I2NSF Network Security Functions-Facing Interface YANG Data Model

(draft-kim-i2nsf-nsf-facing-interface-data-model-02)

IETF 99, Prague, Czech

July 18, 2017

Jinyoung Tim Kim, Jaehoon Paul Jeong,
Jung-Soo Park, Susan Hares, Liang Xia

Introduction

- This draft is an updated version from draft-kim-i2nsf-nsf-facing-interface-data-model-01.
- This draft defines a YANG data model corresponding to the information model for NSF-Facing Interface.
- We refer to draft-xibassnz-i2nsf-capability-01.
- We verified our YANG data model through a prototype in IETF-99 Hackathon Project.

Difference Between NSF-Facing and Capability YANG Data Model

- NSF-Facing YANG Data Model: NSF-Facing Interface YANG Data Model is used to configure the rules of a policy into NSFs.

- Capability YANG Data Model: Capability YANG Data Model is used to retrieve capability information of an NSF.

Updates from -01 Version

- Modification of Event Component.
  - Usr-sec-event-format
  - Usr-sec-event-type
  - Dev-sec-event-format
  - Dev-sec-event-type
  - Dev-sec-event-type-severity
  - Sys-sec-event-format
  - Sys-sec-event-type

- Modification of Action Component.
  - Ingress Action
  - Egress Action
  - Apply Profile Action

- Minor Error Modification.

Modification of Event Component

```
leaf usr-sec-event-type {
  type uint8;
  mandatory true;
  description
   "This is a mandatory uint 8 enumerated integer, which
    is used to specify the type of Event that involves
    this user. The content and format are specified in
    the usrSecEventContent and usrSecEventFormat class
    attributes, respectively. An example of the
    usrSecEventContent attribute is string hrAdmin,
    with the usrSecEventFormat attribute set to 1 (GUID)
    and the usrSecEventType attribute set to 5
   (new logon).";
}
```

```
leaf usr-sec-event-type {
  type enumeration {
      enum unknown {
          description
            "If usrSecEventType is unknown";
      }
      enum user-created {
          description
            "If usrSecEventType is new user created";
      }
      enum user-grp-created {
          description
            "If usrSecEventType is new user group created";
      }
      enum user-deleted {
          description
            "If usrSecEventType is user deleted";
      }
      enum user-grp-deleted {
          description
            "If usrSecEventType is user group deleted";
      }
      enum user-logon {
          description
            "If usrSecEventType is user logon";
      }
      enum user-logoff {
          description
            "If usrSecEventType is user logoff";
      }
      enum user-access-request {
          description
            "If usrSecEventType is user access request";
      }
      enum user-access-granted {
          description
            "If usrSecEventType is user granted";
      }
      enum user-access-violation {
          description
            "If usrSecEventType is user violation";
      }
  }
```

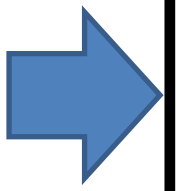
Modification of Action Component (1/2)

```
choice ingress-action-type {
  description
    "Ingress action type: permit, deny, and mirror.";
  case pass {
    description
      "Pass case.";
    leaf pass {
      type boolean;
      mandatory true;
      description
        "Packet flow is passed.";
    }
  }
  case drop {
    description
      "Drop case.";
    leaf drop {
      type boolean;
      mandatory true;
      description
        "Packet flow is droped.";
    }
  }
  case reject {
    description
      "Reject case.";
    leaf reject {
      type boolean;
      mandatory true;
      description
        "Packet flow is rejected.";
    }
  }
  case alert {
    description
      "Alert case.";
    leaf alert {
      type boolean;
      mandatory true;
      description
        "Packet flow is alerted.";
    }
  }
```

```
typedef ingress-action {
    type enumeration {
      enum pass {
          description
            "If ingress action is pass";
      }
      enum drop {
          description
            "If ingress action is drop";
      }
      enum reject {
          description
            "If ingress action is reject";
      }
      enum alert {
          description
            "If ingress action is alert";
      }
      enum mirror {
          description
            "If ingress action is mirror";
      }
    }
    description
      "This is used for ingress action.";
}
```

Modification of Action Component (2/2)

```
+--: (apply-profile-action)
   +--rw (apply-profile-action-type)?
     +--: (content-security-control)
      |  +--rw content-security-control-types
      |     +--rw antivirus
      |     | +--rw antivirus-insp?  boolean
      |     +--rw ips
      |     | +--rw ips-insp?  boolean
      |     +--rw ids
      |     |  +--rw ids-insp?  boolean
      |     +--rw url-filtering
      |     |  +--rw url-filtering-insp?  boolean
      |     +--rw data-filtering
      |     |  +--rw data-filtering-insp?  boolean
      |     +--rw mail-filtering
      |     |  +--rw mail-filtering-insp?  boolean
      |     +--rw file-blocking
      |     |  +--rw file-blocking-insp?  boolean
      |     +--rw file-isolate
      |     |  +--rw file-isolate-insp?  boolean
      |     +--rw pkt-capture
      |     |  +--rw pkt-capture-insp?  boolean
      |     +--rw application-control
      |     |  +--rw application-control-insp?  boolean
      |     +--rw voip-volte
      |        +--rw voip-volte-insp? boolean
```



```
+--:(apply-profile-action)
   +--rw (apply-profile-action-type)?
      +--:(content-security-control)
      |  +--rw content-security-control-types
      |     +--rw antivirus-insp?              boolean
      |     +--rw ips-insp?                    boolean
      |     +--rw ids-insp?                    boolean
      |     +--rw url-filtering-insp?          boolean
      |     +--rw data-filtering-insp?         boolean
      |     +--rw mail-filtering-insp?         boolean
      |     +--rw file-blocking-insp?          boolean
      |     +--rw file-isolate-insp?           boolean
      |     +--rw pkt-capture-insp?            boolean
      |     +--rw application-control-insp?    boolean
      |     +--rw voip-volte-insp?             boolean
```

Next Steps

- We will add YANG data models for content security and attack mitigation.

- We will verify the YANG data models by implementing a prototype by IETF-100 Hackathon.