IETF-116
I2NSF Analytics Interface

draft-lingga-i2nsf-analytics-interface-dm-01

March 30th, 2023

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

Sungkyunkwan University

Email: {patricklink, pauljeong}@skku.edu, cyc79@etri.re.kr

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.

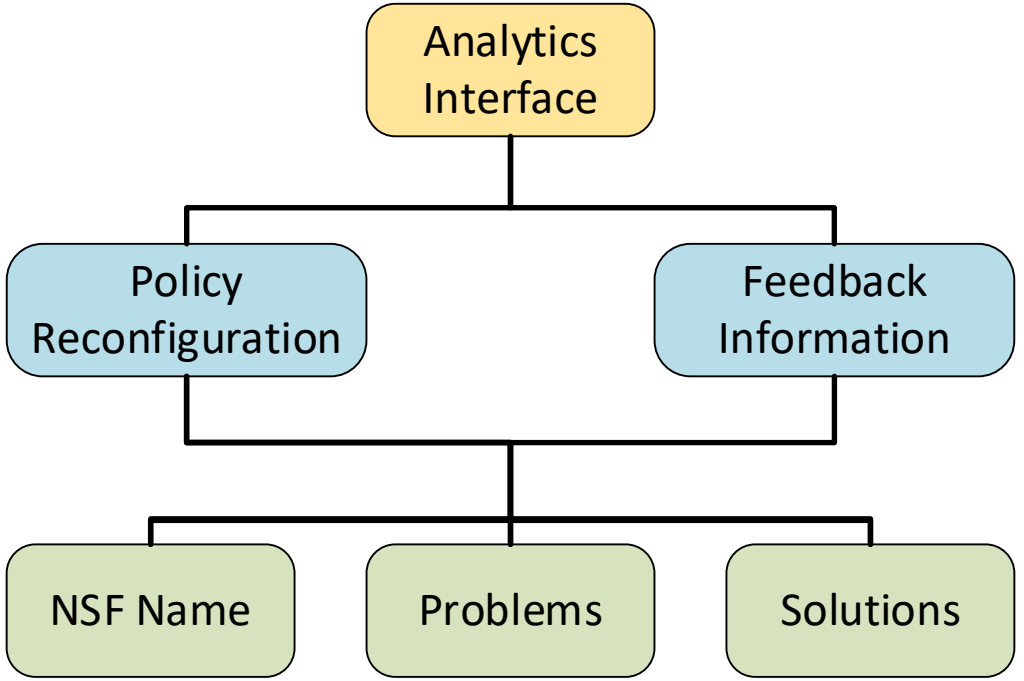
- It is important to have an analyzer to monitor and analyze the activity and performance of NSFs for a **closed-loop security control**.
  - It enhances network security through the analysis of monitoring data.

- 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

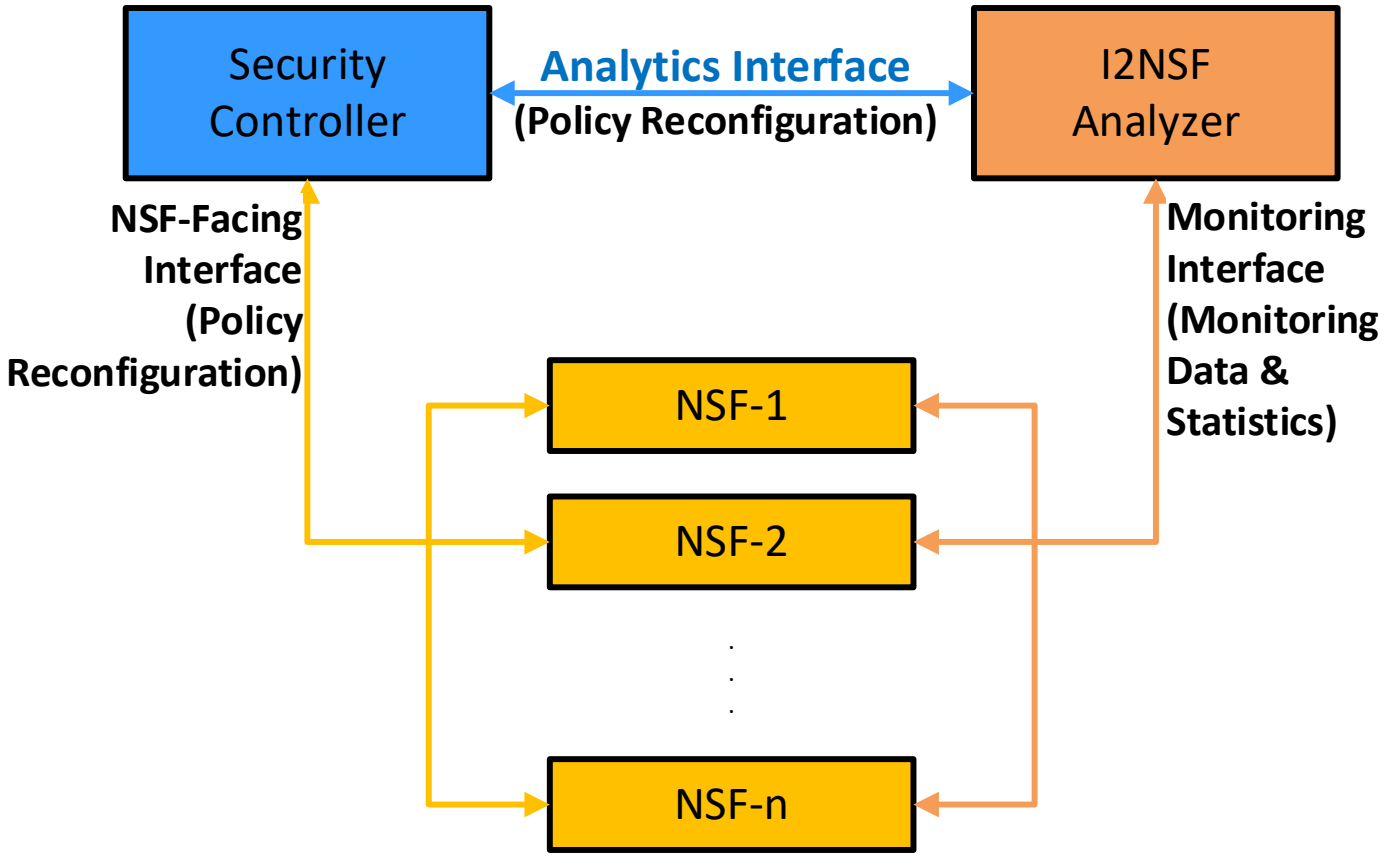
- Two Roles of Analytics Interface:
  1. **Policy Reconfiguration**
  2. **Feedback Information**

- 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.



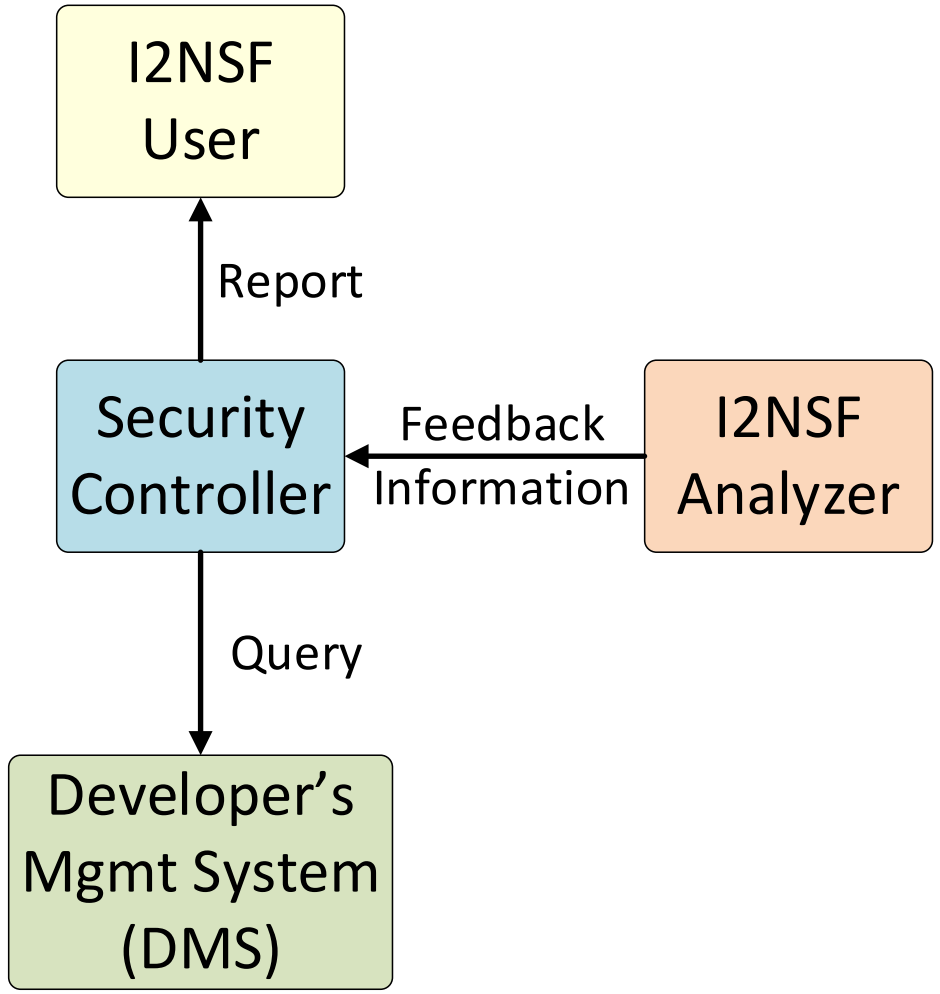
Policy Reconfiguration

- 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 (i.e., NSF-Facing and Monitoring Interfaces).

- **How to proceed with its standardization in IETF?**
  - Independent Submission or Another WG (e.g., OPSAWG)?