I2NSF Project @ IETF-97 Hackathon

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

Why Do We this Project?

- I2NSF: Chartered to use NETCONF/RESTCONF + 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 put open source code for VOIP/VoLTE and 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!!
  - 25 new 1st timers at IETF
  - Put Code on Web

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

Champions: Jaehoon Paul Jeong, Jinyong Tim Kim (SKKU), Jung-Soo Park (ETRI), and Tae-Jin Ahn (KT)

Professors

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

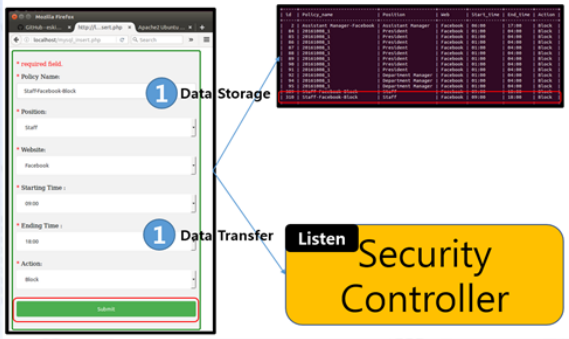
Collaborators

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

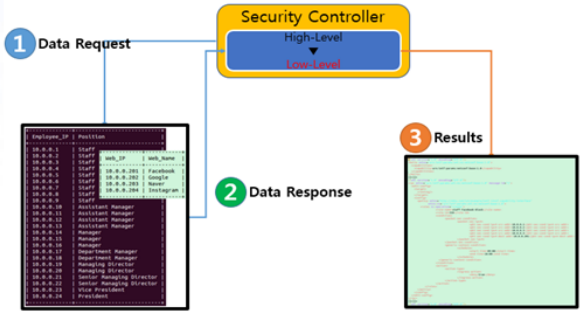
Students

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

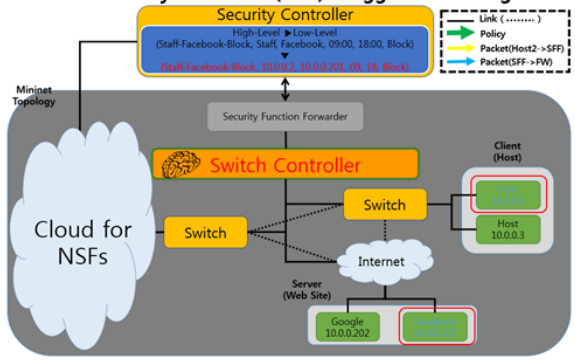
I2NSF Client (Web)



Security Controller



Network Security Functions (NSF) -Triggered Steering



Where to get code

- Github – Source code
  - ✓ https://github.com/YunSukYeo/secuBrain/invitations
- USB – Source code & environment
  - ✓ Provided by USB Driver

What to pull down to set-up environment

- OS : Ubuntu 14.04TL
- Netconfd : 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

- README.txt

Contents of Implementation

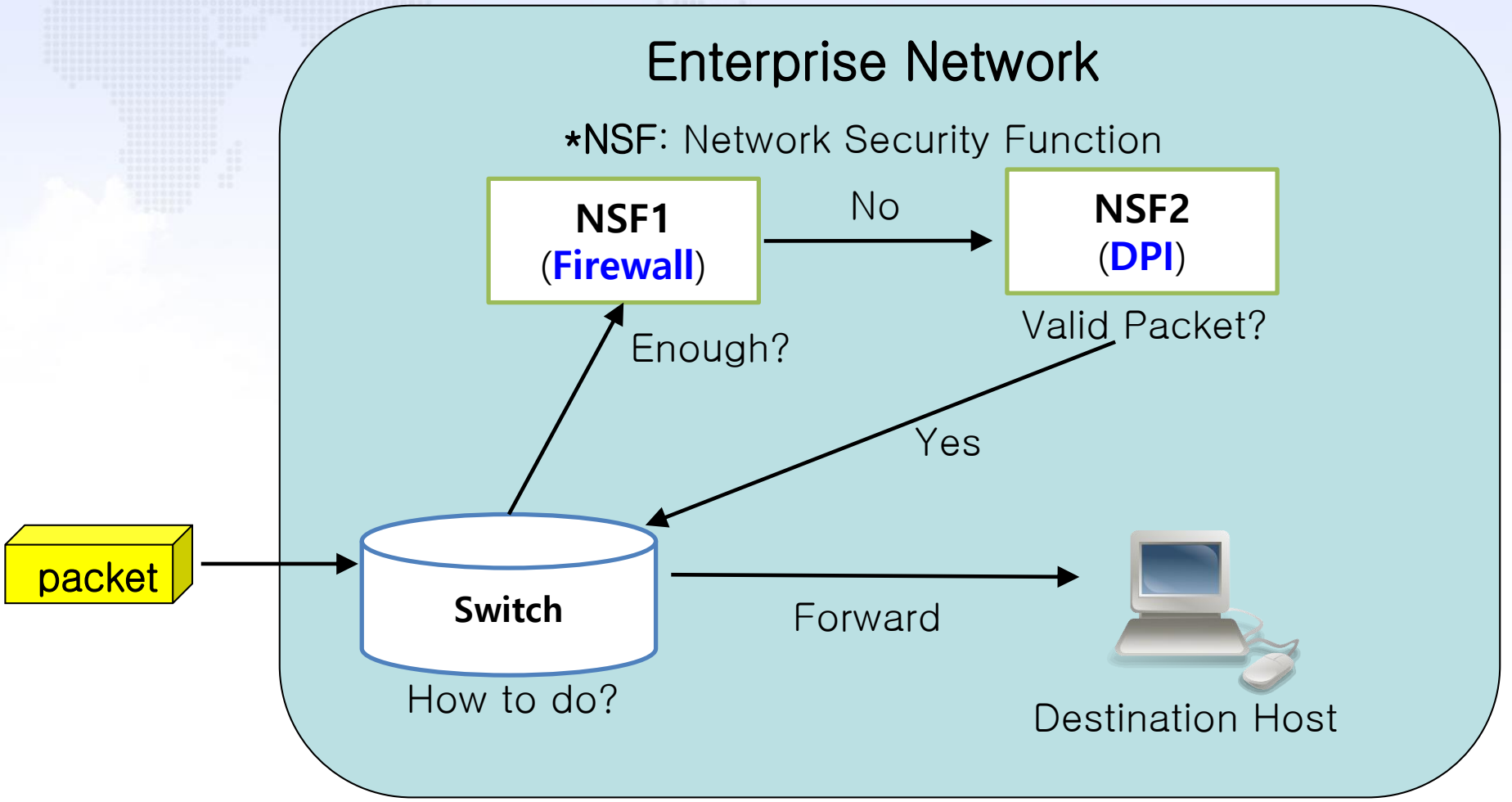
- Firewall
- DPI for VoIP-VoLTE Security Service

Mission

- Firewall
  - ✓ Deletion of policy
  - ✓ Update of policy
  - ✓ Avoidance of the duplication of policy
- VoIP-VoLTE Security Service
  - ✓ Deletion of policy
  - ✓ Update of policy
  - ✓ Avoidance of the duplication of policy

성균관대학교 SUNGKYUNKWAN UNIVERSITY ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute kt

What are Network Security Functions (NSFs)?



Goal of I2NSF Project

Given the code base of I2NSF Framework for provisioning Network Security Functions (NSFs), we implemented two things:

(i) Firewall for Web-filtering in I2NSF Framework using SDN and

(ii) Deep Packet Inspection (DPI) for VoIP/VoLTE Security Service in I2NSF Framework.

Contributions for the Goal

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

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

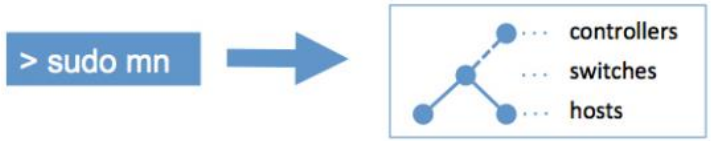
3. **Feasibility of Data-driven Approach (YANG) for Network Security Services.**

Hackathon Development

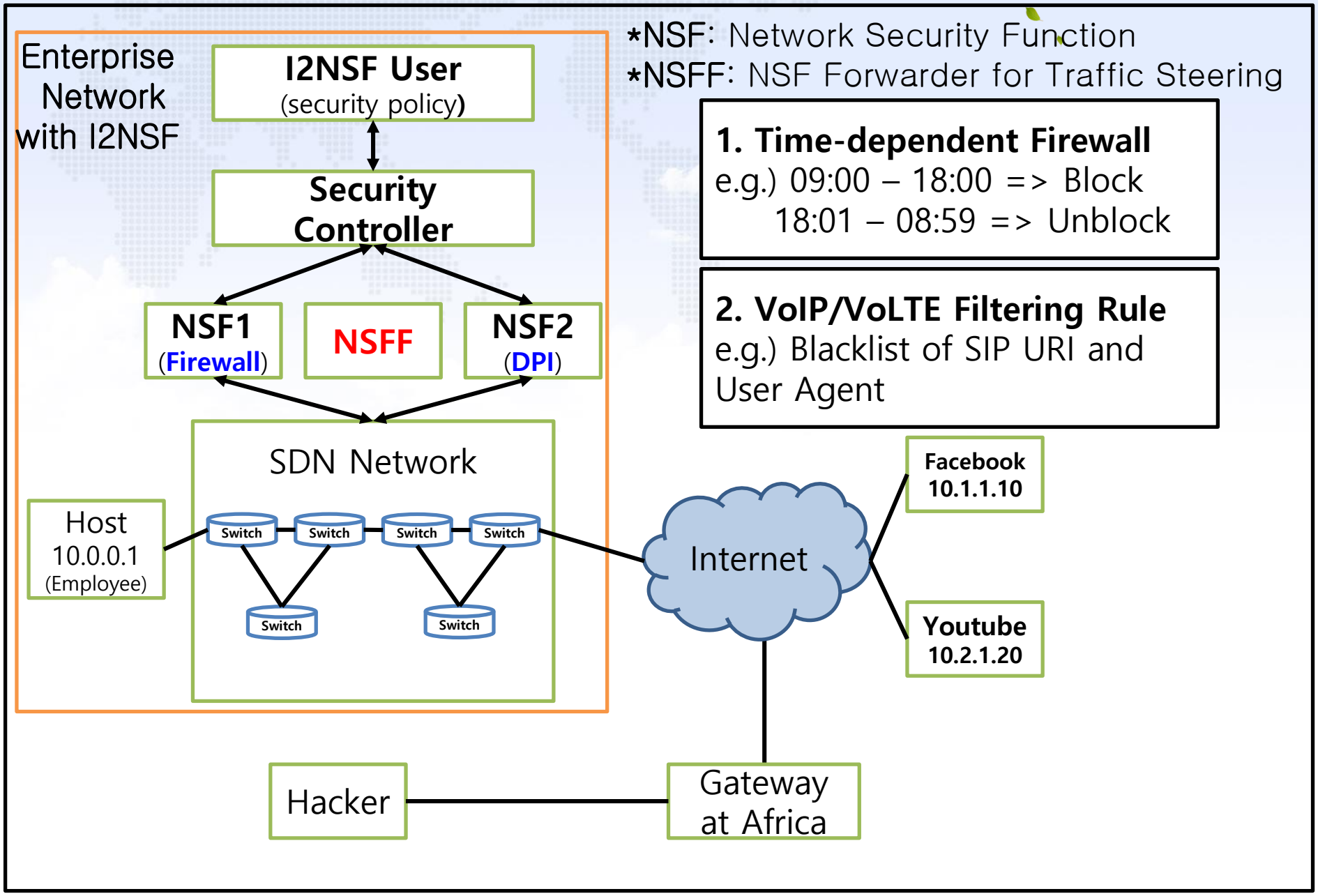
Building Environment

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



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 NETCONF
   - **OpenDaylight** for SDN Controller
   - **Mininet** for SDN Network
   - **RestAPI** for I2NSF Interface
2. **Validity of I2NSF Interface Design** for I2NSF Framework:
   - Firewall for Web Filtering
   - DPI for VoIP/VoLTE (e.g., Blacklist and Whitelist)
3. **Feasibility of Data-driven Approach** (YANG) for Network Security:
   - YANG Data Models for I2NSF Interfaces among System Entities (I2NSF User, Security Controller, NSFs)