Security Policy Translation in I2NSF

draft-yang-i2nsf-security-policy-translation-03

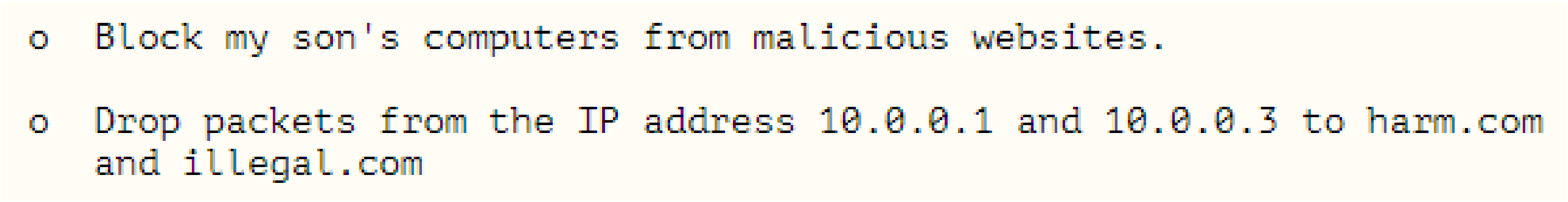
IETF 104, Prague

March 26, 2019

Jinhyuk Yang, Jaehoon (Paul) Jeong, and Jinyong (Tim) Kim

Necessity for Policy Translator

- Policy Representation according to Users
  - The first policy is for I2NSF Users, and the second policy is for NSFs.



```
o   Block my son's computers from malicious websites.

o   Drop packets from the IP address 10.0.0.1 and 10.0.0.3 to harm.com
    and illegal.com
```

  - Even if I2NSF User gives the first high-level policy, I2NSF System needs to automatically translate it into the second low-level policy.

Previous Translation

- XSLT-based Policy Translation
  – Popular method of XML-based policy translation.
  – Proposed by W3C at 1999.

- Limitation

  1. Difficulty of Security Policy Construction

     - The manager MUST select the proper NSF directly.

  2. Inefficient Maintenance

     - Cannot adapt automatically to a Data Model’s changes.

Proposed Translation

- Automata-based Policy Translation
  - New method for XML-based policy translation.

- Approach

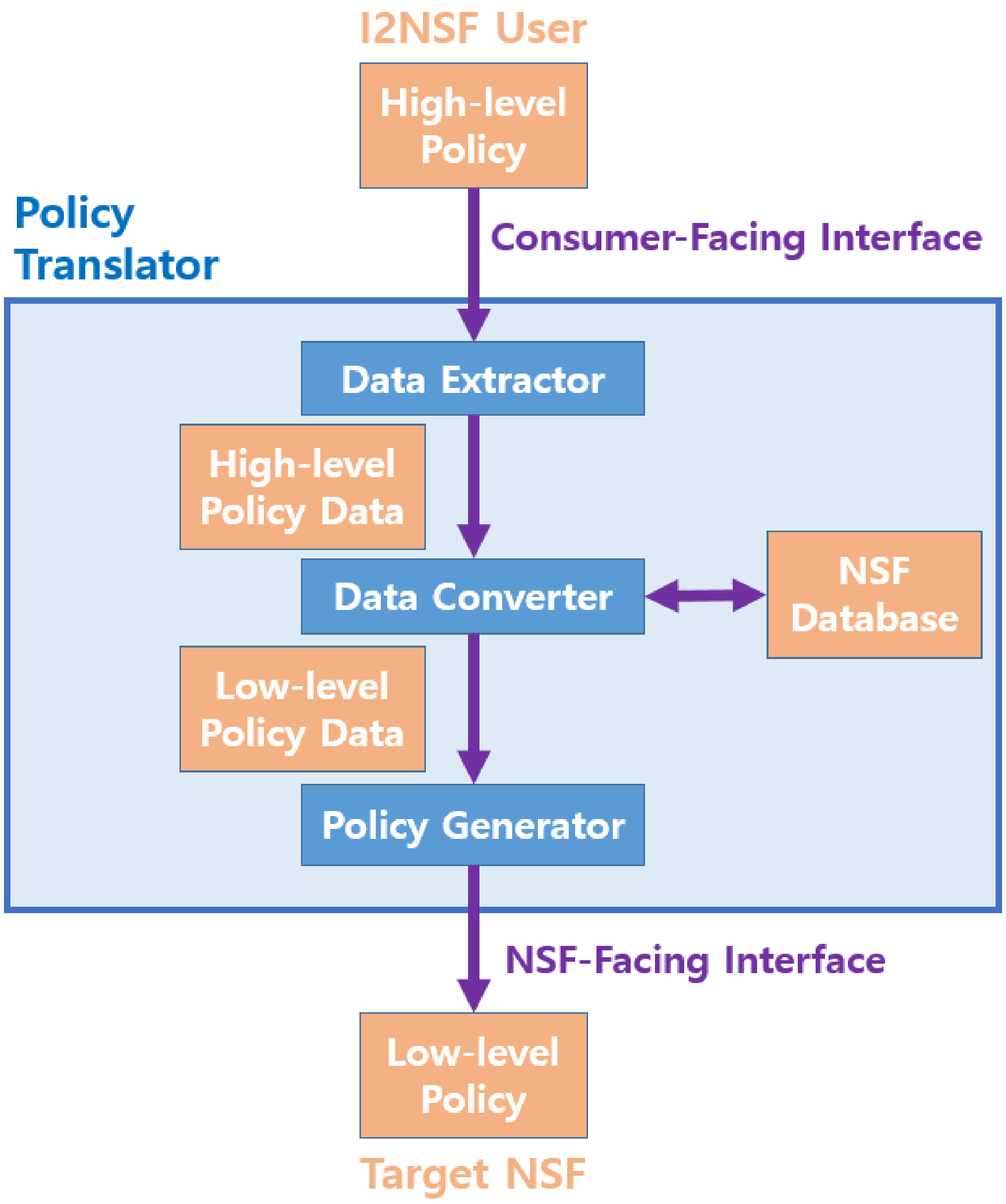
1. Ease of Security Policy Construction

   - The manager doesn't need to select the proper NSF.

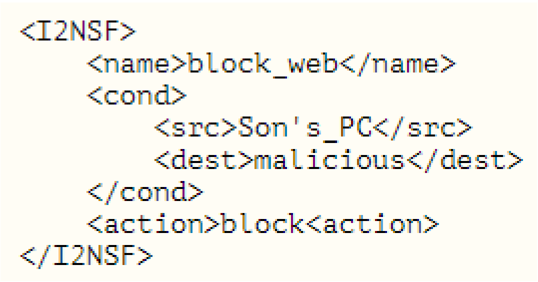
2. Efficient Maintenance

   - Can adapt automatically to a Data Model's changes.

Translation Architecture



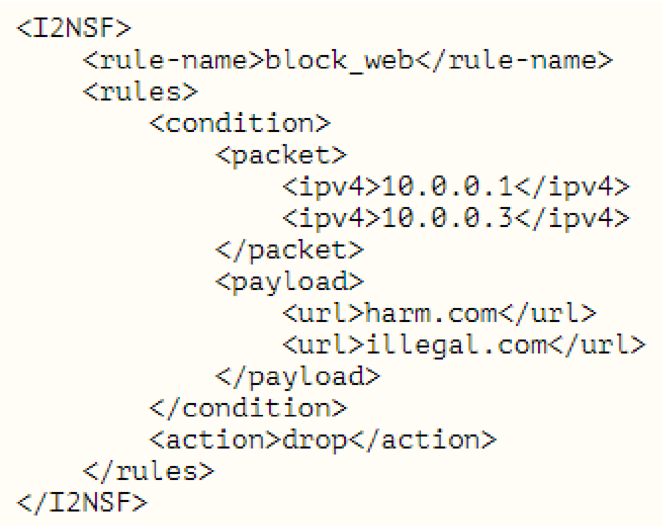
High-level policy



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

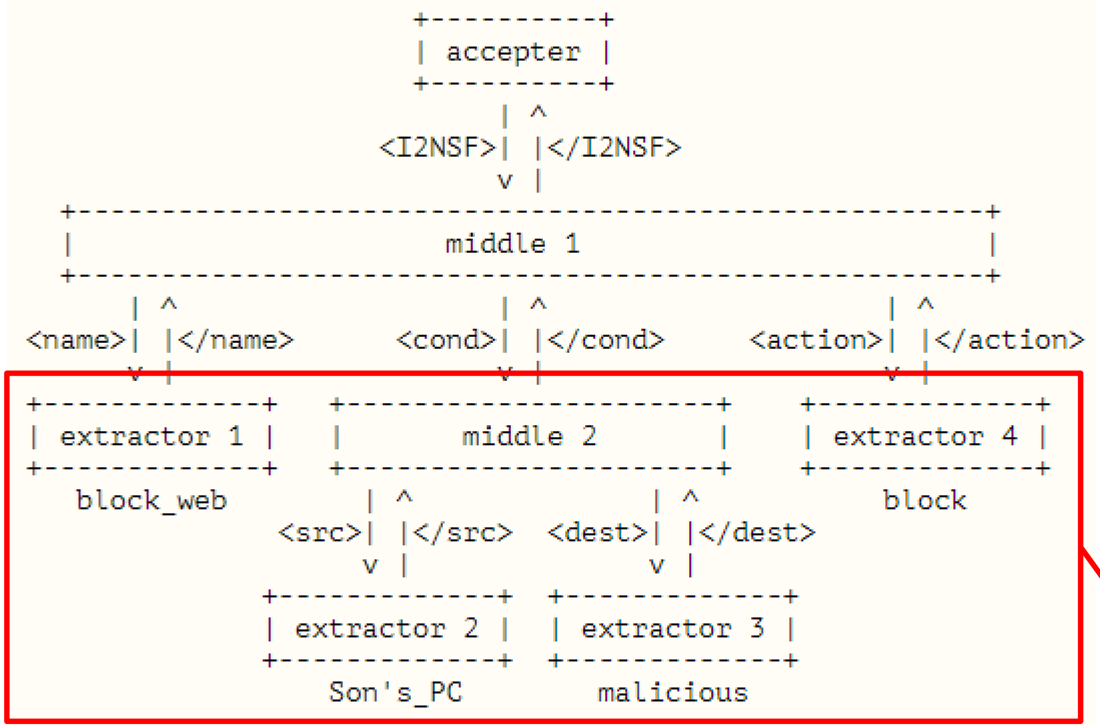
Translation

Low-level policy



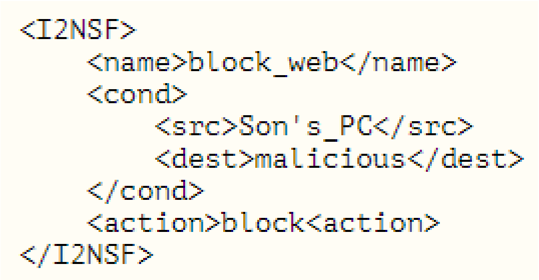
```
<I2NSF>
    <rule-name>block_web</rule-name>
    <rules>
        <condition>
            <packet>
                <ipv4>10.0.0.1</ipv4>
                <ipv4>10.0.0.3</ipv4>
            </packet>
            <payload>
                <url>harm.com</url>
                <url>illegal.com</url>
            </payload>
        </condition>
        <action>drop</action>
    </rules>
</I2NSF>
```

Step 1: Extractor (DFA)



```
                       +----------+
                       | accepter |
                       +----------+
                            | ^
                     <I2NSF>| |</I2NSF>
                            v |
  +------------------------------------------------------+
  |                     middle 1                         |
  +------------------------------------------------------+
      | ^                   | ^                    | ^
<name>| |</name>      <cond>| |</cond>     <action>| |</action>
      v |                   v |                    v |
+-------------+   +----------------------+    +-------------+
| extractor 1 |   |       middle 2       |    | extractor 4 |
+-------------+   +----------------------+    +-------------+
   block_web        | ^              | ^           block
               <src>| |</src>  <dest>| |</dest>
                    v |              v |
              +-------------+  +-------------+
              | extractor 2 |  | extractor 3 |
              +-------------+  +-------------+
                  Son's_PC        malicious
```

High-level policy



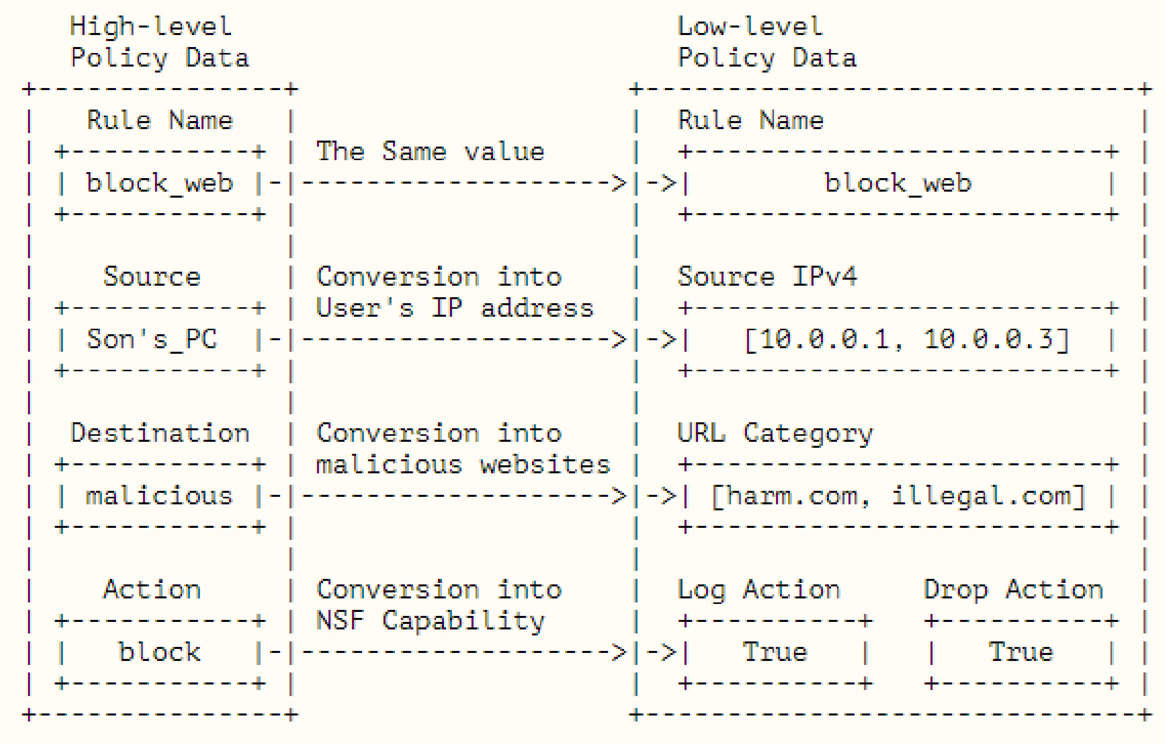
```
<I2NSF>
    <name>block_web</name>
    <cond>
        <src>Son's_PC</src>
        <dest>malicious</dest>
    </cond>
    <action>block<action>
</I2NSF>
```

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                          Low-level
   Policy Data                         Policy Data
+---------------+                    +-----------------------------+
|   Rule Name   |                    |  Rule Name                  |
| +-----------+ | The Same value     |  +------------------------+ |
| | block_web |-|------------------->|->|       block_web        | |
| +-----------+ |                    |  +------------------------+ |
|               |                    |                             |
|    Source     | Conversion into    |  Source IPv4                |
| +-----------+ | User's IP address  |  +------------------------+ |
| | Son's_PC  |-|------------------->|->|   [10.0.0.1, 10.0.0.3] | |
| +-----------+ |                    |  +------------------------+ |
|               |                    |                             |
|  Destination  | Conversion into    |  URL Category               |
| +-----------+ | malicious websites |  +------------------------+ |
| | malicious |-|------------------->|->| [harm.com, illegal.com] | |
| +-----------+ |                    |  +------------------------+ |
|               |                    |                             |
|    Action     | Conversion into    |  Log Action    Drop Action  |
| +-----------+ | NSF Capability     |  +----------+  +----------+ |
| |   block   |-|------------------->|->|   True   |  |   True   | |
| +-----------+ |                    |  +----------+  +----------+ |
+---------------+                    +-----------------------------+
```

High-level policy data

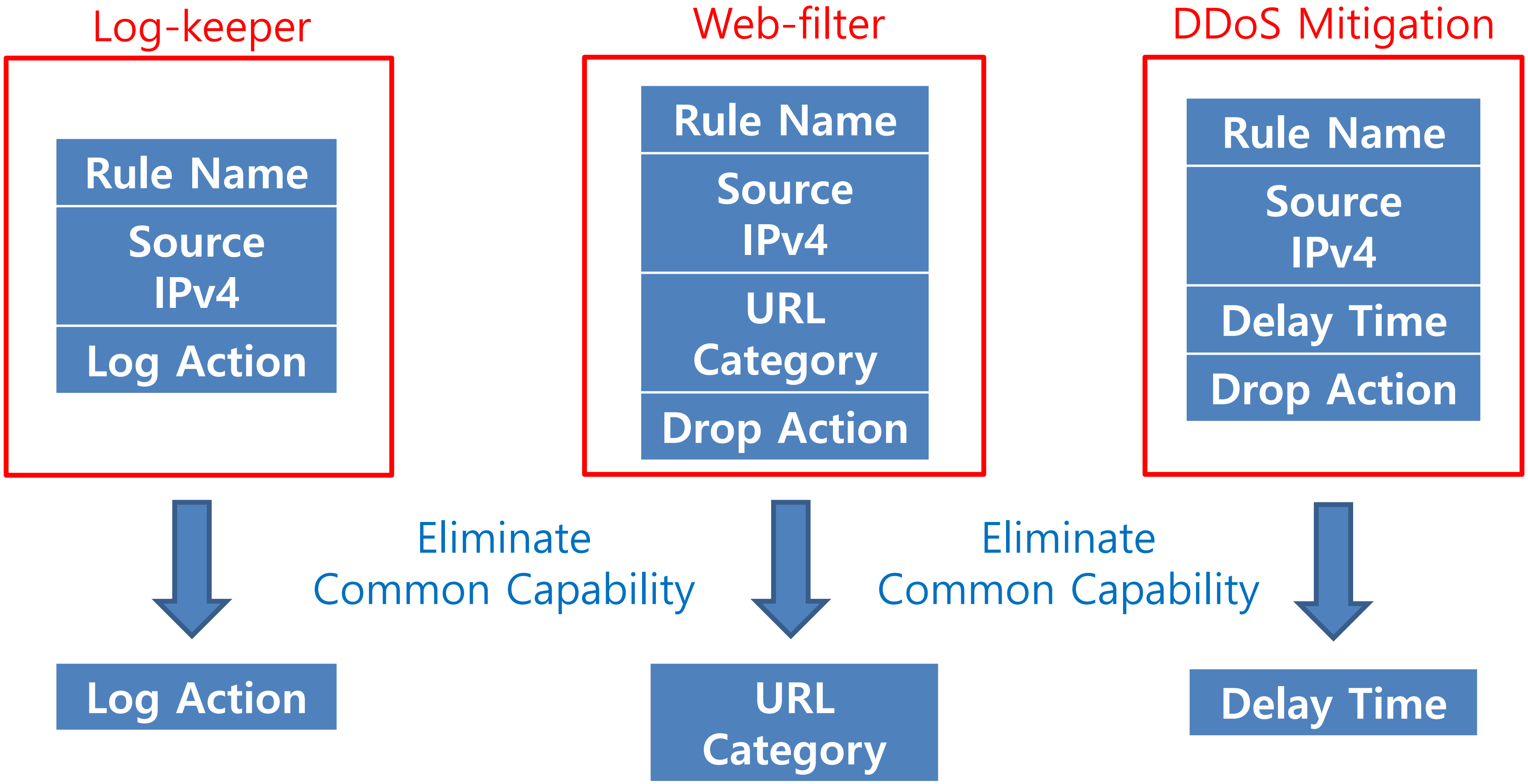
Rule Name	block_web
Source	Son’s_PC
Destination	malicious
Action	block

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)



Log-keeper

Rule Name

Source IPv4

Log Action

Web-filter

Rule Name

Source IPv4

URL Category

Drop Action

DDoS Mitigation

Rule Name

Source IPv4

Delay Time

Drop Action

Eliminate Common Capability

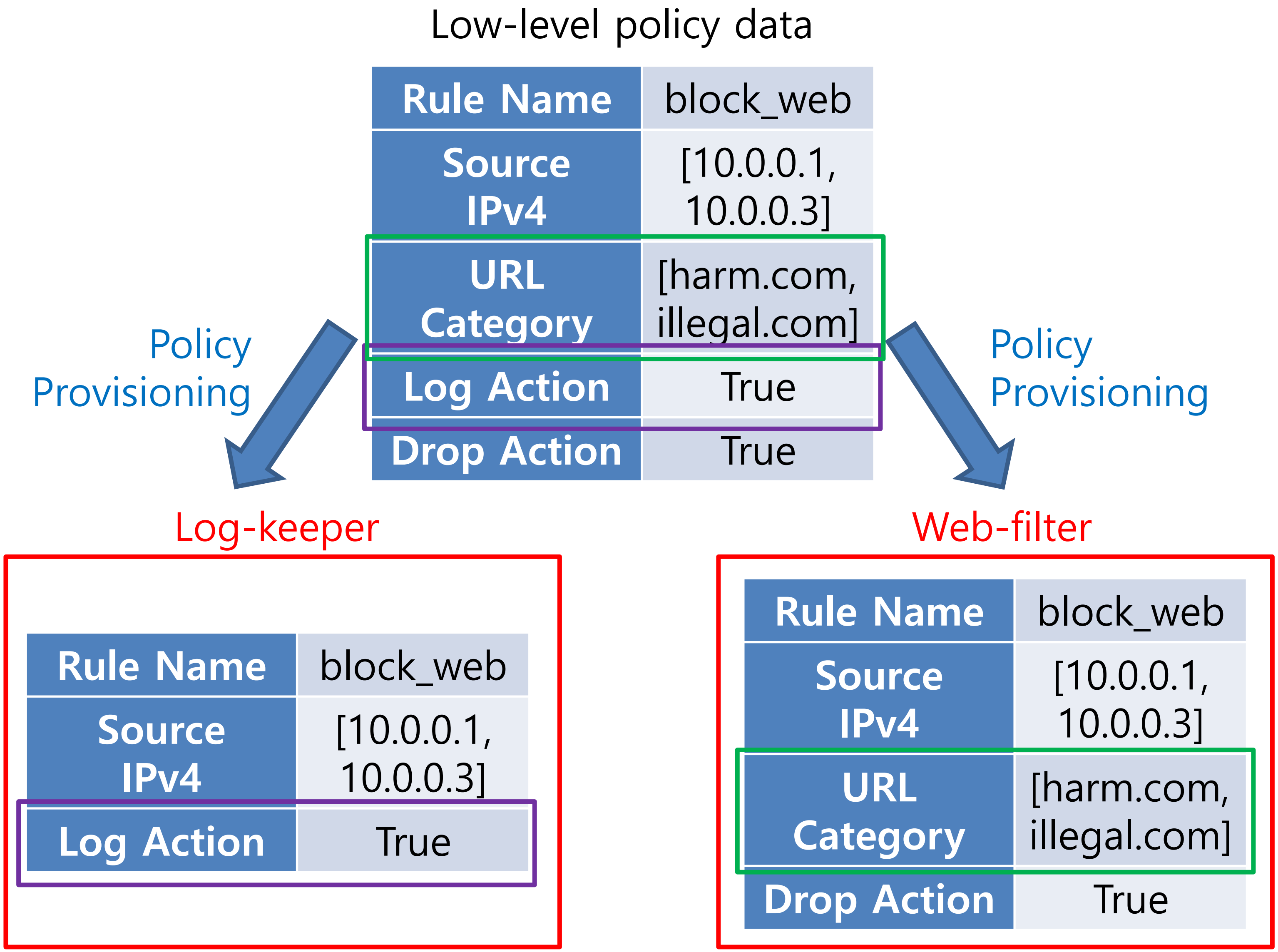
Eliminate Common Capability

Log Action

URL Category

Delay Time

Step 2: Data Converter (3/3)



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

Policy Provisioning

Policy Provisioning

Log-keeper

Rule Name	block_web
Source IPv4	[10.0.0.1, 10.0.0.3]
Log Action	True

Web-filter

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

Step 3: Generator (CFG)

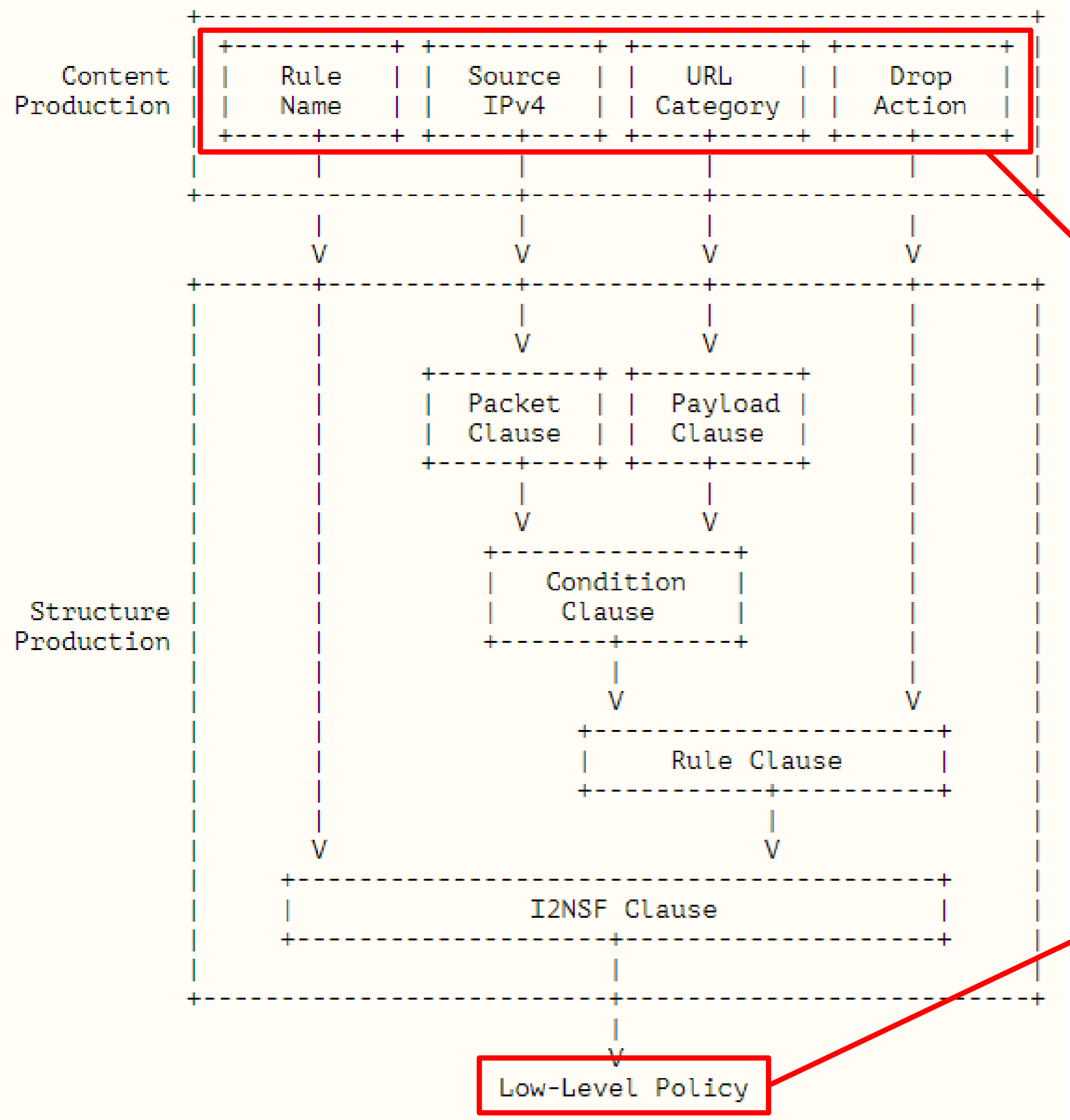


Figure 7: Generator Construction for Web-Filter NSF

Low-level policy data

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

Generation

Low-level policy

```
<I2NSF>
    <rule-name>block_web</rule-name>
    <rules>
        <condition>
            <packet>
                <ipv4>10.0.0.1</ipv4>
                <ipv4>10.0.0.3</ipv4>
            </packet>
            <payload>
                <url>harm.com</url>
                <url>illegal.com</url>
            </payload>
        </condition>
        <action>drop</action>
    </rules>
</I2NSF>
```

Updates from the Previous Versions

- The Previous Draft:
  - draft-yang-i2nsf-security-policy-translastion-02

- Changes from the previous versions
  - Explanations have been added for explaining NSF Database component.
  - The section “Implementation Consideration” is added for guidelines.
  - Other changes are described in detail in Appendix section.

Next Steps

- **WG Adoption Call at IETF 104**
  - Key Functionality for I2NSF's Implementation & Deployment in the real world.
  - This draft can provide the I2NSF developers with the guidelines to implement Security Policy Translator.
  - This draft aims at an Informational RFC.
  - The security policy translator is proved through IETF-104 Hackathon.