

I2NSF Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: September 9, 2021

J. Kim, Ed.  
J. Jeong, Ed.  
Sungkyunkwan University  
J. Park  
ETRI  
S. Hares  
Q. Lin  
Huawei  
March 8, 2021

I2NSF Network Security Function-Facing Interface YANG Data Model  
draft-ietf-i2nsf-nsf-facing-interface-dm-12

## Abstract

This document defines a YANG data model for configuring security policy rules on Network Security Functions (NSF) in the Interface to Network Security Functions (I2NSF) framework. The YANG data model in this document corresponds to the information model for NSF-Facing Interface in the I2NSF framework.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 9, 2021.

## Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents

carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Terminology . . . . .	3
3. YANG Tree Diagram . . . . .	3
3.1. General I2NSF Security Policy Rule . . . . .	3
3.2. Event Clause . . . . .	5
3.3. Condition Clause . . . . .	6
3.4. Action Clause . . . . .	12
4. YANG Data Model of NSF-Facing Interface . . . . .	13
4.1. YANG Module of NSF-Facing Interface . . . . .	14
5. XML Configuration Examples of Low-Level Security Policy Rules	85
5.1. Security Requirement 1: Block Social Networking Service (SNS) Access during Business Hours . . . . .	85
5.2. Security Requirement 2: Block Malicious VoIP/VoLTE Packets Coming to a Company . . . . .	89
5.3. Security Requirement 3: Mitigate HTTP and HTTPS Flood Attacks on a Company Web Server . . . . .	92
6. IANA Considerations . . . . .	95
7. Security Considerations . . . . .	95
8. Acknowledgments . . . . .	96
9. Contributors . . . . .	97
10. References . . . . .	98
10.1. Normative References . . . . .	98
10.2. Informative References . . . . .	101
Authors' Addresses . . . . .	101

## 1. Introduction

This document defines a YANG [RFC6020][RFC7950] data model for security policy rule configuration of Network Security Functions (NSF). The YANG data model in this document is based on the information model in [I-D.ietf-i2nsf-capability-data-model] for the NSF-Facing Interface in the Interface to Network Security Functions (I2NSF) architecture [RFC8329]. The YANG data model in this document focuses on security policy configuration for generic network security functions (e.g., firewall, web filter, and Distributed-Denial-of-Service (DDoS) attack mitigator) [I-D.ietf-i2nsf-capability-data-model]. Security policy configuration for advanced network security functions is out of the scope of this document, such as Intrusion Prevention System (IPS) and anti-virus [I-D.ietf-i2nsf-capability-data-model].

This YANG data model uses an "Event-Condition-Action" (ECA) policy model that is used as the basis for the design of I2NSF Policy described in [RFC8329] and [I-D.ietf-i2nsf-capability-data-model].

The "ietf-i2nsf-policy-rule-for-nsf" YANG module defined in this document provides the configuration of the following features.

- o A general security policy rule of a generic network security function.
- o An event clause of a generic network security function.
- o A condition clause of a generic network security function.
- o An action clause of a generic network security function.

## 2. Terminology

This document uses the terminology described in [RFC8329].

This document follows the guidelines of [RFC8407], uses the common YANG types defined in [RFC6991], and adopts the Network Management Datastore Architecture (NMDA). The meaning of the symbols in tree diagrams is defined in [RFC8340].

## 3. YANG Tree Diagram

This section shows a YANG tree diagram of generic network security functions. Advanced network security functions can be defined in future. Advanced network security functions is out of the scope of this document can be defined in future, such as Intrusion Prevention System (IPS), Distributed-Denial-of-Service (DDoS) attack mitigator, and anti-virus [I-D.ietf-i2nsf-capability-data-model].

### 3.1. General I2NSF Security Policy Rule

This section shows a YANG tree diagram for a general I2NSF security policy rule for generic network security functions.

```

module: ietf-i2nsf-policy-rule-for-nsf
  +--rw i2nsf-security-policy
    +--rw system-policy* [system-policy-name]
      +--rw system-policy-name      string
      +--rw priority-usage?         identityref
      +--rw resolution-strategy?    identityref
      +--rw default-action?         identityref
      +--rw rules* [rule-name]
        +--rw rule-name              string
        +--rw rule-description?     string
        +--rw rule-priority?        uint8
        +--rw rule-enable?          boolean
        +--rw rule-session-aging-time? uint16
        +--rw rule-long-connection
          +--rw enable?             boolean
          +--rw duration?           uint16
        +--rw time-intervals
          +--rw absolute-time-interval
            +--rw start-time?       start-time-type
            +--rw end-time?         end-time-type
          +--rw periodic-time-interval
            +--rw day
              +--rw every-day?      boolean
              +--rw specific-day*   day-type
            +--rw month
              +--rw every-month?    boolean
              +--rw specific-month* month-type
        +--rw event-clause-container
          ...
        +--rw condition-clause-container
          ...
        +--rw action-clause-container
          ...
      +--rw rule-group
        +--rw groups* [group-name]
          +--rw group-name          string
          +--rw rule-range
            +--rw start-rule?       string
            +--rw end-rule?         string
          +--rw enable?             boolean
          +--rw description?        string

```

Figure 1: YANG Tree Diagram for Network Security Policy

The system policy provides for multiple system policies in one NSF, and each system policy is used by one virtual instance of the NSF/device. The system policy includes system policy name, priority usage, resolution strategy, default action, and rules.

A resolution strategy is used to decide how to resolve conflicts that occur between the actions of the same or different policy rules that are matched and contained in a particular NSF. The resolution strategy is defined as First Matching Rule (FMR), Last Matching Rule (LMR), Prioritized Matching Rule (PMR) with Errors (PMRE), and Prioritized Matching Rule with No Errors (PMRN). The resolution strategy can be extended according to specific vendor action features. The resolution strategy is described in detail in [I-D.ietf-i2nsf-capability-data-model].

A default action is used to execute I2NSF policy rule when no rule matches a packet. The default action is defined as pass, drop, reject, alert, and mirror. The default action can be extended according to specific vendor action features. The default action is described in detail in [I-D.ietf-i2nsf-capability-data-model].

The rules include rule name, rule description, rule priority, rule enable, time zone, event clause container, condition clause container, and action clause container.

### 3.2. Event Clause

This section shows a YANG tree diagram for an event clause for a general I2NSF security policy rule for generic network security functions.

```

module: ietf-i2nsf-policy-rule-for-nsf
  +--rw i2nsf-security-policy
    +--rw system-policy* [system-policy-name]
      ...
    +--rw rules* [rule-name]
      |
      | ...
      | +--rw event-clause-container
      | | +--rw event-clause-description? string
      | | +--rw event-clauses
      | |   +--rw system-event* identityref
      | |   +--rw system-alarm* identityref
      | | +--rw condition-clause-container
      | | | ...
      | | +--rw action-clause-container
      | | | ...
      | +--rw rule-group
      | ...

```

Figure 2: YANG Tree Diagram for an Event Clause

An event clause is any important occurrence at a specific time of a change in the system being managed, and/or in the environment of the

system being managed. An event clause is used to trigger the evaluation of the condition clause of the I2NSF Policy Rule. The event clause is defined as a system event and system alarm [I-D.ietf-i2nsf-nsf-monitoring-data-model]. The event clause can be extended according to specific vendor event features. The event clause is described in detail in [I-D.ietf-i2nsf-capability-data-model].

### 3.3. Condition Clause

This section shows a YANG tree diagram for a condition clause for a general I2NSF security policy rule for generic network security functions.

```

module: ietf-i2nsf-policy-rule-for-nsf
+--rw i2nsf-security-policy
  ...
  +--rw rules* [rule-name]
    |
    | ...
    | +--rw event-clause-container
    | |
    | | ...
    | +--rw condition-clause-container
    | |
    | | +--rw condition-clause-description?                string
    | | +--rw packet-security-ipv4-condition
    | | |
    | | | +--rw ipv4-description?                        string
    | | | +--rw pkt-sec-ipv4-header-length
    | | | |
    | | | | +--rw (match-type)?
    | | | | |
    | | | | | +--:(exact-match)
    | | | | | |
    | | | | | | +--rw ipv4-header-length*                uint8
    | | | | | | +--:(range-match)
    | | | | | | +--rw range-ipv4-header-length*
    | | | | [start-ipv4-header-length end-ipv4-header-length]
    | | | | |
    | | | | | +--rw start-ipv4-header-length            uint8
    | | | | | +--rw end-ipv4-header-length              uint8
    | | | +--rw pkt-sec-ipv4-tos*                        identityref
    | | | +--rw pkt-sec-ipv4-total-length
    | | | |
    | | | | +--rw (match-type)?
    | | | | |
    | | | | | +--:(exact-match)
    | | | | | |
    | | | | | | +--rw ipv4-total-length*                  uint16
    | | | | | | +--:(range-match)
    | | | | | | +--rw range-ipv4-total-length*
    | | | | [start-ipv4-total-length end-ipv4-total-length]
    | | | | |
    | | | | | +--rw start-ipv4-total-length              uint16
    | | | | | +--rw end-ipv4-total-length                uint16
    | | | +--rw pkt-sec-ipv4-id*                          uint16
    | | | +--rw pkt-sec-ipv4-fragment-flags*              identityref
    | | | +--rw pkt-sec-ipv4-fragment-offset
    | | | |
    | | | | +--rw (match-type)?
  
```

```

| | | | | +---:(exact-match)
| | | | | | +---rw ipv4-fragment-offset*          uint16
| | | | | +---:(range-match)
| | | | | | +---rw range-ipv4-fragment-offset*
[start-ipv4-fragment-offset end-ipv4-fragment-offset]
| | | | | | +---rw start-ipv4-fragment-offset      uint16
| | | | | | +---rw end-ipv4-fragment-offset        uint16
| | | | | +---rw pkt-sec-ipv4-ttl
| | | | | | +---rw (match-type)?
| | | | | | +---:(exact-match)
| | | | | | | +---rw ipv4-ttl*          uint8
| | | | | | +---:(range-match)
| | | | | | | +---rw range-ipv4-ttl*
[start-ipv4-ttl end-ipv4-ttl]
| | | | | | +---rw start-ipv4-ttl      uint8
| | | | | | +---rw end-ipv4-ttl        uint8
| | | | | +---rw pkt-sec-ipv4-protocol*  identityref
| | | | | +---rw pkt-sec-ipv4-src
| | | | | | +---rw (match-type)?
| | | | | | +---:(exact-match)
| | | | | | | +---rw ipv4-address* [ipv4]
| | | | | | | +---rw ipv4              inet:ipv4-address
| | | | | | | +---rw (subnet)?
| | | | | | | +---:(prefix-length)
| | | | | | | | +---rw prefix-length?  uint8
| | | | | | | +---:(netmask)
| | | | | | | | +---rw netmask?        yang:dotted-quad
| | | | | | +---:(range-match)
| | | | | | | +---rw range-ipv4-address*
[start-ipv4-address end-ipv4-address]
| | | | | | +---rw start-ipv4-address  inet:ipv4-address
| | | | | | +---rw end-ipv4-address    inet:ipv4-address
| | | | | +---rw pkt-sec-ipv4-dest
| | | | | | +---rw (match-type)?
| | | | | | +---:(exact-match)
| | | | | | | +---rw ipv4-address* [ipv4]
| | | | | | | +---rw ipv4              inet:ipv4-address
| | | | | | | +---rw (subnet)?
| | | | | | | +---:(prefix-length)
| | | | | | | | +---rw prefix-length?  uint8
| | | | | | | +---:(netmask)
| | | | | | | | +---rw netmask?        yang:dotted-quad
| | | | | | +---:(range-match)
| | | | | | | +---rw range-ipv4-address*
[start-ipv4-address end-ipv4-address]
| | | | | | +---rw start-ipv4-address  inet:ipv4-address
| | | | | | +---rw end-ipv4-address    inet:ipv4-address
| | | | | +---rw pkt-sec-ipv4-ipopts*  identityref

```

```

| | | +--rw pkt-sec-ipv4-same-ip?          boolean
| | | +--rw pkt-sec-ipv4-geo-ip*          string
| | | +--rw packet-security-ipv6-condition
| | |   +--rw ipv6-description?          string
| | |   +--rw pkt-sec-ipv6-traffic-class* identityref
| | |   +--rw pkt-sec-ipv6-flow-label
| | |     +--rw (match-type)?
| | |       +--:(exact-match)
| | |       | +--rw ipv6-flow-label*      uint32
| | |       +--:(range-match)
| | |       +--rw range-ipv6-flow-label*
| | | [start-ipv6-flow-label end-ipv6-flow-label]
| | |   +--rw start-ipv6-flow-label      uint32
| | |   +--rw end-ipv6-flow-label        uint32
| | |   +--rw pkt-sec-ipv6-payload-length
| | |     +--rw (match-type)?
| | |       +--:(exact-match)
| | |       | +--rw ipv6-payload-length*  uint16
| | |       +--:(range-match)
| | |       +--rw range-ipv6-payload-length*
| | | [start-ipv6-payload-length end-ipv6-payload-length]
| | |   +--rw start-ipv6-payload-length  uint16
| | |   +--rw end-ipv6-payload-length    uint16
| | |   +--rw pkt-sec-ipv6-next-header*  identityref
| | |   +--rw pkt-sec-ipv6-hop-limit
| | |     +--rw (match-type)?
| | |       +--:(exact-match)
| | |       | +--rw ipv6-hop-limit*      uint8
| | |       +--:(range-match)
| | |       +--rw range-ipv6-hop-limit*
| | | [start-ipv6-hop-limit end-ipv6-hop-limit]
| | |   +--rw start-ipv6-hop-limit        uint8
| | |   +--rw end-ipv6-hop-limit          uint8
| | |   +--rw pkt-sec-ipv6-src
| | |     +--rw (match-type)?
| | |       +--:(exact-match)
| | |       | +--rw ipv6-address* [ipv6]
| | |       |   +--rw ipv6             inet:ipv6-address
| | |       |   +--rw prefix-length?   uint8
| | |       +--:(range-match)
| | |       +--rw range-ipv6-address*
| | | [start-ipv6-address end-ipv6-address]
| | |   +--rw start-ipv6-address          inet:ipv6-address
| | |   +--rw end-ipv6-address            inet:ipv6-address
| | |   +--rw pkt-sec-ipv6-dest
| | |     +--rw (match-type)?
| | |       +--:(exact-match)
| | |       | +--rw ipv6-address* [ipv6]

```



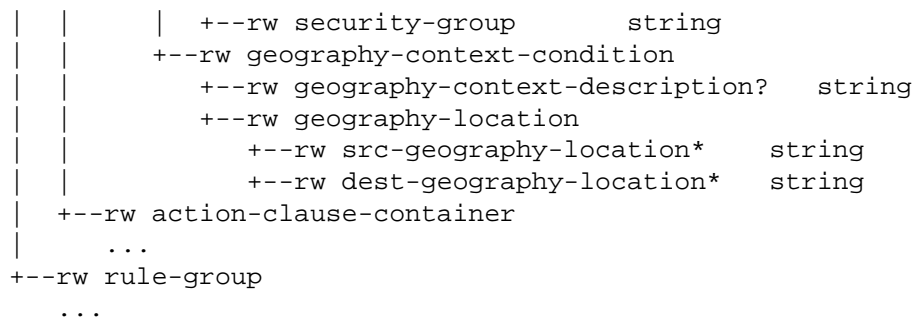
```

| | | | | +--rw ipv6 inet:ipv6-address
| | | | | +--rw prefix-length? uint8
| | | | | +---:(range-match)
| | | | | +--rw range-ipv6-address*
[start-ipv6-address end-ipv6-address]
| | | | | +--rw start-ipv6-address inet:ipv6-address
| | | | | +--rw end-ipv6-address inet:ipv6-address
+--rw packet-security-tcp-condition
| +--rw tcp-description? string
| +--rw pkt-sec-tcp-src-port-num
| | +--rw (match-type)?
| | +---:(exact-match)
| | | +--rw port-num* inet:port-number
| | +---:(range-match)
| | +--rw range-port-num*
[start-port-num end-port-num]
| | | +--rw start-port-num inet:port-number
| | | +--rw end-port-num inet:port-number
+--rw pkt-sec-tcp-dest-port-num
| +--rw (match-type)?
| +---:(exact-match)
| | +--rw port-num* inet:port-number
| +---:(range-match)
| +--rw range-port-num*
[start-port-num end-port-num]
| | | +--rw start-port-num inet:port-number
| | | +--rw end-port-num inet:port-number
+--rw pkt-sec-tcp-flags* identityref
+--rw packet-security-udp-condition
| +--rw udp-description? string
| +--rw pkt-sec-udp-src-port-num
| | +--rw (match-type)?
| | +---:(exact-match)
| | | +--rw port-num* inet:port-number
| | +---:(range-match)
| | +--rw range-port-num*
[start-port-num end-port-num]
| | | +--rw start-port-num inet:port-number
| | | +--rw end-port-num inet:port-number
+--rw pkt-sec-udp-dest-port-num
| +--rw (match-type)?
| +---:(exact-match)
| | +--rw port-num* inet:port-number
| +---:(range-match)
| +--rw range-port-num*
[start-port-num end-port-num]
| | | +--rw start-port-num inet:port-number
| | | +--rw end-port-num inet:port-number

```



```
[start-port-num end-port-num]
    +--rw start-port-num      inet:port-number
    +--rw end-port-num        inet:port-number
    +--rw pkt-sec-dccp-service-code*  uint32
+--rw packet-security-icmp-condition
    +--rw icmp-description?      string
    +--rw pkt-sec-icmp-type-and-code*  identityref
+--rw packet-security-url-category-condition
    +--rw url-category-description?  string
    +--rw pre-defined-category*      string
    +--rw user-defined-category*     string
+--rw packet-security-voice-condition
    +--rw voice-description?        string
    +--rw pkt-sec-src-voice-id*     string
    +--rw pkt-sec-dest-voice-id*    string
    +--rw pkt-sec-user-agent*       string
+--rw packet-security-ddos-condition
    +--rw ddos-description?        string
    +--rw pkt-sec-alert-packet-rate?  uint32
    +--rw pkt-sec-alert-flow-rate?   uint32
    +--rw pkt-sec-alert-byte-rate?   uint32
+--rw packet-security-payload-condition
    +--rw packet-payload-description?  string
    +--rw pkt-payload-content*         string
+--rw context-condition
    +--rw context-description?        string
    +--rw application-condition
        +--rw application-description?  string
        +--rw application-object*       string
        +--rw application-group*       string
        +--rw application-label*       string
        +--rw category
            +--rw application-category*
[name application-subcategory]
    +--rw name                      string
    +--rw application-subcategory    string
+--rw target-condition
    +--rw target-description?        string
    +--rw device-sec-context-cond
        +--rw target-device*        identityref
+--rw users-condition
    +--rw users-description?        string
    +--rw user      [user-name user-id]
        +--rw user-name*            string
        +--rw user-id*              uint32
    +--rw group      [group-name group-id]
        +--rw group-name            string
        +--rw group-id              uint32
```



```

module: ietf-i2nsf-policy-rule-for-nsf
  +--rw i2nsf-security-policy
    ...
    +--rw rules* [rule-name]
      |
      | ...
      | +--rw event-clause-container
      | | ...
      | +--rw condition-clause-container
      | | ...
      | +--rw action-clause-container
      | |   +--rw action-clause-description?  string
      | |   +--rw packet-action
      | |   |   +--rw ingress-action?  identityref
      | |   |   +--rw egress-action?   identityref
      | |   |   +--rw log-action?      identityref
      | |   +--rw flow-action
      | |   |   +--rw ingress-action?  identityref
      | |   |   +--rw egress-action?   identityref
      | |   |   +--rw log-action?      identityref
      | |   +--rw advanced-action
      | |   |   +--rw content-security-control*  identityref
      | |   |   +--rw attack-mitigation-control* identityref
      | +--rw rule-group
      |
      | ...

```

Figure 4: YANG Tree Diagram for an Action Clause

An action is used to control and monitor aspects of flow-based NSFs when the policy rule event and condition clauses are satisfied. NSFs provide security services by executing various actions. The action clause is defined as ingress action, egress action, or log action for packet action, flow action, and advanced action for additional inspection. The packet action is an action for an individual packet such as an IP datagram. The flow action is an action of a traffic flow such as the packets of a TCP session (e.g., an HTTP/HTTPS session). The advanced action is an action of an advanced action (e.g., web filter and DDoS-attack mitigator) for either a packet or a traffic flow. The action clause can be extended according to specific vendor action features. The action clause is described in detail in [[I-D.ietf-i2nsf-capability-data-model](#)].

#### 4. YANG Data Model of NSF-Facing Interface

The main objective of this data model is to provide both an information model and the corresponding YANG data model of I2NSF NSF-Facing Interface. This interface can be used to deliver control and management messages between Security Controller and NSFs for the I2NSF low-level security policies.

This data model is designed to support the I2NSF framework that can be extended according to the security needs. In other words, the model design is independent of the content and meaning of specific policies as well as the implementation approach.

With the YANG data model of I2NSF NSF-Facing Interface, this document suggests use cases for security policy rules such as time-based firewall, web filter, VoIP/VoLTE security service, and DDoS-attack mitigation in [Section 5](#).

#### 4.1. YANG Module of NSF-Facing Interface

This section describes a YANG module of NSF-Facing Interface. This YANG module imports from [\[RFC6991\]](#). It makes references to [\[RFC0768\]](#) [\[RFC0791\]](#) [\[RFC0792\]](#) [\[RFC0793\]](#) [\[RFC3261\]](#) [\[RFC4443\]](#) [\[RFC8200\]](#) [\[RFC8329\]](#) [\[RFC8335\]](#) [\[RFC8344\]](#) [\[ISO-Country-Codes\]](#) [\[IANA-Protocol-Numbers\]](#).

```
<CODE BEGINS> file "ietf-i2nsf-policy-rule-for-nsf@2021-03-08.yang"
module ietf-i2nsf-policy-rule-for-nsf {
  yang-version 1.1;
  namespace
    "urn:ietf:params:xml:ns:yang:ietf-i2nsf-policy-rule-for-nsf";
  prefix
    nsfintf;

  import ietf-inet-types{
    prefix inet;
    reference "RFC 6991";
  }
  import ietf-yang-types{
    prefix yang;
    reference "RFC 6991";
  }

  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>

     Editor: Jingyong Tim Kim
     <mailto:timkim@skku.edu>

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

`description`

"This module is a YANG module for Network Security Functions (NSF)-Facing Interface.

Copyright (c) 2021 IETF Trust and the persons identified as authors of the code. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted pursuant to, and subject to the license terms contained in, the Simplified BSD License set forth in [Section 4.c](#) of the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>).

This version of this YANG module is part of RFC XXXX (<https://www.rfc-editor.org/info/rfcXXXX>); see the RFC itself for full legal notices."

```
revision "2021-03-08"{
  description "The latest revision.";
  reference
    "RFC XXXX: I2NSF Network Security Function-Facing Interface
    YANG Data Model";
}
```

```
/*
 * Identities
 */
```

```
identity priority-usage-type {
  description
    "Base identity for priority usage type.";
}
```

```
identity priority-by-order {
  base priority-usage-type;
  description
    "Identity for priority by order";
}
```

```
identity priority-by-number {
  base priority-usage-type;
  description
    "Identity for priority by number";
}
```

```
identity event {
  description
```

```
    "Base identity for policy events";
  reference
    "draft-ietf-i2nsf-nsf-monitoring-data-model-04: I2NSF NSF
    Monitoring YANG Data Model - Event";
}

identity system-event {
  base event;
  description
    "Identity for system events";
  reference
    "draft-ietf-i2nsf-nsf-monitoring-data-model-04: I2NSF NSF
    Monitoring YANG Data Model - System event";
}

identity system-alarm {
  base event;
  description
    "Identity for system alarms";
  reference
    "draft-ietf-i2nsf-nsf-monitoring-data-model-04: I2NSF NSF
    Monitoring YANG Data Model - System alarm";
}

identity access-violation {
  base system-event;
  description
    "Identity for access violation
    system events";
  reference
    "draft-ietf-i2nsf-nsf-monitoring-data-model-04: I2NSF NSF
    Monitoring YANG Data Model - System event for access
    violation";
}

identity configuration-change {
  base system-event;
  description
    "Identity for configuration change
    system events";
  reference
    "draft-ietf-i2nsf-nsf-monitoring-data-model-04: I2NSF NSF
    Monitoring YANG Data Model - System event for configuration
    change";
}

identity memory-alarm {
  base system-alarm;
```



```
    description
      "Identity for memory alarm
      system alarms";
    reference
      "draft-ietf-i2nsf-nsf-monitoring-data-model-04: I2NSF NSF
      Monitoring YANG Data Model - System alarm for memory";
  }

  identity cpu-alarm {
    base system-alarm;
    description
      "Identity for CPU alarm
      system alarms";
    reference
      "draft-ietf-i2nsf-nsf-monitoring-data-model-04: I2NSF NSF
      Monitoring YANG Data Model - System alarm for CPU";
  }

  identity disk-alarm {
    base system-alarm;
    description
      "Identity for disk alarm
      system alarms";
    reference
      "draft-ietf-i2nsf-nsf-monitoring-data-model-04: I2NSF NSF
      Monitoring YANG Data Model - System alarm for disk";
  }

  identity hardware-alarm {
    base system-alarm;
    description
      "Identity for hardware alarm
      system alarms";
    reference
      "draft-ietf-i2nsf-nsf-monitoring-data-model-04: I2NSF NSF
      Monitoring YANG Data Model - System alarm for hardware";
  }

  identity interface-alarm {
    base system-alarm;
    description
      "Identity for interface alarm
      system alarms";
    reference
      "draft-ietf-i2nsf-nsf-monitoring-data-model-04: I2NSF NSF
      Monitoring YANG Data Model - System alarm for interface";
  }
}
```

```
identity type-of-service {
  description
    "Base identity for type of service of IPv4";
  reference
    "RFC 791: Internet Protocol - Type of Service";
}

identity traffic-class {
  description
    "Base identity for traffic-class of IPv6";
  reference
    "RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - Traffic Class";
}

identity normal {
  base type-of-service;
  base traffic-class;
  description
    "Identity for normal IPv4 TOS and IPv6 Traffic Class";
  reference
    "RFC 791: Internet Protocol - Type of Service
    RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - Traffic Class";
}

identity minimize-cost {
  base type-of-service;
  base traffic-class;
  description
    "Identity for 'minimize monetary cost' IPv4 TOS and
    IPv6 Traffic Class";
  reference
    "RFC 791: Internet Protocol - Type of Service
    RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - Traffic Class";
}

identity maximize-reliability {
  base type-of-service;
  base traffic-class;
  description
    "Identity for 'maximize reliability' IPv4 TOS and
    IPv6 Traffic Class";
  reference
    "RFC 791: Internet Protocol - Type of Service
    RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - Traffic Class";
}
```

```
}

identity maximize-throughput {
  base type-of-service;
  base traffic-class;
  description
    "Identity for 'maximize throughput' IPv4 TOS and
    IPv6 Traffic Class";
  reference
    "RFC 791: Internet Protocol - Type of Service
    RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - Traffic Class";
}

identity minimize-delay {
  base type-of-service;
  base traffic-class;
  description
    "Identity for 'minimize delay' IPv4 TOS and
    IPv6 Traffic Class";
  reference
    "RFC 791: Internet Protocol - Type of Service
    RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - Traffic Class";
}

identity maximize-security {
  base type-of-service;
  base traffic-class;
  description
    "Identity for 'maximize security' IPv4 TOS and
    IPv6 Traffic Class";
  reference
    "RFC 791: Internet Protocol - Type of Service
    RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - Traffic Class";
}

identity fragmentation-flags-type {
  description
    "Base identity for fragmentation flags type";
  reference
    "RFC 791: Internet Protocol - Fragmentation Flags";
}

identity fragment {
  base fragmentation-flags-type;
  description
```

```
    "Identity for 'More fragment' flag";
  reference
    "RFC 791: Internet Protocol - Fragmentation Flags";
}

identity no-fragment {
  base fragmentation-flags-type;
  description
    "Identity for 'Do not fragment' flag";
  reference
    "RFC 791: Internet Protocol - Fragmentation Flags";
}

identity reserved {
  base fragmentation-flags-type;
  description
    "Identity for reserved flags";
  reference
    "RFC 791: Internet Protocol - Fragmentation Flags";
}

identity protocol {
  description
    "Base identity for protocol of IPv4";
  reference
    "IANA: Assigned Internet Protocol Numbers
    RFC 791: Internet Protocol - Protocol";
}

identity next-header {
  description
    "Base identity for IPv6 next header";
  reference
    "RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - Next Header";
}

identity icmp {
  base protocol;
  base next-header;
  description
    "Identity for ICMP IPv4 protocol and
    IPv6 next header";
  reference
    "IANA: Assigned Internet Protocol Numbers
    RFC 791: Internet Protocol - Protocol
    RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - Next Header";
}
```

```
}

identity igmp {
  base protocol;
  base next-header;
  description
    "Identity for IGMP IPv4 protocol and
    IPv6 next header";
  reference
    "IANA: Assigned Internet Protocol Numbers
    RFC 791: Internet Protocol - Protocol
    RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - Next Header";
}

identity tcp {
  base protocol;
  base next-header;
  description
    "Identity for TCP protocol";
  reference
    "IANA: Assigned Internet Protocol Numbers
    RFC 791: Internet Protocol - Protocol
    RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - Next Header";
}

identity igmp {
  base protocol;
  base next-header;
  description
    "Identity for IGRP IPv4 protocol
    and IPv6 next header";
  reference
    "IANA: Assigned Internet Protocol Numbers
    RFC 791: Internet Protocol - Protocol
    RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - Next Header";
}

identity udp {
  base protocol;
  base next-header;
  description
    "Identity for UDP IPv4 protocol
    and IPv6 next header";
  reference
    "IANA: Assigned Internet Protocol Numbers
```

```

    RFC 791: Internet Protocol - Protocol
    RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - Next Header";
}

identity gre {
    base protocol;
    base next-header;
    description
        "Identity for GRE IPv4 protocol
        and IPv6 next header";
    reference
        "IANA: Assigned Internet Protocol Numbers
        RFC 791: Internet Protocol - Protocol
        RFC 8200: Internet Protocol, Version 6 (IPv6)
        Specification - Next Header";
}

identity esp {
    base protocol;
    base next-header;
    description
        "Identity for ESP IPv4 protocol
        and IPv6 next header";
    reference
        "IANA: Assigned Internet Protocol Numbers
        RFC 791: Internet Protocol - Protocol
        RFC 8200: Internet Protocol, Version 6 (IPv6)
        Specification - Next Header";
}

identity ah {
    base protocol;
    base next-header;
    description
        "Identity for AH IPv4 protocol
        and IPv6 next header";
    reference
        "IANA: Assigned Internet Protocol Numbers
        RFC 791: Internet Protocol - Protocol
        RFC 8200: Internet Protocol, Version 6 (IPv6)
        Specification - Next Header";
}

identity mobile {
    base protocol;
    base next-header;
    description
```

```
    "Identity for mobile IPv4 protocol
    and IPv6 next header";
  reference
    "IANA: Assigned Internet Protocol Numbers
    RFC 791: Internet Protocol - Protocol
    RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - Next Header";
}

identity tlsp {
  base protocol;
  base next-header;
  description
    "Identity for TLSP IPv4 protocol
    and IPv6 next header";
  reference
    "IANA: Assigned Internet Protocol Numbers
    RFC 791: Internet Protocol - Protocol
    RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - Next Header";
}

identity skip {
  base protocol;
  base next-header;
  description
    "Identity for skip IPv4 protocol
    and IPv6 next header";
  reference
    "IANA: Assigned Internet Protocol Numbers
    RFC 791: Internet Protocol - Protocol
    RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - Next Header";
}

identity ipv6-icmp {
  base protocol;
  base next-header;
  description
    "Identity for IPv6 ICMP next header";
  reference
    "IANA: Assigned Internet Protocol Numbers
    RFC 4443: Internet Control Message Protocol (ICMPv6)
    for the Internet Protocol Version 6 (IPv6) Specification
    RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - Next Header";
}
```

```
identity eigrp {
  base protocol;
  base next-header;
  description
    "Identity for EIGRP IPv4 protocol
    and IPv6 next header";
  reference
    "IANA: Assigned Internet Protocol Numbers
    RFC 791: Internet Protocol - Protocol
    RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - Next Header";
}

identity ospf {
  base protocol;
  base next-header;
  description
    "Identity for OSPF IPv4 protocol
    and IPv6 next header";
  reference
    "IANA: Assigned Internet Protocol Numbers
    RFC 791: Internet Protocol - Protocol
    RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - Next Header";
}

identity l2tp {
  base protocol;
  base next-header;
  description
    "Identity for L2TP IPv4 protocol
    and IPv6 next header";
  reference
    "IANA: Assigned Internet Protocol Numbers
    RFC 791: Internet Protocol - Protocol
    RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - Next Header";
}

identity ipopts {
  description
    "Base identity for IP options";
  reference
    "RFC 791: Internet Protocol - Options";
}

identity rr {
  base ipopts;
```



```
    description
      "Identity for 'Record Route' IP Option";
    reference
      "RFC 791: Internet Protocol - Options";
  }

  identity eol {
    base ipopts;
    description
      "Identity for 'End of List' IP Option";
    reference
      "RFC 791: Internet Protocol - Options";
  }

  identity nop {
    base ipopts;
    description
      "Identity for 'No Operation' IP Option";
    reference
      "RFC 791: Internet Protocol - Options";
  }

  identity ts {
    base ipopts;
    description
      "Identity for 'Timestamp' IP Option";
    reference
      "RFC 791: Internet Protocol - Options";
  }

  identity sec {
    base ipopts;
    description
      "Identity for 'IP security' IP Option";
    reference
      "RFC 791: Internet Protocol - Options";
  }

  identity esec {
    base ipopts;
    description
      "Identity for 'IP extended security' IP Option";
    reference
      "RFC 791: Internet Protocol - Options";
  }

  identity lsrr {
    base ipopts;
```

```
    description
      "Identity for 'Loose Source Routing' IP Option";
    reference
      "RFC 791: Internet Protocol - Options";
  }

  identity ssrr {
    base ipopts;
    description
      "Identity for 'Strict Source Routing' IP Option";
    reference
      "RFC 791: Internet Protocol - Options";
  }

  identity satid {
    base ipopts;
    description
      "Identity for 'Stream Identifier' IP Option";
    reference
      "RFC 791: Internet Protocol - Options";
  }

  identity any {
    base ipopts;
    description
      "Identity for 'any IP options
      included in IPv4 packet";
    reference
      "RFC 791: Internet Protocol - Options";
  }

  identity tcp-flags {
    description
      "Base identity for TCP flags";
    reference
      "RFC 793: Transmission Control Protocol - Flags";
  }

  identity cwr {
    base tcp-flags;
    description
      "Identity for 'Congestion Window Reduced' TCP flag";
    reference
      "RFC 793: Transmission Control Protocol - Flags";
  }

  identity ecn {
    base tcp-flags;
```

```
    description
      "Identity for 'Explicit Congestion Notification'
      TCP flag";
    reference
      "RFC 793: Transmission Control Protocol - Flags";
  }

  identity urg {
    base tcp-flags;
    description
      "Identity for 'Urgent' TCP flag";
    reference
      "RFC 793: Transmission Control Protocol - Flags";
  }

  identity ack {
    base tcp-flags;
    description
      "Identity for 'acknowledgement' TCP flag";
    reference
      "RFC 793: Transmission Control Protocol - Flags";
  }

  identity psh {
    base tcp-flags;
    description
      "Identity for 'Push' TCP flag";
    reference
      "RFC 793: Transmission Control Protocol - Flags";
  }

  identity rst {
    base tcp-flags;
    description
      "Identity for 'Reset' TCP flag";
    reference
      "RFC 793: Transmission Control Protocol - Flags";
  }

  identity syn {
    base tcp-flags;
    description
      "Identity for 'Synchronize' TCP flag";
    reference
      "RFC 793: Transmission Control Protocol - Flags";
  }

  identity fin {
```

```
    base tcp-flags;
    description
        "Identity for 'Finish' TCP flag";
    reference
        "RFC 793: Transmission Control Protocol - Flags";
}

identity icmp-type {
    description
        "Base identity for ICMP Message types";
    reference
        "RFC 792: Internet Control Message Protocol";
}

identity echo-reply {
    base icmp-type;
    description
        "Identity for 'Echo Reply' ICMP message type";
    reference
        "RFC 792: Internet Control Message Protocol";
}

identity destination-unreachable {
    base icmp-type;
    description
        "Identity for 'Destination Unreachable'
        ICMP message type";
    reference
        "RFC 792: Internet Control Message Protocol";
}

identity redirect {
    base icmp-type;
    description
        "Identity for 'Redirect' ICMP message type";
    reference
        "RFC 792: Internet Control Message Protocol";
}

identity echo {
    base icmp-type;
    description
        "Identity for 'Echo' ICMP message type";
    reference
        "RFC 792: Internet Control Message Protocol";
}
```

```
identity router-advertisement {
  base icmp-type;
  description
    "Identity for 'Router Advertisement'
    ICMP message type";
  reference
    "RFC 792: Internet Control Message Protocol";
}

identity router-solicitation {
  base icmp-type;
  description
    "Identity for 'Router Solicitation'
    ICMP message type";
  reference
    "RFC 792: Internet Control Message Protocol";
}

identity time-exceeded {
  base icmp-type;
  description
    "Identity for 'Time exceeded' ICMP message type";
  reference
    "RFC 792: Internet Control Message Protocol";
}

identity parameter-problem {
  base icmp-type;
  description
    "Identity for 'Parameter Problem'
    ICMP message type";
  reference
    "RFC 792: Internet Control Message Protocol";
}

identity timestamp {
  base icmp-type;
  description
    "Identity for 'Timestamp' ICMP message type";
  reference
    "RFC 792: Internet Control Message Protocol";
}

identity timestamp-reply {
  base icmp-type;
  description
    "Identity for 'Timestamp Reply'
    ICMP message type";
```

```
    reference
      "RFC 792: Internet Control Message Protocol";
  }

  identity datagram-conversion-error {
    base icmp-type;
    description
      "Identity for 'Datagram Conversion Error'
      ICMP message type";
    reference
      "RFC 792: Internet Control Message Protocol";
  }

  identity experimental-mobility-protocols {
    base icmp-type;
    description
      "Identity for 'Experimental Mobility Protocols'
      ICMP message type";
    reference
      "RFC 792: Internet Control Message Protocol";
  }

  identity extended-echo-request {
    base icmp-type;
    description
      "Identity for 'Extended Echo Request'
      ICMP message type";
    reference
      "RFC 792: Internet Control Message Protocol
      RFC 8335: PROBE: A Utility for Probing Interfaces";
  }

  identity extended-echo-reply {
    base icmp-type;
    description
      "Identity for 'Extended Echo Reply'
      ICMP message type";
    reference
      "RFC 792: Internet Control Message Protocol
      RFC 8335: PROBE: A Utility for Probing Interfaces";
  }

  identity net-unreachable {
    base icmp-type;
    description
      "Identity for net unreachable
      in destination unreachable types";
    reference
```

```
    "RFC 792: Internet Control Message Protocol";
}

identity host-unreachable {
    base icmp-type;
    description
        "Identity for host unreachable
        in destination unreachable types";
    reference
        "RFC 792: Internet Control Message Protocol";
}

identity protocol-unreachable {
    base icmp-type;
    description
        "Identity for protocol unreachable
        in destination unreachable types";
    reference
        "RFC 792: Internet Control Message Protocol";
}

identity port-unreachable {
    base icmp-type;
    description
        "Identity for port unreachable
        in destination unreachable types";
    reference
        "RFC 792: Internet Control Message Protocol";
}

identity fragment-set {
    base icmp-type;
    description
        "Identity for fragmentation set
        in destination unreachable types";
    reference
        "RFC 792: Internet Control Message Protocol";
}

identity source-route-failed {
    base icmp-type;
    description
        "Identity for source route failed
        in destination unreachable types";
    reference
        "RFC 792: Internet Control Message Protocol";
}
```

```
identity destination-network-unknown {
  base icmp-type;
  description
    "Identity for destination network unknown
    in destination unreachable types";
  reference
    "RFC 792: Internet Control Message Protocol";
}

identity destination-host-unknown {
  base icmp-type;
  description
    "Identity for destination host unknown
    in destination unreachable types";
  reference
    "RFC 792: Internet Control Message Protocol";
}

identity source-host-isolated {
  base icmp-type;
  description
    "Identity for source host isolated
    in destination unreachable types";
  reference
    "RFC 792: Internet Control Message Protocol";
}

identity communication-prohibited-with-destination-network {
  base icmp-type;
  description
    "Identity for which communication with destination network
    is administratively prohibited in destination unreachable
    types";
  reference
    "RFC 792: Internet Control Message Protocol";
}

identity communication-prohibited-with-destination-host {
  base icmp-type;
  description
    "Identity for which communication with destination host
    is administratively prohibited in destination unreachable
    types";
  reference
    "RFC 792: Internet Control Message Protocol";
}

identity destination-network-unreachable-for-tos {
```



```
    base icmp-type;
    description
      "Identity for destination network unreachable
       for type of service in destination unreachable types";
    reference
      "RFC 792: Internet Control Message Protocol";
  }

  identity destination-host-unreachable-for-tos {
    base icmp-type;
    description
      "Identity for destination host unreachable
       for type of service in destination unreachable types";
    reference
      "RFC 792: Internet Control Message Protocol";
  }

  identity communication-prohibited {
    base icmp-type;
    description
      "Identity for communication administratively prohibited
       in destination unreachable types";
    reference
      "RFC 792: Internet Control Message Protocol";
  }

  identity host-precedence-violation {
    base icmp-type;
    description
      "Identity for host precedence violation
       in destination unreachable types";
    reference
      "RFC 792: Internet Control Message Protocol";
  }

  identity precedence-cutoff-in-effect {
    base icmp-type;
    description
      "Identity for precedence cutoff in effect
       in destination unreachable types";
    reference
      "RFC 792: Internet Control Message Protocol";
  }

  identity redirect-datagram-for-the-network {
    base icmp-type;
    description
      "Identity for redirect datagram for the network
```

```
        (or subnet) in redirect types";
    reference
        "RFC 792: Internet Control Message Protocol";
}

identity redirect-datagram-for-the-host {
    base icmp-type;
    description
        "Identity for redirect datagram for the host
        in redirect types";
    reference
        "RFC 792: Internet Control Message Protocol";
}

identity redirect-datagram-for-the-tos-and-network {
    base icmp-type;
    description
        "Identity for redirect datagram for the type of
        service and network in redirect types";
    reference
        "RFC 792: Internet Control Message Protocol";
}

identity redirect-datagram-for-the-tos-and-host {
    base icmp-type;
    description
        "Identity for redirect datagram for the type of
        service and host in redirect types";
    reference
        "RFC 792: Internet Control Message Protocol";
}

identity normal-router-advertisement {
    base icmp-type;
    description
        "Identity for normal router advertisement
        in router advertisement types";
    reference
        "RFC 792: Internet Control Message Protocol";
}

identity does-not-route-common-traffic {
    base icmp-type;
    description
        "Identity for does not route common traffic
        in router advertisement types";
    reference
        "RFC 792: Internet Control Message Protocol";
}
```

```
}

identity time-to-live-exceeded-in-transit {
  base icmp-type;
  description
    "Identity for time to live exceeded in transit
    in time exceeded types";
  reference
    "RFC 792: Internet Control Message Protocol";
}

identity fragment-reassembly-time-exceeded {
  base icmp-type;
  description
    "Identity for fragment reassembly time exceeded
    in time exceeded types";
  reference
    "RFC 792: Internet Control Message Protocol";
}

identity pointer-indicates-the-error {
  base icmp-type;
  description
    "Identity for pointer indicates the error
    in parameter problem types";
  reference
    "RFC 792: Internet Control Message Protocol";
}

identity missing-a-required-option {
  base icmp-type;
  description
    "Identity for missing a required option
    in parameter problem types";
  reference
    "RFC 792: Internet Control Message Protocol";
}

identity bad-length {
  base icmp-type;
  description
    "Identity for bad length
    in parameter problem types";
  reference
    "RFC 792: Internet Control Message Protocol";
}

identity bad-spi {
```

```
    base icmp-type;
    description
        "Identity for bad spi";
    reference
        "RFC 792: Internet Control Message Protocol";
}

identity authentication-failed {
    base icmp-type;
    description
        "Identity for authentication failed";
    reference
        "RFC 792: Internet Control Message Protocol";
}

identity decompression-failed {
    base icmp-type;
    description
        "Identity for decompression failed";
    reference
        "RFC 792: Internet Control Message Protocol";
}

identity decryption-failed {
    base icmp-type;
    description
        "Identity for decryption failed";
    reference
        "RFC 792: Internet Control Message Protocol";
}

identity need-authentication {
    base icmp-type;
    description
        "Identity for need authentication";
    reference
        "RFC 792: Internet Control Message Protocol";
}

identity need-authorization {
    base icmp-type;
    description
        "Identity for need authorization";
    reference
        "RFC 792: Internet Control Message Protocol";
}

identity req-no-error {
```

```
    base icmp-type;
    description
      "Identity for request with no error
       in extended echo request types";
    reference
      "RFC 792: Internet Control Message Protocol
       RFC 8335: PROBE: A Utility for Probing Interfaces";
  }

  identity rep-no-error {
    base icmp-type;
    description
      "Identity for reply with no error
       in extended echo reply types";
    reference
      "RFC 792: Internet Control Message Protocol
       RFC 8335: PROBE: A Utility for Probing Interfaces";
  }

  identity malformed-query {
    base icmp-type;
    description
      "Identity for malformed query
       in extended echo reply types";
    reference
      "RFC 792: Internet Control Message Protocol
       RFC 8335: PROBE: A Utility for Probing Interfaces";
  }

  identity no-such-interface {
    base icmp-type;
    description
      "Identity for no such interface
       in extended echo reply types";
    reference
      "RFC 792: Internet Control Message Protocol
       RFC 8335: PROBE: A Utility for Probing Interfaces";
  }

  identity no-such-table-entry {
    base icmp-type;
    description
      "Identity for no such table entry
       in extended echo reply types";
    reference
      "RFC 792: Internet Control Message Protocol
       RFC 8335: PROBE: A Utility for Probing Interfaces";
  }
}
```

```
identity multiple-interfaces-satisfy-query {
  base icmp-type;
  description
    "Identity for multiple interfaces satisfy query
    in extended echo reply types";
  reference
    "RFC 792: Internet Control Message Protocol
    RFC 8335: PROBE: A Utility for Probing Interfaces";
}

identity target-device {
  description
    "Base identity for target devices";
  reference
    "draft-ietf-i2nsf-capability-data-model-15:
    I2NSF Capability YANG Data Model";
}

identity computer {
  base target-device;
  description
    "Identity for computer such as personal computer (PC)
    and server";
}

identity mobile-phone {
  base target-device;
  description
    "Identity for mobile-phone such as smartphone and
    cellphone";
}

identity voip-volte-phone {
  base target-device;
  description
    "Identity for voip-volte-phone";
}

identity tablet {
  base target-device;
  description
    "Identity for tablet";
}

identity network-infrastructure-device {
  base target-device;
  description
    "Identity for network infrastructure devices
```

```
        such as switch, router, and access point";
    }

    identity iot {
        base target-device;
        description
            "Identity for IoT (Internet of Things)";
    }

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

    identity content-security-control {
        description
            "Base identity for content security control";
        reference
            "RFC 8329: Framework for Interface to
            Network Security Functions - Flow-Based
            NSF Capability Characterization
            draft-ietf-i2nsf-capability-data-model-15:
            I2NSF Capability YANG Data Model";
    }

    identity firewall {
        base content-security-control;
        description
            "Identity for firewall that monitors
            incoming and outgoing network traffic
            and permits or blocks data packets based
            on a set of security rules.";
    }

    identity antivirus {
        base content-security-control;
        description
            "Identity for antivirus that prevents,
            scans, detects and deletes viruses
            from a computer";
    }

    identity ips {
        base content-security-control;
        description
            "Identity for IPS (Intrusion Prevention System)
```

```
        that prevents malicious activity within a network";
    }

    identity ids {
        base content-security-control;
        description
            "Identity for IDS (Intrusion Detection System)
             that detects malicious activity within a network";
    }

    identity url-filtering {
        base content-security-control;
        description
            "Identity for url filtering that
             limits access by comparing the web traffic's URL
             with the URLs for web filtering in a database";
    }

    identity mail-filtering {
        base content-security-control;
        description
            "Identity for mail filtering that
             filters out a malicious email message by
             comparing its sender email address with the email
             addresses of malicious users in a database";
    }

    identity file-blocking {
        base content-security-control;
        description
            "Identity for file blocking that blocks the
             download or upload of malicious files with the
             information of suspicious files in a database";
    }

    identity pkt-capture {
        base content-security-control;
        description
            "Identity for packet capture that
             intercepts a packet that is crossing or moving
             over a specific network.";
    }

    identity application-control {
        base content-security-control;
        description
            "Identity for application control that
             filters out the packets of malicious applications
```



```
        with the information of those applications in a
        database";
    }

    identity voip-volte {
        base content-security-control;
        description
            "Identity for VoIP/VoLTE security service that
            filters out the packets of malicious users
            with a blacklist of malicious users in a database";
    }

    identity attack-mitigation-control {
        description
            "Base identity for attack mitigation control";
        reference
            "RFC 8329: Framework for Interface to
            Network Security Functions - Flow-Based
            NSF Capability Characterization
            draft-ietf-i2nsf-capability-data-model-15:
            I2NSF Capability YANG Data Model";
    }

    identity syn-flood {
        base attack-mitigation-control;
        description
            "Identity for syn flood
            that weakens the SYN flood attack";
    }

    identity udp-flood {
        base attack-mitigation-control;
        description
            "Identity for udp flood
            that weakens the UDP flood attack";
    }

    identity icmp-flood {
        base attack-mitigation-control;
        description
            "Identity for icmp flood
            that weakens the ICMP flood attack";
    }

    identity ip-frag-flood {
        base attack-mitigation-control;
        description
            "Identity for ip frag flood
```

```
        that weakens the IP fragmentation flood attack";
    }

    identity http-and-https-flood {
        base attack-mitigation-control;
        description
            "Identity for http and https flood
             that weakens the HTTP and HTTPS flood attack";
    }

    identity dns-flood {
        base attack-mitigation-control;
        description
            "Identity for dns flood
             that weakens the DNS flood attack";
    }

    identity dns-amp-flood {
        base attack-mitigation-control;
        description
            "Identity for dns amp flood
             that weakens the DNS amplification flood attack";
    }

    identity ntp-amp-flood {
        base attack-mitigation-control;
        description
            "Identity for ntp amp flood
             that weakens the NTP amplification flood attack";
    }

    identity ssl-ddos {
        base attack-mitigation-control;
        description
            "Identity for ssl ddos
             that weakens the SSL DDoS attack";
    }

    identity ip-sweep {
        base attack-mitigation-control;
        description
            "Identity for ip sweep
             that weakens the IP sweep attack";
    }

    identity port-scanning {
        base attack-mitigation-control;
        description
```

```
    "Identity for port scanning
      that weakens the port scanning attack";
  }

  identity ping-of-death {
    base attack-mitigation-control;
    description
      "Identity for ping-of-death
        that weakens the ping-of-death attack";
  }

  identity teardrop {
    base attack-mitigation-control;
    description
      "Identity for teardrop
        that weakens the teardrop attack";
  }

  identity oversized-icmp {
    base attack-mitigation-control;
    description
      "Identity for oversized icmp
        that weakens the oversized icmp attack";
  }

  identity tracert {
    base attack-mitigation-control;
    description
      "Identity for tracert
        that weakens the tracert attack";
  }

  identity ingress-action {
    description
      "Base identity for action";
    reference
      "draft-ietf-i2nsf-capability-data-model-15:
        I2NSF Capability YANG Data Model - Ingress Action";
  }

  identity egress-action {
    description
      "Base identity for egress action";
    reference
      "draft-ietf-i2nsf-capability-data-model-15:
        I2NSF Capability YANG Data Model - Egress Action";
  }
}
```

```
identity default-action {
  description
    "Base identity for default action";
  reference
    "draft-ietf-i2nsf-capability-data-model-15:
     I2NSF Capability YANG Data Model - Default Action";
}

identity pass {
  base ingress-action;
  base egress-action;
  base default-action;
  description
    "Identity for pass";
  reference
    "draft-ietf-i2nsf-capability-data-model-15:
     I2NSF Capability YANG Data Model - Actions and
     Default Action";
}

identity drop {
  base ingress-action;
  base egress-action;
  base default-action;
  description
    "Identity for drop";
  reference
    "draft-ietf-i2nsf-capability-data-model-15:
     I2NSF Capability YANG Data Model - Actions and
     Default Action";
}

identity reject {
  base ingress-action;
  base egress-action;
  base default-action;
  description
    "Identity for reject";
  reference
    "draft-ietf-i2nsf-capability-data-model-15:
     I2NSF Capability YANG Data Model - Actions and
     Default Action";
}

identity alert {
  base ingress-action;
  base egress-action;
  base default-action;
```

```
    description
      "Identity for alert";
    reference
      "draft-ietf-i2nsf-capability-data-model-15:
      I2NSF Capability YANG Data Model - Actions and
      Default Action";
  }

  identity mirror {
    base ingress-action;
    base egress-action;
    base default-action;
    description
      "Identity for mirror";
    reference
      "draft-ietf-i2nsf-capability-data-model-15:
      I2NSF Capability YANG Data Model - Actions and
      Default Action";
  }

  identity log-action {
    description
      "Base identity for log action";
  }

  identity rule-log {
    base log-action;
    description
      "Identity for rule log";
  }

  identity session-log {
    base log-action;
    description
      "Identity for session log";
  }

  identity invoke-signaling {
    base egress-action;
    description
      "Identity for invoke signaling";
  }

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

```
identity forwarding {
  base egress-action;
  description
    "Identity for forwarding";
}

identity redirection {
  base egress-action;
  description
    "Identity for redirection";
}

identity resolution-strategy {
  description
    "Base identity for resolution strategy";
  reference
    "draft-ietf-i2nsf-capability-data-model-15:
    I2NSF Capability YANG Data Model - Resolution Strategy";
}

identity fmr {
  base resolution-strategy;
  description
    "Identity for First Matching Rule (FMR)";
  reference
    "draft-ietf-i2nsf-capability-data-model-15:
    I2NSF Capability YANG Data Model - Resolution Strategy";
}

identity lmr {
  base resolution-strategy;
  description
    "Identity for Last Matching Rule (LMR)";
  reference
    "draft-ietf-i2nsf-capability-data-model-15:
    I2NSF Capability YANG Data Model - Resolution Strategy";
}

identity pmr {
  base resolution-strategy;
  description
    "Identity for Prioritized Matching Rule (PMR)";
  reference
    "draft-ietf-i2nsf-capability-data-model-15:
    I2NSF Capability YANG Data Model - Resolution Strategy";
}
```

```
identity pmre {
  base resolution-strategy;
  description
    "Identity for Prioritized Matching Rule
    with Errors (PMRE)";
  reference
    "draft-ietf-i2nsf-capability-data-model-15:
    I2NSF Capability YANG Data Model - Resolution Strategy";
}

identity pmrn {
  base resolution-strategy;
  description
    "Identity for Prioritized Matching Rule
    with No Errors (PMRN)";
  reference
    "draft-ietf-i2nsf-capability-data-model-15:
    I2NSF Capability YANG Data Model - Resolution Strategy";
}

/*
 * Typedefs
 */

typedef start-time-type {
  type union {
    type string {
      pattern '\d{2}:\d{2}:\d{2}(\.\d+)?'
        + '(Z|[\+-]\d{2}:\d{2})';
    }

    type enumeration {
      enum right-away {
        description
          "Immediate rule execution
          in the system.";
      }
    }
  }

  description
    "Start time when the rules are applied.";
}

typedef end-time-type {
  type union {
    type string {
      pattern '\d{2}:\d{2}:\d{2}(\.\d+)?'
```

```
        + '(Z|[\+\-]\d{2}:\d{2})';
    }

    type enumeration {
        enum infinitely {
            description
                "Infinite rule execution
                in the system.";
        }
    }
}
description
    "End time when the rules are applied.";
}

typedef day-type {
    type enumeration {
        enum sunday {
            description
                "Sunday for periodic day";
        }
        enum monday {
            description
                "Monday for periodic day";
        }
        enum tuesday {
            description
                "Tuesday for periodic day";
        }
        enum wednesday {
            description
                "Wednesday for periodic day";
        }
        enum thursday {
            description
                "Thursday for periodic day";
        }
        enum friday {
            description
                "Friday for periodic day";
        }
        enum saturday {
            description
                "Saturday for periodic day";
        }
    }
}
description
    "This can be used for the rules to be applied
```



```
        according to periodic day";
    }

typedef month-type {
    type enumeration {
        enum january {
            description
                "January for periodic month";
        }
        enum february {
            description
                "February for periodic month";
        }
        enum march {
            description
                "March for periodic month";
        }
        enum april {
            description
                "April for periodic month";
        }
        enum may {
            description
                "May for periodic month";
        }
        enum june {
            description
                "June for periodic month";
        }
        enum july {
            description
                "July for periodic month";
        }
        enum august {
            description
                "August for periodic month";
        }
        enum september {
            description
                "September for periodic month";
        }
        enum october {
            description
                "October for periodic month";
        }
        enum november {
            description
                "November for periodic month";
        }
    }
}
```

```
    }
    enum december {
        description
            "December for periodic month";
    }
}
description
    "This can be used for the rules to be applied
    according to periodic month";
}

/*
 * Groupings
 */

grouping ipv4 {
    list ipv4-address {
        key "ipv4";
        description
            "The list of IPv4 addresses.";

        leaf ipv4 {
            type inet:ipv4-address;
            description
                "The value of IPv4 address.";
        }
        choice subnet {
            description
                "The subnet can be specified as a prefix length or
                netmask.";
            leaf prefix-length {
                type uint8 {
                    range "0..32";
                }
                description
                    "The length of the subnet prefix.";
            }
            leaf netmask {
                type yang:dotted-quad;
                description
                    "The subnet specified as a netmask.";
            }
        }
    }
}
description
    "Grouping for an IPv4 address";

reference
```

```
    "RFC 791: Internet Protocol - IPv4 address
    RFC 8344: A YANG Data Model for IP Management";
}

grouping ipv6 {
  list ipv6-address {
    key "ipv6";
    description
      "The list of IPv6 addresses.";

    leaf ipv6 {
      type inet:ipv6-address;
      description
        "The value of IPv6 address.";
    }

    leaf prefix-length {
      type uint8 {
        range "0..128";
      }
      description
        "The length of the subnet prefix.";
    }
  }
  description
    "Grouping for an IPv6 address";

  reference
    "RFC 8200: Internet Protocol, Version 6 (IPv6)
    Specification - IPv6 address
    RFC 8344: A YANG Data Model for IP Management";
}

grouping pkt-sec-ipv4 {
  choice match-type {
    description
      "There are two types of security policy IPv4 address
      matching - exact match and range match.";
    case exact-match {
      uses ipv4;
      description
        "Exact match for an IPv4 address.";
    }
    case range-match {
      list range-ipv4-address {
        key "start-ipv4-address end-ipv4-address";
        leaf start-ipv4-address {
          type inet:ipv4-address;

```

```
        description
            "Starting IPv4 address for a range match.";
    }

    leaf end-ipv4-address {
        type inet:ipv4-address;
        description
            "Ending IPv4 address for a range match.";
    }
    description
        "Range match for an IPv4 address.";
    }
}
}
description
    "Grouping for an IPv4 address.";

reference
    "RFC 791: Internet Protocol - IPv4 address";
}

grouping pkt-sec-ipv6 {
    choice match-type {
        description
            "There are two types of security policy IPv6 address
            matching - exact match and range match.";
        case exact-match {
            uses ipv6;
            description
                "Exact match for an IPv6 address.";
        }
        case range-match {
            list range-ipv6-address {
                key "start-ipv6-address end-ipv6-address";
                leaf start-ipv6-address {
                    type inet:ipv6-address;
                    description
                        "Starting IPv6 address for a range match.";
                }

                leaf end-ipv6-address {
                    type inet:ipv6-address;
                    description
                        "Ending IPv6 address for a range match.";
                }
            }
            description
                "Range match for an IPv6 address.";
        }
    }
}
```

```
    }
  }
  description
    "Grouping for IPv6 address.";

  reference
    "RFC 8200: Internet Protocol, Version 6 (IPv6)
     Specification - IPv6 address";
}

grouping pkt-sec-port-number {
  choice match-type {
    description
      "There are two types of security policy TCP/UDP port
       matching - exact match and range match.";
    case exact-match {
      leaf-list port-num {
        type inet:port-number;
        description
          "Exact match for a port number.";
      }
    }
    case range-match {
      list range-port-num {
        key "start-port-num end-port-num";
        leaf start-port-num {
          type inet:port-number;
          description
            "Starting port number for a range match.";
        }
        leaf end-port-num {
          type inet:port-number;
          description
            "Ending port number for a range match.";
        }
      }
      description
        "Range match for a port number.";
    }
  }
}
description
  "Grouping for port number.";

reference
  "RFC 793: Transmission Control Protocol - Port number
   RFC 768: User Datagram Protocol - Port Number";
}
```

```
/*
 * Data nodes
 */

container i2nsf-security-policy {
  description
    "Container for security policy
    including a set of security rules according to certain logic,
    i.e., their similarity or mutual relations, etc. The network
    security policy can be applied to both the unidirectional
    and bidirectional traffic across the NSF.
    The I2NSF security policies use the Event-Condition-Action
    (ECA) policy model ";

  reference
    "RFC 8329: Framework for Interface to Network Security
    Functions - I2NSF Flow Security Policy Structure
    draft-ietf-i2nsf-capability-data-model-15:
    I2NSF Capability YANG Data Model - Design Principles and
    ECA Policy Model Overview";

  list system-policy {
    key "system-policy-name";
    description
      "The system-policy represents there could be multiple system
      policies in one NSF, and each system policy is used by
      one virtual instance of the NSF/device.";

    leaf system-policy-name {
      type string;
      description
        "The name of the policy.
        This must be unique.";
    }

    leaf priority-usage {
      type identityref {
        base priority-usage-type;
      }
      default priority-by-order;
      description
        "Priority usage type for security policy rule:
        priority by order and priority by number";
    }

    leaf resolution-strategy {
      type identityref {
        base resolution-strategy;
      }
    }
  }
}
```

```
    }
    default fmr;
    description
        "The resolution strategies that can be used to
        specify how to resolve conflicts that occur between
        actions of the same or different policy rules that
        are matched and contained in this particular NSF";

    reference
        "draft-ietf-i2nsf-capability-data-model-15:
        I2NSF Capability YANG Data Model - Resolution strategy";
}

leaf default-action {
    type identityref {
        base default-action;
    }
    default alert;
    description
        "This default action can be used to specify a predefined
        action when no other alternative action was matched
        by the currently executing I2NSF Policy Rule. An analogy
        is the use of a default statement in a C switch statement.";

    reference
        "draft-ietf-i2nsf-capability-data-model-15:
        I2NSF Capability YANG Data Model - Default Action";
}

list rules {
    key "rule-name";
    description
        "This is a rule for network security functions.";

    leaf rule-name {
        type string;
        description
            "The name of the rule.";
    }

    leaf rule-description {
        type string;
        description
            "This description gives more information about
            rules.";
    }

    leaf rule-priority {
```

```
    type uint8 {
      range "1..255";
    }
    description
      "The priority keyword comes with a mandatory
       numeric value which can range from 1 till 255.
       Note that a higher number means a higher priority";
  }

  leaf rule-enable {
    type boolean;
    description
      "True is enable.
       False is not enable.";
  }

  leaf session-aging-time {
    type uint16;
    units "second";
    description
      "This is session aging time.";
  }

  container long-connection {
    description
      "This is long-connection";

    leaf enable {
      type boolean;
      description
        "True is enable.
         False is not enable.";
    }

    leaf duration {
      type uint16;
      description
        "This is the duration of the long-connection.";
    }
  }

  container time-intervals {
    description
      "Time zone when the rules are applied";
    container absolute-time-interval {
      description
        "Rule execution according to the absolute time.
         The absolute time interval means the exact time to
```



```
        start or end.";

    leaf start-time {
        type start-time-type;
        default right-away;
        description
            "Start time when the rules are applied";
    }
    leaf end-time {
        type end-time-type;
        default infinitely;
        description
            "End time when the rules are applied";
    }
}

container periodic-time-interval {
    description
        "Rule execution according to the periodic time.
        The periodic time interval means the repeated time
        such as a day, week, or month.";

    container day {
        description
            "Rule execution according to day.";
        leaf every-day {
            type boolean;
            default true;
            description
                "Rule execution every day";
        }

        leaf-list specific-day {
            when "../every-day = 'false'";
            type day-type;
            description
                "Rule execution according
                to specific day";
        }
    }
}

container month {
    description
        "Rule execution according to month.";
    leaf every-month {
        type boolean;
        default true;
    }
}
```

```
        description
            "Rule execution every day";
    }

    leaf-list specific-month {
        when "../every-month = 'false'";
        type month-type;
        description
            "Rule execution according
             to month day";
    }
}

}

container event-clause-container {
    description
        "An event is defined as any important
         occurrence in time of a change in the system being
         managed, and/or in the environment of the system being
         managed. When used in the context of policy rules for
         a flow-based NSF, it is used to determine whether the
         Condition clause of the Policy Rule can be evaluated
         or not. Examples of an I2NSF event include time and
         user actions (e.g., logon, logoff, and actions that
         violate any ACL.).";

    reference
        "RFC 8329: Framework for Interface to Network Security
         Functions - I2NSF Flow Security Policy Structure
         draft-ietf-i2nsf-capability-data-model-15:
         I2NSF Capability YANG Data Model - Design Principles and
         ECA Policy Model Overview
         draft-ietf-i2nsf-nsf-monitoring-data-model-04: I2NSF
         NSF Monitoring YANG Data Model - Alarms, Events, Logs,
         and Counters";

    leaf event-clause-description {
        type string;
        description
            "Description for an event clause";
    }

    container event-clauses {
        description
            "System Event Clause - either a system event or
             system alarm";
        reference

```

"RFC 8329: Framework for Interface to Network Security Functions - I2NSF Flow Security Policy Structure [draft-ietf-i2nsf-capability-data-model-15](#): I2NSF Capability YANG Data Model - Design Principles and ECA Policy Model Overview [draft-ietf-i2nsf-nsf-monitoring-data-model-04](#): I2NSF NSF Monitoring YANG Data Model - Alarms, Events, Logs, and Counters";

```
leaf-list system-event {
  type identityref {
    base system-event;
  }
  description
    "The security policy rule according to
    system events.";
}

leaf-list system-alarm {
  type identityref {
    base system-alarm;
  }
  description
    "The security policy rule according to
    system alarms.";
}
}

container condition-clause-container {
  description
    "A condition is defined as a set
    of attributes, features, and/or values that are to be
    compared with a set of known attributes, features,
    and/or values in order to determine whether or not the
    set of Actions in that (imperative) I2NSF Policy Rule
    can be executed or not. Examples of I2NSF Conditions
    include matching attributes of a packet or flow, and
    comparing the internal state of an NSF to a desired
    state.";
  reference
    "RFC 8329: Framework for Interface to Network Security
    Functions - I2NSF Flow Security Policy Structure
    draft-ietf-i2nsf-capability-data-model-15:
    I2NSF Capability YANG Data Model - Design Principles and
    ECA Policy Model Overview";

  leaf condition-clause-description {
```

```
    type string;
    description
      "Description for a condition clause.";
  }

  container packet-security-ipv4-condition {
    description
      "The purpose of this container is to represent IPv4
      packet header information to determine if the set
      of policy actions in this ECA policy rule should be
      executed or not.";
    reference
      "RFC 791: Internet Protocol";

    leaf ipv4-description {
      type string;
      description
        "ipv4 condition textual description.";
    }

    container pkt-sec-ipv4-header-length {
      choice match-type {
        description
          "Security policy IPv4 Header length match -
          exact match and range match.";
        case exact-match {
          leaf-list ipv4-header-length {
            type uint8 {
              range "5..15";
            }
            description
              "Exact match for an IPv4 header length.";
          }
        }
        case range-match {
          list range-ipv4-header-length {
            key "start-ipv4-header-length
              end-ipv4-header-length";
            leaf start-ipv4-header-length {
              type uint8 {
                range "5..15";
              }
            }
            description
              "Starting IPv4 header length for a range match.";
          }

          leaf end-ipv4-header-length {
            type uint8 {
```

```
        range "5..15";
    }
    description
        "Ending IPv4 header length for a range match.";
    }
    description
        "Range match for an IPv4 header length.";
    }
}
}
description
    "The security policy rule according to
    IPv4 header length.";
reference
    "RFC 791: Internet Protocol - Header length";
}

leaf-list pkt-sec-ipv4-tos {
    type identityref {
        base type-of-service;
    }
    description
        "The security policy rule according to
        IPv4 type of service.";
    reference
        "RFC 791: Internet Protocol - Type of service";
}

container pkt-sec-ipv4-total-length {
    choice match-type {
        description
            "Security policy IPv4 total length matching
            - exact match and range match.";
        case exact-match {
            leaf-list ipv4-total-length {
                type uint16;
                description
                    "Exact match for an IPv4 total length.";
            }
        }
        case range-match {
            list range-ipv4-total-length {
                key "start-ipv4-total-length end-ipv4-total-length";
                leaf start-ipv4-total-length {
                    type uint16;
                    description
                        "Starting IPv4 total length for a range match.";
                }
            }
        }
    }
}
```

```
        leaf end-ipv4-total-length {
            type uint16;
            description
                "Ending IPv4 total length for a range match.";
        }
        description
            "Range match for an IPv4 total length.";
    }
}
description
    "The security policy rule according to
    IPv4 total length.";
reference
    "RFC 791: Internet Protocol - Total length";
}

leaf-list pkt-sec-ipv4-id {
    type uint16;
    description
        "The security policy rule according to
        IPv4 identification.";
    reference
        "RFC 791: Internet Protocol - Identification";
}

leaf-list pkt-sec-ipv4-fragment-flags {
    type identityref {
        base fragmentation-flags-type;
    }
    description
        "The security policy rule according to
        IPv4 fragment flags.";
    reference
        "RFC 791: Internet Protocol - Fragment flags";
}

container pkt-sec-ipv4-fragment-offset {
    choice match-type {
        description
            "There are two types to configure a security
            policy for IPv4 fragment offset, such as exact match
            and range match.";
        case exact-match {
            leaf-list ipv4-fragment-offset {
                type uint16 {
                    range "0..16383";
                }
            }
        }
    }
}
```

```
        description
            "Exact match for an IPv4 fragment offset.";
    }
}
case range-match {
    list range-ipv4-fragment-offset {
        key "start-ipv4-fragment-offset
            end-ipv4-fragment-offset";
        leaf start-ipv4-fragment-offset {
            type uint16 {
                range "0..16383";
            }
            description
                "Starting IPv4 fragment offset for a range match.";
        }
        leaf end-ipv4-fragment-offset {
            type uint16 {
                range "0..16383";
            }
            description
                "Ending IPv4 fragment offset for a range match.";
        }
        description
            "Range match for an IPv4 fragment offset.";
    }
}
}
description
    "The security policy rule according to
    IPv4 fragment offset.";
reference
    "RFC 791: Internet Protocol - Fragment offset";
}

container pkt-sec-ipv4-ttl {
    choice match-type {
        description
            "There are two types to configure a security
            policy for IPv4 TTL, such as exact match
            and range match.";
        case exact-match {
            leaf-list ipv4-ttl {
                type uint8;
                description
                    "Exact match for an IPv4 TTL.";
            }
        }
        case range-match {
```

```
    list range-ipv4-ttl {
      key "start-ipv4-ttl end-ipv4-ttl";
      leaf start-ipv4-ttl {
        type uint8;
        description
          "Starting IPv4 TTL for a range match.";
      }
      leaf end-ipv4-ttl {
        type uint8;
        description
          "Ending IPv4 TTL for a range match.";
      }
      description
        "Range match for an IPv4 TTL.";
    }
  }
}
description
  "The security policy rule according to
  IPv4 time-to-live (TTL).";
reference
  "RFC 791: Internet Protocol - Time to live";
}

leaf-list pkt-sec-ipv4-protocol {
  type identityref {
    base protocol;
  }
  description
    "The security policy rule according to
    IPv4 protocol.";
  reference
    "RFC 791: Internet Protocol - Protocol";
}

container pkt-sec-ipv4-src {
  uses pkt-sec-ipv4;
  description
    "The security policy rule according to
    IPv4 source address.";
  reference
    "RFC 791: Internet Protocol - IPv4 Address";
}

container pkt-sec-ipv4-dest {
  uses pkt-sec-ipv4;
  description
```



```
        "The security policy rule according to
        IPv4 destination address.";
    reference
        "RFC 791: Internet Protocol - IPv4 Address";
}

leaf-list pkt-sec-ipv4-iptests {
    type identityref {
        base iptests;
    }
    description
        "The security policy rule according to
        IPv4 tests.";
    reference
        "RFC 791: Internet Protocol - Options";
}

leaf pkt-sec-ipv4-same-ip {
    type boolean;
    description
        "Match on packets with the same IPv4 source
        and IPv4 destination address.";
}

leaf-list pkt-sec-ipv4-geo-ip {
    type string;
    description
        "The geo-ip keyword enables you to match on
        source and destination IP addresses of network
        traffic and to see to which country it belongs.";
    reference
        "ISO 3166: Codes for the representation of
        names of countries and their subdivisions";
}
}

container packet-security-ipv6-condition {
    description
        "The purpose of this container is to represent
        IPv6 packet header information to determine
        if the set of policy actions in this ECA policy
        rule should be executed or not.";
    reference
        "RFC 8200: Internet Protocol, Version 6 (IPv6)
        Specification";

    leaf ipv6-description {
        type string;
    }
}
```

```
    description
      "This is description for ipv6 condition.";
  }

  leaf-list pkt-sec-ipv6-traffic-class {
    type identityref {
      base traffic-class;
    }
    description
      "The security policy rule according to
      IPv6 traffic class.";
    reference
      "RFC 8200: Internet Protocol, Version 6 (IPv6)
      Specification - Traffic class";
  }

  container pkt-sec-ipv6-flow-label {
    choice match-type {
      description
        "There are two types to configure a security
        policy for IPv6 flow label, such as exact match
        and range match.";
      case exact-match {
        leaf-list ipv6-flow-label {
          type uint32 {
            range "0..1048575";
          }
          description
            "Exact match for an IPv6 flow label.";
        }
      }
      case range-match {
        list range-ipv6-flow-label {
          key "start-ipv6-flow-label end-ipv6-flow-label";
          leaf start-ipv6-flow-label {
            type uint32 {
              range "0..1048575";
            }
            description
              "Starting IPv6 flow label for a range match.";
          }
          leaf end-ipv6-flow-label {
            type uint32 {
              range "0..1048575";
            }
            description
              "Ending IPv6 flow label for a range match.";
          }
        }
      }
    }
  }
}
```

```
    }
    description
      "Range match for an IPv6 flow label.";
  }
}
description
  "The security policy rule according to
  IPv6 flow label.";
reference
  "RFC 8200: Internet Protocol, Version 6 (IPv6)
  Specification - Flow label";
}

container pkt-sec-ipv6-payload-length {
  choice match-type {
    description
      "There are two types to configure a security
      policy for IPv6 payload length, such as
      exact match and range match.";
    case exact-match {
      leaf-list ipv6-payload-length {
        type uint16;
        description
          "Exact match for an IPv6 payload length.";
      }
    }
    case range-match {
      list range-ipv6-payload-length {
        key "start-ipv6-payload-length
            end-ipv6-payload-length";
        leaf start-ipv6-payload-length {
          type uint16;
          description
            "Starting IPv6 payload length for a range match.";
        }
        leaf end-ipv6-payload-length {
          type uint16;
          description
            "Ending IPv6 payload length for a range match.";
        }
        description
          "Range match for an IPv6 payload length.";
      }
    }
  }
}
description
  "The security policy rule according to
```

```
        IPv6 payload length.";
    reference
        "RFC 8200: Internet Protocol, Version 6 (IPv6)
        Specification - Payload length";
}

leaf-list pkt-sec-ipv6-next-header {
    type identityref {
        base next-header;
    }
    description
        "The security policy rule according to
        IPv6 next header.";
    reference
        "RFC 8200: Internet Protocol, Version 6 (IPv6)
        Specification - Next header";
}

container pkt-sec-ipv6-hop-limit {
    choice match-type {
        description
            "There are two types to configure a security
            policy for IPv6 hop limit, such as exact match
            and range match.";
        case exact-match {
            leaf-list ipv6-hop-limit {
                type uint8;
                description
                    "Exact match for an IPv6 hop limit.";
            }
        }
        case range-match {
            list range-ipv6-hop-limit {
                key "start-ipv6-hop-limit end-ipv6-hop-limit";
                leaf start-ipv6-hop-limit {
                    type uint8;
                    description
                        "Start IPv6 hop limit for a range match.";
                }
                leaf end-ipv6-hop-limit {
                    type uint8;
                    description
                        "End IPv6 hop limit for a range match.";
                }
            }
            description
                "Range match for an IPv6 hop limit.";
        }
    }
}
```

```
    }
    description
      "The security policy rule according to
       IPv6 hop limit.";
    reference
      "RFC 8200: Internet Protocol, Version 6 (IPv6)
       Specification - Hop limit";
  }

  container pkt-sec-ipv6-src {
    uses pkt-sec-ipv6;
    description
      "The security policy rule according to
       IPv6 source address.";
    reference
      "RFC 8200: Internet Protocol, Version 6 (IPv6)
       Specification - IPv6 address";
  }

  container pkt-sec-ipv6-dest {
    uses pkt-sec-ipv6;
    description
      "The security policy rule according to
       IPv6 destination address.";
    reference
      "RFC 8200: Internet Protocol, Version 6 (IPv6)
       Specification - IPv6 address";
  }
}

container packet-security-tcp-condition {
  description
    "The purpose of this container is to represent
     TCP packet header information to determine
     if the set of policy actions in this ECA policy
     rule should be executed or not.";
  reference
    "RFC 793: Transmission Control Protocol";

  leaf tcp-description {
    type string;
    description
      "This is description for tcp condition.";
  }

  container pkt-sec-tcp-src-port-num {
    uses pkt-sec-port-number;
  }
}
```

```
    description
      "The security policy rule according to
       tcp source port number.";
    reference
      "RFC 793: Transmission Control Protocol
       - Port number";
  }

  container pkt-sec-tcp-dest-port-num {
    uses pkt-sec-port-number;
    description
      "The security policy rule according to
       tcp destination port number.";
    reference
      "RFC 793: Transmission Control Protocol
       - Port number";
  }

  leaf-list pkt-sec-tcp-flags {
    type identityref {
      base tcp-flags;
    }
    description
      "The security policy rule according to
       tcp flags.";
    reference
      "RFC 793: Transmission Control Protocol
       - Flags";
  }
}

container packet-security-udp-condition {
  description
    "The purpose of this container is to represent
     UDP packet header information to determine
     if the set of policy actions in this ECA policy
     rule should be executed or not.";
  reference
    "RFC 793: Transmission Control Protocol";

  leaf udp-description {
    type string;
    description
      "This is description for udp condition.";
  }

  container pkt-sec-udp-src-port-num {
    uses pkt-sec-port-number;
```

```
description
  "The security policy rule according to
  udp source port number.";
reference
  "RFC 768: User Datagram Protocol
  - Total Length";
}

container pkt-sec-udp-dest-port-num {
  uses pkt-sec-port-number;
  description
    "The security policy rule according to
    udp destination port number.";
  reference
    "RFC 768: User Datagram Protocol
    - Total Length";
}

container pkt-sec-udp-total-length {
  choice match-type {
    description
      "There are two types to configure a security
      policy for udp sequence number,
      such as exact match and range match.";
    case exact-match {
      leaf-list udp-total-length {
        type uint32;
        description
          "Exact match for an udp-total-length.";
      }
    }
    case range-match {
      list range-udp-total-length {
        key "start-udp-total-length end-udp-total-length";
        leaf start-udp-total-length {
          type uint32;
          description
            "Start udp total length for a range match.";
        }
        leaf end-udp-total-length {
          type uint32;
          description
            "End udp total length for a range match.";
        }
      }
      description
        "Range match for a udp total length.";
    }
  }
}
```

```
    }
  }
  description
    "The security policy rule according to
    udp total length.";
  reference
    "RFC 768: User Datagram Protocol
    - Total Length";
}
}

container packet-security-sctp-condition {
  description
    "The purpose of this container is to represent
    SCTP packet header information to determine
    if the set of policy actions in this ECA policy
    rule should be executed or not.";
  leaf sctp-description {
    type string;
    description
      "This is description for sctp condition.";
  }

  container pkt-sec-sctp-src-port-num {
    uses pkt-sec-port-number;
    description
      "The security policy rule according to
      sctp source port number.";
    reference
      "RFC 4960: Stream Control Transmission Protocol
      - Port number";
  }

  container pkt-sec-sctp-dest-port-num {
    uses pkt-sec-port-number;
    description
      "The security policy rule according to
      sctp destination port number.";
    reference
      "RFC 4960: Stream Control Transmission Protocol
      - Total Length";
  }

  leaf-list pkt-sec-sctp-verification-tag {
    type uint32;
    description
      "The security policy rule according to
```



```
        udp total length.";
    reference
        "RFC 4960: Stream Control Transmission Protocol
        - Verification Tag";
}

leaf-list pkt-sec-sctp-chunk-type {
    type uint8;
    description
        "The security policy rule according to
        sctp chunk type ID Value.";
    reference
        "RFC 4960: Stream Control Transmission Protocol
        - Chunk Type";
}
}

container packet-security-dccp-condition {
    description
        "The purpose of this container is to represent
        DCCP packet header information to determine
        if the set of policy actions in this ECA policy
        rule should be executed or not.";
    leaf dccp-description {
        type string;
        description
            "This is description for dccp condition.";
    }
}

container pkt-sec-dccp-src-port-num {
    uses pkt-sec-port-number;
    description
        "The security policy rule according to
        dccp source port number.";
    reference
        "RFC 4340: Datagram Congestion Control Protocol (DCCP)
        - Port number";
}

container pkt-sec-dccp-dest-port-num {
    uses pkt-sec-port-number;
    description
        "The security policy rule according to
        dccp destination port number.";
    reference
        "RFC 4340: Datagram Congestion Control Protocol (DCCP)
        - Port number";
}
```

```
leaf-list pkt-sec-dccp-service-code {
  type uint32;
  description
    "The security policy rule according to
    dccp service code.";
  reference
    "RFC 4340: Datagram Congestion Control Protocol (DCCP)
    - Service Codes
    RFC 5595: The Datagram Congestion Control Protocol (DCCP)
    Service Codes
    RFC 6335: Internet Assigned Numbers Authority (IANA)
    Procedures for the Management of the Service Name and
    Transport Protocol Port Number Registry - Service Code";
}
}

container packet-security-icmp-condition {
  description
    "The purpose of this container is to represent
    ICMP packet header information to determine
    if the set of policy actions in this ECA policy
    rule should be executed or not.";
  reference
    "RFC 792: Internet Control Message Protocol
    RFC 8335: PROBE: A Utility for Probing Interfaces";

  leaf icmp-description {
    type string;
    description
      "This is description for icmp condition.";
  }

  leaf-list pkt-sec-icmp-type-and-code {
    type identityref {
      base icmp-type;
    }
    description
      "The security policy rule according to
      ICMP parameters.";
    reference
      "RFC 792: Internet Control Message Protocol
      RFC 8335: PROBE: A Utility for Probing Interfaces";
  }
}

container packet-security-url-category-condition {
  description
    "Condition for url category";
```

```
leaf url-category-description {
  type string;
  description
    "This is description for the condition of a URL's
    category such as SNS sites, game sites, ecommerce
    sites, company sites, and university sites.";
}

leaf-list pre-defined-category {
  type string;
  description
    "This is pre-defined-category.";
}
leaf-list user-defined-category {
  type string;
  description
    "This user-defined-category.";
}
}

container packet-security-voice-condition {
  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.";
  reference
    "RFC 3261: SIP: Session Initiation Protocol";

  leaf voice-description {
    type string;
    description
      "This is description for voice condition.";
  }

  leaf-list pkt-sec-src-voice-id {
    type string;
    description
      "The security policy rule according to
      a source voice ID for VoIP and VoLTE.";
  }
}
```

```
    leaf-list pkt-sec-dest-voice-id {
      type string;
      description
        "The security policy rule according to
         a destination voice ID for VoIP and VoLTE.";
    }

    leaf-list pkt-sec-user-agent {
      type string;
      description
        "The security policy rule according to
         an user agent for VoIP and VoLTE.";
    }
  }

  container packet-security-ddos-condition {
    description
      "Condition for DDoS attack.";

    leaf ddos-description {
      type string;
      description
        "This is description for ddos condition.";
    }

    leaf pkt-sec-alert-packet-rate {
      type uint32;
      units "pps";
      description
        "The alert rate of flood detection for
         packets per second (PPS) of an IP address.";
    }

    leaf pkt-sec-alert-flow-rate {
      type uint32;
      description
        "The alert rate of flood detection for
         flows per second of an IP address.";
    }

    leaf pkt-sec-alert-byte-rate {
      type uint32;
      units "BPS";
      description
        "The alert rate of flood detection for
         bytes per second of an IP address.";
    }
  }
}
```

```
container packet-security-payload-condition {
  description
    "Condition for packet payload";
  leaf packet-payload-description {
    type string;
    description
      "This is description for payload condition.";
  }
  leaf-list pkt-payload-content {
    type string;
    description
      "This is a condition for packet payload content.";
  }
}

container context-condition {
  description
    "Condition for context";
  leaf context-description {
    type string;
    description
      "This is description for context condition.";
  }
}

container application-condition {
  description
    "Condition for application";
  leaf application-description {
    type string;
    description
      "This is description for application condition.";
  }
  leaf-list application-object {
    type string;
    description
      "This is application object.";
  }
  leaf-list application-group {
    type string;
    description
      "This is application group.";
  }
  leaf-list application-label {
    type string;
    description
      "This is application label.";
  }
  container category {
```

```
description
  "This is application category";
list application-category {
  key "name application-subcategory";
  description
    "This is application category list";

  leaf name {
    type string;
    description
      "This is name for application category.";
  }
  leaf application-subcategory {
    type string;
    description
      "This is application subcategory.";
  }
}

}

}

container target-condition {
  description
    "Condition for target";
  leaf target-description {
    type string;
    description
      "This is description for target condition.
      Vendors can write instructions for target condition
      that vendor made";
  }
}

container device-sec-context-cond {
  description
    "The device attribute that can identify a device,
    including the device type (i.e., router, switch,
    pc, ios, or android) and the device's owner as
    well.";

  leaf-list target-device {
    type identityref {
      base target-device;
    }
    description
      "Leaf list for target devices";
  }
}
}
```

```
container users-condition {
  description
    "Condition for users";
  leaf users-description {
    type string;
    description
      "This is the description for users' condition.";
  }
  list user{
    key "user-id";
    description
      "The user (or user group) information with which
       network flow is associated: The user has many
       attributes such as name, id, password, type,
       authentication mode and so on.
       id is often used in the security policy to
       identify the user.
       Besides, an NSF is aware of the IP address of the
       user provided by a unified user management system
       via network. Based on name-address association,
       an NSF is able to enforce the security functions
       over the given user (or user group)";

    leaf user-id {
      type uint32;
      description
        "The ID of the user.";
    }
    leaf user-name {
      type string;
      description
        "The name of the user.";
    }
  }
  list group {
    key "group-id";
    description
      "The user (or user group) information with which
       network flow is associated: The user has many
       attributes such as name, id, password, type,
       authentication mode and so on.
       id is often used in the security policy to
       identify the user.
       Besides, an NSF is aware of the IP address of the
       user provided by a unified user management system
       via network. Based on name-address association,
       an NSF is able to enforce the security functions
       over the given user (or user group)";
```

```
    leaf group-id {
      type uint32;
      description
        "The ID of the group.";
    }
    leaf group-name {
      type string;
      description
        "The name of the group.";
    }
  }

  leaf security-group {
    type string;
    description
      "security-group.";
  }
}

container geography-context-condition {
  description
    "Condition for generic context";
  leaf geography-context-description {
    type string;
    description
      "This is description for generic context condition.
      Vendors can write instructions for generic context
      condition that vendor made";
  }
}

container geography-location {
  description
    "The location which network traffic flow is associated
    with. The region can be the geographical location
    such as country, province, and city,
    as well as the logical network location such as
    IP address, network section, and network domain.";

  leaf-list src-geography-location {
    type string;
    description
      "The src-geography-location is a geographical
      location mapped into an IP address. It matches the
      mapped IP address to the source IP address of the
      traffic flow.";
    reference
      "ISO 3166: Codes for the representation of
      names of countries and their subdivisions";
  }
}
```



```
    }

    leaf-list dest-geography-location {
      type string;
      description
        "The dest-geography-location is a geographical
        location mapped into an IP address. It matches the
        mapped IP address to the destination IP address of
        the traffic flow.";
      reference
        "ISO 3166: Codes for the representation of
        names of countries and their subdivisions";
    }
  }
}

container action-clause-container {
  description
    "An action is used to control and monitor aspects of
    flow-based NSFs when the event and condition clauses
    are satisfied. NSFs provide security functions by
    executing various Actions. Examples of I2NSF Actions
    include providing intrusion detection and/or protection,
    web and flow filtering, and deep packet inspection
    for packets and flows.";
  reference
    "RFC 8329: Framework for Interface to Network Security
    Functions - I2NSF Flow Security Policy Structure
    draft-ietf-i2nsf-capability-data-model-15:
    I2NSF Capability YANG Data Model - Design Principles and
    ECA Policy Model Overview";

  leaf action-clause-description {
    type string;
    description
      "Description for an action clause.";
  }

  container packet-action {
    description
      "Action for packets";
    reference
      "RFC 8329: Framework for Interface to Network Security
      Functions - I2NSF Flow Security Policy Structure
      draft-ietf-i2nsf-capability-data-model-15:
      I2NSF Capability YANG Data Model - Design Principles and
```

```
    ECA Policy Model Overview";

    leaf ingress-action {
      type identityref {
        base ingress-action;
      }
      description
        "Action: pass, drop, reject, alert, and mirror.";
    }

    leaf egress-action {
      type identityref {
        base egress-action;
      }
      description
        "Egress action: pass, drop, reject, alert, mirror,
        invoke-signaling, tunnel-encapsulation,
        forwarding, and redirection.";
    }

    leaf log-action {
      type identityref {
        base log-action;
      }
      description
        "Log action: rule log and session log";
    }
  }

  container flow-action {
    description
      "Action for flows";
    reference
      "RFC 8329: Framework for Interface to Network Security
      Functions - I2NSF Flow Security Policy Structure
      draft-ietf-i2nsf-capability-data-model-15:
      I2NSF Capability YANG Data Model - Design Principles and
      ECA Policy Model Overview";

    leaf ingress-action {
      type identityref {
        base ingress-action;
      }
      description
        "Action: pass, drop, reject, alert, and mirror.";
    }
  }
```

```
    leaf egress-action {
      type identityref {
        base egress-action;
      }
      description
        "Egress action: pass, drop, reject, alert, mirror,
        invoke-signaling, tunnel-encapsulation,
        forwarding, and redirection.";
    }

    leaf log-action {
      type identityref {
        base log-action;
      }
      description
        "Log action: rule log and session log";
    }
  }

  container advanced-action {
    description
      "If the packet needs to be additionally inspected,
      the packet is passed to advanced network
      security functions according to the profile.
      The profile means the types of NSFs where the packet
      will be forwarded in order to additionally
      inspect the packet.";
    reference
      "RFC 8329: Framework for Interface to Network Security
      Functions - Differences from ACL Data Models";

    leaf-list content-security-control {
      type identityref {
        base content-security-control;
      }
      description
        "Content-security-control is the NSFs that
        inspect the payload of the packet.
        The Profile is divided into content security
        control and attack-mitigation-control.
        Content security control: antivirus, ips, ids,
        url filtering, mail filtering, file blocking,
        file isolate, packet capture, application control,
        voip and volte.";
    }

    leaf-list attack-mitigation-control {
```

```
    type identityref {
      base attack-mitigation-control;
    }
    description
      "Attack-mitigation-control is the NSFs that weaken
      the attacks related to a denial of service
      and reconnaissance.
      The Profile is divided into content security
      control and attack-mitigation-control.
      Attack mitigation control: syn flood, udp flood,
      icmp flood, ip frag flood, ipv6 related, http flood,
      https flood, dns flood, dns amp flood, ssl ddos,
      ip sweep, port scanning, ping of death, teardrop,
      oversized icmp, tracerp.";
  }
}
}
}
container rule-group {
  description
    "This is rule group";

  list groups {
    key "group-name";
    description
      "This is a group for rules";

    leaf group-name {
      type string;
      description
        "This is a group for rules";
    }
  }

  container rule-range {
    description
      "This is a rule range.";

    leaf start-rule {
      type string;
      description
        "This is a start rule";
    }
    leaf end-rule {
      type string;
      description
        "This is a end rule";
    }
  }
}
```

```

leaf enable {
    type boolean;
    description
        "This is enable
        False is not enable.";
}
leaf description {
    type string;
    description
        "This is a description for rule-group";
}
}
}
}
}
}
<CODE ENDS>

```

Figure 5: YANG Data Module of I2NSF NSF-Facing-Interface

## 5. XML Configuration Examples of Low-Level Security Policy Rules

This section shows XML configuration examples of low-level security policy rules that are delivered from the Security Controller to NSFs over the NSF-Facing Interface. For security requirements, we assume that the NSFs (i.e., General firewall, Time-based firewall, URL filter, VoIP/VoLTE filter, and http and https flood mitigation ) described in Section Configuration Examples of [I-D.ietf-i2nsf-capability-data-model] are registered in the I2NSF framework. With the registered NSFs, we show configuration examples for security policy rules of network security functions according to the following three security requirements: (i) Block Social Networking Service (SNS) access during business hours, (ii) Block malicious VoIP/VoLTE packets coming to the company, and (iii) Mitigate http and https flood attacks on company web server.

### 5.1. Security Requirement 1: Block Social Networking Service (SNS) Access during Business Hours

This section shows a configuration example for blocking SNS access during business hours in IPv4 networks or IPv6 networks.

```
<i2nsf-security-policy
xmlns="urn:ietf:params:xml:ns:yang:ietf-i2nsf-policy-rule-for-nsf">
<system-policy>
  <system-policy-name>sns_access</system-policy-name>
  <rules>
    <rule-name>block_sns_access_during_operation_time</rule-name>
    <time-intervals>
      <absolute-time-interval>
        <start-time>09:00:00Z</start-time>
        <end-time>18:00:00Z</end-time>
      </absolute-time-interval>
    </time-intervals>
    <condition-clause-container>
      <packet-security-ipv4-condition>
        <pkt-sec-ipv4-src>
          <range-ipv4-address>
            <start-ipv4-address>192.0.2.11</start-ipv4-address>
            <end-ipv4-address>192.0.2.90</end-ipv4-address>
          </range-ipv4-address>
        </pkt-sec-ipv4-src>
      </packet-security-ipv4-condition>
    </condition-clause-container>
    <action-clause-container>
      <advanced-action>
        <content-security-control>url-filtering</content-security-control>
      </advanced-action>
    </action-clause-container>
  </rules>
</system-policy>
</i2nsf-security-policy>
```

Figure 6: Configuration XML for Time-based Firewall to Block SNS Access during Business Hours in IPv4 Networks

```
<i2nsf-security-policy
xmlns="urn:ietf:params:xml:ns:yang:ietf-i2nsf-policy-rule-for-nsf">
<system-policy>
  <system-policy-name>sns_access</system-policy-name>
  <rules>
    <rule-name>block_sns_access_during_operation_time</rule-name>
    <time-intervals>
      <absolute-time-interval>
        <start-time>09:00:00Z</start-time>
        <end-time>18:00:00Z</end-time>
      </absolute-time-interval>
    </time-intervals>
    <condition-clause-container>
      <packet-security-ipv6-condition>
        <pkt-sec-ipv6-src>
          <range-ipv6-address>
            <start-ipv6-address>2001:DB8:0:1::11</start-ipv6-address>
            <end-ipv6-address>2001:DB8:0:1::90</end-ipv6-address>
          </range-ipv6-address>
        </pkt-sec-ipv6-src>
      </packet-security-ipv6-condition>
    </condition-clause-container>
    <action-clause-container>
      <advanced-action>
        <content-security-control>url-filtering</content-security-control>
      </advanced-action>
    </action-clause-container>
  </rules>
</system-policy>
</i2nsf-security-policy>
```

Figure 7: Configuration XML for Time-based Firewall to Block SNS  
Access during Business Hours in IPv6 Networks

```
<i2nsf-security-policy
xmlns="urn:ietf:params:xml:ns:yang:ietf-i2nsf-policy-rule-for-nsf">
<system-policy>
  <system-policy-name>sns_access</system-policy-name>
  <rules>
    <rule-name>block_sns_access_during_operation_time</rule-name>
    <time-intervals>
      <absolute-time-interval>
        <start-time>09:00:00Z</start-time>
        <end-time>18:00:00Z</end-time>
      </absolute-time-interval>
    </time-intervals>
    <condition-clause-container>
      <packet-security-url-category-condition>
        <user-defined-category>SNS_1</user-defined-category>
        <user-defined-category>SNS_2</user-defined-category>
      </packet-security-url-category-condition>
    </condition-clause-container>
    <action-clause-container>
      <flow-action>
        <egress-action>drop</egress-action>
      </flow-action>
    </action-clause-container>
  </rules>
</system-policy>
</i2nsf-security-policy>
```

Figure 8: Configuration XML for Web Filter to Block SNS Access during Business Hours

Figure 6 (or Figure 7) and Figure 8 show the configuration XML documents for time-based firewall and web filter to block SNS access during business hours in IPv4 networks (or IPv6 networks). For the security requirement, two NSFs (i.e., a time-based firewall and a web filter) were used because one NSF cannot meet the security requirement. The instances of XML documents for the time-based firewall and the web filter are as follows: Note that a detailed data model for the configuration of the advanced network security function (i.e., web filter) can be defined as an extension in future.

Time-based Firewall is as follows:

1. The name of the system policy is sns\_access.
2. The name of the rule is block\_sns\_access\_during\_operation\_time.



3. The rule is operated during the business hours (i.e., from 9 a.m. to 6 p.m.).
4. The rule inspects a source IPv4 address (i.e., from 192.0.2.11 to 192.0.2.90) to inspect the outgoing packets of employees. For the case of IPv6 networks, the rule inspects a source IPv6 address (i.e., from 2001:DB8:0:1::11 to 2001:DB8:0:1::90) to inspect the outgoing packets of employees.
5. If the outgoing packets match the rules above, the time-based firewall sends the packets to url filtering for additional inspection because the time-based firewall can not inspect contents of the packets for the SNS URL.

Web Filter is as follows:

1. The name of the system policy is sns\_access.
2. The name of the rule is block\_SNS\_1\_and\_SNS\_2.
3. The rule inspects URL address to block the access packets to the SNS\_1 or the SNS\_2.
4. If the outgoing packets match the rules above, the packets are blocked.

#### 5.2. Security Requirement 2: Block Malicious VoIP/VoLTE Packets Coming to a Company

This section shows a configuration example for blocking malicious VoIP/VoLTE packets coming to a company.

```
<i2nsf-security-policy
xmlns="urn:ietf:params:xml:ns:yang:ietf-i2nsf-policy-rule-for-nsf">
<system-policy>
  <system-policy-name>voip_volte_inspection</system-policy-name>
  <rules>
    <rule-name>block_malicious_voice_id</rule-name>
    <condition-clause-container>
      <packet-security-ipv4-condition>
        <pkt-sec-ipv4-dest>
          <range-ipv4-address>
            <start-ipv4-address>192.0.2.11</start-ipv4-address>
            <end-ipv4-address>192.0.2.90</end-ipv4-address>
          </range-ipv4-address>
        </pkt-sec-ipv4-dest>
      </packet-security-ipv4-condition>
      <packet-security-tcp-condition>
        <pkt-sec-tcp-dest-port-num>
          <port-num>5060</port-num>
          <port-num>5061</port-num>
        </pkt-sec-tcp-dest-port-num>
      </packet-security-tcp-condition>
    </condition-clause-container>
    <action-clause-container>
      <advanced-action>
        <content-security-control>voip-volte</content-security-control>
      </advanced-action>
    </action-clause-container>
  </rules>
</system-policy>
</i2nsf-security-policy>
```

Figure 9: Configuration XML for General Firewall to Block Malicious VoIP/VoLTE Packets Coming to a Company

```
<i2nsf-security-policy
xmlns="urn:ietf:params:xml:ns:yang:ietf-i2nsf-policy-rule-for-nsf">
<system-policy>
  <system-policy-name>voip_volte_inspection</system-policy-name>
  <rules>
    <rule-name>block_malicious_voice_id</rule-name>
    <condition-clause-container>
      <packet-security-voice-condition>
        <pkt-sec-src-voice-id>user1@voip.malicious.example.com</pkt-sec-src-voice-id>
        <pkt-sec-src-voice-id>user2@voip.malicious.example.com</pkt-sec-src-voice-id>
      </packet-security-voice-condition>
    </condition-clause-container>
    <action-clause-container>
      <flow-action>
        <ingress-action>drop</ingress-action>
      </flow-action>
    </action-clause-container>
  </rules>
</system-policy>
</i2nsf-security-policy>
```

Figure 10: Configuration XML for VoIP/VoLTE Filter to Block Malicious VoIP/VoLTE Packets Coming to a Company

Figure 9 and Figure 10 show the configuration XML documents for general firewall and VoIP/VoLTE filter to block malicious VoIP/VoLTE packets coming to a company. For the security requirement, two NSFs (i.e., a general firewall and a VoIP/VoLTE filter) were used because one NSF can not meet the security requirement. The instances of XML documents for the general firewall and the VoIP/VoLTE filter are as follows: Note that a detailed data model for the configuration of the advanced network security function (i.e., VoIP/VoLTE filter) can be described as an extension in future.

General Firewall is as follows:

1. The name of the system policy is `voip_volte_inspection`.
2. The name of the rule is `block_malicious_voip_volte_packets`.
3. The rule inspects a destination IPv4 address (i.e., from 192.0.2.11 to 192.0.2.90) to inspect the packets coming into the company.
4. The rule inspects a port number (i.e., 5060 and 5061) to inspect VoIP/VoLTE packet.

5. If the incoming packets match the rules above, the general firewall sends the packets to VoIP/VoLTE filter for additional inspection because the general firewall can not inspect contents of the VoIP/VoLTE packets.

VoIP/VoLTE Filter is as follows:

1. The name of the system policy is `malicious_voice_id`.
2. The name of the rule is `block_malicious_voice_id`.
3. The rule inspects the voice id of the VoIP/VoLTE packets to block the malicious VoIP/VoLTE packets (i.e., `user1@voip.malicious.example.com` and `user2@voip.malicious.example.com`).
4. If the incoming packets match the rules above, the packets are blocked.

### 5.3. Security Requirement 3: Mitigate HTTP and HTTPS Flood Attacks on a Company Web Server

This section shows a configuration example for mitigating http and https flood attacks on a company web server.

```
<i2nsf-security-policy
xmlns="urn:ietf:params:xml:ns:yang:ietf-i2nsf-policy-rule-for-nsf">
<system-policy>
  <system-policy-name>flood_attack_mitigation</system-policy-name>
  <rules>
    <rule-name>mitigate_http_and_https_flood_attack</rule-name>
    <condition-clause-container>
      <packet-security-ipv4-condition>
        <pkt-sec-ipv4-dest>
          <ipv4-address>
            <ipv4>192.0.2.11</ipv4>
          </ipv4-address>
        </pkt-sec-ipv4-dest>
      </packet-security-ipv4-condition>
      <packet-security-tcp-condition>
        <pkt-sec-tcp-dest-port-num>
          <port-num>80</port-num>
          <port-num>443</port-num>
        </pkt-sec-tcp-dest-port-num>
      </packet-security-tcp-condition>
    </condition-clause-container>
    <action-clause-container>
      <advanced-action>
        <attack-mitigation-control>http-and-https-flood
      </attack-mitigation-control>
    </advanced-action>
  </action-clause-container>
</rules>
</system-policy>
</i2nsf-security-policy>
```

Figure 11: Configuration XML for General Firewall to Mitigate HTTP and HTTPS Flood Attacks on a Company Web Server

```
<i2nsf-security-policy
xmlns="urn:ietf:params:xml:ns:yang:ietf-i2nsf-policy-rule-for-nsf">
<system-policy>
  <system-policy-name>flood_attack_mitigation</system-policy-name>
  <rules>
    <rule-name>mitigate_http_and_https_flood_attack</rule-name>
    <condition-clause-container>
      <packet-security-ddos-condition>
        <pkt-sec-alert-packet-rate>100</pkt-sec-alert-packet-rate>
      </packet-security-ddos-condition>
    </condition-clause-container>
    <action-clause-container>
      <flow-action>
        <ingress-action>drop</ingress-action>
      </flow-action>
    </action-clause-container>
  </rules>
</system-policy>
</i2nsf-security-policy>
```

Figure 12: Configuration XML for HTTP and HTTPS Flood Attack Mitigation to Mitigate HTTP and HTTPS Flood Attacks on a Company Web Server

Figure 11 and Figure 12 show the configuration XML documents for general firewall and http and https flood attack mitigation to mitigate http and https flood attacks on a company web server. For the security requirement, two NSFs (i.e., a general firewall and a http and https flood attack mitigation) were used because one NSF can not meet the security requirement. The instances of XML documents for the general firewall and http and https flood attack mitigation are as follows: Note that a detailed data model for the configuration of the advanced network security function (i.e., http and https flood attack mitigation) can be defined as an extension in future.

General Firewall is as follows:

1. The name of the system policy is flood\_attack\_mitigation.
2. The name of the rule is mitigate\_http\_and\_https\_flood\_attack.
3. The rule inspects a destination IPv4 address (i.e., 192.0.2.11) to inspect the access packets coming into the company web server.
4. The rule inspects a port number (i.e., 80 and 443) to inspect http and https packet.

5. If the packets match the rules above, the general firewall sends the packets to http and https flood attack mitigation for additional inspection because the general firewall can not control the amount of packets for http and https packets.

HTTP and HTTPS Flood Attack Mitigation is as follows:

1. The name of the system policy is `http_and_https_flood_attack_mitigation`.
2. The name of the rule is `100_per_second`.
3. The rule controls the http and https packets according to the amount of incoming packets.
4. If the incoming packets match the rules above, the packets are blocked.

## 6. IANA Considerations

This document requests IANA to register the following URI in the "IETF XML Registry" [[RFC3688](#)]:

URI: `urn:ietf:params:xml:ns:yang:ietf-i2nsf-policy-rule-for-nsf`

Registrant Contact: The IESG.

XML: N/A; the requested URI is an XML namespace.

This document requests IANA to register the following YANG module in the "YANG Module Names" registry [[RFC7950](#)][[RFC8525](#)].

name: `ietf-i2nsf-policy-rule-for-nsf`

namespace: `urn:ietf:params:xml:ns:yang:ietf-i2nsf-policy-rule-for-nsf`

prefix: `nsfintf`

reference: RFC XXXX

## 7. Security Considerations

The YANG module specified in this document defines a data schema designed to be accessed through network management protocols such as NETCONF [[RFC6241](#)] or RESTCONF [[RFC8040](#)]. The lowest NETCONF layer is the secure transport layer, and the required secure transport is Secure Shell (SSH) [[RFC6242](#)]. The lowest RESTCONF layer is HTTPS, and the required secure transport is TLS [[RFC8446](#)].

The NETCONF access control model [[RFC8341](#)] provides a means of restricting access to specific NETCONF or RESTCONF users to a

preconfigured subset of all available NETCONF or RESTCONF protocol operations and content.

There are a number of data nodes defined in this YANG module that are writable/creatable/deletable (i.e., config true, which is the default). These data nodes may be considered sensitive or vulnerable in some network environments. Write operations (e.g., edit-config) to these data nodes without proper protection can have a negative effect on network operations. These are the subtrees and data nodes and their sensitivity/vulnerability:

- o ietf-i2nsf-policy-rule-for-nsf: Writing to almost any element of this YANG module would directly impact on the configuration of NSFs, e.g., completely turning off security monitoring and mitigation capabilities; altering the scope of this monitoring and mitigation; creating an overwhelming logging volume to overwhelm downstream analytics or storage capacity; creating logging patterns which are confusing; or rendering useless trained statistics or artificial intelligence models.

Some of the readable data nodes in this YANG module may be considered sensitive or vulnerable in some network environments. It is thus important to control read access (e.g., via get, get-config, or notification) to these data nodes. These are the subtrees and data nodes and their sensitivity/vulnerability:

- o ietf-i2nsf-policy-rule-for-nsf: The attacker may gather the security policy information of any target NSFs and misuse the security policy information for subsequent attacks.

In this YANG data module, note that the identity information of users can be exchanged for security policy configuration based on a user's information. This implied that to improve the network security there is a tradeoff between a user's information privacy and network security. For container users-conditions in this YANG data module, the identity information of users can be exchanged between Security Controller and an NSF for security policy configuration based on users' information. Thus, for this exchange of the identity information of users, there is a proportional relationship between the release level of a user's privacy information and the network security strength of an NSF.

## 8. Acknowledgments

This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea MSIT (Ministry of Science and ICT) (R-20160222-002755, Cloud based Security Intelligence Technology Development for the Customized



Security Service Provisioning). This work was supported in part by the IITP (2020-0-00395, Standard Development of Blockchain based Network Management Automation Technology).

## 9. Contributors

This document is made by the group effort of I2NSF working group. Many people actively contributed to this document, such as Acee Lindem and Roman Danyliw. The authors sincerely appreciate their contributions.

The following are co-authors of this document:

Patrick Lingga  
Department of Computer Science and Engineering  
Sungkyunkwan University  
2066 Seo-ro Jangan-gu  
Suwon, Gyeonggi-do 16419  
Republic of Korea

EMail: [patricklink@skku.edu](mailto:patricklink@skku.edu)

Hyounghick Kim  
Department of Computer Science and Engineering  
Sungkyunkwan University  
2066 Seo-ro Jangan-gu  
Suwon, Gyeonggi-do 16419  
Republic of Korea

EMail: [hyoung@skku.edu](mailto:hyoung@skku.edu)

Daeyoung Hyun  
Department of Computer Science and Engineering  
Sungkyunkwan University  
2066 Seo-ro Jangan-gu  
Suwon, Gyeonggi-do 16419  
Republic of Korea

EMail: [dyhyun@skku.edu](mailto:dyhyun@skku.edu)

Dongjin Hong  
Department of Electronic, Electrical and Computer Engineering  
Sungkyunkwan University  
2066 Seo-ro Jangan-gu  
Suwon, Gyeonggi-do 16419

Republic of Korea

EMail: dong.jin@skku.edu

Liang Xia  
Huawei  
101 Software Avenue  
Nanjing, Jiangsu 210012  
China

EMail: Frank.Xialiang@huawei.com

Tae-Jin Ahn  
Korea Telecom  
70 Yuseong-Ro, Yuseong-Gu  
Daejeon, 305-811  
Republic of Korea

EMail: taejin.ahn@kt.com

Se-Hui Lee  
Korea Telecom  
70 Yuseong-Ro, Yuseong-Gu  
Daejeon, 305-811  
Republic of Korea

EMail: sehuilee@kt.com

## 10. References

### 10.1. Normative References

- [I-D.ietf-i2nsf-capability-data-model]  
Hares, S., Jeong, J., Kim, J., Moskowitz, R., and Q. Lin,  
"I2NSF Capability YANG Data Model", [draft-ietf-i2nsf-capability-data-model-15](#) (work in progress), January 2021.
- [I-D.ietf-i2nsf-sdn-ipsec-flow-protection]  
Marin-Lopez, R., Lopez-Millan, G., and F. Pereniguez-Garcia, "Software-Defined Networking (SDN)-based IPsec Flow Protection", [draft-ietf-i2nsf-sdn-ipsec-flow-protection-12](#) (work in progress), October 2020.

- [RFC0768] Postel, J., "User Datagram Protocol", STD 6, [RFC 768](#), DOI 10.17487/RFC0768, August 1980, <<https://www.rfc-editor.org/info/rfc768>>.
- [RFC0791] Postel, J., "Internet Protocol", STD 5, [RFC 791](#), DOI 10.17487/RFC0791, September 1981, <<https://www.rfc-editor.org/info/rfc791>>.
- [RFC0792] Postel, J., "Internet Control Message Protocol", STD 5, [RFC 792](#), DOI 10.17487/RFC0792, September 1981, <<https://www.rfc-editor.org/info/rfc792>>.
- [RFC0793] Postel, J., "Transmission Control Protocol", STD 7, [RFC 793](#), DOI 10.17487/RFC0793, September 1981, <<https://www.rfc-editor.org/info/rfc793>>.
- [RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", [RFC 3261](#), DOI 10.17487/RFC3261, June 2002, <<https://www.rfc-editor.org/info/rfc3261>>.
- [RFC3688] Mealling, M., "The IETF XML Registry", [BCP 81](#), [RFC 3688](#), DOI 10.17487/RFC3688, January 2004, <<https://www.rfc-editor.org/info/rfc3688>>.
- [RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, [RFC 4443](#), DOI 10.17487/RFC4443, March 2006, <<https://www.rfc-editor.org/info/rfc4443>>.
- [RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", [RFC 6020](#), DOI 10.17487/RFC6020, October 2010, <<https://www.rfc-editor.org/info/rfc6020>>.
- [RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", [RFC 6241](#), DOI 10.17487/RFC6241, June 2011, <<https://www.rfc-editor.org/info/rfc6241>>.
- [RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", [RFC 6242](#), DOI 10.17487/RFC6242, June 2011, <<https://www.rfc-editor.org/info/rfc6242>>.

- [RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types", [RFC 6991](#), DOI 10.17487/RFC6991, July 2013, <<https://www.rfc-editor.org/info/rfc6991>>.
- [RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", [RFC 7950](#), DOI 10.17487/RFC7950, August 2016, <<https://www.rfc-editor.org/info/rfc7950>>.
- [RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", [RFC 8040](#), DOI 10.17487/RFC8040, January 2017, <<https://www.rfc-editor.org/info/rfc8040>>.
- [RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, [RFC 8200](#), DOI 10.17487/RFC8200, July 2017, <<https://www.rfc-editor.org/info/rfc8200>>.
- [RFC8335] Bonica, R., Thomas, R., Linkova, J., Lenart, C., and M. Boucadair, "PROBE: A Utility for Probing Interfaces", [RFC 8335](#), DOI 10.17487/RFC8335, February 2018, <<https://www.rfc-editor.org/info/rfc8335>>.
- [RFC8340] Bjorklund, M. and L. Berger, Ed., "YANG Tree Diagrams", [BCP 215](#), [RFC 8340](#), DOI 10.17487/RFC8340, March 2018, <<https://www.rfc-editor.org/info/rfc8340>>.
- [RFC8341] Bierman, A. and M. Bjorklund, "Network Configuration Access Control Model", STD 91, [RFC 8341](#), DOI 10.17487/RFC8341, March 2018, <<https://www.rfc-editor.org/info/rfc8341>>.
- [RFC8344] Bjorklund, M., "A YANG Data Model for IP Management", [RFC 8344](#), DOI 10.17487/RFC8344, March 2018, <<https://www.rfc-editor.org/info/rfc8344>>.
- [RFC8407] Bierman, A., "Guidelines for Authors and Reviewers of Documents Containing YANG Data Models", [BCP 216](#), [RFC 8407](#), DOI 10.17487/RFC8407, October 2018, <<https://www.rfc-editor.org/info/rfc8407>>.
- [RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", [RFC 8446](#), DOI 10.17487/RFC8446, August 2018, <<https://www.rfc-editor.org/info/rfc8446>>.
- [RFC8525] Bierman, A., Bjorklund, M., Schoenwaelder, J., Watsen, K., and R. Wilton, "YANG Library", [RFC 8525](#), DOI 10.17487/RFC8525, March 2019, <<https://www.rfc-editor.org/info/rfc8525>>.

## 10.2. Informative References

- [I-D.ietf-i2nsf-nsf-monitoring-data-model]  
Jeong, J., Lingga, P., Hares, S., Xia, L., and H. Birkholz, "I2NSF NSF Monitoring YANG Data Model", [draft-ietf-i2nsf-nsf-monitoring-data-model-04](#) (work in progress), September 2020.
- [IANA-Protocol-Numbers]  
"Assigned Internet Protocol Numbers", Available: <https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>, January 2021.
- [ISO-Country-Codes]  
"Codes for the representation of names of countries and their subdivisions", ISO 3166, September 2018.
- [RFC8329] Lopez, D., Lopez, E., Dunbar, L., Strassner, J., and R. Kumar, "Framework for Interface to Network Security Functions", [RFC 8329](#), DOI 10.17487/RFC8329, February 2018, <<https://www.rfc-editor.org/info/rfc8329>>.

### Authors' Addresses

Jinyong (Tim) Kim (editor)  
Department of Electronic, Electrical and Computer Engineering  
Sungkyunkwan University  
2066 Seobu-Ro, Jangan-Gu  
Suwon, Gyeonggi-Do 16419  
Republic of Korea

Phone: +82 10 8273 0930  
EMail: [timkim@skku.edu](mailto:timkim@skku.edu)

Jaehoon (Paul) Jeong (editor)  
Department of Computer Science and Engineering  
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](mailto:pauljeong@skku.edu)  
URI: <http://iotlab.skku.edu/people-jaehoon-jeong.php>

Jung-Soo Park  
Electronics and Telecommunications Research Institute  
218 Gajeong-Ro, Yuseong-Gu  
Daejeon 34129  
Republic of Korea

Phone: +82 42 860 6514  
EMail: pjs@etri.re.kr

Susan Hares  
Huawei  
7453 Hickory Hill  
Saline, MI 48176  
USA

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

Qiushi Lin  
Huawei  
Huawei Industrial Base  
Shenzhen, Guangdong 518129  
China

EMail: linqiushi@huawei.com