IETF-115

I2NSF Intelligent Detection

draft-wang-i2nsf-intelligent-detection-00

November 8, 2022

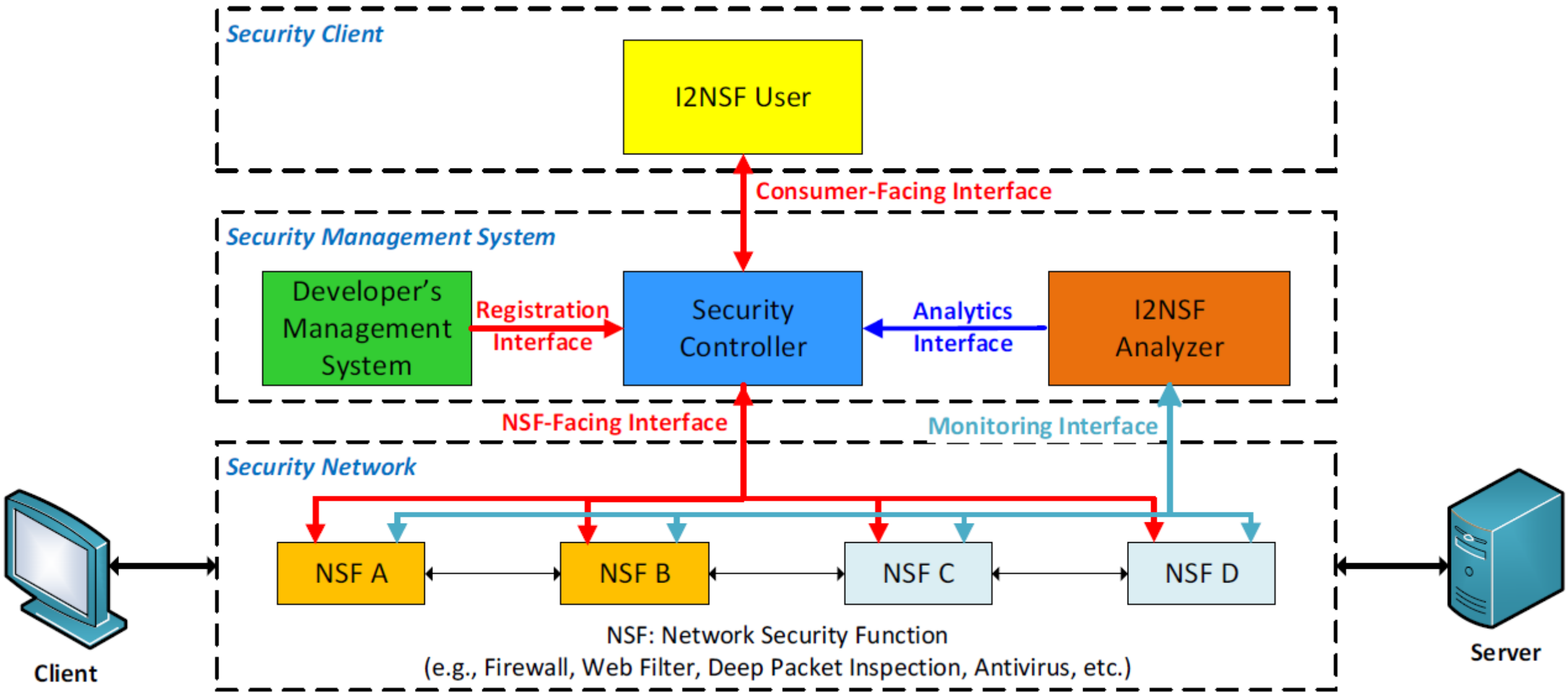
Weilin Wang, Huachun Zhou, Man Li, Qi Guo and Shuangxing Deng

Beijing Jiaotong University

New Terminology

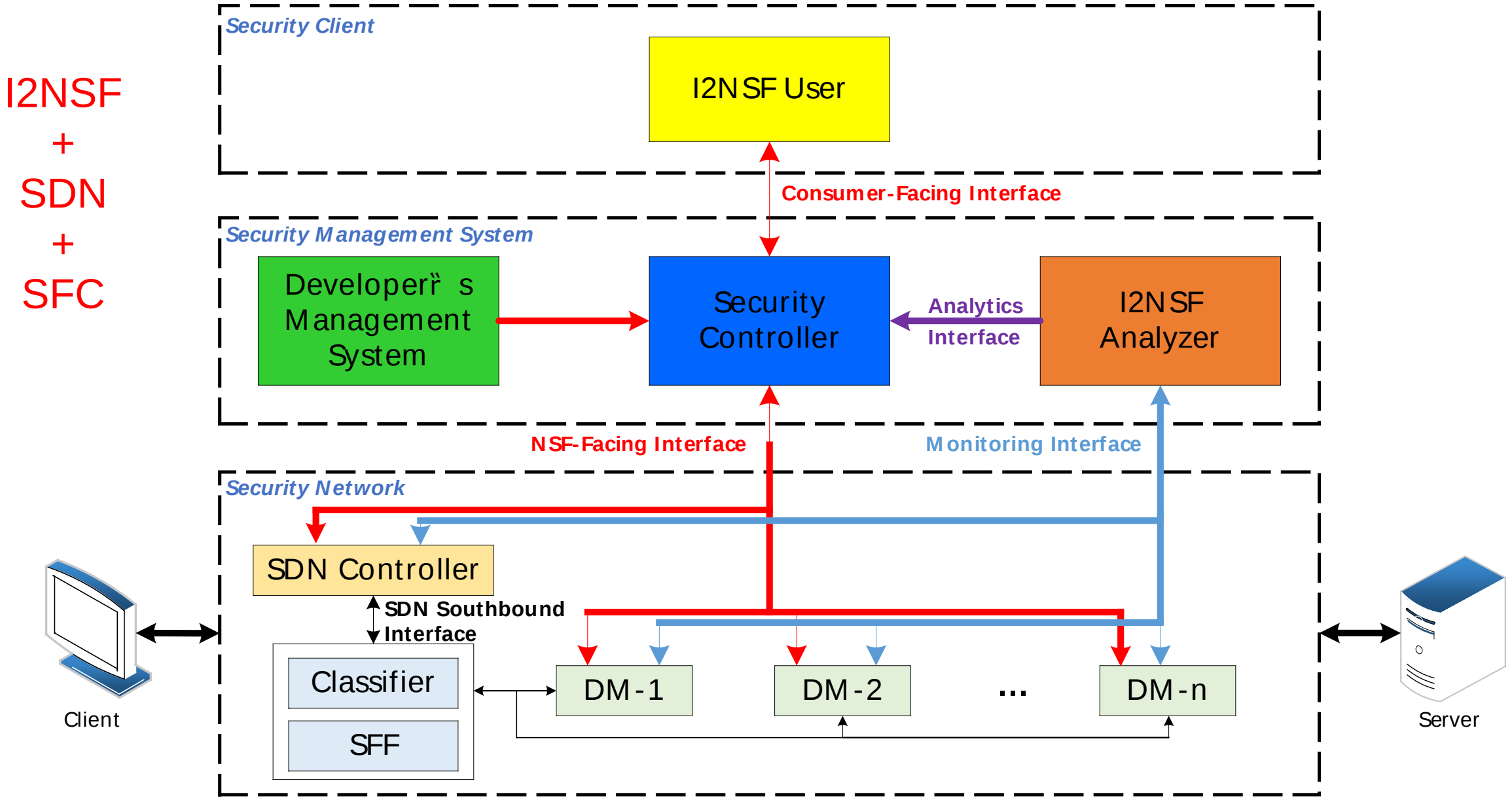
- **Intelligent Detection:** The network can dynamically adjust detection policies based on the feedback resource status, traffic features, and detection results.
- **Detection Module (DM):** The NSF with detection capability. Different DMs apply to different types of attacks, such as DDoS attacks, worm attacks and so on.

I2NSF Framework for Security Management Automation



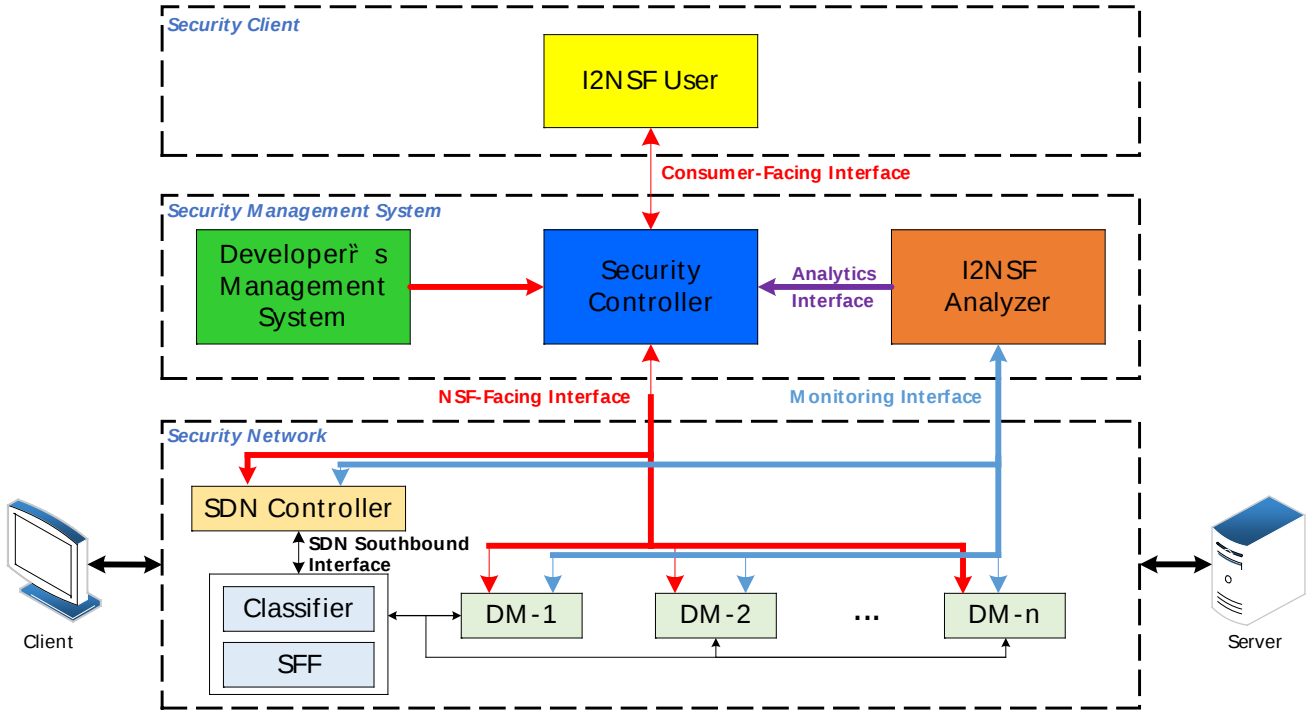
draft-jeong-i2nsf-security-management-automation-04

I2NSF Framework for Attacks Intelligent Detection (AID)



I2NSF Framework for AID: Components

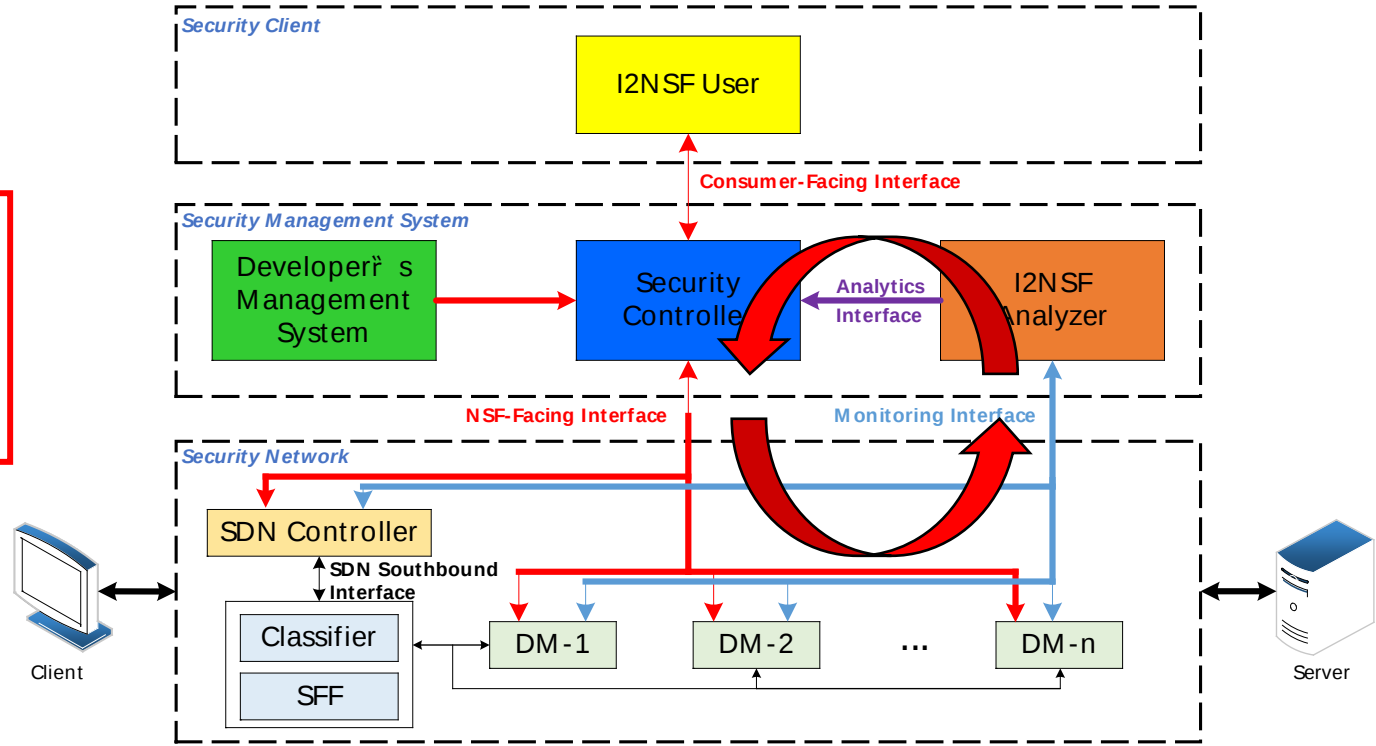
- I2NSF User
  - An entity that delivers a high-level security policy to Security Controller.
- Security Controller
  - An entity that controls and manages other system components in the I2NSF framework. It translates a high-level security policy (from I2NSF User) or reconfiguration policy (from I2NSF Analyzer) into the corresponding low-level security policy.
- Developer's Management System (DMS)
  - The provider of the NSFs. It registers the capability of an NSF with Security Controller.
- I2NSF Analyzer
  - The entity that collects monitoring data from NSFs and analyzes the activity and performance of NSFs for a closed-loop control.
- SDN Controller
  - An entity that provides a means to program, orchestrate, control and manage the network resources through software. It can parse path rules of the low-level security policy and deliver flow tables to CFs and SFFs to form SFPs
- Detection Module (DM)
  - The NSFs with detection capability.



I2NSF Framework for AID: Interfaces

- Consumer-Facing Interface
  - An interface between I2NSF User and Security Controller for the delivery of a high-level security policy.
- NSF-Facing Interface
  - An interface between Security Controller and an NSF for the delivery of a low-level security policy.
- Registration Interface
  - Interface used for DMS to register an NSF and its capabilities with Security Controller.
- Analytics Interface
  - Interface used for I2NSF Analyzer to deliver its analytics information to Security Controller for a closed-loop security control.
- SDN Southbound Interface
  - The application programming interface provided by the SDN Controller to interact with the SDN nodes
- Monitoring Interface
  - Interface used for an NSF to deliver its monitoring data to I2NSF Analyzer.

Closed-Loop Intelligent Detection



Extended YANG Data Models

- Monitoring Interface
  - **Traffic features**: measurement-time, packets-per-second, bytes-per-second, packet-size-mean, …
  - **Resource utilization logs**: system-status, cpu-usage, cpu-freq, memory-usage, memory-total, …
  - **DM detection results**: detection-module-name, time-stamp, response-time, start-time, end-time, attack-id, attack-type, attack-src-ip, attack-dst-port, …

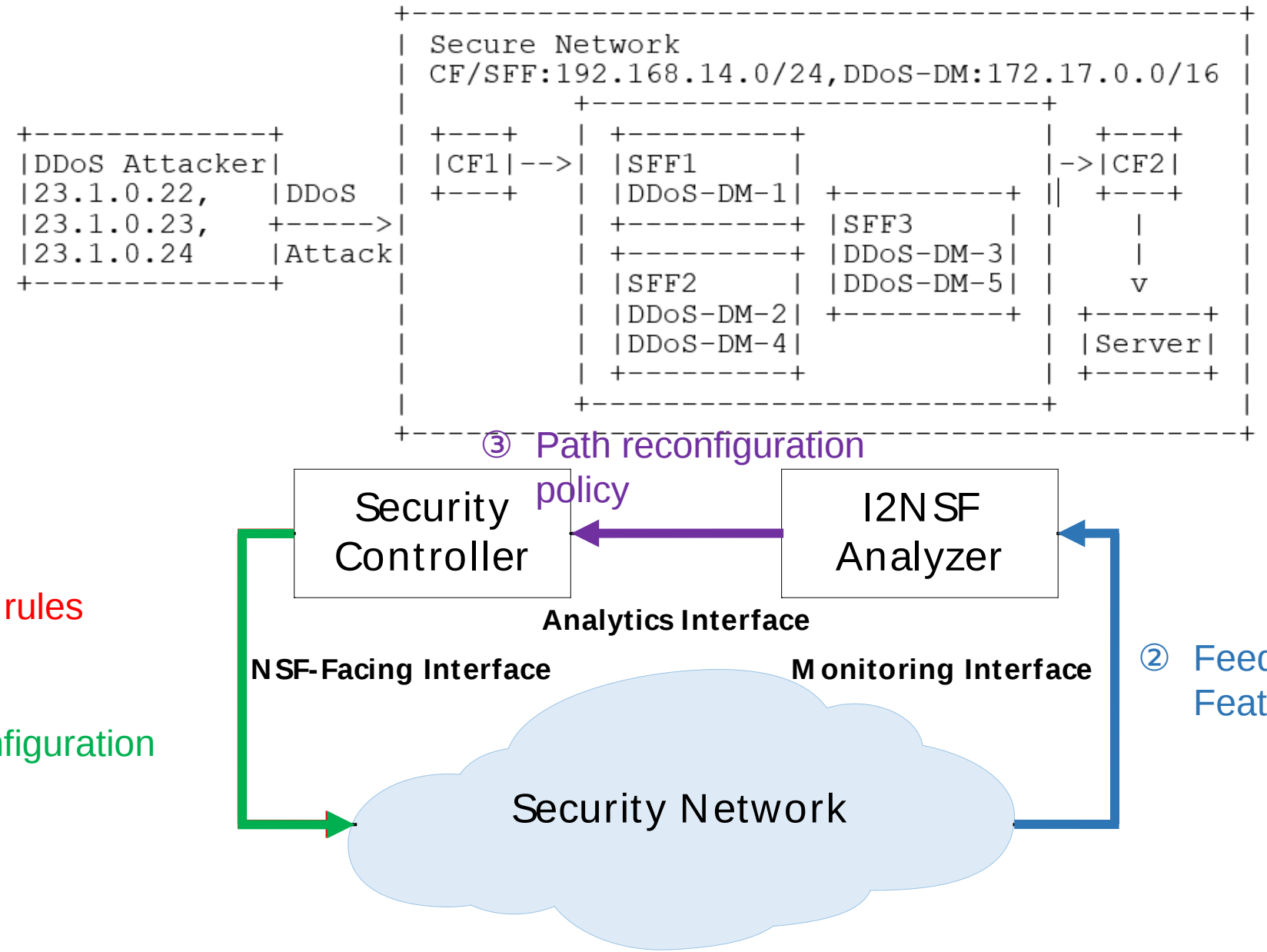
- Analytics Interface
  - **Path reconfiguration policy**

```
+--rw i2nsf-reconfiguration-policy* [name]
   +--rw name                                    string
   +--rw (policy-type)?
      +--:(path-reconfiguration-policy)
         +--rw path-reconfiguration-policy
            +--rw service-function-path* [path-id]
               +--rw path-id                     string
               +--rw nsfs
                  +--rw nsf* [nsf-name]
                     +--rw nsf-name              string
                     +--rw sequence-number?      uint64
```

- NSF-Facing Interface
  - **Path reconfiguration rule**

```
+--rw i2nsf-security-policy* [policy-name]
   +--rw policy-name                    string
   +--rw path-configuration-rule
      +--rw path-id?       string
      +--rw classifiers
      |  +--rw classifier* [classifier-name]
      |     +--rw classifier-name       string
      |     +--rw classifier-ip?        inet:ip-address-no-zone
      +--rw nsfs
         +--rw nsf* [nsf-name]
            +--rw nsf-name            string
            +--rw sequence-number?    uint64
            +--rw ip-address
               +--rw nsf-ip?    inet:ip-address-no-zone
               +--rw sff-ip?    inet:ip-address-no-zone
```

Use Case


Secure Network
CF/SFF:192.168.14.0/24,DDoS-DM:172.17.0.0/16
DDoS Attacker
23.1.0.22,
23.1.0.23,
23.1.0.24
DDoS
Attack
CF1
SFF1
DDoS-DM-1
SFF3
DDoS-DM-3
SFF2
DDoS-DM-2
DDoS-DM-4
DDoS-DM-5
CF2
Server
③ Path reconfiguration policy
Security Controller
I2NSF Analyzer
Analytics Interface
NSF-Facing Interface
Monitoring Interface
Security Network
① Initial path rules
② Feedback Traffic Flow Features
④ Path reconfiguration rules

Use Case

① Initial path rules

Path1= {DDoS-DM-2, DDoS-DM-1, DDoS-DM-4, DDoS-DM-3}

② Feedback Traffic Flow Features

```
<i2nsf-traffic-flow-features>
  <measurement-time>5</measurement-time>
  <packets-per-second>400.18</packets-per-second>
  <bytes-per-second>450643.1</bytes-per-second>
  <packet-size-mean>1126.1</packet-size-mean>
  <src-ip-entropy>3.27</src-ip-entropy>
  <dst-ip-entropy>1.71</dst-ip-entropy>
  <TTL-entropy>3.17</TTL-entropy>
  <tcp-src-port-entropy>5.34</tcp-src-port-entropy>
  <tcp-dst-port-entropy>4.44</tcp-dst-port-entropy>
  <udp-src-port-entropy>5.02</udp-src-port-entropy>
  <udp-dst-port-entropy>5.02</udp-dst-port-entropy>
  <packet-size-entropy>2.5</packet-size-entropy>
  <packets-variance>0</packets-variance>
</i2nsf-traffic-flow-features>
```

③ Path reconfiguration policy

```
<service-function-path>
  <path-id>path2</path-id>
  <nsfs>
    <nsf>
      <nsf-name>DDoS-DM-5</nsf-name>
      <sequence-number>1</sequence-number>
    </nsf>
    <nsf>
      <nsf-name>DDoS-DM-3</nsf-name>
      <sequence-number>2</sequence-number>
    </nsf>
    <nsf>
      <nsf-name>DDoS-DM-4</nsf-name>
      <sequence-number>3</sequence-number>
    </nsf>
  </nsfs>
</service-function-path>
```

④ Path reconfiguration rules

```
<path-configuration-rule>
  <path-id>path2</path-id>
  <classifiers>
    <classifier>
      <classifier-name>CF1</classifier-name>
      <classifier-ip>192.168.14.7</classifier-ip>
    </classifier>
    <classifier>
      <classifier-name>CF2</classifier-name>
      <classifier-ip>192.168.14.8</classifier-ip>
    </classifier>
  </classifiers>
  <nsfs>
    <nsf>
      <nsf-name>DDoS-DM-5</nsf-name>
      <sequence-number>1</sequence-number>
      <ip-address>
        <nsf-ip>172.17.23.2</nsf-ip>
        <sff-ip>192.168.14.23</sff-ip>
      </ip-address>
    </nsf>
    <nsf>
      <nsf-name>DDoS-DM-3</nsf-name>
      <sequence-number>2</sequence-number>
      <ip-address>
        <nsf-ip>172.17.23.3</nsf-ip>
        <sff-ip>192.168.14.23</sff-ip>
      </ip-address>
    </nsf>
    <nsf>
      <nsf-name>DDoS-DM-4</nsf-name>
      <sequence-number>3</sequence-number>
      <ip-address>
        <nsf-ip>172.17.24.2</nsf-ip>
        <sff-ip>192.168.14.24</sff-ip>
      </ip-address>
    </nsf>
  </nsfs>
</path-configuration-rule>
```

Path2= {DDoS-DM-5, DDoS-DM-3, DDoS-DM-4}

Summary

- I2NSF Framework for Attacks Intelligent Detection is the application of I2NSF Framework for Security Management Automation for attacks intelligent detection in SDN and SFC environment.
- Its YANG data models are based on the existing I2NSF YANG data models (NSF-Facing, Monitoring and Analytics Interface).
- It implements closed-loop intelligent detection by dynamically adjust detection policies .
- The use case shows the dynamic automatic adjustment of DDoS attack detection path policy based on the closed-loop feedback.

Thank you!