IETF-114

I2NSF Analytics Interface

draft-lingga-i2nsf-analytics-interface-dm-00

July 26, 2022

Patrick Lingga, Jaehoon (Paul) Jeong, and Yunchul Choi

Sungkyunkwan University

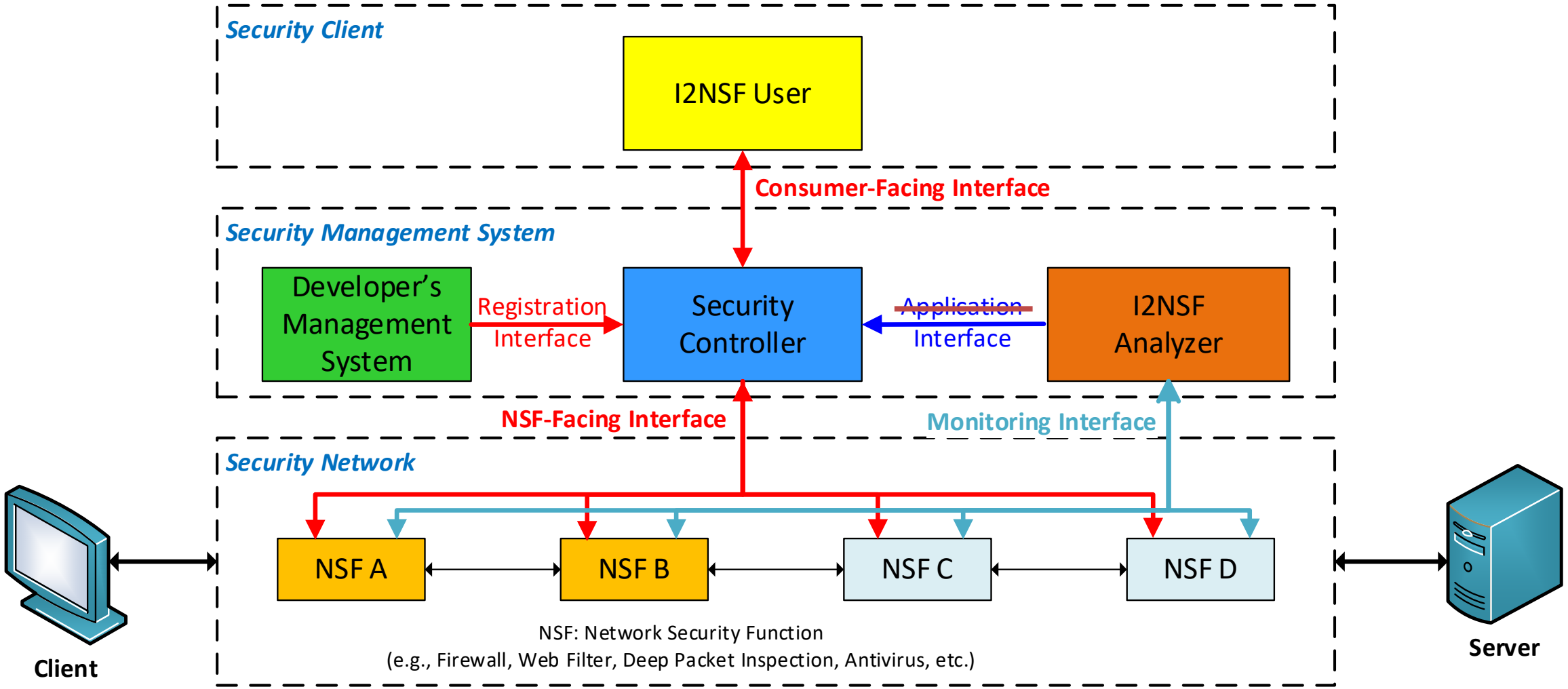
Major Update

- The Document Name and Title are changed to clarify a new interface to deliver Analytics Information based on NSF Monitoring Data.

- OLD
  - I2NSF Application Interface YANG Data Model
    - draft-lingga-i2nsf-application-interface-dm-03

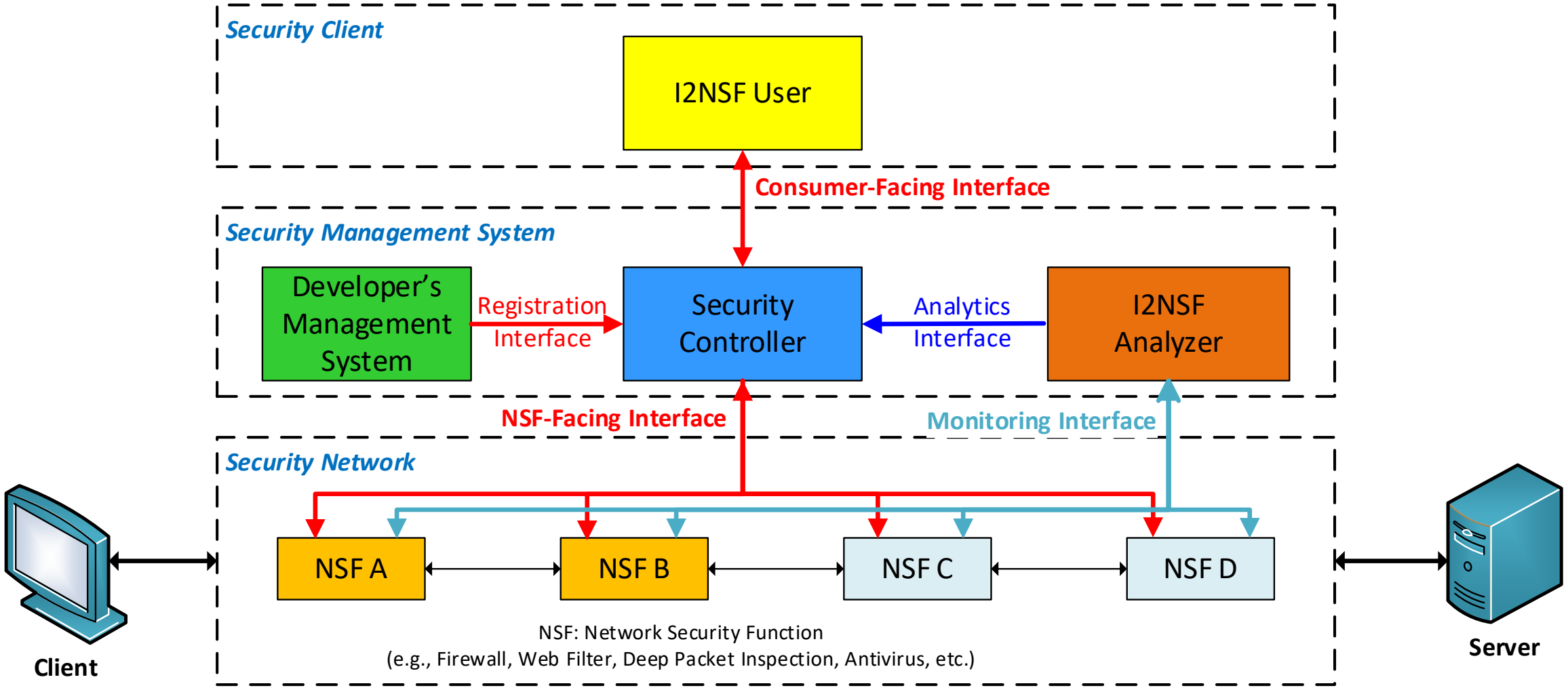
- NEW
  - I2NSF Analytics Interface YANG Data Model
    - draft-lingga-i2nsf-analytics-interface-dm-00

An Updated I2NSF Framework for Security Management Automation (1/2)



draft-lingga-i2nsf-application-interface-dm-03

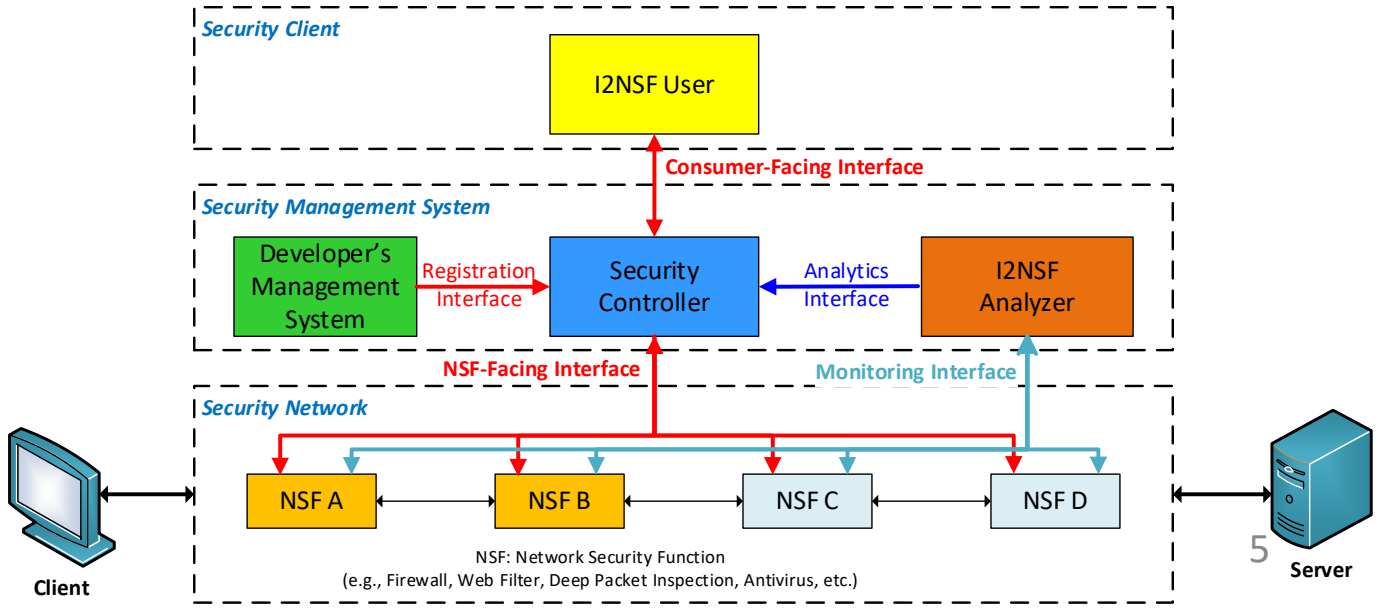
An Updated I2NSF Framework for Security Management Automation (2/2)



draft-lingga-i2nsf-analytics-interface-dm-00

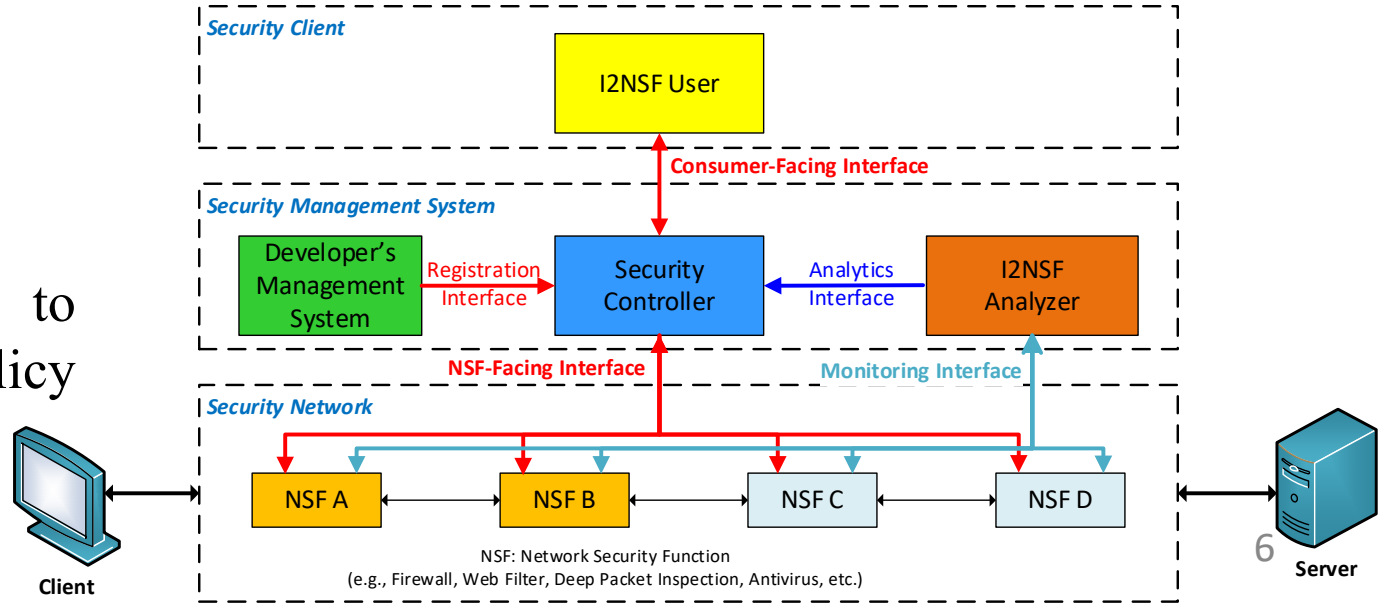
I2NSF Framework: Components

- I2NSF User
  - The user of the I2NSF Framework who controls and manipulates the configuration of NSF with a high-level security policy.
- Security Controller
  - The instance that controls the NSFs with the policy received from I2NSF user. It **translates** the high-level security policy into the low-level security policy.
- Developer's Management System (DMS)
  - The provider of the NSFs. It registers the capability of an NSF with Security Controller
- Network Security Functions (NSFs)
  - The network functions that provide security services for a target network.
- I2NSF Analyzer
  - The entity that collects monitoring data from NSFs and analyzes the activity and performance of NSFs for a closed-loop control.



I2NSF Framework: Interfaces

- Registration Interface
  - Interface used for DMS to register an NSF and its capabilities with Security Controller.
- Consumer-Facing Interface
  - Interface used for I2NSF User to deliver a high-level security policy to Security Controller.
- NSF-Facing Interface
  - Interface used for Security Controller to deliver a translated low-level security policy to the appropriate NSFs.
- Monitoring Interface
  - Interface used for an NSF to deliver its monitoring data to I2NSF Analyzer.
- Analytics Interface
  - Interface used for I2NSF Analyzer to deliver its analytics information to Security Controller for a closed-loop security control.



Motivation of I2NSF Analytics Interface

- The conditions of servers and networks are not stable and can change quickly in any circumstances.
  - A server can go down or an attack can happen at any given time.

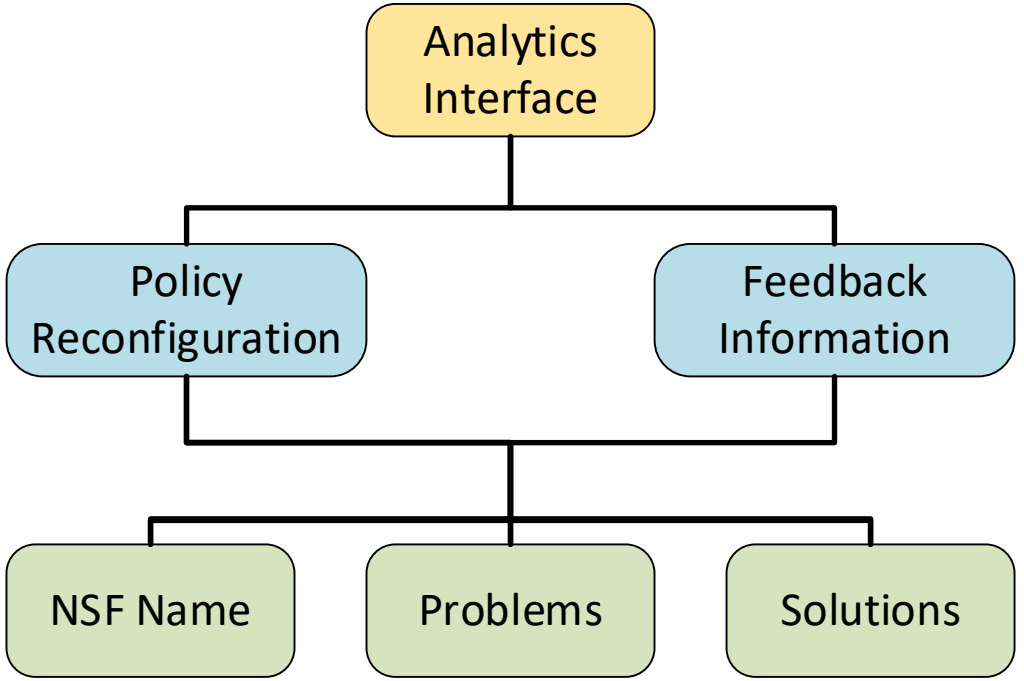
- It is important to have an analyzer to monitor and analyze the activity and performance of NSFs for a **closed-loop security control**.
  - It enhances network security through the analysis of monitoring data.

- The addition of the **I2NSF Analyzer** and **Analytics Interface** allows **Security Management Automation** in the I2NSF Framework.
  - It supports an automatic adaptation to the current network condition.

Analytics Interface

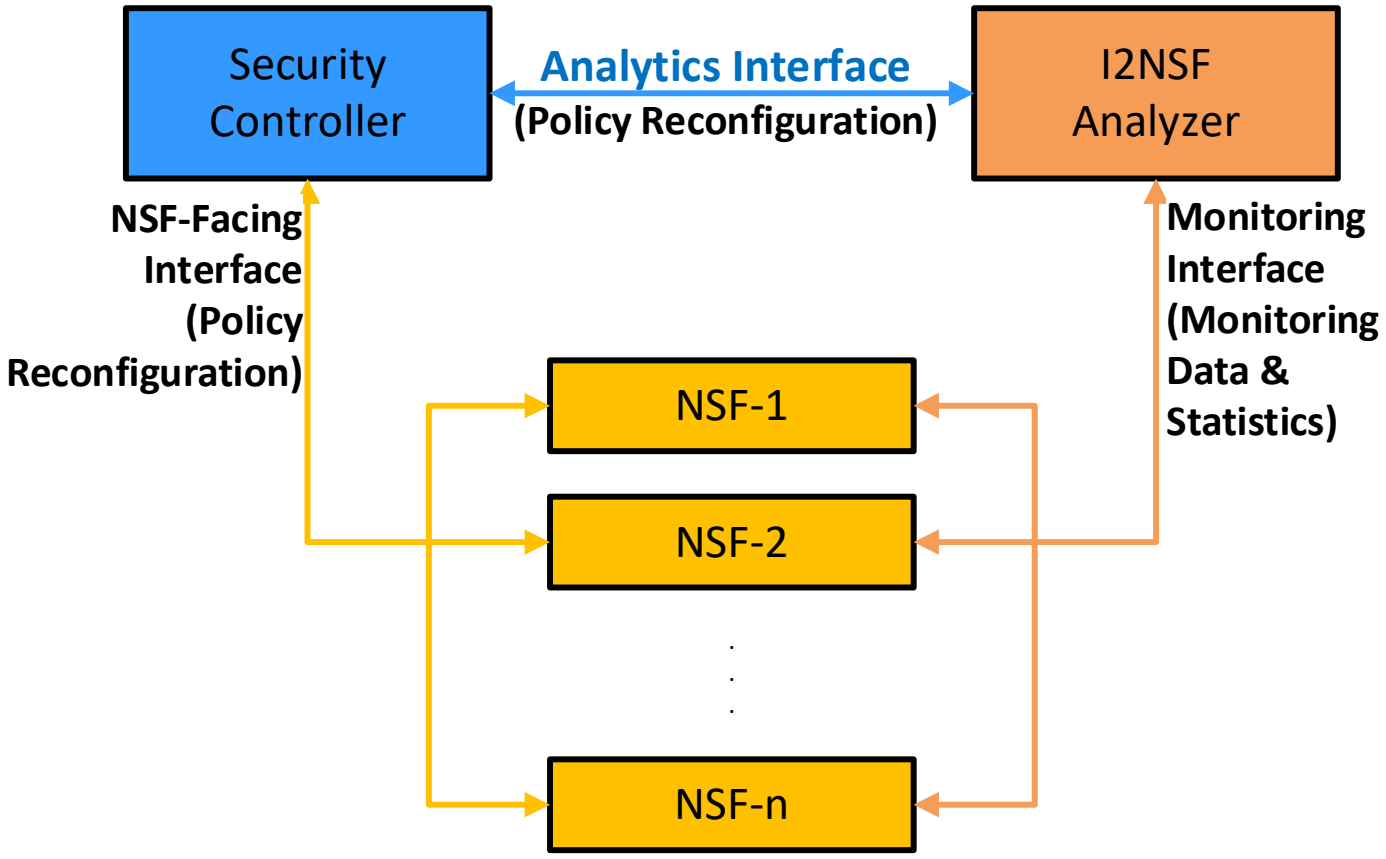
- Two Roles of Analytics Interface:
  1. **Policy Reconfiguration**
  2. **Feedback Information**

- Three fields for Analytics Interface:
  1. **NSF Name:** A name or an IP address of the NSF for identifying the NSF with problems.
  2. **Problem:** Issue(s) in the NSF that needs to be handled.
  3. **Solution:** Possible solution(s) for the problem.



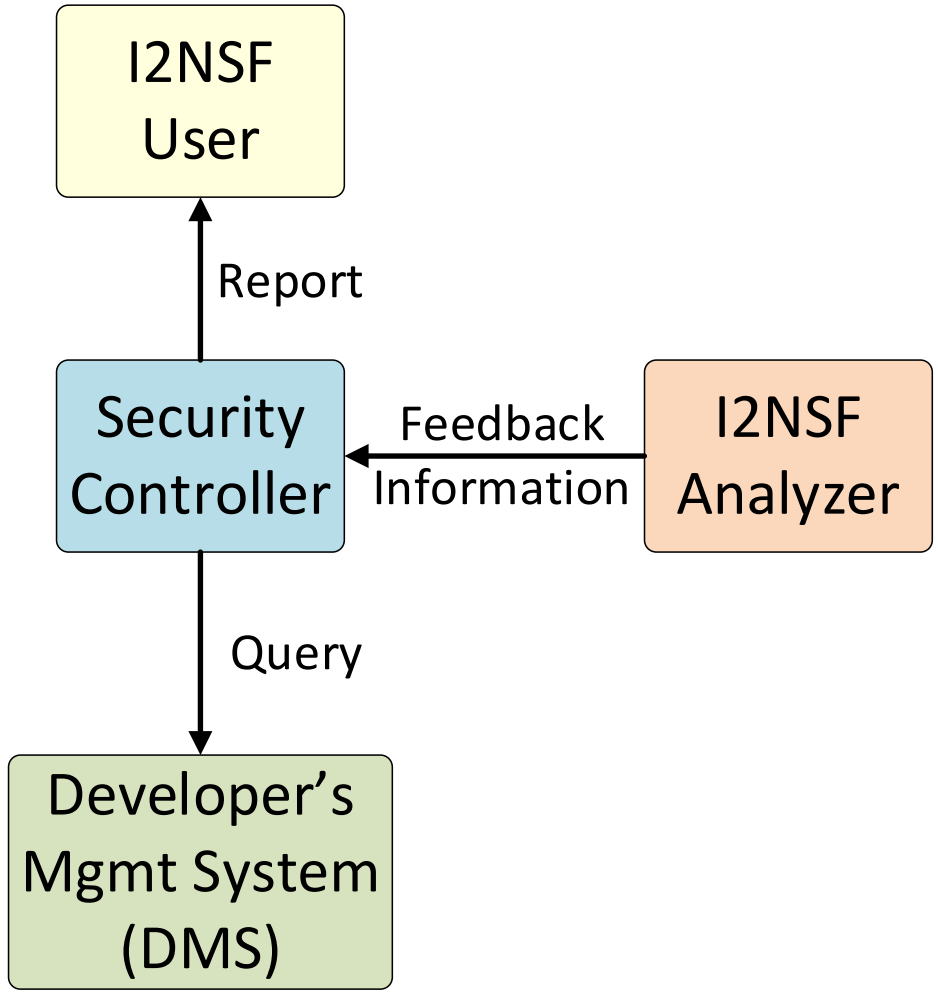
Policy Reconfiguration

- NSFs provide their monitoring data to I2NSF Analyzer.
- I2NSF Analyzer analyzes the monitoring data including NSF Events (e.g., DDoS attack) and makes (re)configuration of a security policy.
- Solutions suggested by I2NSF Analyzer are delivered to the appropriate NSFs through NSF-Facing Interface.



Feedback Information

- Feedback Information is used to tackle the problem(s) of an NSF system itself (e.g., system resource over-usage and malfunction).
- Since the feedback information is not a security policy, Security Controller takes an action to handle the reported problem(s).
- The action includes both the report to I2NSF User and the query for system resource management of the NSF(s) to DMS.



Next Step

- Analytics Interface is an interface for Security Management Automation with Closed-loop Security Control.
- Its YANG data model is based on with the existing I2NSF YANG data models (NSF-Facing and Monitoring Interfaces).
- It can facilitate both a report and query for Security Management Automation.
- This draft is proposed as a WG item in I2NSF Re-chartering.