

IPFIX 仕様と実装

Tajima Hirotaka / FIVEFRONT

Dec.14,2011 ENOGI2

IPFIX vs. NetFlow v9

- version番号が違う w (IPFIXは10)
- 可変長情報要素(e.g. URL)
- セキュリティ(TLS, DTLS)
- テンプレートとデータを別ストリームで転送可
- テンプレートの明示的なwithdraw
- 多くの情報要素IDは共通
- etc...

IPFIX テンプレート

Filter: Exp

No.	Time	Source
-----	------	--------

▶ Frame 11: 142 bytes on wire (1136 bits), 142 bytes captured

▶ Ethernet II, Src: Netscreen_24:47:d2 (00:10:db:24:47:d2), D

▶ Internet Protocol Version 4, Src: 10.9.100.140 (10.9.100.14

▶ User Datagram Protocol, Src Port: 33018 (33018), Dst Port:

▼ Cisco NetFlow/IPFIX

Version: 10

Length: 100

▶ Timestamp: Sep 26, 2011 16:46:10.000000000 JST

FlowSequence: 0

Observation Domain Id: 513

▼ Set 1

FlowSet Id: Data Template (V10 [IPFIX]) (2)

FlowSet Length: 84

▼ Template (Id = 256, Count = 19)

Template Id: 256

Field Count: 19

▶ Field (1/19): IP_SRC_ADDR

▶ Field (2/19): IP_DST_ADDR

▶ Field (3/19): IP_TOS

▶ Field (4/19): PROTOCOL

▶ Field (5/19): L4_SRC_PORT

▶ Field (6/19): L4_DST_PORT

▶ Field (7/19): ICMP_TYPE

▶ Field (8/19): INPUT_SNMP

▶ Field (9/19): SRC_MASK

▶ Field (10/19): DST_MASK

▶ Field (11/19): SRC_AS

▶ Field (12/19): DST_AS

▶ Field (13/19): IP_NEXT_HOP

▶ Field (14/19): TCP_FLAGS

NFv9 テンプレート

Filter: Expres

No.	Time	Source
-----	------	--------

▶ Frame 36: 146 bytes on wire (1168 bits), 146 bytes captured (1

▶ Ethernet II, Src: Inventec_e7:cc:23 (00:a0:d1:e7:cc:23), Dst:

▶ Internet Protocol Version 4, Src: [REDACTED] 7

▶ User Datagram Protocol, Src Port: 45165 (45165), Dst Port: iop

▼ Cisco NetFlow/IPFIX

Version: 9

Count: 1

SysUptime: 1170058122

▶ Timestamp: Jun 10, 2010 17:47:24.000000000 JST

FlowSequence: 507118

SourceId: 17

▼ FlowSet 1

FlowSet Id: Data Template (V9) (0)

FlowSet Length: 84

▼ Template (Id = 266, Count = 19)

Template Id: 266

Field Count: 19

▶ Field (1/19): PKTS

▶ Field (2/19): BYTES

▶ Field (3/19): IPV6_SRC_ADDR

▶ Field (4/19): IPV6_DST_ADDR

▶ Field (5/19): INPUT_SNMP

▶ Field (6/19): OUTPUT_SNMP

▶ Field (7/19): FIRST_SWITCHED

▶ Field (8/19): LAST_SWITCHED

▶ Field (9/19): FLOW_LABEL

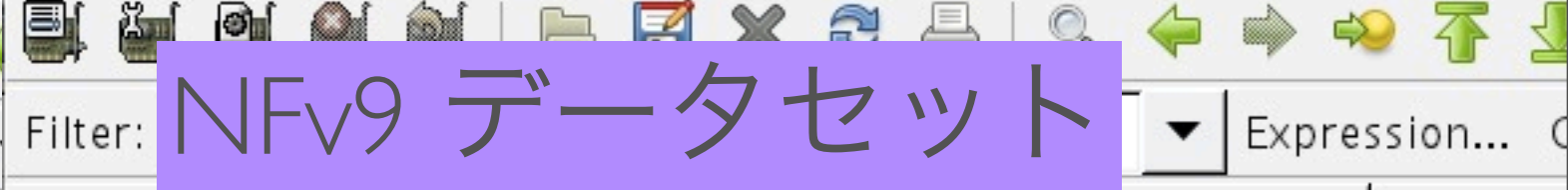
▶ Field (10/19): IPV6_OPTION_HEADERS

▶ Field (11/19): L4_SRC_PORT



No.	Time	Source
-----	------	--------

▶ Frame 18: 630 bytes on wire (5040 bits), 630 bytes captured (5040 bits) on interface
 ▶ Ethernet II, Src: Netscreen_24:47:d2 (00:10:db:24:47:d2), Dst: Dell_39:b6:00 (00:07:09:39:b6:00)
 ▶ Internet Protocol Version 4, Src: 10.9.100.140 (10.9.100.140), Dst: 50.0.125.1 (50.0.125.1)
 ▶ User Datagram Protocol, Src Port: 33018 (33018), Dst Port: 80 (80)
 ▼ Cisco NetFlow/IPFIX
 Version: 10
 Length: 588
 ▶ Timestamp: Sep 26, 2011 16:46:12.000000000 JST
 FlowSequence: 182163
 Observation Domain Id: 512
 ▼ Set 1
 FlowSet Id: (Data) (256)
 FlowSet Length: 572
 ▼ Flow 1
 SrcAddr: 100.0.125.1 (100.0.125.1)
 DstAddr: 50.0.125.1 (50.0.125.1)
 IP ToS: 0x00
 Protocol: 6
 SrcPort: 49600
 DstPort: 80
 ICMP Type: 0
 InputInt: 643
 SrcMask: 24
 DstMask: 24
 SrcAS: 3000
 DstAS: 2000
 NextHop: 10.0.1.100 (10.0.1.100)
 TCP Flags: 0x00
 OutputInt: 630
 Octets: 73164
 Packets: 403



No.	Time	Source	Destination
-----	------	--------	-------------

▶ Frame 37: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface
 ▶ Ethernet II, Src: Inventec_e7:cc:23 (00:a0:d1:e7:cc:23), Dst: Dell_39:b6:00 (00:07:09:39:b6:00)
 ▶ Internet Protocol Version 4, Src: 72.16.1.12 (72.16.1.12), Dst: 50.0.125.1 (50.0.125.1)
 ▶ User Datagram Protocol, Src Port: 45165 (45165), Dst Port: iop (2055)
 ▼ Cisco NetFlow/IPFIX
 Version: 9
 Count: 1
 SysUptime: 1170059127
 ▶ Timestamp: Jun 10, 2010 17:47:25.000000000 JST
 FlowSequence: 507119
 SourceId: 17
 ▼ FlowSet 1
 FlowSet Id: (Data) (260)
 FlowSet Length: 64
 ▼ Flow 1
 Packets: 2
 Octets: 2498
 SrcAddr: [REDACTED]
 DstAddr: [REDACTED]
 InputInt: 24
 OutputInt: 7
 ▶ [Duration: 4.363000000 seconds]
 SrcPort: 51368
 DstPort: 53872
 SrcAS: 0
 DstAS: 0
 BGPNextHop: [REDACTED]
 SrcMask: 24
 DstMask: 16

世の中の実装

(exporter)

- Commercial
 - Juniper MX series
 - Extreme BlackDiamond 8900modules
 - SonicWall,NORTEL
- Open Source
 - nProbe,VERMONT,(softflowd)

世の中の実装 (Collector)

- Commercial
 - GenieATM, Arbor PeakflowSP
 - InMon, Scrutinizer, Netflow Analyzer, ORION NTA
 - etc...
- Open Source
 - ntop, Vermont,

transport

- IPFIXはtransportに依存しない設計
- SCTPはMUST
- TCPとUDPはMAY
- 現状は。。。

情報要素(IE)

- IPFIXは多数のIEがのせられる
- 現状は。。。。