An Architecture for Security Management in I2NSF Framework

(draft-kim-i2nsf-security-management-architecture-01)

Hyoungshick Kim, Hoon Ko, Sanghak Oh, Jaehoon Paul Jeong, and Se-Hui Lee

IETF 96, Berlin, Germany

July 21, 2016
Motivation

- A service provider *controls or governs* various security management systems in their cloud data centers.

- **Security Controllers** can be triggered by events at **NSFs** for a high-level policy update at **I2NSF Client**.

- It is hard for an administrator to define low-level action rules at a network level.
Objectives

- We propose a **security management architecture** that integrates additional components for security management into the I2NSF framework.
  
  - Propose the design of a **generic security management architecture** to support the enforcement of flexible and effective security policies in NSFs.
  
  - Provide the reflection of the updated low-level security policies for new security attacks for the corresponding high-level security policies.
- **Application Logic** generates a high-level policy in accordance with new security attacks.

- **Policy Updater** distributes such a policy to Security Policy Manager.

- **Security Policy Manager** maps the high-level policy into several low-level policies relevant to NSF capability.
  - Security Policy Manager delivers those policies to NSF through NSF Facing Interface.
Use Case: Security Management for VoIP-VoLTE

1) **VoIP-VoLTE Security Manager** generates a new high-level security policy and sends it to Policy Updater.
   - Blocking the list of illegal devices using IP address, source ports, etc.

2) **Policy Updater** distributes the high-level policy to Security Controller(s).

3) **Security Policy Manager** maps the high-level policy into several low-level policies and sends them to NSF.
1) NSF detects an anomalous message transmitted from an IP address and sends the IP address to Security Controller via NSF Facing Interface.

2) Security Controller delivers the IP address to Policy Collector.

3) Policy Collector forwards the IP address to VoIP-VoLTE Security Manager and VoIP-VoLTE Security Manager adds it to a blacklist.
Next Steps

- We will make the **information and data models of Client facing interface** at security management by referring to SUPA information model.

- We will develop a **reference implementation for our architecture**.

- We will prepare for our reference implementation as **Hackathon in IETF 97 Seoul Meeting** in November, 2016.