IETF-114 I2NSF WG Meeting

I2NSF WG Re-Chartering

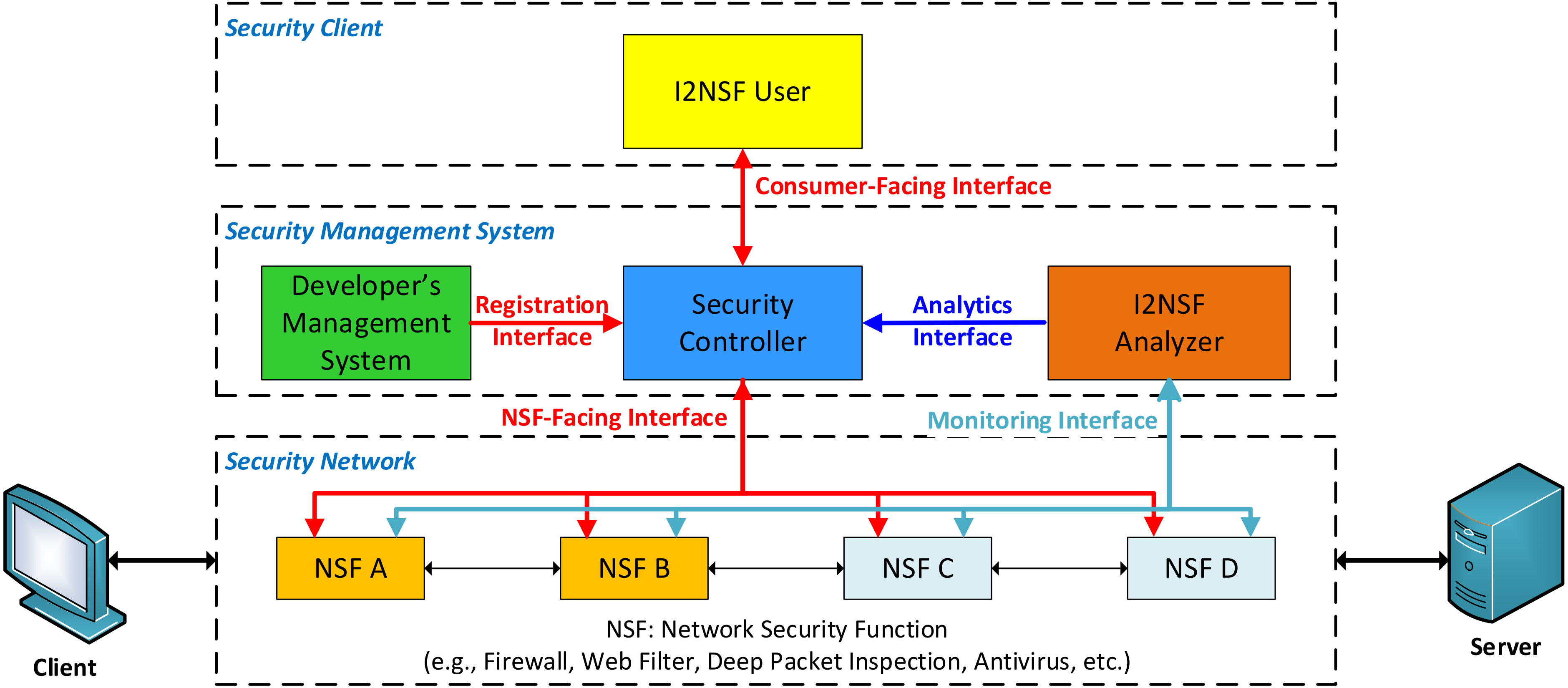
July 26, 2022
Philadelphia

Authors: Jaehoon (Paul) Jeong (SKKU) and Diego Lopez (Telefonica I+D)

(Email: pauljeong@skku.edu, diego.r.lopez@telefonica.com)

I E T F

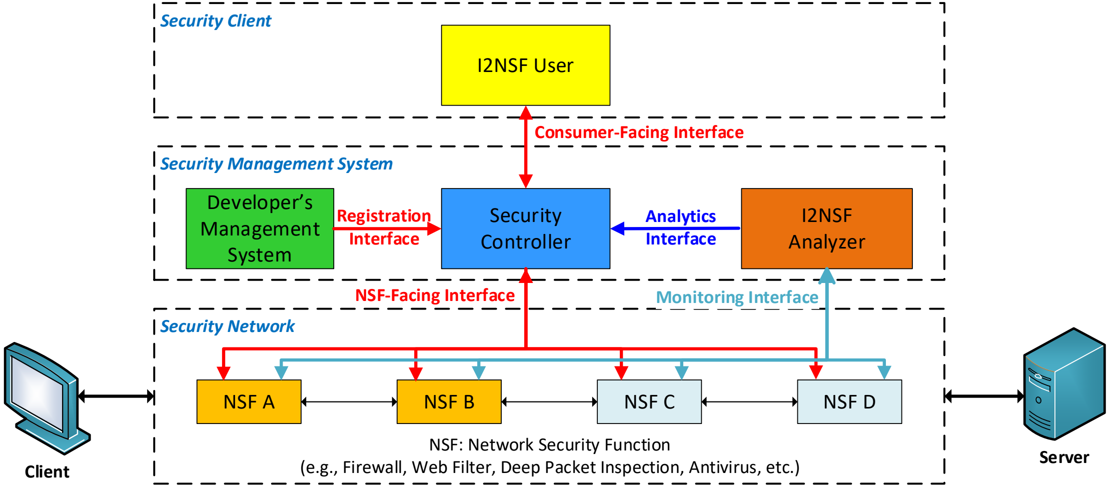
Security Management Automation in I2NSF



Source: An Extension of I2NSF Framework for Security Management Automation in Cloud-Based Security Services, draft-jeong-i2nsf-security-management-automation-04.

An Augmented I2NSF Framework: Interfaces

- Registration Interface
  - Developer's Management System (DMS) registers an NSF with Security Controller.
- Consumer-Facing Interface
  - I2NSF User delivers a high-level security policy to Security Controller.
- NSF-Facing Interface
  - Security Controller delivers a low-level security polity to an NSF.
- Monitoring Interface
  - An NSF delivers its monitoring data to I2NSF Analyzer.
- Analytics Interface
  - I2NSF Analyzer delivers its analytics information to Security Controller for policy (re)configuration.



I2NSF WG Re-chartering (1/8)

- **Introduction**

Interface to Network Security Functions (I2NSF) provides security function vendors, users, and operators with a standard framework and interfaces for cloud-based security services. The I2NSF framework for those security services consists of I2NSF User, Security Controller, Network Security Functions (NSF), Developer's Management System (DMS), and I2NSF Analyzer.

I2NSF WG Re-chartering (2/8)

- **Goals**

I2NSF Working Group (WG) will standardize a framework and interfaces for security management automation in an autonomous security system. For this goal, it is necessary to have a closed-loop security control consisting of security policy configuration, monitoring, notification, data analysis, analytics information delivery, and security policy (re)configuration. However, the following are needed for I2NSF:

I2NSF WG Re-chartering (3/8)

- **Goals (Con’t)**

1. The I2NSF framework needs a new interface (called Analytics Interface) to deliver feedback messages for a security policy from I2NSF Analyzer to Security Controller, or to share them among collaborating domains. In addition, a proper translation of the planned actions for a given security policy onto NSF capabilities requires a well-defined model for representing these actions in Security Controller.

I2NSF WG Re-chartering (4/8)

- **Goals (Con’t)**

2. The I2NSF framework needs Security Policy Translation from a high-level security policy to a low-level security policy. To build a security policy translator, a fundamental understanding is required for the relationship of Consumer-Facing Interface and NSF-Facing Interface. An exemplary architecture and procedure will be used for security policy translator.

I2NSF WG Re-chartering (5/8)

- **Goals (Con’t)**

3. I2NSF is vulnerable to insider and supply chain attacks. The security system may collapse if there is a malicious attack to the NSF capabilities registration, the I2NSF user security policies declaration, the Security Controller, or the monitoring data from an NSF. To prevent this malicious activity from happening in the I2NSF framework or detect the root of a security attack, all the activities in the I2NSF framework should be logged for auditing in a security audit system (e.g., remote attestation and Blockchain).

I2NSF WG Re-chartering (6/8)

- **Program of Work**

1. A single document for security management automation in I2NSF framework. This document will initially be used to enhance I2NSF framework for security management automation. It can be used as an applicability document for security management automation in real environments.

2. A YANG data model document for I2NSF Analytics Interface to deliver analytics information from I2NSF Analyzer to Security Controller.

I2NSF WG Re-chartering (7/8)

- **Program of Work (Con’t)**

3. A single document for Guidelines for Security Policy Translation to support the mapping between a high-level YANG module and a low-level YANG module. This document can give feedback to discussions by NETMOD and OPSAWG.

4. A YANG data model document for Remote Attestation for I2NSF components, based on the work of the RATS WG.

I2NSF WG Re-chartering (8/8)

- **Milestones**

1. November 2022 Adopt security management automation in I2NSF framework as a WG document

2. November 2022: Adopt a YANG data model for I2NSF Analytics Interface as a WG document

3. November 2022: Adopt guidelines for security policy translation as a WG document

4. March 2023: Adopt a YANG data model for Remote Attestation Interface as a WG document