Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 13, 2017

S. Hares
Huawei
R. Moskowitz
HTT Consulting
L. Xia
Huawei
J. Jeong
J. Kim
Sungkyunkwan University

March 12, 2017

I2NSF Capability YANG Data Model
draft-hares-i2nsf-capability-data-model-01

Abstract

This document defines a YANG data model for capabilities that enables an I2NSF user to control various network security functions in network security devices via an I2NSF security controller.

Table of Contents

1. Introduction 3
2. Requirements Language 3
3. Terminology 3
3.1. Tree Diagrams 4
4. High-Level YANG 4
4.1. Capabilities per NSF 4
4.2. Network Security Control 5
4.3. Content Security Control 6
4.4. Attack Mitigation Control 7
4.5. IT Resources linked to Capabilities 9
4.6. Actions 10
5. YANG Modules 10
6. IANA Considerations 32
7. Security Considerations 32
8. Acknowledgements 32
9. References 32
9.1. Normative References 32
9.2. Informative References 32
Appendix A. Changes from draft-hares-i2nsf-capability-data-model-00 33

1. Introduction

[i2nsf-problem-statement] proposes two different types of interfaces:

- Interface between I2NSF user and I2NSF security controller called I2NSF consumer-facing interface

- Interface between I2NSF security controller and network security functions (NSFs) called I2NSF NSF-facing interface

This document provides a YANG model that defines the capabilities for security devices that can be utilized by I2NSF NSF-facing interface between the I2NSF security controller and the NSF devices to express the capabilities of NSF devices. This YANG model can also be used by the IN2SF user (or I2NSF client) to provide security controller with a complete list of the I2NSF capabilities that can be controlled by security controller. This document defines a YANG [RFC6020] data model based on the [i2nsf-cap-im]. Terms used in document are defined in [i2nsf-terminology]. [i2nsf-cap-im] defines the following type of functionality in NSFs.

- Network Security Control

- Content Security Control

- Attack Mitigation Control

This document contains high-level YANG for each type of control.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Terminology

This document uses the terminology described in [i2nsf-cap-im] [i2rs-rib-data-model] [supa-policy-info-model]. Especially, the following terms are from [supa-policy-info-model]:

- Data Model: A data model is a representation of concepts of interest to an environment in a form that is dependent on data repository, data definition language, query language, implementation language, and protocol.

- Information Model: An information model is a representation of concepts of interest to an environment in a form that is

independent of data repository, data definition language, query language, implementation language, and protocol.

3.1. Tree Diagrams

A simplified graphical representation of the data model is used in this document. The meaning of the symbols in these diagrams [i2rs-rib-data-model] is as follows:

- Brackets "[" and "]" enclose list keys.
- Abbreviations before data node names: "rw" means configuration (read-write) and "ro" state data (read-only).
- Symbols after data node names: "?" means an optional node and "*" denotes a "list" and "leaf-list".
- Parentheses enclose choice and case nodes, and case nodes are also marked with a colon (":").
- Ellipsis ("...") stands for contents of subtrees that are not shown.

4. High-Level YANG

This section provides an overview of the high-level YANG.

4.1. Capabilities per NSF

The high-level YANG capabilities per NSF devices, controller, or application is the following:

```
module : ietf-i2nsf-capability
  +--rw sec-ctl-capabilities
  +--rw nsf-capabilities
    +--rw nsf* [nsf-name]
      +--rw nsf-name  string
      +--rw nsf-address
      |  +--rw (nsf-address-type)?
      |    +--: (ipv4-address)
      |    |  +--rw ipv4-address  inet:ipv4-address
      |    +--: (ipv6-address)
      |       +--rw ipv6-address  inet:ipv6-address
      +--rw net-sec-control-capabilities
      |  uses i2nsf-net-sec-control-caps
      +--rw con-sec-control-capabilities
      |  uses i2nsf-con-sec-control-caps
      +--rw attack-mitigation-capabilities
      |  uses i2nsf-attack-mitigation-control-caps
      +--rw it-resource
      |  uses i2nsf-it-resources
```

Figure 1: High-Level YANG of I2NSF Capability Interface

Each of these section mirror sections in: [i2nsf-cap-im]. The high-level YANG for net-sec-control-capabilities, con-sec-control-capabilities, and attack-mitigation-capabilities. This draft is also utilizes the concepts originated in Basile, Lioy, Pitscheider, and Zhao[2015] concerning conflict resoulution, use of external data, and IT-Resources. The authors are grateful to Cataldo for pointing out this excellent work.

4.2. Network Security Control

This section expands the

```
+--rw net-sec-control-capabilities
| uses i2nsf-net-sec-control-caps
```

Network Security Control

```
  +--rw i2nsf-net-sec-control-caps
    +--rw network-security-control
      +--rw nsc-support?  boolean
      +--rw nsc-fcn*  [nsc-fcn-name]
        +--rw nsc-fcn-name  string  //std or vendor name
```

Figure 2: High-Level YANG of Network Security Control

4.3. Content Security Control

This section expands the

```
            +--rw net-sec-control-capabilities
            | uses i2nsf-con-sec-control-caps
```

Content Security Control

```
  +--rw i2nsf-con-sec-control-caps
    +--rw content-security-control
      +--rw antivirus
      |  +--rw antivirus-support?  boolean
      |  +--rw antivirus-fcn*  [antivirus-fcn-name]
      |    +--rw antivirus-fcn-name  string  //std or vendor name
      +--rw ips
      |  +--rw ips-support?  boolean
      |  +--rw ips-fcn*  [ips-fcn-name]
      |    +--rw ips-fcn-name  string  //std or vendor name
      +--rw ids
      |  +--rw ids-support?  boolean
      |  +--rw ids-fcn*  [ids-fcn-name]
      |    +--rw ids-fcn-name  string  //std or vendor name
      +--rw url-filter
      |  +--rw url-filter-support?  boolean
      |  +--rw url-filter-fcn*  [url-filter-fcn-name]
      |    +--rw url-filter-fcn-name  string  //std or vendor name
      +--rw data-filter
      |  +--rw data-filter-support?  boolean
      |  +--rw data-filter-fcn*  [data-filter-fcn-name]
      |    +--rw data-filter-fcn-name  string  //std or vendor name
      +--rw mail-filter
      |  +--rw mail-filter-support?  boolean
      |  +--rw mail-filter-fcn*  [mail-filter-fcn-name]
      |    +--rw mail-filter-fcn-name  string  //std or vendor name
      +--rw dns-filter
      |  +--rw dns-filter-support?  boolean
      |  +--rw dns-filter-fcn*  [dns-filter-name]
      |    +--rw dns-filter-fcn-name  string  //std or vendor name
      +--rw ftp-filter
      |  +--rw ftp-filter-support?  boolean
      |  +--rw ftp-filter-fcn*  [ftp-filter-fcn-name]
      |    +--rw ftp-filter-fcn-name  string  //std or vendor name
      +--rw games-filter
      |  +--rw games-filter-support?  boolean
      |  +--rw games-filter-fcn*  [games-filter-fcn-name]
      |    +--rw games-filter-fcn-name  string  //std or vendor name
      +--rw p2p-filter
```

```
|  +--rw p2p-filter-support?  boolean
|  +--rw p2p-filter-fcn*  [p2p-filter-fcn-name]
|    +--rw p2p-filter-fcn-name  string  //std or vendor name
+--rw rpc-filter
|  +--rw rpc-filter-support?  boolean
|  +--rw rpc-filter-fcn*  [rpc-filter-fcn-name]
|    +--rw rpc-filter-fcn-name  string  //std or vendor name
+--rw sql-filter
|  +--rw sql-filter-support?  boolean
|  +--rw sql-filter-fcn*  [sql-filter-fcn-name]
|    +--rw sql-filter-fcn-name  string  //std or vendor name
+--rw telnet-filter
|  +--rw telnet-filter-support?  boolean
|  +--rw telnet-filter-fcn*  [telnet-filter-fcn-name]
|    +--rw telnet-filter-fcn-name  string  //std or vendor name
+--rw tftp-filter
|  +--rw tftp-filter-support?  boolean
|  +--rw tftp-filter-fcn*  [tftp-filter-fcn-name]
|    +--rw tftp-filter-fcn-name  string  //std or vendor name
+--rw file-blocking
|  +--rw file-blocking-support?  boolean
|  +--rw file-blocking-fcn*  [file-blocking-fcn-name]
|    +--rw file-blocking-fcn-name  string  //std or vendor name
+--rw pkt-capture
|  +--rw pkt-capture-support?  boolean
|  +--rw pkt-capture-fcn*  [pkt-capture-fcn-name]
|    +--rw pkt-capture-fcn-name  string  //std or vendor name
+--rw app-control
|  +--rw app-control-support?  boolean
|  +--rw app-control-fcn*  [app-control-fcn-name]
|    +--rw app-control-fcn-name  string  //std or vendor name
+--rw voip-volte
   +--rw voip-volte-support?  boolean
   +--rw voip-volte-fcn*  [voip-volte-fcn-name]
     +--rw voip-volte-fcn-name  string  //std or vendor name
```

Figure 3: High-Level YANG of Content Security Control

4.4. Attack Mitigation Control

This high-level YANG below expands the following section of the top-level model:

```
+--rw attack-mitigation-control-capabilities
| uses i2nsf-attack-mitigation-control-caps
```

Attack Mitigation Control

```
   +--rw i2nsf-attack-mitigation-control-caps
     +--rw attack-mitigation-control
       +--rw (attack-mitigation-control-type)?
         +--: (ddos-attack)
         |  +--rw (ddos-attack-type)?
         |    +--: (network-layer-ddos-attack)
         |    |  +--rw network-layer-ddos-attack-types
         |    |    +--rw syn-flood-attack
         |    |    |  +--rw syn-flood-attack-support?  boolean
         |    |    |  +--rw syn-flood-fcn*  [syn-flood-fcn-name]
         |    |    |    +--rw syn-flood-fcn-name  string
         |    |    +--rw udp-flood-attack
         |    |    |  +--rw udp-flood-attack-support?  boolean
         |    |    |  +--rw udp-flood-fcn*  [udp-flood-fcn-name]
         |    |    |    +--rw udp-flood-fcn-name  string
         |    |    +--rw icmp-flood-attack
         |    |    |  +--rw icmp-flood-attack-support?  boolean
         |    |    |  +--rw icmp-flood-fcn*  [icmp-flood-fcn-name]
         |    |    |    +--rw icmp-flood-fcn-name  string
         |    |    +--rw ip-fragment-flood-attack
         |    |    |  +--rw ip-fragment-flood-attack-support?  boolean
         |    |    |  +--rw ip-frag-flood-fcn*  [ip-frag-flood-fcn-name]
         |    |    |    +--rw ip-frag-flood-fcn-name  string
         |    |    +--rw ipv6-related-attack
         |    |       +--rw ipv6-related-attack-support?  boolean
         |    |       +--rw ipv6-related-fcn*  [ipv6-related-fcn-name]
         |    |         +--rw ipv6-related-fcn-name  string
         |    +--: (app-layer-ddos-attack)
         |       +--rw app-layer-ddos-attack-types
         |         +--rw http-flood-attack
         |         |  +--rw http-flood-attack-support?  boolean
         |         |  +--rw http-flood-fcn*  [http-flood-fcn-name]
         |         |    +--rw http-flood-fcn-name  string
         |         +--rw https-flood-attack
         |         |  +--rw https-flood-attack-support?  boolean
         |         |  +--rw https-flood-fcn*  [https-flood-fcn-name]
         |         |    +--rw https-flood-fcn-name  string
         |         +--rw dns-flood-attack
         |         |  +--rw dns-flood-attack-support?  boolean
         |         |  +--rw dns-flood-fcn*  [dns-flood-fcn-name]
         |         |    +--rw dns-flood-fcn-name  string
         |         +--rw dns-amp-flood-attack
         |         |  +--rw dns-amp-flood-attack-support?  boolean
         |         |  +--rw dns-amp-flood-fcn*  [dns-amp-flood-fcn-name]
         |         |    +--rw dns-amp-flood-fcn-name  string
         |         +--rw ssl-ddos-attack
         |            +--rw ssl-ddos-attack-support?  boolean
         |            +--rw ssl-ddos-fcn*  [ssl-ddos-fcn-name]
```

```
|              +--rw ssl-ddos-fcn-name  string
+--: (single-packet-attack)
   +--rw (single-packet-attack-type)?
     +--: (scan-and-sniff-attack)
     |  +--rw ip-sweep-attack
     |  |  +--rw ip-sweep-attack-support?  boolean
     |  |  +--rw ip-sweep-fcn*  [ip-sweep-fcn-name]
     |  |    +--rw ip-sweep-fcn-name  string
     |  +--rw port-scanning-attack
     |     +--rw port-scanning-attack-support?  boolean
     |     +--rw port-scanning-fcn*  [port-scanning-fcn-name]
     |       +--rw port-scanning-fcn-name  string
     +--: (malformed-packet-attack)
     |  +--rw ping-of-death-attack
     |  |  +--rw ping-of-death-attack-support?  boolean
     |  |  +--rw ping-of-death-fcn*  [ping-of-death-fcn-name]
     |  |    +--rw ping-of-death-fcn-name  string
     |  +--rw teardrop-attack
     |     +--rw teardrop-attack-support?  boolean
     |     +--rw tear-drop-fcn*  [tear-drop-fcn-name]
     |       +--rw tear-drop-fcn-name  string
     +--: (special-packet-attack)
        +--rw oversized-icmp-attack
        |  +--rw oversized-icmp-attack-support?  boolean
        |  +--rw oversized-icmp-fcn*  [oversized-icmp-fcn-name]
        |    +--rw oversized-icmp-fcn-name  string
        +--rw tracert-attack
           +--rw tracert-attack-support?  boolean
           +--rw tracert-fcn*  [tracert-fcn-name]
             +--rw tracert-fcn-name  string
```

Figure 4: High-Level YANG of Attack Mitigation Control

4.5. IT Resources linked to Capabilities

This section provides a link between capabilities and IT resources. This section has a list of IT resources by name. Additional input is needed.

```
               +--rw it-resource
               | uses i2nsf-it-resources
```

It Resource

```
               +--rw i2nsf-it-resources
                 +--rw it-resources* [it-resource-id]
                    +--rw it-resource-id  uint64
                    +--rw it-resource-name  string
```

Figure 5: High-Level YANG of IT Resources

4.6. Actions

Notifications indicate when rules are added or deleted. These notifications will be defined later.

5. YANG Modules

This section introduces a YANG module for the information model of I2NSF capability interface, as defined in the [i2nsf-cap-im].

<CODE BEGINS> file "ietf-i2nsf-capability@2017-03-12.yang"

```
module ietf-i2nsf-capability {
  namespace
    "urn:ietf:params:xml:ns:yang:ietf-i2nsf-capability";
  prefix
    i2nsf-capability;

  import ietf-inet-types{
    prefix inet;
  }

  organization
    "IETF I2NSF (Interface to Network Security Functions)
     Working Group";

  contact
    "WG Web: <http://tools.ietf.org/wg/i2nsf>
     WG List: <mailto:i2nsf@ietf.org>

     WG Chair: Adrian Farrel
     <mailto:Adrain@olddog.co.uk>

     WG Chair: Linda Dunbar
```

```
        <mailto:Linda.duhbar@huawei.com>

        Editor: Susan Hares
        <mailto:shares@ndzh.com>

        Editor: Jaehoon Paul Jeong
        <mailto:pauljeong@skku.edu>

        Editor: Jinyong Tim Kim
        <mailto:wlsdyd0930@nate.com>";

    description
      "This module describes a capability model
      for I2NSF devices.";

    revision "2017-03-12"{
      description "The fourth revision";
      reference
        "draft-xibassnez-i2nsf-capability-00
         draft-hares-i2nsf-capability-data-model-01";
    }

    container sec-ctl-capabilities {
      description
        "sec-ctl-capabilities";
    }



    grouping i2nsf-net-sec-control-caps {
      description
        "i2nsf-net-sec-control-caps";
      container network-security-control {
        description
          "i2nsf-net-sec-control-caps";
        leaf nsc-support {
          type boolean;
          mandatory true;
          description
            "nsc-support";
        }
        list nsc-fcn {
          key "nsc-fcn-name";
          description
            "nsc-fcn";
          leaf nsc-fcn-name {
            type string;
            mandatory true;
```

```
            description
              "nsc-fcn-name";
          }
        }
      }
    }

    grouping i2nsf-con-sec-control-caps {
      description
        "i2nsf-con-sec-control-caps";

      container content-security-control {
        description
          "content-security-control";

        container antivirus {
          description
            "antivirus";

          leaf antivirus-support {
            type boolean;
            mandatory true;
            description
              "antivirus-support";
          }
          list antivirus-fcn-name {
            key "antivirus-fcn-name";
            description
              "antivirus-fcn-name";

            leaf antivirus-fcn-name {
              type string;
              mandatory true;
              description
                "antivirus-fcn-name";
            }
          }
        }

        container ips {
          description
            "ips";

          leaf ips-support {
            type boolean;
            mandatory true;
            description
              "ips-support";
```

```
          }
          list ips-fcn {
            key "ips-fcn-name";
            description
              "ips-fcn";

            leaf ips-fcn-name {
              type string;
              mandatory true;
              description
                "ips-fcn-name";
            }
          }
        }

        container ids {
          description
            "ids";

          leaf ids-support {
            type boolean;
            mandatory true;
            description
              "ids-support";
          }
          list ids-fcn {
            key "ids-fcn-name";
            description
              "ids-fcn";

            leaf ids-fcn-name {
              type string;
              mandatory true;
              description
                "ids-fcn-name";
            }
          }
        }

        container url-filter {
          description
            "url-filter";

          leaf url-filter-support {
            type boolean;
            mandatory true;
            description
              "url-filter-support";
```

```
            }
            list url-filter-fcn {
              key "url-filter-fcn-name";
              description
                "url-filter-fcn";

              leaf url-filter-fcn-name {
                type string;
                mandatory true;
                description
                  "url-filter-fcn-name";
              }
            }
          }

          container data-filter {
            description
              "data-filter";

            leaf data-filter-support {
              type boolean;
              mandatory true;
              description
                "data-filter-support";
            }
            list data-filter-fcn {
              key "data-filter-fcn-name";
              description
                "data-filter-fcn";

              leaf data-filter-fcn-name {
                type string;
                mandatory true;
                description
                  "data-filter-fcn-name";
              }
            }
          }

          container mail-filter {
            description
              "mail-filter";

            leaf mail-filter-support {
              type boolean;
              mandatory true;
              description
                "mail-filter-support";
```

```
          }
          list mail-filter-fcn {
            key "mail-filter-fcn-name";
            description
              "mail-filter-fcn";

            leaf mail-filter-fcn-name {
              type string;
              mandatory true;
              description
                "mail-filter-fcn-name";
            }
          }
        }

        container dns-filter {
          description
            "dns-filter";

          leaf dns-filter-support {
            type boolean;
            mandatory true;
            description
              "dns-filter-support";
          }
          list dns-filter-fcn {
            key "dns-filter-fcn-name";
            description
              "dns-filter-fcn";

            leaf dns-filter-fcn-name {
              type string;
              mandatory true;
              description
                "dns-filter-fcn-name";
            }
          }
        }

        container ftp-filter {
          description
            "ftp-filter";

          leaf ftp-filter-support {
            type boolean;
            mandatory true;
            description
              "ftp-filter-support";
```

```
          }
          list ftp-filter-fcn {
            key "ftp-filter-fcn-name";
            description
              "ftp-filter-fcn";

            leaf ftp-filter-fcn-name {
              type string;
              mandatory true;
              description
                "ftp-filter-fcn-name";
            }
          }
        }

        container games-filter {
          description
            "games-filter";

          leaf games-filter-support {
            type boolean;
            mandatory true;
            description
              "games-filter-support";
          }
          list games-filter-fcn {
            key "games-filter-fcn-name";
            description
              "games-filter-fcn";

            leaf games-filter-fcn-name {
              type string;
              mandatory true;
              description
                "games-filter-fcn-name";
            }
          }
        }

        container p2p-filter {
          description
            "p2p-filter";

          leaf p2p-filter-support {
            type boolean;
            mandatory true;
            description
              "p2p-filter-support";
```

```
          }
          list p2p-filter-fcn {
            key "p2p-filter-fcn-name";
            description
              "p2p-filter-fcn";

            leaf p2p-filter-fcn-name {
              type string;
              mandatory true;
              description
                "p2p-filter-fcn-name";
            }
          }
        }

        container rpc-filter {
          description
            "rpc-filter";

          leaf rpc-filter-support {
            type boolean;
            mandatory true;
            description
              "rpc-filter-support";
          }
          list rpc-filter-fcn {
            key "rpc-filter-fcn-name";
            description
              "rpc-filter-fcn";

            leaf rpc-filter-fcn-name {
              type string;
              mandatory true;
              description
                "rpc-filter-fcn-name";
            }
          }
        }

        container sql-filter {
          description
            "sql-filter";

          leaf sql-filter-support {
            type boolean;
            mandatory true;
            description
              "sql-filter-support";
```

```
          }
          list sql-filter-fcn {
            key "sql-filter-fcn-name";
            description
              "sql-filter-fcn";

            leaf sql-filter-fcn-name {
              type string;
              mandatory true;
              description
                "sql-filter-fcn-name";
            }
          }
        }

        container telent-filter {
          description
            "telent-filter";

          leaf telent-filter-support {
            type boolean;
            mandatory true;
            description
              "telent-filter-support";
          }
          list telent-filter-fcn {
            key "telent-filter-fcn-name";
            description
              "telent-filter-fcn";

            leaf telent-filter-fcn-name {
              type string;
              mandatory true;
              description
                "telent-filter-fcn-name";
            }
          }
        }

        container tftp-filter {
          description
            "tftp-filter";

          leaf tftp-filter-support {
            type boolean;
            mandatory true;
            description
              "tftp-filter-support";
```

```
          }
          list tftp-filter-fcn {
            key "tftp-filter-fcn-name";
            description
              "tftp-filter-fcn";

            leaf tftp-filter-fcn-name {
              type string;
              mandatory true;
              description
                "tftp-filter-fcn-name";
            }
          }
        }

        container file-blocking {
          description
            "file-blocking";

          leaf file-blocking-support {
            type boolean;
            mandatory true;
            description
              "file-blocking-support";
          }
          list file-blocking-fcn {
            key "file-blocking-fcn-name";
            description
              "file-blocking-fcn";

            leaf file-blocking-fcn-name {
              type string;
              mandatory true;
              description
                "file-blocking-fcn-name";
            }
          }
        }

        container file-isolate {
          description
            "file-isolate";

          leaf file-isolate-support {
            type boolean;
            mandatory true;
            description
              "file-isolate-support";
```

```
          }
          list file-isolate-fcn {
            key "file-isolate-fcn-name";
            description
              "file-isolate-fcn";

            leaf file-isolate-fcn-name {
              type string;
              mandatory true;
              description
                "file-isolate-fcn-name";
            }
          }
        }

        container pkt-capture {
          description
            "pkt-capture";

          leaf pkt-capture-support {
            type boolean;
            mandatory true;
            description
              "pkt-capture-support";
          }
          list pkt-capture-fcn {
            key "pkt-capture-fcn-name";
            description
              "pkt-capture-fcn";

            leaf pkt-capture-fcn-name {
              type string;
              mandatory true;
              description
                "pkt-capture-fcn-name";
            }
          }
        }

        container app-control {
          description
            "app-control";

          leaf app-control-support {
            type boolean;
            mandatory true;
            description
              "app-control-support";
```

```
          }
          list app-control-fcn {
            key "app-control-fcn-name";
            description
              "app-control-fcn";

            leaf app-control-fcn-name {
              type string;
              mandatory true;
              description
                "app-control-fcn-name";
            }
          }
        }

        container voip-volte {
          description
            "voip-volte";

          leaf voip-volte-support {
            type boolean;
            mandatory true;
            description
              "voip-volte-support";
          }
          list voip-volte-fcn {
            key "voip-volte-fcn-name";
            description
              "voip-volte-fcn";

            leaf voip-volte-fcn-name {
              type string;
              mandatory true;
              description
                "voip-volte-fcn-name";
            }
          }
        }
      }
    }

    grouping i2nsf-attack-mitigation-control-caps {
      description
        "i2nsf-attack-mitigation-control-caps";

      container attack-mitigation-control {
        description
          "attack-mitigation-control";
```

```
          choice attack-mitigation-control-type {
            description
              "attack-mitigation-control-type";
            case ddos-attack {
              description
                "ddos-attack";
              choice ddos-attack-type {
                description
                  "ddos-attack-type";
                case network-layer-ddos-attack {
                  description
                    "network-layer-ddos-attack";
                  container network-layer-ddos-attack-types {
                    description
                      "network-layer-ddos-attack-type";
                    container syn-flood-attack {
                      description
                        "syn-flood-attack";
                      leaf syn-flood-attack-support {
                        type boolean;
                        mandatory true;
                        description
                          "syn-flood-attack-support";
                      }
                      list syn-flood-fcn {
                        key "syn-flood-fcn-name";
                        description
                          "syn-flood-fcn";
                        leaf syn-flood-fcn-name {
                          type string;
                          mandatory true;
                          description
                            "syn-flood-fcn-name";
                        }
                      }
                    }
                    container udp-flood-attack {
                      description
                        "udp-flood-attack";
                      leaf udp-flood-attack-support {
                        type boolean;
                        mandatory true;
                        description
                          "udp-flood-attack-support";
                      }
                      list udp-flood-fcn {
                        key "udp-flood-fcn-name";
                        description
```

```
          "udp-flood-fcn";
        leaf udp-flood-fcn-name {
          type string;
          mandatory true;
          description
            "udp-flood-fcn-name";
        }
      }
    }
    container icmp-flood-attack {
      description
        "icmp-flood-attack";
      leaf icmp-flood-attack-support {
        type boolean;
        mandatory true;
        description
          "icmp-flood-attack-support";
      }
      list icmp-flood-fcn {
        key "icmp-flood-fcn-name";
        description
          "icmp-flood-fcn";
        leaf icmp-flood-fcn-name {
          type string;
          mandatory true;
          description
            "icmp-flood-fcn-name";
        }
      }
    }
    container ip-fragment-flood-attack {
      description
        "ip-fragment-flood-attack";
      leaf ip-fragment-flood-attack-support {
        type boolean;
        mandatory true;
        description
          "ip-fragment-flood-attack-support";
      }
      list frag-flood-fcn {
        key "ip-frag-flood-fcn-name";
        description
          "frag-flood-fcn";
        leaf ip-frag-flood-fcn-name {
          type string;
          mandatory true;
          description
            "ip-frag-flood-fcn-name";
```

```
                    }
                  }
                }
                container ipv6-related-attack {
                  description
                    "ipv6-related-attack";
                  leaf ipv6-related-attack-support {
                    type boolean;
                    mandatory true;
                    description
                      "ipv6-related-attack-support";
                  }
                  list ipv6-related-fcn {
                    key "ipv6-related-fcn-name";
                    description
                      "ipv6-related-fcn";
                    leaf ipv6-related-fcn-name {
                      type string;
                      mandatory true;
                      description
                        "ipv6-related-fcn-name";
                    }
                  }
                }
              }
            }
            case app-layer-ddos-attack {
              description
                "app-layer-ddos-attack";
              container app-layer-ddos-attack-types {
                description
                  "app-layer-ddos-attack-types";
                container http-flood-attack {
                  description
                    "http-flood-attack";
                  leaf http-flood-attack-support {
                    type boolean;
                    mandatory true;
                    description
                      "http-flood-attack-support";
                  }
                  list http-flood-fcn {
                    key "http-flood-fcn-name";
                    description
                      "http-flood-fcn";
                    leaf http-flood-fcn-name {
                      type string;
                      mandatory true;
```

```
        description
          "http-flood-fcn-name";
      }
    }
  }
  container https-flood-attack {
    description
      "https-flood-attack";
    leaf https-flood-attack-support {
      type boolean;
      mandatory true;
      description
        "https-flood-attack-support";
    }
    list https-flood-fcn {
      key "https-flood-fcn-name";
      description
        "https-flood-fcn";
      leaf https-flood-fcn-name {
        type string;
        mandatory true;
        description
          "https-flood-fcn-name";
      }
    }
  }
  container dns-flood-attack {
    description
      "dns-flood-attack";
    leaf dns-flood-attack-support {
      type boolean;
      mandatory true;
      description
        "dns-flood-attack-support";
    }
    list dns-flood-fcn {
      key "dns-flood-fcn-name";
      description
        "dns-flood-fcn";
      leaf dns-flood-fcn-name {
        type string;
        mandatory true;
        description
          "dns-flood-fcn-name";
      }
    }
  }
  container dns-amp-flood-attack {
```

```
                    description
                      "dns-amp-flood-attack";
                    leaf dns-flood-attack-support {
                      type boolean;
                      mandatory true;
                      description
                        "dns-flood-attack-support";
                    }
                    list dns-amp-flood-fcn {
                      key "dns-amp-flood-fcn-name";
                      description
                        "dns-amp-flood-fcn";
                      leaf dns-amp-flood-fcn-name {
                        type string;
                        mandatory true;
                        description
                          "dns-amp-flood-fcn-name";
                      }
                    }
                  }
                  container ssl-ddos-attack {
                    description
                      "ssl-ddos-attack";
                    leaf ssl-ddos-attack-support {
                      type boolean;
                      mandatory true;
                      description
                        "ssl-ddos-attack-support";
                    }
                    list ssl-ddos-fcn {
                      key "ssl-ddos-fcn-name";
                      description
                        "ssl-ddos-fcn";
                      leaf ssl-ddos-fcn-name {
                        type string;
                        mandatory true;
                        description
                          "ssl-ddos-fcn-name";
                      }
                    }
                  }
                }
              }
            }
          }

          case single-packet-attack {
            description
```

```
              "single-packet-attack";
            choice single-packet-attack-type {
              description
                "single-packet-attack-type";
              case scan-and-sniff-attack {
                description
                  "scan-and-sniff-attack";
                container ip-sweep-attack {
                  description
                    "ip-sweep-attack";
                  leaf ip-sweep-attack-suppor {
                    type boolean;
                    mandatory true;
                    description
                      "ip-sweep-attack-suppor";
                  }
                  list ip-sweep-fcn {
                    key "ip-sweep-fcn-name";
                    description
                      "ip-sweep-fcn";
                    leaf ip-sweep-fcn-name {
                      type string;
                      mandatory true;
                      description
                        "ip-sweep-fcn-name";
                    }
                  }
                }
                container port-scanning-attack {
                  description
                    "port-scanning-attack";
                  leaf port-scanning-attack-support {
                    type boolean;
                    mandatory true;
                    description
                      "port-scanning-attack-support";
                    }
                  list port-scanning-fcn {
                    key "port-scanning-fcn-name";
                    description
                      "port-scanning-fcn";
                    leaf port-scanning-fcn-name {
                      type string;
                      mandatory true;
                      description
                        "port-scanning-fcn-name";
                    }
                  }
```

```
        }
      }
      case malformed-packet-attack {
        description
          "malformed-packet-attack";
        container ping-of-death-attack {
          description
            "ping-of-death-attack";
          leaf ping-of-death-attack-support {
            type boolean;
            mandatory true;
            description
              "ping-of-death-attack-support";
          }
          list ping-of-death-fcn {
            key "ping-of-death-fcn-name";
            description
              "ping-of-death-fcn";
            leaf ping-of-death-fcn-name {
              type string;
              mandatory true;
              description
                "ping-of-death-fcn-name";
            }
          }
        }
        container teardrop-attack {
          description
            "teardrop-attack";
          leaf teardrop-attack-support {
            type boolean;
            mandatory true;
            description
              "teardrop-attack-support";
          }
          list tear-drop-fcn {
            key "tear-drop-fcn-name";
            description
              "tear-drop-fcn";
            leaf tear-drop-fcn-name {
              type string;
              mandatory true;
              description
                "tear-drop-fcn-name";
            }
          }
        }
      }
```

```
            case special-packet-attack {
              description
                "special-packet-attack";
              container oversized-icmp-attack {
                description
                  "oversized-icmp-attack";
                leaf oversized-icmp-attack-support {
                  type boolean;
                  mandatory true;
                  description
                    "oversized-icmp-attack-support";
                }
                list oversized-icmp-fcn {
                  key "oversized-icmp-fcn-name";
                  description
                    "oversized-icmp-fcn";
                  leaf oversized-icmp-fcn-name {
                    type string;
                    mandatory true;
                    description
                      "oversized-icmp-fcn-name";
                  }
                }
              }
              container tracert-attack {
                description
                  "tracert-attack";
                leaf tracert-attack-support {
                  type boolean;
                  mandatory true;
                  description
                    "tracert-attack-support";
                }
                list tracert-fcn {
                  key "tracert-fcn-name";
                  description
                    "tracert-fcn";
                  leaf tracert-fcn-name {
                    type string;
                    mandatory true;
                    description
                      "tracert-fcn-name";
                  }
                }
              }
            }
          }
        }
```

```
        }
      }
    }

    grouping i2nsf-it-resources {
      description
        "i2nsf-it-resource";
      list it-resources {
        key "it-resource-id";
        description
          "it-resource";
        leaf it-resource-id {
          type uint64;
          mandatory true;
          description
            "it-resource-id";
        }
        leaf it-resource-name {
          type string;
          mandatory true;
          description
            "it-resource-name";
        }
      }
    }

    container nsf-capabilities {
      description
        "nsf-capabilities";

      list nsf {
        key "nsf-name";
        description
          "nsf";
        leaf nsf-name {
          type string;
          mandatory true;
          description
            "nsf-name";
        }
        container nsf-address {
          description
            "nsf-address";
          choice nsf-address-type {
            description
              "nsf address type: ipv4 and ipv4";
            case ipv4-address {
              description
```

```
                "ipv4 case";
              leaf ipv4-address {
                type inet:ipv4-address;
                mandatory true;
                description
                  "nsf address type is ipv4";
              }
            }
            case ipv6-address {
              description
                "ipv6 case";
              leaf ipv6-address {
                type inet:ipv6-address;
                mandatory true;
                description
                  "nsf address type is ipv6";
              }
            }
          }
        }

        container net-sec-control-capabilities {
          uses i2nsf-net-sec-control-caps;
          description
            "net-sec-control-capabilities";
        }
        container con-sec-control-capabilities {
          uses i2nsf-con-sec-control-caps;
          description
            "con-sec-control-capabilities";
        }
        container attack-mitigation-capabilities {
          uses i2nsf-attack-mitigation-control-caps;
          description
            "attack-mitigation-capabilities";
        }
        container it-resource {
          uses i2nsf-it-resources;
          description
            "it-resource";
        }
      }
    }
  }
```

<CODE ENDS>

Figure 6: Data Model of I2NSF Capability Interface

6. IANA Considerations

No IANA considerations exist for this document at this time. URL will be added.

7. Security Considerations

This document introduces no additional security threats and SHOULD follow the security requirements as stated in [i2nsf-framework].

8. Acknowledgements

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.R-20160222-002755, Cloud based Security Intelligence Technology Development for the Customized Security Service Provisioning).

This document has greatly benefited from inputs by Daeyoung Hyun, Hyoungshick Kim, Jung-Soo Park, Tae-Jin Ahn, and Se-Hui Lee.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC6020] Bjorklund, M., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, October 2010.

9.2. Informative References

[i2nsf-cap-im] Xia, L., Strassner, J., Zhang, D., Li, K., Basile, C., Lioy, A., Lopez, D., Lopez, E., BOUTHORS, N., and L. Fang, "Information Model of NSFs Capabilities", draft-xibassnez-i2nsf-capability-00 (work in progress), Novemver 2016.

[i2nsf-problem-statement] Hares, S., Lopez, D., Zarny, M., Jacquenet, C., Kumar, R., and J. Jeong, "I2NSF Problem Statement and Use cases",

draft-ietf-i2nsf-problem-and-use-cases-11 (work in progress), March 2017.

[i2nsf-terminology] Hares, S., Strassner, J., Lopez, D., Xia, L., and H. Birkholz, "Interface to Network Security Functions (I2NSF) Terminology", draft-ietf-i2nsf-terminology-03 (work in progress), March 2017.

[i2rs-rib-data-model] Wang, L., Ananthakrishnan, H., Chen, M., Dass, A., Kini, S., and N. Bahadur, "A YANG Data Model for Routing Information Base (RIB)", draft-ietf-i2rs-rib-data-model-07 (work in progress), January 2017.

[supa-policy-info-model] Strassner, J., Halpern, J., and S. Meer, "Generic Policy Information Model for Simplified Use of Policy Abstractions (SUPA)", draft-ietf-supa-generic-policy-info-model-02 (work in progress), January 2017.

[i2nsf-framework] Lopez, D., Lopez, E., Dunbar, L., Strassner, J., and R. Kumar, "Framework for Interface to Network Security Functions", draft-ietf-i2nsf-framework-04 (work in progress), October 2016.

Appendix A. Changes from draft-hares-i2nsf-capability-data-model-00

The following changes are made from draft-hares-i2nsf-capability-data-model-00:

- IPv6 is supported for the addresses of NSF devices.
- Content Security Control is supported for various content-based security services, such as dns-filter, ftp-filter, games-filter, p2p-filter, rpc-filter, sql-filter, telnet-filter, and tftp-filter.

Authors' Addresses

Susan Hares
Huawei
7453 Hickory Hill
Saline, MI 48176
USA

Phone: +1-734-604-0332
EMail: shares@ndzh.com

Robert Moskowitz
HTT Consulting
Oak Park, MI
USA

Phone: +1-248-968-9809
EMail: rgm@htt-consult.com

Liang Xia (Frank)
Huawei
101 Software Avenue, Yuhuatai District
Nanjing, Jiangsu
China

Phone:
EMail: Frank.xialiang@huawei.com

Jaehoon Paul Jeong
Department of Software
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 16419
Republic of Korea

Phone: +82 31 299 4957
Fax: +82 31 290 7996
EMail: pauljeong@skku.edu
URI: http://iotlab.skku.edu/people-jaehoon-jeong.php

Jinyong Tim Kim
Department of Computer Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 16419
Republic of Korea

Phone: +82 10 8273 0930
EMail: wlsdyd0930@nate.com