

Network Security Functions Facing Interface YANG Data Model (draft-ietf-i2nsf-nsf-facing-interface-dm-00)

IETF 101, London March 21, 2018

Jinyong (Tim) Kim [Presenter], Jaehoon Paul Jeong, Jung-Soo Park, Susan Hares, and Qiushi Lin

Updates from the Previous Version

- The Previous Draft:
 - draft-kim-i2nsf-nsf-facing-interface-data-model-04
- Now adopted as a new WG document:
 - draft-ietf-i2nsf-nsf-facing-interface-dm-00
- This document defines a YANG Data Model (DM) corresponding to the Information Model (IM) for NSF-Facing Interface:
 - draft-ietf-i2nsf-capability-00.
- This YANG data module was verified through a prototype implemented at IETF-101 Hackathon.

List of Updates

- Modification of YANG Module Name
 - John's Comments (Resolved)
- Modification of Time Zone
 - Dongyue's Comments (Resolved)
- Addition of Port Number to Condition Clause
 - Dongyue's Comments (Resolved)
- Modification of Choice-Case Structure into Container Structure
 - Dongyue's Comments (Resolved)
- Consistency between Capability Information Model (IM) and NSF-Facing Interface YANG Data Model (DM)
 - John's Comments (Ongoing)
- Object-Oriented Features
 - John's Comments (Ongoing)

Modification of YANG Module Name

• The YANG module name becomes ietf-i2nsf-policy-rule-for-nsf.

N 1 - N A /

OLD:	NEW:
<pre>module: ietf-i2nsf-nsf-facing-interface +rw generic-nsf </pre>	<pre>module: ietf-i2nsf-policy-rule-for-nsf +rw i2nsf-security-policy* [policy-name]</pre>
<pre>+rw i2nsf-security-policy* [policy-name] +rw policy-name string +rw time-zone ++rw start-time? yang:date-and-time +rw eca-policy-rules* [rule-id] +rw rule-id uint8 +rw rule-description? string ++rw rule-priority? uint8 ++rw rule-priority? uint8 ++rw policy-event-clause-agg-ptr* instance-identifier ++rw policy-condition-clause-agg-ptr* instance-identifier ++rw resolution-strategy-type)? ++:(fmr) ++:(fmr) ++:w last-matching-rule? boolean ++:w default-action-type? ingress-action +rw event-clause-container +rw action-clause-container</pre>	<pre>trw policy-name string trw time-zone trw time-zone trw time-zone trw start-time? yang:date-and-time trw end-time? yang:date-and-time trw end-time? yang:date-and-time trw eca-policy-rules* [rule-id] trw rule-id uint8 t+rw rule-description? string t+rw rule-description? string t+rw rule-priority? uint8 t+rw policy-event-clause-agg-ptr* instance-identifier t+-rw policy-condition-clause-agg-ptr* instance-identifier t+-rw resolution-strategy t+rw (resolution-strategy-type)? t+rw (resolution-strategy-type)? t+rw first-matching-rule? boolean t+rw default-action t+rw default-action t+rw default-action t+rw condition-clause-container t+rw action-clause-container t+</pre>

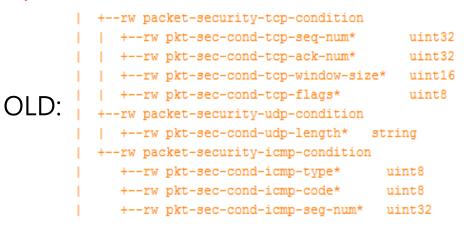
Modification of Time Zone

 We added not only an absolute time zone but also a periodic time zone to eca-policy-rules.

<pre>module: istf-i2nsf-asif-facing-interface +ry generic-naf +ry generic-naf +ry policy-chance string +ry policy-chance string +ry policy-chance string +ry policy-chance string +ry policy-chance string +ry stat-time? yang:date-and-time +ry policy-condition-clause-agg-ptr* instance-identifier +ry policy-condition-clause-agg-ptr* instance-identifier +ry vice-identifier +ry vice-identifier ++ry treestition-strategy + +ry treestition-strategy + +ry default-action-type? ingress-action +ry default-action-type? boolean +ry default-boolean +ry default-action-type? boolean +ry default-boolean +ry default</pre>				
<pre>trw generic-asf trw generic-asf trw policy-name string t</pre>		module: ietf-i2nsf-policy-rule-for-nsf		
<pre> +-rw infor-security-policy-mask = suring + -rw wolldy-mask = suring + -rw wolldy-mask = suring + -rw wolldy-mask = suring + -rw security-policy-mises = suring + -rw security = yangidate-and-time + -rw security = yangidate-and-time + -rw security = yangidate-and-time + -rw security = units + -rw securi</pre>	-	+rw i2nsf-security-policy* [policy-name]		
<pre>t +-rw policy-name string t +-rw policy-name string t +-rw policy-name string t +-rw start-time? yangidate-and-time t +-rw scapplory-rules' (public-time) t +-rw scapplory-rules' (public-time) t +-rw scapplory-rules' (public-time) t +-rw vule-time? yangidate-and-time t +-rw vule-rev? uint8 t +-rw vule-rev? uint8 t + +-rw policy-condition-clause-agg-ptr* instance-identifier t +-rw policy-condition-clause-agg-ptr* instance-identifier t +-rw vule-rev? uint8 t +-rw vule-rev? uint8 t + +-rw vule-rev? uint8 t + +-rw vule-time? yangidate-and-time t +-rw vule-time? boolean t +-rw vul</pre>	-	+rw policy-name string		
<pre>1 +rw time-fone 1 +rw stat-time? yang:date-and-time 1 +rw stat-time? yang:date-and-time 1 +rw stat-time? yang:date-and-time 1 +rw stat-time? yang:date-and-time 1 +rw stat-time? unit8 1 +rw stat-time? unit8 1 +rw stat-time? yang:date-and-time 1 +rw stat-time? yang:date-and-time 1 +rw policy-condition-clause-agg-ptr* instance-identifier 1 +rw policy-condition-clause-agg-ptr* instance-identifier 1 +rw stat-time? yang:date-and-time 1 +rw stat-time? boolean 1 +rw state-time? b</pre>		<pre>+rw eca-policy-rules* [rule-id]</pre>		
<pre>1 +rw tart-time? yang:date-and-time +-rw eda-policy-rules' [rule-1d] 1 +rw rule-fuce-original string 1 +rw rule-rev? uint8 1 +rw rule-rev? uint8 1 +rw rule-rev? uint8 1 +rw policy-cent-clause-agg-ptr* instance-identifier 1 +rw policy-cention-clause-agg-ptr* instance-identifier 1 +rw resolution-strategy 1 +rw frequence-strategy 1 +rw frequence-strategy 1</pre>		+rw rule-id uint8		
<pre> +rw rule-junc? yangidate-and-time +rw rule-id uint8 +rw rule-description? string +rw rule-description? string +rw rule-priority? uint8 +rw rule-priority? uint8 +rw rule-priority? uint8 +rw policy-condition-clause-agg-ptr* instance-identifier +rw policy-condition-clause-agg-ptr* instance-identifier +rw resolution-strategy-ptr* instance-identifier +rw resolution-strategy-ptr* instance-identifier +rw resolution-strategy-ptr* instance-identifier +rw resolution-strategy-ptr* instance-identifier +rw first-matching-rule? bolean +rw first-matching-rule? bolean +rw default-action +rw default-action-type? ingress-action +rw event-clause-container +rw action-clause-container +rw action-clause-co</pre>		+rw rule-description? string		
<pre>i +rw eca-policy-rules* [rule-id] i +rw rule-id uint8 i +rw rule-description? string i +rw rule-description? string i +rw rule-rev? uint8 i +rw rule-rev? uint8 i +rw rule-rev? uint8 i +rw policy-action-clause-agg-ptr* instance-identifier i +rw policy-action-clause-agg-ptr* instance-identifier i +rw resolution-strategy-trype)? i +rw tabulue-rule? boolean i +rw default-action-type? ingress-action +rw weth-clause-container +rw action-clause-container +rw</pre>				
<pre>1 +rw pile-id uin8 1 +rw rule-description? string 1 + +-rw rule-retex? uin8 1 + +-rw rule-priority? uin8 1 + +-rw policy-event-clause-agg-pt* instance-identifier 1 + +-rw policy-event-clause-agg-pt* instance-identifier 1 + +-rw policy-condition-clause-agg-pt* instance-identifier 1 + +-rw policy-condition-strategy-tr* instance-identifier 1 + +-rw tabelute-time? yang:date-and-time 1 + +-rw dat(-trw etabelute-time? yang:date-and-time 1 + +-rw yang:date-and-time 1 + +-rw watch(-trw etabelute-time? boolean 1 + +-rw and y bo</pre>	+rw end-time? yang:date-and-time			
<pre>1 + +-rw file-description? string 1 ++-rw rule-description? string 1 ++-rw rule-description? string 1 ++-rw rule-description? uint8 1 ++-rw rule-description? uint8 1 ++-rw policy-extine-clause-agg-ptr* instance-identifier 1 ++-rw policy-condition-clause-agg-ptr* instance-identifier 1 ++-rw time 1 ++-rw time 1 </pre>	+rw eca-policy-rules* [rule-id]			
<pre>1 +rw intereaser approx = = = = = = = = = = = = = = = = = = =</pre>	+rw rule-id uint8			
<pre>+rw subsuble-time-zone +rw absolute-time-zone +rw absolute-time-zone ++rw time ++rw policy-extin-clause-agg-ptr* instance-identifier ++rw policy-action-clause-agg-ptr* instance-identifier ++rw resolution-strategy ++rw state-time? yang:date-and-time ++rw absolute-time-zone ++rw absolute-time? yang:date-and-time ++rw absolute-time? boolean ++rw absolute-time? boolean ++rw absolute-time? boolean ++rw aprin? bo</pre>	+rw rule-description? string	+rw policy-action-clause-agg-ptr* instance-identifier		
<pre>+rw rule-priority? uint8 +rw policy-event-clause-agg-ptr* instance-identifier +rw policy-action-clause-agg-ptr* instance-identifier +rw resolution-strategy +rw resolution-strategy-type)? +rw resolution-strategy-type)? +rw default-action-rule? boolean +rw default-action-type? ingress-action +rw default-action-type? ingress-action +rw default-action-type? ingress-action +rw secton-clause-container +rw action-clause-container +rw action-clause-</pre>	+rw rule-rev? uint8			
<pre> +rw policy-event-clause-agg-ptr* instance-identifier +rw policy-condition-clause-agg-ptr* instance-identifier +rw scolution-strategy +rw date +rw first-matching-rule? bolean +rw date. +rw fall. +rw fall.</pre>				
<pre> +rw policy-condition-clause-agg-ptr* instance-identifier +rw policy-action-clause-agg-ptr* instance-identifier + +rw resolution-strategy +rw resolution-strategy +rw first-matching-rule? boolean +rw first-matching-rule? boolean +rw default-action +rw solution-clause-container +rw action-clause-container +rw action-clause-container </pre>				
<pre> +rw policy-action-clause-agg-ptr* instance-identifier +rw resolution-strategy ++rw resolution-strategy-type)? ++rw first-matching-rule? boolean ++rw datu ++rw sunday? boolean ++rw default-action ++rw default-action +rw default-action-type? ingress-action +rw event-clause-container +rw action-clause-container +rw action-clause-container </pre>		I I I I I I I I I I I I I I I I I I I		
<pre>+rw resolution-strategy +rw (resolution-strategy-type)? + +rw (resolution-strategy-type)? + +rw (resolution-strategy-type)? + +rw first-matching-rule? boolean + +rw default-action + +rw default-action-type? ingress-action + +rw default-action-type? ingress-action + +rw condition-clause-container +rw condition-clause-container +rw action-clause-container +rw action-clau</pre>				
<pre>+rw (resolution-strategy-type)? +rw day +rw day +rw day +rw day +rw day? boolean +rw default-action +rw default-action-type? boolean +rw default-action-type? ingress-action +rw condition-clause-container +rw condition-clause-container +rw action-clause-container +rw acti</pre>				
<pre>1 +:(fmr) 1 +:(fmr) 1 +:w first-matching-rule? boolean 1 +:w first-matching-rule? boolean 1 +:w last-matching-rule? boolean 1 +:w default-action 1 +:w default-action-type? ingress-action 1 +:w default-action-type? ingress-action 1 +:w condition-clause-container 1 +:w condition-clause-container 1 +:w action-clause-container 1 +:w action-clause-cont</pre>				
+rw first-matching-rule? boolean +rw sunday? boolean +rw list-matching-rule? boolean +rw monday? boolean +rw default-action +rw wednesday? boolean +rw default-action-type? ingress-action +rw thursday? boolean +rw condition-clause-container +rw month +rw condition-clause-container +rw first-matching +rw condition-clause-container +rw month +rw default-action +rw condition-clause-container +rw month +rw action-clause-container +rw february? boolean +rw action-clause-container +rw march? boolean +rw september? boolean +rw noreber? boolean				
+:(lmr) +rw monday? boolean +rw last-matching-rule? boolean +rw wordsday? boolean +rw default-action +rw wordsday? boolean +rw default-action-type? ingress-action +rw thursday? boolean +rw event-clause-container +rw sturday? boolean +rw dofault-action-clause-container +rw action-clause-container +rw default-clause-container +rw action-clause-container +rw action-clause-container +rw action-clause-container +rw april? boolean +rw action-clause-container +rw april? boolean +rw action-clause-container +rw april? boolean +rw action-clause-container +rw april? boolean +rw action-clause-container +rw april? boolean +rw april? boolean +rw april? boolean +rw april? boolean +rw				
<pre>1 +rw last-matching-rule? boolean +rw tuesday? boolean 1 +rw default-action +rw wednesday? boolean 1 +rw default-action-type? ingress-action +rw thursday? boolean +rw event-clause-container +rw saturday? boolean 1 +rw condition-clause-container +rw january? boolean 1 +rw action-clause-container +rw fabruary? boolean +rw action-clause-container +rw march? boolean +rw march? boolean +rw march? boolean +rw may? boolean +rw may? boolean</pre>				
<pre>1 +rw default-action 1 +rw default-action-type? ingress-action 1 +rw efault-action-type? ingress-action 1 +rw event-clause-container 1 +rw event-clause-container 1 +rw condition-clause-container 1 +rw condition-clause-container 1 +rw action-clause-container 1 +rw april? boolean 1 +rw april? boolean 1 +rw jul? boolean 1 +rw jul? boolean 1 +rw jul? boolean 1 +rw september? boolean 1 +rw september? boolean 1 +rw otober? boolean</pre>				
<pre>1 +rw default-action 1 +rw default-action-type? ingress-action 1 +rw event-clause-container 1 +rw condition-clause-container 1 +rw condition-clause-container 1 +rw action-clause-container 1 +rw march? boolean +rw march? boolean 1 +rw september? boolean 1 +rw souther? boolean 1 +rw november? boolean</pre>	+rw last-matching-rule? boolean			
<pre>1 +rw defailt-action-type? Ingress-action 1 +rw event-clause-container 1 1 +rw saturday? boolean 1 +rw month +rw february? boolean 1 +rw february? boolean 1 +rw march? boolean 1 +rw march? boolean 1 +rw may? boolean 1 +rw may? boolean 1 +rw july? boolean 1 +rw ignes? boolean 1 +rw igne</pre>	+rw default-action			
<pre>+rw event-clause-container +rw condition-clause-container +rw condition-clause-container +rw march? boolean +rw action-clause-container +rw march? boolean +rw april? boolean +rw may? boolean +rw may? boolean +rw june? boolean +rw june? boolean +rw september? boolean +rw october? boolean +rw november? boolean +rw november? boolean</pre>	<pre>+rw default-action-type? ingress-action</pre>			
<pre>1 +rw condition-clause-container 1 +rw action-clause-container </pre> 1 +rw march? boolean +rw action-clause-container 1 +rw march? boolean 1 +rw march? boolean 1 +rw march? boolean 1 +rw march? boolean 1 +rw jung? boolean 1 +rw jung? boolean 1 +rw jung: boolean 1 +rw september? boolean 1 +rw september? boolean 1 +rw october? boolean 1 +rw november? boolean	+rw event-clause-container			
<pre>+rw condition-clause-container +rw action-clause-container +rw february? boolean +rw action-clause-container +rw march? boolean +rw march? boolean +rw may? boolean +rw june? boolean +rw june? boolean +rw august? boolean +rw september? boolean +rw september? boolean +rw november? boolean</pre>	1			
<pre>1 +rw action-clause-container </pre>	+rw condition-clause-container			
+rw action-clause-container 	1			
<pre></pre>				
<pre>+rw may? boolean +rw june? boolean +rw june? boolean +rw july? boolean +rw august? boolean +rw september? boolean +rw october? boolean +rw november? boolean</pre>				
I+rw june? booleanI+rw july? booleanI+rw august? booleanI+rw september? booleanI+rw october? booleanI+rw november? booleanI+rw november? boolean				
i +rw july? boolean i +rw august? boolean i +rw september? boolean i +rw october? boolean i +rw november? boolean				
I +rw august? boolean I +rw september? boolean I +rw october? boolean I +rw november? boolean				
+rw september? boolean +rw october? boolean +rw november? boolean				
+rw october? boolean +rw november? boolean				
+rw november? boolean				

Addition of Port Number to Condition Clause

• We added a port number to a condition clause.



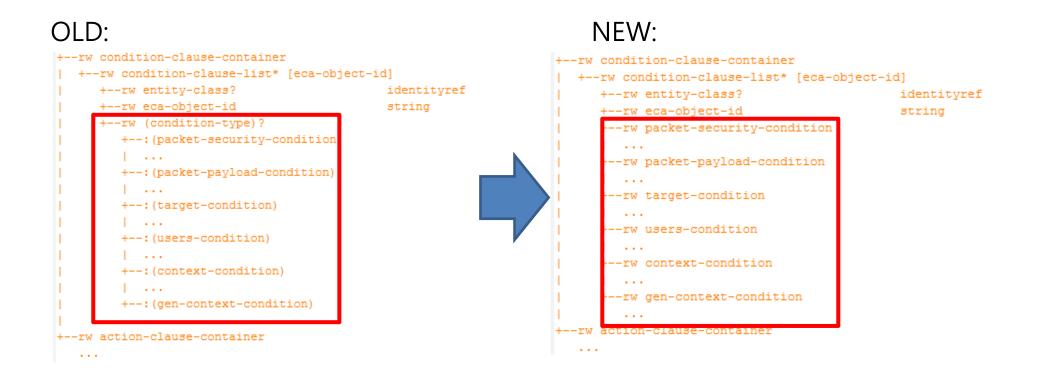


+--rw packet-security-tcp-condition

	- I IW packet becarity cop condition	
	+rw pkt-sec-cond-tcp-src-port*	inet:port-number
	+rw pkt-sec-cond-tcp-dest-port*	inet:port-number
	+rw pkt-sec-cond-tcp-seq-num*	uint32
	+rw pkt-sec-cond-tcp-ack-num*	uint32
	+rw pkt-sec-cond-tcp-window-size*	uint16
NEW:	+rw pkt-sec-cond-tcp-flags*	uint8
INLVV.	+rw packet-security-udp-condition	
	+rw pkt-sec-cond-udp-src-port*	inet:port-number
	+rw pkt-sec-cond-udp-dest-port*	inet:port-number
	+rw pkt-sec-cond-udp-length* str	ing
	<pre>+rw packet-security-icmp-condition</pre>	
	+rw pkt-sec-cond-icmp-type* u	int8
	<pre>+rw pkt-sec-cond-icmp-code* u</pre>	int8

Modification of Choice-Case Structure into Container Structure (1/2)

 We changed a choice-case structure into a container structure about a condition clause for a multiple configuration.



Modification of Choice-Case Structure into Container Structure (2/2)

 We changed a choice-case structure into a container structure about an action clause for a multiple configuration.

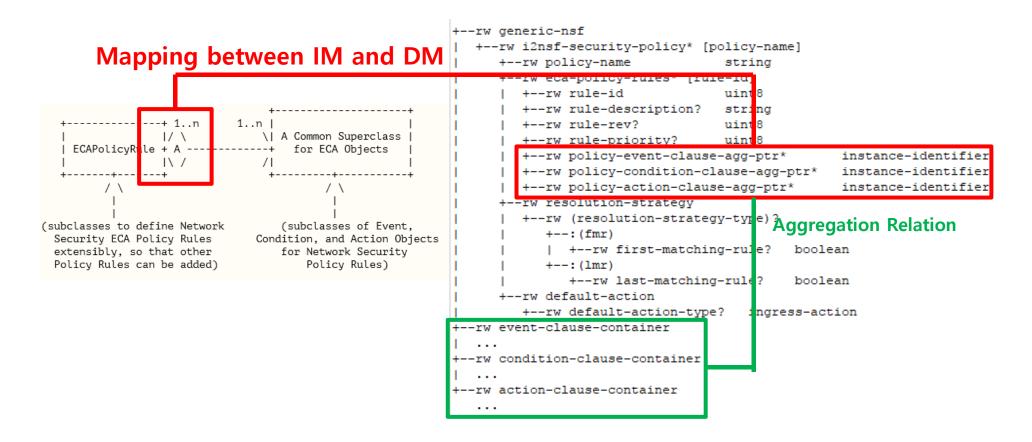
NFW.

OLD:

```
module: ietf-i2nsf-policy-rule-for-nsf
module: ietf-i2nsf-nsf-facing-interface
                                                                      +--rw i2nsf-security-policy* [policy-name]
+--rw generic-nsf
   +--rw i2nsf-security-policy* [policy-name]
                                                                            . . .
      . . .
                                                                         +--rw eca-policy-rules* [rule-id]
     +--rw eca-policy-rules* [rule-id]
        . . .
                                                                         +--rw resolution-strategy
      +--rw resolution-strategy
                                                                            . . .
         .....
                                                                         +--rw default-action
      +--rw default-action
         . . .
                                                                      +--rw event-clause-container
  -rw event-clause-container
                                                                       +--rw condition-clause-container
+--rw condition-clause-container
                                                                      +--rw action-clause-container
+--rw action-clause-container
                                                                         +--rw action-clause-list* [eca-object-id]
   +--rw action-clause-list* [eca-object-id]
                                                                            +--rw entity-class?
                                                                                                                      identityref
      +--rw entity-class?
                                                identityref
                                                                            +--rw eca-object-id
                                                                                                                      string
      +--rw eca-object-id
                                                string
                                                                                +--rw ingress-action
      +--rw (action-type)?
         +--: (ingress-action)
                                                                                +--rw egress-action
         +--:(egress-action)
                                                                                +--rw apply-profile
         +--: (apply-profile)
```

Consistency between Capability IM and NSF-Facing Interface DM (Ongoing)

• We have modified event, condition, and action clauses to be aggregated into a policy.



Next Steps

- We will change the current YANG data model to the YANG data model of Object-Oriented (OO) Style.
- We will verify the OO YANG data model by implementing a prototype in the next Hackathon.