SDN-Based Security Services using I2NSF
draft-jeong-i2nsf-sdn-security-services-04

Updates of Version -04

• Korea Telecom (KT) joined as co-authors.
  – Tae-Jin Ahn and Se-Hui Lee

• A new use case is added as the third one.
  – VoIP/VoLTE
  – Note: Version -03 had two use cases:
    • Firewall
    • DDoS mitigator

• Two new requirements for VoIP/VoLTE are added:
  – To support the seamless services to mitigate network attacks.
  – To provide the dynamic control of network resources to mitigate network attacks.
I2NSF Architecture for VoIP IPS (1/2)

Application
Action
Parameter
OK
Cancel

Service-layer Interface

[High-Level Policy → Low-Level Policy]

(Event, Condition, Action)

(Time, VoIP/Context, mirror/IPS/drop)

Capability-layer Interface

VoIP IPS Plus
Firewall Plus
DDoS-Attack Mitigator Plus

Development Environment

<Platform>
OS: Linux-Ubunt-14.0

<App Gateway>
Language: Javascript, html, xml

<Security Controller>
Language: Python

<Security Functions>
C Language

<App Gateway-Security Controller Interface>
Rest API

<Security Controller-Security Function Interface>
NETCONF/YANG
I2NSF Architecture for VoIP IPS (2/2)

Security Functions

VoIP IPS Plus

Firewall Plus

DDoS-Attack Mitigator Plus

Southbound Interface

Switch Controller

Northbound Interface

Development Environment

<Security Functions>
VoIP IPS Plus: C Language
Firewall Plus: C Language
DDoS-Attack Mitigator Plus: C language

<Switch Controller>
Construction using OpenDaylight

<Switches>
Construction using Mininet

<Security Function-Switch Controller Interface>
Rest API

<Switch Controller-Switch Interface>
OpenFlow

Incoming packets

Switch \( \text{Switch}_1 \)

Switch \( \text{Switch}_2 \)

Switch \( \text{Switch}_3 \)
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 IPS Plus

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
Implementation based on OpenDaylight

Security Controller

High-Level Policy → Low-Level Policy

Script Command

`jinyong@jinyong-VirtualBox:~$ sudo ./autoconfiguration`

Service-layer Interface

(Shell Script)

Capability-layer Interface

(NETCONF/YANG)

VoIP IPS Plus

Switch Controller

Switch 1

Switch 2

Switch 3

Incoming packets

I2NSF Framework
Next Steps for this Draft

• Provisioning of the Information Model (and Data Model) needed for the VoIP/VoLTE for Security Controller, i.e.,
  – the Service-layer Interface between App Gateway (for VoIP/VoLTE) and Security Controller, and
  – the Capability-layer Interface between Security Controller and VoIP IPS Plus (as security function).

• Proto-type Implementation of VoIP/VoLTE in I2NSF Framework with SDN/NFV