Applicability of Interfaces to Network Security Functions to Networked Security Services
(draft-jeong-i2nsf-applicability-01)

IETF 99, Prague, Czech
July 18, 2017

Jaehoon (Paul) Jeong*, Sangwon Hyun, Tae-Jin Ahn, Susan Hares, and Diego Lopez
Motivation of This Draft

- **I2NSF Applicability**
  - I2NSF Chartered Working Item
  - This draft explains how I2NSF framework and interfaces can be used for real network services.

- **Contents**
  - An I2NSF Framework with Software-Defined Networking (SDN)
  - Use Cases
    - Firewall
    - Deep Packet Inspection
    - Attack Mitigation
Why the Combination of I2NSF and SDN?

- **Accelerated Security Service**
  - SDN switch can perform simple firewall services.
  - SDN's flow table is good at basic security actions (e.g., forward, drop, and mirror).
  - Complicated security services (e.g., session-based firewall) can be performed at a close or remote NSF.

- **I2NSF Policy Rule Enforcement**
  - I2NSF User's firewall policies (according to the Capability Information Model) can be set up in both an NSF and SDN Switches via SDN Switch Control.
  - NSF-Facing Interface can be used for this configuration setup.
1. **I2NSF User** asks for security services with high-level security policies to **Security Controller** via **Consumer-Facing Interface**.

2. **Security Controller** delivers low-level security policies to NSFs and **Switch Controller** via **NSF-Facing Interface**.

3. **Network Security Function** configures such low-level security policies into its local system.

4. **Switch Controller** sets up filtering rules for the low-level policies on Switches via **Southbound Interface**.
Information and Data Models for I2NSF

- **Consumer-Facing Interface**
  - Information Model
    - draft-kumar-i2nsf-client-facing-interface-im-03
  - Data Model
    - draft-jeong-i2nsf-consumer-facing-interface-dm-02

- **NSF-Facing Interface**
  - Information Model
    - draft-xibassnez-i2nsf-capability-02
  - Data Model
    - draft-kim-i2nsf-nsf-facing-interface-data-model-02

- **Registration Interface**
  - Information Model
    - draft-hyun-i2nsf-registration-interface-im-02
  - Data Model
    - draft-hyun-i2nsf-registration-interface-dm-01
Security Service Procedure in I2NSF Framework

1. Consumer-Facing Interface (RESTCONF/YANG)
   - I2NSF User

2. NSF-Facing Interface (NETCONF/YANG)
   - Security Controller
     - High-level Policy
     - Low-level Policy

3. Southbound Interface (Openflow or I2RS)
   - Packet Filtering
     - Install new rules (e.g., drop packets with security policy)

4. Traffic Generation
   - Clients

5. Packet Filtering
   - Switch Controller
     - Switch\textsubscript{1}
     - Switch\textsubscript{2}
     - Valid packets
     - Invalid packets

6. Filter-Passed Packets
   - Outgoing packets

NSFs

Clients

Incoming packets
I2NSF Security Services with SDN

- **Firewall**
- **VoIP DPI**
- **DDoS-Attack Mitigator**

**Switch Controller**

Install new rules
(e.g., drop packets with suspicious patterns)

- **Incoming packets**
- **Switch**
  - Switch 1
  - Switch 2
  - Switch 3

(e.g., drop packets with suspicious patterns)
Use Cases

- Centralized Firewall System
  - This is for malicious packets.

- Centralized VoIP/VoLTE Security System
  - This is for Hacker’s invalid voice call packets.

- Centralized DDoS–Attack Mitigator
  - This is for DDoS–attack packets.
Centralized Firewall System (1/2)

1. Switch$_1$ forwards an unknown flow’s packet to Firewall via Switch Controller.
2. Firewall investigates the packet.
3. Firewall regards it as a malicious packet with suspicious patterns.
Centralized Firewall System (2/2)

The malicious packets are dropped by switches.

Firewall

Switch Controller

Install new rules (e.g., drop packets with suspicious patterns)

Report the malicious packet to Switch Controller

Incoming packets

Switch 1

Switch 2

Switch 3
Centralized VoIP/VoLTE System (1/2)

1. Switch$_1$ forwards an unknown flow's packet or mirrors a matched SIP packet to VoIP IPS Plus via Switch Controller.

2. VoIP IPS Plus analyzes the headers and contents of the forwarded packet.

3. VoIP IPS Plus regards the packet as a spoofed or scanning packet.
Centralized VoIP/VoLTE System (2/2)

VoIP DPI

Switch Controller

Install new rules
(e.g., block packets that have the same call-id)

The spoofed or scanning packets are dropped by Switches

Report a spoofed or scanning packet to Switch Controller

Incoming packets

Switch $1$

Cisco

Switch $2$

HP

Switch $3$

TP-LINK
Centralized DDoS-Attack Mitigator (1/2)

1. Switch\textsubscript{1} suspects a flow’s packets with inter-arrival patterns.
2. Switch\textsubscript{1} reports this flow to DDoS-Attack Mitigator via Switch Controller.
3. DDoS-Attack Mitigator computes a separate path for the suspicious flow.
Centralized DDoS-Attack Mitigator (2/2)

DDoS–Attack Mitigator

Switch Controller

Install new rules
(e.g., forward packets with suspicious inter-arrival patterns to a separate path with random drop)

Report the suspicious flow to Switch Controller

The suspicious flow’s packets are randomly dropped by Switch\(_3\) on the separate path

Incoming packets

Undropped Incoming packets
Next Steps

- Use Cases for SFC-based Security Function Chaining will be added.
  - Firewall and Web Filter
  - Firewall and DDoS-Attack Mitigator

- Reflection of I2NSF Hackathon Experience
  - This draft will be described in more detail with the experience and lessons from IETF I2NSF Hackathon Project.

- Can this draft be adopted as a WG document?

- Welcome your Feedback!