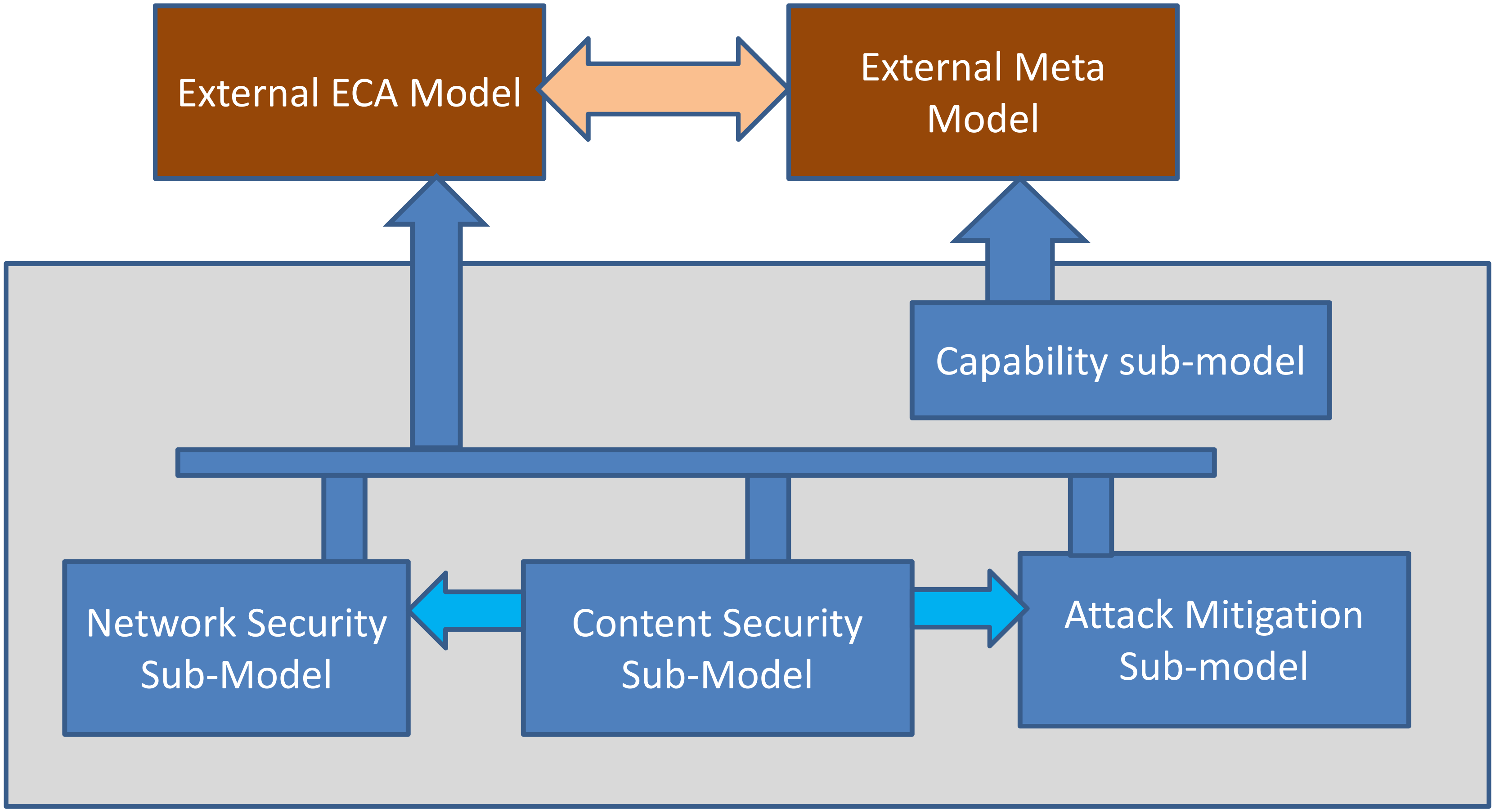
Yang Models for I2NSF Capabilities

draft-hares-i2nsf-capabilities-yang

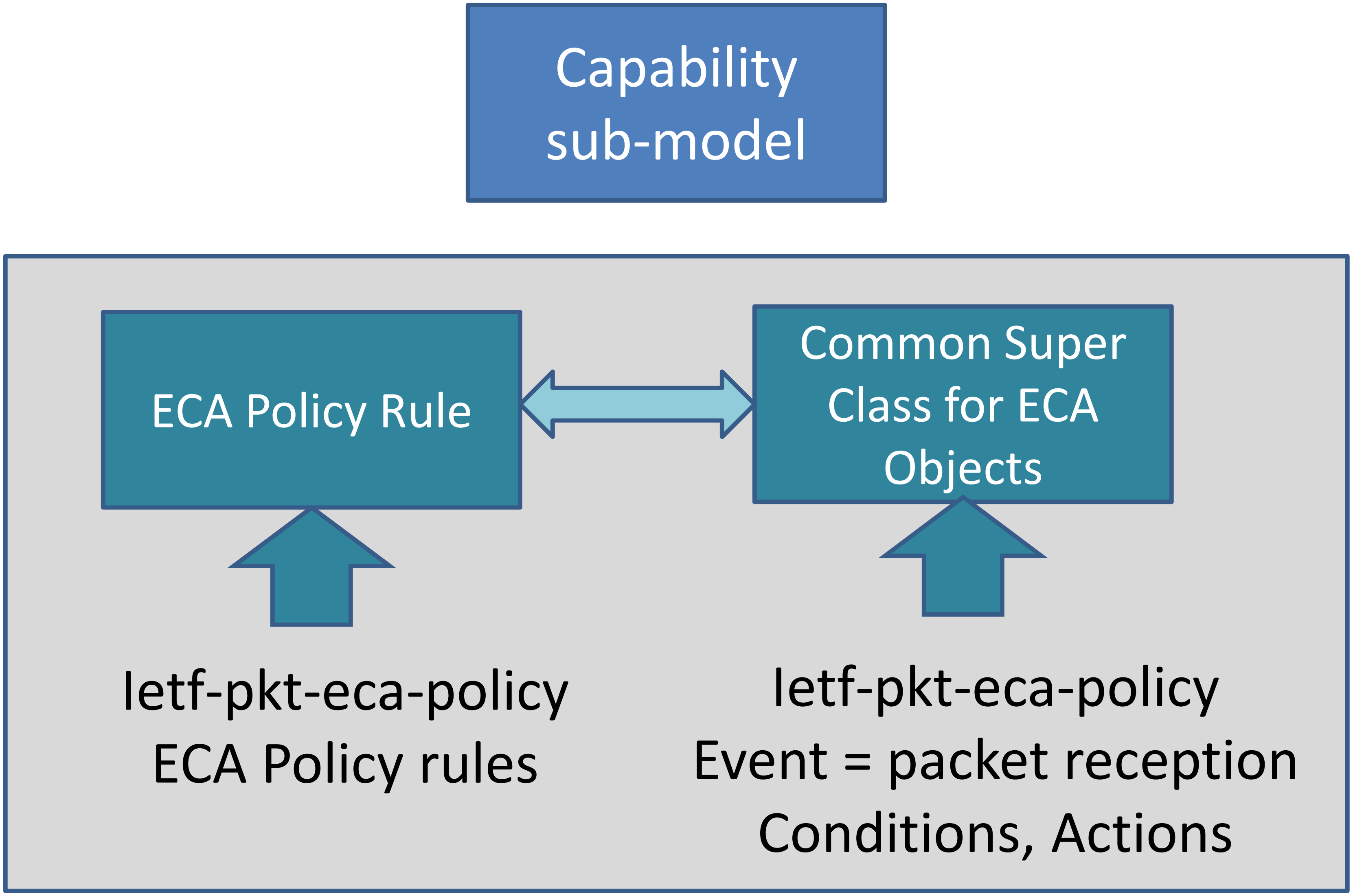
Susan Hares

Co-author: Robert Moskowitz`

Capability Model (Xia, et al.)


External ECA Model
External Meta Model
Capability sub-model
Network Security Sub-Model
Content Security Sub-Model
Attack Mitigation Sub-model

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



Capability sub-model

ECA Policy Rule

Common Super Class for ECA Objects

Ietf-pkt-eca-policy
ECA Policy rules

Ietf-pkt-eca-policy
Event = packet reception
Conditions, Actions

```
ietf-i2nsf-capability
 +--rw nsf-capabilities
    +--rw capability* [name]
    +--rw nsf-name  string
    +--rw cfg-net-secctl-capabilities
    |  uses pkt-eca-policy:pkt-eca-policy-set
    +--rw cfg-net-sec-content-capabilities
    |  uses i2nsf-content-caps
    |  uses i2nsf-content-sec-actions
    +--rw cfg-attack-mitigate-capabilities*
    |  uses i2nsf-mitigate-caps
    +--rw ITResource [ITresource-name]
    |  uses cfg-ITResources
```

Uses common packet ECA Filter with config, I2RS, BGP-FS storage

Common packet ECA Filters are done so that common actions in routers with firewalls, or firewalls with routing have common policy rules to compare for conflict resolution

Network Security

Network Security
Sub-Model

```
+--rw cfg-net-secctl-capabilities
|  uses pkt-eca-policy:pkt-eca-policy-set

module ietf-pkt-eca-policy
    +--rw pkt-eca-policy-cfg
     |  +--rw pkt-eca-policy-set
     |     +--rw groups* [group-name]
     |     |  +--rw group-name string
     |     |  +--rw vrf-name string
     |     |  +--rw address-family
     |     |  +--rw group-rule-list* [rule-name]
     |     |  |  +--rw rule-name
     |     |  |  +--rw rule-order-id
      |    |  |  +--rw default-action-id integer
      |    |  |  +--rw default-resolution-strategy-id integer
```

Additional Index by which to loo-up information – Not in Global Model,
but necessary for ease of use

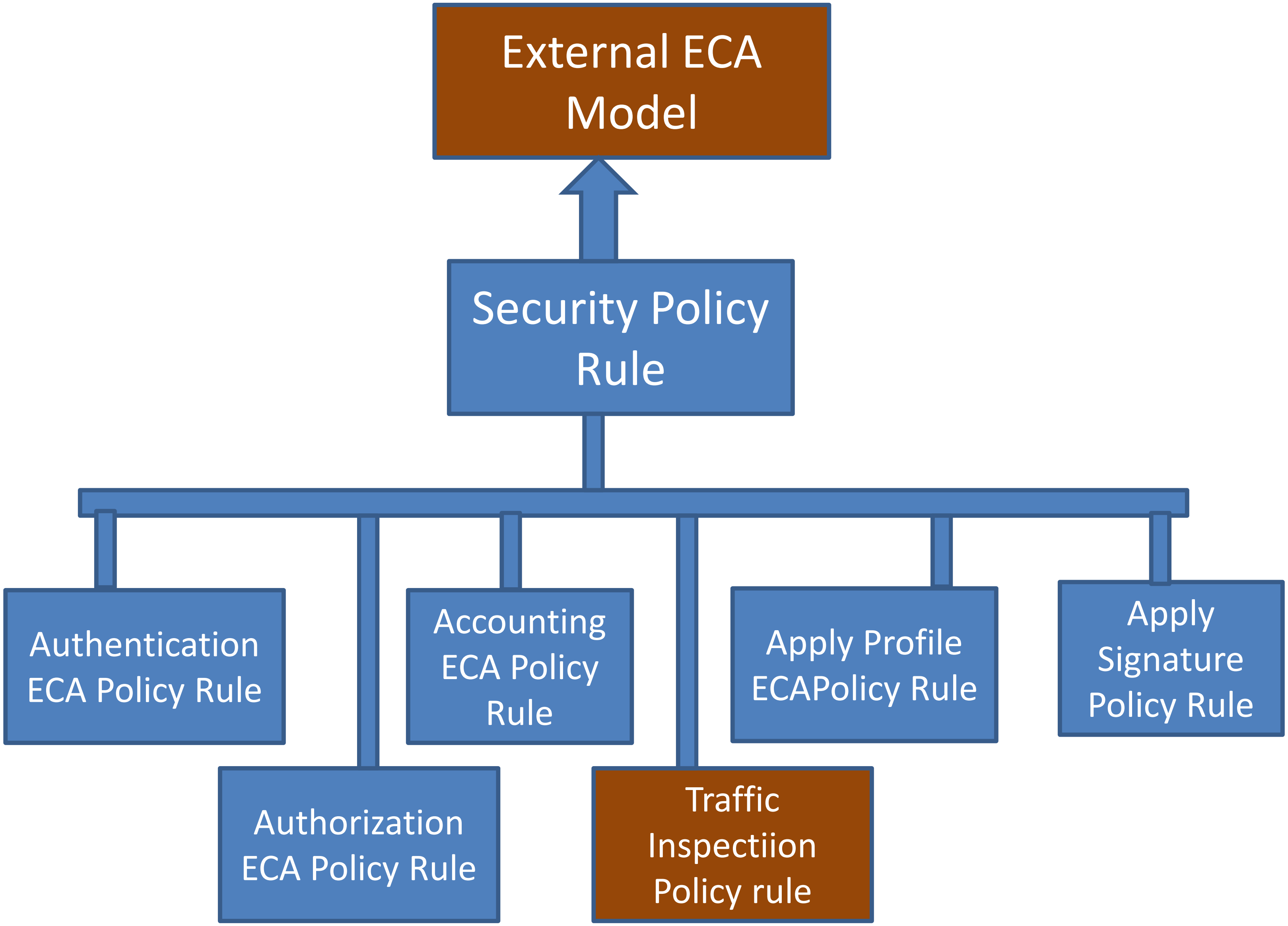
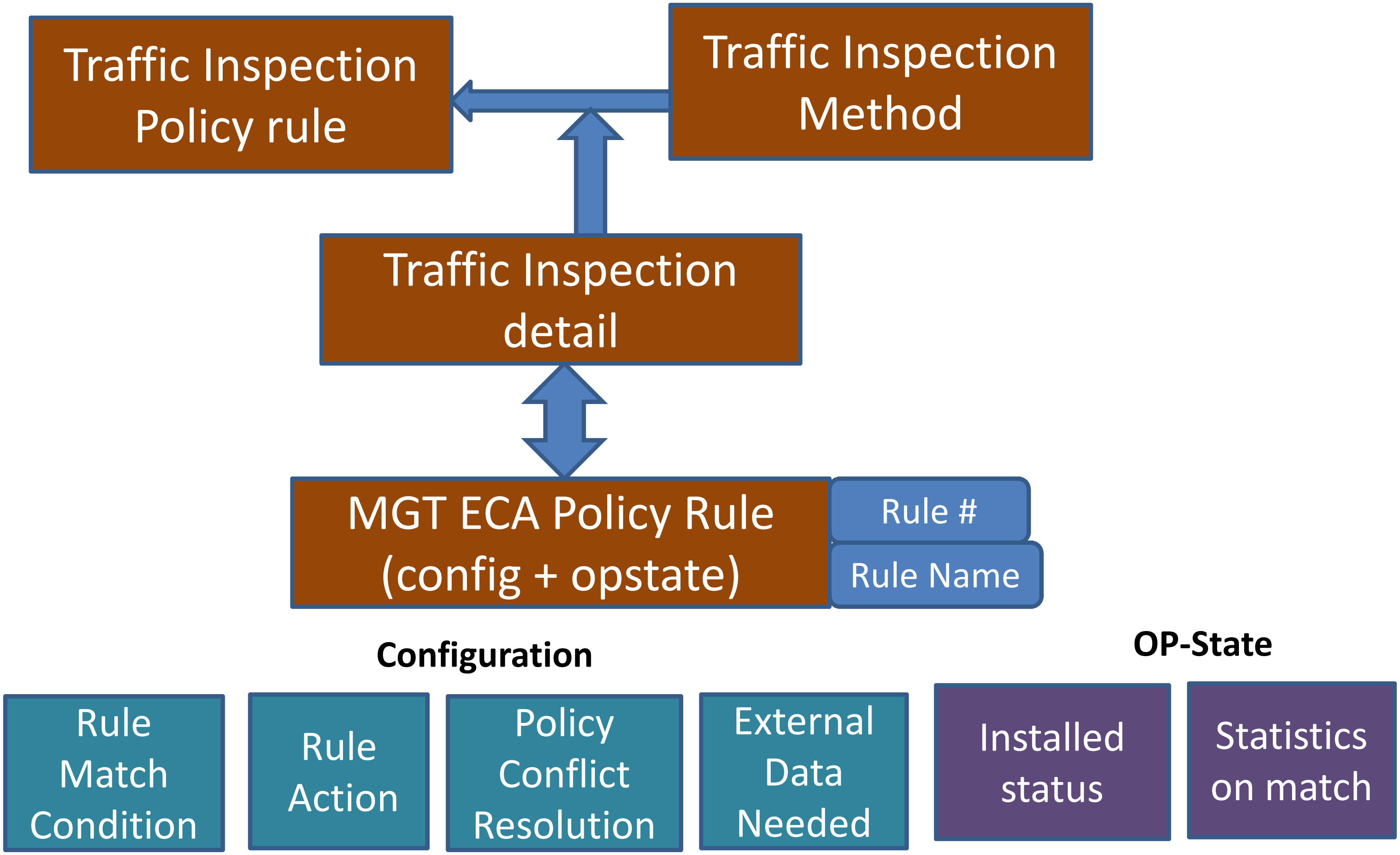

External ECA Model
Security Policy Rule
Authentication ECA Policy Rule
Authorization ECA Policy Rule
Accounting ECA Policy Rule
Traffic Inspectiion Policy rule
Apply Profile ECAPolicy Rule
Apply Signature Policy Rule

Figure 7 (Xia, et al) Linked to Yang



Traffic Inspection Policy rule

Traffic Inspection Method

Traffic Inspection detail

MGT ECA Policy Rule (config + opstate)

Rule #

Rule Name

Configuration

Rule Match Condition

Rule Action

Policy Conflict Resolution

External Data Needed

OP-State

Installed status

Statistics on match

Xia et al. Info Model Lacks detail on

Content Security Control Capabilities

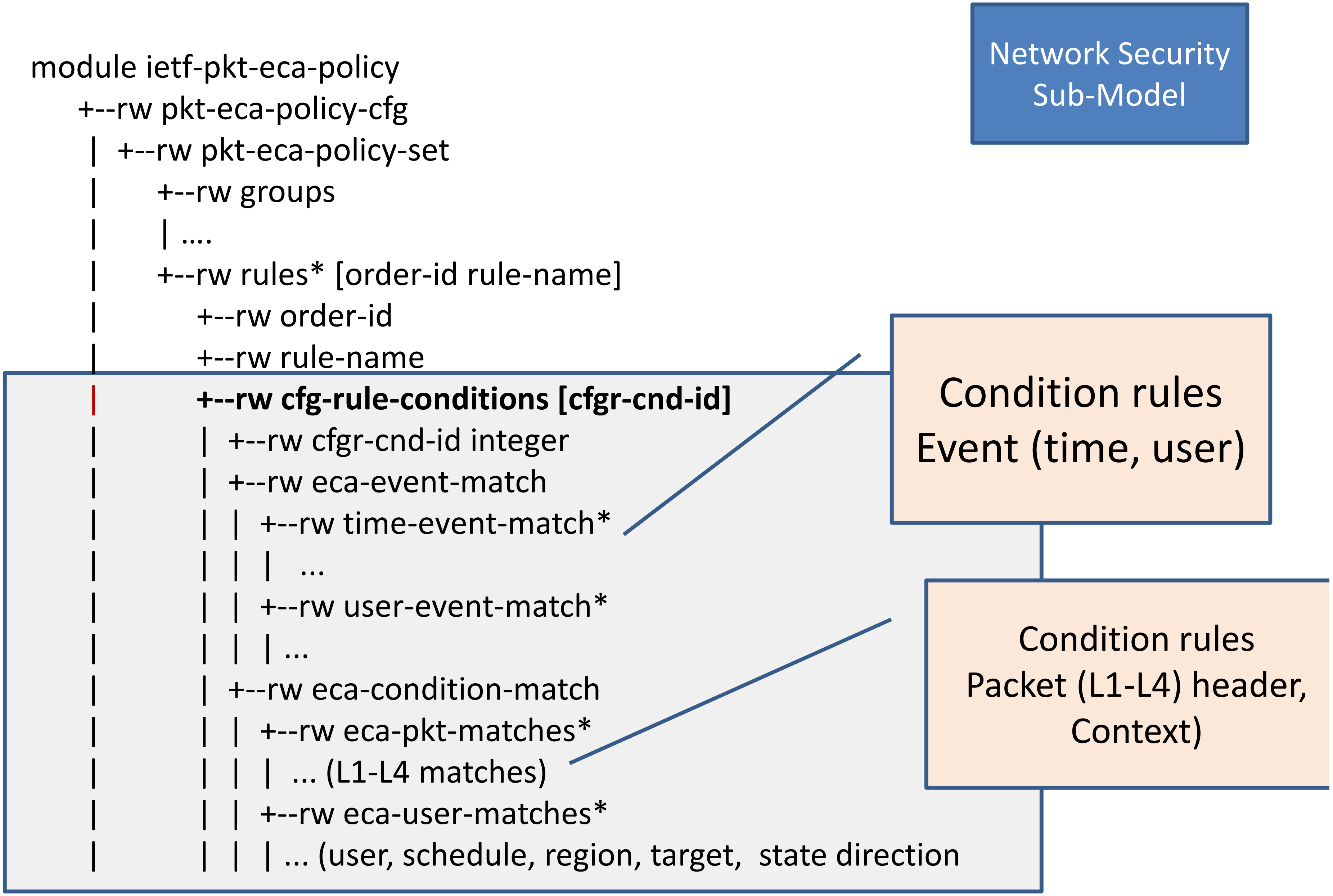
- Anti-virus
- Intrusion Prevention
- URL Filtering
- File Blocking
- Data Filtering
- Application Behavior Control
- Mail Filtering
- Packet Capturing
- File Isolation

Draft-hares-i2nsf-capability treats as capabilities to be queried

Attack Mitigation capabilities

Attack 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

Draft-jeong-i2nsf-capbility-interface treats as actions



Network Security Sub-Model

```
module ietf-pkt-eca-policy
   +--rw pkt-eca-policy-cfg
     |  +--rw pkt-eca-policy-set
     |      +--rw groups
     |      | ....
     |      +--rw rules* [order-id rule-name]
     |          +--rw order-id
     |          +--rw rule-name
     |          +--rw cfg-rule-conditions [cfgr-cnd-id]
     |          |  +--rw cfgr-cnd-id integer
     |          |  +--rw eca-event-match
     |          |  |  +--rw time-event-match*
     |          |  |  |   ...
     |          |  |  +--rw user-event-match*
     |          |  |  | ...
     |          |  +--rw eca-condition-match
     |          |  |  +--rw eca-pkt-matches*
     |          |  |  |  ... (L1-L4 matches)
     |          |  |  +--rw eca-user-matches*
     |          |  |  | ... (user, schedule, region, target,  state direction
```

Condition rules
Event (time, user)

Condition rules
Packet (L1-L4) header,
Context)

Jeong Comparison

```
+--rw policy
    +--rw policy-name  string
    +--rw policy-id  string
    +--rw rule  *[rule-id]
      +--rw rule-name  string
      +--rw rule-id  uint 8
      +--rw event
      |  +--rw time-event-list?  *[time-id]
      |    ....
      |  +--rw user-action?
      |  …
      +--rw condition
      |  +--rw packet-content-values
      |  ….
      |  +--rw context values
      |  (user, schedule, region, target, device, state)
```

Condition rules
Event (time, user)

Condition rules
Packet (L1-L4) header,
Context)

Network Security Sub-Model

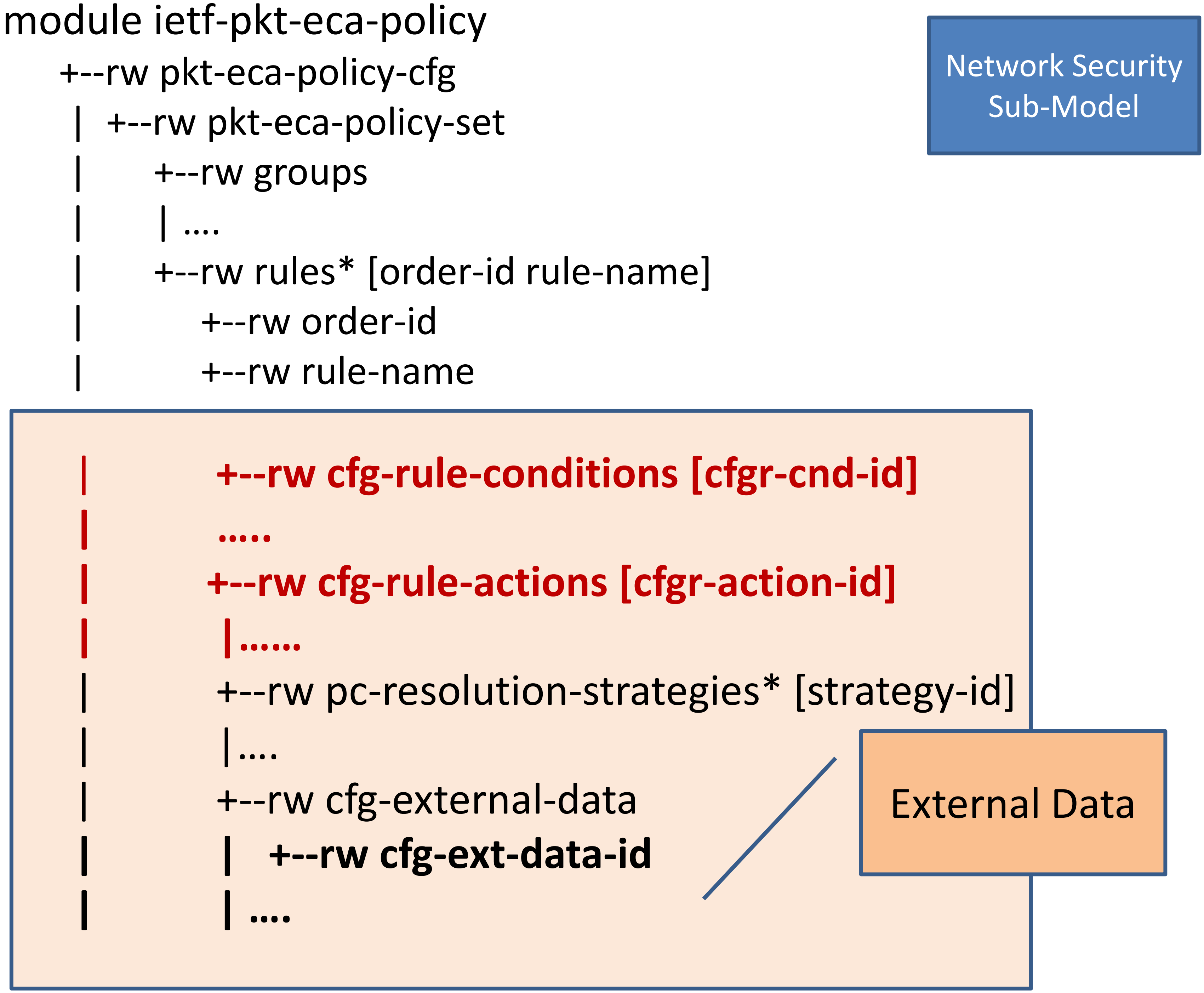
```
module ietf-pkt-eca-policy
   +--rw pkt-eca-policy-cfg
    |  +--rw pkt-eca-policy-set
    |       +--rw groups
    |       | ....
    |       +--rw rules* [order-id rule-name]
    |           +--rw order-id
    |           +--rw rule-name
    |           +--rw cfg-rule-conditions [cfgr-cnd-id]
    |           .....
    |          +--rw cfg-rule-actions [cfgr-action-id]
    |           |  +--rw cfgr-action-id
    |           |  +--rw eca-actions* [action-id]
    |           |  |  +--rw action-id uint32
    |           |  |  +--rw eca-ingress-act*
    |           |  |  | ... (permit, deny, mirror)
    |           |  |  +--rw eca-fwd-actions*
    |           |  |  | ...  (invoke, tunnel encap, fwd)
    |           |  |  +--rw eca-egress-act*
    |           |  |  | .. .
    |           |  |  +--rw eca-qos-actions*
    |           |  |  | ...
    |            |  |  +--rw eca-security-actions*
```

Actions

```
module ietf-pkt-eca-policy
     +--rw pkt-eca-policy-cfg
      |  +--rw pkt-eca-policy-set
      |      +--rw groups
      |      | ….
      |      +--rw rules* [order-id rule-name]
      |          +--rw order-id
      |          +--rw rule-name
       |          +--rw cfg-rule-conditions [cfgr-cnd-id]
       |          …..
       |         +--rw cfg-rule-actions [cfgr-action-id]
       |          |……
       |         +--rw pc-resolution-strategies* [strategy-id]
       |              +--rw strategy-id integer
       |               +--rw filter-strategy identityref
       |               |  .. FMR, ADTP, Longest-match
       |               |  +--rw global-strategy identityref
       |               |  +--rw mandatory-strategy identityref
       |               |  +--rw local-strategy identityref
       |               |  +--rw resolution-fcn uint32
       |               |  +--rw resolution-value uint32
       |               |  +--rw resolution-info  string
       |               |  +--rw associated-ext-data*
       |               |  |  +--rw ext-data-id integer
*
```

Network Security Sub-Model

Policy on resolving Policy conflicts – Not in global model



```
module ietf-pkt-eca-policy
   +--rw pkt-eca-policy-cfg
    |  +--rw pkt-eca-policy-set
    |     +--rw groups
    |     | ....
    |     +--rw rules* [order-id rule-name]
    |        +--rw order-id
    |        +--rw rule-name
    |         +--rw cfg-rule-conditions [cfgr-cnd-id]
    |         .....
    |        +--rw cfg-rule-actions [cfgr-action-id]
    |         |......
    |         +--rw pc-resolution-strategies* [strategy-id]
    |         |....
    |         +--rw cfg-external-data
    |         |  +--rw cfg-ext-data-id
    |         | ....
```

Jeong Comparison

```
+--rw policy
   +--rw policy-name  string
   +--rw policy-id  string
   +--rw rule  *[rule-id]
     +--rw rule-name  string
     +--rw rule-id  uint 8
     +--rw event
     |  …
     +--rw condition
     |  ….
     +--rw action
      |  choice of ingress, egress, advance actions)
      |  advance actions  = content security control (normal + voip)
      |                                  + attack mitigation
      |
      +--rpcs (time-event add/delete, user add/delete, region add/delete)
```

Advanced security actions need to be resolved

Recommendation

- **IM/DM need to determine if** Content Security Control Capabilities and Attack Mitigation capabilities - are queried or advanced actions,
- Use of rpcs for addition:
  - Events
  - Conditions,
  - Actions
- Merging of basic functions