Information Model of Interface to Network Security Functions Capability Interface

draft-xia-i2nsf-capability-interface-im-06

Liang Xia	Huawei
John Strassner	Huawei
Kepeng Li	Alibaba
DaCheng Zhang	Alibaba
Edward Lopez	Fortinet
Nicolas BOUTHORS	Qosmos
Luyuan Fang	Microsoft

June 2016 Berlin

Capability Interface

- Recall that a Capability
  - Defines a set of features that are available from a managed entity (from draft-ietf-i2nsf-terminology-01)
  - Therefore, there should be no difference in defining consumer vs provider Capabilities
  - There IS a difference in how they are used

Monitoring Part of I2NSF Architecture

Consumer Interface

(Client-Facing Interface)

For clients or App Gateway to express and monitor security policies for their specific flows. Also enables Controllers to express Capabilities to the Client.

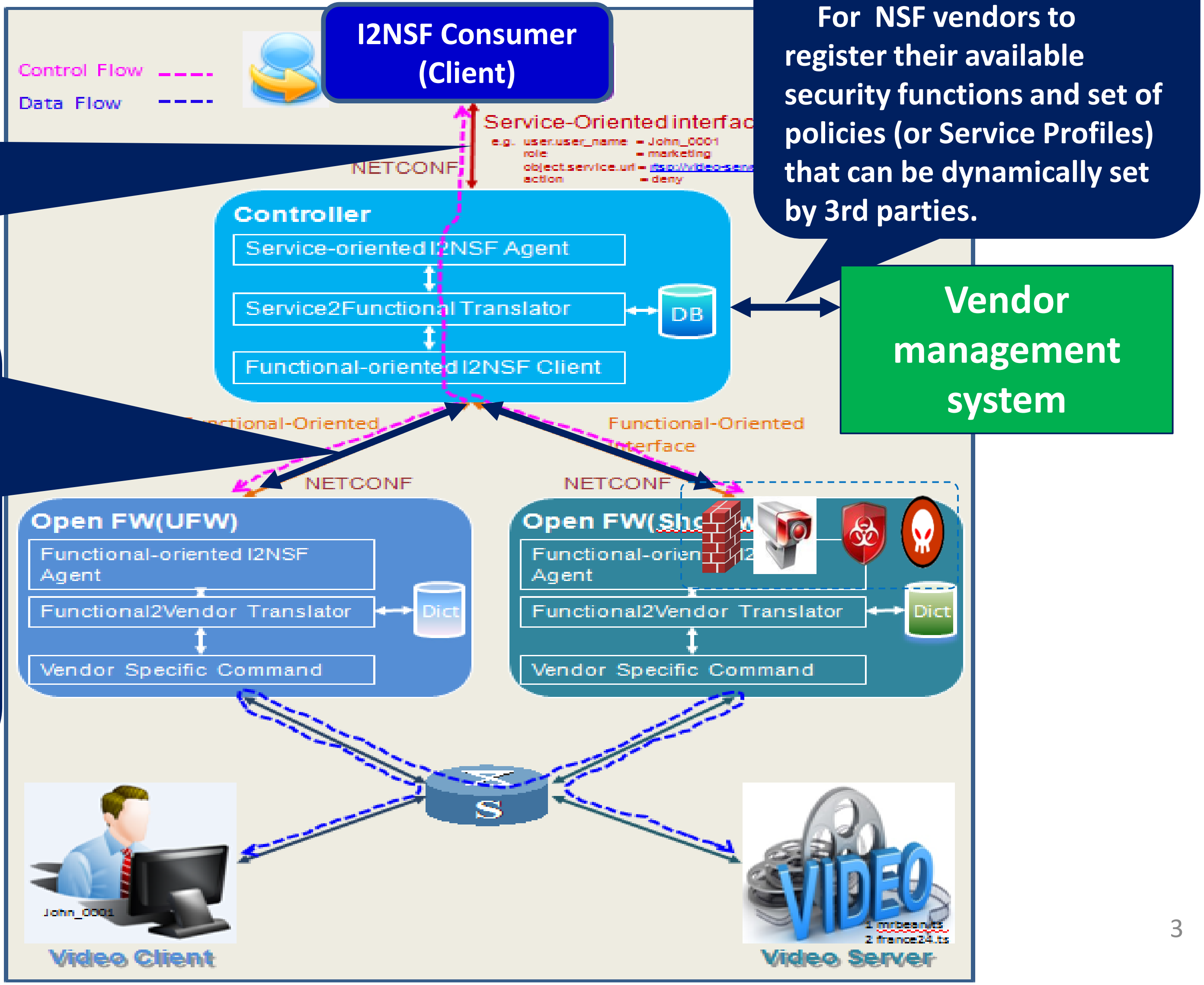
Provider Interface

(NSF-Facing Interface)

For controller to define explicit rules for individual NSFs to treat packets, as well as methods to monitor the execution status of those functions. Also enables NSFs to express Capabilities they support to Controller.

NSF Registration

For NSF vendors to register their available security functions and set of policies (or Service Profiles) that can be dynamically set by 3rd parties.



I2NSF Consumer (Client)
Control Flow
Data Flow
Service-Oriented interfac
e.g. user.user_name = John_0001
role = marketing
object.service.url = http://video-serv
action = deny
NETCONF
Controller
Service-oriented I2NSF Agent
Service2Functional Translator
DB
Functional-oriented I2NSF Client
Vendor management system
Functional-Oriented
Functional-Oriented Interface
NETCONF
NETCONF
Open FW(UFW)
Functional-oriented I2NSF Agent
Functional2Vendor Translator
Dict
Vendor Specific Command
Open FW(Sho
Functional-orien I2 Agent
Functional2Vendor Translator
Dict
Vendor Specific Command
S
John_0001
Video Client
VIDEO
1 mrbean.ts
2 france24.ts
Video Server

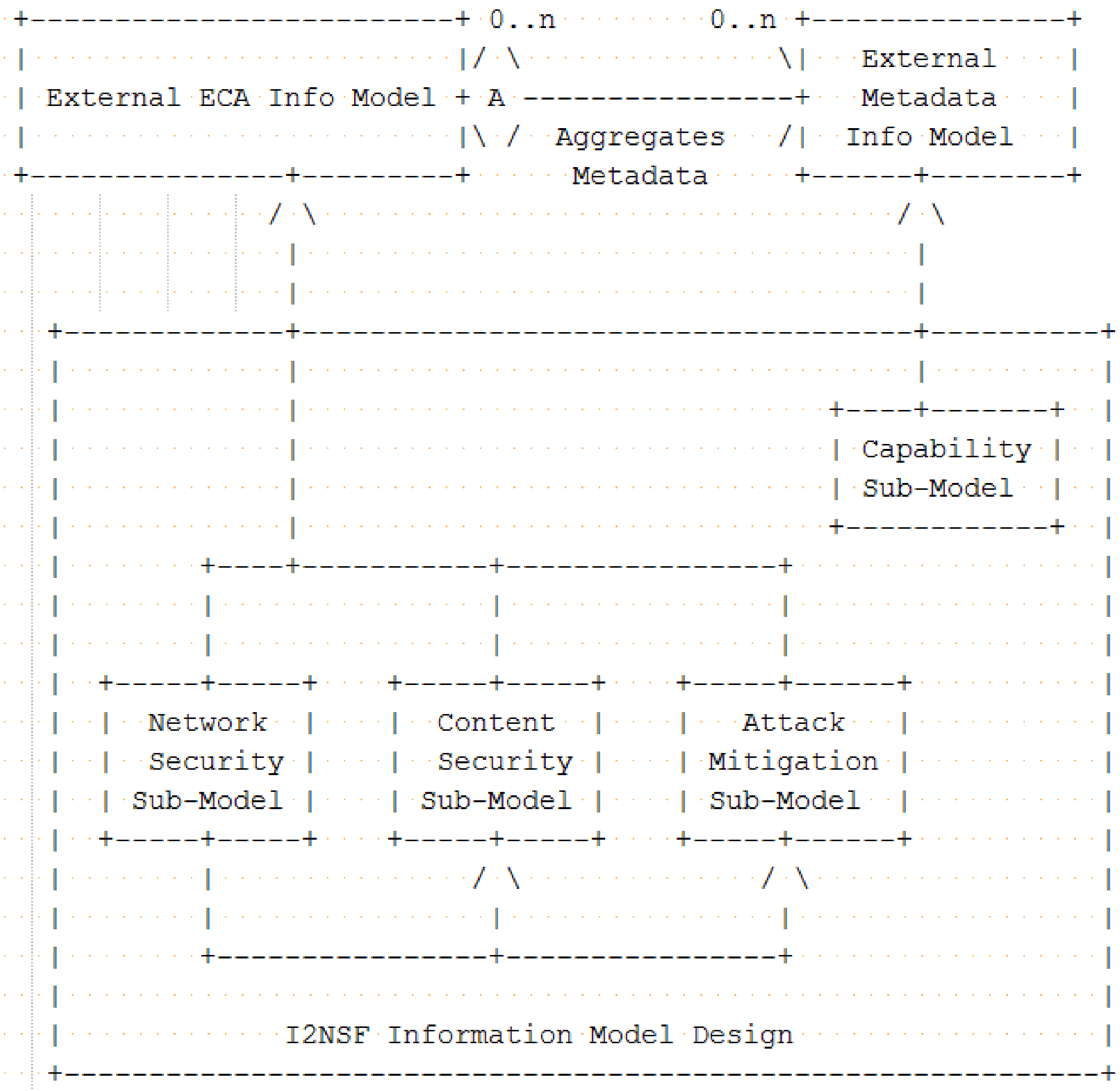
From -05 to -06

- Redesigned the I2NSF ECA information model:
  - Introduce a generic Info Model for Security ECA Policy Rules, Security Policy Metadata, and enabled it to subclass from an externally defined information model;
  - Specify the I2NSF capability Info Model by inheriting and extending from generic ECA IM;
  - Introduce software pattern to define behavior of Security Policies
  - Specify the aggregation and association relation among the I2NSF sub-models.
- Add more details by defining sub-classes of the “Event”, “Condition”, “Action” classes for Network Security sub-model;
- Make a lot of editorial text changes;
- Have More co-authors joining.

3 Categories of Security Capabilities

1. Network Security:
   - Inspecting and processing network packets/flows;
   - Contextually inspects packet contents, and decide on actions to take;
   - Use an “Event-Condition-Action" paradigm to construct the security rule;
   - ECA rule is a generic container; specific usage is a function of ECA components and metadata
2. Content Security:
   - Detect malicious contents in application layer (e.g., file, url, data block)
   - Apply security profiles or signature files with standardized input/output parameters;
   - Possibly need a standardized interface for updating its intelligence: signature, and algorithm.
3. Attack Mitigation:
   - Detect and mitigate various types of network attacks (e.g., DDoS attacks, single-packet attacks, IPv6 related attack);
   - A standard interface for the security controller to choose and customize the given security capability.

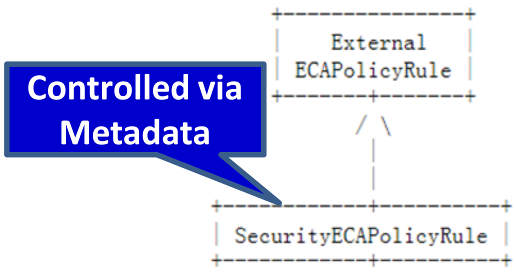
The Overall I2NSF IM Design



```
+-------------------------+ 0..n         0..n +---------------+
|                         |/ \               \|   External    |
| External ECA Info Model + A ----------------+   Metadata    |
|                         |\ /  Aggregates   /|  Info Model   |
+---------------+---------+      Metadata     +------+--------+
               / \                                  / \
                |                                    |
                |                                    |
  +-------------+------------------------------------+----------+
  |             |                                    |          |
  |             |                               +----+-------+  |
  |             |                               | Capability |  |
  |             |                               | Sub-Model  |  |
  |             |                               +------------+  |
  |        +----+-----------+----------------+                  |
  |        |                |                |                  |
  |        |                |                |                  |
  |  +-----+-----+    +-----+-----+    +-----+------+           |
  |  |  Network  |    |  Content  |    |   Attack   |           |
  |  |  Security |    |  Security |    | Mitigation |           |
  |  | Sub-Model |    | Sub-Model |    | Sub-Model  |           |
  |  +-----+-----+    +-----+-----+    +-----+------+           |
  |        |               / \              / \                 |
  |        |                |                |                  |
  |        +----------------+----------------+                  |
  |                                                             |
  |             I2NSF Information Model Design                  |
  +-------------------------------------------------------------+
```

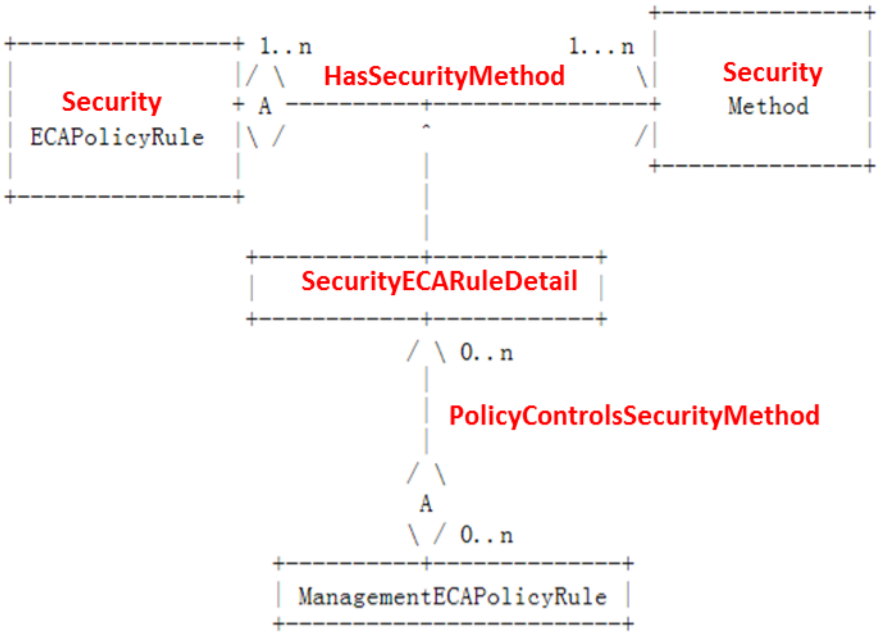
Figure 1. The Overall I2NSF Information Model Design

Network Security Info Sub-Model ECAPolicyRule Extensions – Next Version



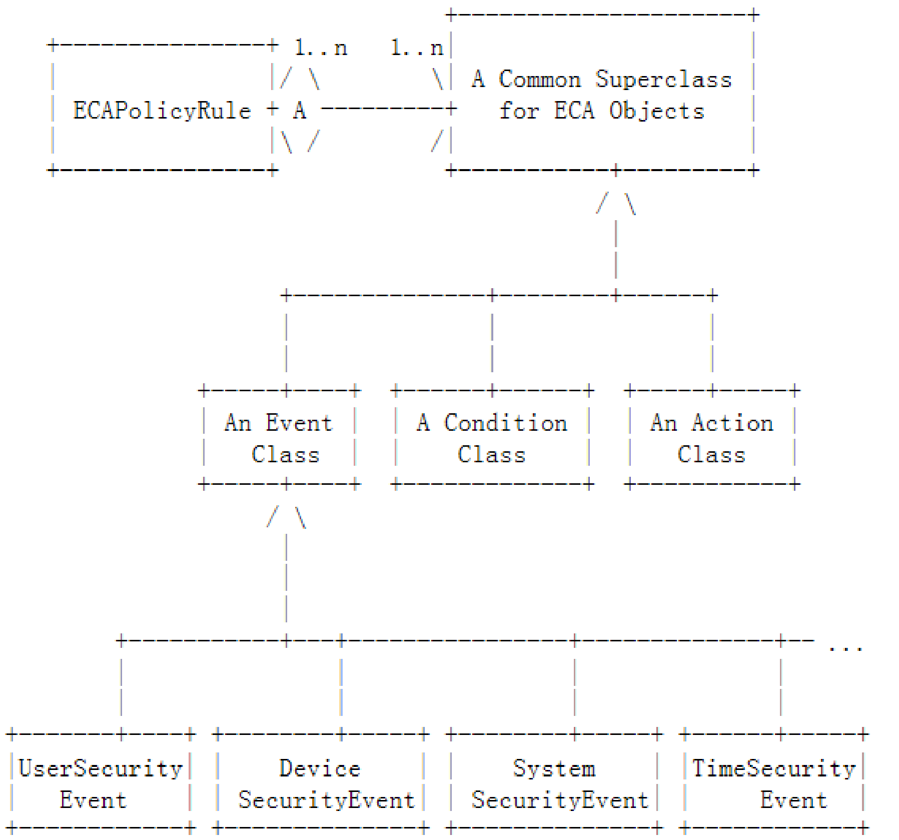
Controlled via Metadata

```
+----------------+
|    External    |
|  ECAPolicyRule |
+-------+--------+
       / \
        |
        |
+-------+---------------+
| SecurityECAPolicyRule |
+-------+---------------+
```



```
                                                  +---------------+
+---------------+ 1..n                      1...n |               |
|               |/ \   HasSecurityMethod       \|   Security    |
|   Security    + A ----------------+-----------+    Method     |
| ECAPolicyRule |\ /                ^          /|               |
|               |                   |           +---------------+
+---------------+                   |
                                    |
                       +------------+-------------+
                       |  SecurityECARuleDetail   |
                       +------------+-------------+
                                   / \ 0..n
                                    |
                                    |  PolicyControlsSecurityMethod
                                    |
                                   / \
                                    A
                                   \ / 0..n
                          +---------+---------------+
                          | ManagementECAPolicyRule |
                          +-------------------------+
```

Event sub-class for Network Security



```
                                +---------------------+
+---------------+ 1..n   1..n|                     |
|               |/ \         \| A Common Superclass |
| ECAPolicyRule + A ---------+   for ECA Objects   |
|               |\ /         /|                     |
+---------------+            +----------+----------+
                                        / \
                                         |
                                         |
                    +--------------+--------+-------+
                    |              |                |
                    |              |                |
              +-----+-----+  +-----+------+  +-----+-----+
              | An Event  |  | A Condition |  | An Action |
              |   Class   |  |    Class    |  |   Class   |
              +-----+-----+  +-------------+  +-----------+
                   / \
                    |
                    |
                    |
    +----------+---+--------------+-------------+-- ...
    |              |                 |              |
    |              |                 |              |
+-----+-----+ +-----+------+ +-------+------+ +-----+-----+
|UserSecurity| |    Device    | |    System    | |TimeSecurity|
|   Event    | |SecurityEvent| |SecurityEvent| |   Event    |
+------------+ +--------------+ +--------------+ +------------+
```

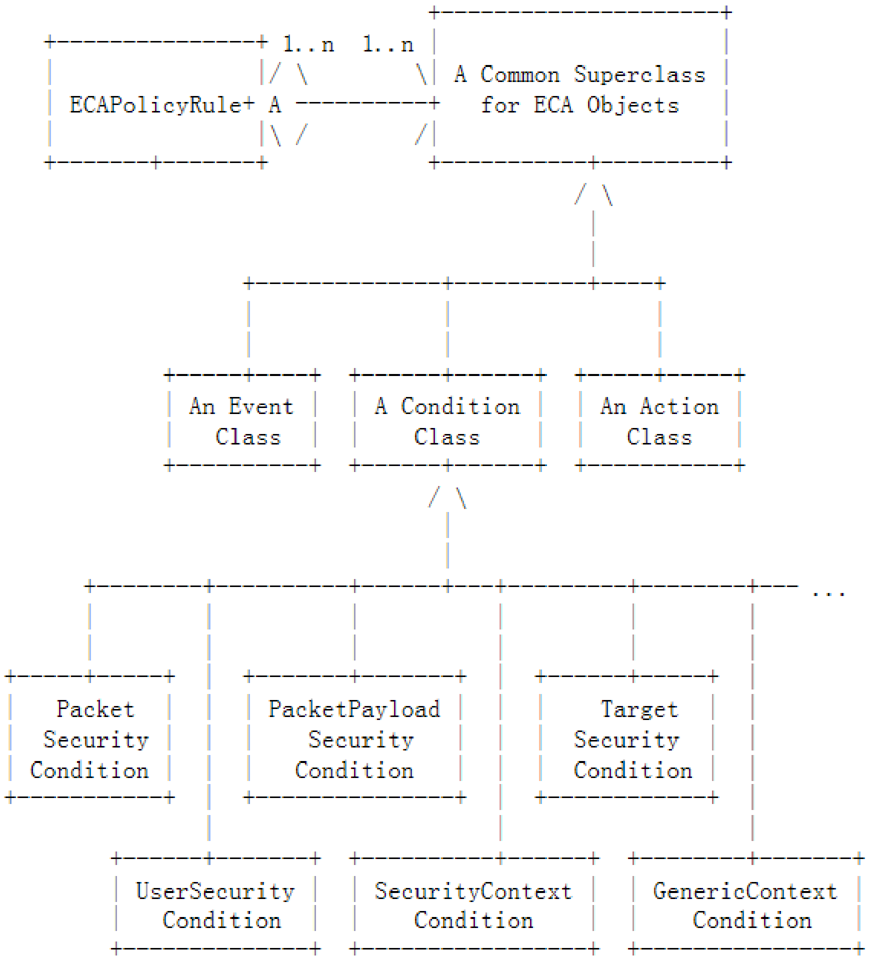
Figure 10. Network Security Info Sub-Model Event Class Extensions

Example:

UserSecurityEvent has the attributes as below:

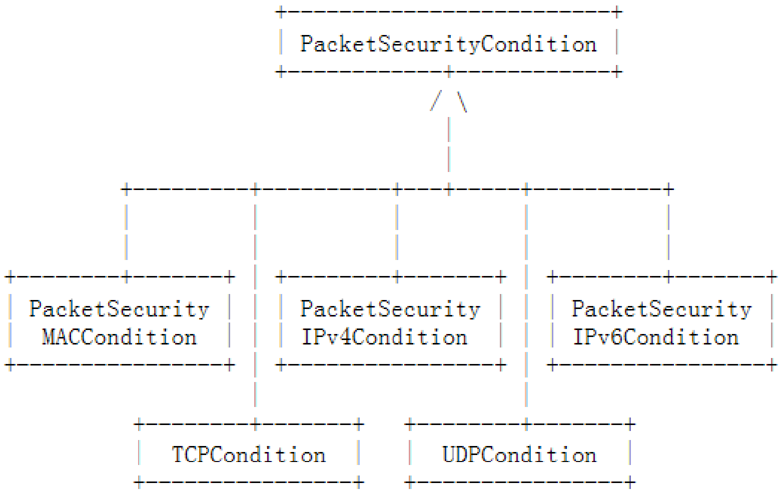
- **usrSecEventContent**: string;
- **usrSecEventFormat**
  - 0: unknown
  - 1: GUID (Generic Unique IDentifier)
  - 2: UUID (Universal Unique IDentifier)
  - 3: URI (Uniform Resource Identifier)
  - 4: FQDN (Fully Qualified Domain Name)
  - 5: FQPN (Fully Qualified Path Name)
- **usrSecEventType**
  - 0: unknown
  - 1: new user created
  - 2: new user group created
  - 3: user deleted
  - 4: user group deleted
  - 5: user logon
  - 6: user logoff
  - 7: user access request
  - 8: user access granted
  - 9: user access violation

Condition sub-class for Network Security



```
                               +---------------------+
+---------------+ 1..n  1..n   |                     |
|               |/ \         \| A Common Superclass |
| ECAPolicyRule+ A ----------+   for ECA Objects   |
|               |\ /         /|                     |
+-------+-------+              +----------+----------+
                                         / \
                                          |
                                          |
                  +--------------+-----------+----+
                  |              |                |
                  |              |                |
             +-----+-----+  +------+------+  +-----+-----+
             | An Event  |  | A Condition |  | An Action |
             |   Class   |  |    Class    |  |   Class   |
             +-----------+  +------+------+  +-----------+
                                  / \
                                   |
                                   |
     +--------+----------+------+----+---------+--------+--- ...
     |        |          |           |         |        |
     |        |          |           |         |        |
+-----+-----+ |  +--------+-------+  |  +-----+-----+   |
|  Packet   | |  | PacketPayload  |  |  |   Target  |   |
|  Security | |  |    Security    |  |  |  Security |   |
| Condition | |  |   Condition    |  |  | Condition |   |
+-----------+ |  +----------------+  |  +-----------+   |
              |                      |                  |
       +------+-------+   +----------+-------+   +--------+-------+
       | UserSecurity |   | SecurityContext  |   | GenericContext |
       |   Condition  |   |    Condition     |   |    Condition   |
       +--------------+   +------------------+   +----------------+
```

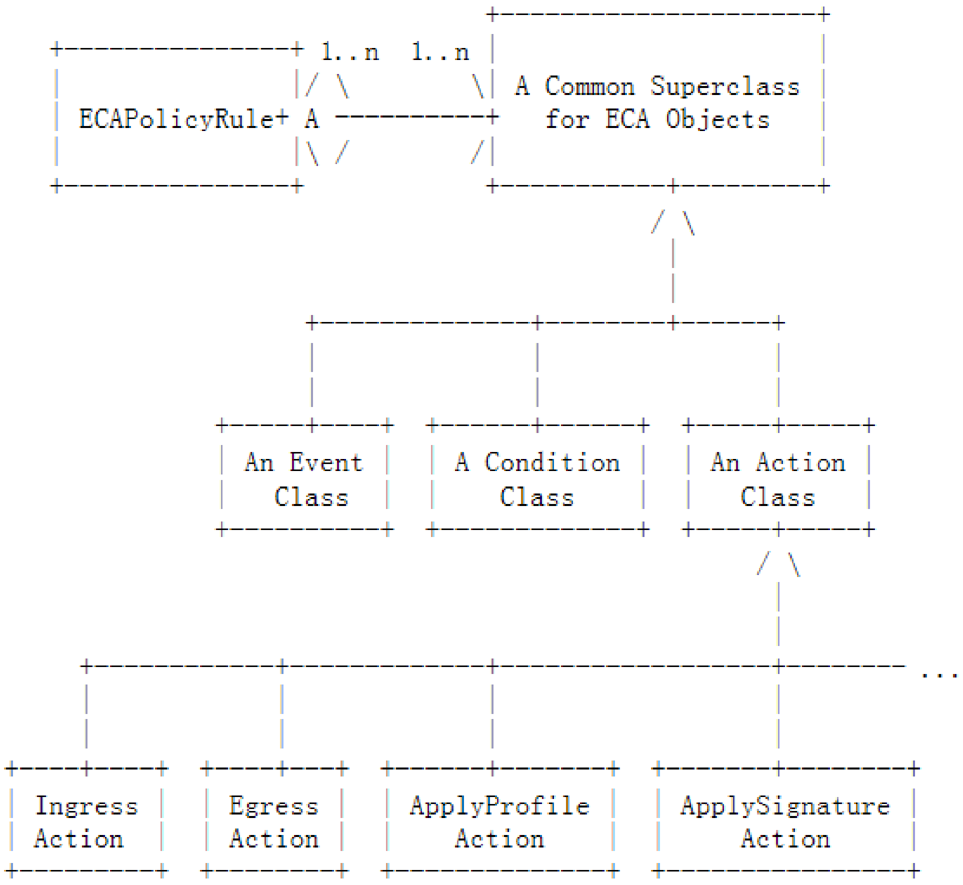
Figure 11. Network Security Info Sub-Model Condition Class Extensions



```
                   +-------------------------+
                   | PacketSecurityCondition |
                   +------------+------------+
                               / \
                                |
                                |
       +---------+----------+---+------+---------+
       |         |          |          |         |
       |         |          |          |         |
+--------+-------+ | +--------+-------+ | +--------+-------+
| PacketSecurity | | | PacketSecurity | | | PacketSecurity |
|  MACCondition  | | | IPv4Condition  | | | IPv6Condition  |
+----------------+ | +----------------+ | +----------------+
                   |                    |
          +--------+-------+   +--------+-------+
          |  TCPCondition  |   |  UDPCondition  |
          +----------------+   +----------------+
```

Figure 12. Network Security Info Sub-Model PacketSecurityCondition Class Extensions

Action sub-class for Network Security

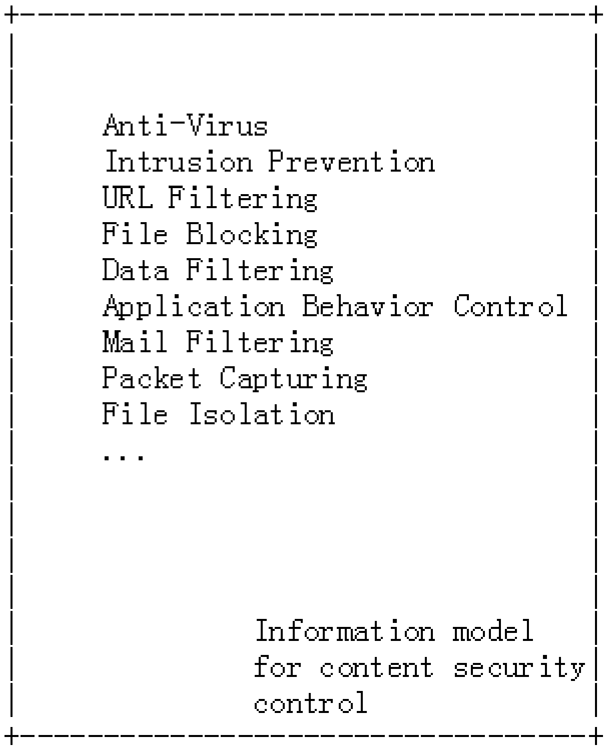


```
                              +----------------------+
 +---------------+ 1..n  1..n |                      |
 |               |/ \        \| A Common Superclass  |
 | ECAPolicyRule+ A ----------+   for ECA Objects    |
 |               |\ /        /|                      |
 +---------------+            +-----------+----------+
                                         / \
                                          |
                                          |
                 +------------+-----------+------+
                 |            |                  |
                 |            |                  |
           +-----+----+ +-----+-------+    +-----+-----+
           | An Event | | A Condition |    | An Action |
           |  Class   | |    Class    |    |   Class   |
           +----------+ +-------------+    +-----+-----+
                                                / \
                                                 |
                                                 |
    +----------+-----------+----------------+---------- ...
    |          |           |                |
    |          |           |                |
+---+-----+ +--+----+ +----+--------+ +-----+------------+
| Ingress | | Egress| | ApplyProfile| | ApplySignature   |
| Action  | | Action| |    Action   | |     Action       |
+---------+ +-------+ +-------------+ +------------------+
```

Figure 13. Network Security Info Sub-Model Action Extensions

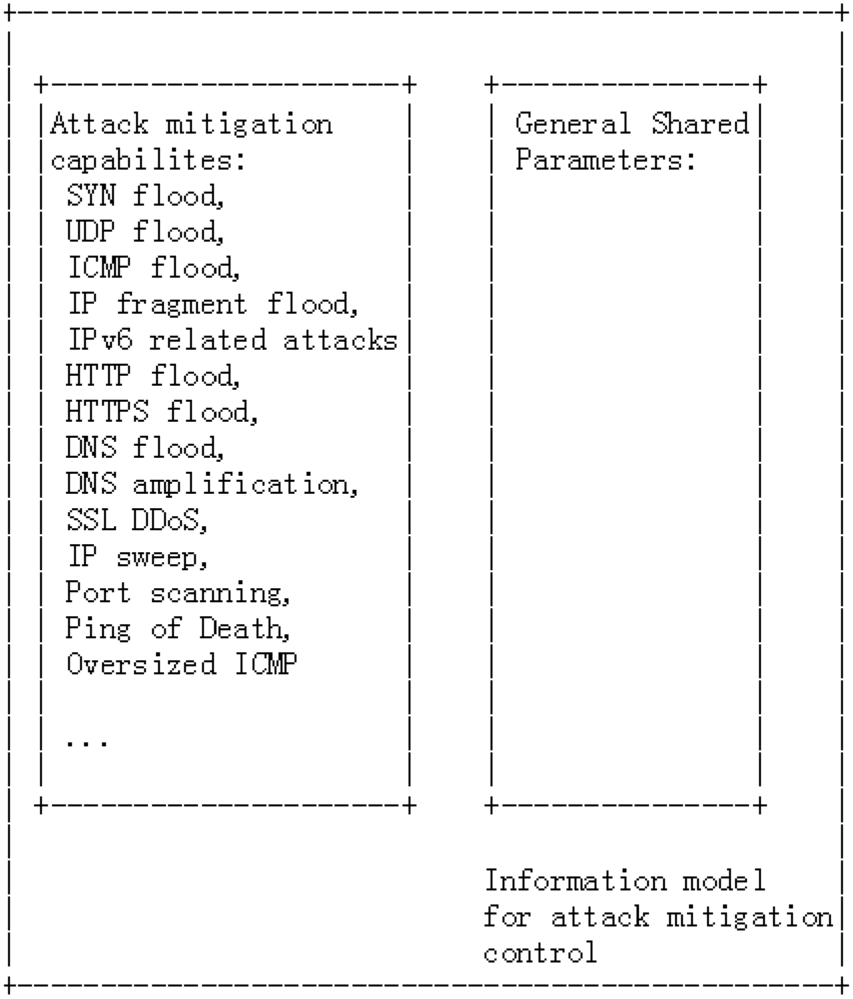
- **IngressAction**: The purpose of this Class is to represent actions performed on packets that enter an NSF. Examples include pass, drop, mirror traffic.
- **EgressAction**: The purpose of this Class is to represent actions performed on packets that exit an NSF. Examples include pass, drop, mirror traffic, signal, encapsulate.
- **ApplyProfileAction**: The purpose of this Class is to represent applying a profile to packets to perform content security and/or attack mitigation control.
- **ApplySignatureAction**: The purpose of this Class is to represent applying a signature file to packets to perform content security and/or attack mitigation control.

Information Model for Content Security



```
+-----------------------------------+
|                                   |
|                                   |
|     Anti-Virus                    |
|     Intrusion Prevention          |
|     URL Filtering                 |
|     File Blocking                 |
|     Data Filtering                |
|     Application Behavior Control  |
|     Mail Filtering                |
|     Packet Capturing              |
|     File Isolation                |
|     ...                           |
|                                   |
|                                   |
|                                   |
|              Information model    |
|              for content security|
|              control              |
+-----------------------------------+
```

Information Model for Attack Mitigation



```
+-------------------------------------------------+
|                                                 |
| +---------------------+    +---------------+    |
| |Attack mitigation    |    | General Shared|    |
| |capabilites:         |    | Parameters:   |    |
| | SYN flood,          |    |               |    |
| | UDP flood,          |    |               |    |
| | ICMP flood,         |    |               |    |
| | IP fragment flood,  |    |               |    |
| | IPv6 related attacks|    |               |    |
| | HTTP flood,         |    |               |    |
| | HTTPS flood,        |    |               |    |
| | DNS flood,          |    |               |    |
| | DNS amplification,  |    |               |    |
| | SSL DDoS,           |    |               |    |
| | IP sweep,           |    |               |    |
| | Port scanning,      |    |               |    |
| | Ping of Death,      |    |               |    |
| | Oversized ICMP      |    |               |    |
| |                     |    |               |    |
| | ...                 |    |               |    |
| |                     |    |               |    |
| +---------------------+    +---------------+    |
|                                                 |
|                            Information model    |
|                            for attack mitigation|
|                            control              |
+-------------------------------------------------+
```

Next Steps

- Comments are welcome!
- Align with I2NSF framework and terminology drafts
- Go further into the IM design
  - content security sub-model;
  - attack mitigation sub-model;
  - MERGE with draft-baspez-i2nsf-capabilities*
  - MERGE with draft-you-i2nsf-user-group-policy-capability*
- Call for WG adoption

** We still probably need individual I-Ds at the data model level*

Thanks!