I2NSF Project @ IETF-99 Hackathon

IETF 99, Prague, Czech

July 16, 2017

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

Why Did We Do this Project?

- I2NSF: Use NETCONF + YANG Data Models
  - Is I2NSF 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 for Firewall and Web Filter?
- Result: I2NSF WG approach works, fast time to market
  - NM/OPS should expand their work into Security.
  - I2NSF follows up with other WGs (e.g., MILE, SACM, DOTS, and SECEVENT).
- Is this work a student project? – Yes!!
  - 7 graduate students at Sungkyunkwan University
  - Source Code on Github

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

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

Professors

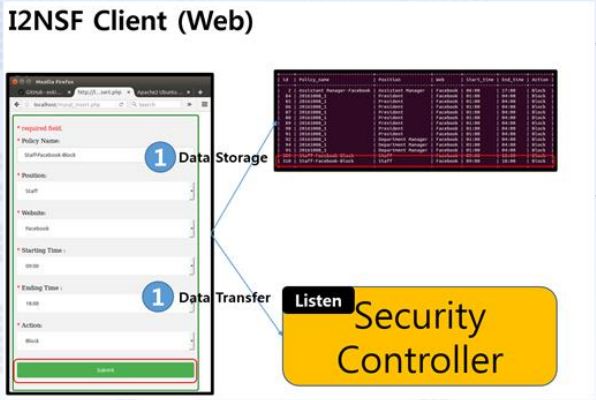
- Jaehoon (Paul) Jeong (Sungkyunkwan)
- Hyoungshick Kim (Sungkyunkwan)
- Sangwon Hyun (Sungkyunkwan)

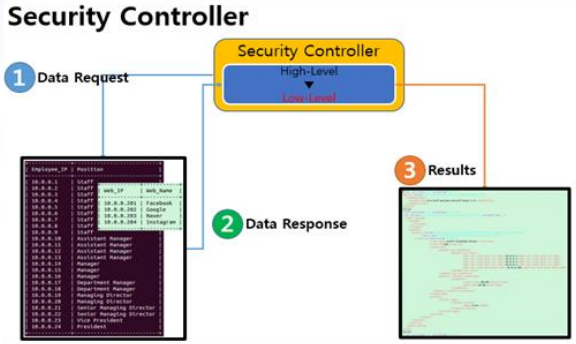
Collaborators

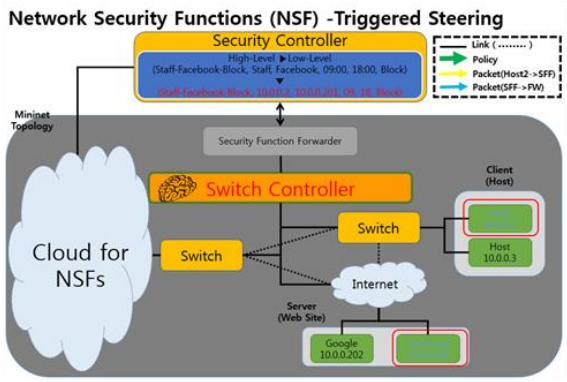
- Jung-Soo Park (ETRI)
- Tae-Jin Ahn (Korea Telecom)

Students

- Jinyong Tim Kim
- Daeyoung Hyun
- Eunsoo Kim
- Dongjin Hong
- Tae-Kyun Roh
- Sarang Wi
- Seungjin Lee







Where to get code

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

What to pull down to set-up environment

- OS: Ubuntu 14.04TL
- Confd for NETCONF: 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
- XSLT (Extensible StyleSheet Languages Transformations)

Manual for Operation Process

- README.txt

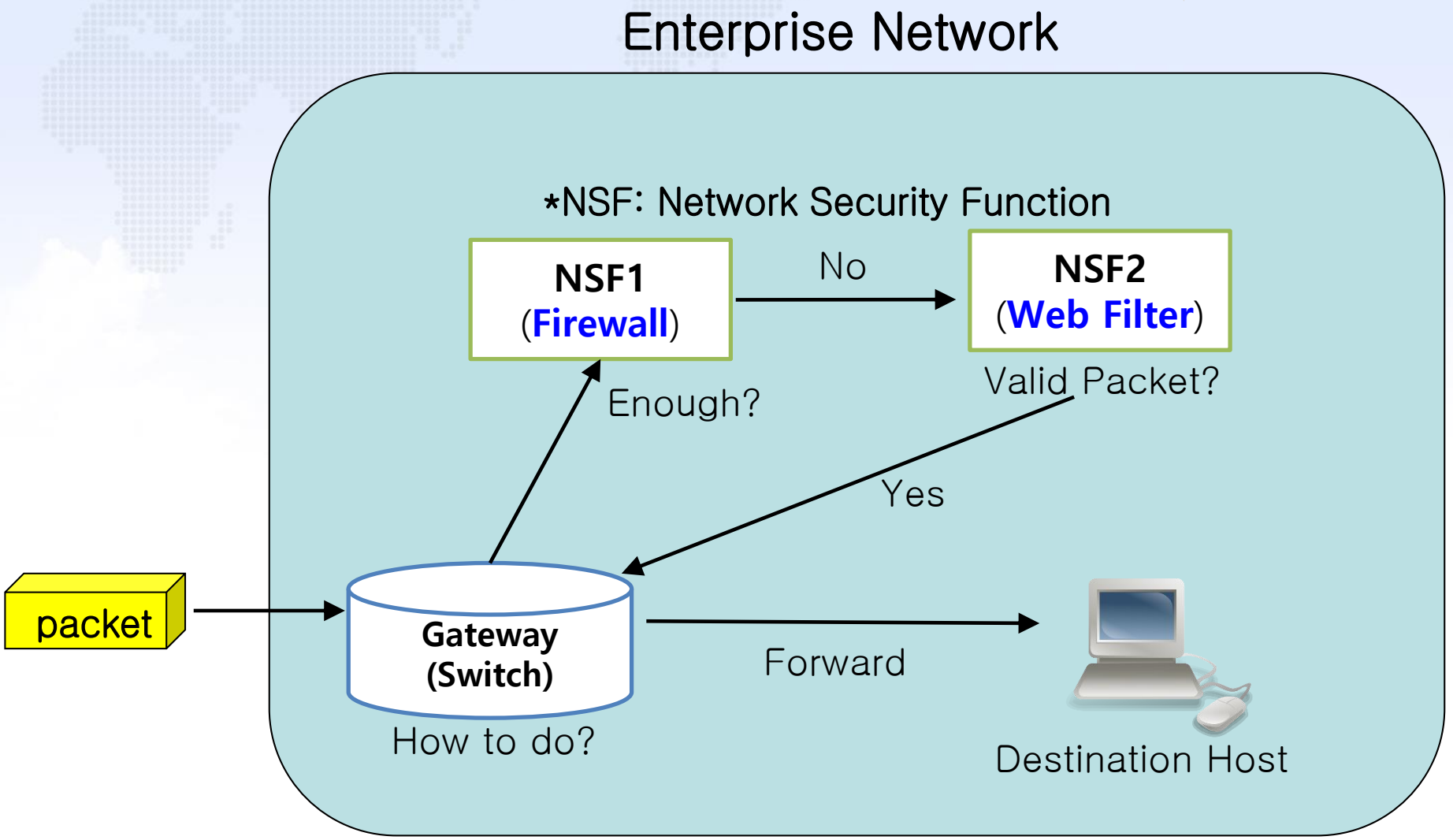
Contents of Implementation

- Firewall
- Web Filter

Mission

- Firewall and Web Filter for Enterprise
  - ✓ I2NSF User
    - ➢ Delivery of a high-level policy to security controller.
  - ✓ Security Controller
    - ➢ Translation from a high-level policy to a low-level policy.
    - ➢ NSF-Facing Interface for delivering a low-level policy to network security functions
  - ➢ Network Security Functions & Security Function Forwarder
    - ➢ Prototype of firewall and web filter

What are Network Security Functions (NSFs)?



Goal of I2NSF Project

I2NSF Framework is extended with

1. **Firewall for Port-based Packet Blocking using Suricata, which is an open source for IDS/IPS.**
2. **Web Filter for Content-based Packet Blocking using Suricata.**
3. **Service Function Chaining (SFC) for arranging the order of NSFs (e.g., Firewall and Web Filter).**
4. **Policy Translation using XSLT.**

Contributions for the Goal

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

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

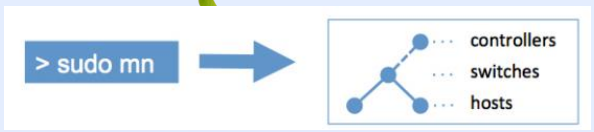
3. **Feasibility of Data-driven Approach (YANG) for Network Security Services.**

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

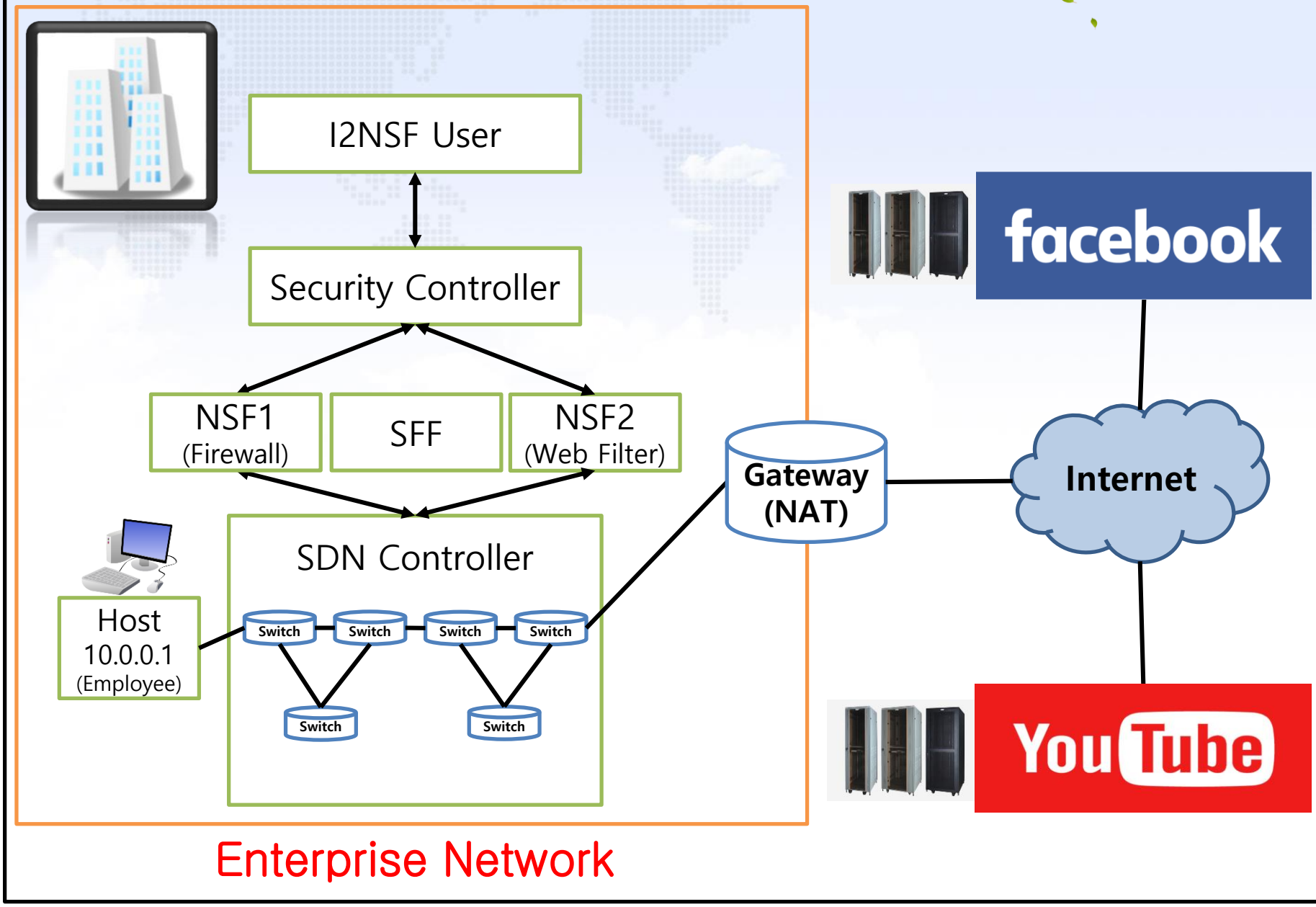
5. Mininet
   - 2.2.1 Version



6. OpenDaylight
   - Distribution-karaf-0.4.3-Beryllium-SR3
7. Suricata
   - 3.2.1 RELEASE
8. XSLT (Extensible StyleSheet Languages Transformations)
   - xsltproc

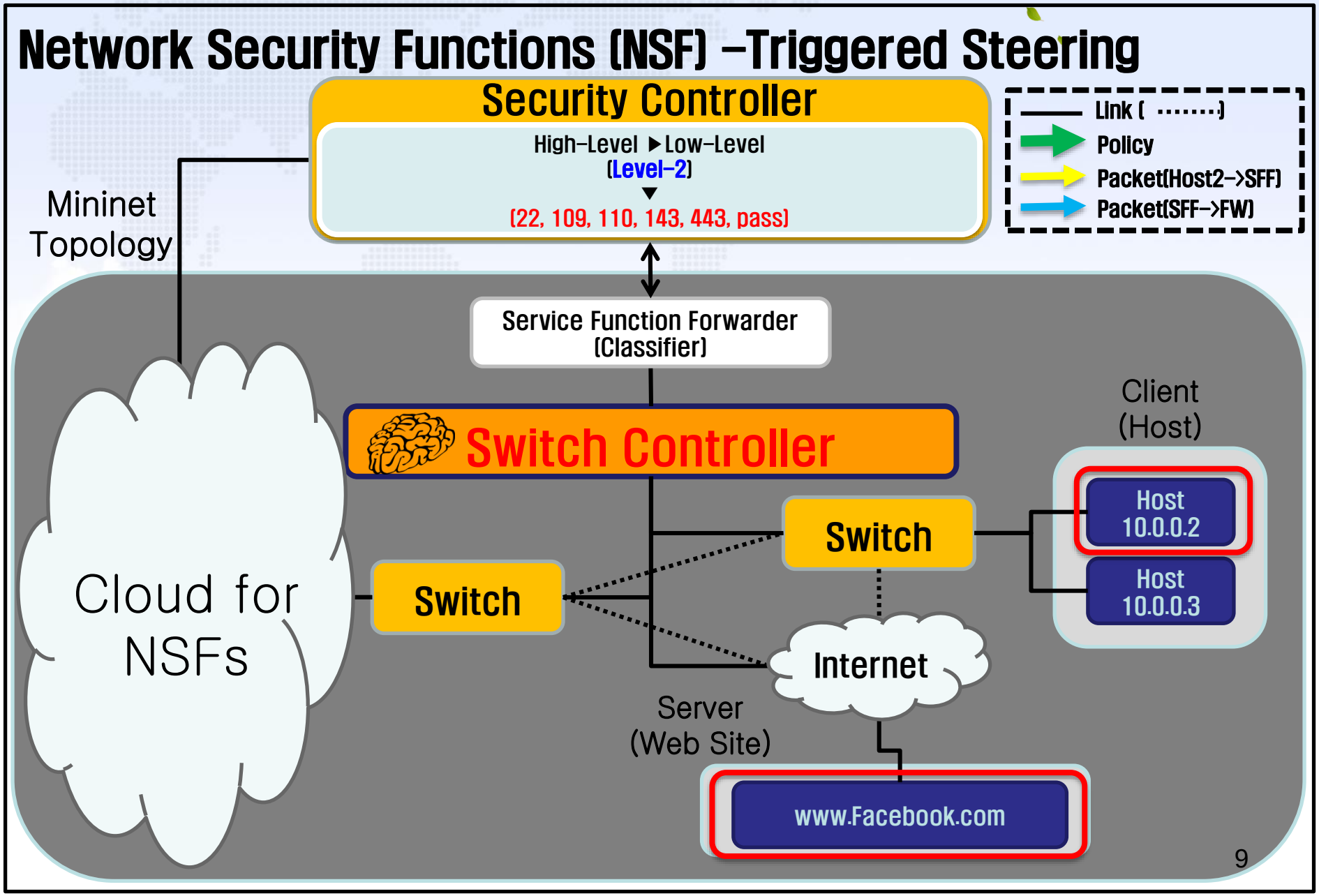
ubuntu

Network Configuration for Hackathon



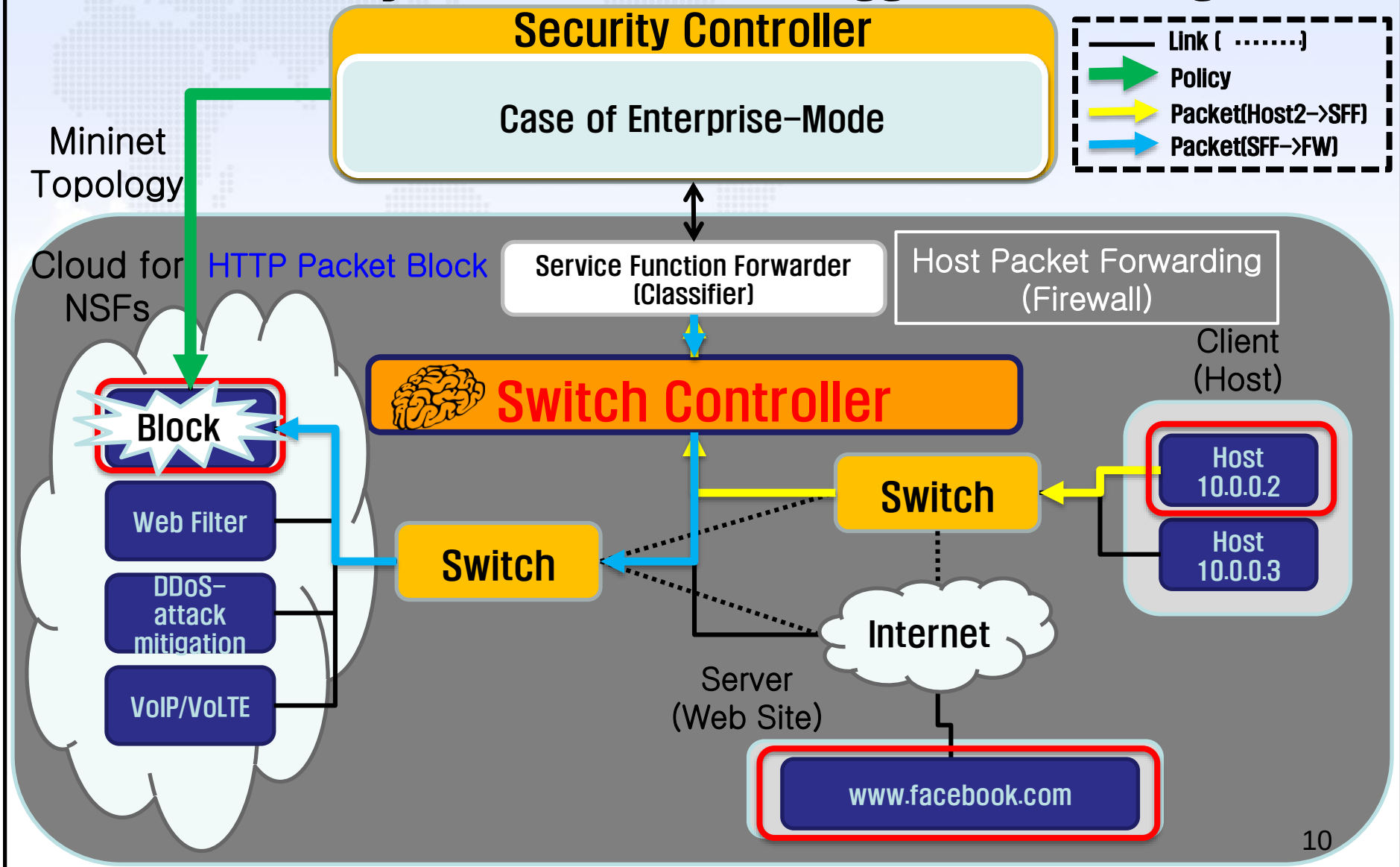
Enterprise Network with I2NSF Framework

Network Security Functions (NSF) –Triggered Steering



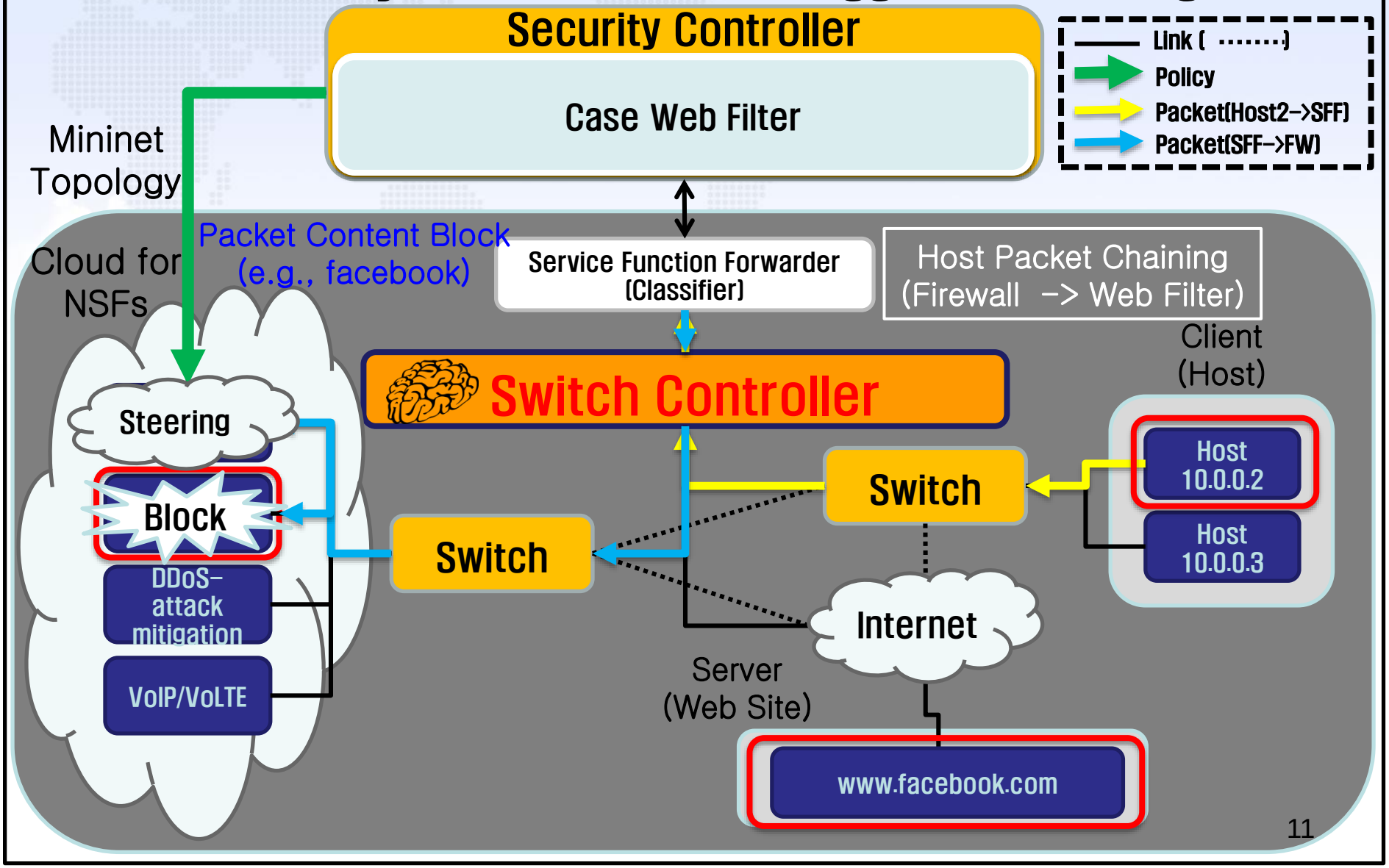
Firewall for HTTP Packet Blocking

Network Security Functions (NSF) –Triggered Steering



Web Filter for Packet Content Blocking

Network Security Functions (NSF) –Triggered Steering



Information of I2NSF Hackathon Project

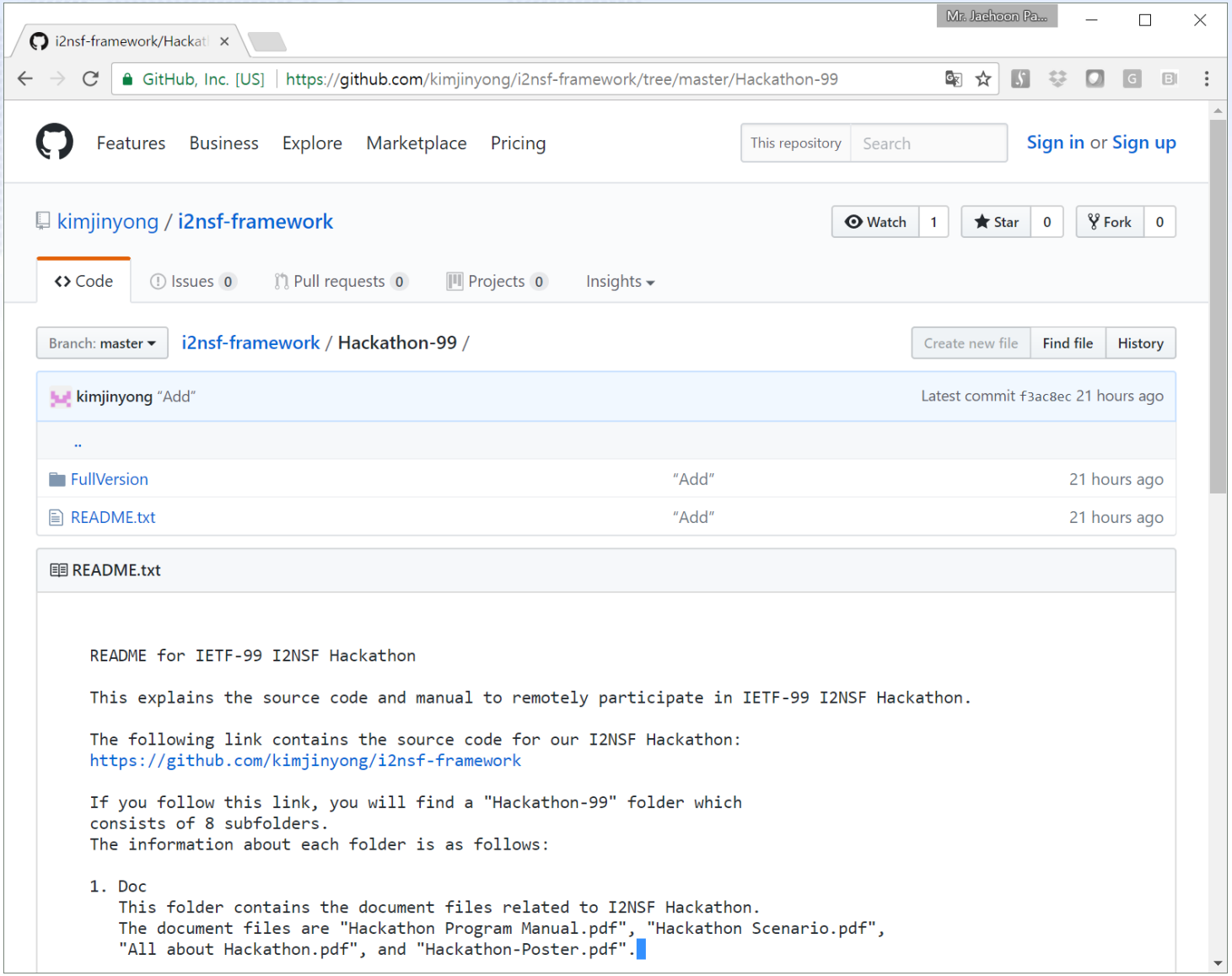
Github for I2NSF Hackathon and YouTube for Video Demonstration

1. Documents and Source Code
   https://github.com/kimjinyong/i2nsf-framework

2. YouTube Videoclip
   https://www.youtube.com/watch?v=fRCnQX2aFa4

Github Code of I2NSF Implementation

https://github.com/kimjinyong/i2nsf-framework/tree/master/ Hackathon-99



Lessons from the Implementation @ Hackathon

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