



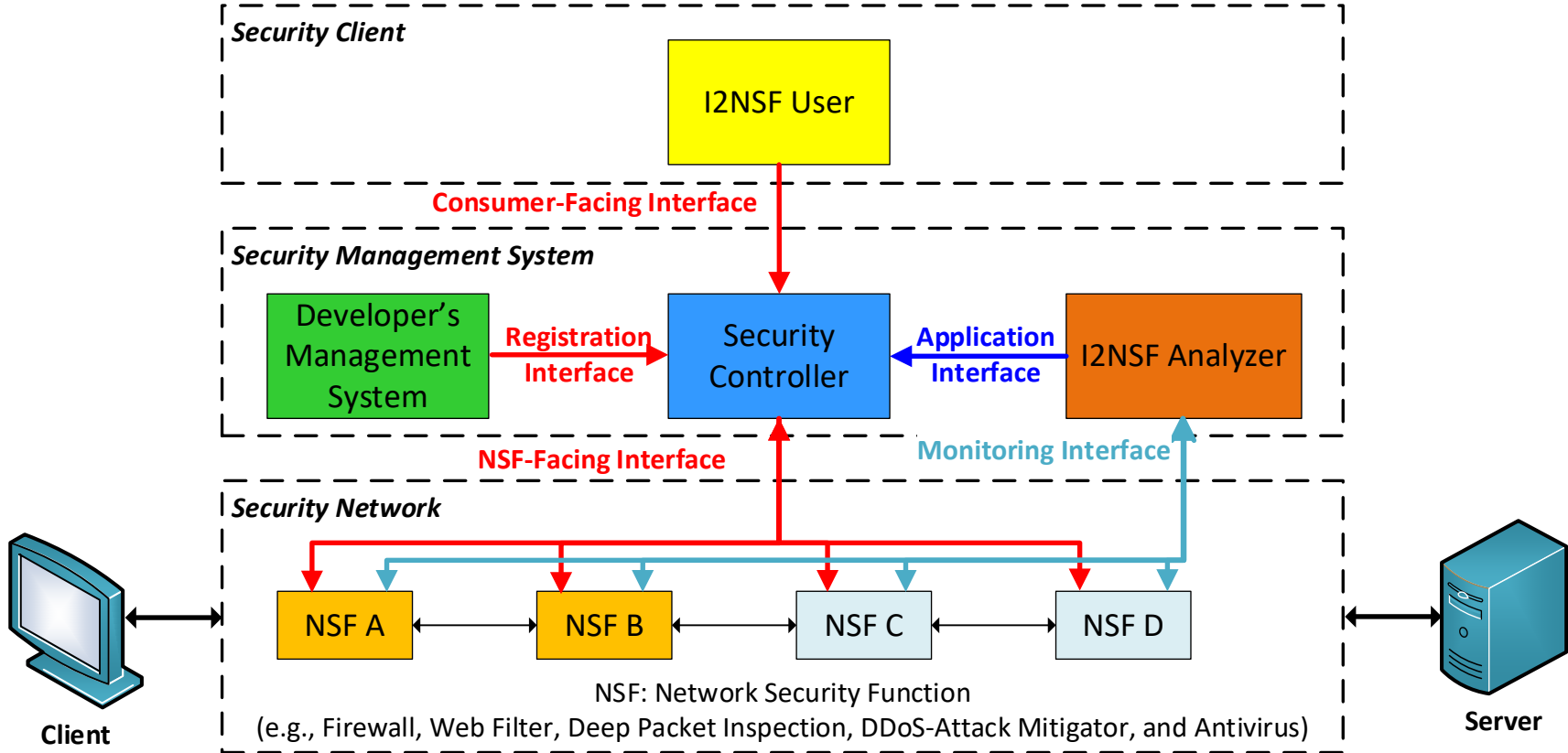
IETF-113 I2NSF WG Meeting

I2NSF WG Re-Chartering

March 24, 2022
Vienna

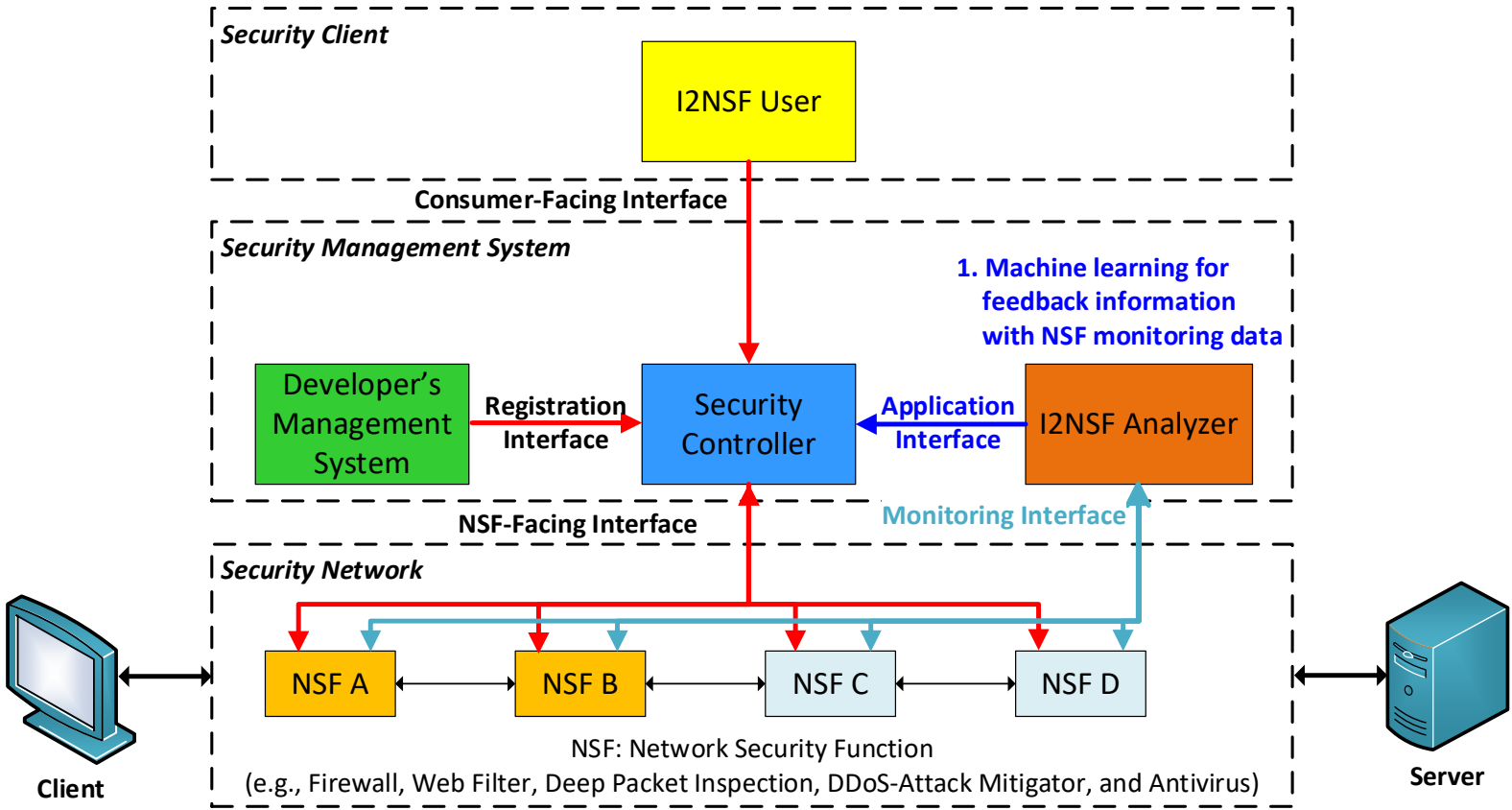
Authors: Jaehoon (Paul) Jeong (SKKU)
and Diego Lopez (Telefonica I+D)
(Email: pauljeong@skku.edu,
diego.r.lopez@telefonica.com)

I2NSF for Security Management Automation (1/3)



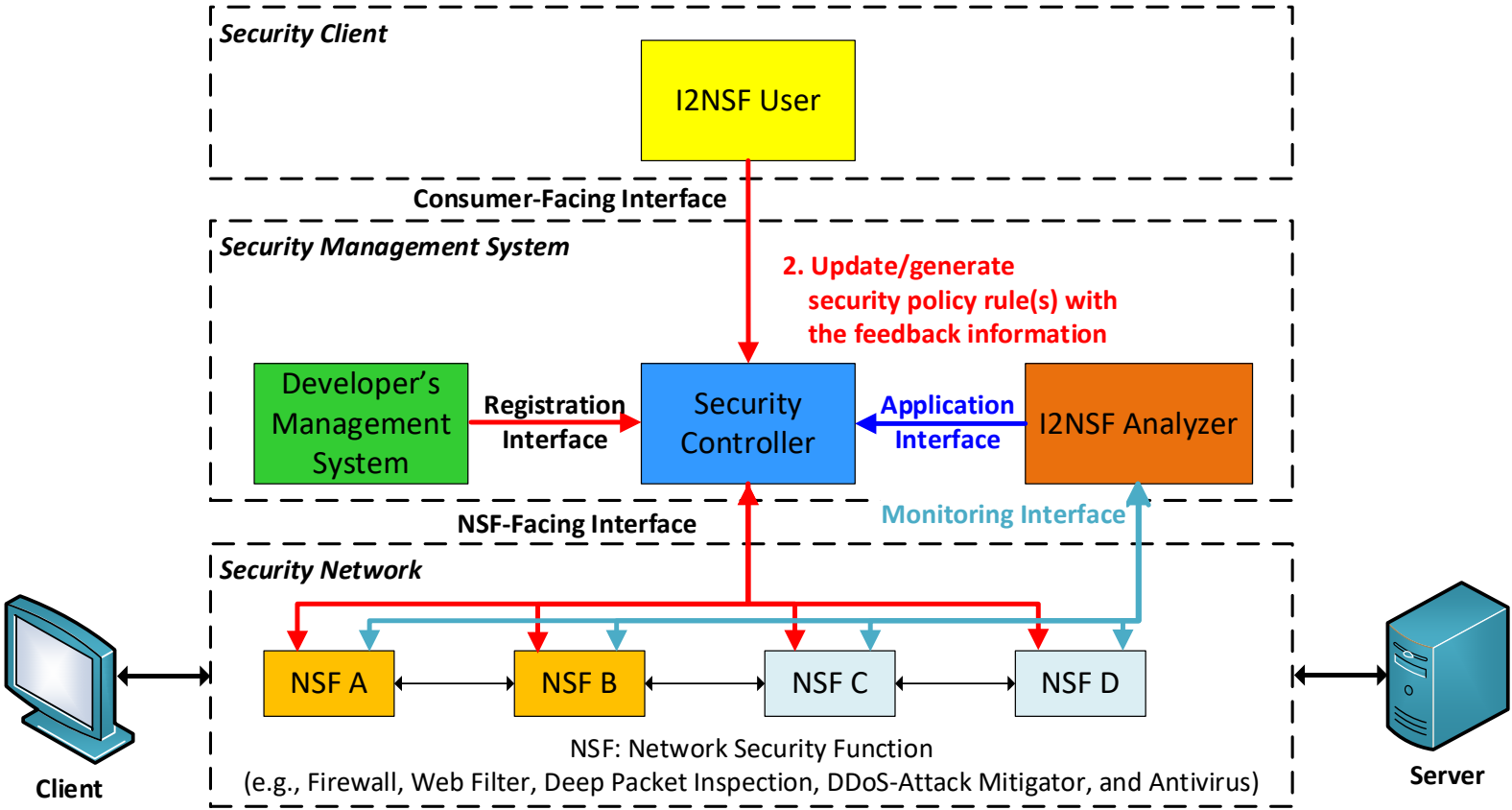
Source: An Extension of I2NSF Framework for Security Management Automation in Cloud-Based Security Services, draft-jeong-i2nsf-security-management-automation-03.

I2NSF for Security Management Automation (2/3)



Source: An Extension of I2NSF Framework for Security Management Automation in Cloud-Based Security Services, draft-jeong-i2nsf-security-management-automation-03.

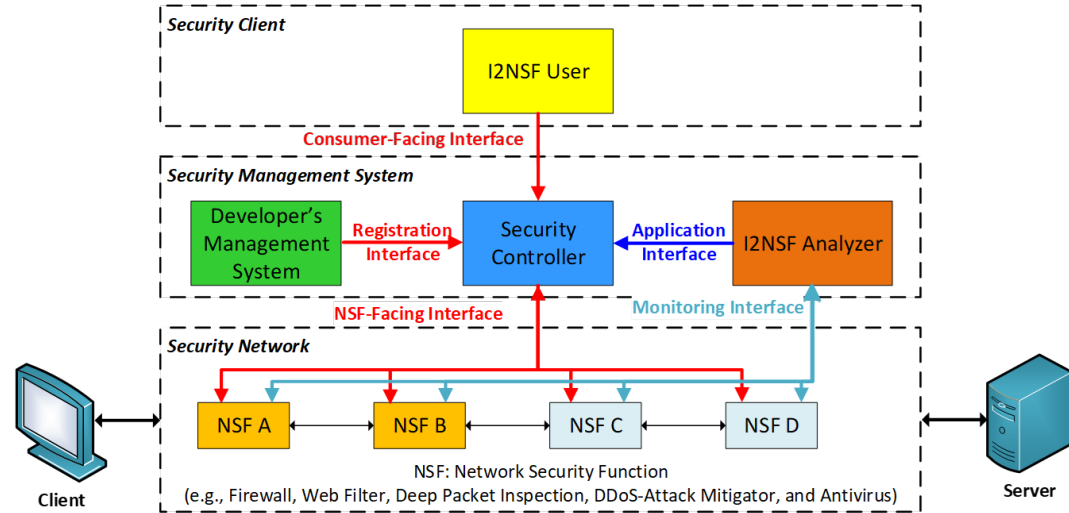
I2NSF for Security Management Automation (3/3)



Source: An Extension of I2NSF Framework for Security Management Automation in Cloud-Based Security Services, draft-jeong-i2nsf-security-management-automation-03.

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 policy to an NSF.
- Monitoring Interface
 - An NSF delivers its monitoring data to I2NSF Analyzer.
- Application Interface
 - I2NSF Analyzer delivers its feedback to Security Controller for policy update.



I2NSF WG Re-chartering (1/13)

- **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 (2/13)

- **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 feedback control loop consisting of security policy configuration, monitoring, notification, data analysis, feedback delivery, and security policy augmentation/generation. However, the following key components for I2NSF are needed:

I2NSF WG Re-chartering (3/13)

- **Goals (Con't)**

1. The **data analysis entities**, **feedback delivery** and **security policy augmentation**. The **I2NSF Analyzer** is to process and make data from NSFs available in a way that they are auditable, undeniable, and tamper-resistant.

2. The I2NSF framework needs **a new interface** (called **Application 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 (4/13)

- **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 either a centralized way (e.g., database) or a decentralized way (e.g., Blockchain as a distributed ledger technology (DLT)).

I2NSF WG Re-chartering (5/13)

- **Goals (Con't)**

4. The provenance and status of the I2NSF components (i.e., I2NSF User, Security Controller, NSF, DMS, and I2NSF Analyzer) need to be verified by **remote attestation**. This remote attestation can detect **supply chain attacks**. Beyond this, it would be necessary to analyze the **impact of new mechanisms for establishing roots of trust**, such as Quantum Key Distribution (QKD), and providing crypto capabilities, such as Post Quantum Cryptography (PQC), on the management mechanisms described in RFC9061. In addition, **recording events** (like done with DLT such as Blockchain), or **implementing data paths and computational services** (as supported by in-network computing) needs to be evaluated.

I2NSF WG Re-chartering (6/13)

- **Goals (Con't)**

5. I2NSF can work effectively and efficiently on **container deployments in a cloud native NFV architecture**. For the operations in this cloud native NFV architecture, the YANG data models of the I2NSF interfaces need to be augmented appropriately.

6. I2NSF needs to **support recently developed protocols** such as QUIC and HTTP/3.

I2NSF WG Re-chartering (7/13)

- **Program of Work**

1. A single document for **an extension of I2NSF framework for security management automation**. This document will initially be produced for reference as a living list to track and record discussions. The working group may decide not to publish this document as an RFC.

2. A YANG data model document for **I2NSF Application Interface** to deliver feedback from I2NSF Analyzer to Security Controller.

I2NSF WG Re-chartering (8/13)

- **Program of Work (Con't)**

3. A single document for **a framework for security policy translation** to support the mapping between a high-level YANG module and a low-level YANG module. The working group may decide not to publish this document as an RFC. This document will apply the recommendations under discussion in NETMOD and OPSAWG on event modeling.

4. A single document for **remote attestation for I2NSF components**, based on the work of the RATS WG.

I2NSF WG Re-chartering (9/13)

- **Program of Work (Con't)**

5. A YANG data model document for the **support of DLT-based distributed system auditing** (e.g., Blockchain) in the I2NSF framework.

6. A single document for **I2NSF on container deployments** in a cloud native NFV architecture.

7. A single document for **applicability and use cases** in I2NSF-based security management automation.

I2NSF WG Re-chartering (10/13)

- **Program of Work (Con't)**

8. A YANG data model document for **I2NSF Capability** for security management automation and recently developed protocols (e.g., QUIC and HTTP/3).

9. A YANG data model document for **I2NSF NSF-Facing Interface** for security management automation and recently developed protocols (e.g., QUIC and HTTP/3).

10. A YANG data model document for **I2NSF Consumer-Facing Interface** for security management automation and recently developed protocols (e.g., QUIC and HTTP/3).

I2NSF WG Re-chartering (11/13)

- **Milestones**

1. July 2022 Adopt an extension of I2NSF framework for security management automation as WG document
2. July 2022: Adopt a YANG data model for I2NSF Application Interface as WG document
3. July 2022: Adopt a framework for security policy translation as WG document
4. November 2022: Adopt remote attestation for I2NSF components, based on the work of RATS, as WG document

I2NSF WG Re-chartering (12/13)

- **Milestones (Con't)**

5. March 2023: Adopt a YANG data model for DLT-based distributed system auditing as WG document

6. March 2023: Adopt I2NSF on container deployments in a cloud native NFV architecture as WG document

7. July 2023: Adopt applicability and use cases in I2NSF-based security management automation as WG document

8. November 2023: Adopt a YANG data model for I2NSF Capability for security management automation as WG document

I2NSF WG Re-chartering (13/13)

- **Milestones (Con't)**

9. November 2023: Adopt a YANG data model for I2NSF NSF-Facing Interface for security management automation as WG document

10. November 2023: Adopt a YANG data model for I2NSF Consumer-Facing Interface for security management automation as WG document



Appendices

Appendix A – I2NSF Remote Attestation

Appendix B – Security Policy Translation

Appendix A – I2NSF Remote Attestation

draft-yang-i2nsf-remote-attestation-interface-dm-00

Relationship between RATS and I2NSF Remote Attestation


RATS:

RATS defines the basic architecture of remote attestation, different types of remote attestation evidence (e.g. based on TPM and TEE respectively), and other drafts like attestation result, etc.

- Remote Attestation Procedures Architecture
- The Entity Attestation Token (EAT)
- A YANG Data Model for Challenge-Response-based Remote Attestation Procedures using TPMs
- etc.

I2NSF Remote Attestation:

I2NSF remote attestation focuses on the remote attestation of an NSF in I2NSF framework. The remote attestation target is an NSF and its platform. The root of trust in I2NSF is unlimited, the Verifier and Relying Party is I2NSF Security Controller (TBD).

- 
- I2NSF Remote Attestation

Necessity of I2NSF Remote Attestation

Security Reasons

- Inappropriate deployment of an NSF.
- Potential attacks by the remote platform who carries an NSF.
- Security status of an NSF.

Future Extension Reasons

- Zero Trust concept may use I2NSF remote attestation to assess an NSF's trust status.
- SASE (Security Access Service Edge) may use I2NSF remote attestation to enhance an edge's security function.
- Security automation may use I2NSF remote attestation to manage an NSF.
- Decentralized security intelligence sharing may use remote attestation to judge the trustworthiness of such intelligence.

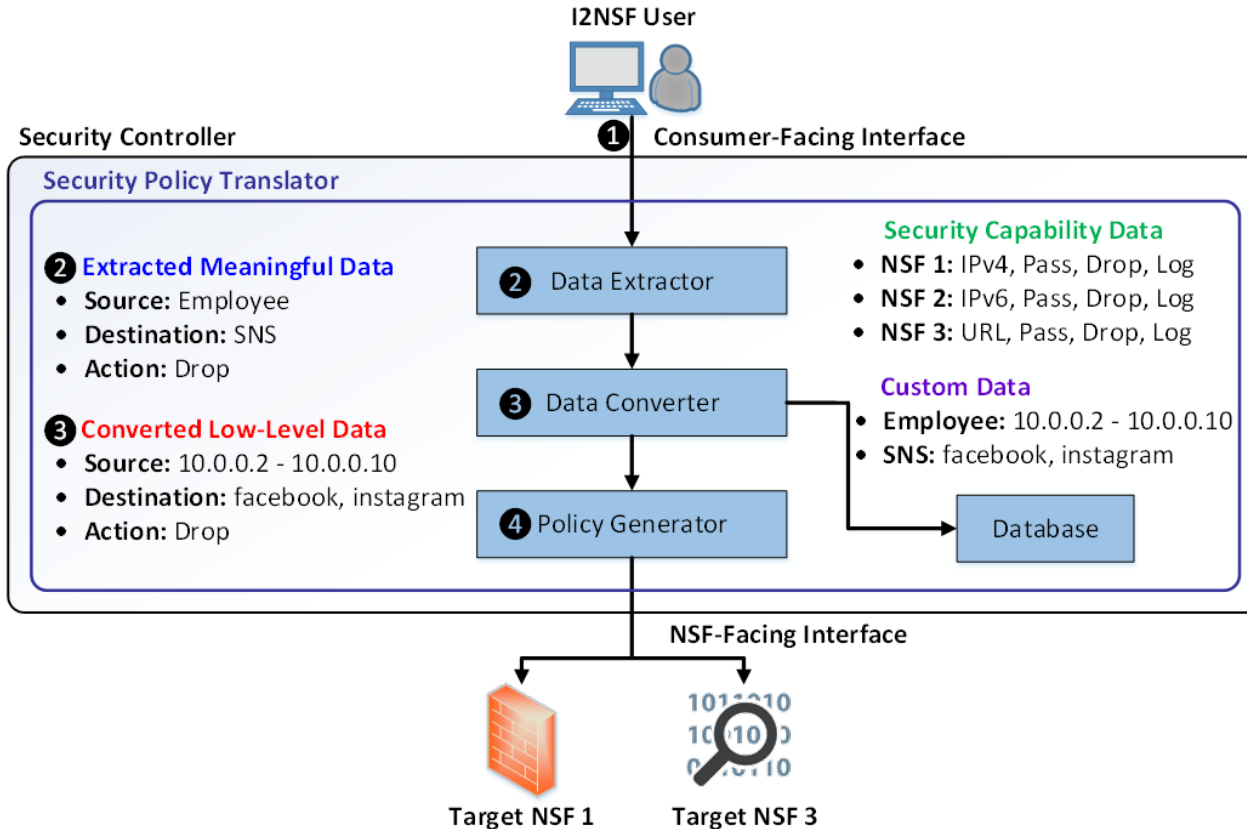
Practicability Reasons

- The target and the granularity should be NSF.
- RATs architecture is inconvenient to use in I2NSF directly.
- Different device may have different root of trust, one unified remote attestation interface would be more convenient for I2NSF to implementation .

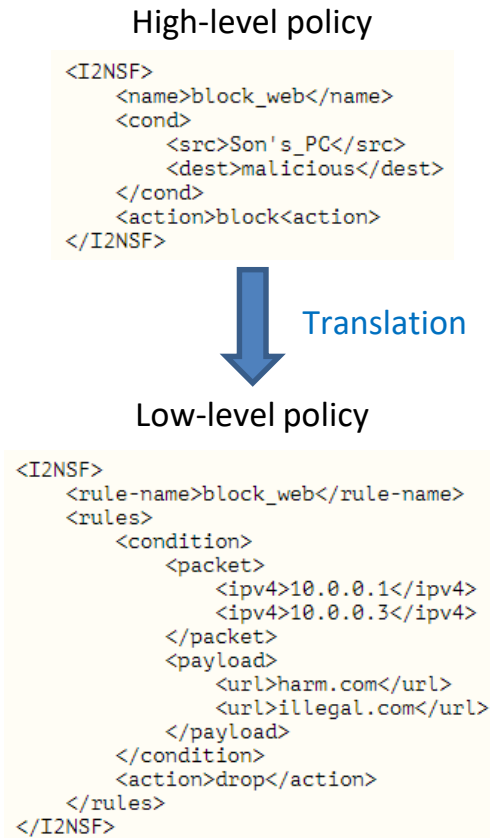
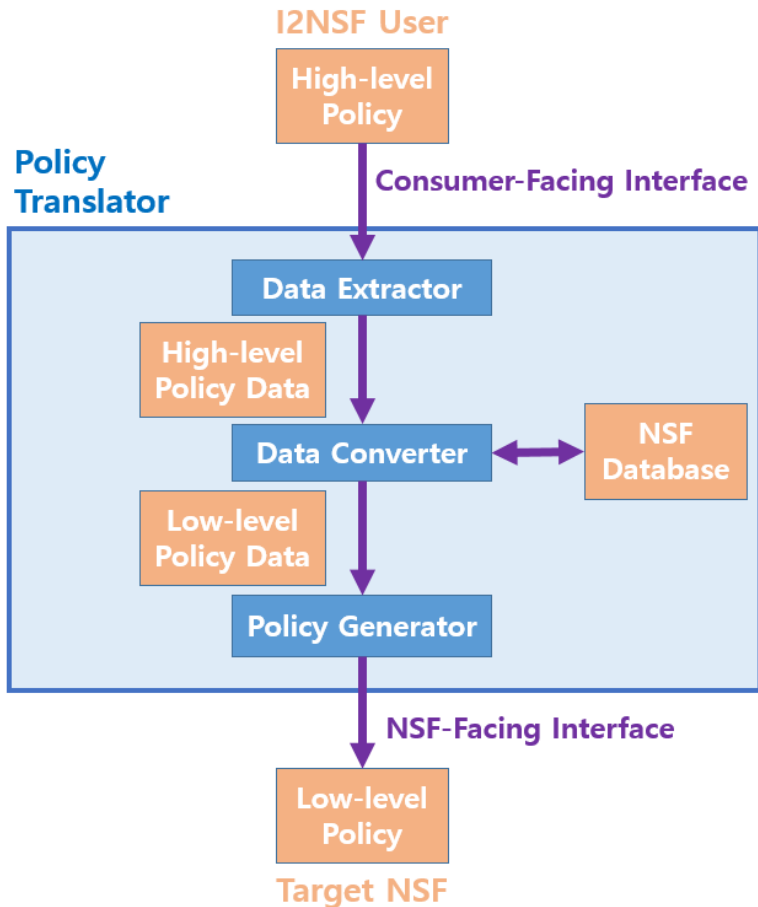
Appendix B – Security Policy Translation

draft-yang-i2nsf-security-policy-translation-10

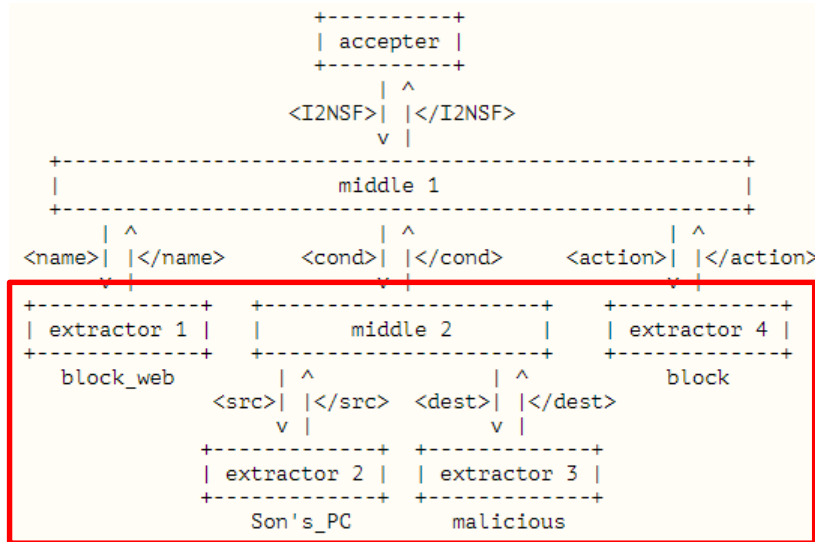
Security Policy Translation in I2NSF



Translation Architecture

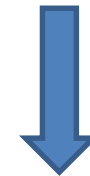


Step 1: Extractor (DFA)



High-level policy

```
<I2NSF>  
<name>block_web</name>  
<cond>  
  <src>Son's_PC</src>  
  <dest>malicious</dest>  
</cond>  
<action>block</action>  
</I2NSF>
```

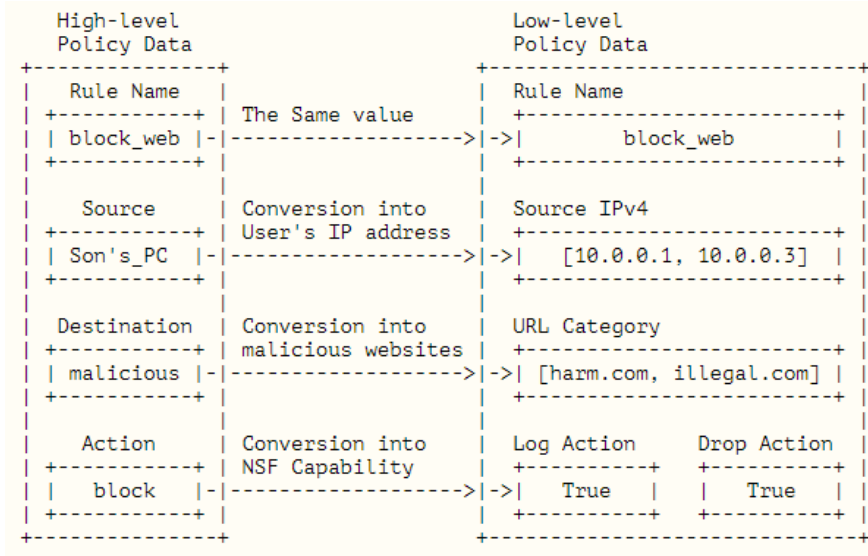


Extraction

High-level policy data

Rule Name	block_web
Source	Son's_PC
Destination	malicious
Action	block

Step 2: Data Converter (1/3)



High-level policy data

Rule Name	block_web
Source	Son's_PC
Destination	malicious
Action	block

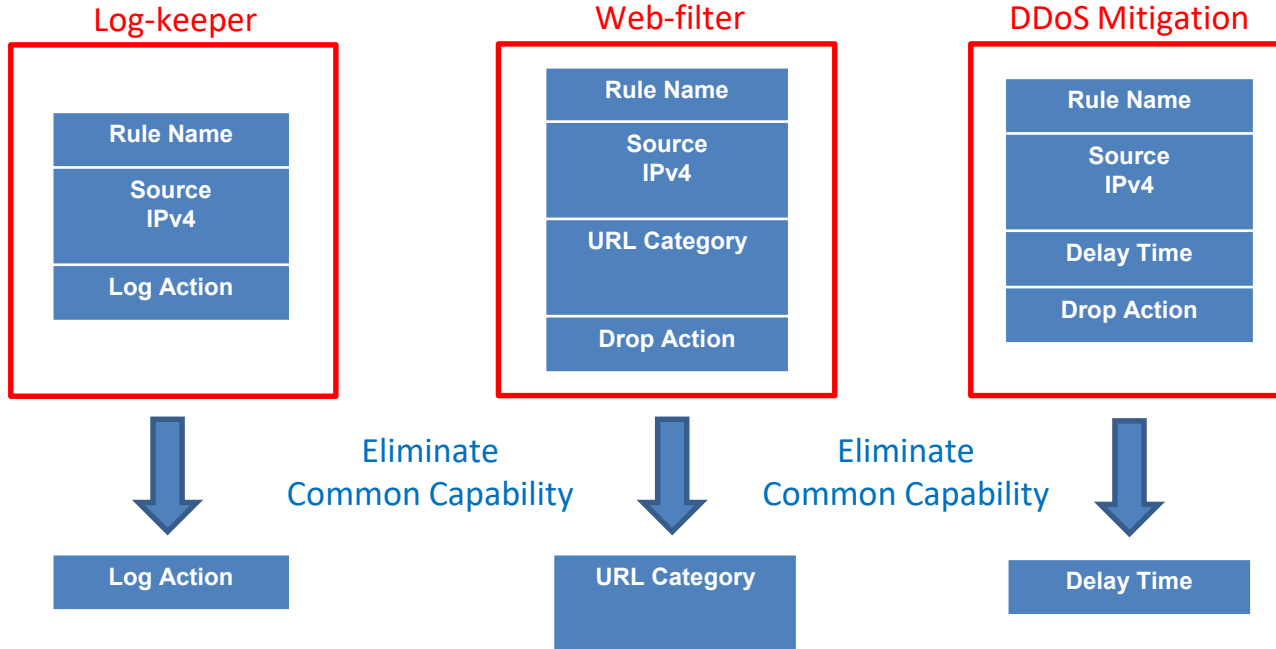


Data Conversion

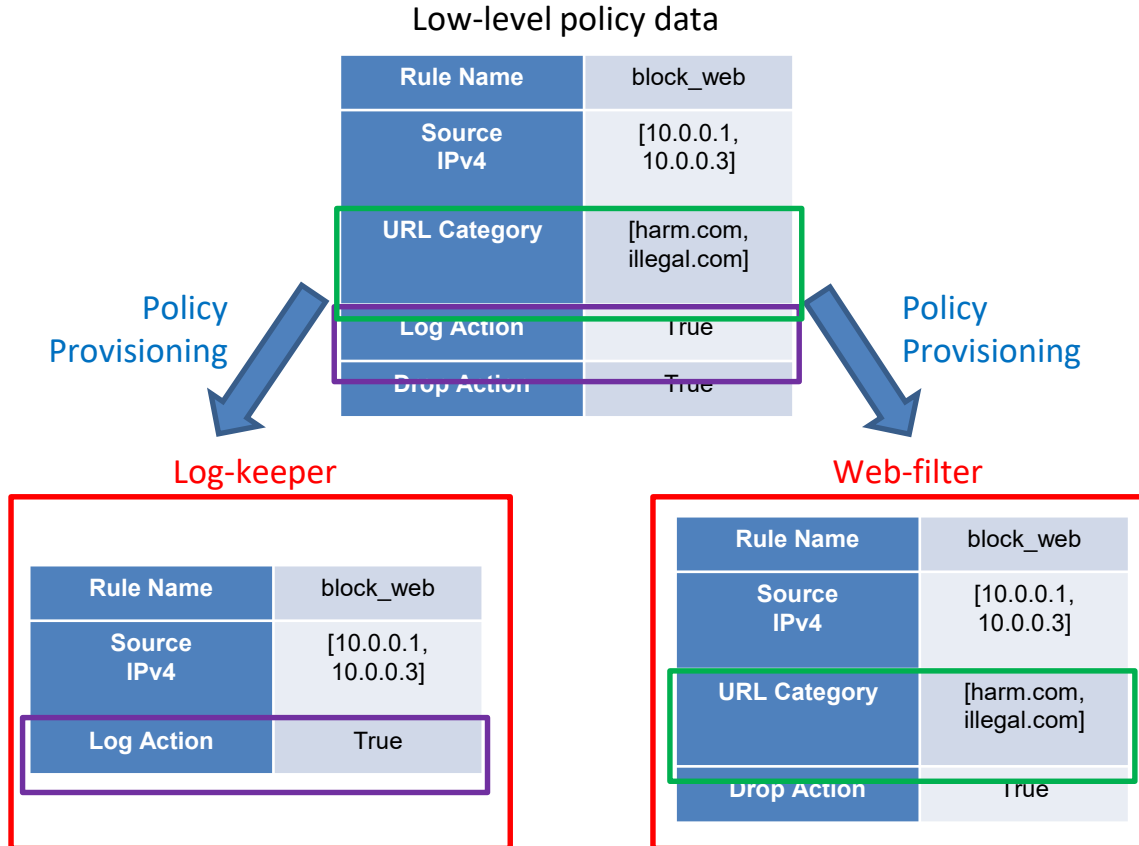
Low-level policy data

Rule Name	block_web
Source IPv4	[10.0.0.1, 10.0.0.3]
URL Category	[harm.com, illegal.com]
Log Action	True
Drop Action	True

Step 2: Data Converter (2/3)



Step 2: Data Converter (3/3)



Step 3: Generator (CFG)

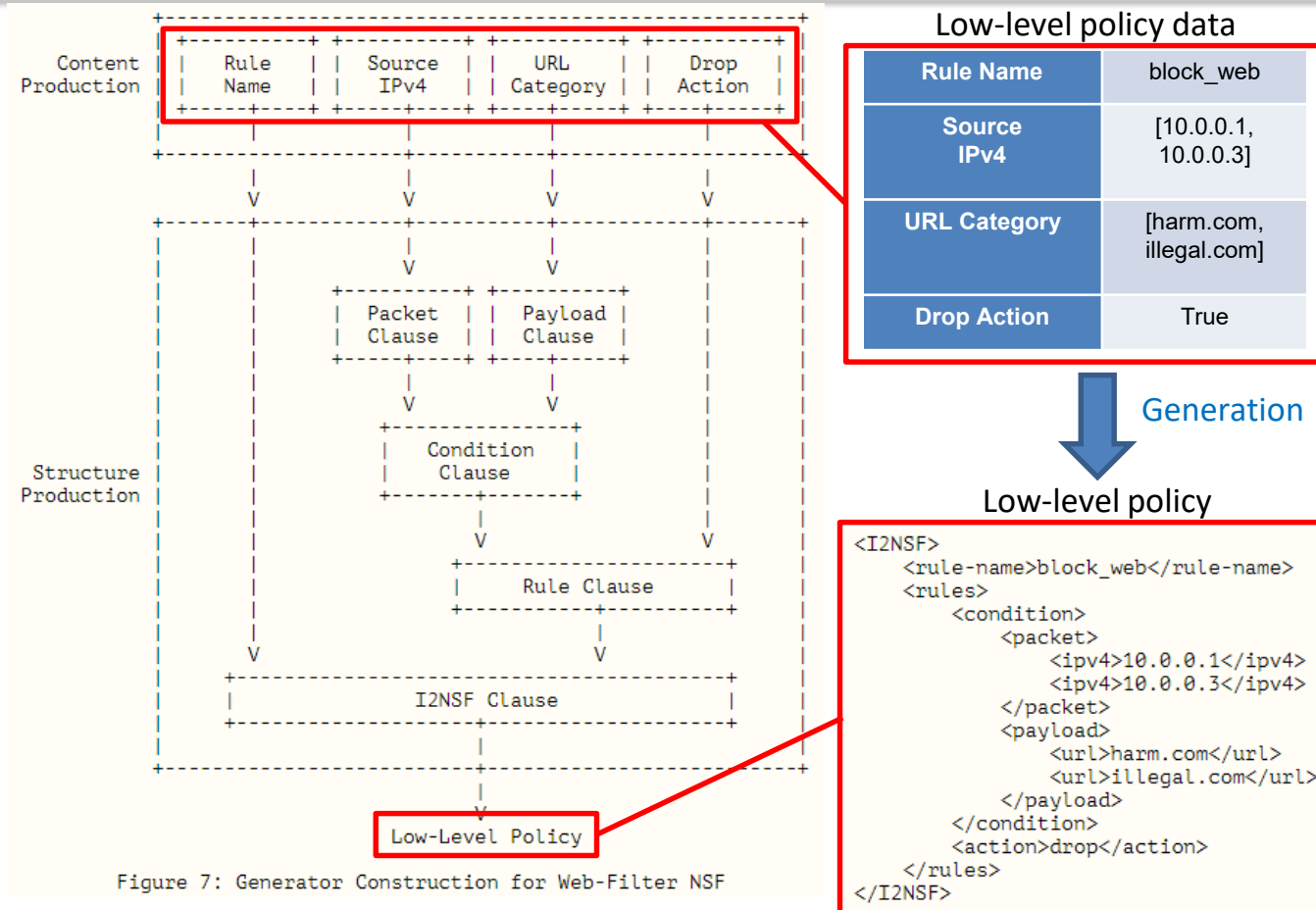


Figure 7: Generator Construction for Web-Filter NSF