在SNA上配置遥测接收的NetFlow/IPFIX

目录

简介

本文档介绍安全网络分析(SNA)遥测接收所需的Netflow/IPFIX的最佳实践和基本配置。

先决条件

- Cisco SNA知识
- NetFlow/IPFIX知识

要求

- 7.2.1或更高版本中的安全网络分析
- 7.2.1或更高版本的流量收集器
- 作为流量收集器根的CLI访问

使用的组件

- 这完全取决于您的网络设计和您选择将NetFlow/IPFIX发送到安全网络分析的设备。每个导出器上的NetFlow/IPFIX配置不同，有关详细配置，请联系每个导出器的支持团队。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

流量收集器是一种SNA设备，负责收集、处理和存储发送到安全网络分析的流量。对于NetFlow版本9或IPFIX，可以在NetFlow/IPFIX模板上包含多个字段，以添加有关网络流量的详细信息，但是，NetFlow/IPFIX模板中必须包含9个特定字段，流量收集器才能处理这些流量。流量收集器不会处

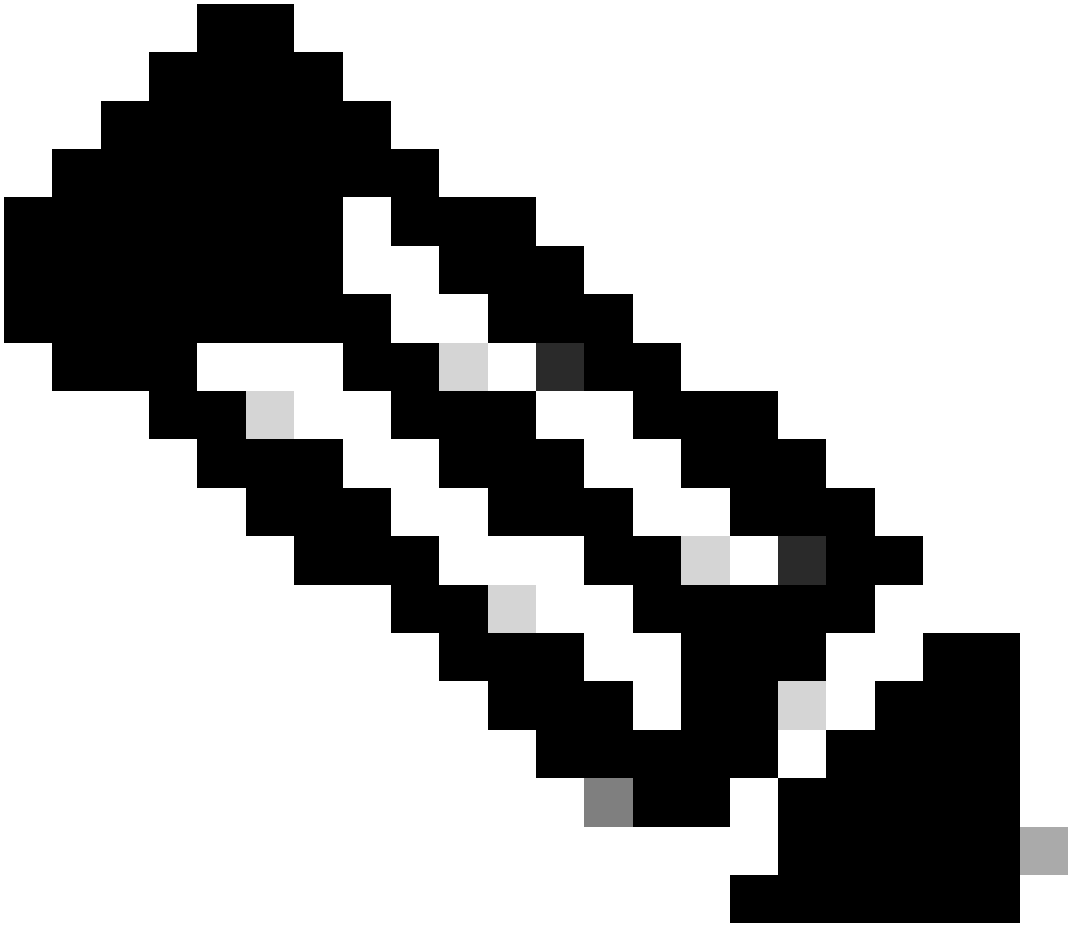
理包含无效模板的传入流量，因此SNA不会在Web UI或桌面客户端下显示这些导出器的流量信息。

配置

必需字段

NetFlow/IPFIX模板中必须包含用于遥测接收的下一个字段。确保在NetFlow/IPFIX模板中包含这9个字段，以便安全网络分析处理传入流量。

- 源 IP 地址
- 目的 IP 地址
- 源端口
- 目标端口
- 第3层协议
- 字节计数
- 数据包计数
- 流开始时间
- 流结束时间



注意：NetFlow/IPFIX配置中可以包含更多字段，但之前的字段是用于遥测接收的安全网络分析的最低要求。

推荐字段

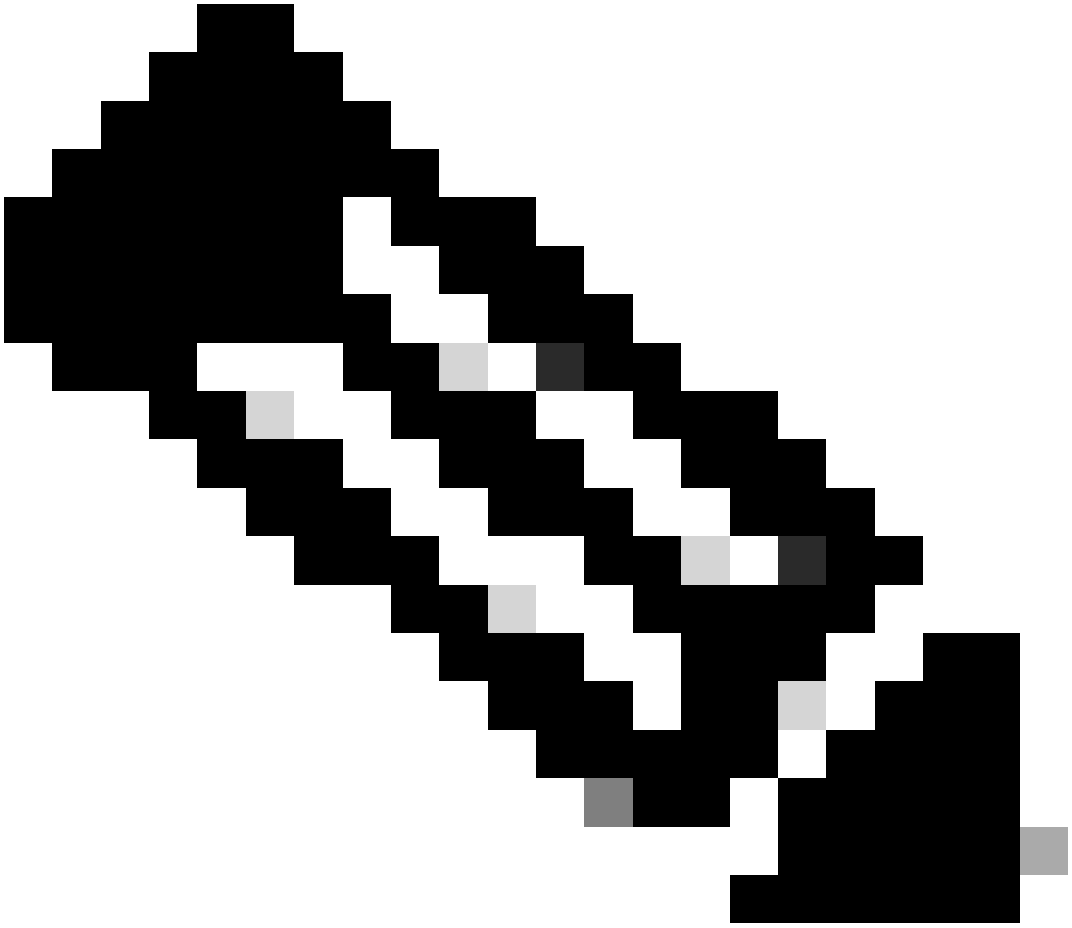
建议在NetFlow/IPFIX模板中包括以下字段以收集有关接口信息的信息，需要使用此配置来显示接口信息（例如名称和速度）：

- 接口输入
- 接口输出

最佳实践

此外，建议使用后续设置作为最佳实践，以确保安全网络分析的正确性能。

- 将活动超时设置为60秒
- 将非活动超时设置为15秒
- 将模板超时设置为30秒



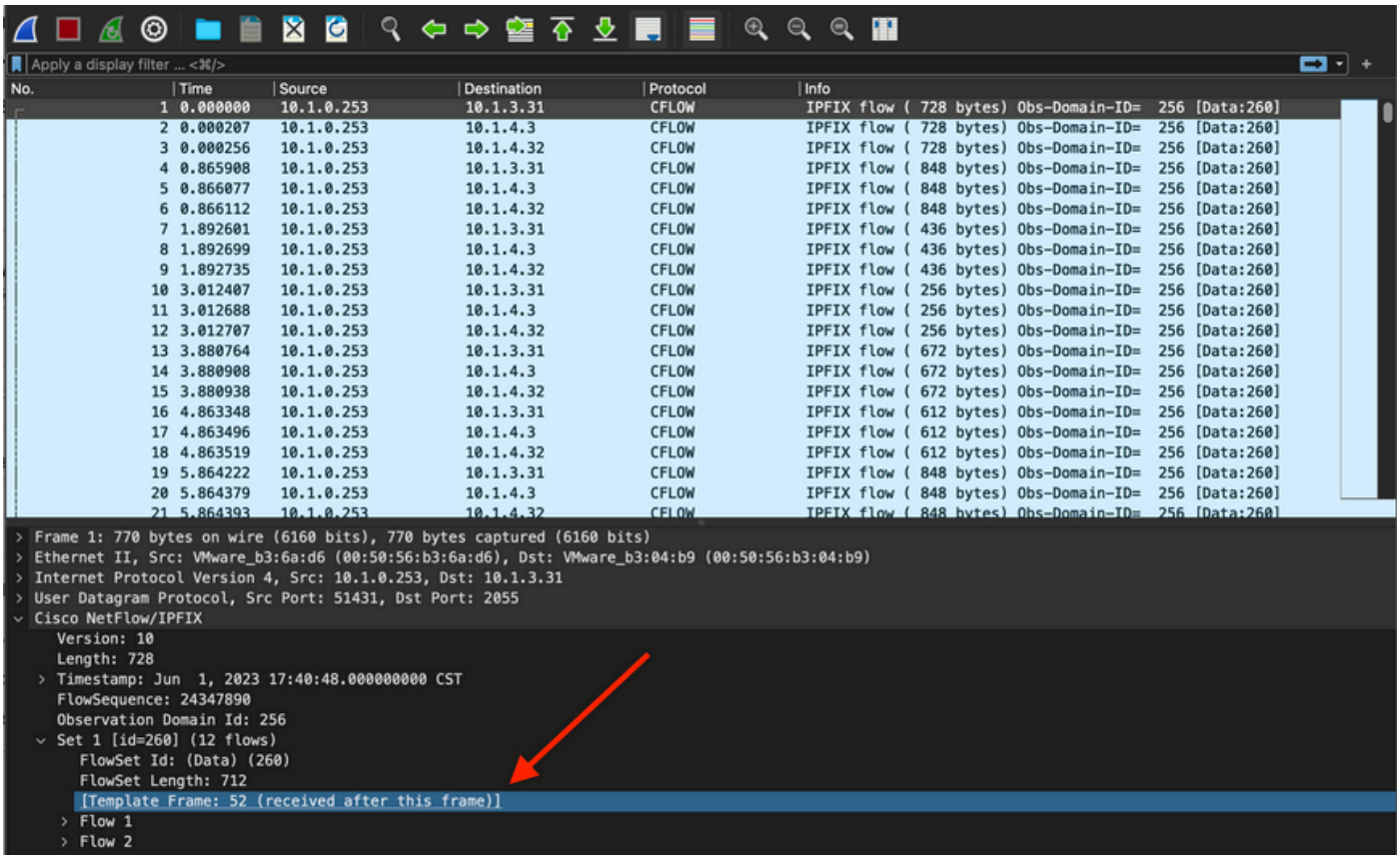
注意：NetFlow的默认端口是2055，但您可以选择其他端口，请确保在流量收集器的lc-ast过程中使用同一端口。

验证

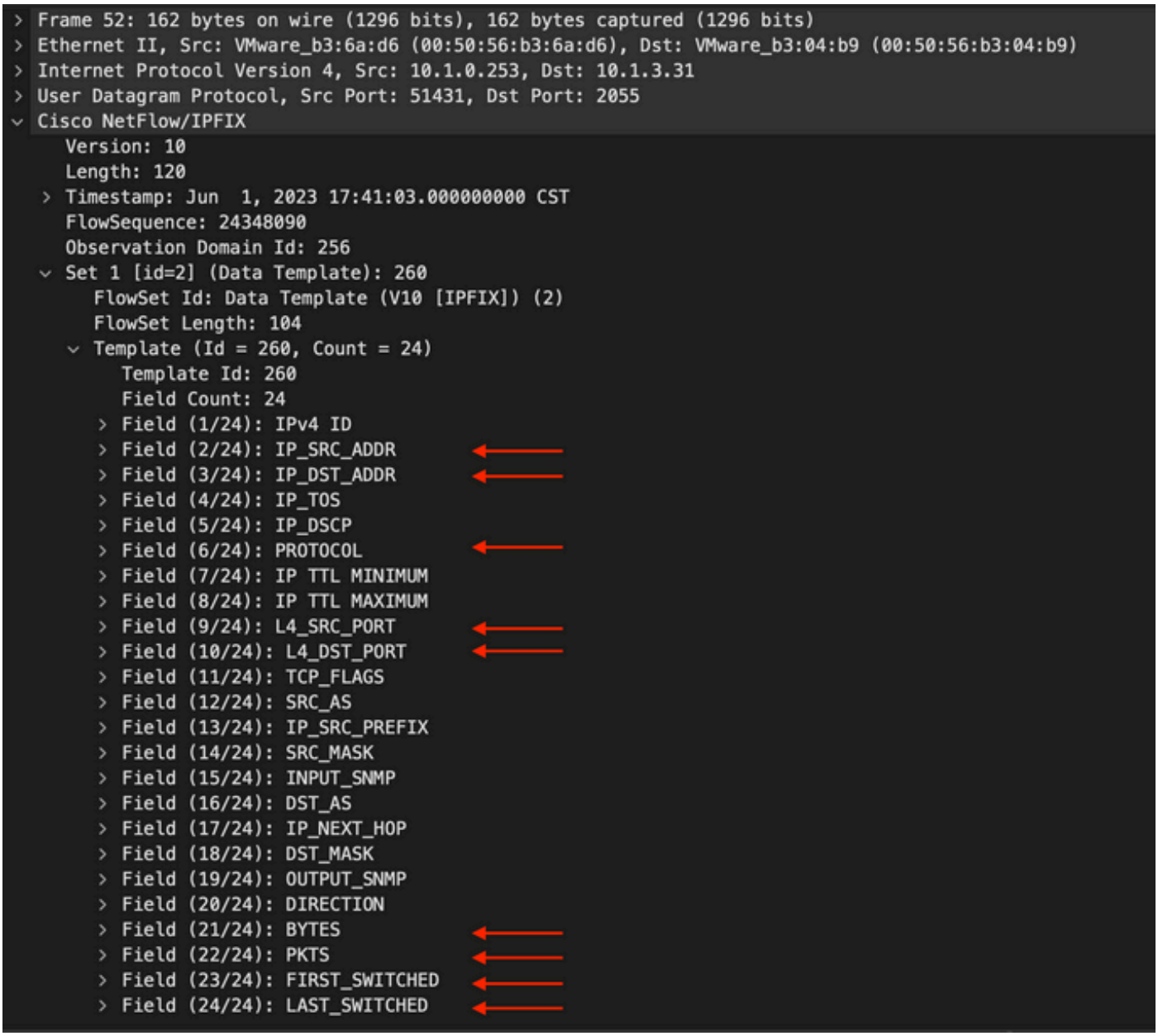
要验证NetFlow/IPFIX模板配置，您可以在导出器和流量收集器之间运行数据包捕获。使用root用户通过SSH登录流量收集器并运行命令：

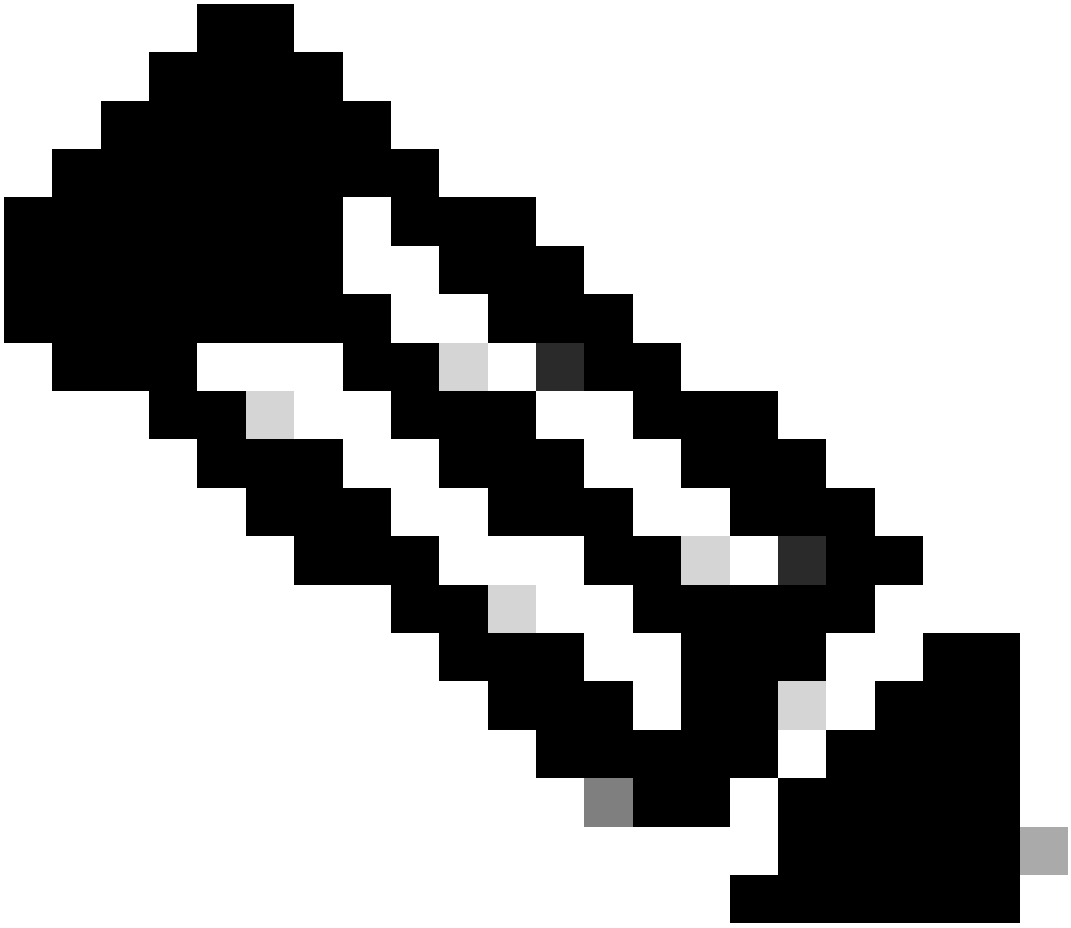
```
tcpdump -nli [Collecting_Interface] host [Exporter_IP_Address] and port [NetFlow_Port] -w /lancope/var/
```

- 使用SCP工具将数据包捕获从流量收集器(位于/lancope/var/tcpdump中)导出到您的本地计算机，然后在Wireshark上打开它



- 确定接收NetFlow/IPFIX模板的帧并打开该帧以验证模板所包含的字段


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
Cisco NetFlow/IPFIX
Version: 10
Length: 120
Timestamp: Jun 1, 2023 17:41:03.000000000 CST
FlowSequence: 24348090
Observation Domain Id: 256
Set 1 [id=2] (Data Template): 260
FlowSet Id: Data Template (V10 [IPFIX]) (2)
FlowSet Length: 104
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



注意：显示的字段名称在每个导出器上可能不同，这只是对如何验证这些字段的参考。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。