-interface/endpoint-groups
                /location-group/range-ipv6-address
                /("start" and "end")
      -> mapping: /ietf-i2nsf-nsf-facing-interface
                  /i2nsf-security-policy/rules/condition/ipv6
                  /("source-ipv6-network" or "source-ipv6-range")
```

Updates of Security Policy Translation Draft (3/4)

OLD Data Model:

```
|   |  +--rw voice-condition
|   |  |  +--rw source-id*        string
|   |  |  +--rw destination-id*   string
|   |  |  +--rw user-agent*       string
```

NEW Data Model:

```
|   +--rw voice
|   |  +--rw source-id*         -> /endpoint-groups/voice-group/name
|   |  +--rw destination-id*    -> /endpoint-groups/voice-group/name
|   |  +--rw user-agent*        string

...
 +--rw voice-group* [name]
     +--rw name       string
     +--rw sip-id*    inet:uri
```

OLD Guideline:

```
#voice-condition mapping
/consumer-facing/i2nsf-cfi-policy/rules/condition
/voice-condition/source-id
    -> mapping: /nsf-facing/i2nsf-security-policy
                /rules/condition/voice
                /source-voice-id

/consumer-facing/i2nsf-cfi-policy/rules/condition
/voice-condition/destination-id
    -> mapping: /nsf-facing/i2nsf-security-policy
                /rules/condition/voice
                /destination-voice-id
```

NEW Guideline:

```
#voice-condition mapping
/ietf-i2nsf-cons-facing-interface/i2nsf-cfi-policy/rules/condition
/voice/source-id
  -> reference: /ietf-i2nsf-cons-facing-interface/endpoint-groups
                /voice-group/name
    -> extract: /ietf-i2nsf-cons-facing-interface/endpoint-groups
                /voice-group/sip-id
      -> mapping: /ietf-i2nsf-nsf-facing-interface
                  /i2nsf-security-policy/rules/condition/voice
                  /source-voice-id

/ietf-i2nsf-cons-facing-interface/i2nsf-cfi-policy/rules/condition
/voice/destination-id
  -> reference: /ietf-i2nsf-cons-facing-interface/endpoint-groups
                /voice-group/name
    -> extract: /ietf-i2nsf-cons-facing-interface/endpoint-groups
                /voice-group/sip-id
      -> mapping: /ietf-i2nsf-nsf-facing-interface
                  /i2nsf-security-policy/rules/condition/voice
                  /destination-voice-id
```

Updates of Security Policy Translation Draft (4/4)

Added missing Mapping Guideline:

```
#language mapping
/ietf-i2nsf-cons-facing-interface/i2nsf-cfi-policy/language
  -> mapping: /ietf-i2nsf-nsf-facing-interface/i2nsf-security-policy
              /language

#resolution-strategy mapping
/ietf-i2nsf-cons-facing-interface/i2nsf-cfi-policy/resolution-strategy
  -> mapping: /ietf-i2nsf-nsf-facing-interface/i2nsf-security-policy
              /resolution-strategy

#event mapping
/ietf-i2nsf-cons-facing-interface/i2nsf-cfi-policy/rules/event
/system-event
  -> mapping: /ietf-i2nsf-nsf-facing-interface/i2nsf-security-policy
              /rules/event/system-event

/ietf-i2nsf-cons-facing-interface/i2nsf-cfi-policy/rules/event
/system-alarm
  -> mapping: /ietf-i2nsf-nsf-facing-interface/i2nsf-security-policy
              /rules/event/system-alarm

#application mapping
/ietf-i2nsf-cons-facing-interface/i2nsf-cfi-policy/rules/condition
/context/application/protocol
  -> mapping: /ietf-i2nsf-nsf-facing-interface/i2nsf-security-policy
              /rules/condition/context/application/protocol
```

```
#time mapping
/ietf-i2nsf-cons-facing-interface/i2nsf-cfi-policy/
/rules/condition/context/time/period/start-time
  -> mapping: /ietf-i2nsf-nsf-facing-interface/i2nsf-security-policy
              /rules/condition/context/time/period/start-time

/ietf-i2nsf-cons-facing-interface/i2nsf-cfi-policy/
/rules/condition/context/time/period/end-time
  -> mapping: /ietf-i2nsf-nsf-facing-interface/i2nsf-security-policy
              /rules/condition/context/time/period/end-time

#device-type mapping
/ietf-i2nsf-cons-facing-interface/i2nsf-cfi-policy/rules/condition
/context/device-type/device
  -> mapping: /ietf-i2nsf-nsf-facing-interface/i2nsf-security-policy
              /rules/condition/context/device-type/device

#users mapping
/ietf-i2nsf-cons-facing-interface/i2nsf-cfi-policy/rules/condition
/context/users/user/id
  -> mapping: /ietf-i2nsf-nsf-facing-interface/i2nsf-security-policy
              /rules/condition/context/users/user/id

/ietf-i2nsf-cons-facing-interface/i2nsf-cfi-policy/rules/condition
/context/users/group/name
  -> mapping: /ietf-i2nsf-nsf-facing-interface/i2nsf-security-policy
              /rules/condition/context/users/group/name
```

Next Step

- This document purpose is to **help the developer in managing the translation** within I2NSF Framework.

- It suggests an **architecture and procedure as an example** for Security Policy Translator (SPT).

- This draft is **proposed as an informational draft** for I2NSF Framework.

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