

# Report of I2NSF Hackathon Project @ IETF-97 Hackathon November 14, 2016



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

# Why did we do 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!!

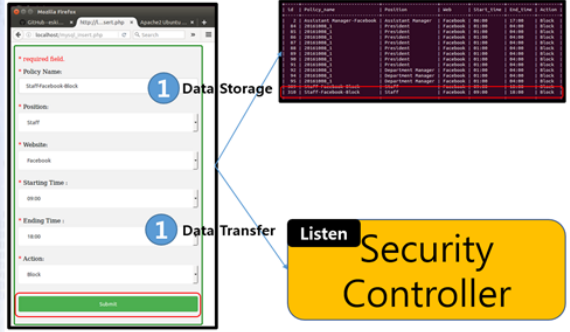
- 25 new 1<sup>st</sup> timers at IETF
- Put Code on Web

# 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)



## I2NSF Client (Web)



## 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

## Professors

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

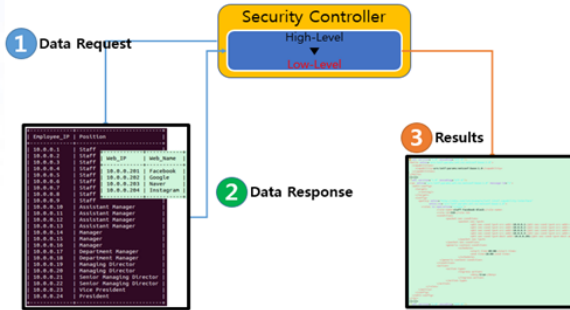
## Collaborators

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

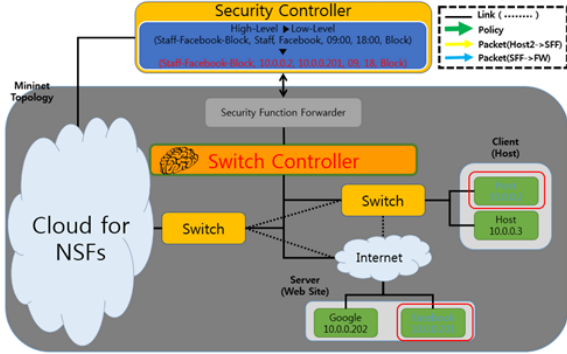
## Students

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

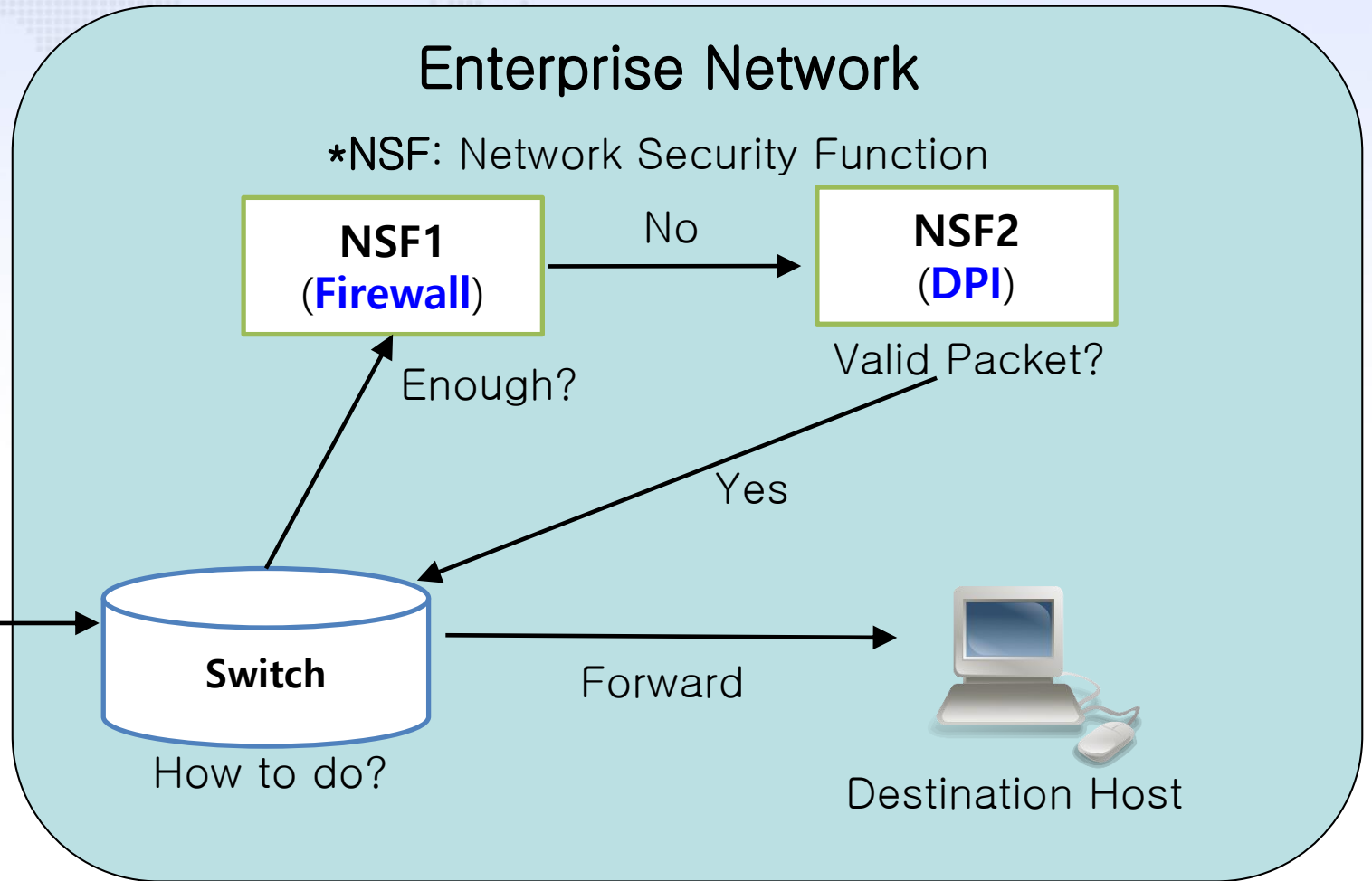
## Security Controller



## Network Security Functions (NSF) -Triggered Steering



# 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.**



# Environment of Hackathon Development

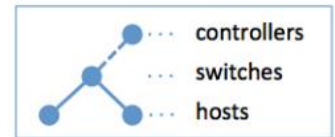
## Building Environment

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

```
> sudo mn
```



ubuntu

# **I2NSF Drafts** of this I2NSF Project

## **I2NSF Working Group Drafts**

<https://tools.ietf.org/html/draft-ietf-i2nsf-framework-04>

<https://tools.ietf.org/html/draft-hares-i2nsf-capability-data-model-00>

<https://tools.ietf.org/html/draft-kim-i2nsf-nsf-facing-interface-data-model-00>

<https://tools.ietf.org/html/draft-jeong-i2nsf-sdn-security-services-05>

<https://tools.ietf.org/html/draft-kim-i2nsf-security-management-architecture-03>

<https://tools.ietf.org/html/draft-kim-i2nsf-consumer-facing-interface-dm-00>

<https://tools.ietf.org/html/draft-hyun-i2nsf-nsf-triggered-steering-00>

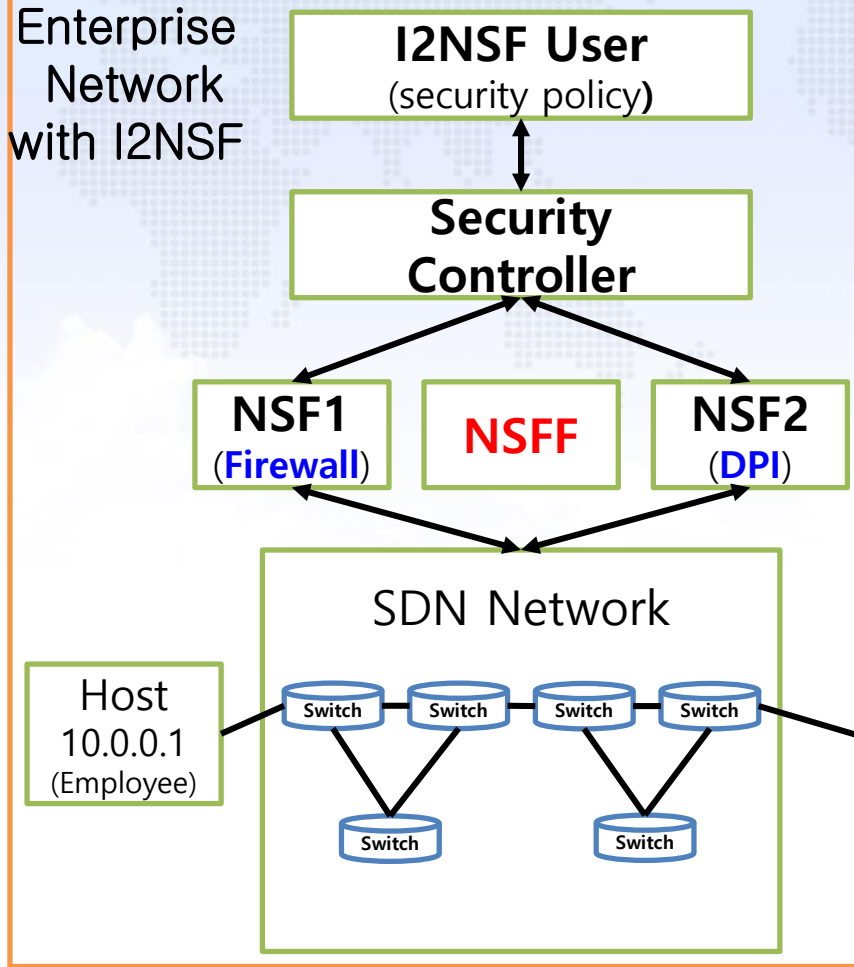
<https://tools.ietf.org/html/draft-hyun-i2nsf-registration-interface-im-00>

<https://tools.ietf.org/html/draft-ahn-i2nsf-communications-security-use-case-01>



# Scenario of Security Services in I2NSF Testbed

Enterprise Network with I2NSF



- \*NSF: Network Security Function
- \*NSFF: NSF Forwarder for Traffic Steering

## 1. Time-dependent Firewall

e.g.) 09:00 – 18:00 => Block  
18:01 – 08:59 => Unblock

## 2. VoIP/VoLTE Filtering Rule

e.g.) Blacklist of SIP URI and User Agent

Facebook  
10.1.1.10

Youtube  
10.2.1.20

Hacker

Gateway  
at Africa

# **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)**

# Demonstration of I2NSF Implementation

YouTube Videoclip:

<https://www.youtube.com/watch?v=5iflpVt4l6U&feature=youtu.be>

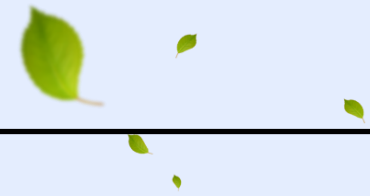
The screenshot shows a YouTube video player with a search bar at the top. The video content is a terminal window on the left and a network topology diagram on the right. The terminal window displays the following text:

```
*** Adding hosts:
admin dpi facebook firewall google instagram manager naver pkt_gen pr
aff_1 staff_2
*** Adding switches:
switch1 switch2 switch3 switch4
*** Adding links:
(admin, switch1) (dpi, switch1) (facebook, switch3) (firewall, switch
tch3) (instagram, switch3) (manager, switch4) (naver, switch3) (pkt_g
resident, switch4) (sff1, switch2) (staff_1, switch4) (staff_2, swit
switch2) (switch2, switch3) (switch2, switch4)
*** Configuring hosts
admin dpi facebook firewall google instagram manager naver pkt_gen pr
aff_1 staff_2
*** Starting controller
c0
*** Starting 4 switches
switch1 switch2 switch3 switch4 ...
*** Ping: testing ping reachability
admin -> X facebook firewall google instagram manager naver pkt_gen p
taff_1 staff_2
dpi -> admin facebook firewall google instagram manager naver pkt_gen
staff_1 staff_2
facebook -> admin dpi firewall google instagram manager naver pkt_gen
staff_1 staff_2
firewall -> admin dpi facebook google instagram manager naver pkt_gen
staff_1 staff_2
google -> admin dpi facebook firewall instagram manager naver pkt_gen
staff_1 staff_2
instagram -> admin dpi facebook firewall google manager naver pkt_gen
staff_1 staff_2
manager -> admin dpi facebook firewall google instagram naver pkt_gen
staff_1 staff_2
naver -> admin dpi facebook firewall google instagram manager naver p
kt_gen -> admin dpi facebook firewall google instagram manager naver
resident -> admin dpi facebook firewall google instagram manager naver
staff_1 staff_2
sff1 -> admin dpi facebook firewall google instagram manager naver pk
staff_1 staff_2
staff_1 -> admin dpi facebook firewall google instagram manager naver
ent sff1 staff_2
staff_2 -> admin dpi facebook firewall google instagram manager naver
ent sff1 staff_1
*** Results: 0% dropped (155/156 received)
*** Starting CLI:
mininet>
```

The network topology diagram on the right shows a central switch (switch1) connected to four other switches (switch2, switch3, switch4, and switch5). Each of these four switches is connected to a corresponding host (dpi, facebook, firewall, google, instagram, manager, naver, pkt\_gen, resident, sff1, staff\_1, staff\_2). The diagram is titled "www.Bandicam.co.kr" and "OPEN DAYLIGHT Topology".

Demo Slides: <https://github.com/kimjinyong/i2nsf-framework/blob/master/Hackathon/Doc/All%20about%20Hackathon.pptx>

# More Information of this Project



## 1. **GitHub** for I2NSF Open Source Project:

- Link: <https://github.com/kimjinyong/i2nsf-framework>
- Documents: <https://github.com/kimjinyong/i2nsf-framework/tree/master/Hackathon/Doc>
- Source Code: <https://github.com/kimjinyong/i2nsf-framework/tree/master/FullVersion>

## 2. **IETF-97 Hackathon** having this Project

- Link: <https://www.ietf.org/hackathon/97-hackathon.html>
- Wiki: <https://www.ietf.org/registration/MeetingWiki/wiki/97hackathon>
- Slides: <https://datatracker.ietf.org/meeting/97/session/hackathon>