I2NSF WG Side Meeting

IETF 106, Singapore

Nov 21, 2019

Organizer: Jaehoon Paul Jeong

Agenda

- I2NSF Hackathon Project Report (Jaehoon Paul Jeong, 5 min)

- I2NSF Data Model Drafts Update (Jaehoon Paul Jeong, 10 min)
  - I2NSF Capability YANG Data Model
  - I2NSF Consumer-Facing Interface YANG Data Model
  - I2NSF Network Security Function-Facing Interface YANG Data Model
  - I2NSF Registration Interface YANG Data Model
  - I2NSF NSF Monitoring YANG Data Model

- Security Policy Translator Draft Update (Chaehong Chung, 5 min)

- Open Discussion: Possible Work Items for I2NSF Rechartering (30 min)

IETF Hackathon Report

IETF 106, Singapore

Nov 21, 2019

Jaehoon (Paul) Jeong

Sungkyunkwan University

Introduction (1/2)

Goals of IETF-106 I2NSF Hackathon

1. Previous Implementation of the I2NSF Framework for NSF in OpenStack Environment with
   ✓Registration Interface via NETCONF/YANG
   ✓Consumer-Facing Interface via RESTCONF/YANG
   ✓NSF-Facing Interface via NETCONF/YANG
   ✓Security Policy Translation in Security Controller

2. I2NSF NSF Monitoring in IETF-106 Hackathon
   ✓NSF Monitoring between NSFs and Security Controller via NETCONF/YANG

Introduction (2/2)

Build Environment

1. OS
   - Ubuntu 18.04 LTS
2. ConfD
   - 6.6 Version
3. OpenStack
   - Mitaka
4. Suricata
   - 3.2.1 RELEASE

I2NSF Framework Project

I2NSF (Interface to Network Security Functions) Framework Project

Champion: Jaehoon Paul Jeong (SKKU)

Professor

- Jaehoon Paul Jeong (SKKU)

Collaborator

- Jong-Hyun Kim (ETRI)

Student

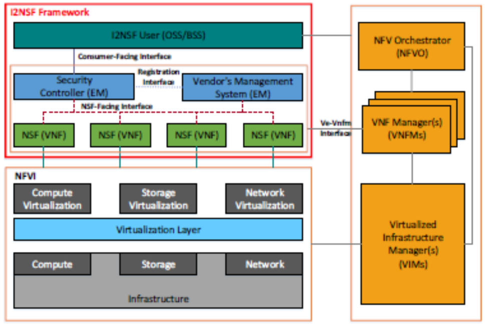
- Chaehong Chung (SKKU)

Participants

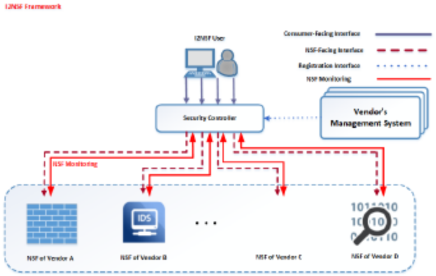
- Yongjoon Joe (LSware)
- Duke Moon (Hansol)

openstack. SURICATA

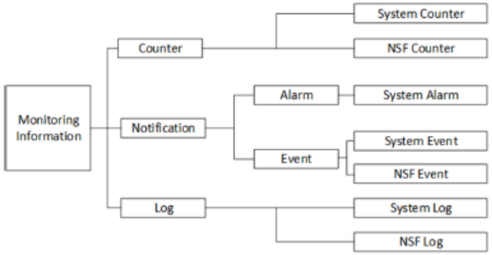
I2NSF Architecture in NFV Reference



Application of I2NSF Monitoring



NSF Monitoring Information Model



Where to get code

- Github – Source Code
  - ✓ https://github.com/ kimjinyong/i2nsf-framework

What to pull down to set up an environment

- OS: Ubuntu 18.04 LTS
- ConfD for NETCONF: 6.6 Version
- OpenStack: Mitaka
- NSF: Suricata

Manual for Operation Process

- Detailed description about operation process in Manual.txt (It can be found in Open Source Project folder.)

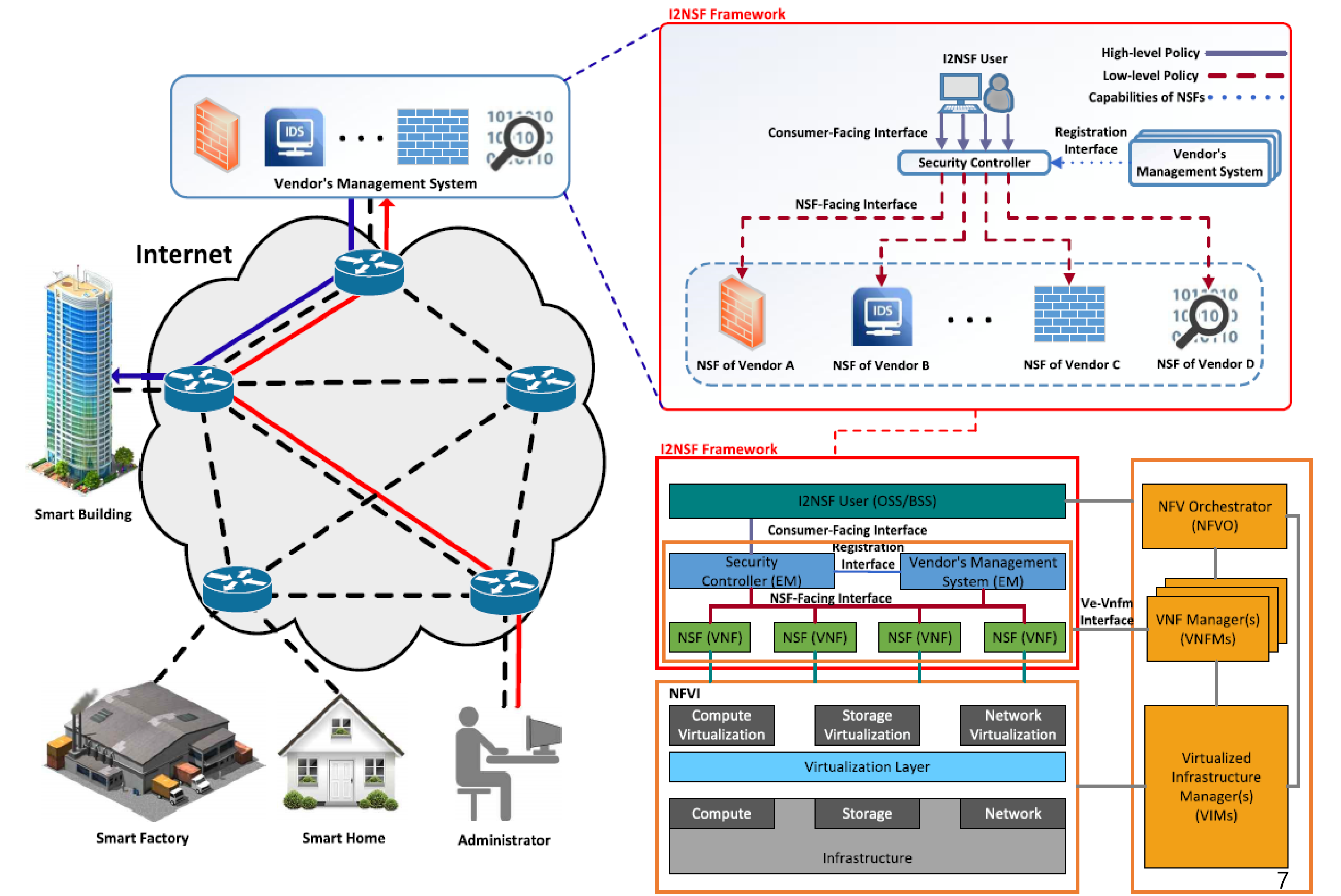
Contents of Implementation

- I2NSF Framework for Network Security Functions (NSFs)
  - ✓ Registration Interface via NETCONF/YANG
  - ✓ NSF-Facing Interface via NETCONF/YANG
  - ✓ I2NSF Framework in OpenStack NFV Environment
  - ✓ NSF Database Management via Consumer-Facing Interface
  - ✓ Interface Data Model Auto-Adoption
- Network Security Functions
  - ✓ Firewall and Web-filter using SDN and Suricata
- Advanced Functions
  - ✓ Security Policy Translation
  - ✓ NSF Monitoring via NETCONF/YANG (New Feature)

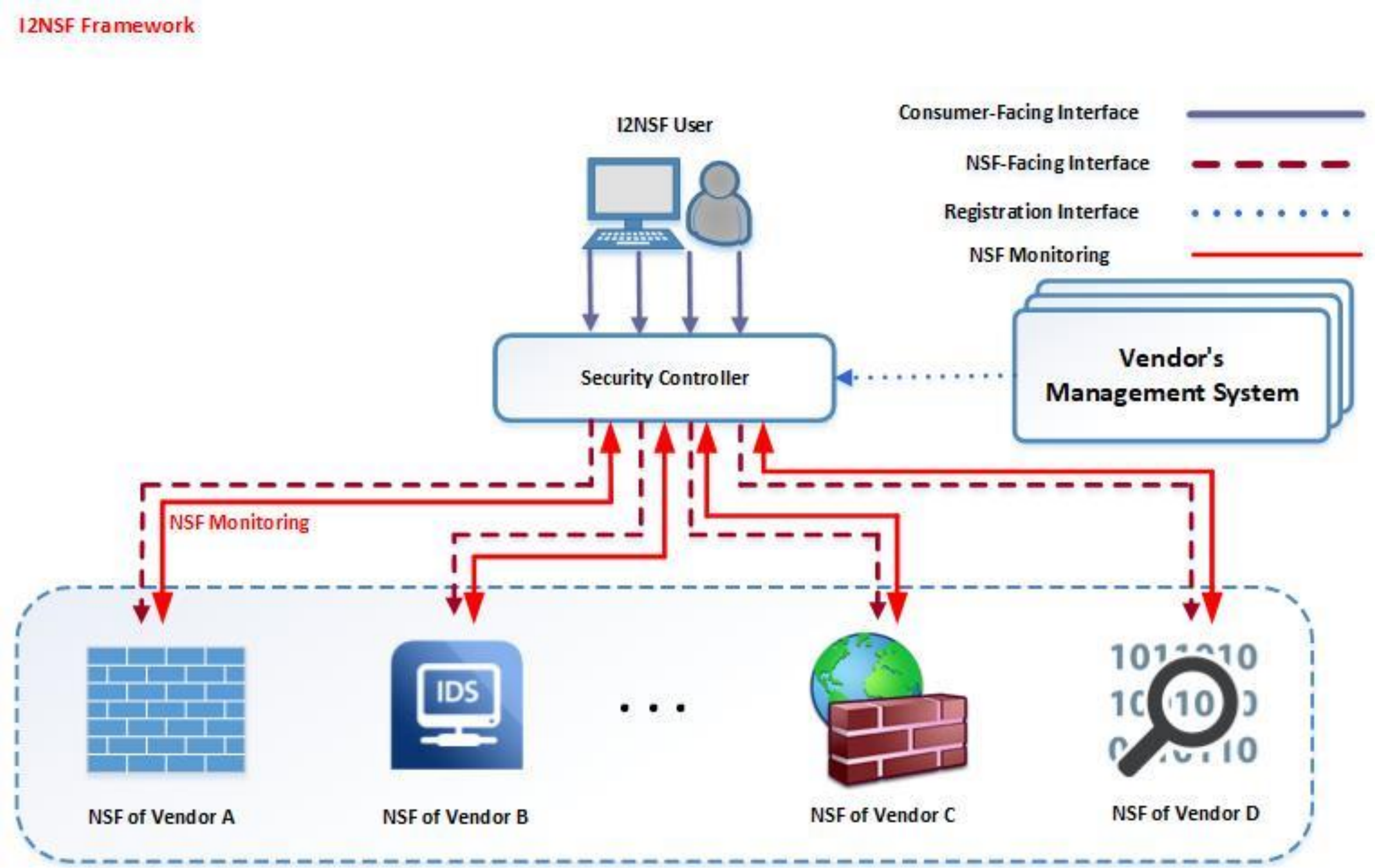
성균관대학교 SUNGKYUN KWAN UNIVERSITY

ETRI 한국전자통신연구원

I2NSF System using NSF Framework

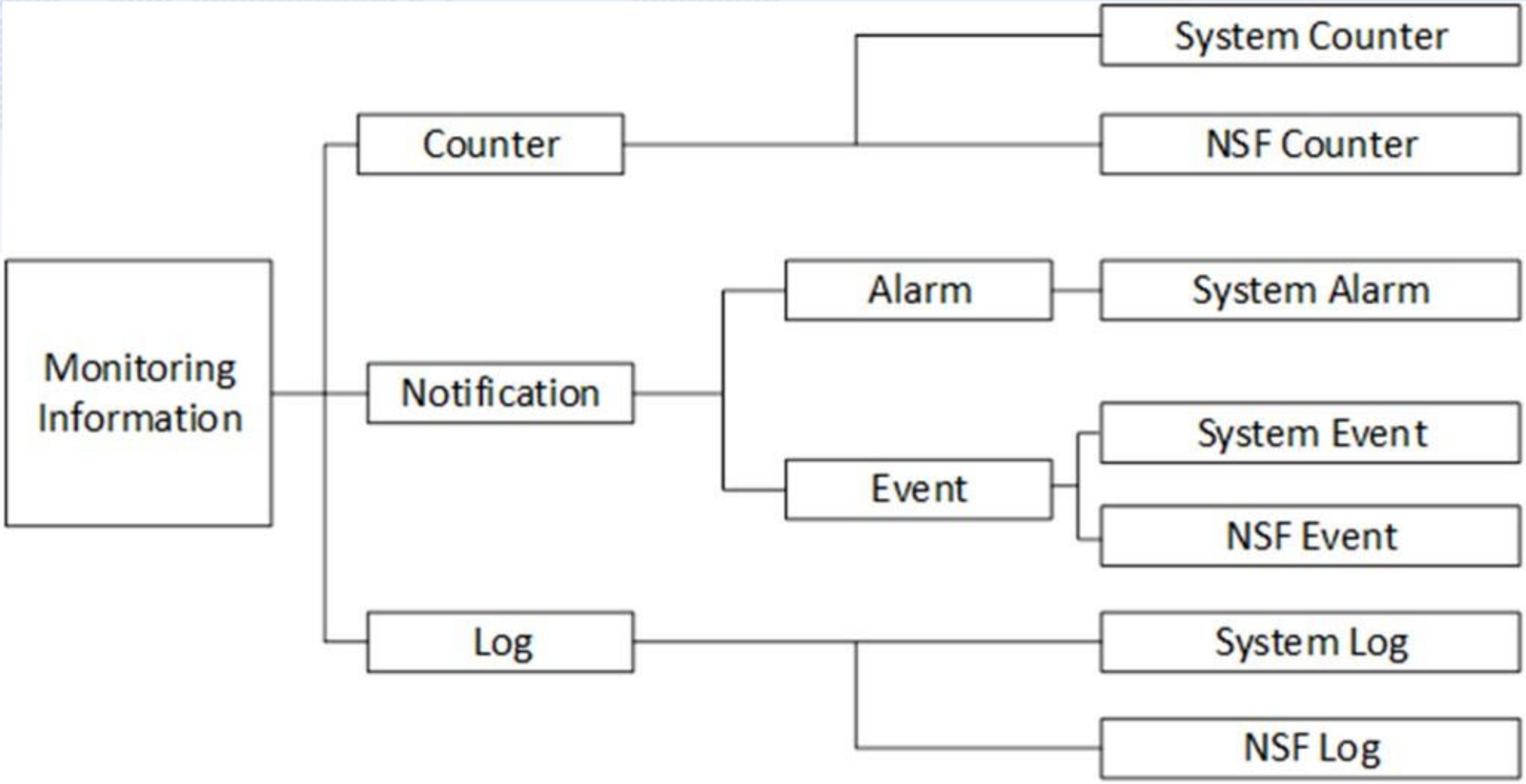


Implementation of I2NSF Hackathon Project (1/2)



1. Application of I2NSF Monitoring (on going)

Implementation of I2NSF Hackathon Project (2/2)



2. **NSF Monitoring Data Model**
   https://tools.ietf.org/html/draft-ietf-i2nsf-nsf-monitoring-data-model-02

Lessons from IETF-106 Hackathon

- **Proof of Concept (POC) of I2NSF Framework**
  - **I2NSF Interfaces (Consumer-Facing, NSF-Facing, and Registration Interface)**
  - **I2NSF Security Policy Translator**

- **Direction of NSF Monitoring Implementation**
  - **Application of I2NSF NSF Monitoring**
  - **We got the direction of implementation of NSF Monitoring.**
  - **This is the last-piece Data Model draft in I2NSF's current charter.**

I2NSF YANG Data Models

draft-ietf-i2nsf-capability-data-model-05
draft-ietf-i2nsf-consumer-facing-interface-dm-07
draft-ietf-i2nsf-nsf-facing-interface-dm-08
draft-ietf-i2nsf-registration-interface-dm-05
draft-ietf-i2nsf-nsf-monitoring-data-model-02

IETF 106, Singapore
Nov 21, 2019

Jaehoon Paul Jeong
pauljeong@skku.edu
Sungkyunkwan University

WG Documents of YANG Data Models

- Information Model Draft on NSF Capabilities
  - draft-ietf-i2nsf-capability-05
- Base YANG Data Model Draft
  - draft-ietf-i2nsf-capability-data-model-05
- I2NSF Interface YANG Data Model Drafts
  - draft-ietf-i2nsf-consumer-facing-interface-dm-07
  - draft-ietf-i2nsf-nsf-facing-interface-dm-08
  - draft-ietf-i2nsf-registration-interface-dm-05
  - draft-ietf-i2nsf-nsf-monitoring-data-model-02
- Verification of those YANG Data Models
  - Those will be verified through the **10 IETF Hackathons** (IETF 97 ~ IETF 106).
  - **4 Awards among 10 Hackathons**

Updates from the Previous Versions

- Consistency with **NSF Capabilities Information Model**
  - draft-ietf-i2nsf-capability-05

- We have addressed the comments from YANG doctors to the Data Model (DM) drafts and submitted the revised drafts:
  - NSF Capability DM
  - Registration Interface DM
  - NSF-Facing Interface DM
  - Consumer-Facing Interface DM
    - New comments from a YANG doctor (Jan Lindblad) will be reflected in the next revision.

Updates of Capability Data Model (DM) (1/2)

- Consistency with NSF Capabilities Information Model
  - – draft-ietf-i2nsf-capability-05
- Relationship with Other YANG Data Models
  - – draft-ietf-i2nsf-consumer-facing-interface-dm-07
  - – draft-ietf-i2nsf-nsf-facing-interface-dm-08
  - – draft-ietf-i2nsf-registration-interface-dm-05
- Revision from YANG doctors' comments
  - Refer to Appendix for more detailed revision

Updates of Capability Data Model (DM) (2/2)

- Major Comment
  - The "Security Considerations" in section 8
    - not conform to the recommended template; https://trac.ietf.org/trac/ops/wiki/yang-security-guidelines

- Changed to
  - **The attacker may provide incorrect information of the security capability of any target NSF by illegally modifying this.**
  - **The attacker may gather the security capability information of any target NSF and misuse the information for subsequent attacks.**

Updates of NSF-Facing Interface DM

- The leveraging of the definitions in RFC 8519 for packet matching.
- Date and time are defined in RFC 6991.
- For intervals, time-zones are replaced by time-intervals.
- acl-number is deleted and RFC 8519 is referred to for ACL.
- The overlap of definitions with the I2NSF capabilities draft is explained.
- “Security Considerations” Section according to the recommended template.

Updates of Consumer-Facing Interface DM (1/2)

- In Section 1, Figure 1 is modified such that "Multi-Tenancy" is deleted because "Multi-Tenancy" can be described by "Endpoint Groups" in a policy rule.

- In Section 4, Figure 2 is modified such that the YANG data model of a policy having at least one rule has a hierarchical structure rather than a flat structure by deleing the "Multi-Tenancy" field.

- The section named "Information Model for Multi-Tenancy" is deleted. The multi-tenancy can be specified by "Endpoint Groups“ along with "Network Configuration Access Control Model (NACM)“ mechanisms.

- In Section 5.1, "NACM" is applied in "user-group" and for its access control.

Updates of Consumer-Facing Interface DM (2/2)

- In Section 5.2, Figure 10 is modified because the "protocol" field was missed in the previous version.

- Section 7 is added as "Network Configuration Access Control Model (NACM)" in order to provide the Consumer-Facing Interface with the existing access control mechanisms. Also, the reference of [RFC8341] is added for NACM.

- The section named "Role-based Access Control (RBAC)" is deleted since this access control can be replaced by "NACM".

- In Section 8, the YANG data module is modified according to the above changes.

Updates of Registration Interface DM (1/2)

- Revision from a YANG doctor’s comments
  - Refer to Appendix for more detailed revision
- Revision of YANG Module structure according to RFC 8407 Appendix B
- Addition of detailed description of each component of the YANG module
- Changed the prefix with “nsfreg”

Updates of Registration Interface DM (2/2)

- Modified nsf-address to deal with both IPv4 and IPv6 addresses

- Revised all examples to use IPv6 address specified in RFC 3849 in Appendix A

- “nsf-port-address” has been changed into “nsf-port”.

- Revised security considerations section, and added more explanation to Section 4

Updates of NSF Monitoring DM

- YANG Data Model (DM) corresponding to the Information Model (IM) for NSF-Facing Interface:
  - draft-ietf-i2nsf-capability-05

- Major Update
  - Section 7 is reorganized with the subsections for the monitored objects (i.e., event, log, and counter) of System and NSF.
  - Those subsections are listed up pairwisely with a pair of System and NSF except alarm because alarm is a monitored object to only System.

Next Steps

- WGLC for three data model drafts after IETF-106 Meeting
  - NSF Capability DM Draft
  - NSF-Facing Interface DM
  - Registration Interface DM
- Consumer-Facing Interface DM
  - Revise this draft and ask for the review of a YANG doctor
- NSF Monitoring Data Model Draft
  - We are planning to test it in IETF-107 Hackathon
  - WGLC in IETF-107 Meeting

Security Policy Translation in I2NSF

draft-yang-i2nsf-security-policy-translation-05

IETF 106, Singapore

Nov 21, 2019

Chaehong Chung, Jaehoon (Paul) Jeong

Sungkyunkwan University

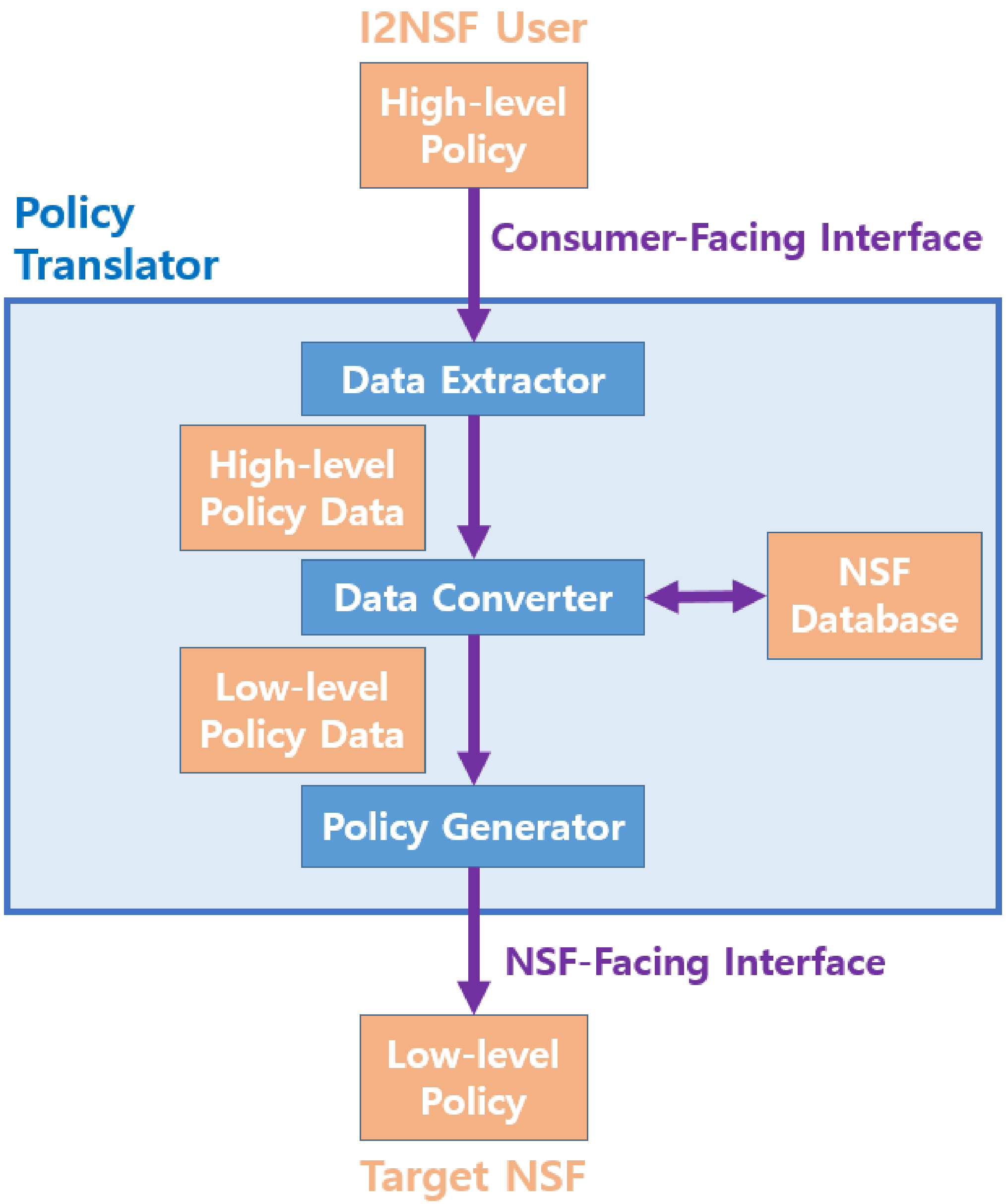
Current Status of Security Policy Translation

- Document name
  - draft-yang-i2nsf-security-policy-translation-05 (last updated: 2019/11/04)
- Document link
  - https://datatracker.ietf.org/doc/draft-yang-i2nsf-security-policy-translation/
- Document status
  - Individual draft

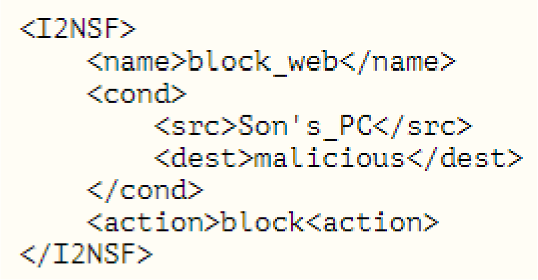
Updates from the Previous Versions

- The mapping information is annotated with comments.
  - The mapping information between the data models of the Consumer-Facing Interface and the NSF-Facing Interface
  - It is for data conversion of High-level security policy into Low-level security policy.
  - Comments are shown in Figure 7.

Security Policy Translator



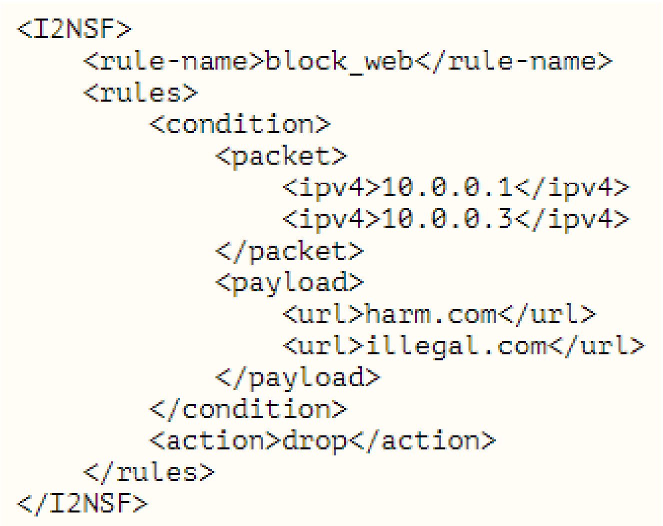
High-level policy



```
<I2NSF>
    <name>block_web</name>
    <cond>
        <src>Son's_PC</src>
        <dest>malicious</dest>
    </cond>
    <action>block<action>
</I2NSF>
```

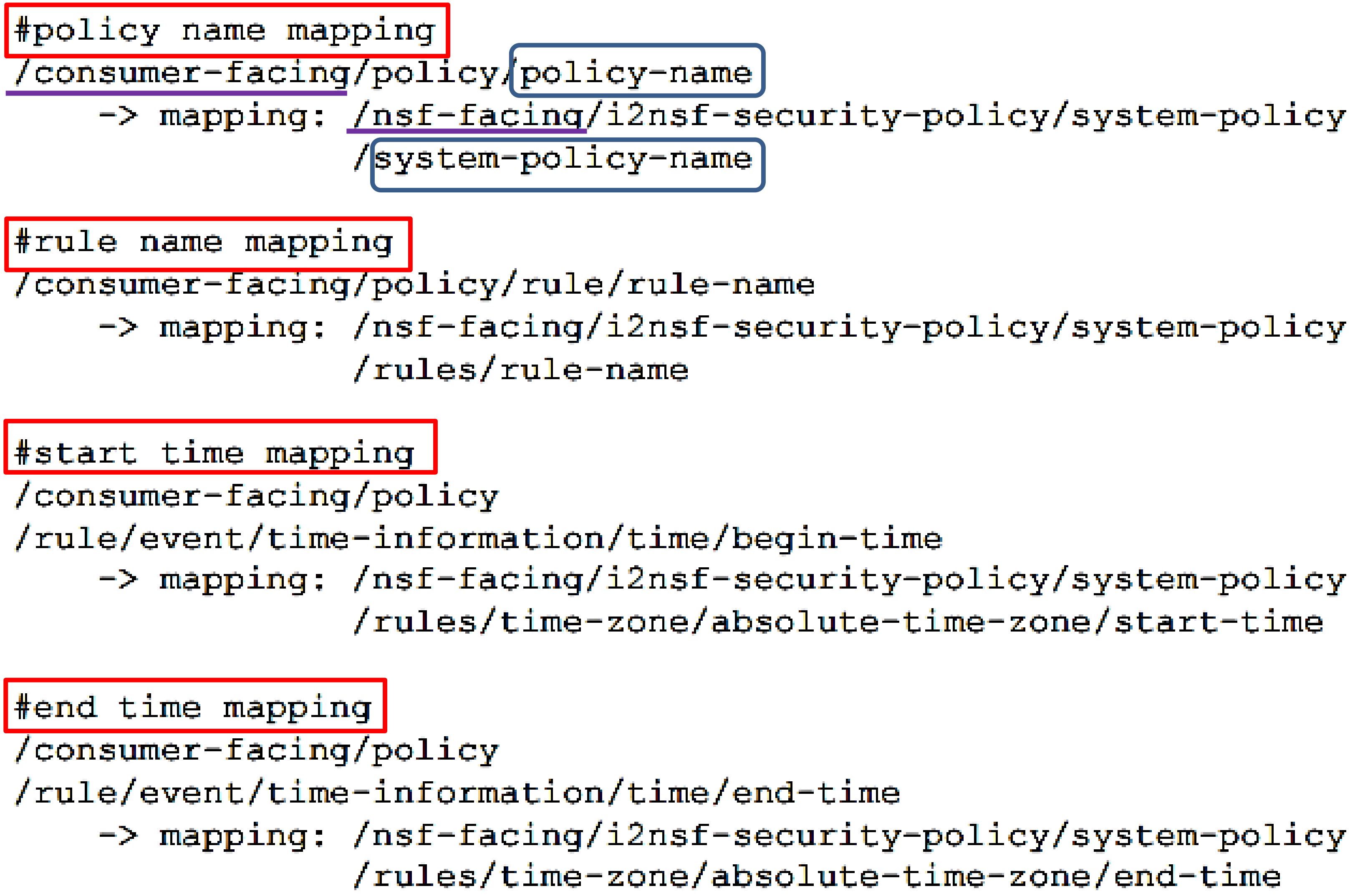
Translation

Low-level policy



```
<I2NSF>
    <rule-name>block_web</rule-name>
    <rules>
        <condition>
            <packet>
                <ipv4>10.0.0.1</ipv4>
                <ipv4>10.0.0.3</ipv4>
            </packet>
            <payload>
                <url>harm.com</url>
                <url>illegal.com</url>
            </payload>
        </condition>
        <action>drop</action>
    </rules>
</I2NSF>
```

Examples of
Mapping Information Comments



```
#policy name mapping
/consumer-facing/policy/policy-name
    -> mapping: /nsf-facing/i2nsf-security-policy/system-policy
                /system-policy-name

#rule name mapping
/consumer-facing/policy/rule/rule-name
    -> mapping: /nsf-facing/i2nsf-security-policy/system-policy
                /rules/rule-name

#start time mapping
/consumer-facing/policy
/rule/event/time-information/time/begin-time
    -> mapping: /nsf-facing/i2nsf-security-policy/system-policy
                /rules/time-zone/absolute-time-zone/start-time

#end time mapping
/consumer-facing/policy
/rule/event/time-information/time/end-time
    -> mapping: /nsf-facing/i2nsf-security-policy/system-policy
                /rules/time-zone/absolute-time-zone/end-time
```

Next Steps

- We will reflect the YANG Doctors' reviews of Consumer-Facing and NSF-Facing DMs.

- We will work for a general translator for network and device configuration as well as security policy configuration.

New WG Items for I2NSF

IETF 106, Singapore

Nov 21, 2019

Jaehoon (Paul) Jeong

Sungkyunkwan University

New WG Items

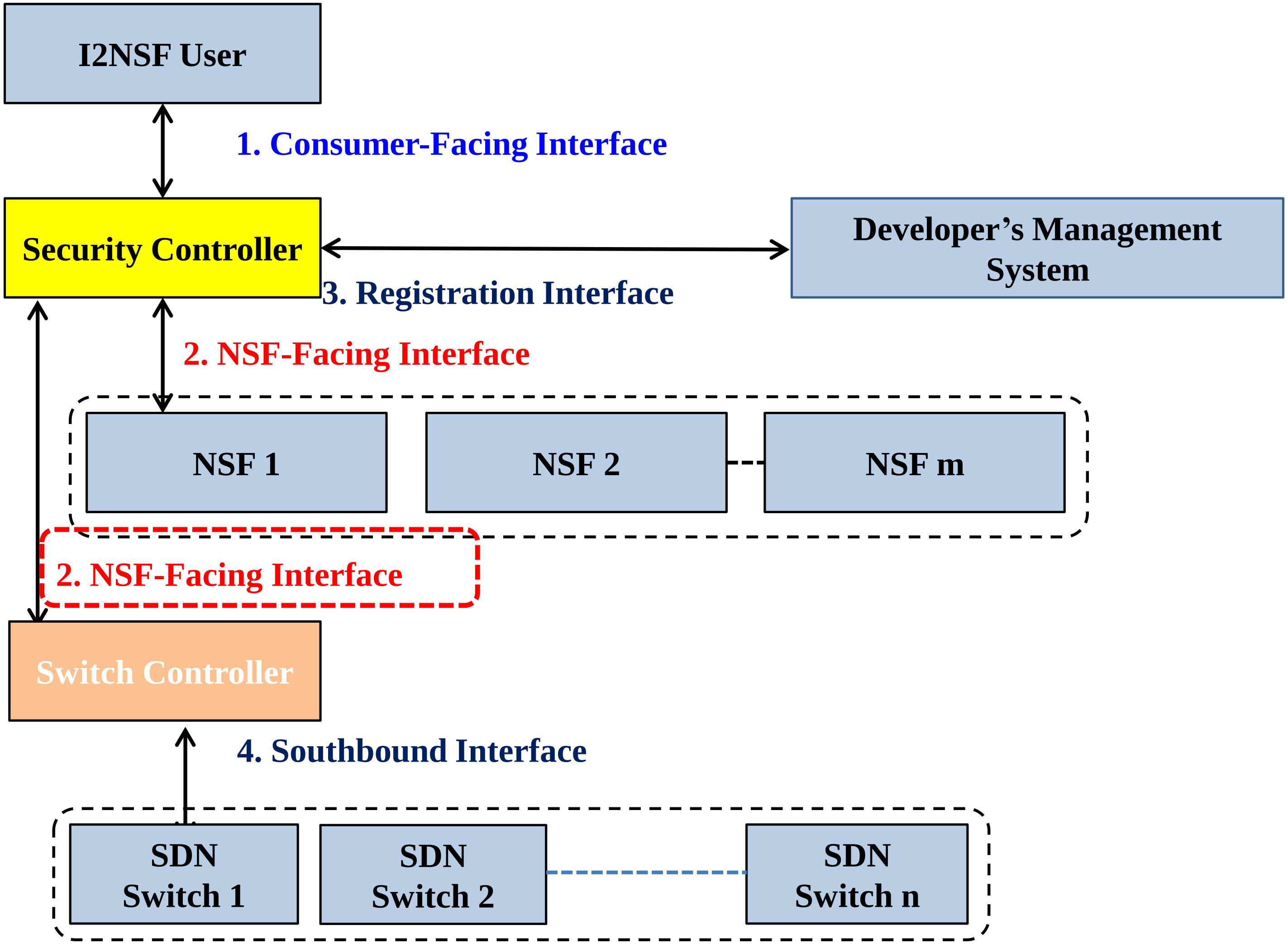
- YANG data model of the interface between I2NSF Security Controller and SDN Switch Controller

- YANG data model of the interface between I2NSF Security Controller and SFC Classifier

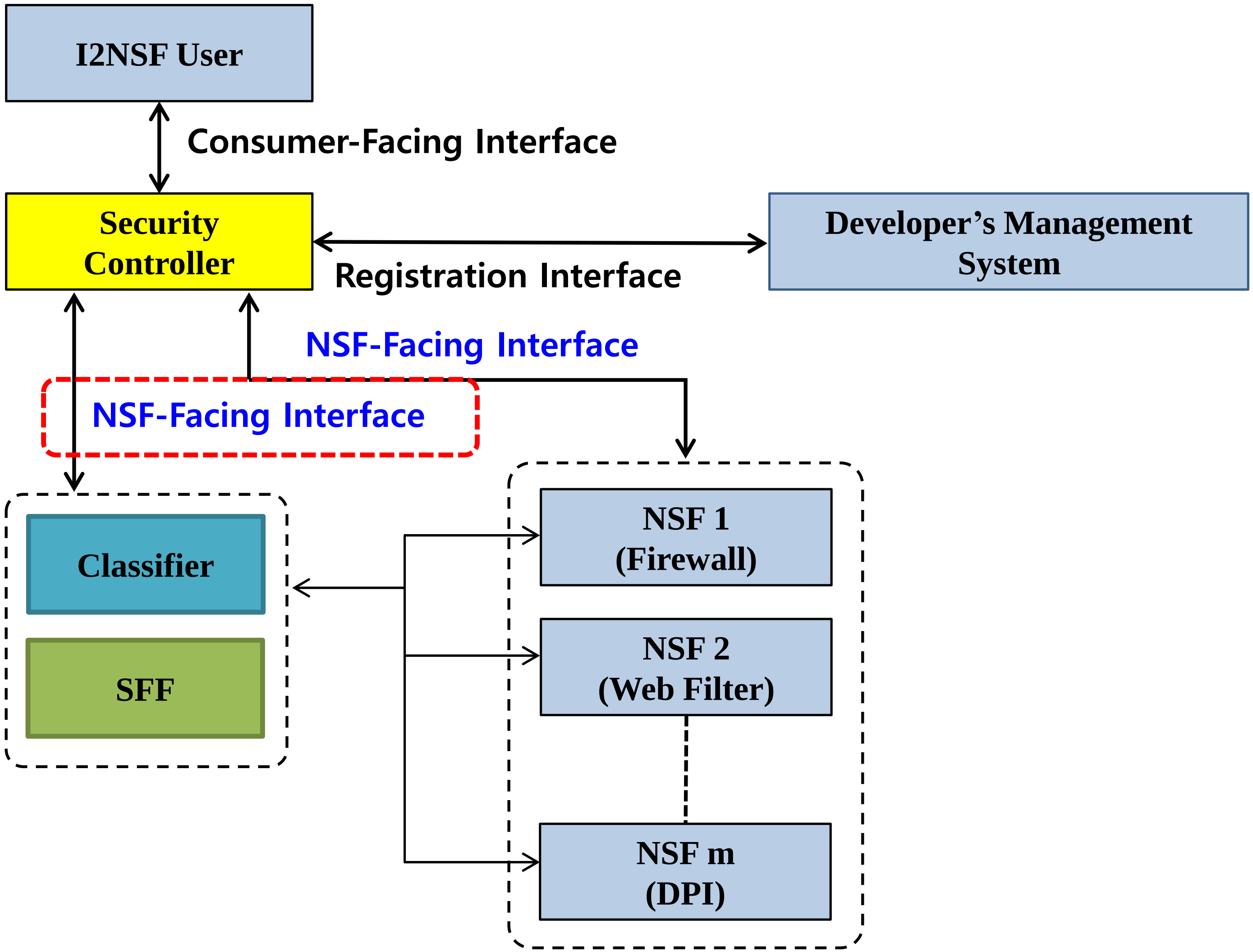
- Configuration of Advanced Security Functions with I2NSF Security Controller

- Policy Object for Interface to Network Security Functions (I2NSF)

The Interface between I2NSF Security Controller and SDN Switch Controller



The Interface between I2NSF Security Controller and SFC Classifier



Configuration of Advanced Security Functions with I2NSF Security Controller

- With the current NSF-Facing Interface, we can configure basic security functions, such as firewall, deep packet inspection, and DDoS attack mitigator.
- For rich network security functions, the YANG data model of advanced security services needs to be developed.
- https://tools.ietf.org/html/draft-dong-i2nsf-asf-config-01

Policy Object for Interface to Network Security Functions (I2NSF)

- Policy objects for I2NSF security policy rules can provide the I2NSF system with reusability for security policy construction by defining essential attributes for each policy object.

- This will be useful for security policy rule generation in the I2NSF system.

- https://tools.ietf.org/html/draft-xia-i2nsf-security-policy-object-01