Solución de problemas de NetFlow/IPFIX Telemetry Ingest en Secure Network Analytics

Contenido

Introducción

Este documento describe cómo resolver problemas de ingesta de telemetría de Netflow en Secure Network Analytics (SNA).

Prerequisites

- Conocimiento de Cisco SNA
- Conocimiento de NetFlow/IPFIX

Requirements

- Secure Network Analytics en 7.5.0 o posterior
- Flow Collector en 7.5.0 o posterior
- Acceso CLI como administrador del sistema al Flow Collector
- Acceso a la IU de administrador como administrador del Flow Collector

Guías de Configuración

- Configuración de NetFlow/IPFIX para la ingesta de telemetría en Secure Network Analytics

Componentes Utilizados

- Administrador SNA y Flow Collector en 7.5.0
- Software Wireshark

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

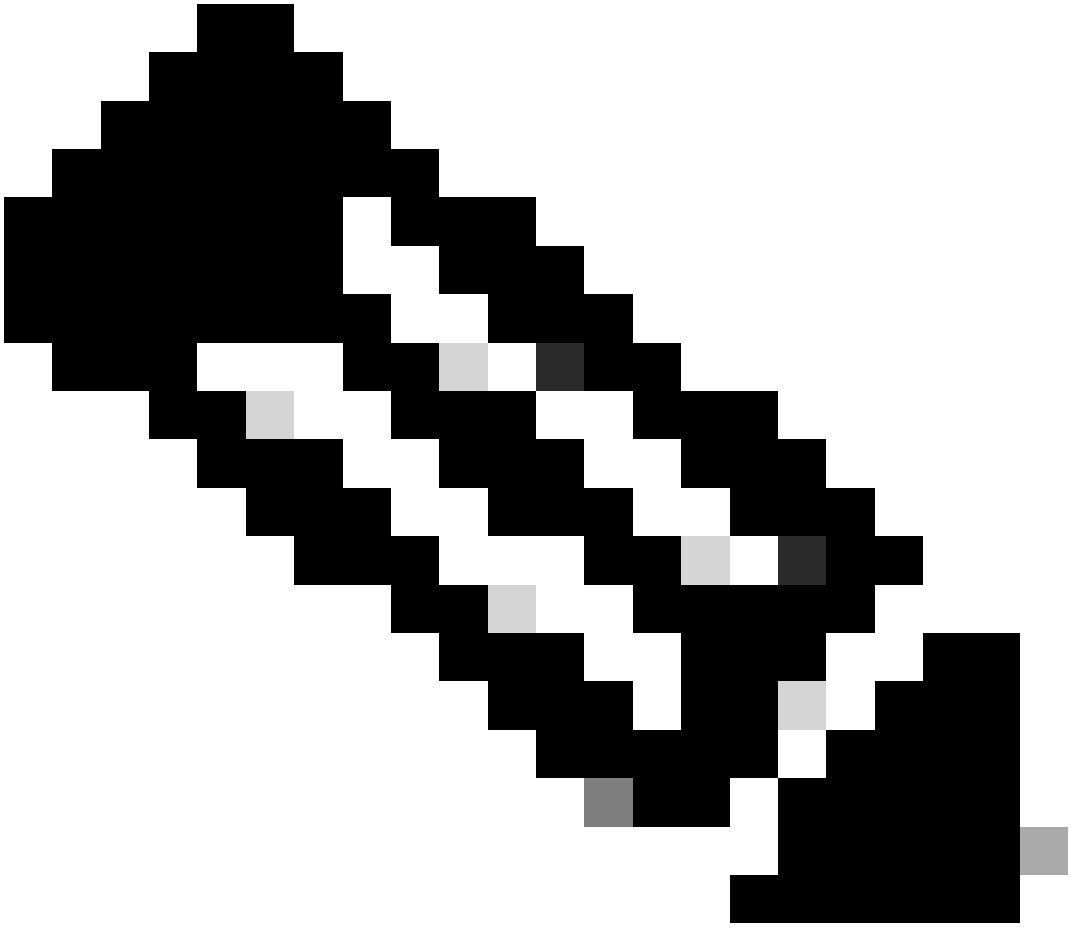
Antecedentes

Flow Collector es un dispositivo SNA encargado de recopilar, procesar y almacenar los flujos que se envían a Secure Network Analytics. Para NetFlow versión 9 o IPFIX, se podrían incluir varios campos en la plantilla NetFlow/IPFIX para agregar más información relacionada con el tráfico de red; sin embargo, hay 9 campos específicos que se deben incluir en la plantilla NetFlow/IPFIX para que Flow Collector procese esos flujos. Flow Collector no procesa los flujos entrantes que incluyen una plantilla no válida, por lo que SNA no muestra la información de flujo de esos exportadores en la interfaz de usuario web o el cliente de escritorio.

Campos obligatorios

Los siguientes campos deben incluirse en la plantilla NetFlow/IPFIX para la ingesta de telemetría. Asegúrese de que estos 9 campos estén incluidos en la plantilla NetFlow/IPFIX para que Secure Network Analytics procese los flujos entrantes.

- Dirección IP de origen
- Dirección IP de destino
- Puerto de Origen
- Puerto de Destino
- Protocolo de capa 3
- Recuento de bytes
- Recuento de paquetes
- Tiempo de inicio de flujo
- Tiempo de finalización de flujo



Nota: Se podrían incluir más campos en la configuración de NetFlow/IPFIX; sin embargo, los campos anteriores son los requisitos mínimos de Secure Network Analytics for Telemetry Ingest.

Proceso de Troubleshooting

Verificar la ingesta de telemetría de NetFlow/IPFIX

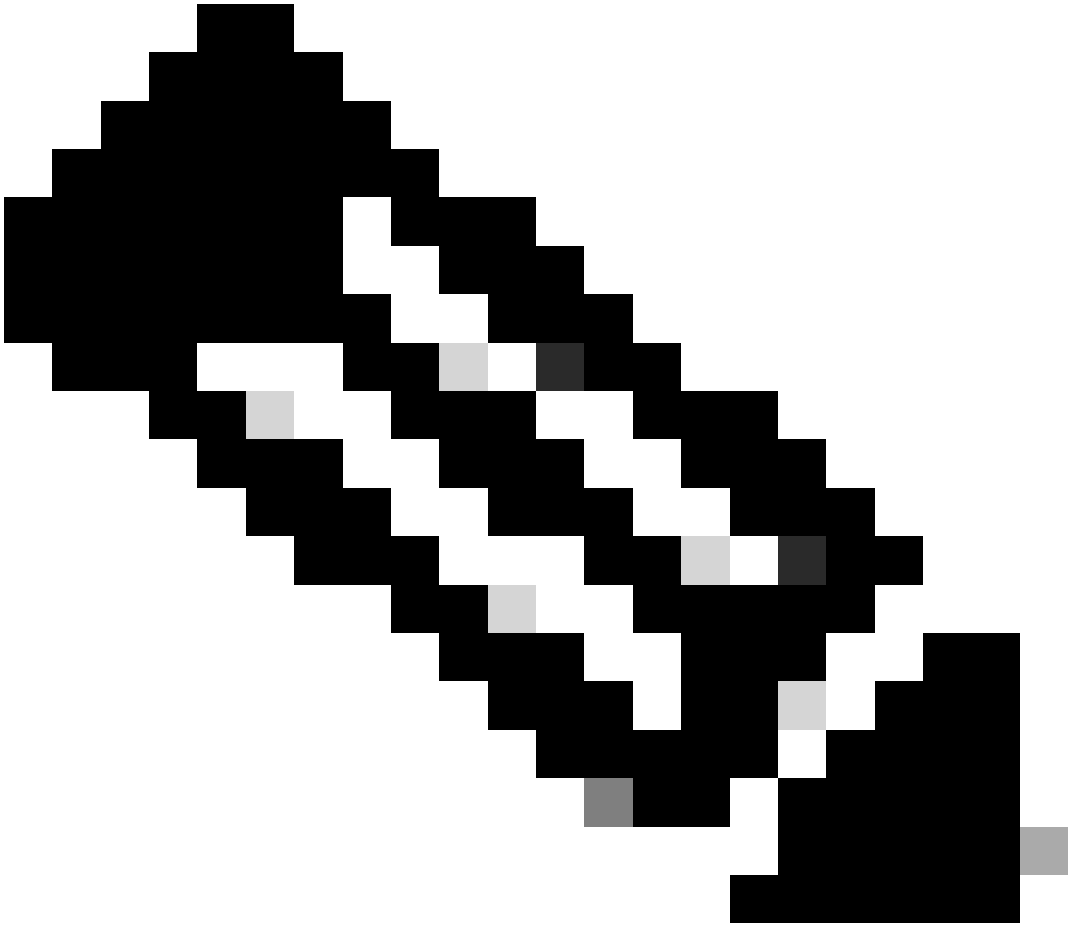
Para confirmar si SNA Flow Collector recibe e inserta telemetría de NetFlow/IPFIX de los exportadores:

1. Inicie sesión en la interfaz de usuario de administración de Flow Collector de SNA con credenciales de administrador: https://<Dirección IP de Flow Collector>/swa/login.html
2. En el panel izquierdo, navegue hasta Soporte > Examinar archivos
3. Vaya a la siguiente carpeta: sw > today > logs
4. Haga clic en el archivo sw.log para descargarlo en su equipo local y abrirlo en un editor de

texto.

5. Busque estas líneas en la parte inferior del registro; este resumen se crea cada cinco minutos:

```
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
```



Nota: La línea 8 indica que hay flujos descartados debido a que los datos de plantilla del último período son insuficientes.

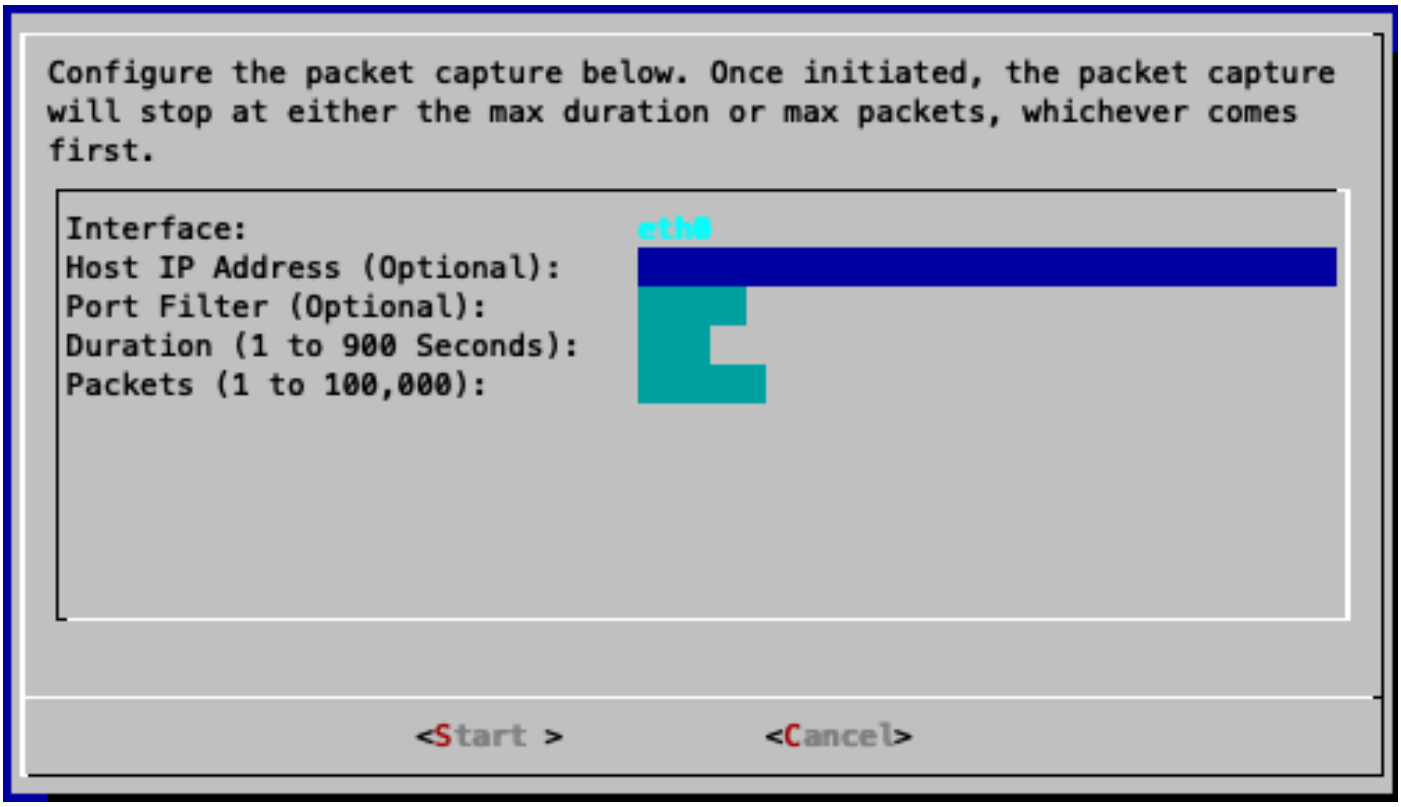
Verificar plantilla NetFlow/IPFIX

Para confirmar los campos incluidos en la plantilla NetFlow/IPFIX:

1. Inicie sesión en la CLI del colector de flujo SNA con credenciales de sysadmin.

2. En el menú SystemConfig, vaya a: Avanzado **>** Captura de paquetes

3. Introduzca la información del exportador que no muestra flujos en SNA:



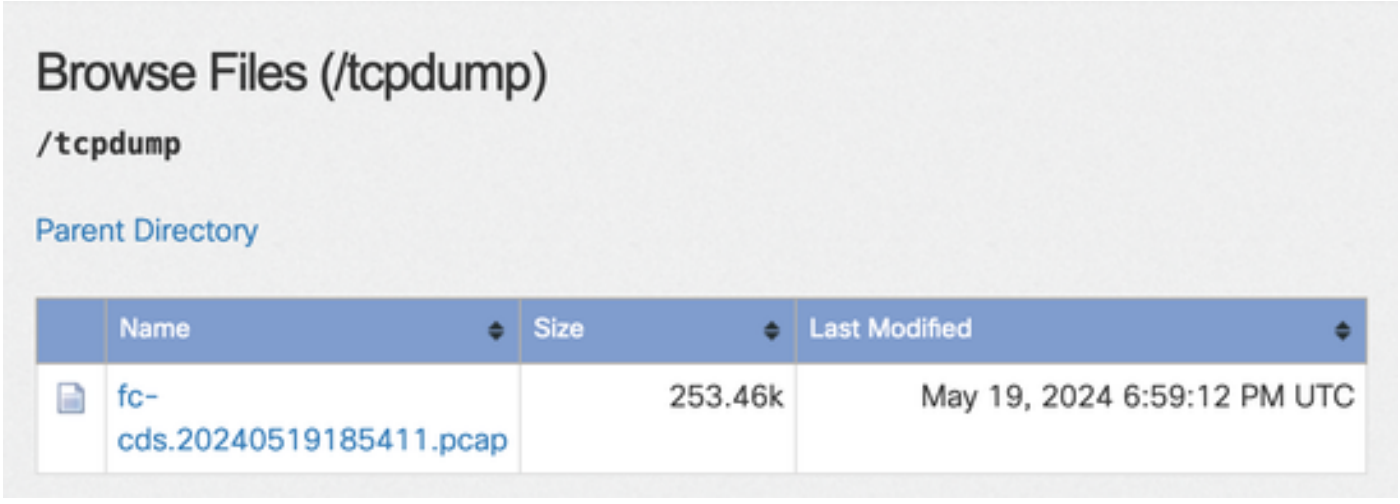
4. Espere hasta que se complete el proceso.

5. Para descargar el archivo, inicie sesión en la interfaz de usuario de administración de Flow Collector de SNA con credenciales de administrador: https://<Dirección IP de Flow Collector>/swa/login.html

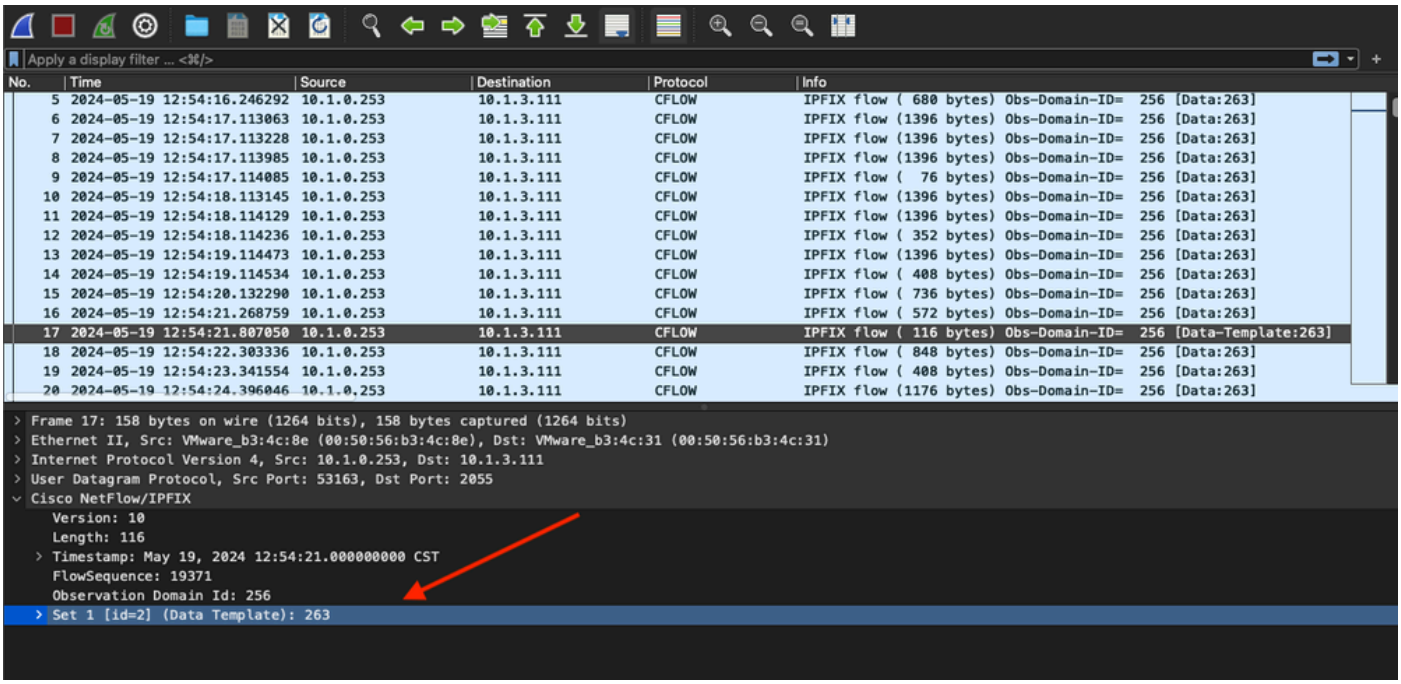
6.En el panel izquierdo, navegue hasta Soporte > Examinar archivos

7. Acceda a la siguiente carpeta: tcpdump

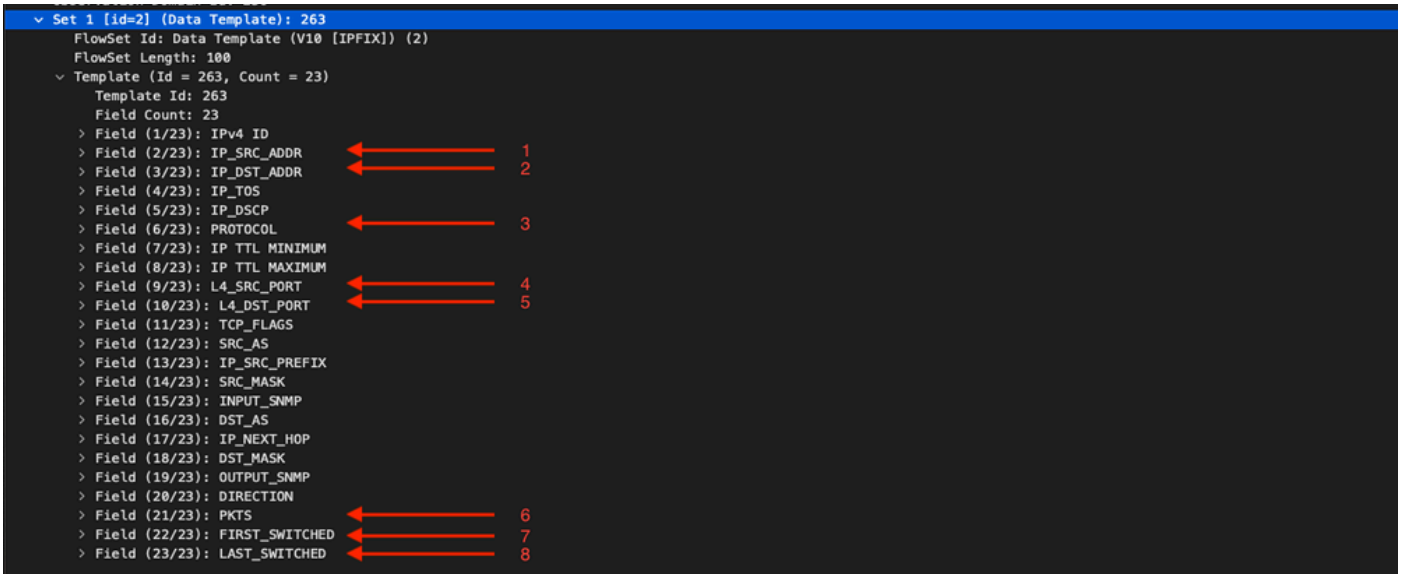
8. Haga clic en el archivo de captura de paquetes para descargarlo en su máquina local y abrirlo en Wireshark:

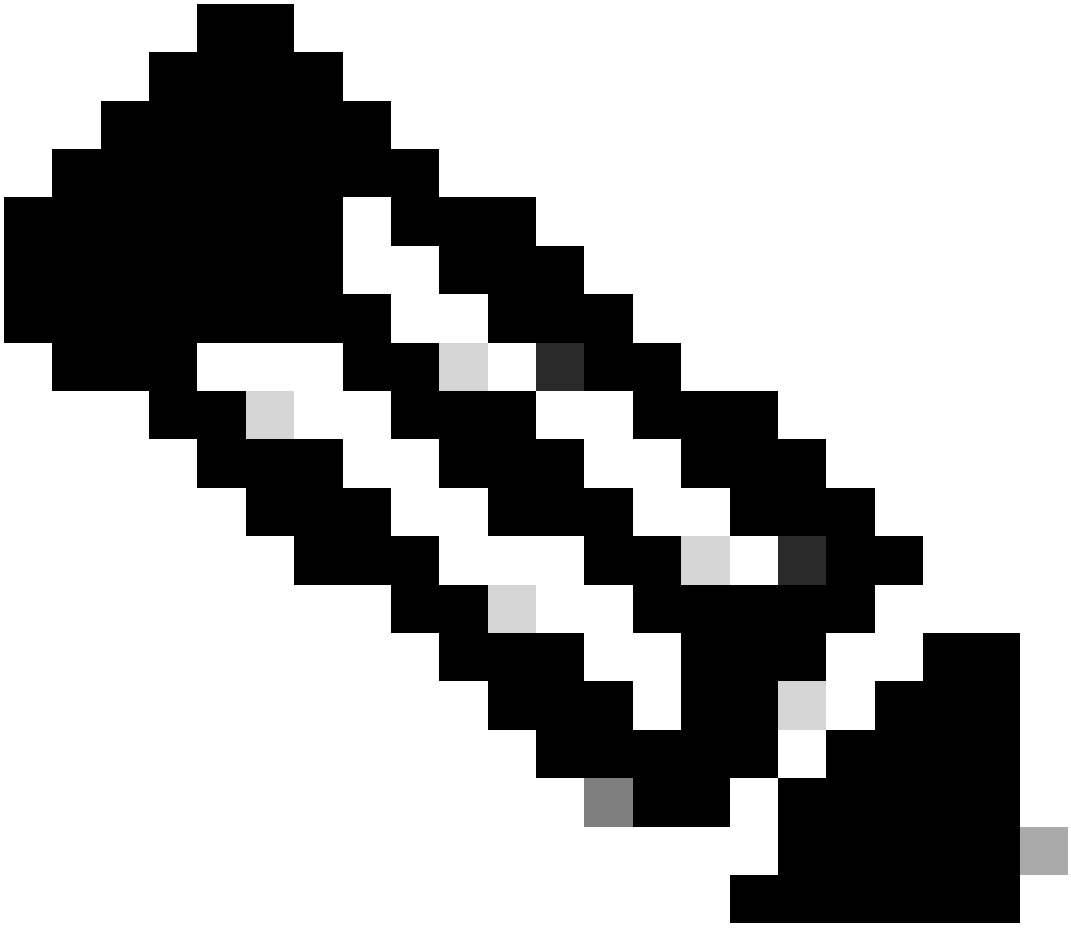


9. Identifique la trama en la que se recibió la plantilla NetFlow/IPFIX.



10. Compruebe que los 9 campos obligatorios aparecen en la plantilla





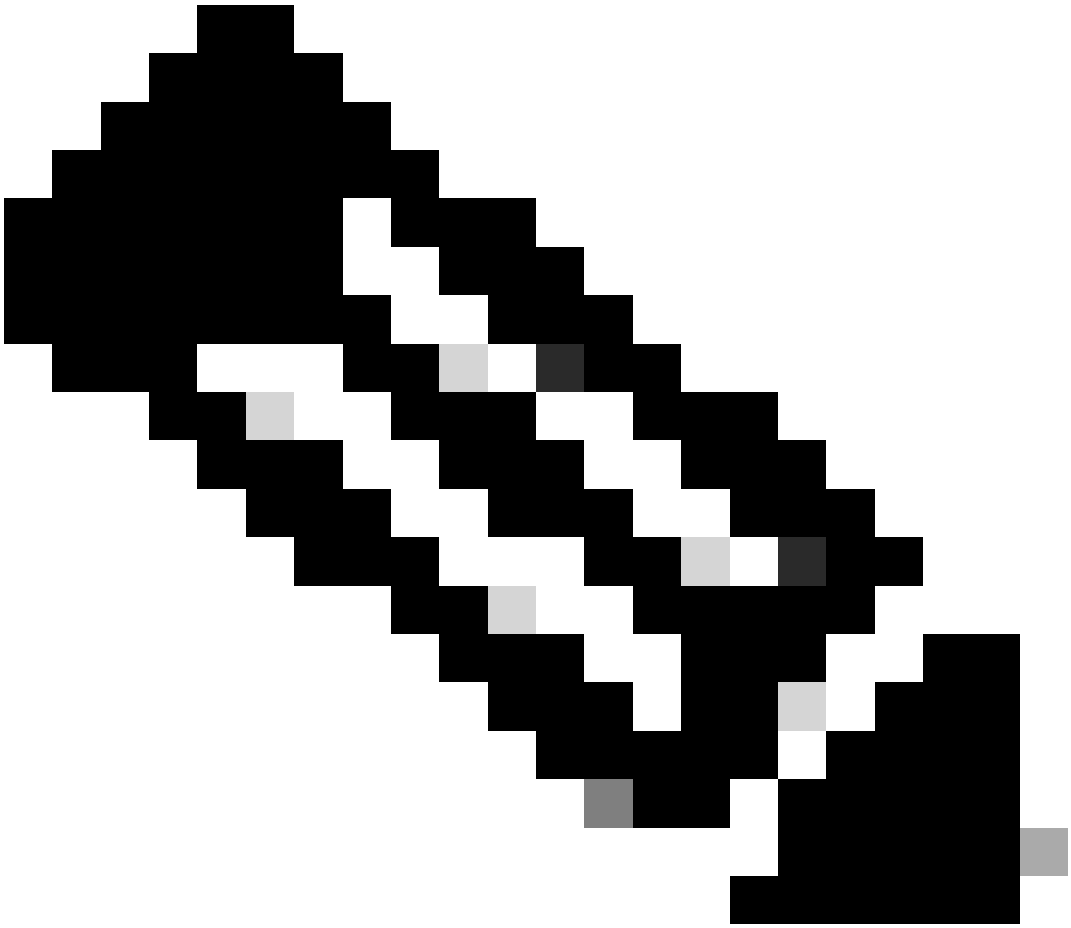
> Nota: Observe que en la plantilla solo hay 8 de los 9 campos obligatorios que SNA requiere para la ingesta de telemetría; para este escenario, falta el campo BYTES.

Verifique NetFlow/IPFIX Telemetry Ingest después de agregar los campos que faltan

Para confirmar si SNA Flow Collector recibe e inserta telemetría de NetFlow/IPFIX del exportador después del cambio:

1. Inicie sesión en la interfaz de usuario de administración de Flow Collector de SNA con credenciales de administrador: https://<Dirección IP de Flow Collector>/swa/login.html
2. En el panel izquierdo, navegue hasta Soporte > Examinar archivos
3. Vaya a la siguiente carpeta: sw > today > logs
4. Haga clic en el archivo sw.log para descargarlo en su equipo local y abrirlo en un editor de texto.
5. Busque estas líneas al final del registro

```
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
```



Nota: La línea 8 indica que no hay flujos descartados en el último período.

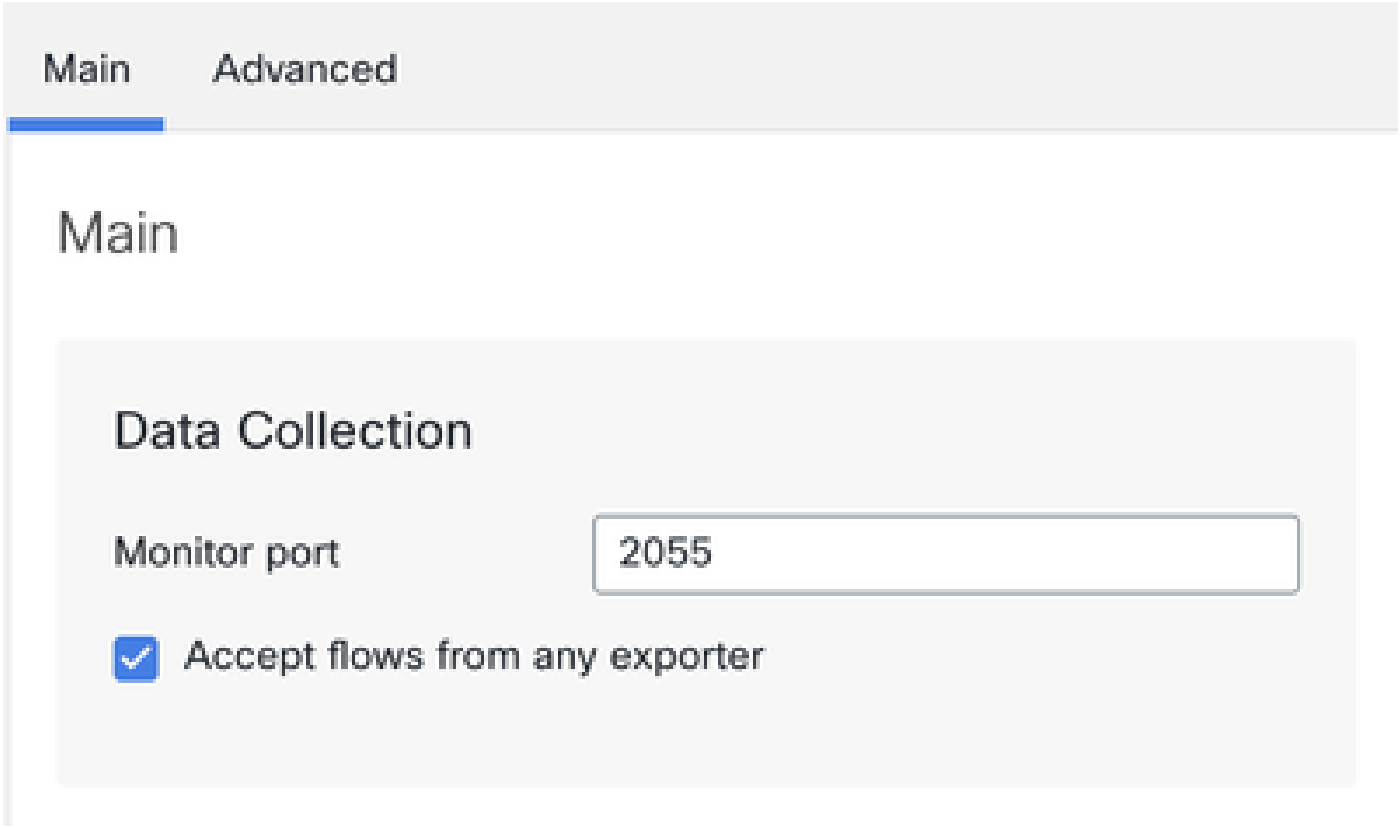
Verificar puerto de ingesta de telemetría de NetFlow/IPFIX

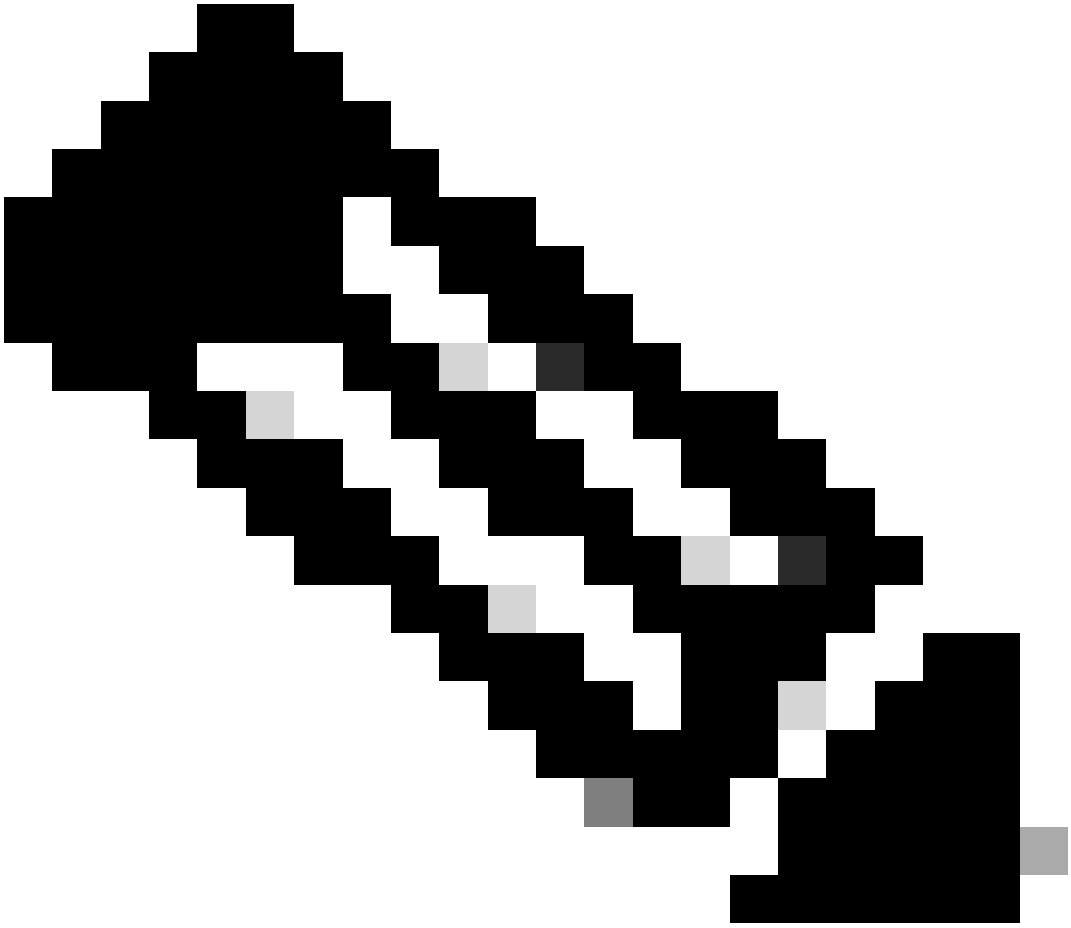
Para confirmar si el colector de flujo SNA recibe telemetría de NetFlow/IPFIX de los exportadores en el puerto correcto:

1. Inicie sesión en la interfaz de usuario web de SNA con un usuario con permisos de administrador.

2. En el menú superior, acceda a Configurar y seleccione Flow Collector (Recopiladores de flujos)

3. Confirme que SNA Flow Collector utilice el mismo puerto que los exportadores han configurado para enviar NetFlow/IPFIX





> Nota: El puerto predeterminado para NetFlow es 2055; sin embargo, puede seleccionar otro puerto; asegúrese de utilizar el mismo puerto durante el proceso de configuración inicial en los Flow Collector(s).

Verifique que la opción NetFlow/IPFIX Telemetry Ingest NetFlow esté habilitada

Para confirmar si la opción SNA Flow Collector para la ingesta de telemetría de NetFlow/IPFIX está habilitada:

1. Inicie sesión en la interfaz de usuario de administración de Flow Collector de SNA con credenciales de administrador: https://<Dirección IP de Flow Collector>/swa/login.html
2. En el panel izquierdo, navegue hasta Soporte > Configuración avanzada
3. Confirme que la opción enable_netflow se establezca en 1:

Información Relacionada

- Para obtener asistencia adicional, póngase en contacto con el Technical Assistance Center (TAC). Se necesita un contrato de asistencia válido: Contactos de asistencia globales de Cisco.
- También puede visitar la Comunidad de análisis de seguridad de Cisco aquí.
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).