I2NSF Capability YANG Data Model
(draft-hares-i2nsf-capability-data-model-00)

@IETF-97 I2NSF WG
November 14, 2016

Susan hares, R. Moskowitz, L. xia,
J. Kim, and J. Jeong.

Introduction

- This draft introduces a YANG data model for capabilities per NSF devices, controller, or application.

- This draft is an updated version from draft-hare-i2nsf-capability-yang-01.

- This version focuses on registering network security functions (NSFs).
- Long message on next steps
  - https://www.ietf.org/mail-archive/web/i2nsf/current/msg01344.html

Good Changes

- Split between capability and NSF interface model
  - draft-kim-i2nsf-consumer-facing-interface-dm-00
  - Registration concepts
- Need to do this for client side
  - Group policy needs to be added
    - Type 1: Grouping of names
    - Type 2: Group Policy (draft-you-i2nsf-user-group-policy-capability)

Problematic

- The link between I2NSF Capabilities and Flow Policy has been broken
  - Choice 1: Stay with simple
  - Choice 2: Go back to draft-hares-pkt-eca-policy
  - Choice 3: Add choices (Best)
    - Simple – what is in the model
    - I2RS filter level – draft-hares-pkt-eca-policy
- Need feedback

Overall High Level YANG Module

- This is an overall high-level YANG module for capabilities per NSF devices, controller, or application.

```
module : ietf-i2nsf-capability
  +--rw sec-ctl-capabilities
  +--rw nsf-capabilities
    +--rw nsf* [nsf-name]
      +--rw nsf-name  string
      +--rw nsf-address  inet:ipv4-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

Security Controller Capabilities

- sec-ctl-capabilities
  - This component is high-level YANG for capabilities per Security Controller.
  - This component can manage NSFs through scalability, load balancing and etc.
  - These sec-ctl-capabilities will be defined later.

```
module : ietf-i2nsf-capability
  +--rw sec-ctl-capabilities
  +--rw nsf-capabilities
    +--rw nsf* [nsf-name]
      +--rw nsf-name  string
      +--rw nsf-address  inet:ipv4-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

NSF Capabilities

- nsf-capabilities
  - This component is a high-level YANG for capabilities per NSF devices.
  - This component can register NSFs with the name, address, and types of NSFs, and also IT resources.

```
module : ietf-i2nsf-capability
  +--rw sec-ctl-capabilities
  +--rw nsf-capabilities
    +--rw nsf* [nsf-name]
      +--rw nsf-name  string
      +--rw nsf-address  inet:ipv4-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

NSF Capabilities

- i2nsf-net-sec-control-caps
  - This component is a high-level YANG for network security control.
    - nsc-support.
    - nsc-fcn.
      - nsc-fcn-name.

```
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
```

NSF Capabilities

- i2nsf-con-sec-control-caps
  - This component is a high-level YANG for network security content.
    - csc-support.
    - csc-fcn.
      - csc-fcn-name.

```
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
```

NSF Capabilities

- i2nsf-net-sec-control-caps
  - This component is a high-level YANG for attack mitigation control.
    - amc-support.
    - amc-fcn.
      - amc-fcn-name.

```
+--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]
```

IT Resources

- i2nsf-net-sec-control-caps
  - This component is A high-level YANG for IT resources.
    - amc-support.
    - amc-fcn.
      - amc-fcn-name.

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

Next Steps

- Construction of YANG data models for capability per security controller.

- We will implement and test this data YANG model for capabilities to prove its validity.