Security Policy Translation in Interface to Network Security Functions
(draft-yang-i2nsf-security-policy-translation-01)

IETF 102, Montreal
July 18, 2018

Jinhyuk Yang [Presenter], Jaehoon Paul Jeong, and Jinyong (Tim) Kim
Sungkyunkwan University
Motivation

• The **Limitations** of XSLT-Based Policy Translation

  1. **Difficulty of Security Policy Construction**
     - I2NSF User MUST select target NSFs for a high-level security policy by himself.
     - This selection requires the knowledge of NSFs corresponding to capabilities from I2NSF User.
     - Thus, I2NSF User MUST be a security expert.

  2. **Inefficient Maintenance in Policy Translation**
     - If a Data Model (in either Consumer-Facing Interface or NSF-Facing Interface) is revised, a system manager SHOULD revise all XSLT stylesheets (i.e., xml files) of each NSF.
Our Approach

• Automata-Based Policy Translation

  1. **Ease of Security Policy Construction**
     - I2NSF User doesn’t need to select target NSFs for a high-level security policy by himself.
     - This selection will be performed by Security Controller having knowledge of NSFs corresponding to capabilities for the sake of I2NSF User.
     - Thus, I2NSF User doesn’t need to be a security expert.

  2. **Efficient Maintenance in Policy Translation**
     - If a Data Model (in either Consumer-Facing Interface or NSF-Facing Interface) is revised, a system manager needs to update only Translation Mapping Information in Security Controller.
Architecture of Security Policy Translator

I2NSF User

High Level Policy

Extractor (DFA)

High-Level Policy Data

Security Policy Translator

Data Converter

NSF Database

Generator (Context-free Grammar)

Low-Level Policy Data

Target NSF

Low Level Policy
Security Policy Translation (Web Filter)

High-level Policy

Low-level Policy
Step 1: Extractor (DFA)

**• Easily Extract Data from High-Level Policy**
- Acceptable if a high-level policy follows the rules of a data model hierarchy.

**• Detection of Grammar Error**
- If the hierarchy of the policy is wrong or there are some wrong tags, Extractor can detect it.
Step 2: Data Converter (1/2)

**High-level Policy Data**

- **Rule 1**
  - **Start Time**: 09:00
  - **End Time**: 13:00
  - **Source**: Staff
  - **Destination**: Google
  - **Action**: Drop, Log

**Low-level Policy Data**

- **Rule 1**
  - **Start Time**: 09:00
  - **End Time**: 13:00
  - **Source IPv4**: [10.0.0.1, 10.0.0.3]
  - **User-Defined URL Category**: [Google]
  - **Log Action**: True
  - **Drop Action**: True

**Database of Employee’s IP address**

- **Position**: Staff
  - **IP**: 10.0.0.1
- **Position**: Manager
  - **IP**: 10.0.0.2
- **Position**: Staff
  - **IP**: 10.0.0.3

**Data Conversion from Keyword to Values**

- **Position IP**
  - Staff 10.0.0.1
  - Manager 10.0.0.2
  - Staff 10.0.0.3

- **Compare with IP List**
  - [10.0.0.1, 10.0.0.3]

- **Compare with Capabilities**
  - Database of Action Capability
    - Log
    - Reject
    - Drop

- **Compare with Capabilities**
  - Database of Action Capability

- **Action**
  - Drop
Step 2: Data Converter (2/2)

NSF Provisioning: Mapping from Capabilities to NSFs

Select target NSFs which cover all contents of low-level policy. (NSF Provisioning)
Step 3: Generator

Content Production: for including data

Firewall NSF

Construct Tree for Context-free Grammar

Web-filter NSF

Rule Name
Start Time
End Time
Source IP
Log Action

Rule Name
Source IP
User-Defined URL Category
Drop Action

Time Information
Condition Clause
Action Clause

Rule Clause

Time Information
Condition Clause
Action Clause

Rule Clause

Low-level Policy for Firewall

Context-free Grammar based on NSF-Facing Interface Data Model

Low-level Policy for Web-filter

Low-level Policy Construction for NSFs
Next Steps

• **WG Adoption Call** after IETF-102
  - Security Policy Translation is important for I2NSF Implementation.
  - This draft can provide implementers with good guidelines.
  - This draft aims at an Informational RFC.

• We will enhance our draft through IETF-103 Hackathon.
  - We will develop a Tool for Policy Translator management.