Revision Letter

I2NSF Consumer-Facing Interface YANG Data Model

- **Old Draft Name: draft-ietf-i2nsf-consumer-facing-interface-dm-09**
- **New Draft Name: draft-ietf-i2nsf-consumer-facing-interface-dm-10**

Jaehoon Paul Jeong

August 28, 2020

Dear Jan Lindblad,

I sincerely appreciate your further valuable comments on the Consumer-Facing Interface Data Model document. Your comments use a bold font, and my answers use a regular font with the prefix [PAUL].

Document: draft-ietf-i2nsf-consumer-facing-interface-dm-09

Reviewer: Jan Lindblad

Review Date: July 23, 2020

Review Type: Working Group Last Call

Intended Status: Standards Track

Paul,
Good work with the module, and sorry for the slow response. I have been OOO. I read through this again today, and I have some comments, if you are interested. I guess this is not part of any formal review any more.

1. Figure 1: Not sure I understand what the arrow from "Consumer-Facing Interface Information Model" ---> "Consumer-Facing Interface Data Model" means, but it probably does no harm.

=> [Paul] I have removed the information model box from Figure 1 as follows.

OLD:

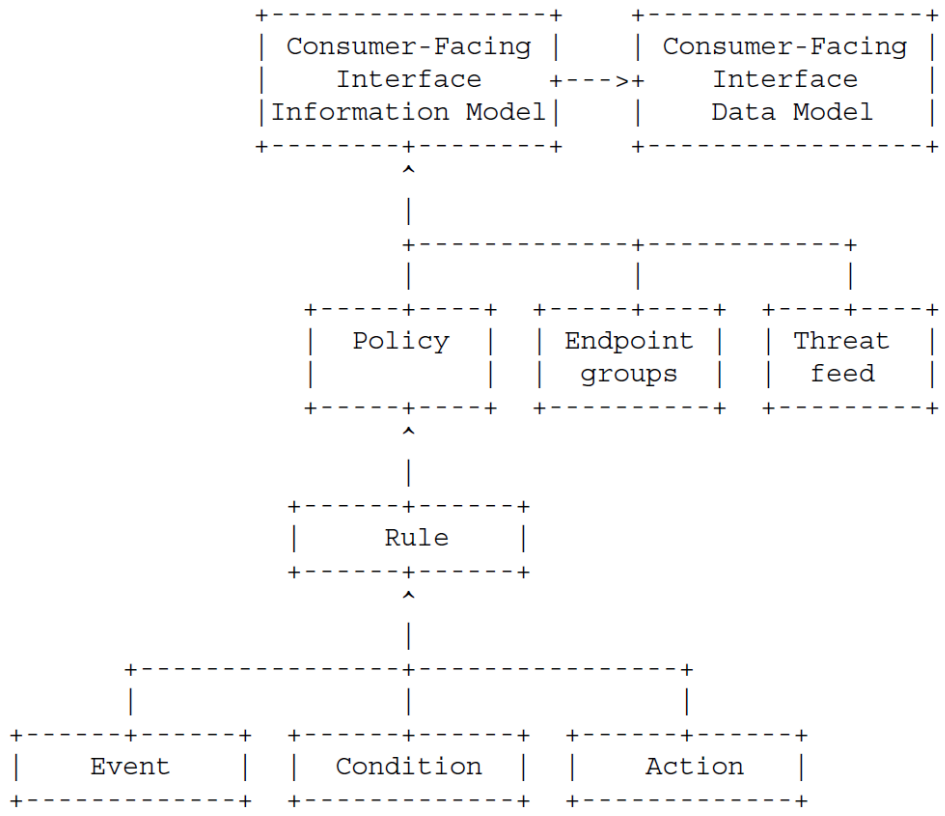

Figure 1: Diagram for High-level Abstraction of Consumer-Facing Interface

NEW:

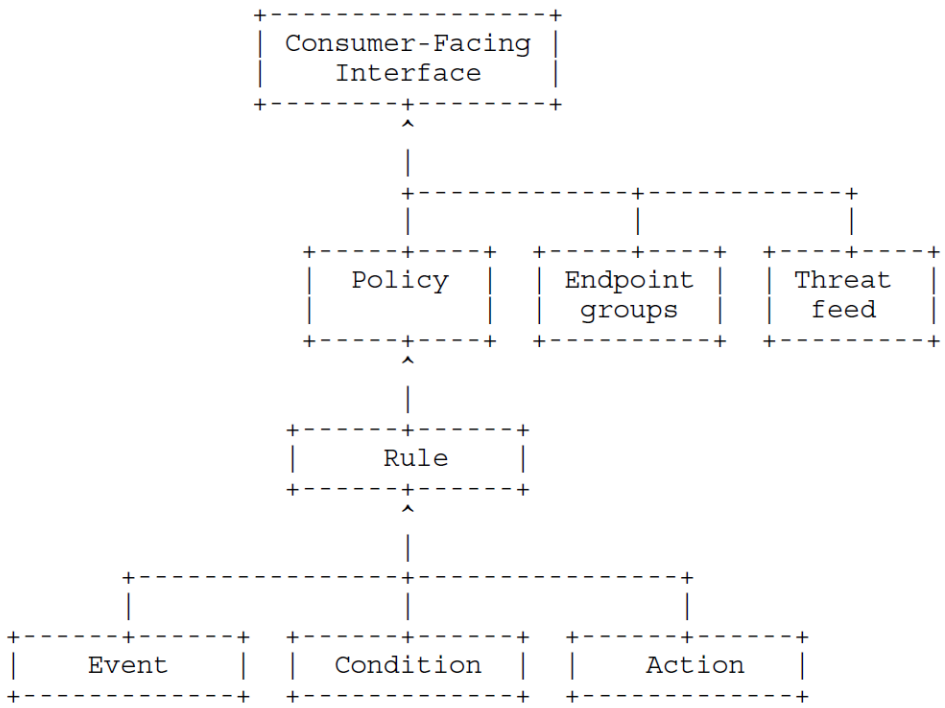

Figure 1: Diagram for High-level Abstraction of Consumer-Facing Interface

2. Figure 5: The tree diagram leafref paths are strange (e.g. -> /../../user-group/name)
=> [Paul] We have changed the path of each leafref into the correct path.
OLD:

```
      +--rw condition
         +--:firewall-condition
         |  +--rw source  -> /../../user-group/name
         |  +--rw destination* -> /../../user-group/name
         +--:ddos-condition
         |  +--rw source* -> /../../device-group/name
         |  +--rw destination* -> /../../device-group/name
         |  +--rw rate-limit
         |     +--rw packet-threshold-per-second? uint32
         +--:location-condition
         |  +--rw source* -> /../../location-group/name
         |  +--rw destination  -> /../../location-group/name
         +--:custom-condition
         |  +--rw source* -> /../../payload-content/name
         |  +--rw destination  -> /../../payload-content/name
         +--:threat-feed-condition
         +--rw source* -> /../../threat-feed-list/name
         +--rw destination  -> /../../threat-feed-list/name
```

Figure 5: Condition Sub-model YANG Data Tree

NEW:

```
+--rw condition
   +--:firewall-condition
   |  +--rw source
   |  |       -> /i2nsf-cfi-policy/endpoint-groups/user-group/name
   |  +--rw destination*
   |  |       -> /i2nsf-cfi-policy/endpoint-groups/user-group/name
   +--:ddos-condition
   |  +--rw source*
   |  |       -> /i2nsf-cfi-policy/endpoint-groups/device-group/name
   |  +--rw destination*
   |  |       -> /i2nsf-cfi-policy/endpoint-groups/device-group/name
   |  +--rw rate-limit
   |  |  +--rw packet-threshold-per-second? uint32
   +--:location-condition
   |  +--rw source*
   |  |       -> /i2nsf-cfi-policy/endpoint-groups/location-group/name
   |  +--rw destination
   |  |       -> /i2nsf-cfi-policy/endpoint-groups/location-group/name
   +--:custom-condition
   |  +--rw source*
   |  |       -> /i2nsf-cfi-policy/threat-preventions/payload-content/name
   |  +--rw destination?
   |  |       -> /i2nsf-cfi-policy/threat-preventions/payload-content/name
   +--:threat-feed-condition
      +--rw source*
      |       -> /i2nsf-cfi-policy/threat-preventions/threat-feed-list/name
      +--rw destination?
      |       -> /i2nsf-cfi-policy/threat-preventions/threat-feed-list/name
```

Figure 5: Condition Sub-model YANG Data Tree

3. Figure 7, figure 12: The UML diagram cardinality is given as "1..n" in several places. In the actual YANG, the cardinality is "0..n"
=> [Paul] We changed the cardinality from 1..n to 0..n in Figure 7 and Figure 12.

OLD:

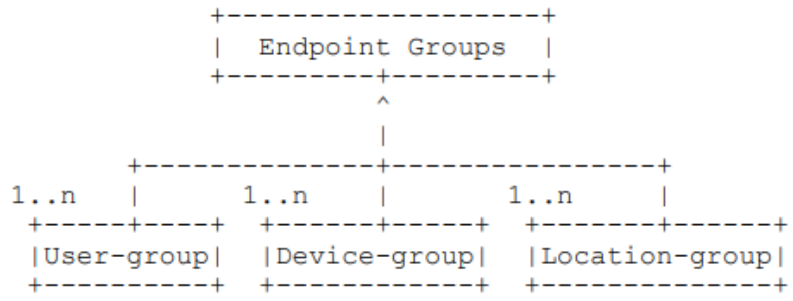

Figure 7: Endpoint Group Diagram

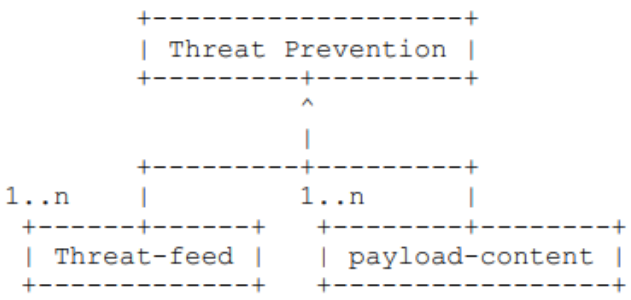

Figure 12: Threat Prevention Diagram

NEW:

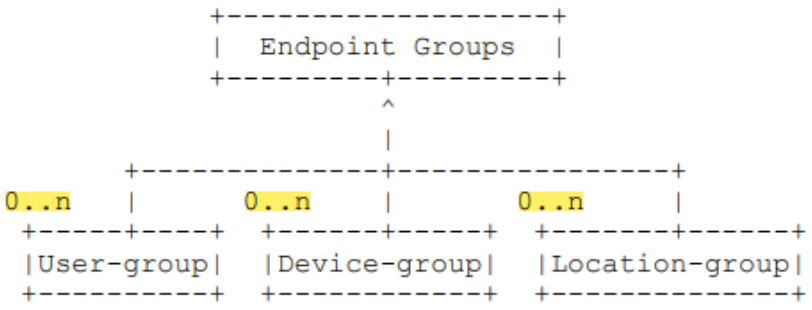

Figure 7: Endpoint Group Diagram

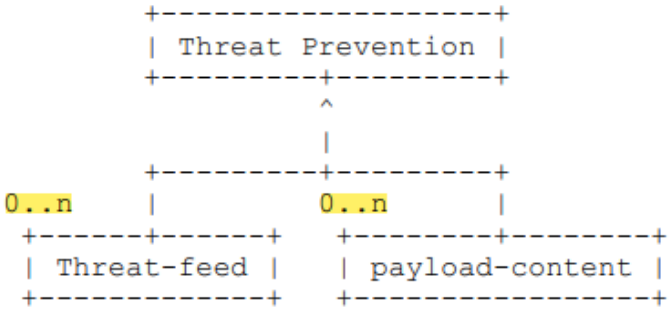

Figure 12: Threat Prevention Diagram

4. Section 5: The endpoint groups are mapped to a single IP or IP range. Is that sufficient for your use cases? Also, much of this information are IP addresses for users, devices and geo locations in the world are probably available in other systems with most network operators. Is it advisable to duplicate that information here? Sounds difficult to keep all this information in sync.

=> [Paul] Yes, that sufficient for our use cases. In our use cases, it is assumed that the information of Endpoint Groups (e.g., User-group, Device-group, and Location-group) IP addresses of users' devices are stored in the I2NSF database available to the I2NSF Security Controller, and that the IP address information in the I2NSF databased is synchronized with other systems in the networks under the same administration.

Section 5. Information Model for Policy Endpoint Groups (Page 10): The 2nd Paragraph

OLD	NEW
5. Information Model for Policy Endpoint Groups The Policy Endpoint Group is a very important part of building User- Construct based policies. A Security Administrator would create and use these objects to represent a logical entity in their business environment, where a Security Policy is to be applied. There are multiple managed objects that constitute a Policy's Endpoint Group as shown in Figure 7. Figure 8 shows the YANG tree of the Endpoint- Groups object. This section lists these objects and relationship among them.	5. Information Model for Policy Endpoint Groups The Policy Endpoint Group is a very important part of building User- Construct based policies. A Security Administrator would create and use these objects to represent a logical entity in their business environment, where a Security Policy is to be applied. There are multiple managed objects that constitute a Policy's Endpoint Group, as shown in Figure 7. Figure 8 shows the YANG tree of the Endpoint- Groups object. This section lists these objects and relationship among them. It is assumed that the information of Endpoint Groups (e.g., User-group, Device-group, and Location-group) such as the IP address(es) of each member in a group are stored in the I2NSF database available to the Security Controller, and that the IP address information of each group in the I2NSF database is synchronized with other systems in the networks under the same administration.

5. Section 6: Threat signatures and content patterns can be configured here. Is the expectation that the I2NSF client (operator?) configures these patterns, and the I2NSF server communicates these patterns to the threat feed servers, as a sort of controller? How this part of the model would be used is not clear to me.
=> [Paul] Yes, it is expected that the I2NSF Client (i.e., I2NSF User), which obtained the threat signatures (i.e., threat content patterns), delivers those threat signatures to the Security Controller. The retrieval of the threat signatures by the I2NSF User is out of the scope in this document.

Section 6.1. Threat Feed (Page 15): the 2nd Paragraph

OLD	NEW
6.1. Threat Feed … signatures: This field contains the signatures of malicious programs or activities provided by the threat-feed. The examples of signature types are "YARA", "SURICATA", and "SNORT".	6.1. Threat Feed … Signatures: This field contains the threat signatures of malicious programs or activities provided by the threat-feed. The examples of signature types are "YARA", "SURICATA", and "SNORT". It is assumed that the I2NSF User obtains the threat signatures (i.e., threat content patterns) from a threat-feed server (i.e., feed provider), which is a server providing threat signatures. With the obtained threat signatures, the I2NSF User can deliver them to the Security Controller. The retrieval of the threat signatures by the I2NSF User is out of scope in this document.

6. Section 9: The examples should use prefixed identity names. For example:
<protocol>http</protocol> should be <protocol>i2nsf-cfi:http</protocol>
and
<day>monday</day> should be <day>i2nsf-cfi:monday</day>
=> [Paul] We have added the prefix for identity names in our XML examples.

OLD:

```
<?xml version="1.0" encoding="UTF-8" ?>
<i2nsf-cfi-policy xmlns="urn:ietf:params:xml:ns:yang:ietf-i2nsf-cfi-policy">
  <endpoint-groups>
    <user-group>
      <name>employees</name>
      <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>
    </user-group>
    <device-group>
      <name>webservers</name>
      <range-ipv4-address>
        <start-ipv4-address>221.159.112.91</start-ipv4-address>
        <end-ipv4-address>221.159.112.97</end-ipv4-address>
      </range-ipv4-address>
      <protocol>http</protocol>
      <protocol>https</protocol>
    </device-group>
  </endpoint-groups>
</i2nsf-cfi-policy>
```

NEW:

```
<?xml version="1.0" encoding="UTF-8" ?>
<i2nsf-cfi-policy xmlns="urn:ietf:params:xml:ns:yang:ietf-i2nsf-cfi-policy">
  <endpoint-groups>
    <user-group>
      <name>employees</name>
      <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>
    </user-group>
    <device-group>
      <name>webservers</name>
      <range-ipv4-address>
        <start-ipv4-address>221.159.112.91</start-ipv4-address>
        <end-ipv4-address>221.159.112.97</end-ipv4-address>
      </range-ipv4-address>
      <protocol>cfi-policy:http</protocol>
      <protocol>cfi-policy:https</protocol>
    </device-group>
  </endpoint-groups>
</i2nsf-cfi-policy>
```

OLD:

```
<?xml version="1.0" encoding="UTF-8" ?>
<i2nsf-cfi-policy xmlns="urn:ietf:params:xml:ns:yang:ietf-i2nsf-cfi-policy">
  <policy-name>security_policy_for_blocking_sns123</policy-name>
  <rules>
    <rule>
      <rule-name>block_access_to_sns_during_office_hours</rule-name>
      <event>
        <time-information>
          <start-date-time>2020-03-11T09:00:00.00Z</start-date-time>
          <end-date-time>2020-12-31T18:00:00.00Z</end-date-time>
          <period>
            <start-time>09:00:00Z</start-time>
            <end-time>18:00:00Z</end-time>
            <day>monday</day>
            <day>tuesday</day>
            <day>wednesday</day>
            <day>thursday</day>
            <day>friday</day>
          </period>
        </time-information>
        <frequency>weekly</frequency>
      </event>
      <condition>
        <firewall-condition>
          <source>employees</source>
        </firewall-condition>
      </condition>
      <actions>
        <primary-action>drop</primary-action>
      </actions>
    </rule>
  </rules>
</i2nsf-cfi-policy>
```

NEW:

```
<?xml version="1.0" encoding="UTF-8" ?>
<i2nsf-cfi-policy xmlns="urn:ietf:params:xml:ns:yang:ietf-i2nsf-cfi-policy">
  <policy-name>security_policy_for_blocking_sns123</policy-name>
  <rules>
    <rule>
      <rule-name>block_access_to_sns_during_office_hours</rule-name>
      <event>
        <time-information>
          <start-date-time>2020-03-11T09:00:00.00Z</start-date-time>
          <end-date-time>2020-12-31T18:00:00.00Z</end-date-time>
          <period>
            <start-time>09:00:00Z</start-time>
            <end-time>18:00:00Z</end-time>
            <day>cfi-policy:monday</day>
            <day>cfi-policy:tuesday</day>
            <day>cfi-policy:wednesday</day>
            <day>cfi-policy:thursday</day>
            <day>cfi-policy:friday</day>
          </period>
        </time-information>
        <frequency>weekly</frequency>
      </event>
      <condition>
        <firewall-condition>
          <source>employees</source>
        </firewall-condition>
        <custom-condition>
          <destination>sns-websites</destination>
        </custom-condition>
      </condition>
      <actions>
        <primary-action>cfi-policy:drop</primary-action>
      </actions>
    </rule>
  </rules>
</i2nsf-cfi-policy>
```

7. Section 9.2 and 9.3: Even though the examples text talks about the value of "destination", no such tag is actually present in the XML.
=> [Paul] We have included the value of “destination” of custom-condition to properly express the XML example in Section 9.2 as follows. The XML example in Section 9.3 have already had the value of “destination” of firewall-condition.

OLD:

```
<?xml version="1.0" encoding="UTF-8" ?>
<i2nsf-cfi-policy xmlns="urn:ietf:params:xml:ns:yang:ietf-i2nsf-cfi-policy">
  <policy-name>security_policy_for_blocking_sns123</policy-name>
  <rules>
    <rule>
      <rule-name>block_access_to_sns_during_office_hours</rule-name>
      <event>
        <time-information>
          <start-date-time>2020-03-11T09:00:00.00Z</start-date-time>
          <end-date-time>2020-12-31T18:00:00.00Z</end-date-time>
          <period>
            <start-time>09:00:00Z</start-time>
            <end-time>18:00:00Z</end-time>
            <day>monday</day>
            <day>tuesday</day>
            <day>wednesday</day>
            <day>thursday</day>
            <day>friday</day>
          </period>
        </time-information>
        <frequency>weekly</frequency>
      </event>
      <condition>
        <firewall-condition>
          <source>employees</source>
        </firewall-condition>
      </condition>
      <actions>
        <primary-action>drop</primary-action>
      </actions>
    </rule>
  </rules>
</i2nsf-cfi-policy>
```

NEW:

```
<?xml version="1.0" encoding="UTF-8" ?>
<i2nsf-cfi-policy xmlns="urn:ietf:params:xml:ns:yang:ietf-i2nsf-cfi-policy">
  <policy-name>security_policy_for_blocking_sns123</policy-name>
  <rules>
    <rule>
      <rule-name>block_access_to_sns_during_office_hours</rule-name>
      <event>
        <time-information>
          <start-date-time>2020-03-11T09:00:00.00Z</start-date-time>
          <end-date-time>2020-12-31T18:00:00.00Z</end-date-time>
          <period>
            <start-time>09:00:00Z</start-time>
            <end-time>18:00:00Z</end-time>
            <day>cfi-policy:monday</day>
            <day>cfi-policy:tuesday</day>
            <day>cfi-policy:wednesday</day>
            <day>cfi-policy:thursday</day>
            <day>cfi-policy:friday</day>
          </period>
        </time-information>
        <frequency>weekly</frequency>
      </event>
      <condition>
        <firewall-condition>
          <source>employees</source>
        </firewall-condition>
        <custom-condition>
          <destination>sns-websites</destination>
        </custom-condition>
      </condition>
      <actions>
        <primary-action>cfi-policy:drop</primary-action>
      </actions>
    </rule>
  </rules>
</i2nsf-cfi-policy>
```

Then in the YANG module itself:

8. In ip-ranges like container range-ipv4-address, what happens if either of start- or end- address is omitted? Maybe explain in the description, or make both leafs mandatory?
=> [Paul] We make the fields of start- and end- (ipv4 and ipv6) addresses be mandatory as follows.

OLD:

```
case range-match-ipv4 {
  container range-ipv4-address {
    leaf start-ipv4-address {
      type inet:ipv4-address;
      description
        "Start IPv4 address for a range match.";
    }
    leaf end-ipv4-address {
      type inet:ipv4-address;
      description
        "End IPv4 address for a range match.";
    }
    description
      "Range match for an IP-address.";
  }
}
case range-match-ipv6 {
  container range-ipv6-address {
    leaf start-ipv6-address {
      type inet:ipv6-address;
      description
        "Start IPv6 address for a range match.";
    }
    leaf end-ipv6-address {
      type inet:ipv6-address;
      description
        "End IPv6 address for a range match.";
    }
    description
      "Range match for an IP-address.";
  }
}
```

NEW:

```
case range-match-ipv4 {
  container range-ipv4-address {
    leaf start-ipv4-address {
      type inet:ipv4-address;
      mandatory true;
      description
        "Start IPv4 address for a range match.";
    }
    leaf end-ipv4-address {
      type inet:ipv4-address;
      mandatory true;
      description
        "End IPv4 address for a range match.";
    }
    description
      "Range match for an IP-address.";
  }
}
case range-match-ipv6 {
  container range-ipv6-address {
    leaf start-ipv6-address {
      type inet:ipv6-address;
      mandatory true;
      description
        "Start IPv6 address for a range match.";
    }
    leaf end-ipv6-address {
      type inet:ipv6-address;
      mandatory true;
      description
        "End IPv6 address for a range match.";
    }
    description
      "Range match for an IP-address.";
  }
}
```

9. In container period there are several when-expressions that mean something else than you think:

```
container period{
    when
        "/i2nsf-cfi-policy/rules/rule/event/frequency!='only-once'";
```

By using an absolute path like this, the XPath expression looks for matching instances across all rules. This means this expression is true as soon as there is at least one rule with a frequency != 'only-once'. There are several other when expressions here with the same problem. What I think you mean is this:

```
container period{
    when
        "../../frequency!='only-once'";
```

This expression looks only at the frequency leaf in the same rule instance as the period container is in. The other when expressions can be fixed in a similar way.

=> [Paul] As the intent of the data model is to work only the frequency leaf in the same rule as you mention, I have changed the expression to have the proper path.

OLD:

```
container period{
  when
    "/i2nsf-cfi-policy/rules/rule/event/frequency!='only-once'";
  description
    "This represents the repetition time.
    In case of frequency is weekly, the days
    can be set.";
  leaf start-time {
    type time;
    description
      "This is period start time for event.";
  }
  leaf end-time {
    type time;
    description
      "This is period end time for event.";
  }
  leaf-list day {
    when
      "/i2nsf-cfi-policy/rules/rule/event/frequency='weekly'";
    type identityref{
      base day;
    }
    description
      "This represents the repeated day of
      every week (e.g., monday and tuesday).
      More than one day can be specified";
  }
  leaf-list date {
    when
      "/i2nsf-cfi-policy/rules/rule/event/frequency='monthly'";
    type int32{
      range "1..31";
    }
    description
      "This represents the repeated date of
      every month. More than one date can be
      specified.";
  }
  leaf-list month {
    when
      "/i2nsf-cfi-policy/rules/rule/event/frequency='yearly'";
    type string{
      pattern '\d{2}-\d{2}';
    }
    description
      "This represents the repeated date and month
      of every year. More than one can be specified.
      Pattern used is Month-Date (MM-DD).";
  }
}
```

NEW:

```
container period{
  when "../../frequency!='only-once'";
  description
    "This represents the repetition time.
    In case of frequency is weekly, the days
    can be set.";
  leaf start-time {
    type time;
    description
      "This is period start time for event.";
  }
  leaf end-time {
    type time;
    description
      "This is period end time for event.";
  }
  leaf-list day {
    when "../../../frequency='weekly'";
    type identityref{
      base day;
    }
    min-elements 1;
    description
      "This represents the repeated day of
      every week (e.g., monday and tuesday).
      More than one day can be specified";
  }
  leaf-list date {
    when "../../../frequency='monthly'";
    type int32{
      range "1..31";
    }
    min-elements 1;
    description
      "This represents the repeated date of
      every month. More than one date can be
      specified.";
  }
  leaf-list month {
    when "../../../frequency='yearly'";
    type string{
      pattern '\d{2}-\d{2}';
    }
    min-elements 1;
    description
      "This represents the repeated date and month
      of every year. More than one can be specified.
      Pattern used is Month-Date (MM-DD).";
  }
}
```

10. leaf frequency: What happens if this leaf is set to weekly and no day is specified? Or monthly, etc? One way of modeling this to avoid the problem is to make the leaf-list day, leaf-list date, leaf-list month etc a choice, so that the frequency is implicit by configuring a day, date or month. If none of them are set, that would mean only-once. Just a thought.

=> [Paul] I have made the leaf-list day, leaf-list date, and leaf-list month set at least one field to a value in the case where the frequency is set to weekly, monthly, or yearly. Hence, the configuration of day, date, or month holds at least field value as follows.

OLD:

```
leaf-list day {
  when
    "/i2nsf-cfi-policy/rules/rule/event/frequency='weekly'";
  type identityref{
    base day;
  }
  description
    "This represents the repeated day of
    every week (e.g., monday and tuesday).
    More than one day can be specified";
}
leaf-list date {
  when
    "/i2nsf-cfi-policy/rules/rule/event/frequency='monthly'";
  type int32{
    range "1..31";
  }
  description
    "This represents the repeated date of
    every month. More than one date can be
    specified.";
}
leaf-list month {
  when
    "/i2nsf-cfi-policy/rules/rule/event/frequency='yearly'";
  type string{
    pattern '\d{2}-\d{2}';
  }
  description
    "This represents the repeated date and month
    of every year. More than one can be specified.
    Pattern used is Month-Date (MM-DD).";
}
```

NEW:

```
leaf-list day {
  when
    "../../../frequency='weekly'";
  type identityref{
    base day;
  }
  min-elements 1;
  description
    "This represents the repeated day of
    every week (e.g., monday and tuesday).
    More than one day can be specified";
}
leaf-list date {
  when
    "../../../frequency='monthly'";
  type int32{
    range "1..31";
  }
  min-elements 1;
  description
    "This represents the repeated date of
    every month. More than one date can be
    specified.";
}
leaf-list month {
  when
    "../../../frequency='yearly'";
  type string{
    pattern '\d{2}-\d{2}';
  }
  min-elements 1;
  description
    "This represents the repeated date and month
    of every year. More than one can be specified.
    Pattern used is Month-Date (MM-DD).";
}
```

Thanks for your intensive and detailed comments to improve our draft.

Best Regards,

Paul

==========

Mr. Jaehoon (Paul) Jeong, Ph.D.

Associate Professor

Department of Software

Sungkyunkwan University

Office: +82-31-299-4957

Email: jaehoon.paul@gmail.com, pauljeong@skku.edu

Personal Homepage: http://iotlab.skku.edu/people-jaehoon-jeong.php