Configuration Data Model for IPFIX and PSAMP

draft-ietf-ipfix-configuration-model-03

Gerhard Münz, Benoit Claise, Paul Aitken

75th IETF Meeting, Stockholm, 2009
Changes in -03

- Many editorial changes
- UML class diagrams:
  - "readOnly" property
  - parameter multiplicity
    - [0..X] = does not have to be configured
    - text and YANG description explains how to interpret or handle a non-existing parameter (specific meaning, default value, or value set by device)
- Relationship
  Observation Domain $\Leftrightarrow$ Selection Process/Cache
  clarified (slide 3)
- New parameters regarding transport layer security (slide 4)
- Update of YANG module

Example:
```
+----------------------------+
| Selector                  |
+----------------------------+
| name                      |
| selectorId[0..1]          |
| packetsObserved {readOnly} |
| packetsDropped {readOnly} |
+----------------------------+
```
**Observation Domain ↔ Selection Process/Cache**

The Observed Packet Stream at the input of a Selection Process MUST only contain packets originating from a single Observation Domain. Similarly, the Selected Packet Stream at the input of a Cache MUST only contain packets originating from a single Observation Domain. Packets from Observation Points belonging to different Observation Domains MUST NOT enter the same Selection Process or the same Cache.

**Definition of Observation Domain** in RFC 5101:

An Observation Domain is the largest set of Observation Points for which Flow information can be aggregated by a Metering Process.

**Clarification in -03:**

The Observed Packet Stream at the input of a Selection Process MUST only contain packets originating from a single Observation Domain. Similarly, the Selected Packet Stream at the input of a Cache MUST only contain packets originating from a single Observation Domain. Packets from Observation Points belonging to different Observation Domains MUST NOT enter the same Selection Process or the same Cache.

**YANG module:**

- enforced with **must** statements for non-cascaded Selection Processes
- other cases covered by **description** statement, only
## Configuration of Mutual Authentication (+ Authorization)

Enable (D)TLS separately for every destination of an Exporting Process and every receiver of a Collecting Process

- **local* parameters:**
  - identify/restrict certificates to be used to authenticate local endpoint
  - configuration error if no matching certificate is installed on the Monitoring Device

- **remote* parameters:**
  - restrict authentication of remote endpoint (authorization)

```
+--------------------------------------+
| TransportLayerSecurity               |
| -------------------------------------+
| localCertificationAuthorityDN[0..*]  |
| localSubjectDN[0..*]                 |
| localSubjectFQDN[0..*]               |
| remoteCertificationAuthorityDN[0..*] |
| remoteSubjectDN[0..*]                |
| remoteSubjectFQDN[0..*]              |
+-------------------------------------+
```
Open issues

- **PSAMP parameters**
  - goal: same parameters as in PSAMP-MIB
  - still waiting for feedback/answers from PSAMP-MIB authors…

- **TLS/DTLS parameters**
  - additional parameters going beyond certificates?
    - e.g. enable message authentication, message encryption, …

- **WGLC to see…**
  - if people understand the model and
  - where further clarification is needed