I2NSF Framework @ IETF-98 Hackathon

IETF 98, Chicago, US

March 26, 2017

Jaehoon (Paul) Jeong
Sungkyunkwan University
pauljeong@skku.edu

Why Did We Do this Project?

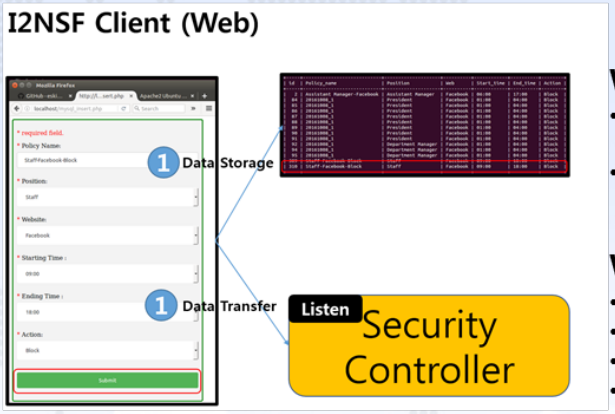
- I2NSF: Use NETCONF/RESTCONF + YANG Data Models
  - Is this approach reasonable for management of security devices?
  - Is it better than writing another security protocol?
  - Can we get I2NSF **Key Data Model (Capability) refined**, and use open source code (e.g., Suricata) for Firewall?

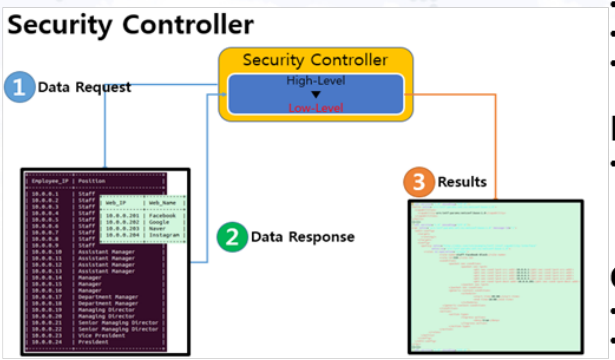
- Result: I2NSF WG approach works, fast time to market
  - NM/OPS should expand their work into Security
  - I2NSF follows up with MILE, SACM, DOTS, and SECEVENTs

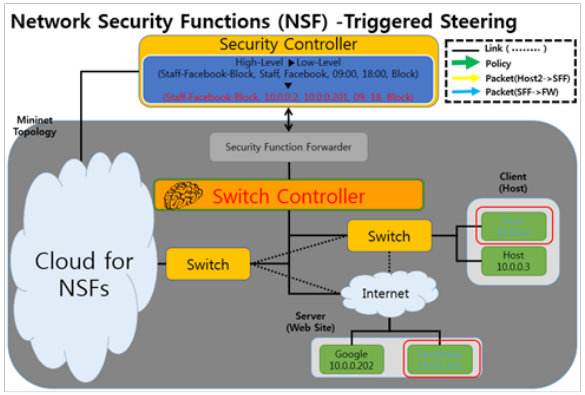
- Does this work for a student project – Yes!!
  - 9 graduate students
  - Put Code on Web

IETF I2NSF (Interface to Network Security Functions) Working Group: I2NSF Framework Project

Champions: Jaehoon Paul Jeong, Sang Won Hyun, and Jinyong Tim Kim (SKKU)







Professors

- Jaehoon (Paul) Jeong (Sungkyunkwan)
- Hyoungshick Kim (Sungkyunkwan)
- Hoon Ko (Sungkyunkwan)
- Sangwon Hyun (Sungkyunkwan)

Collaborators

- Jung-Soo Park (ETRI)
- Tae-Jin Ahn (Korea Telecom)

Students

- Jinyong Tim Kim
- Sanguk Woo
- Daeyoung Hyun
- Eunsoo Kim
- Mahdi Daghmehchi Firoozjaei
- Sanghak Oh
- Yunsuk Yeo
- Soyoung Kim

Where to get code

- Github – Source code
  - ✓ https://github.com/kimjinyong/i2nsf-framework
- USB – Source code & environment
  - ✓ Provided by USB Driver

What to pull down to set-up environment

- OS : Ubuntu 14.04TL
- Confd : 6.2 Version
- Apache2 : 2.4.7 Version
- MySQL : 14.14 Version
- PHP : 5.5.9 Version
- Mininet : 2.2.1 Version
- OpenDaylight : Distribution-karaf-0.4.3-Beryllium-SR3

Manual for Operation Process

- https://github.com/kimjinyong/i2nsf-framework/README.txt

Contents of Implementation

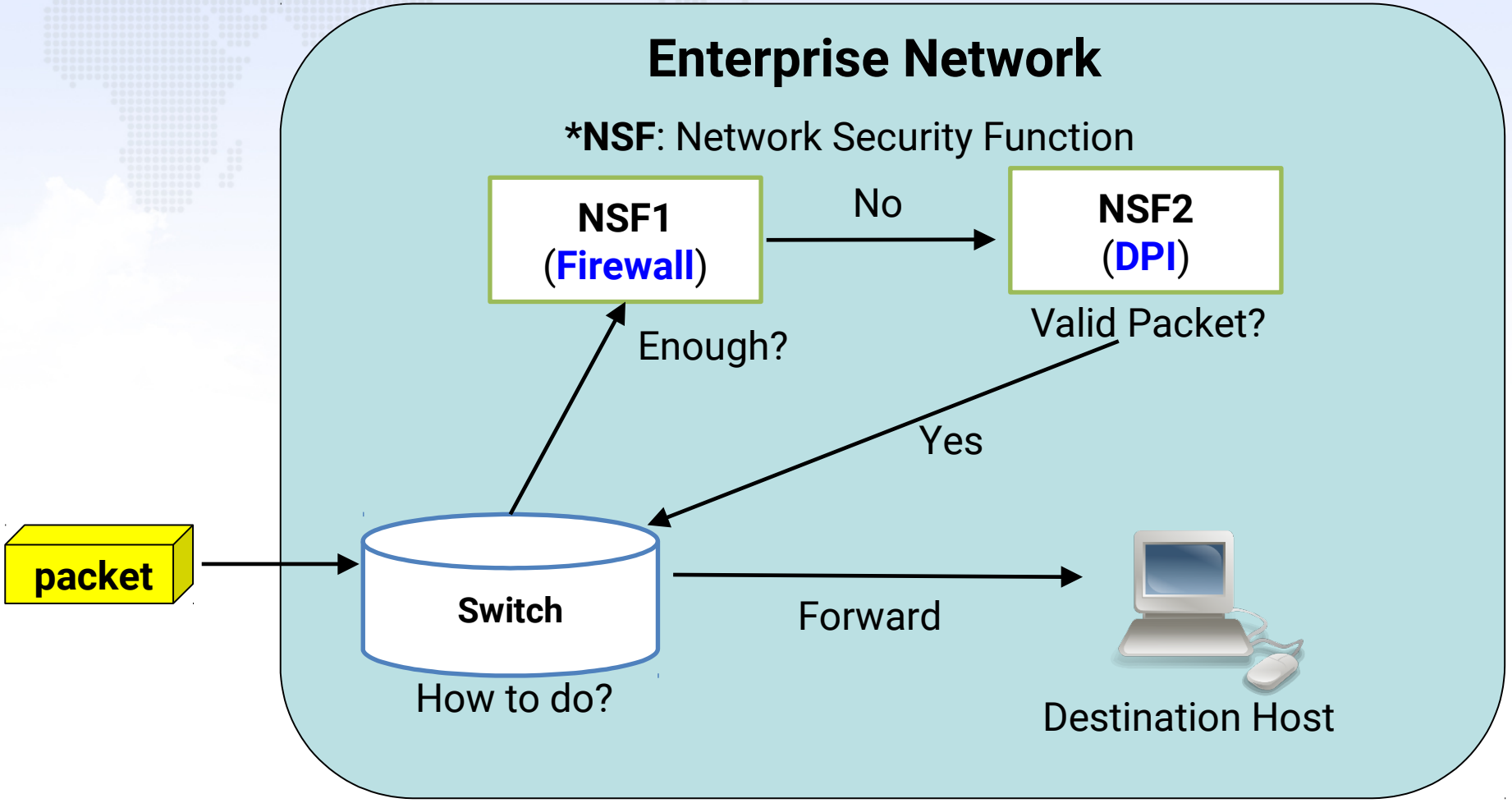
- Firewall
- DPI for VoIP-VoLTE Security Service

Mission

- Firewall
  - ✓ Deletion of policy
  - ✓ Update of policy
  - ✓ Avoidance of the duplication of policy

Remote Participants at SKKU in Korea

What are Network Security Functions (NSFs)?



Goal of I2NSF Project

for provisioning Network Security Functions (NSFs), we implemented one thing:

- **Firewall** for Web-filtering in I2NSF Framework using **Suricata**, which is an open source for IDS/IPS.

Contributions for the Goal

1. **Proof of Concept (POC) of I2NSF Framework using Open Sources.**

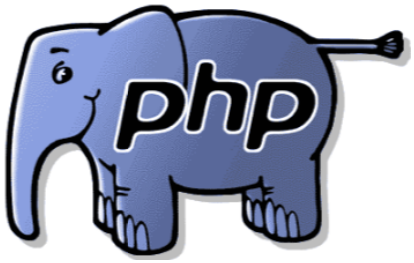
2. **Validity of I2NSF Interface Design for I2NSF Framework.**

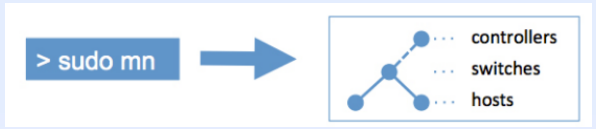
3. **Feasibility of Data-driven Approach (YANG) for Network Security Services.**

Hackathon Development

Build Environment

1. **OS**
   - Ubuntu 14.04TL
2. **Netconfd**
   - 6.2 Version
3. **Apache2**
   - 2.4.7 Version
4. **MySQL**
   - 14.14 Version
5. **PHP**
   - 5.5.9 Version

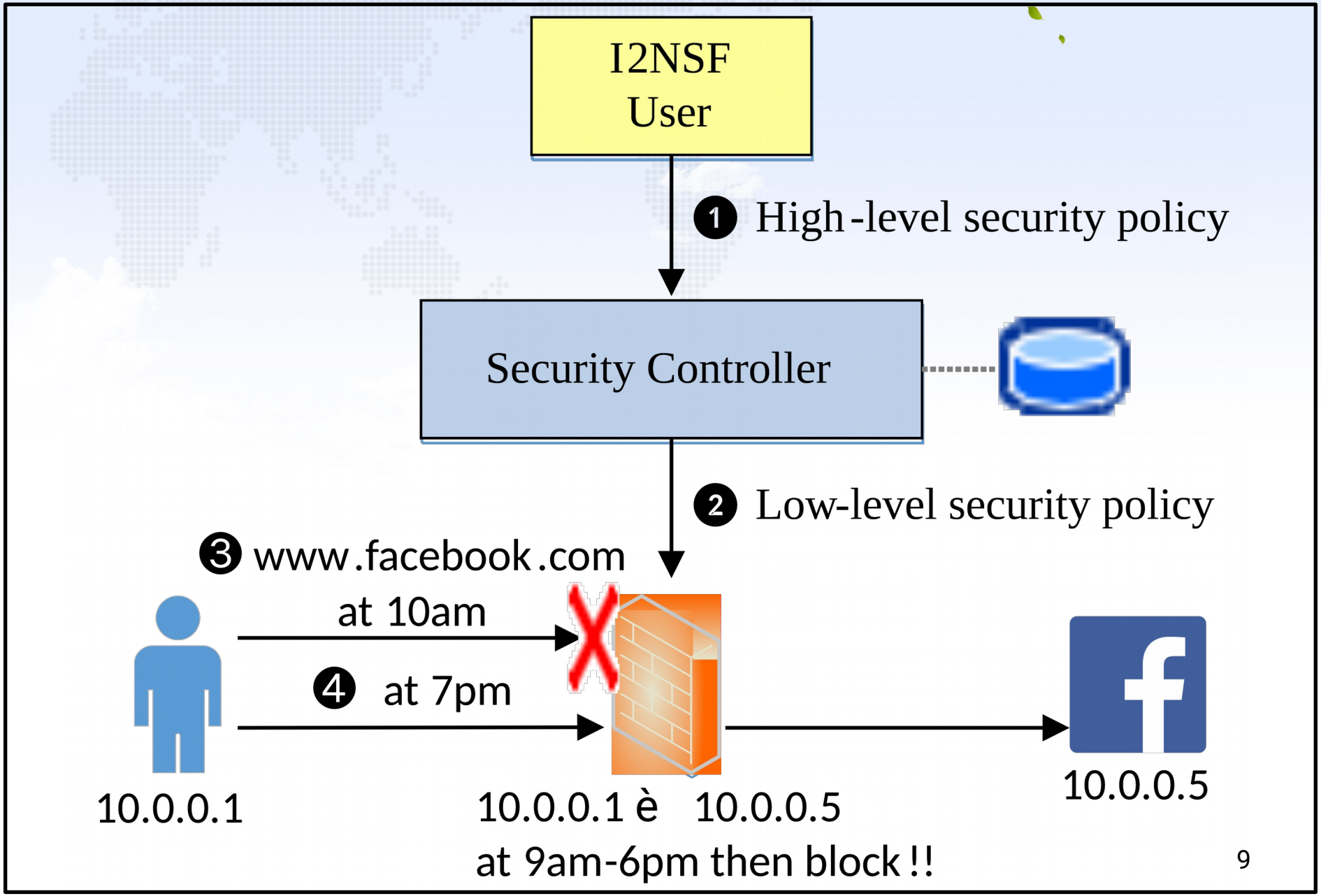




5. **Mininet**
   - 2.2.1 Version
6. **OpenDaylight**
   - Distribution-karaf-0.4.3-Beryllium-SR3
7. **Suricata**
   - 3.2.1 RELEASE

ubuntu

Scenario of Security Services in I2NSF Testbed



Lessons from the Implementation @ Hackathon

1. Proof of Concept (POC) of I2NSF Framework using Open Sources:
   - Confd for I2NSF NSF-Facing Interface
   - Restconf for I2NSF Consumer-Facing Interface
   - Suricata for Firewall NSF
   - OpenDaylight for SDN Controller
   - Mininet for SDN Network
2. Validity of I2NSF Interface Design for I2NSF Framework:
   - Firewall for Web Filtering
3. Feasibility of Data-driven Approach (YANG) for Network Security:
   - YANG Data Models for I2NSF Interfaces among System Entities (I2NSF User, Security Controller, NSFs).

Github Code of I2NSF Implementation