Identificar e solucionar problemas de inclusão de telemetria NetFlow/IPFIX na análise de rede segura

Contents

Introdução

Este documento descreve como solucionar problemas de Ingestão de Telemetria de Netflow na Análise de Rede Segura (SNA).

Pré-requisitos

- Conhecimento de SNA da Cisco
- Conhecimento de NetFlow/IPFIX

Requisitos

- Análise de rede segura na versão 7.5.0 ou mais recente
- Flow Collector na versão 7.5.0 ou mais recente
- Acesso CLI como sysadmin para o Flow Collector
- Acesso de IU de administração como administrador para o coletor de fluxo

Guias de configuração

- Configurar o NetFlow/IPFIX para a inclusão de telemetria na análise de rede segura

Componentes Utilizados

- SNA Manager e Flow Collector no 7.5.0
- Software Wireshark

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

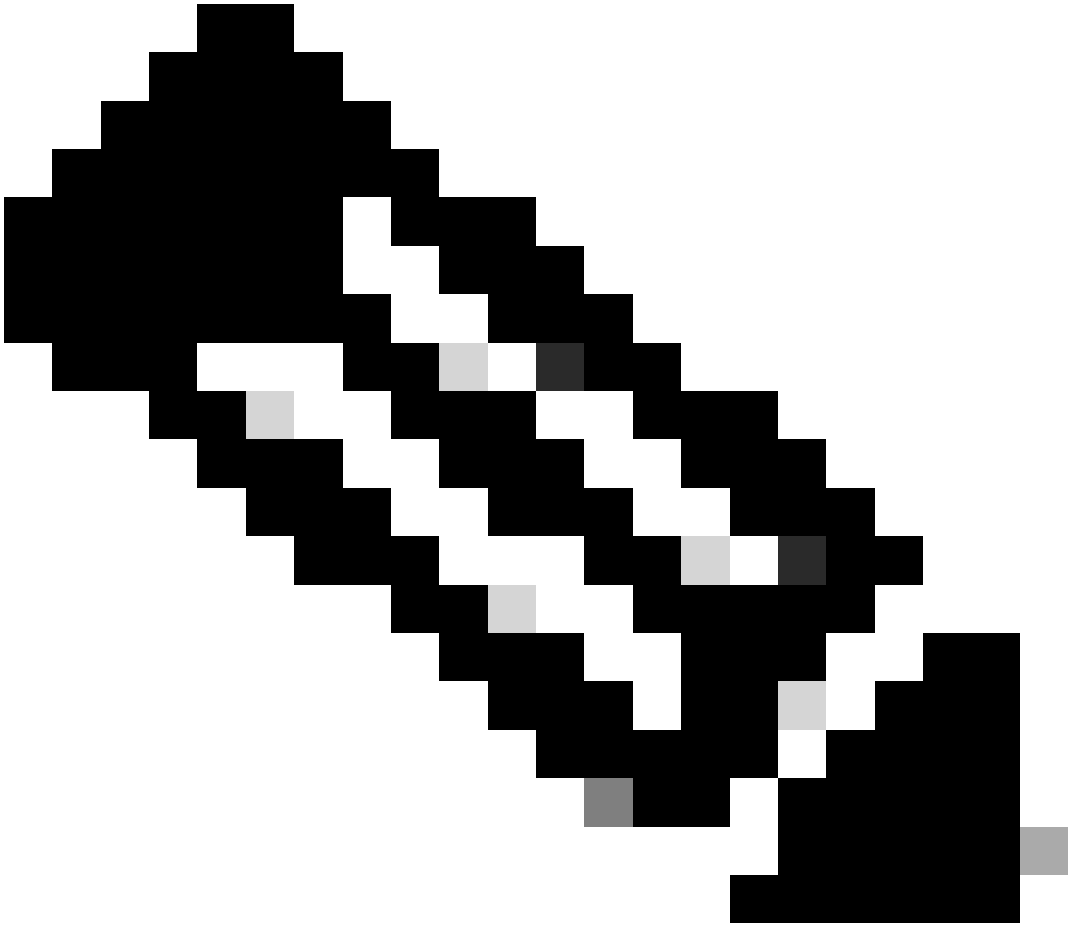
Informações de Apoio

O Flow Collector é um dispositivo SNA encarregado de coletar, processar e armazenar fluxos que são enviados para o Secure Network Analytics. Para o NetFlow versão 9 ou IPFIX, vários campos podem ser incluídos no modelo NetFlow/IPFIX para adicionar mais informações relacionadas ao tráfego de rede. No entanto, há 9 campos específicos que devem ser incluídos no modelo NetFlow/IPFIX para que o Flow Collector processe esses fluxos. O Flow Collector não processa fluxos de entrada que incluam um modelo não válido, portanto, o SNA não exibe informações de fluxo desses exportadores na IU da Web ou no Desktop Client.

Campos Obrigatórios

Os próximos campos devem ser incluídos no modelo NetFlow/IPFIX para inclusão de telemetria. Certifique-se de que esses 9 campos estejam incluídos no modelo NetFlow/IPFIX, para que o Secure Network Analytics processe os fluxos de entrada.

- Endereço IP origem
- Endereço IP de destino
- Porta de origem
- Porta de Destino
- Protocolo de Camada 3
- Contagem de Bytes
- Contagem de pacotes
- Hora de início do fluxo
- Hora de término do fluxo



Note: Mais campos podem ser incluídos na configuração NetFlow/IPFIX, no entanto, os campos anteriores são os requisitos mínimos do Secure Network Analytics para Ingestão de Telemetria.

Processo de solução de problemas

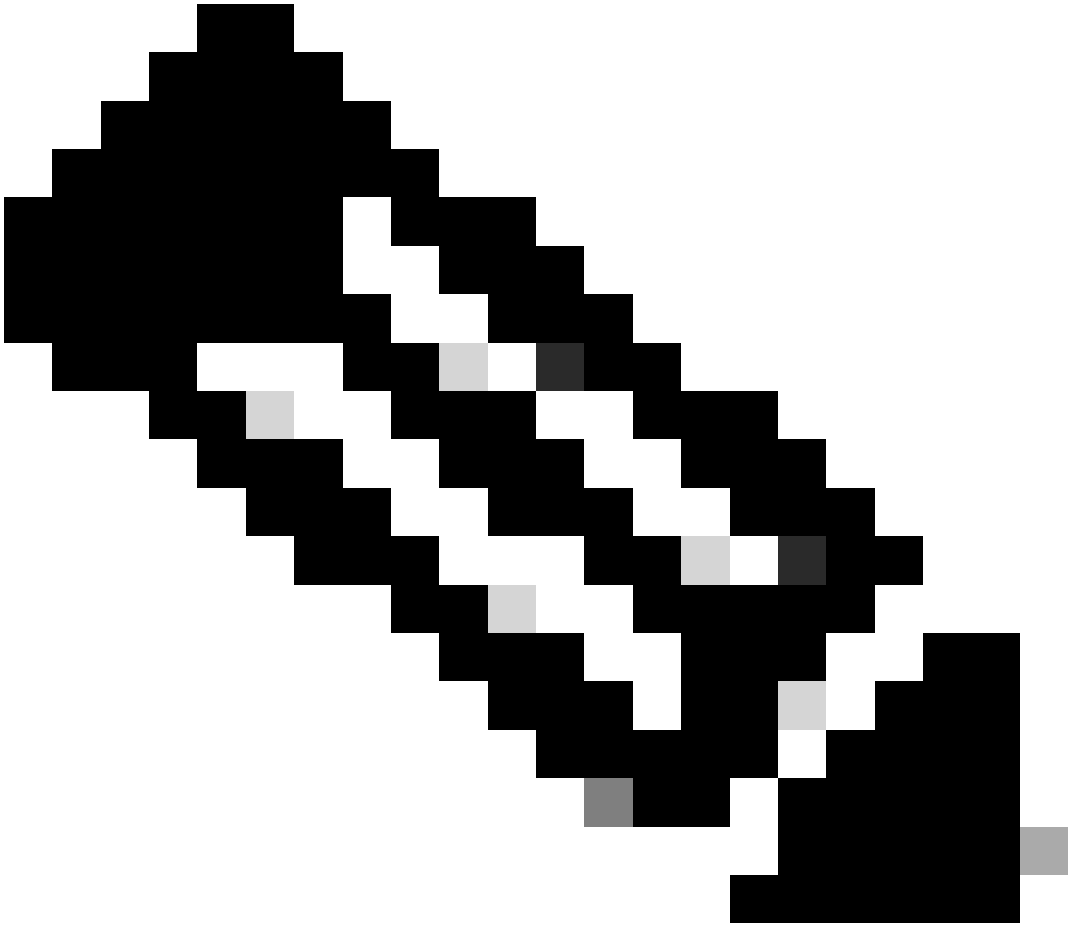
Verificar a inclusão da telemetria NetFlow/IPFIX

Para confirmar se o SNA Flow Collector recebe e insere telemetria NetFlow/IPFIX dos exportadores:

1. Faça login na interface de usuário do SNA Flow Collector Admin com credenciais de administrador: https://<Endereço IP do Flow Collector>/swa/login.html
2. No painel esquerdo, navegue até Suporte > Procurar arquivos
3. Navegue até a próxima pasta: sw > hoje > logs
4. Clique no arquivo sw.log para baixá-lo na máquina local e abri-lo em um editor de texto.

5. Procure essas linhas na parte inferior do registro. Esse resumo é criado a 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
```



Note: A linha 8 indica que há fluxos descartados devido a dados de modelo insuficientes no último período.

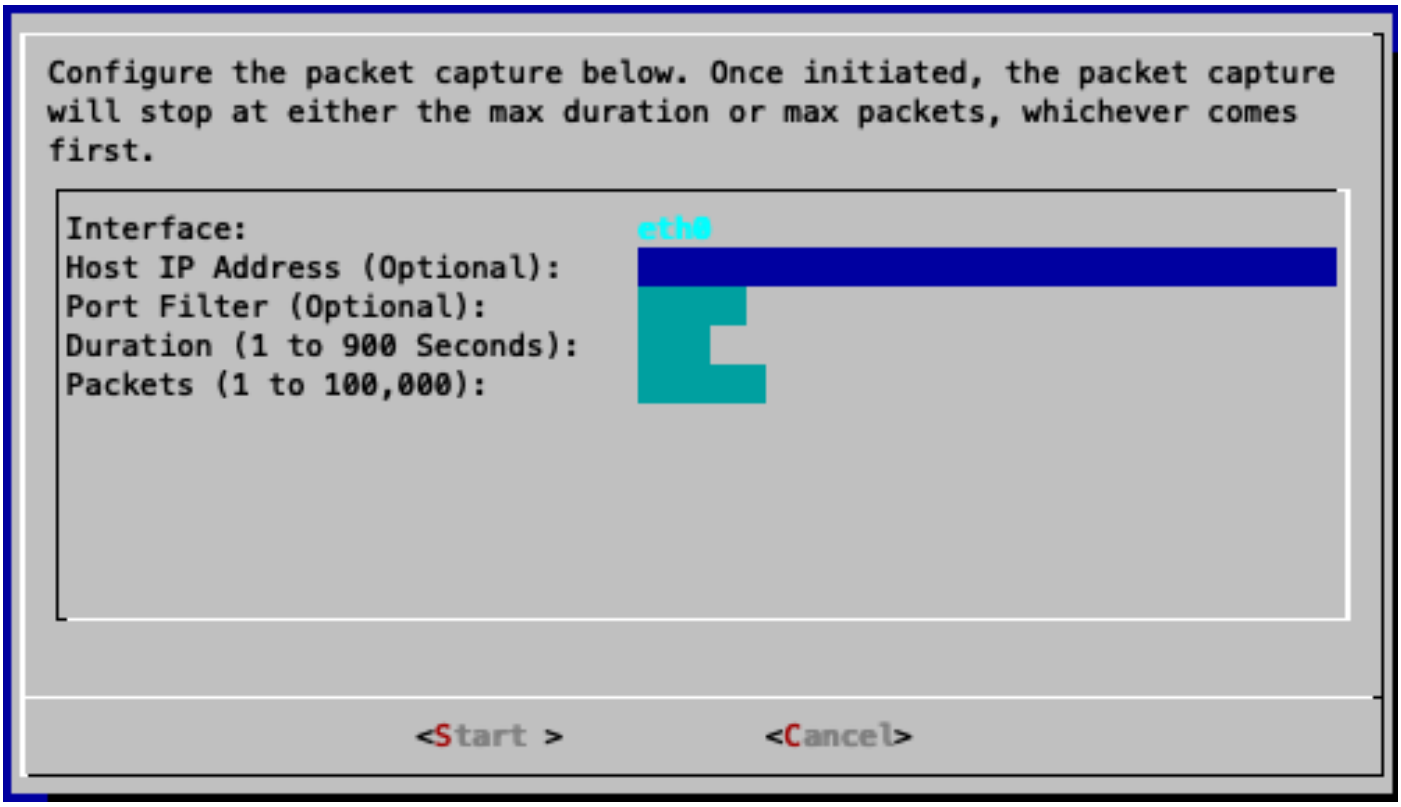
Verificar modelo do NetFlow/IPFIX

Para confirmar os campos incluídos no modelo NetfFlow/IPFIX:

1. Faça login no SNA Flow Collector CLI com as credenciais do sysadmin.

2. No menu SystemConfig, navegue para: Avançado > Captura de pacotes

3. Especifique as informações do exportador que não estão mostrando fluxos no SNA:



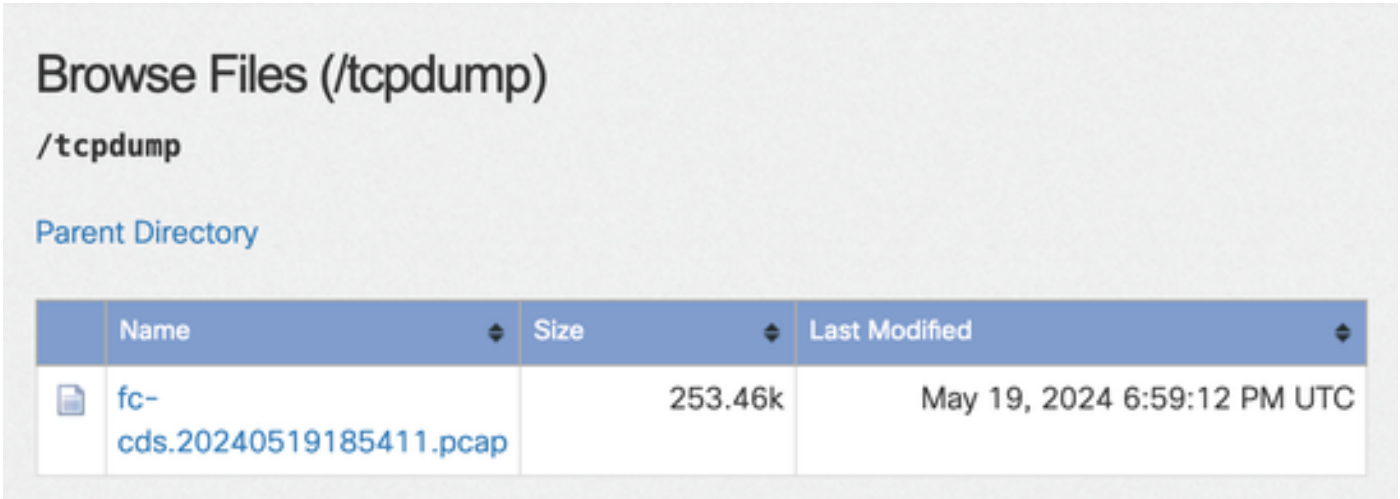
4. Aguarde até que o processo seja concluído.

5. Para baixar o arquivo, faça login na interface do usuário do SNA Flow Collector Admin com as credenciais de admin: https://<Endereço IP do Flow Collector>/swa/login.html

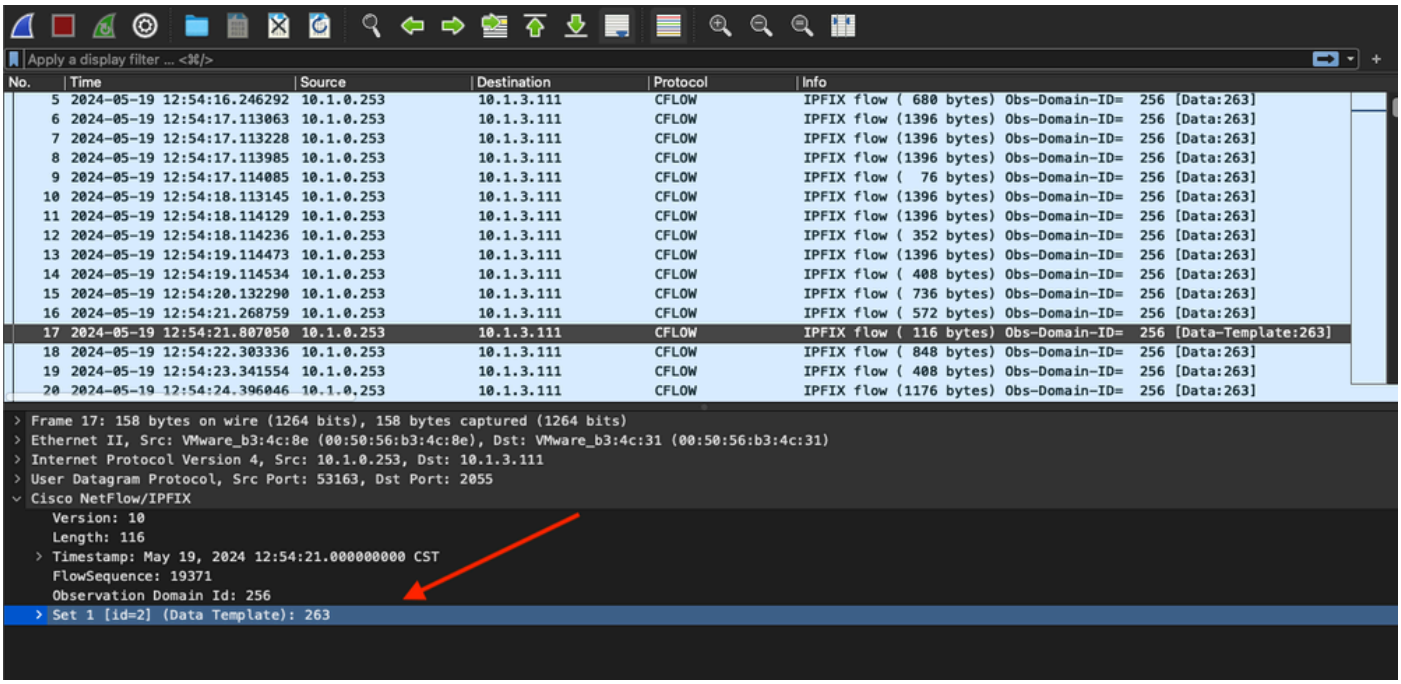
6.No painel esquerdo, navegue até Suporte > Procurar arquivos

7. Navegue até a próxima pasta: tcpdump

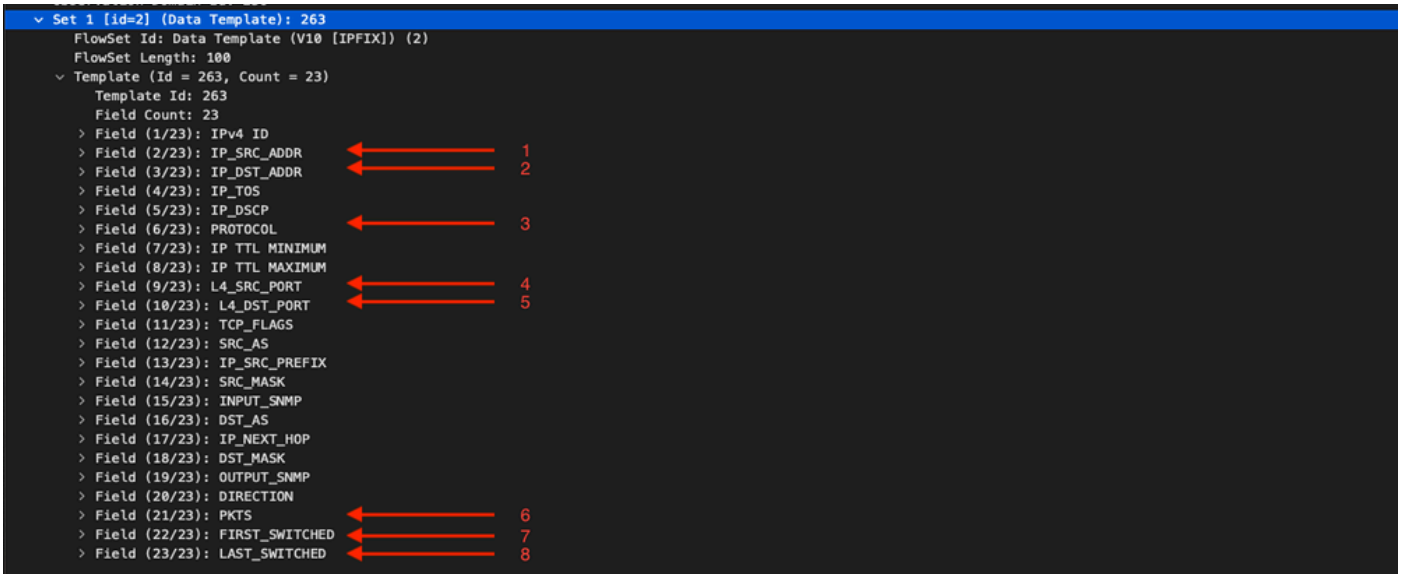
8. Clique no arquivo de captura de pacote para baixá-lo em sua máquina local e abri-lo no Wireshark:

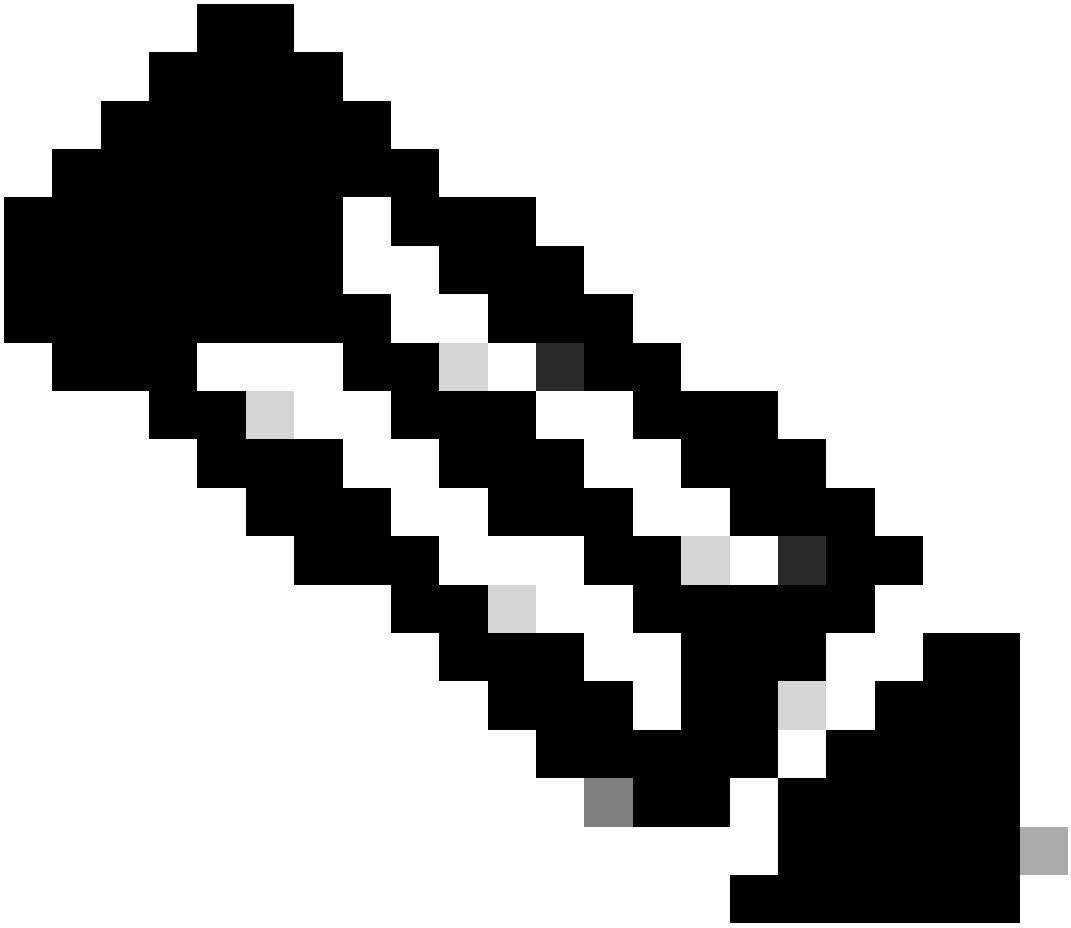


9. Identifique o quadro no qual o modelo NetFlow/IPFIX foi recebido.



10. Valide se os 9 campos obrigatórios aparecem no modelo





> Note: Observe que no modelo há apenas 8 dos 9 campos obrigatórios que o SNA exige para a inclusão de telemetria, para esse cenário, o campo BYTES está faltando.

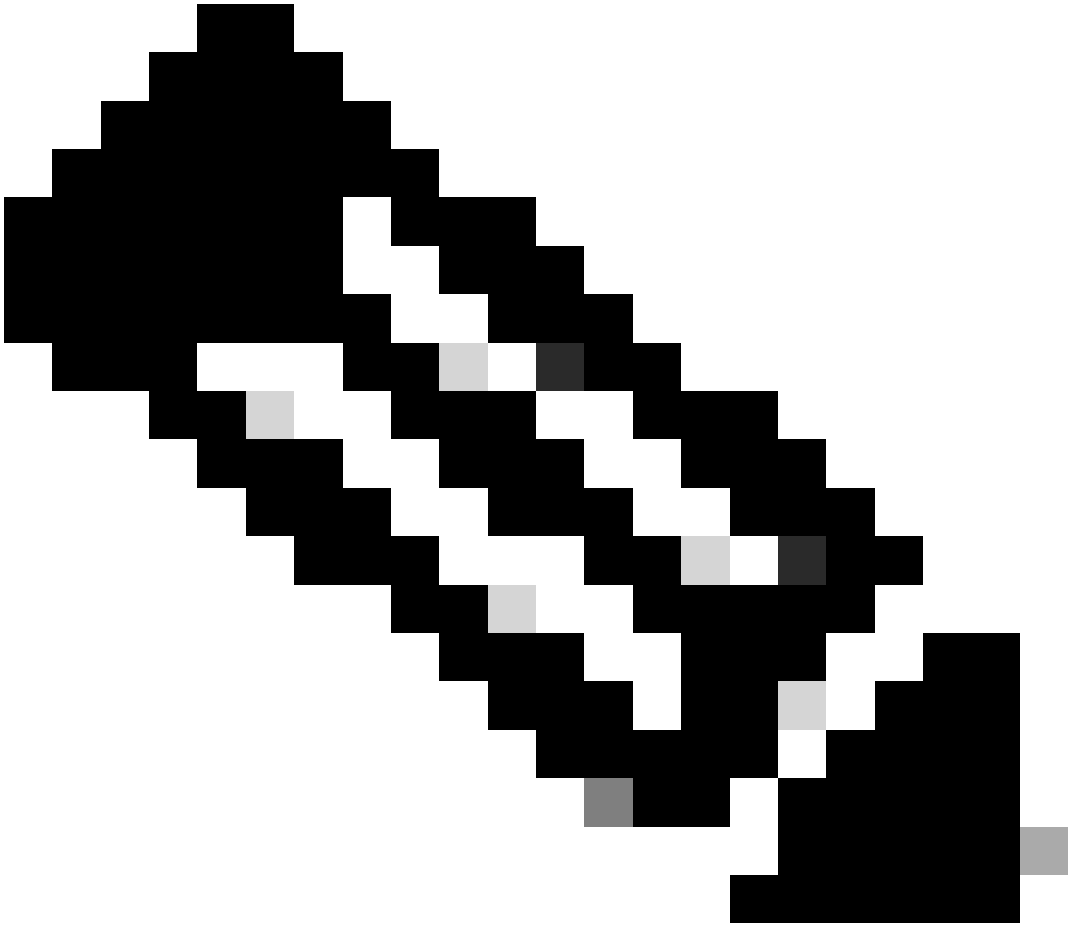
Verificar a inclusão da telemetria NetFlow/IPFIX depois de adicionar o(s) campo(s) ausente(s)

Para confirmar se o SNA Flow Collector recebe e insere a telemetria NetFlow/IPFIX do exportador após a alteração:

1. Faça login na interface de usuário do SNA Flow Collector Admin com as credenciais de admin: https://<Endereço IP do Flow Collector>/swa/login.html
2. No painel esquerdo, navegue até Suporte > Procurar arquivos
3. Navegue até a próxima pasta: sw > hoje > logs
4. Clique no arquivo sw.log para baixá-lo na máquina local e abri-lo em um editor de texto.
5. Procurar estas linhas na parte inferior do 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
```



Note: A linha 8 indica que não há fluxos descartados no último período.

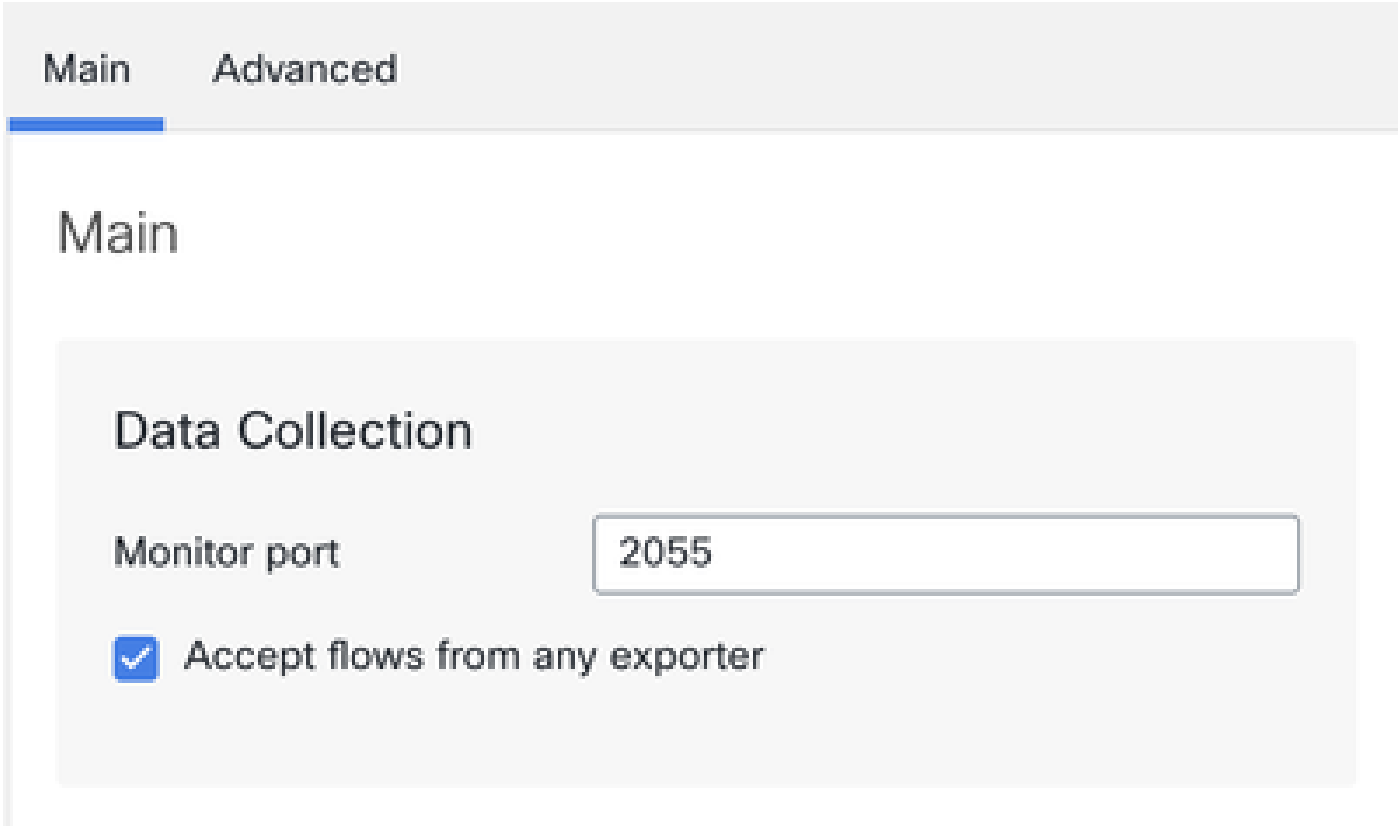
Verificar a porta de entrada da telemetria NetFlow/IPFIX

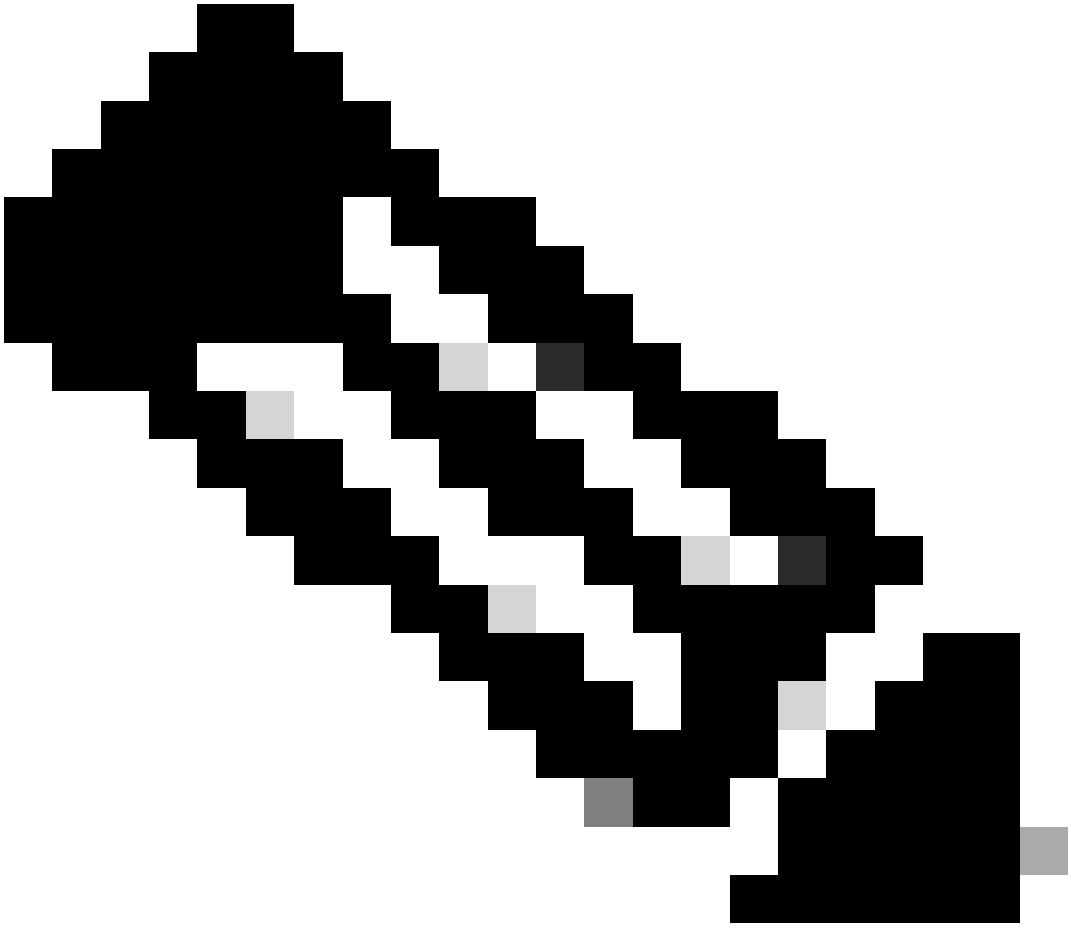
Para confirmar se o SNA Flow Collector recebe telemetria NetFlow/IPFIX dos exportadores na porta correta:

1. Faça login na interface do usuário do SNA Web com um usuário com permissões de administrador.

2. No menu superior, navegue até Configurar e escolha Flow Collectors

3. Confirme se o SNA Flow Collector usa a mesma porta que os exportadores configuraram para enviar NetFlow/IPFIX





Note: A porta padrão para o NetFlow é 2055. No entanto, você pode selecionar outra porta. Certifique-se de usar a mesma porta durante o processo de instalação de primeira vez em coletores de fluxo.

Verificar se a opção NetFlow/IPFIX Telemetry Ingest NetFlow está habilitada

Para confirmar se a opção SNA Flow Collector para inclusão de telemetria do NetFlow/IPFIX está habilitada:

1. Faça login na interface de usuário administrativa do coletor de fluxo SNA com credenciais de administrador: https://<Endereço IP do Flow Collector>/swa/login.html
2. No painel esquerdo, navegue até Suporte > Configurações avançadas
3. Confirme se a opção enable_netflow está definida como 1:

Informações Relacionadas

- Para obter assistência adicional, entre em contato com o Technical Assistance Center (TAC). É necessário um contrato de suporte válido: Cisco Worldwide Support Contacts.
- Você também pode visitar a comunidade de análise de segurança da Cisco aqui.
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.