Applicability of Interfaces to Network Security Functions to Networked Security Services

(draft-ietf-i2nsf-applicability-04)

IETF 102, Montreal

July 18, 2018

Jaehoon (Paul) Jeong [Presenter], Sangwon Hyun, Tae-Jin Ahn,
Susan Hares, and Diego Lopez

Updates from the Previous Versions

- The following changes have been made from draft-ietf-i2nsf-applicability-02 and -03:
  - We added Section 4 that explains an integration of I2NSF framework and SFC to support chaining NSFs.
  - We added Section 6 that describes an implementation of I2NSF framework based on an NFV reference architecture.
  - NSF-Facing Interface is used for the interface between Security Controller and SFC Classifier (or SFF) instead of I2NSF-SFC Interface.

Motivation of this Document

- I2NSF Applicability
  - I2NSF Chartered Working Item
  - This draft explains how I2NSF framework and interfaces can be used for real network security services.

- Contents
  - Security service procedure in I2NSF framework
    - Time-dependent web access control with firewall & web filter
  - Combination of I2NSF and SDN
  - Combination of I2NSF and SFC
  - Combination of I2NSF and NFV

Why combining I2NSF with SFC?

- Motivation: Supporting advanced security actions in I2NSF framework that allow an NSF to trigger another type of NSF

- SFC can be used to enable advanced security actions by steering traffic packets through multiple NSFs.

- Benefits
  - Composite security inspection of packets with multiple types of NSFs
  - Flexible application of multiple types of NSFs according to the suspiciousness levels of packets

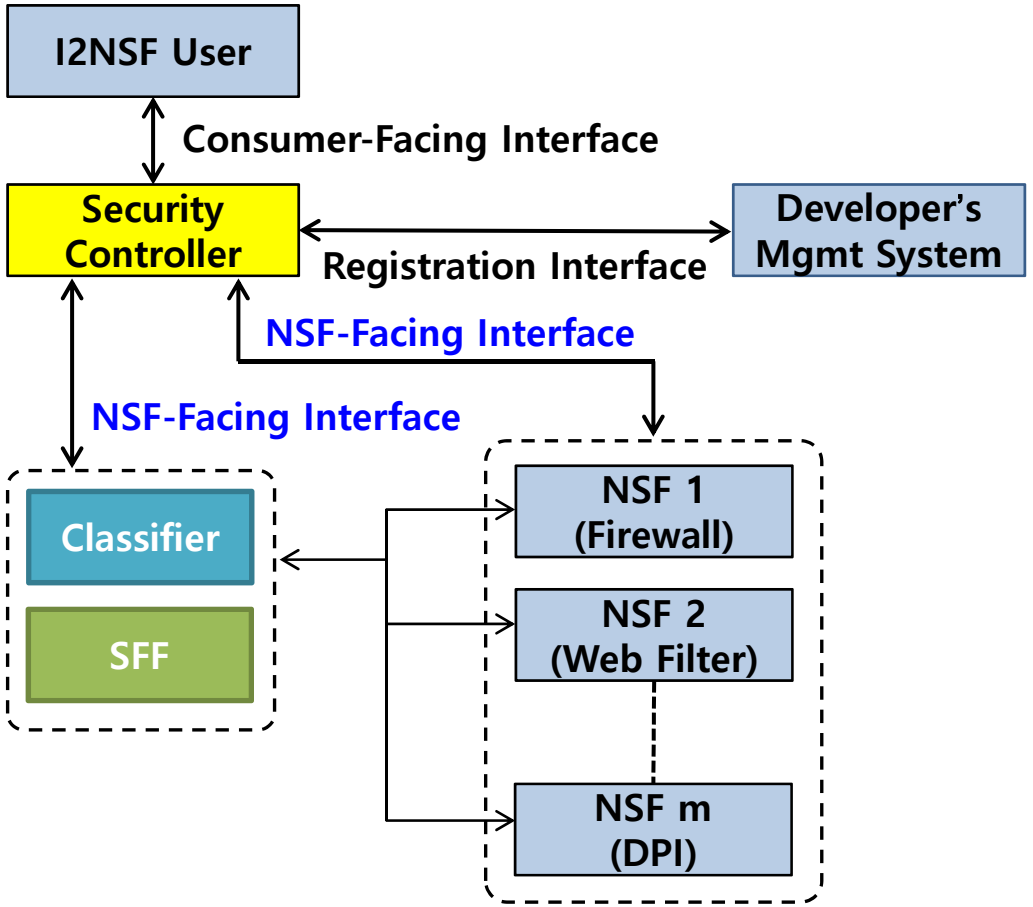
I2NSF Framework with SFC

An I2NSF Framework with SFC for flexible applications of multiple NSFs

1. An **NSF** triggers an advanced security action on a suspicious packet by appending a metadata describing the required security capability to the NSH of the packet**.**

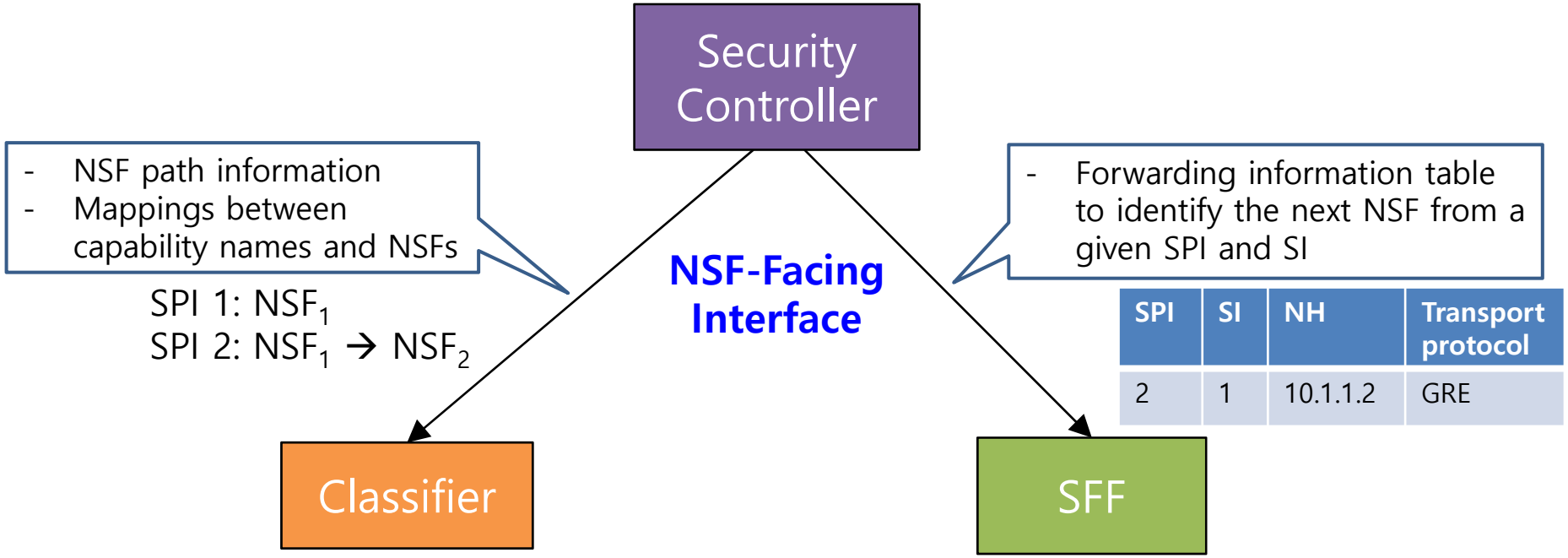
2. The **classifier** properly updates the NSH information of the packet so that the packet follows an NSF path where an NSF with the required security capability is available.

3. Based on the updated NSH information, the **SFF** forwards the suspicious packet to an NSF with the required security capability.



Configuration for SFC

- **Security Controller** may take responsibilities of configuring classifiers and SFFs with proper rules for SFC via NSF-Facing Interface.
  - Configuring classifiers with service function chain/path information
  - Configuring SFFs with forwarding information tables of NSFs

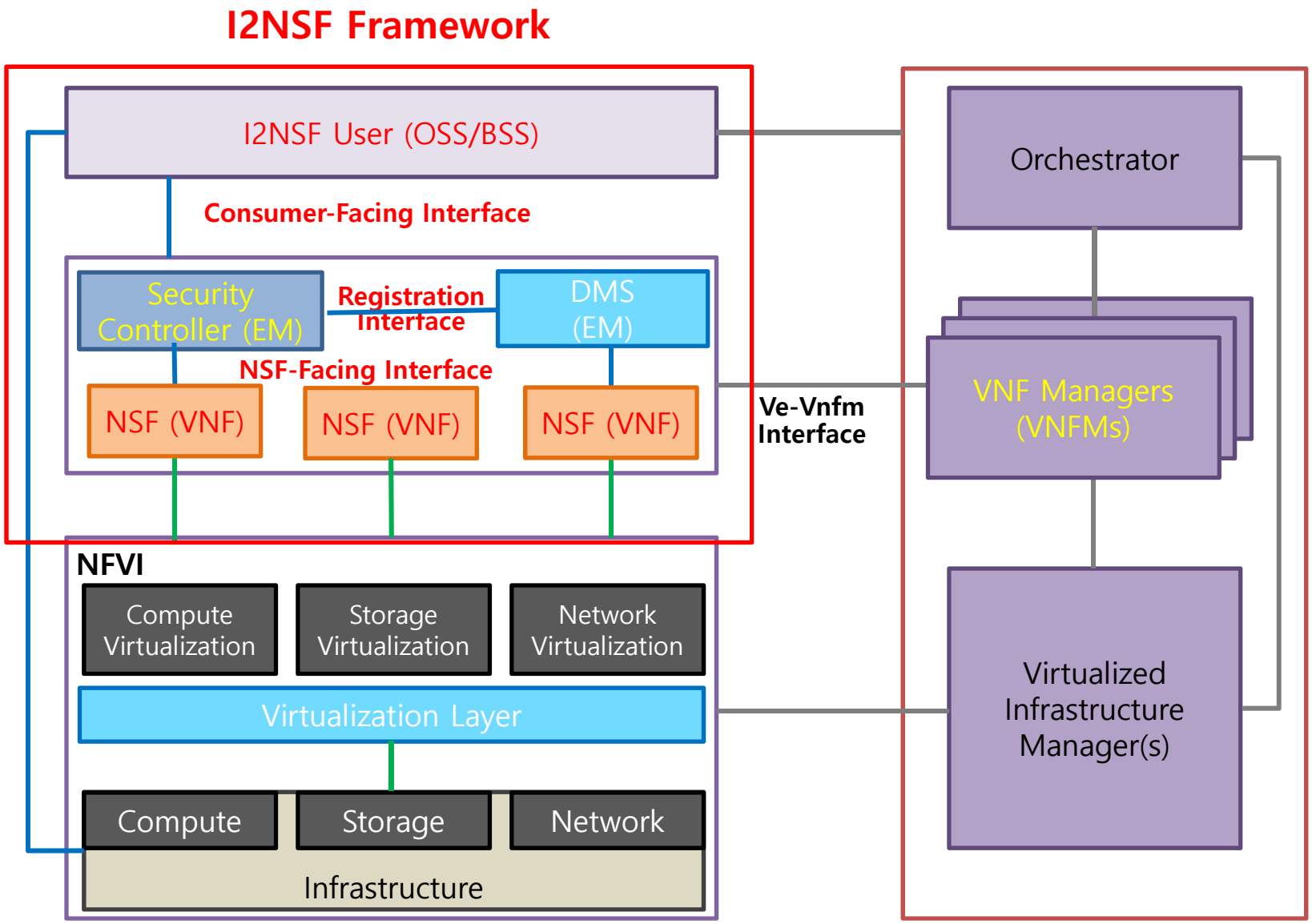


Why combining I2NSF with NFV?

- Motivation: To respond rapidly and flexibly to the amount of service requests through high availability and scalability management of NSFs

- Benefits
  - Improve the elasticity and efficiency of network resource utilization
  - Facilitate flexibly including or excluding NSFs from multiple security solution vendors according to the changes on security requirements.

I2NSF Framework with NFV



Next Steps

- Plan: **WG Lastcall at IETF 102**
- Welcome your Feedback!

APPENDIX: COMBINATION OF I2NSF WITH SDN

Why combining I2NSF with SDN?

- Motivation: Reducing the overhead of security policy enforcement by leveraging SDN technology

- Dividing security policy enforcement
  - SDN switches enforce simple packet filtering rules that can be translated into their packet forwarding rules.
  - NSFs enforce security policy rules requiring complex security capabilities dedicated to them.

- Benefits
  - Avoid unnecessary detouring to NSFs placed in a remote cloud system
  - Avoid unnecessary latency introduced by NSFs for time-consuming tasks
  - Reduce the possibility of congestion in NSFs by using switches

I2NSF Framework with SDN

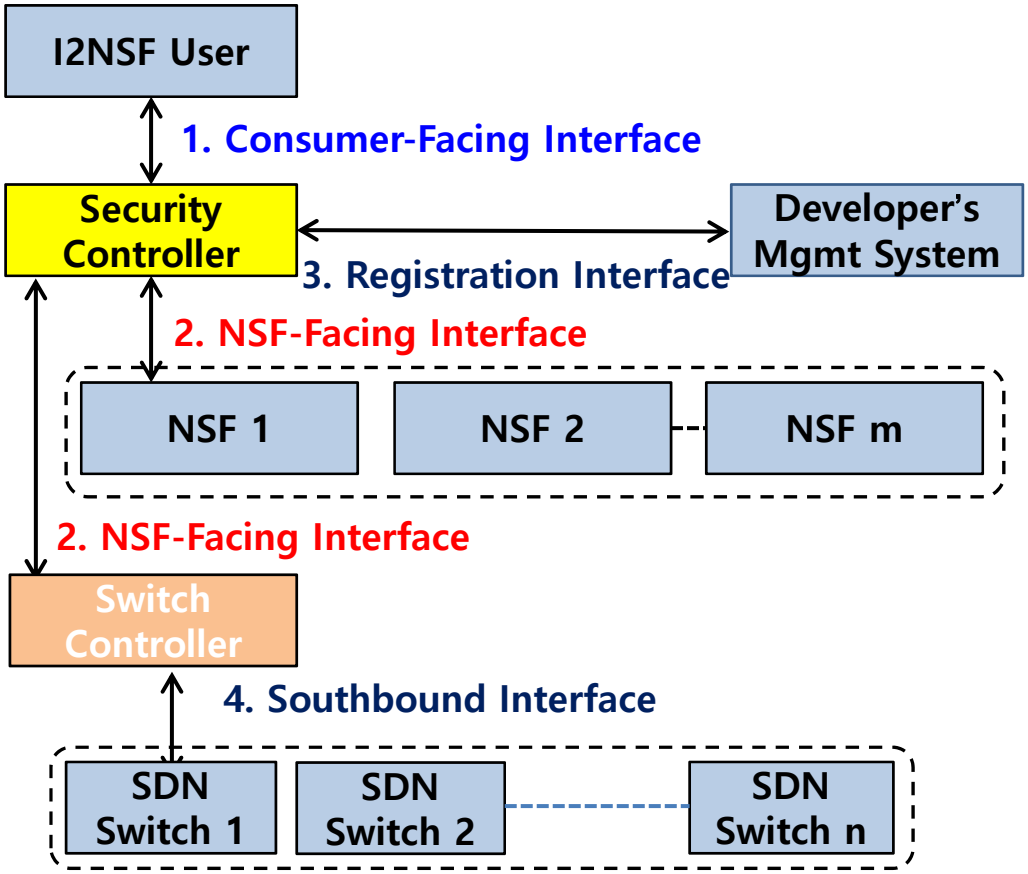
An I2NSF Framework with SDN for Efficient Security Services

1. **I2NSF User** asks for security services with high-level security policies to **Security Controller** via **Consumer-Facing Interface.**

2. **Security Controller** delivers low-level security policies to **NSFs** and **Switch Controller** via **NSF-Facing Interface.**

3. **Network Security Function** configures such low-level security policies into its local system.

4. **Switch Controller** sets up filtering rules for the low-level policies on Switches via **Southbound Interface**.



Information and Data Models for I2NSF

- Consumer-Facing Interface
  - Information Model
    - draft-kumar-i2nsf-client-facing-interface-im-06
  - Data Model
    - draft-ietf-i2nsf-consumer-facing-interface-dm-01
- NSF-Facing Interface
  - Information Model
    - draft-ietf-i2nsf-capability-02
  - Data Model
    - draft-ietf-i2nsf-nsf-facing-interface-dm-01
- Registration Interface
  - Information Model
    - draft-hyun-i2nsf-registration-interface-im-05
  - Data Model
    - draft-hyun-i2nsf-registration-interface-dm-04

Combination of I2NSF and SDN

- Accelerated Security Service
  - Simple packet filtering rules by SDN switches
  - Complicated security inspection by NSFs