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

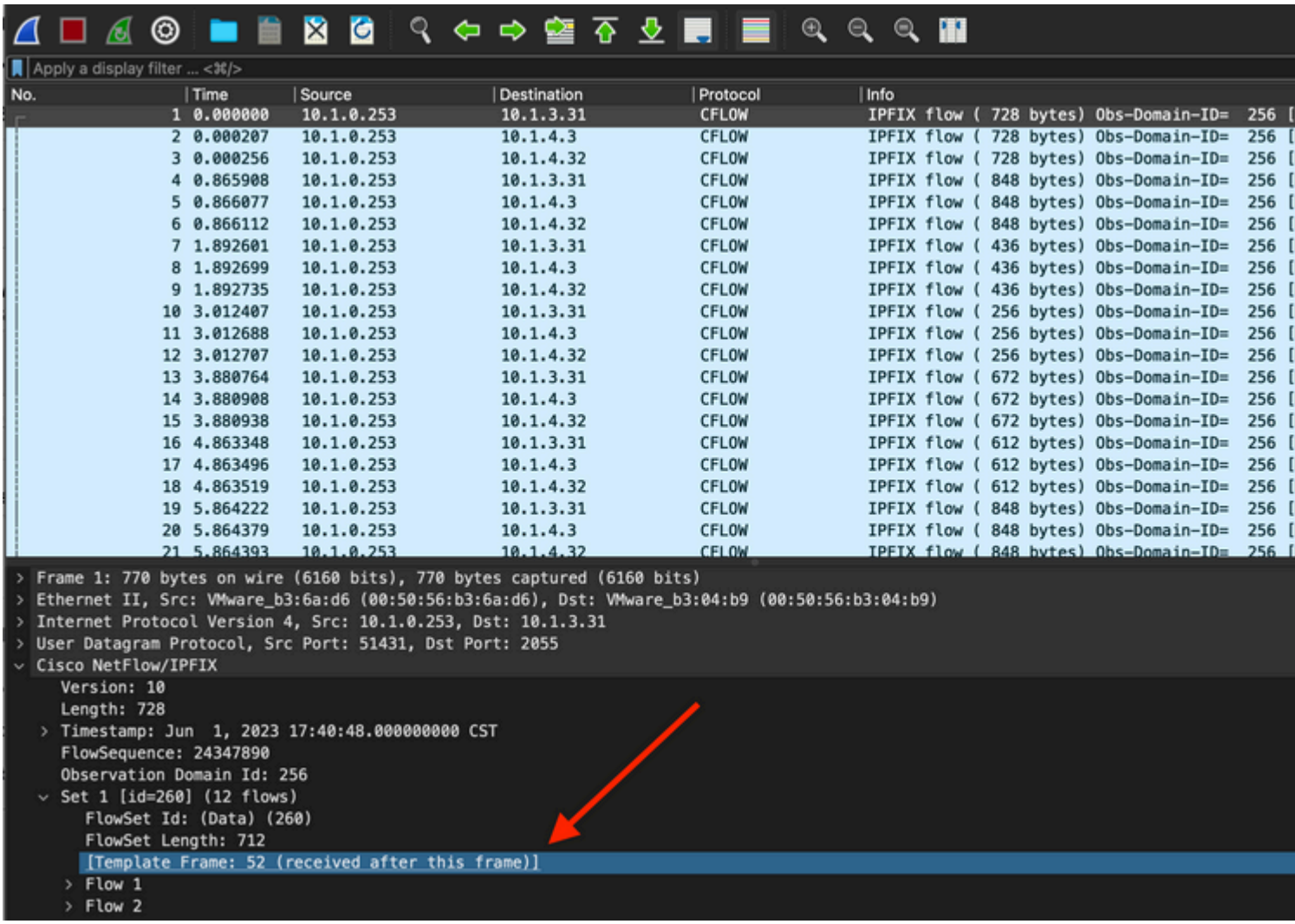
> **Note**: Default port for NetFlow is 2055, however you can select another port, please ensure to use the same port during lc-ast process on Flow Collector(s).

Verify

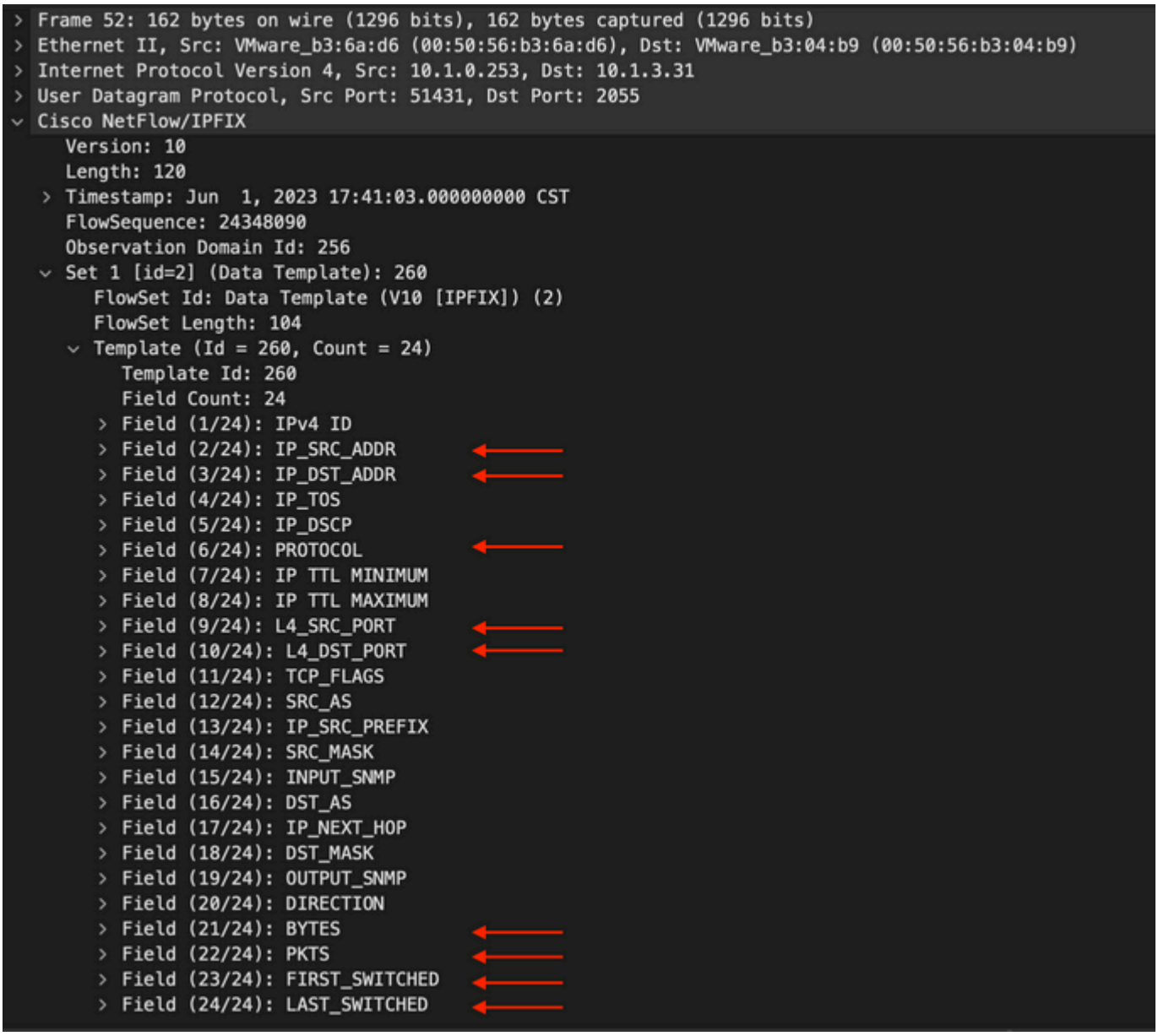
To validate NetFlow/IPFIX template configuration, you can run a packet capture between the exporter and Flow Collector. Log into the Flow Collector with **root** user via SSH and run command:

```
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



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



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