Configure NetFlow/IPFIX for Telemetry Ingest on SNA

Contents

Introduction
Prerequisites
Requirements
Components Used
Background information
Configure
Required Fields
Recommended Fields
Best Practice
Verify

Introduction

This document describes the best practices and basic configuration of Netflow/IPFIX that Secure Network Analytics (SNA) needs for telemetry ingest.

Prerequisites

- Cisco SNA knowledge
- NetFlow/IPFIX knowledge

Requirements

- Secure Network Analytics in 7.2.1 or newer
- Flow Collector in 7.2.1 or newer
- CLI access as root to the Flow Collector

Components Used

- This depends completely on your network design and the devices that you have selected to send NetFlow/IPFIX to Secure Network Analytics. NetFlow/IPFIX configuration is different on each exporter, for detailed configuration please contact the support team of each exporter.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background information

The Flow Collector is a SNA appliance in charge of collect, process and store flows that are sent to Secure Network Analytics. For NetFlow version 9 or IPFIX, several fields could be included on NetFlow/IPFIX template to add more information related to network traffic, however, there are 9 specific fields that must be included in NetFlow/IPFIX template for the Flow Collector to process those Flows. Flow Collector does not process incoming flows which includes a non-valid template, therefore SNA does not display flow information of those exporters under Web UI or Desktop Client.

Configure

Required Fields

Next fields must be included on NetFlow/IPFIX template for Telemetry ingest. Ensure that these 9 fields are included on NetFlow/IPFIX template, in order for Secure Network Analytics to process incoming flows.

- Source IP Address
- Destination IP Address
- Source Port
- Destination Port
- Layer 3 Protocol
- Bytes Count
- Packet count
- Flow Start Time
- Flow End Time

> **Note**: More fields could be included on NetFlow/IPFIX configuration, however the previous fields are the minimum requirements of Secure Network Analytics for Telemetry Ingest.

Recommended Fields

It is recommended to include the next fields on NetFlow/IPFIX template to gather information about interface information, this configuration is required to show interface information such as name and speed:

- Interface input
- Interface output

Best Practice

Additionally, next settings are recommended as best practices to ensure a proper performance of Secure Network Analytics.

- Set active timeout to 60 seconds
- Set inactive timeout to 15 seconds
- Set template timeout to 30 seconds

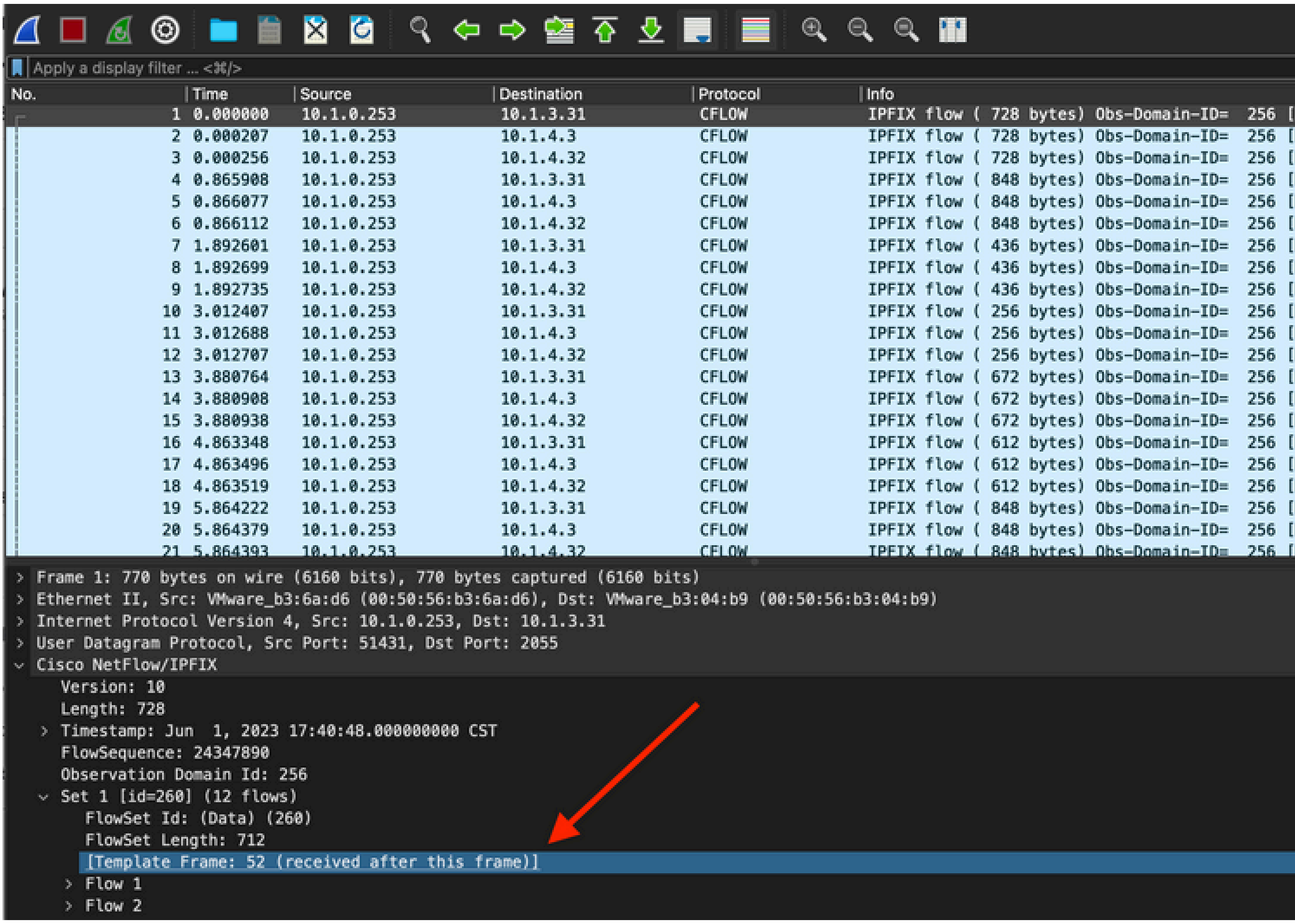
> **Note**: Default port for NetFlow is 2055, however you can select another port, please ensure to use the same port during lc-ast process on Flow Collector(s).

Verify

To validate NetFlow/IPFIX template configuration, you can run a packet capture between the exporter and Flow Collector. Log into the Flow Collector with **root** user via SSH and run command:

```
tcpdump -nli [Collecting_Interface] host [Exporter_IP_Address] and port [NetFlow_Port] -w /lancope/var/t
```

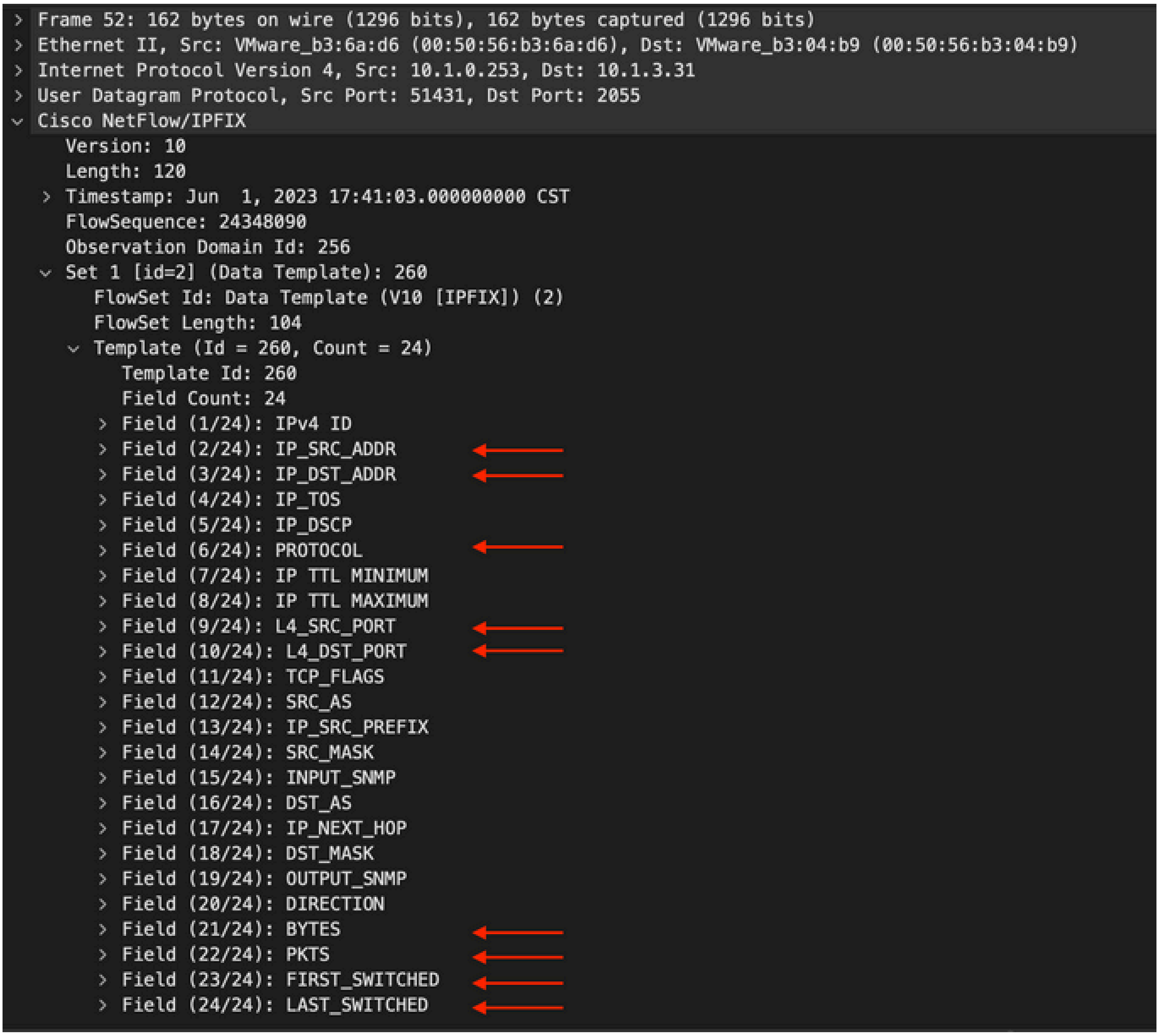
- Use a SCP tool to export the packet capture from the Flow Collector (located in **/lancope/var/tcpdump**) to your local machine and then open it on Wireshark



```
No.   Time       Source        Destination   Protocol   Info
    1 0.000000   10.1.0.253    10.1.3.31     CFLOW      IPFIX flow ( 728 bytes) Obs-Domain-ID=   256 [
    2 0.000207   10.1.0.253    10.1.4.3      CFLOW      IPFIX flow ( 728 bytes) Obs-Domain-ID=   256 [
    3 0.000256   10.1.0.253    10.1.4.32     CFLOW      IPFIX flow ( 728 bytes) Obs-Domain-ID=   256 [
    4 0.865908   10.1.0.253    10.1.3.31     CFLOW      IPFIX flow ( 848 bytes) Obs-Domain-ID=   256 [
    5 0.866077   10.1.0.253    10.1.4.3      CFLOW      IPFIX flow ( 848 bytes) Obs-Domain-ID=   256 [
    6 0.866112   10.1.0.253    10.1.4.32     CFLOW      IPFIX flow ( 848 bytes) Obs-Domain-ID=   256 [
    7 1.892601   10.1.0.253    10.1.3.31     CFLOW      IPFIX flow ( 436 bytes) Obs-Domain-ID=   256 [
    8 1.892699   10.1.0.253    10.1.4.3      CFLOW      IPFIX flow ( 436 bytes) Obs-Domain-ID=   256 [
    9 1.892735   10.1.0.253    10.1.4.32     CFLOW      IPFIX flow ( 436 bytes) Obs-Domain-ID=   256 [
   10 3.012407   10.1.0.253    10.1.3.31     CFLOW      IPFIX flow ( 256 bytes) Obs-Domain-ID=   256 [
   11 3.012688   10.1.0.253    10.1.4.3      CFLOW      IPFIX flow ( 256 bytes) Obs-Domain-ID=   256 [
   12 3.012707   10.1.0.253    10.1.4.32     CFLOW      IPFIX flow ( 256 bytes) Obs-Domain-ID=   256 [
   13 3.880764   10.1.0.253    10.1.3.31     CFLOW      IPFIX flow ( 672 bytes) Obs-Domain-ID=   256 [
   14 3.880908   10.1.0.253    10.1.4.3      CFLOW      IPFIX flow ( 672 bytes) Obs-Domain-ID=   256 [
   15 3.880938   10.1.0.253    10.1.4.32     CFLOW      IPFIX flow ( 672 bytes) Obs-Domain-ID=   256 [
   16 4.863348   10.1.0.253    10.1.3.31     CFLOW      IPFIX flow ( 612 bytes) Obs-Domain-ID=   256 [
   17 4.863496   10.1.0.253    10.1.4.3      CFLOW      IPFIX flow ( 612 bytes) Obs-Domain-ID=   256 [
   18 4.863519   10.1.0.253    10.1.4.32     CFLOW      IPFIX flow ( 612 bytes) Obs-Domain-ID=   256 [
   19 5.864222   10.1.0.253    10.1.3.31     CFLOW      IPFIX flow ( 848 bytes) Obs-Domain-ID=   256 [
   20 5.864379   10.1.0.253    10.1.4.3      CFLOW      IPFIX flow ( 848 bytes) Obs-Domain-ID=   256 [
   21 5.864393   10.1.0.253    10.1.4.32     CFLOW      IPFIX flow ( 848 bytes) Obs-Domain-ID=   256 [
```

```
> Frame 1: 770 bytes on wire (6160 bits), 770 bytes captured (6160 bits)
> Ethernet II, Src: VMware_b3:6a:d6 (00:50:56:b3:6a:d6), Dst: VMware_b3:04:b9 (00:50:56:b3:04:b9)
> Internet Protocol Version 4, Src: 10.1.0.253, Dst: 10.1.3.31
> User Datagram Protocol, Src Port: 51431, Dst Port: 2055
v Cisco NetFlow/IPFIX
    Version: 10
    Length: 728
  > Timestamp: Jun  1, 2023 17:40:48.000000000 CST
    FlowSequence: 24347890
    Observation Domain Id: 256
  v Set 1 [id=260] (12 flows)
      FlowSet Id: (Data) (260)
      FlowSet Length: 712
      [Template Frame: 52 (received after this frame)]
    > Flow 1
    > Flow 2
```

- Identify the frame in which the NetFlow/IPFIX template was received and open it to validate the fields that the template includes



```
> Frame 52: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits)
> Ethernet II, Src: VMware_b3:6a:d6 (00:50:56:b3:6a:d6), Dst: VMware_b3:04:b9 (00:50:56:b3:04:b9)
> Internet Protocol Version 4, Src: 10.1.0.253, Dst: 10.1.3.31
> User Datagram Protocol, Src Port: 51431, Dst Port: 2055
v Cisco NetFlow/IPFIX
    Version: 10
    Length: 120
  > Timestamp: Jun  1, 2023 17:41:03.000000000 CST
    FlowSequence: 24348090
    Observation Domain Id: 256
  v Set 1 [id=2] (Data Template): 260
      FlowSet Id: Data Template (V10 [IPFIX]) (2)
      FlowSet Length: 104
    v Template (Id = 260, Count = 24)
        Template Id: 260
        Field Count: 24
      > Field (1/24): IPv4 ID
      > Field (2/24): IP_SRC_ADDR
      > Field (3/24): IP_DST_ADDR
      > Field (4/24): IP_TOS
      > Field (5/24): IP_DSCP
      > Field (6/24): PROTOCOL
      > Field (7/24): IP TTL MINIMUM
      > Field (8/24): IP TTL MAXIMUM
      > Field (9/24): L4_SRC_PORT
      > Field (10/24): L4_DST_PORT
      > Field (11/24): TCP_FLAGS
      > Field (12/24): SRC_AS
      > Field (13/24): IP_SRC_PREFIX
      > Field (14/24): SRC_MASK
      > Field (15/24): INPUT_SNMP
      > Field (16/24): DST_AS
      > Field (17/24): IP_NEXT_HOP
      > Field (18/24): DST_MASK
      > Field (19/24): OUTPUT_SNMP
      > Field (20/24): DIRECTION
      > Field (21/24): BYTES
      > Field (22/24): PKTS
      > Field (23/24): FIRST_SWITCHED
      > Field (24/24): LAST_SWITCHED
```

Note: The field names showed can look different on each exporter, this is just a reference of how you can validate those fields.