在安全网络分析中排除NetFlow/IPFIX遥测接收故障

目录

简介

先决条件

- 要求
- 配置指南
- 使用的组件

背景信息

- 必需字段

故障排除过程

- 验证NetFlow/IPFIX遥测接收
- 验证NetFlow/IPFIX模板
- 添加缺少的字段后验证NetFlow/IPFIX遥测接收
- 验证NetFlow/IPFIX遥测接收端口
- 验证是否已启用NetFlow/IPFIX遥测接收NetFlow选项

相关信息

简介

本文档介绍如何对安全网络分析(SNA)中的Netflow遥测接收进行故障排除。

先决条件

- Cisco SNA知识
- NetFlow/IPFIX知识

要求

- 7.5.0或更高版本中的安全网络分析
- 7.5.0或更高版本中的流量收集器
- 以系统管理员身份访问流量收集器
- 以管理员身份访问流量收集器的管理员UI

配置指南

- 配置NetFlow/IPFIX以便在安全网络分析上进行遥测接收

使用的组件

- 7.5.0上的SNA管理器和流量收集器
- Wireshark软件

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，NetFlow/IPFIX模板上可以包含多个字段，以添加有关网络流量的详细信息，但是，对于流量收集器，NetFlow/IPFIX模板中必须包含9个特定字段，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。

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。确保这9个字段包含在NetFlow/IPFIX模板中，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配置中可能包含更多字段，但之前的字段是遥测接收的安全网络分析的最低要求。

故障排除过程

验证NetFlow/IPFIX遥测接收

要确认SNA流量收集器是否从导出器接收和插入NetFlow/IPFIX遥感勘测，请执行以下操作：

1. 使用管理员凭证登录到SNA流量收集器管理UI:https://<流量收集器IP地址>/swa/login.html
2. 在左侧面板上，导航到支持 > 浏览文件
3. 导航到下一个文件夹：sw > today > logs
4. 单击sw.log文件将其下载到本地计算机，然后在文本编辑器中将其打开。
5. 在日志底部搜索这些行，每五分钟创建一次此摘要：

```
18:45:00 I-sch-t: process_5_min_period: begin
18:45:00 I-sch-t: process_5_min_period: periods(177)
18:45:00 S-per-t: Performance Period 177
18:45:00 S-per-t:     Engine status Status normal
18:45:00 S-per-t:     Processed 6948 flows at 24 fps this period
18:45:00 S-per-t:     Processed 4226 biflows at 15 fps this period
18:45:00 S-per-t:     Dropped 0 flows this period
18:45:00 S-per-t:     Discarded 4358 flows this period due to insufficient template data
18:45:00 S-per-t:     Processed 1838743 flows at 35 fps today
18:45:00 S-per-t:     Dropped 0 flows today
18:45:00 S-per-t:     Discarded 11069 flows today due to insufficient template data
18:45:00 S-per-t:     Process instance 0 processed 3372 flows at 12 fps this period
18:45:00 S-per-t:     Process instance 0 processed 2066 biflows at 7 fps this period
18:45:00 S-per-t:     Process instance 1 processed 3576 flows at 12 fps this period
18:45:00 S-per-t:     Process instance 1 processed 2160 biflows at 8 fps this period
18:45:00 S-per-t:     Inserted 2048 flow stats at 7 fps this period
18:45:00 S-per-t:     Inserted 2013 interface stats at 7 fps this period
18:45:00 S-per-t:     Inserted 470932 flow stats at 9 fps today
18:45:00 S-per-t:     Inserted 678994 interface stats at 13 fps today
```



注意：第8行表示由于上一时段模板数据不足，有些流被丢弃。

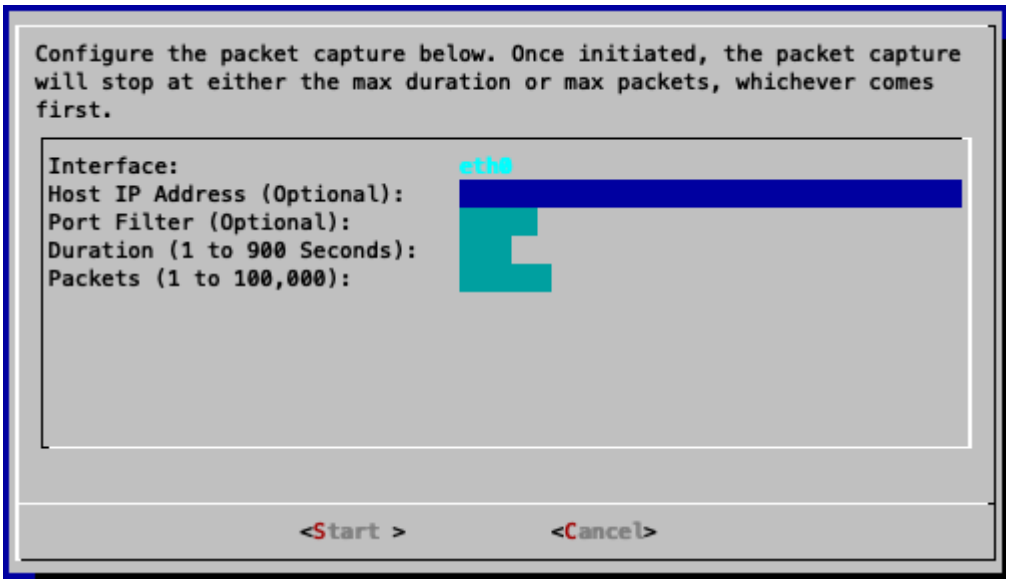
验证NetFlow/IPFIX模板

要确认NetfFlow/IPFIX模板中包含的字段，请执行以下操作：

1.使用sysadmin凭证登录到SNA流量收集器CLI。

2.在SystemConfig菜单中，导航到：Advanced > Packet Capture

3.输入未在SNA上显示流的导出器的信息：



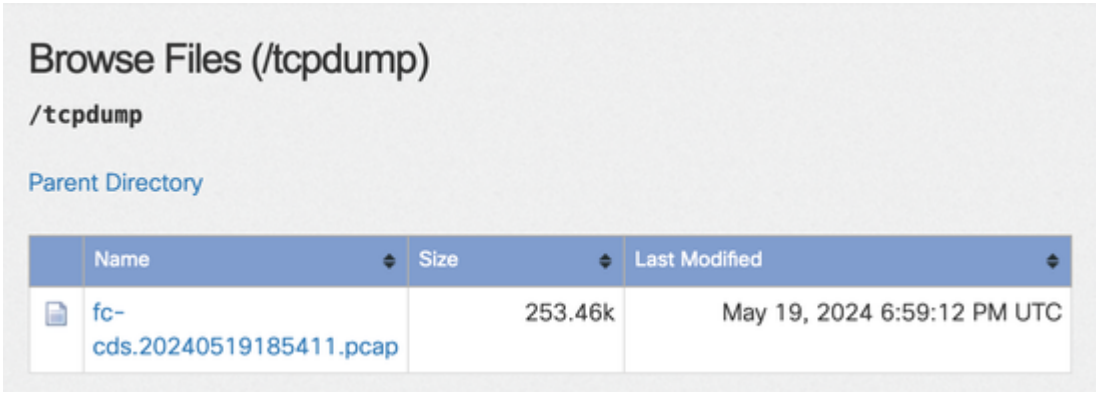
4.等待流程完成。

5.要下载文件，请使用管理员凭证登录到SNA流量收集器管理UI:https://<流量收集器IP地址>/swa/login.html

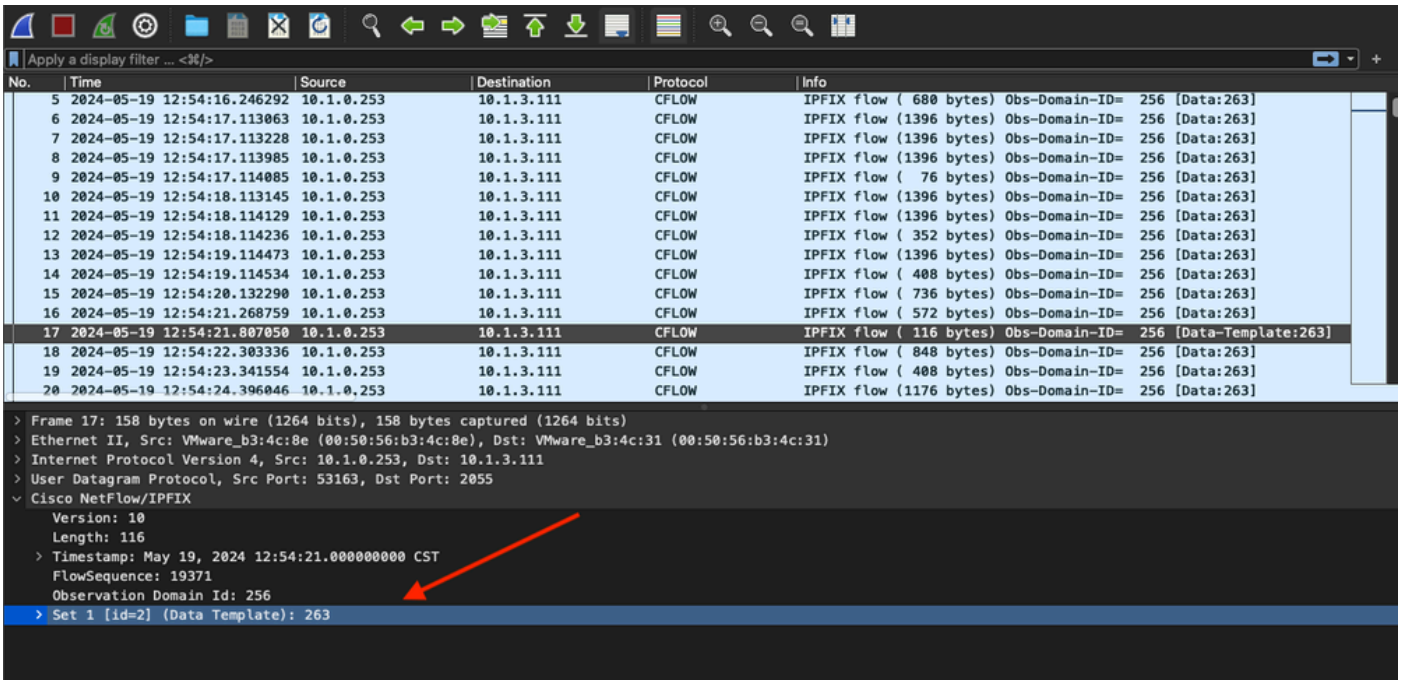
6.在左侧面板上，导航到支持 > 浏览文件

7.定位至下一个文件夹：tcpdump

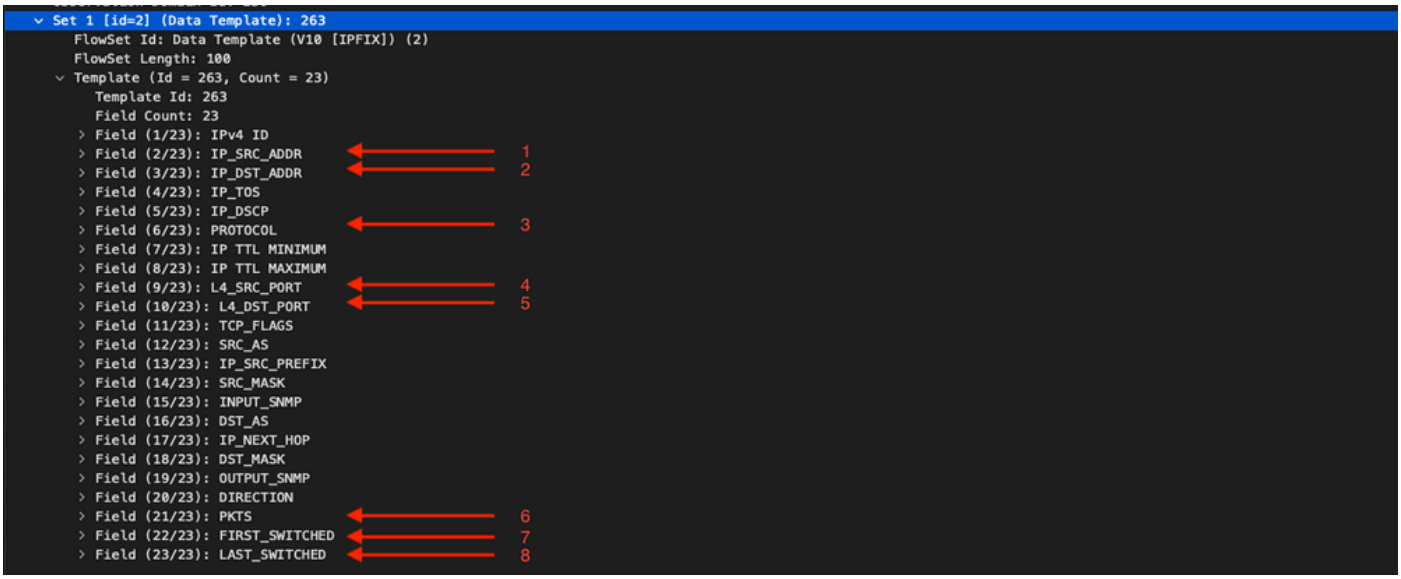
8.单击数据包捕获文件，将其下载到本地计算机，并在Wireshark上打开：



9. 确定接收NetFlow/IPFIX模板的帧。



10.验证9个必填字段是否显示在模板上



注意：请注意，模板上SNA进行遥测接收所需的9个必填字段只有8个，对于此场景，缺少BYTES字段。

添加缺少的字段后验证NetFlow/IPFIX遥测接收

要确认SNA流量收集器是否在更改后接收和插入来自导出器的NetFlow/IPFIX遥感勘测，请执行以下操作：

1. 使用管理员凭证登录到SNA流量收集器管理UI:https://<流量收集器IP地址>/swa/login.html
2. 在左侧面板上，导航到支持 > 浏览文件
3. 导航到下一个文件夹：sw > today > logs
4. 单击sw.log文件将其下载到本地计算机，然后在文本编辑器中打开。
5. 在日志底部搜索这些行

```
19:20:00 I-sch-t: process_5_min_period: begin
19:20:00 I-sch-t: process_5_min_period: periods(184)
19:20:00 S-per-t: Performance Period 184
19:20:00 S-per-t:     Engine status Status normal
19:20:00 S-per-t:     Processed 10992 flows at 37 fps this period
19:20:00 S-per-t:     Processed 4176 biflows at 14 fps this period
19:20:00 S-per-t:     Dropped 0 flows this period
19:20:00 S-per-t:     Discarded 0 flows this period due to insufficient template data
19:20:00 S-per-t:     Processed 1896017 flows at 35 fps today
19:20:00 S-per-t:     Dropped 0 flows today
19:20:00 S-per-t:     Discarded 36041 flows today due to insufficient template data
19:20:00 S-per-t:     Process instance 0 processed 5575 flows at 19 fps this period
19:20:00 S-per-t:     Process instance 0 processed 2195 biflows at 8 fps this period
19:20:00 S-per-t:     Process instance 1 processed 5417 flows at 19 fps this period
19:20:00 S-per-t:     Process instance 1 processed 1981 biflows at 7 fps this period
19:20:00 S-per-t:     Inserted 2878 flow stats at 10 fps this period
19:20:00 S-per-t:     Inserted 4510 interface stats at 16 fps this period
19:20:00 S-per-t:     Inserted 486734 flow stats at 9 fps today
19:20:00 S-per-t:     Inserted 696260 interface stats at 13 fps today
```



注意：第8行表示最后一个时段没有丢弃的流。

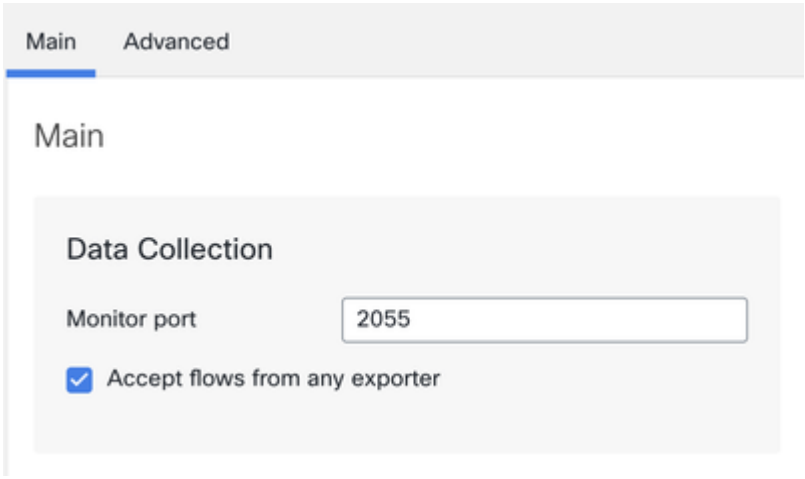
验证NetFlow/IPFIX遥测接收端口

要确认SNA流量收集器是否从正确端口上的导出器接收NetFlow/IPFIX遥感勘测，请执行以下操作：

1.使用具有管理员权限的用户登录SNA Web UI。

2.在顶部菜单上，导航至“配置”并选择“流量收集器”

3.确认SNA流量收集器使用导出器配置用于发送NetFlow/IPFIX的相同端口



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首次设置过程中使用同一端口。

验证是否已启用NetFlow/IPFIX遥测接收NetFlow选项

要确认是否已启用NetFlow/IPFIX遥测接收的SNA流量收集器选项，请执行以下操作：

1. 使用管理员凭证登录到SNA流量收集器管理UI:https://<流量收集器IP地址>/swa/login.html
2. 在左侧面板上，导航到支持 > 高级设置
3. 确认选项enable_netflow设置为1:



相关信息

- 如需其他帮助，请联系技术支持中心(TAC)。联系时需要提供有效的支持合同：思科全球支持联系信息
- 您还可以访问思科安全分析社区，此处。
- 技术支持和文档 - Cisco Systems

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）。