Revision Letter

Editor: Jaehoon Paul Jeong
Date: January 26, 2022

OLD: draft-ietf-i2nsf-nsf-facing-interface-dm-17
NEW: draft-ietf-i2nsf-nsf-facing-interface-dm-18

Dear Dan,

I sincerely appreciate your detailed comments to improve our NSF-Facing Interface YANG Data Model. I have addressed all your comments one by one. I use bold font for your comments and use a regular font for my responses with the prefix "=> [PAUL]".

Reviewer: Dan Romascanu
Review result: Ready with Issues

I am the assigned Gen-ART reviewer for this draft. The General Area Review Team (Gen-ART) reviews all IETF documents being processed by the IESG for the IETF Chair. Please treat these comments just like any other last call comments.

For more information, please see the FAQ at

<https://trac.ietf.org/trac/gen/wiki/GenArtfaq>.

Document: draft-ietf-i2nsf-nsf-facing-interface-dm-17
Reviewer: Dan Romascanu
Review Date: 2022-01-25
IETF LC End Date: 2021-11-23
IESG Telechat date: Not scheduled for a telechat

Summary:

This document defines a YANG data model for configuring security policy rules on Network Security Functions (NSF) in the Interface to the Network Security Functions (I2NSF) framework. It's a solid, well-written and complete document. It needs to be read in the context and together with several other documents belonging to the I2NSF deliveries. The document is Ready from the perspective of Gen-ART with a couple of minor non-blocking issues and a few editorial problems that could be easily clarified and fixed if needed.

Major issues:

Minor issues:

1. How can RFC 8329 be only an Informative Reference. The Introduction dully states that the YANG module is based upon the framework / architecture defined in RFC 8329, and Section 4 uses RFC 8329 in several reference clauses.

=> [PAUL] RFC 8329 (Framework for Interface to Network Security Function) is an Informational RFC. If RFC 8329 is moved to Normative Reference, the ID-NITS tool (https://www6.ietf.org/tools/idnits) returns an error as follows:

"** Downref: Normative reference to an Informational RFC: RFC 8329"

Thus, we put RFC 8329 as an Informative Reference.

2. Section 4.

> leaf frequency {
type enumeration

Is this enumeration sufficient (once, daily, weekly, monthly, yearly)? Are not more cases needed? more flexibility?

=> [PAUL] The usage of "leaf frequency" is combined with the usage of "container period". It determines when a security policy can be applied with more details. For example, if the policy needs to be applied every weekday (i.e., Monday, Tuesday, Wednesday, Thursday, and Friday), it is possible to use the following configuration:

```
<i2nsf-security-policy
xmlns="urn:ietf:params:xml:ns:yang:ietf-i2nsf-policy-rule-for-nsf">
 <name>sns_access</name>
 <rules>
  <name>block_sns_access_during_operation_time</name>
  <event>
    <time>
      <start-date-time>2021-03-11T09:00:00.00Z</start-date-time>
      <end-date-time>2021-12-31T18:00:00.00Z</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>
      <frequency>weekly</frequency>
    </time>
  </event>
  <condition>
   <ipv6>
    <source-ipv6-network>2001:db8:0:1::0/120</source-ipv6-network>
   </ipv6>
  </condition>
  <action>
   <advanced-action>
    <content-security-control>
      url-filtering
    </content-security-control>
   </advanced-action>
  </action>
 </rules>
</i2nsf-security-policy>
```

We believe that the combination of “frequency” and “period” is flexible enough to determine the active time of the security policy.

Nits/editorial comments:

1. Section 3.3:

> A condition clause of generic network security functions is defined as IPv4 condition, IPv6 condition, TCP condition, UDP condition, SCTP condition, DCCP condition, and ICMP (ICMPv4 and ICMPv6) condition.

Should not be rather 'or' instead of 'and'?

=> [PAUL] We change the word “and” to “or” according to your comment.

2. Section 4:

description of identity acces-violation

> "Identity for access-violation. Access-violation system event is an event when a user tries to access (read, write, create, or delete) any information or execute commands above their privilege."

'above their privilege' is vague - probably meaning not-conformant with the access profile

=> [PAUL] We add the clarification to the text following your comment as follows:

OLD:

```
  identity access-violation {
    base system-event;
    description
      "Identity for access-violation. Access-violation system
       event is an event when a user tries to access (read, write,
       create, or delete) any information or execute commands
       above their privilege.";
     reference
      "draft-ietf-i2nsf-nsf-monitoring-data-model-13: I2NSF NSF
       Monitoring YANG Data Model - System event for access
       violation";
  }
```

NEW:

```
  identity access-violation {
    base system-event;
    description
      "Identity for access-violation. Access-violation system
       event is an event when a user tries to access (read, write,
       create, or delete) any information or execute commands
       above their privilege (i.e., not-conformant with the
       access profile).";
    reference
      "draft-ietf-i2nsf-nsf-monitoring-data-model-13: I2NSF NSF
```

```
      Monitoring YANG Data Model - System event for access
      violation";
  }
```

3. Section 4

identity memory-alarm

description
"Identity for memory alarm. Memory is the hardware to store information temporarily or for a short period, i.e., Random Access Memory (RAM). A memory-alarm is emitted when the RAM usage exceeds the threshold.";

memory-alarm is emitted when the memory usage is exceeding the threshold - RAM example does not really help, the alarm applies to all types of memory
=> [PAUL] We updated the description following your comments as follows:

OLD:
```
  identity memory-alarm {
    base system-alarm;
    description
      "Identity for memory alarm. Memory is the hardware to store
       information temporarily or for a short period, i.e., Random
       Access Memory (RAM). A memory-alarm is emitted when the RAM
       usage exceeds the threshold.";
    reference
      "draft-ietf-i2nsf-nsf-monitoring-data-model-13: I2NSF NSF
       Monitoring YANG Data Model - System alarm for memory";
  }
```

NEW:
```
  identity memory-alarm {
    base system-alarm;
    description
      "Identity for memory alarm. Memory is the hardware to store
       information temporarily or for a short period, i.e., Random
       Access Memory (RAM). A memory-alarm is emitted when the memory
       usage is exceeding the threshold.";
    reference
      "draft-ietf-i2nsf-nsf-monitoring-data-model-13: I2NSF NSF
       Monitoring YANG Data Model - System alarm for memory";
  }
```

4. Section 4

```
    identity ot {
       base device-type;
       description
         "Identity for Operational Technology devices";
     }

     identity vehicle {
```

```
    base device-type;
    description
      "Identity for vehicle that connects to and shares
       data through the Internet";
  }
```

reference clauses would help - what is an OT and a 'vehicle' (in this context)?
=> [PAUL] We updated the descriptions to clarify OT and vehicle as follows:

OLD:

```
  identity ot {
    base device-type;
    description
      "Identity for Operational Technology devices";
  }

  identity vehicle {
    base device-type;
    description
      "Identity for vehicle that connects to and shares
       data through the Internet";
  }
```

NEW:

```
  identity ot {
    base device-type;
    description
      "Identity for Operational Technology (OT) devices (also
       known as industrial control systems) that interact
       with the physical environment and detect or cause direct
       change through the monitoring and control of devices,
       processes, and events such as programmable logic
       controllers (PLCs), digital oscilloscopes, building
       management systems (BMS), and fire control systems";
  }

  identity vehicle {
    base device-type;
    description
      "Identity for transportation vehicles that connect to and
       shares data through the Internet over Vehicle-to-Everything
       (V2X) communications.";
  }
```

5. Section 4

```
>     identity forwarding {
       base egress-action;
       description
         "Identity for forwarding. This action forwards the packet to
          another node in the network.";
     }
```

'This action forwards ... ' sounds odd. The action consists of forwarding, but does not perform it. I suggest re-wording. There are a few more such instances of 'This action [does] ...

=> [PAUL] We have updated the descriptions following your comments as follows:

OLD:

```
  identity invoke-signaling {
    base egress-action;
    description
      "Identity for invoke signaling. This action conveys
       information of the event triggering this action to a
       monitoring entity.";
  }

  identity tunnel-encapsulation {
    base egress-action;
    description
      "Identity for tunnel encapsulation. This action encapsulates
       the packet to be tunneled across the network to enable
       a secure connection.";
  }

  identity forwarding {
    base egress-action;
    description
      "Identity for forwarding. This action forwards the packet to
       another node in the network.";
  }

  identity transformation {
    base egress-action;
    description
      "Identity for transformation. This action transforms the
       packet by modifying its protocol header such as HTTP-to-CoAP
       translation.";
    reference
      "RFC 8075: Guidelines for Mapping Implementations: HTTP to the
       Constrained Application Protocol (CoAP) - Translation between
       HTTP and CoAP.";
  }
```

NEW:

```
  identity invoke-signaling {
    base egress-action;
    description
      "Identity for invoke signaling. The invoke signaling action
       is used to convey information of the event triggering this
       action to a monitoring entity.";
  }

  identity tunnel-encapsulation {
    base egress-action;
    description
      "Identity for tunnel encapsulation. The tunnel encapsulation
```

```
      action is used to encapsulate the packet to be tunneled across
      the network to enable a secure connection.";
  }

  identity forwarding {
    base egress-action;
    description
      "Identity for forwarding. The forwarding action is used to
      relay the packet from one network segment to another node
      in the network.";
  }

  identity transformation {
    base egress-action;
    description
      "Identity for transformation. The transformation action is used
      to transform the packet by modifying its protocol header such
      as HTTP-to-CoAP translation.";
    reference
      "RFC 8075: Guidelines for Mapping Implementations: HTTP to the
      Constrained Application Protocol (CoAP) - Translation between
      HTTP and CoAP.";
  }
```

Thanks for your valuable comments.

Best Regards,
Jaehoon (Paul) Jeong