



I2NSF YANG Data Models

draft-ietf-i2nsf-capability-data-model-03
draft-ietf-i2nsf-consumer-facing-interface-dm-03
draft-ietf-i2nsf-nsf-facing-interface-dm-04
draft-ietf-i2nsf-registration-interface-dm-02
draft-ietf-i2nsf-nsf-monitoring-data-model-00

IETF 104, Prague

March 26, 2019

Jaehoon Paul Jeong

pauljeong@skku.edu

Sungkyunkwan University

WG Documents of YANG Data Models

- Information Model Draft on NSF Capabilities
 - draft-ietf-i2nsf-capabilities-04
- Base YANG Data Model Draft
 - draft-ietf-i2nsf-capability-data-model-03
- I2NSF Interface YANG Data Model Drafts
 - draft-ietf-i2nsf-consumer-facing-interface-dm-03
 - draft-ietf-i2nsf-nsf-facing-interface-dm-04
 - draft-ietf-i2nsf-registration-interface-dm-02
 - draft-ietf-i2nsf-nsf-monitoring-data-model-00
- Verification of those YANG Data Models
 - Those will be verified through the 8 IETF Hackathons (IETF 97 ~ IETF 104).

Updates from the Previous Versions

- Consistency with **NSF Capabilities Information Model**
 - draft-ietf-i2nsf-capabilities-04
- Revision of YANG data modules according to YANG guidelines (RFC 6087)
- Synchronization among Data Models of I2NSF Interfaces
 - NSF Capability
 - Consumer-Facing Interface
 - NSF-Facing Interface
 - Registration Interface
 - NSF Monitoring
- XML Files for Three Kinds of Security Services
 - Network Security: Firewall, Time-based Firewall
 - Contents Security: Web Filter, VoIP/VoLTE Security
 - Attack Mitigation Security: HTTP(S) Flood-Attack Mitigator

Updates of Capability Data Model (DM)

- Consistency with NSF Capabilities Information Model
 - draft-ietf-i2nsf-capabilities-04
- Relationship with Other YANG Data Models
 - draft-ietf-i2nsf-consumer-facing-interface-dm-03
 - draft-ietf-i2nsf-nsf-facing-interface-dm-04
 - draft-hyun-i2nsf-registration-interface-dm-02
- Revision of YANG Data Module according to Guidelines in RFC 6087
- Restructure of the Overall YANG Data Module

Revision of YANG Data Module according to Guidelines in RFC 6087

1.	Introduction	3
2.	Terminology	3
2.1.	Requirements Notation	3
2.2.	NETCONF Terms	4
2.3.	YANG Terms	4
2.4.	Terms	4
3.	General Documentation Guidelines	5
3.1.	Module Copyright	5
3.2.	Narrative Sections	6
3.3.	Definitions Section	6
3.4.	Security Considerations Section	6
3.5.	IANA Considerations Section	7
3.5.1.	Documents that Create a New Namespace	7
3.5.2.	Documents that Extend an Existing Namespace	8
3.6.	Reference Sections	8
4.	YANG Usage Guidelines	8
4.1.	Module Naming Conventions	8
4.2.	Identifiers	9
4.3.	Defaults	9
4.4.	Conditional Statements	10
4.5.	XPath Usage	10
4.6.	Lifecycle Management	11
4.7.	Module Header, Meta, and Revision Statements	12
4.8.	Namespace Assignments	13
4.9.	Top-Level Data Definitions	14
4.10.	Data Types	14
4.11.	Reusable Type Definitions	15
4.12.	Data Definitions	15
4.13.	Operation Definitions	17
4.14.	Notification Definitions	17
5.	IANA Considerations	17
6.	Security Considerations	18
6.1.	Security Considerations Section Template	19
7.	Acknowledgments	20
8.	References	20
8.1.	Normative References	20
8.2.	Informative References	21
Appendix A.	Module Review Checklist	22
Appendix B.	YANG Module Template	24

Updates of NSF-Facing Interface DM

- Consistency with NSF Capabilities Information Model
 - draft-ietf-i2nsf-capabilities-04
- Revision of YANG Data Module according to Guidelines in RFC 6087
- Addition of Exact Match Type and Range Match Type
- Addition of Configuration XML Examples
 - Scenario 1 - Block SNS access during business hours
 - Scenario 2 - Block malicious VoIP/VoLTE packets coming to the company
 - Scenario 3 - Mitigate HTTP and HTTPS flood attacks on a company web Server

Addition of Configuration XML Examples

Security Service: Block SNS Access during Business Hours

Time-based Firewall

```
<i2nsf-security-policy
xmlns="urn:ietf:params:xml:ns:yang:ietf-i2nsf-policy-rule-for-nsf">
<system-policy>
  <system-policy-name>sns_access</system-policy-name>
  <rules>
    <rule-name>block_sns_access_during_operation_time</rule-name>
    <time-zone>
      <absolute-time-zone>
        <start-time>09:00:00Z</start-time>
        <end-time>18:00:00Z</end-time>
      </absolute-time-zone>
    </time-zone>
    <condition-clause-container>
      <packet-security-ipv4-condition>
        <pkt-sec-ipv4-src>
          <range-ipv4-address>
            <start-ipv4-address>221.159.112.1</start-ipv4-address>
            <end-ipv4-address>221.159.112.90</end-ipv4-address>
          </range-ipv4-address>
        </pkt-sec-ipv4-src>
      </packet-security-ipv4-condition>
    </condition-clause-container>
    <action-clause-container>
      <advanced-action>
        <content-security-control>url-filtering</content-security-control>
      </advanced-action>
    </action-clause-container>
  </rules>
</system-policy>
</i2nsf-security-policy>
```

Web Filter

```
<i2nsf-security-policy
xmlns="urn:ietf:params:xml:ns:yang:ietf-i2nsf-policy-rule-for-nsf">
<system-policy>
  <system-policy-name>sns_access</system-policy-name>
  <rules>
    <rule-name>block facebook and instagram</rule-name>
    <condition-clause-container>
      <packet-security-http-condition>
        <pkt-sec-url-content>facebook</pkt-sec-url-content>
        <pkt-sec-url-content>instagram</pkt-sec-url-content>
      </packet-security-http-condition>
    </condition-clause-container>
    <action-clause-container>
      <packet-action>
        <egress-action>drop</egress-action>
      </packet-action>
    </action-clause-container>
  </rules>
</system-policy>
</i2nsf-security-policy>
```

Updates of Consumer-Facing Interface DM

- Merging the information model & data model:
 - draft-ietf-i2nsf-consumer-facing-interface-dm-02
 - draft-kumar-i2nsf-client-facing-interface-im-06
- Changes are as follows:
 - More detailed information about each object in DM
 - Grouping is used to group repeated parts in DM
 - DM more generic for various security services

Updates: Grouping

- Grouping to group the repeated parts of the data model.
 - Recurring fields (e.g., “name” and “date”) are grouped as “meta”.

```
grouping meta {  
  leaf name {  
    type string;  
  }  
  leaf date {  
    type yang:date-and-time;  
  }  
}
```

```
grouping ip-address {  
  choice match-type {  
    case exact-match {  
      leaf-list ip-address {  
        type inet:ipv4-address;  
      }  
    }  
    case range-match {  
      list range-ip-address {  
        key "start-ip-address end-ip-address";  
        leaf start-ip-address {  
          type inet:ipv4-address;  
        }  
        leaf end-ip-address {  
          type inet:ip-address;  
        }  
      }  
    }  
  }  
}
```

```
container threat-prevention {  
  list threat-feed-list {  
    uses meta;  
    key "name";  
    container threat-feed-server {  
      uses ip-address;  
      leaf threat-feed-description {  
        type string;  
      }  
    }  
  }  
}
```

Updates: Generic Data Model

- A generic data model is provided.
 - A condition object can cover most of the firewall, DPI, DDoS-mitigation cases.

```
+--rw condition
  +--rw firewall-condition
    | +--rw source-target
    | | +--rw src-target? -> /endpoint-group/...
    | +--rw destination-target
    |   +--rw dest-target* -> /endpoint-group/...
  +--rw ddos-condition
    | +--rw source-target
    | +--rw destination-target
    | +--rw rate-limit
  +--rw custom-condition
    | ...
  +--rw threat-feed-condition
    ...
```

Flexible Conditions:

- The condition object can flexibly cover general network security services.
- Custom-condition can cover DPI which inspects a packet's payload.
- Threat-feed-condition can consider file types and signature information.

Addition of Configuration XML Examples

Security Service: Block SNS Access during Business Hours

Registered User Group

```
<?xml version="1.0" encoding="UTF-8" ?>
<ietf-i2nsf-cfi-policy:endpoint-group>
  <user-group>
    <name>employees</name>
    <range-ip-address>
      <start-ip-address>221.159.112.1</start-ip-address>
      <end-ip-address>221.159.112.90</end-ip-address>
    </range-ip-address>
  </user-group>
  ...
  ...
</ietf-i2nsf-cfi-policy:endpoint-group>
```

"name" as a key

Registered Payload Content

```
<?xml version="1.0" encoding="UTF-8" ?>
<ietf-i2nsf-cfi-policy:threat-prevention>
  <payload-content>
    <name>sns-websites</name>
    <content>facebook</content>
    <content>instagram</content>
    <content>twitter</content>
    ...
  </payload-content>
</ietf-i2nsf-cfi-policy:threat-prevention>
```

"name" as a key

Generated Security Policy

```
<ietf-i2nsf-cfi-policy:policy>
  <policy-name>security_policy_for_blocking_sns</policy-name>
  <rule>
    <rule-name>block_access_to_sns_during_office_hours</rule-name>
    <event>
      <time-information>
        <begin-time>09:00</begin-time>
        <end-time>18:00</end-time>
      </time-information>
    </event>
    <condition>
      <firewall-condition>
        <source-target>
          <src-target>employees</src-target>
        </source-target>
        <destination-target>
          <dest-target>sns-websites</dest-target>
        </destination-target>
      </firewall-condition>
    </condition>
    <action>
      <primary-action>drop</primary-action>
    </action>
  </rule>
</ietf-i2nsf-cfi-policy:policy>
```

Updates of Registration Interface DM

- Clarification of Objectives of I2NSF Registration Interface
 - NSF Capability Registration
 - NSF Capability Query
- Revision of YANG Data Module according to Guidelines in RFC 6087
- Revision of the Overall YANG Data Module
- Addition of Description for YANG Tree Diagram
- Addition of Configuration XML Examples

Addition of Configuration XML Examples

Set-up Service: Registration for Capabilities of General Firewall

```
<i2nsf-nsf-registrations
  xmlns="urn:ietf:params:xml:ns:yang:ietf-i2nsf-reg-interface"
  xmlns:capa="urn:ietf:params:xml:ns:yang:ietf-i2nsf-capability">
  <i2nsf-nsf-capability-registration>
    <nsf-name>general_firewall_capability</nsf-name>
    <nsf-capability-info>
      <i2nsf-capability>
        <condition-capabilities>
          <generic-nsf-capabilities>
            <ipv4-capa>capa:ipv4-protocol</ipv4-capa>
            <ipv4-capa>capa:exact-ipv4-address</ipv4-capa>
            <ipv4-capa>capa:range-ipv4-address</ipv4-capa>
            <tcp-capa>capa:exact-tcp-port-num</tcp-capa>
            <tcp-capa>capa:range-tcp-port-num</tcp-capa>
          </generic-nsf-capabilities>
        </condition-capabilities>
        <action-capabilities>
          <ingress-action-capa>capa:pass</ingress-action-capa>
          <ingress-action-capa>capa:drop</ingress-action-capa>
          <ingress-action-capa>capa:alert</ingress-action-capa>
          <egress-action-capa>capa:pass</egress-action-capa>
          <egress-action-capa>capa:drop</egress-action-capa>
          <egress-action-capa>capa:alert</egress-action-capa>
        </action-capabilities>
      </i2nsf-capability>
    </nsf-capability-info>
  </i2nsf-nsf-capability-registration>
</i2nsf-nsf-registrations>
```

```
<nsf-performance-capability>
  <processing>
    <processing-average>1000</processing-average>
    <processing-peak>5000</processing-peak>
  </processing>
  <bandwidth>
    <outbound>
      <outbound-average>1000</outbound-average>
      <outbound-peak>5000</outbound-peak>
    </outbound>
    <inbound>
      <inbound-average>1000</inbound-average>
      <inbound-peak>5000</inbound-peak>
    </inbound>
  </bandwidth>
</nsf-performance-capability>
</nsf-capability-info>
```

```
<nsf-access-info>
  <nsf-instance-name>general_firewall</nsf-instance-name>
  <nsf-address>221.159.112.100</nsf-address>
  <nsf-port-address>3000</nsf-port-address>
</nsf-access-info>
</i2nsf-nsf-capability-registration>
</i2nsf-nsf-registrations>
```

Updates of NSF Monitoring DM

- Merging of NSF Monitoring Information Model and Data Model Drafts
 - draft-zhang-i2nsf-info-model-monitoring-07
 - draft-hong-i2nsf-nsf-monitoring-data-model-06
- Revision of YANG Data Module according to Guidelines in RFC 6087
- Revision of the Overall YANG Data Module
- Replacing enumeration type with identity type for scalable components
- Addition of Description for YANG Tree Diagram

Next Steps

- WG Last Call for I2NSF Interface Data Models
 - NSF Capability DM
 - NSF-Facing Interface DM
 - Consumer-Facing Interface DM
 - Registration Interface DM
- NSF Monitoring Data Model Draft
 - We will improve it through the implementation of NSF Monitoring DM.
 - We are planning to test it in IETF-105 Hackathon Project.
- Verification of Data Models by YANG Doctors
 - During WG Last Call, I2NSF WG chairs need to ask YANG doctors to review the data models.