I2NSF Framework @ IETF-98 Hackathon

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
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)?

Enterprise Network

*NSF: Network Security Function

NSF1 (Firewall)

NSF2 (DPI)

Switch

packet

Forward

Destination Host

How to do?

Enough?

Valid Packet?

Enough?

Yes

No
Given the code base of I2NSF Framework for provisioning Network Security Functions (NSFs), we implemented one thing:

- **Firewall** for Web-filtering in I2NSF Framework using [Suricata](https://suricata-ids.org), which is an open source for IDS/IPS.
Contributions for the Goal

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


## Build Environment

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. OS</strong></td>
<td>Ubuntu 14.04TL</td>
</tr>
<tr>
<td><strong>2. Netconfd</strong></td>
<td>6.2 Version</td>
</tr>
<tr>
<td><strong>3. Apache2</strong></td>
<td>2.4.7 Version</td>
</tr>
<tr>
<td><strong>5. PHP</strong></td>
<td>5.5.9 Version</td>
</tr>
<tr>
<td><strong>5. Mininet</strong></td>
<td>2.2.1 Version</td>
</tr>
<tr>
<td><strong>6. OpenDaylight</strong></td>
<td>Distribution–karaf–0.4.3–Beryllium–SR3</td>
</tr>
<tr>
<td><strong>7. Suricata</strong></td>
<td>3.2.1 RELEASE</td>
</tr>
</tbody>
</table>
Scenario of Security Services in I2NSF Testbed

1. **High-level security policy**

- User
- Security Controller

2. **Low-level security policy**

- User
- Security Controller

- **Block**
  - www.facebook.com
  - at 10am
  - at 7pm

- **Access**
  - 10.0.0.1
  - 10.0.0.5
  - at 9am-6pm then block!!
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

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

Hackathon-98

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: