YANG Data Model of Interface to Network Security Functions Capability Interface
(draft-jeong-i2nsf-capability-interface-yang-02)

Jaehoon Paul Jeong, J. Kim, D. Hyun, J. Park, and T. Ahn

IETF 96, Berlin, Germany
July 21, 2016
Contents

I Introduction

II Generic Model Structure

III YANG Data Model

IV Next Steps
This document defines a YANF data model corresponding to the information model for I2NSF capability interface (i.e., NSF facing interface).

It describes a data model for three security capabilities (i.e., network security functions).
- Network security control
- Content security control
- Attack mitigation control

It covers three use cases:
- **Firewall** for Network security control
- **VoIP/VoLTE** for Content security control
- **DDoS attack** for Attack mitigation control
Generic Data Model of VoIP/VoLTE

```plaintext
++--: (voip-volte)
    ++--rw voip-volte-rule *[voip-volte-rule-id]
        ++--rw voip-volte-rule-id uint 8
        ++--rw event
            | ++--rw called-voip boolean
            | ++--rw called-volte boolean
        ++--rw condition
            | ++--rw sip-header? *[sip-header-uri]
            |     | ++--rw sip-header-uri string
            |     | ++--rw sip-header-method string
            |     | ++--rw expire-time yang:date-and-time
            |     | ++--rw sip-header-user-agent uint32
            | ++--rw cell-region? *[cell-id-region]
            |     | ++--rw cell-id-region uint 32
        ++--rw action
            | ++--rw (action-type)?
                ++--: (ingress-action)
                | ++--rw (ingress-action-type)?
                |     | ++--: (permit)
                |     |     | ++--rw permit boolean
                |     | ++--: (deny)
                |     |     | ++--rw deny boolean
                |     | ++--: (mirror)
                |     |     | ++--rw mirror boolean
                ++--: (egress-action)
                | ++--rw (egress-action-type)?
                |     | ++--: (redirection)
                |     |     | ++--rw redirection? boolean
```

<Figure 1. Generic Model of VoIP/VoLTE>
YANG Data Model


- We refer to the RFC 6020 for YANG.

- The YANG data model is based on the information model of network security functions, as defined in the [draft-xia-i2nsf-capability-interface-im-05].

- The YANG data model is made of the information model, as shown in Figure 1.
case voip-volte {
  list voip-volte-rule {
    key "voip-volte-rule-id";
    description
    "For the VoIP/VoLTE security system, a VoIP/VoLTE security system can monitor each VoIP/VoLTE flow and manage VoIP/VoLTE security rules controlled by a centralized server for VoIP/VoLTE security service (called VoIP IPS). The VoIP/VoLTE security system controls each switch for the VoIP/VoLTE call flow management by manipulating the rules that can be added, deleted, or modified dynamically."
    leaf voip-volte-rule-id {
      type uint8;
      mandatory true;
      description
      "The ID of the voip-volte-rule. This is the key for voip-volte-rule-list. This must be unique."
    }
  }
}
container event {
    description
    "Event types: VoIP and VoLTE.";
    leaf called-voip {
        type boolean;
        mandatory true;
        description
        "If content-security-control-type is voip.";
    }
    leaf called-volte {
        type boolean;
        mandatory true;
        description
        "If content-security-control-type is volte.";
    }
}
container condition {
    description "TBD."
    list sip-header {
        key "sip-header-uri";
        description "TBD."
        leaf sip-header-uri {
            type string;
            mandatory true;
            description "SIP header URI."
        }
        leaf sip-header-method {
            type string;
            mandatory true;
            description "SIP header method."
        }
        leaf sip-header-expire-time {
            type yang:date-and-time;
            mandatory true;
            description "SIP header expire time."
        }
    }
    list cell-region {
        key "cell-id-region";
        description "TBD."
        leaf cell-id-region {
            type uint32;
            mandatory true;
            description "Cell region."
        }
    }
}

leaf sip-header-user-agent {
    type uint32;
    mandatory true;
    description "SIP header user agent."
}

<Figure 5. YANG Data Model of NSF Facing Interface for VoIP/VoLTE>
Data Model of VoIP/VoLTE (4/4)

```yang
container action {
    description
    "The flow-based NSFs realize the security functions by executing various Actions.";
    choice action-type {
        description
        "Action type: ingress action and egress action.";
        case ingress-action {
            description
            "The ingress actions consist of permit, deny, and mirror.";
            choice ingress-action-type {
                description
                "Ingress-action-type: permit, deny, and mirror.";
                case permit {
                    description
                    "Permit case.";
                    leaf permit {
                        type boolean;
                        mandatory true;
                        description
                        "Packet flow is permitted.";
                    }
                }
                case deny {
                    description
                    "Deny case.";
                }
            }
            case egress-action {
                leaf permit {
                    type boolean;
                    mandatory true;
                    description
                    "Packet flow is permitted.";
                }
                leaf redirection {
                    type boolean;
                    mandatory true;
                    description "TBD.";
                }
            }
        }
    }
    case mirror {
        description
        "Mirror case.";
        leaf mirror {
            type boolean;
            mandatory true;
            description
            "Packet flow is mirrored.";
        }
    }
}
```

*Figure 6. YANG Data Model of NSF Facing Interface for VoIP/VoLTE*
Next Steps

- Susan’s Draft and Jeong’s Draft will be merged for the YANG data model for the updated information model for NSF facing interface:
  - draft-xia-i2nsf-capability-interface-im-06

- Implementation
  - We will develop NSF facing interface using the merged YANG data model.
  - We will prepare for I2NSF Hackathon using the YANG data model in IETF96 Seoul Meeting in November, 2016.