Applicability of Interfaces to Network Security Functions to Networked Security Services

(draft-ietf-i2nsf-applicability-02)

IETF 101, London

March 21, 2018

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

Updates from the Previous Version

- The following changes have been made from draft-ietf-i2nsf-applicability-01:
  - In Section 4, we clarified the motivations and benefits of combining SDN with I2NSF framework.
  - In Section 4, we clarified the types of policy rules that can be enforced by SDN switches or NSFs in I2NSF framework with SDN.
  - In Section 4, we explained the role of the security controller to support the divided security policy enforcement by SDN switches and NSFs.

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
    - Firewall system
    - VoIP/VoLTE security system
    - DDoS-attack mitigation system

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

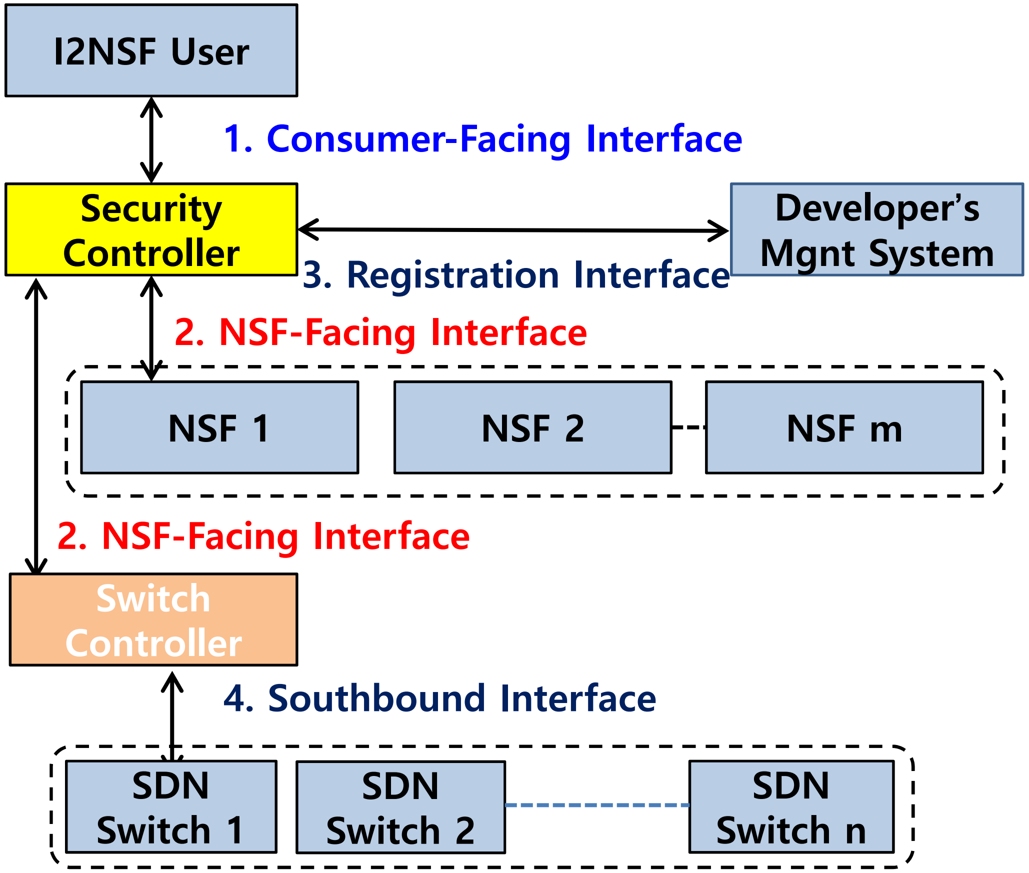
An I2NSF Framework with SDN for Efficient Security Services

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**.

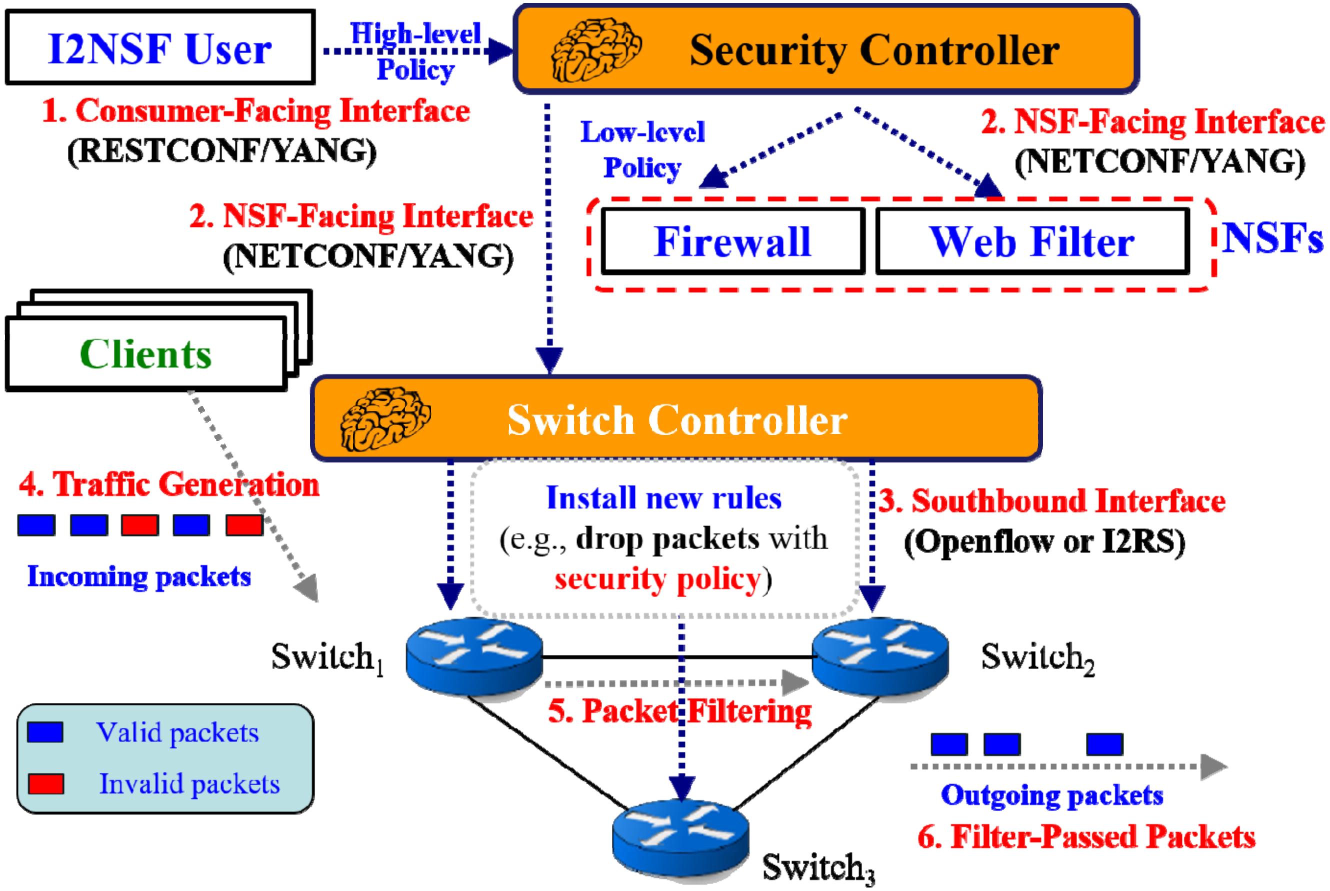


Information and Data Models for I2NSF

- Consumer-Facing Interface
  - Information Model
    - draft-kumar-i2nsf-client-facing-interface-im-05
  - Data Model
    - draft-ietf-i2nsf-consumer-facing-interface-dm-00
- NSF-Facing Interface
  - Information Model
    - draft-ietf-i2nsf-capability-00
  - Data Model
    - draft-ietf-i2nsf-nsf-facing-interface-dm-00
- Registration Interface
  - Information Model
    - draft-hyun-i2nsf-registration-interface-im-04
  - Data Model
    - draft-hyun-i2nsf-registration-interface-dm-03

Combination of I2NSF and SDN

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



Next Steps

- If any suggestion of new use cases of I2NSF, we will reflect them.
- Plan: **WGLC after IETF 101?**
- Welcome your Feedback!