

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

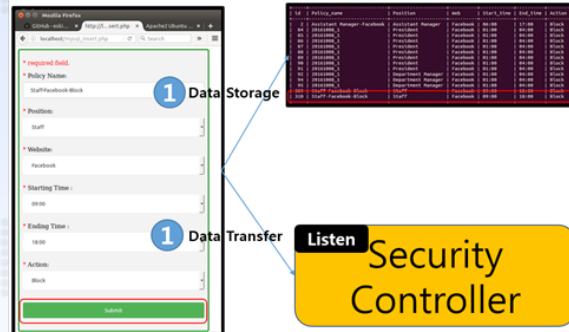
IETF I2NSF (Interface to Network Security Functions) Working Group: I2NSF Framework Project

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

IETF 98 Hackathon

I2NSF Framework Project

I2NSF Client (Web)



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

Professors

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

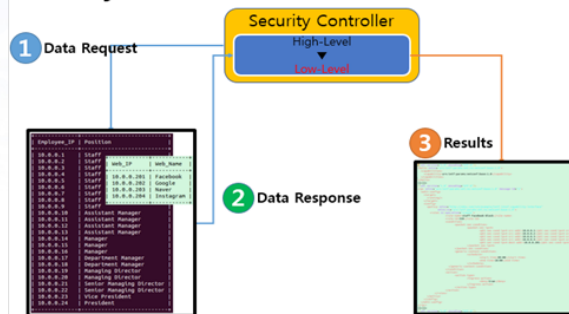
Collaborators

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

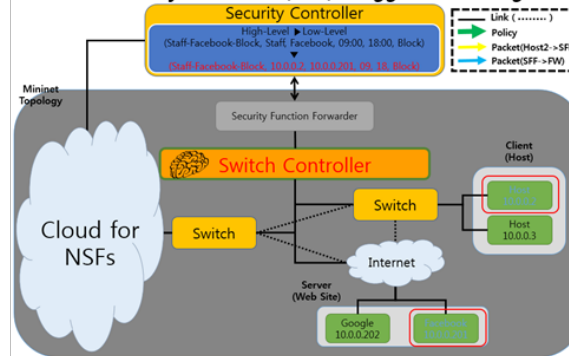
Students

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

Security Controller



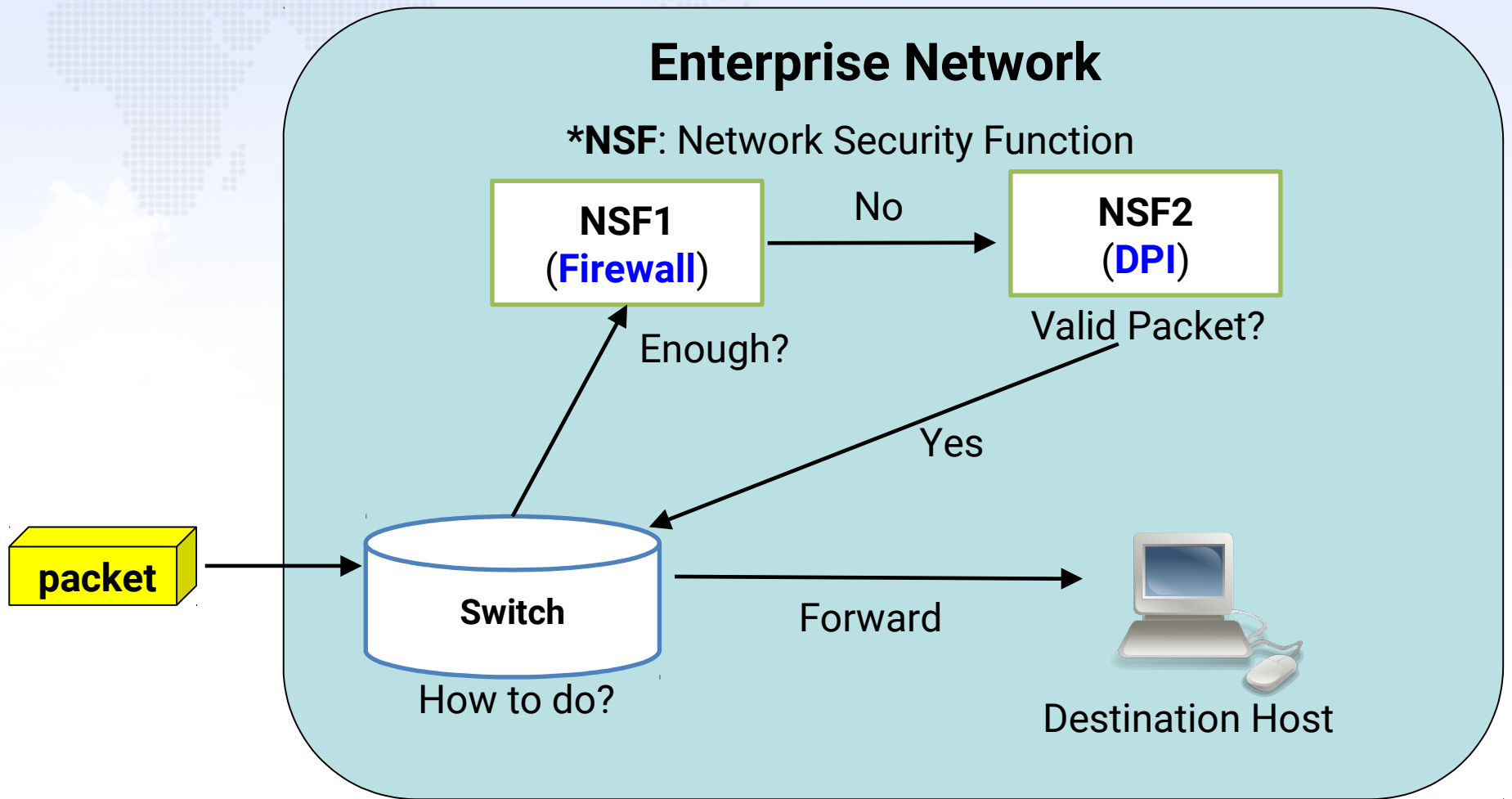
Network Security Functions (NSF) -Triggered Steering



Remote Participants at SKKU in Korea



What are Network Security Functions (NSFs)?



for provisioning Network Security Functions
Goal of I2NSF Project
(NSFs), we implemented one thing:

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

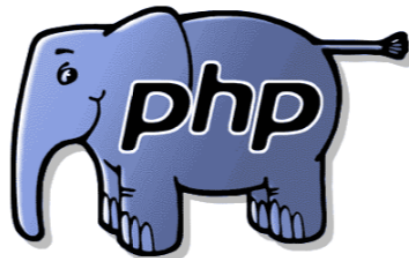
Contributions for the Goal

- 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

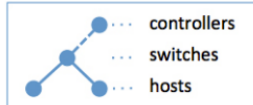
1. **OS**
 - Ubuntu 14.04TL
2. **Netconfd**
 - 6.2 Version
3. **Apache2**
 - 2.4.7 Version
4. **MySQL**
 - 14.14 Version
5. **PHP**
 - 5.5.9 Version



5. Mininet

- 2.2.1 Version

```
> sudo mn
```



6. OpenDaylight

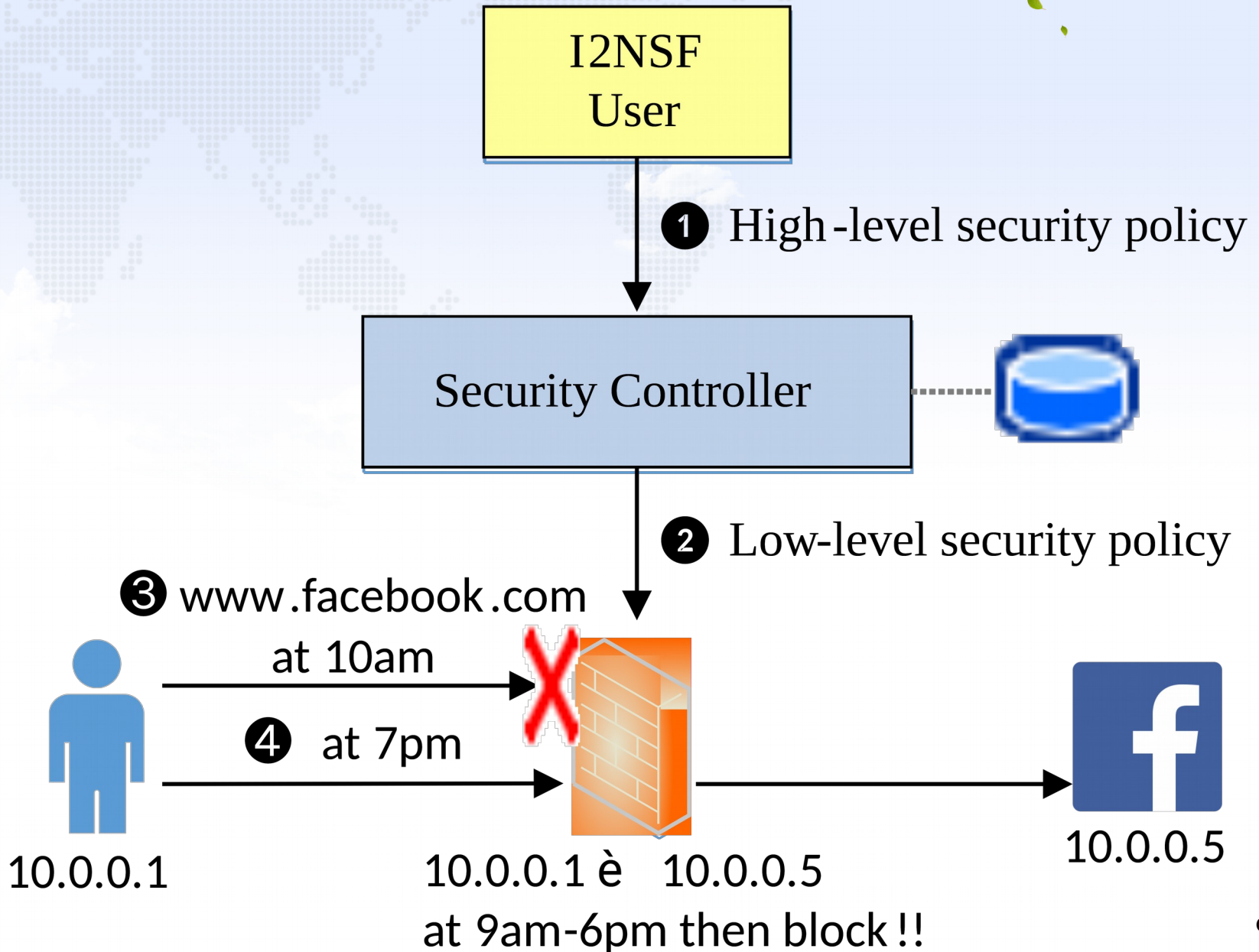
- Distribution-karaf-0.4.3-Beryllium-SR3

7. Suricata

- 3.2.1 RELEASE



Scenario of Security Services in I2NSF Testbed



Lessons from the Implementation @

1. Proof of Concept (POC) of I2NSF Framework Hackathon

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

The screenshot shows a web browser window displaying the GitHub repository page for `i2nsf-framework/Hackathon-98`. The browser's address bar shows the URL `https://github.com/kimjinyong/i2nsf-framework/tree/master/Hackathon-98`. The repository page includes a navigation bar with links for Features, Business, Explore, and Pricing, along with a search bar and a 'Sign in or Sign up' button. Below the navigation bar, the repository name `kimjinyong / i2nsf-framework` is displayed, followed by statistics for Watch (1), Star (0), and Fork (0). A tabbed interface shows 'Code' as the active tab, with other tabs for Issues (0), Pull requests (0), Projects (0), Pulse, and Graphs. The 'Code' tab displays the file structure for the `Hackathon-98` directory, including a 'FullVersion' folder (updated 23 hours ago) and a `README.txt` file (updated 3 days ago). The `README.txt` file is selected, showing its content: 'README for IETF-98 I2NSF Hackathon. This explains the source code and manual to remotely participate in IETF-98 I2NSF Hackathon. The following link contains the source code for our I2NSF Hackathon: https://github.com/kimjinyong/i2nsf-framework. If you follow this link, you will find a "Hackathon-98" folder which consists of 7 subfolders. The information about each folder is as follows:'.

Branch: master `i2nsf-framework / Hackathon-98 /` [Create new file](#) [Find file](#) [History](#)

kimjinyong Update Latest commit 1d6a339 23 hours ago

..

FullVersion	Update	23 hours ago
README.txt	test	3 days ago

README.txt

README for IETF-98 I2NSF Hackathon

This explains the source code and manual to remotely participate in IETF-98 I2NSF Hackathon.

The following link contains the source code for our I2NSF Hackathon:
<https://github.com/kimjinyong/i2nsf-framework>

If you follow this link, you will find a "Hackathon-98" folder which consists of 7 subfolders.
The information about each folder is as follows: