IPFIX Flow Aggregation

draft-dressler-ipfix-aggregation-04

F. Dressler, C. Sommer, G. Münz, A. Kobayashi

70th IETF, Vancouver, BC, Canada

Aggregation Steps

- Flow Selection
- Compound Flow Creation

Src IP	Src Port	Dst IP	Dst Port	Packets
192.0.2.1	64235	192.0.2.101	80	10
192.0.2.2	64236	192.0.2.102	110	10
192.0.2.3	64237	192.0.2.103	80	10
192.0.2.101	64238	192.0.2.1	80	10
192.0.2.102	64239	192.0.2.2	80	10

Aggregation Steps

- Flow Selection
- Compound Flow Creation

Src IP	Src Port	Dst IP	Dst Port	Packets
192.0.2.1	64235	192.0.2.101	80	10
~~192.0.2.2~~	~~64236~~	~~192.0.2.102~~	~~110~~	~~10~~
192.0.2.3	64237	192.0.2.103	80	10
192.0.2.101	64238	192.0.2.1	80	10
192.0.2.102	64239	192.0.2.2	80	10

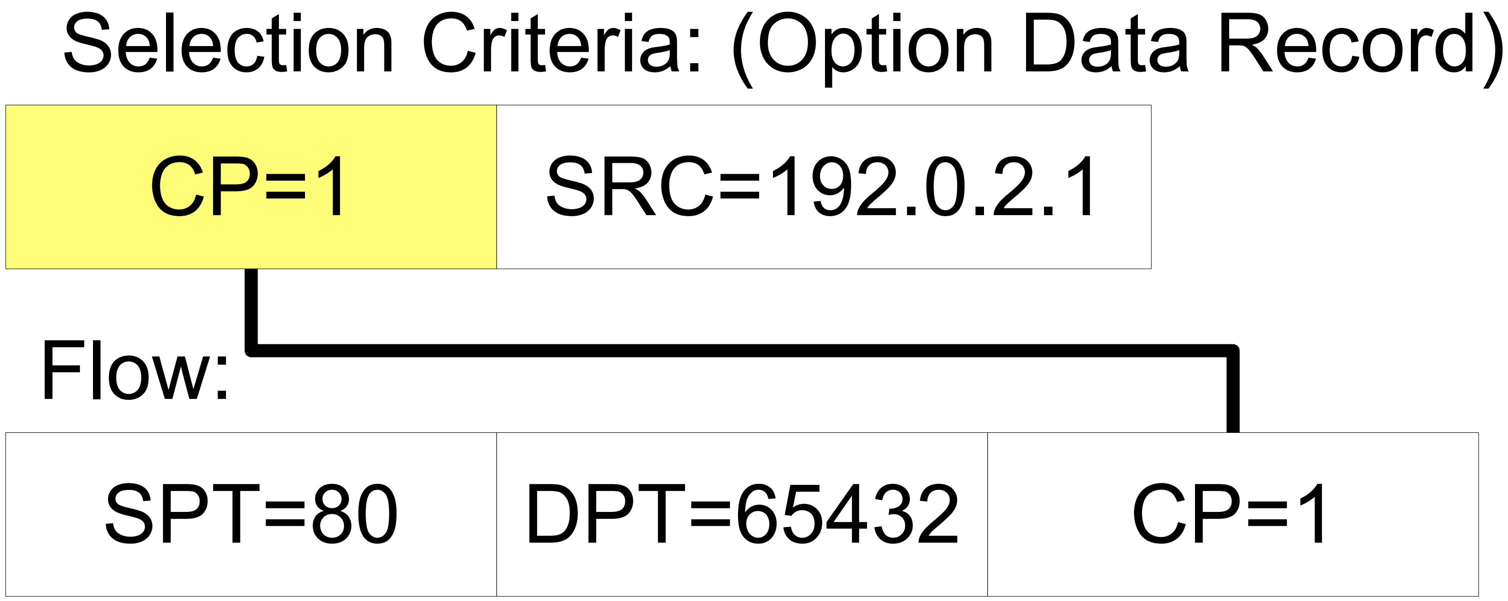
Aggregation Steps

- Flow Selection
- Compound Flow Creation

Src IP	Src Port	Dst IP	Dst Port	Packets
192.0.2.1	64235	192.0.2.101	80	10
192.0.2.2	64236	192.0.2.102	110	10
192.0.2.3	64237	192.0.2.103	80	10
192.0.2.101	64238	192.0.2.1	80	10
192.0.2.102	64239	192.0.2.2	80	10

Flow Selection

- Match incoming Flows against selection criteria of each configured stream of Compound Flows
- Only matching Flows will contribute,
  Flows that don't match are discarded
- Selection Criteria constitute Common Properties



Compound Flow Creation

- “Compound Flow”: Results from aggregation of one or more incoming flows
- For each selected Flow, merge field values into existing Compound Flow (or create new one)
- Flows are merged by
  - discarding configured fields, then
  - aggregating flows with identical remaining values

Aggregation Rules

- “Aggregation Rule”: Lists 3-tuple for each data field to be considered during aggregation
    - Field specifier (e.g. destinationIPv4Address)
    - Selection pattern (e.g. 192.0.2.0/24)
    - Field modifier (discard, keep, mask, aggregate)
- By default, incoming Flow Records checked against (and aggregated according to) all configured Aggregation Rules
- Alternatively: Specify “preceding rule” and consider only Flows for aggregation that didn’t match a PR

Deriving Templates

Selection	Aggregation	Common P	Specific P	F-Key
any	discard			
any	keep / mask		x	x
any	aggregate		x	
pattern	discard	x		
pattern	keep / mask	x	x	x
pattern	aggregate	x	x	

- Problematic combinations:
  Match atomic pattern / Do not discard field values
  Allow any field value / Discard field values
  Match any Pattern / Aggregate field values

Example

IPFIX Field	Selection	Aggregation
sourceIPv4Address		keep
destinationIPv4Address	192.0.2.0/28	mask to 30 bit
destinationTransportPort	80	discard
packetDeltaCount		aggregate

Src IP	Src Port	Dst IP	Dst Port	Packets
192.0.2.1	64235	192.0.2.101	80	10
192.0.2.2	64236	192.0.2.102	110	10
192.0.2.3	64237	192.0.2.103	80	10
192.0.2.101	64238	192.0.2.1	80	10
192.0.2.101	64239	192.0.2.2	80	10

Example

IPFIX Field	Selection	Aggregation
sourceIPv4Address		keep
destinationIPv4Address	192.0.2.0/28	mask to 30 bit
destinationTransportPort	80	discard
packetDeltaCount		aggregate

Src IP	Src Port	Dst IP	Dst Port	Packets
192.0.2.1	64235	192.0.2.101	80	10
192.0.2.2	64236	192.0.2.102	110	10
192.0.2.3	64237	192.0.2.103	80	10
192.0.2.101	64238	192.0.2.1	80	10
192.0.2.101	64239	192.0.2.2	80	10

Example

IPFIX Field	Selection	Aggregation
sourceIPv4Address		keep
destinationIPv4Address	192.0.2.0/28	mask to 30 bit
destinationTransportPort	80	discard
packetDeltaCount		aggregate

Src IP	~~Src Port~~	Dst IP	Dst Port	Packets
~~192.0.2.1~~	~~64235~~	~~192.0.2.101~~	~~80~~	~~10~~
~~192.0.2.2~~	~~64236~~	~~192.0.2.102~~	~~110~~	~~10~~
~~192.0.2.3~~	~~64237~~	~~192.0.2.103~~	~~80~~	~~10~~
192.0.2.101	~~64238~~	192.0.2.1	80	10
192.0.2.101	~~64239~~	192.0.2.2	80	10

Example

IPFIX Field	Selection	Aggregation
sourceIPv4Address		keep
destinationIPv4Address	192.0.2.0/28	mask to 30 bit
destinationTransportPort	80	discard
packetDeltaCount		aggregate

Src IP	Src Port	Dst IP	Dst Port	Packets
~~192.0.2.1~~	~~64235~~	~~192.0.2.101~~	~~80~~	~~10~~
~~192.0.2.2~~	~~64236~~	~~192.0.2.102~~	~~110~~	~~10~~
~~192.0.2.3~~	~~64237~~	~~192.0.2.103~~	~~80~~	~~10~~
192.0.2.101	~~64238~~	192.0.2.1	80	10
192.0.2.101	~~64239~~	192.0.2.2	80	10

Src IP	Dst IP	Dst Port	Packets
192.0.2.101	192.0.2.0/28	80	20

Open Issues

- Forwarding of Option Data Records
  - ODRs that refer to an Observation Domain only include observationDomainId, defined as being unique only to an Exporting Process
  - Easy solution: Mandate OD-Ids be unique in whole aggregation domain, but more generic solution preferable
- Aggregating IP addresses that are pseudonyms
  - If Compound Flow creation not explicitly informed, wrong IP addresses may be merged