Problemen met NetFlow/IPFIX-telemetrie oplossen Investeren in Secure Network Analytics

Inhoud

Inleiding

In dit document wordt beschreven hoe u problemen met Netflow Telemetry Investing in Secure Network Analytics (SNA) kunt oplossen.

Voorwaarden

- Cisco SNA-kennis
- Kennis van NetFlow/IPFIX

Vereisten

- Secure Network Analytics in 7.5.0 of nieuwer
- Stroomcollector in 7.5.0 of nieuwer
- CLI-toegang als sysadmin naar de Flow Collector
- Admin UI-toegang als beheerder van de Flow Collector

Configuratiehandleidingen

- Configureer NetFlow/IPFIX voor Telemetry Ingest op Secure Network Analytics

Gebruikte componenten

- SNA Manager en Flow Collector op 7.5.0
- Wireshark-software

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

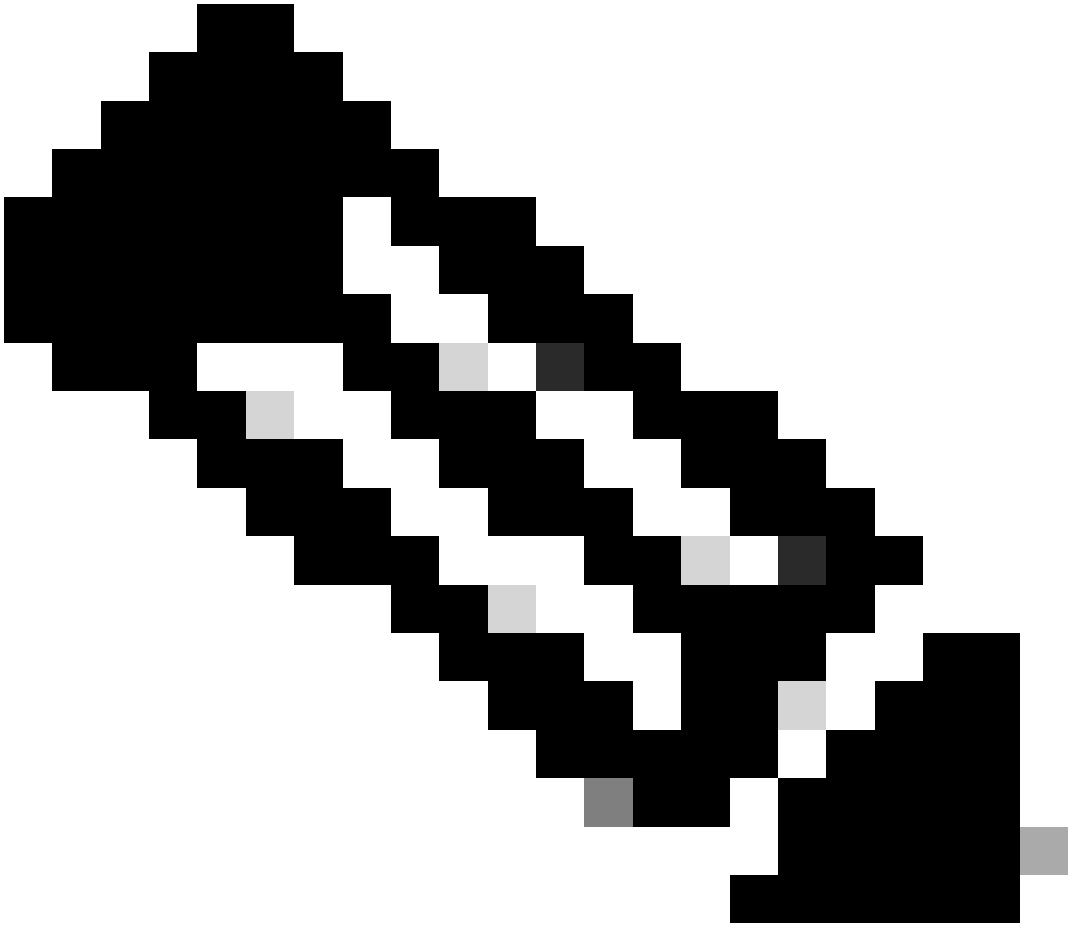
Achtergrondinformatie

De Flow Collector is een SNA-apparaat dat verantwoordelijk is voor het verzamelen, verwerken en opslaan van stromen die naar Secure Network Analytics worden verzonden. Voor NetFlow versie 9 of IPFIX kunnen verschillende velden worden opgenomen in de NetFlow/IPFIX-sjabloon om meer informatie toe te voegen met betrekking tot netwerkverkeer, maar er zijn 9 specifieke velden die moeten worden opgenomen in de NetFlow/IPFIX-sjabloon voor de Flow Collector om die stromen te verwerken. Flow Collector verwerkt geen inkomende stromen die een ongeldige sjabloon bevatten, daarom geeft SNA geen stroominformatie van die exporteurs weer onder Web UI of Desktop Client.

Verplichte velden

Volgende velden moeten worden opgenomen in de NetFlow/IPFIX-sjabloon voor Telemetrie-inname. Zorg ervoor dat deze 9 velden zijn opgenomen in de NetFlow / IPFIX-sjabloon, zodat Secure Network Analytics inkomende stromen kan verwerken.

- bron-IP-adres
- IP-adres van bestemming
- Bronpoort
- bestemmingshaven
- Layer 3-protocol
- aantal bytes
- Pakkettelling
- Begintijd stroom
- eindtijd van de stroom



Opmerking: Meer velden kunnen worden opgenomen in de NetFlow / IPFIX-configuratie, maar de vorige velden zijn de minimale vereisten van Secure Network Analytics voor Telemetry Ingest.

Problemen oplossen

Controleer NetFlow/IPFIX Telemetry Ingest

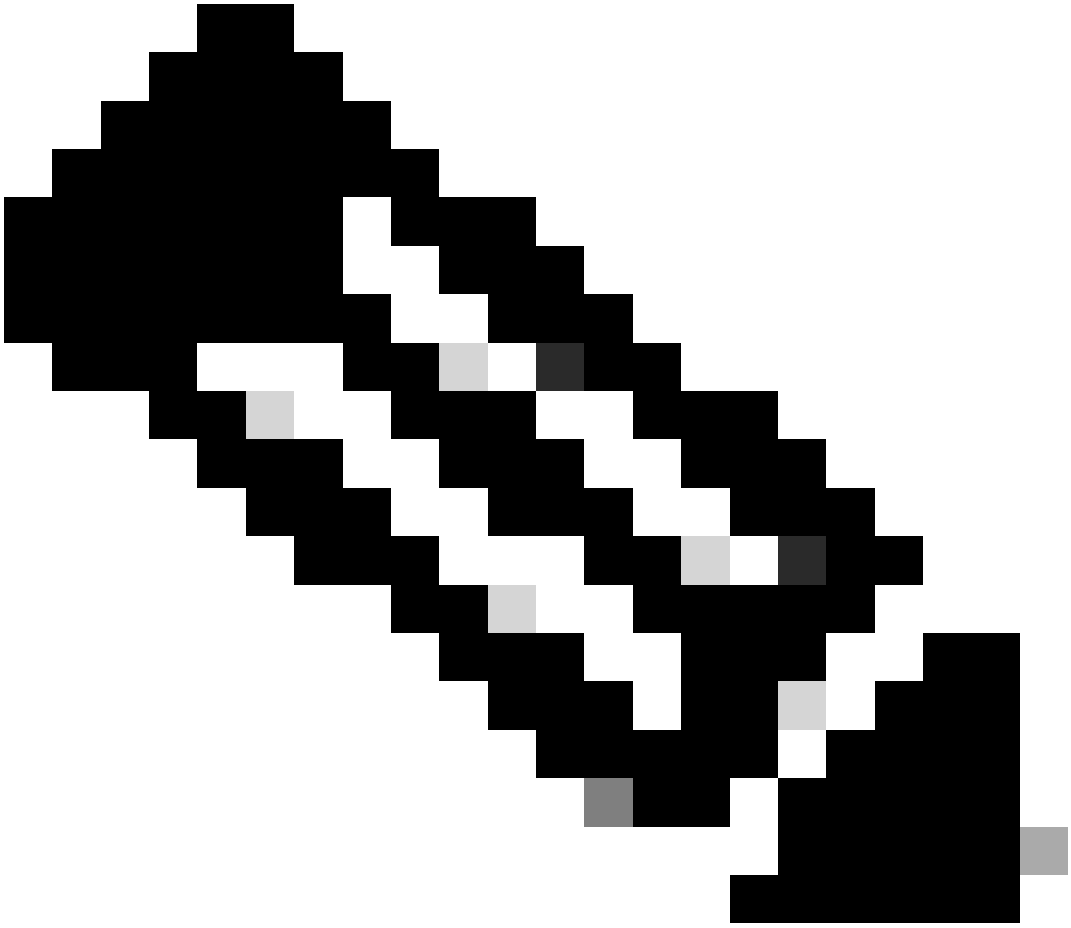
Om te bevestigen of de SNA Flow Collector NetFlow/IPFIX-telemetrie van de exporteurs ontvangt en invoegt:

1. Meld u aan bij de SNA Flow Collector Admin UI met beheerdersreferenties: https://<Flow Collector IP Address>/swa/login.html
2. Navigeer in het linkerdeelvenster naar Ondersteuning > Bestanden bladeren
3. Navigeer naar de volgende map: sw > vandaag > logs
4. Klik op het sw.log bestand om het te downloaden naar uw lokale machine en open het op

een teksteditor.

5. Zoek naar deze regels onderaan het logboek, dit overzicht wordt elke vijf minuten gemaakt:

```
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
```



Toelichting: Lijn 8 geeft aan dat er stromen zijn weggegooid vanwege onvoldoende sjabloongegevens over de laatste periode.

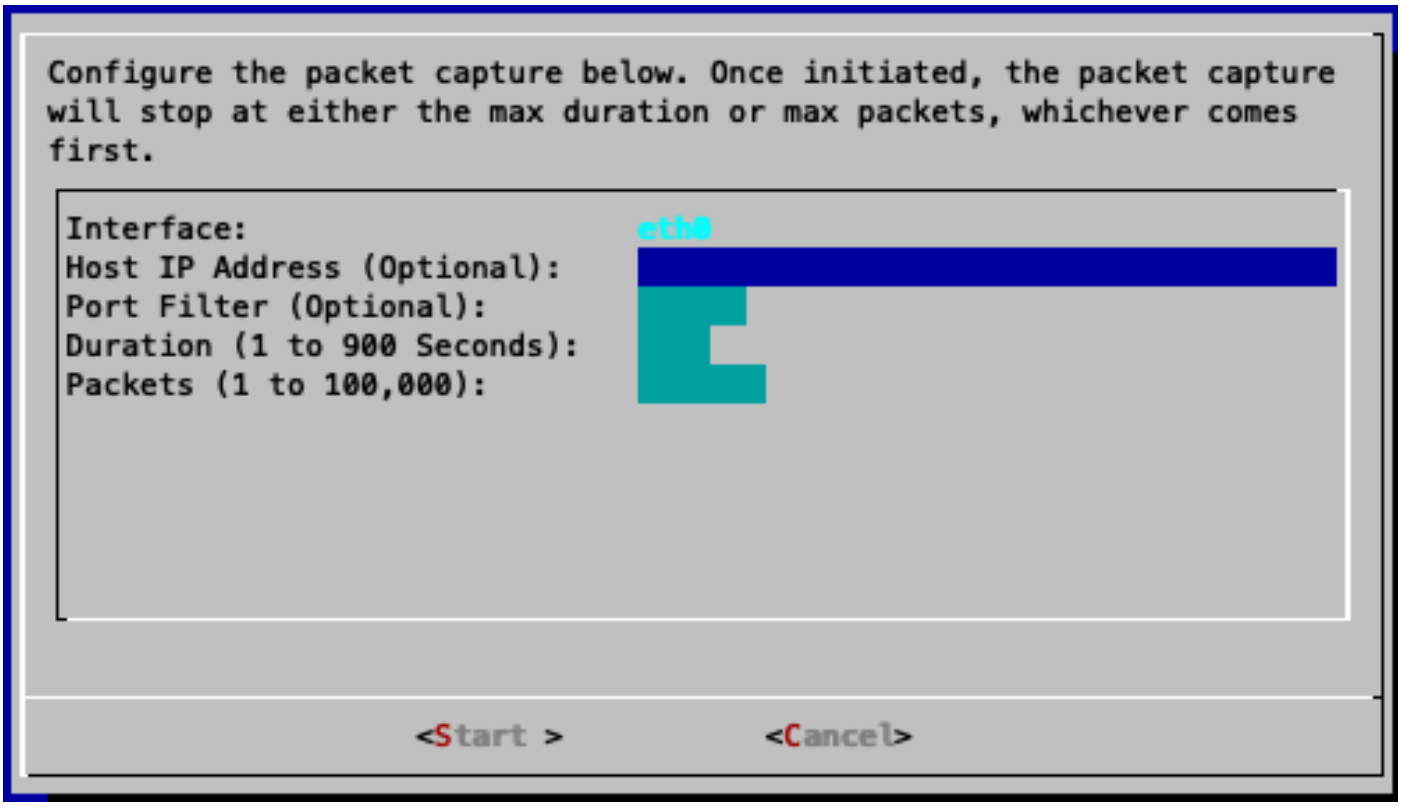
Netflow-/IPFIX-sjabloon verifiëren

Bevestig de velden in de NetFlow/IPFIX-sjabloon:

1. Meld u aan bij de SNA Flow Collector CLI met sysadmin-referenties.

2. Navigeer in het menu SystemConfig naar: Geavanceerd > Pakketvastlegging

3. Vermeld de informatie van de exporteur die geen stromen op het SNA aangeeft:



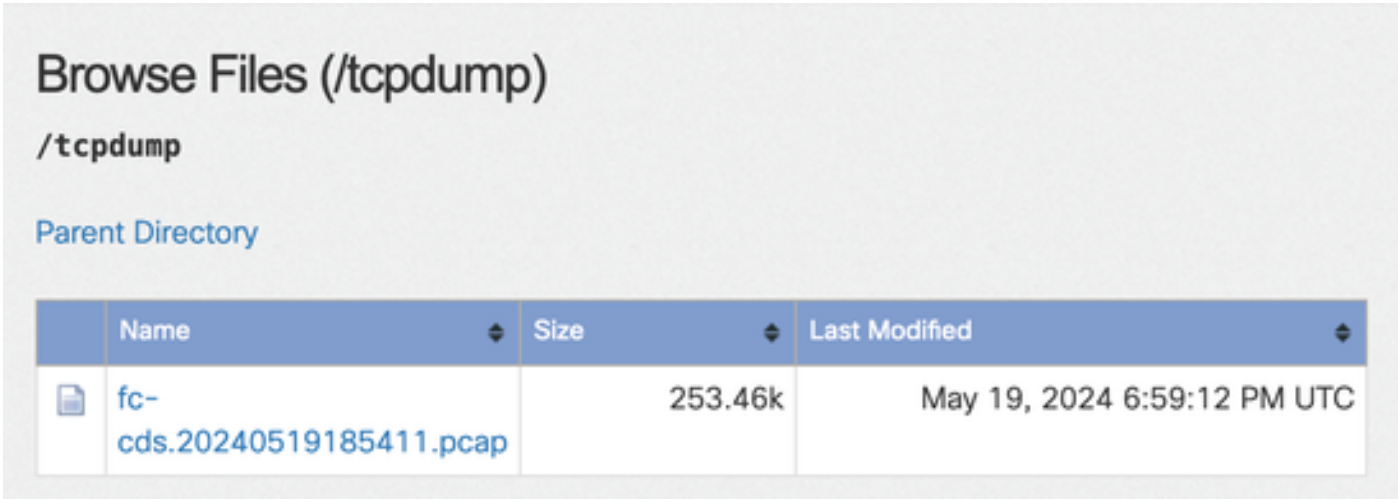
4. Wacht tot het proces is voltooid.

5. Meld u aan bij de gebruikersinterface van SNA Flow Collector Admin met de referenties van de beheerder om het bestand te downloaden: https://<Flow Collector IP Address>/swa/login.html

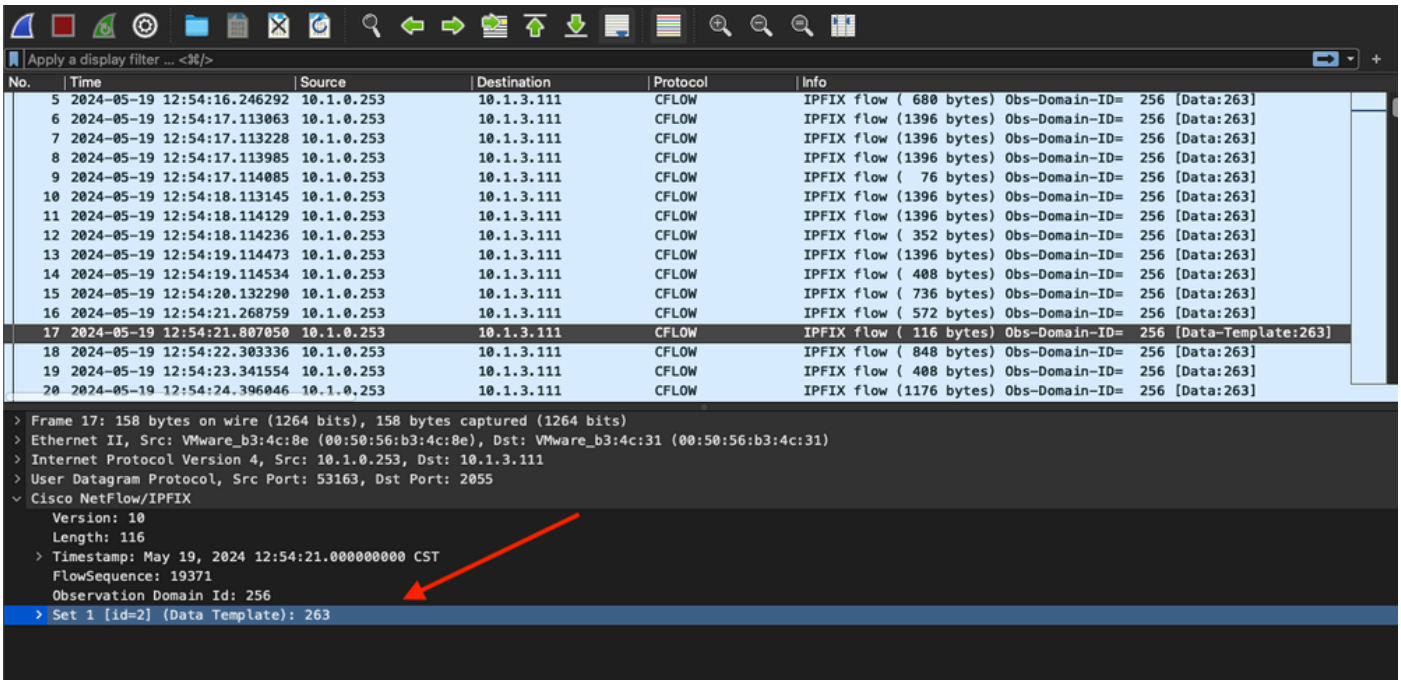
6.Navigeer in het linkerdeelvenster naar Ondersteuning > Bestanden bladeren

7. Navigeer naar de volgende map: tcpdump

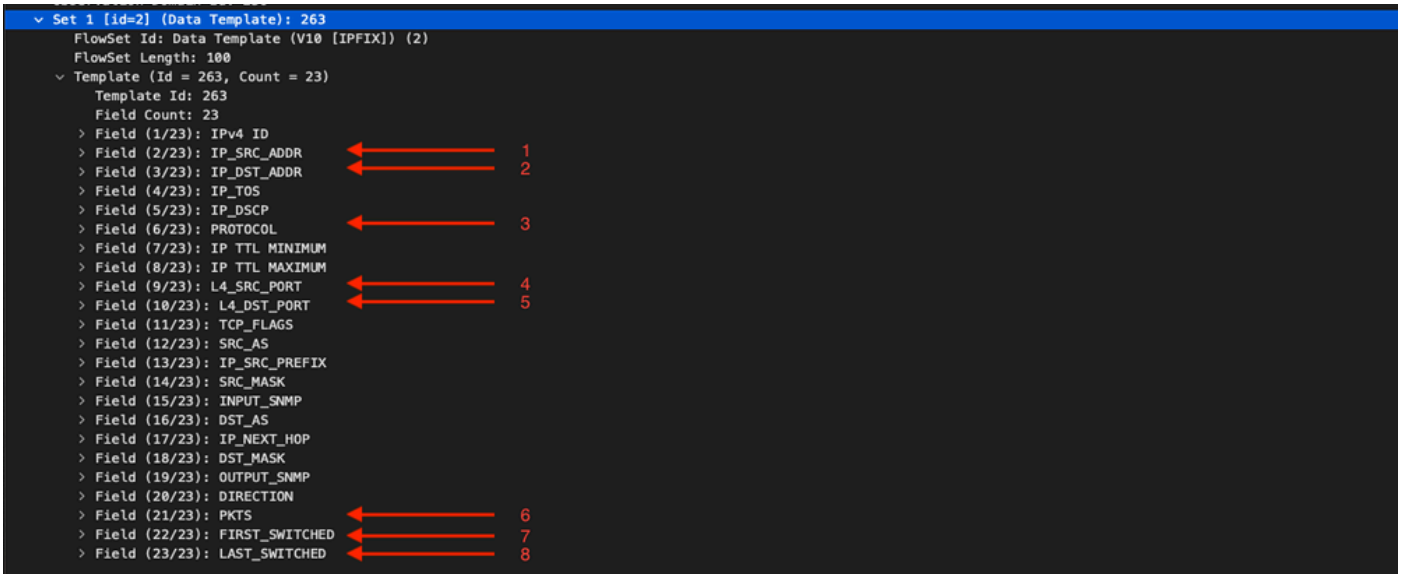
8. Klik op het pakketopnamebestand om het te downloaden naar uw lokale machine en open het op Wireshark:

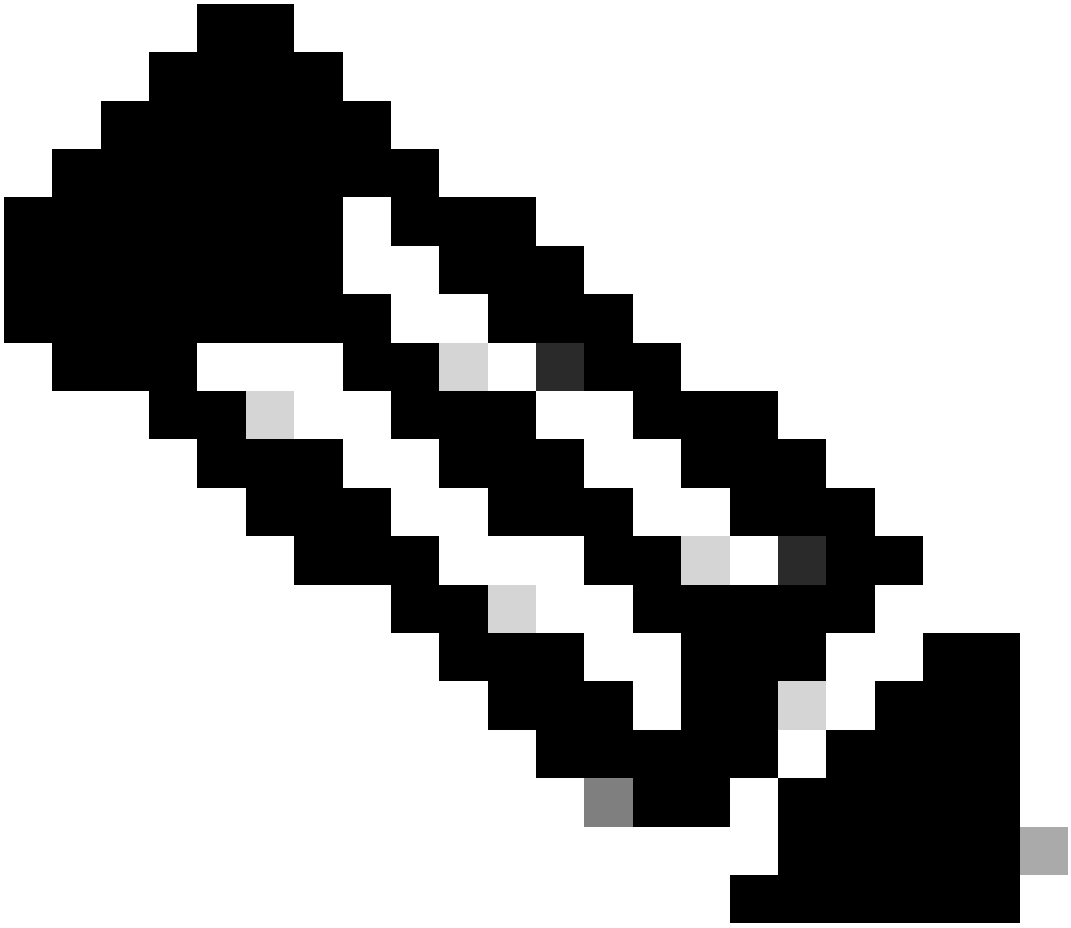


9. Identificeer het kader waarin de NetFlow/IPFIX-template is ontvangen.



10. Valideren dat de 9 vereiste velden in de template worden weergegeven





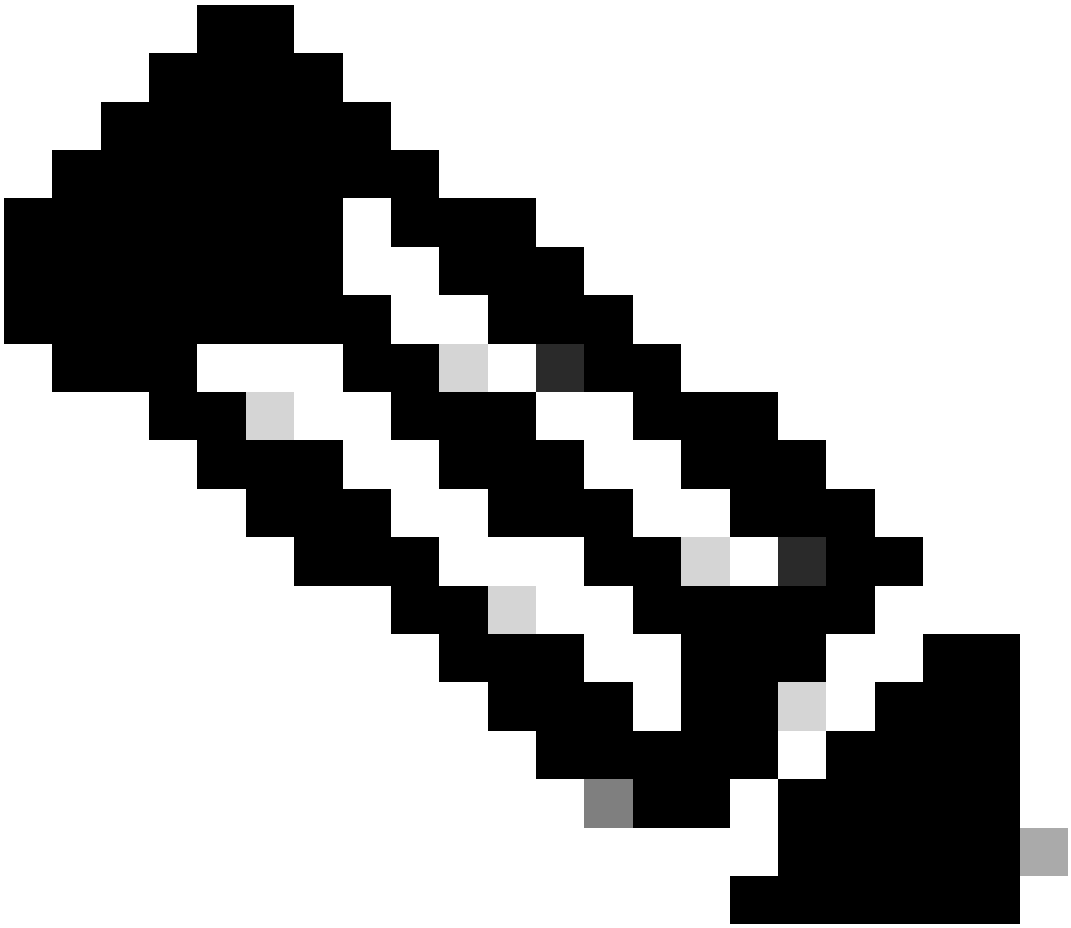
Opmerking: Merk op dat er op de sjabloon slechts 8 van de 9 verplichte velden zijn die SNA vereist voor Telemetry Ingest, voor dit scenario ontbreekt het BYTES-veld.

Controleer NetFlow/IPFIX Telemetry Ingest nadat u de ontbrekende velden hebt toegevoegd

Om te bevestigen of de SNA Flow Collector na de wijziging NetFlow/IPFIX-telemetrie van de exporteur ontvangt en invoegt:

1. Meld u aan bij SNA Flow Collector Admin UI met beheerdersreferenties: https://<Flow Collector IP Address>/swa/login.html
2. Navigeer in het linkerdeelvenster naar Ondersteuning > Bestanden bladeren
3. Navigeer naar de volgende map: sw > vandaag > logs
4. Klik op het sw.log bestand om het te downloaden naar uw lokale machine en open in op een teksteditor.
5. Zoek naar deze regels onderaan het logboek

```
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
```



Opmerking: Lijn 8 geeft aan dat er geen weggegooide stromen zijn over de laatste

---

periode.

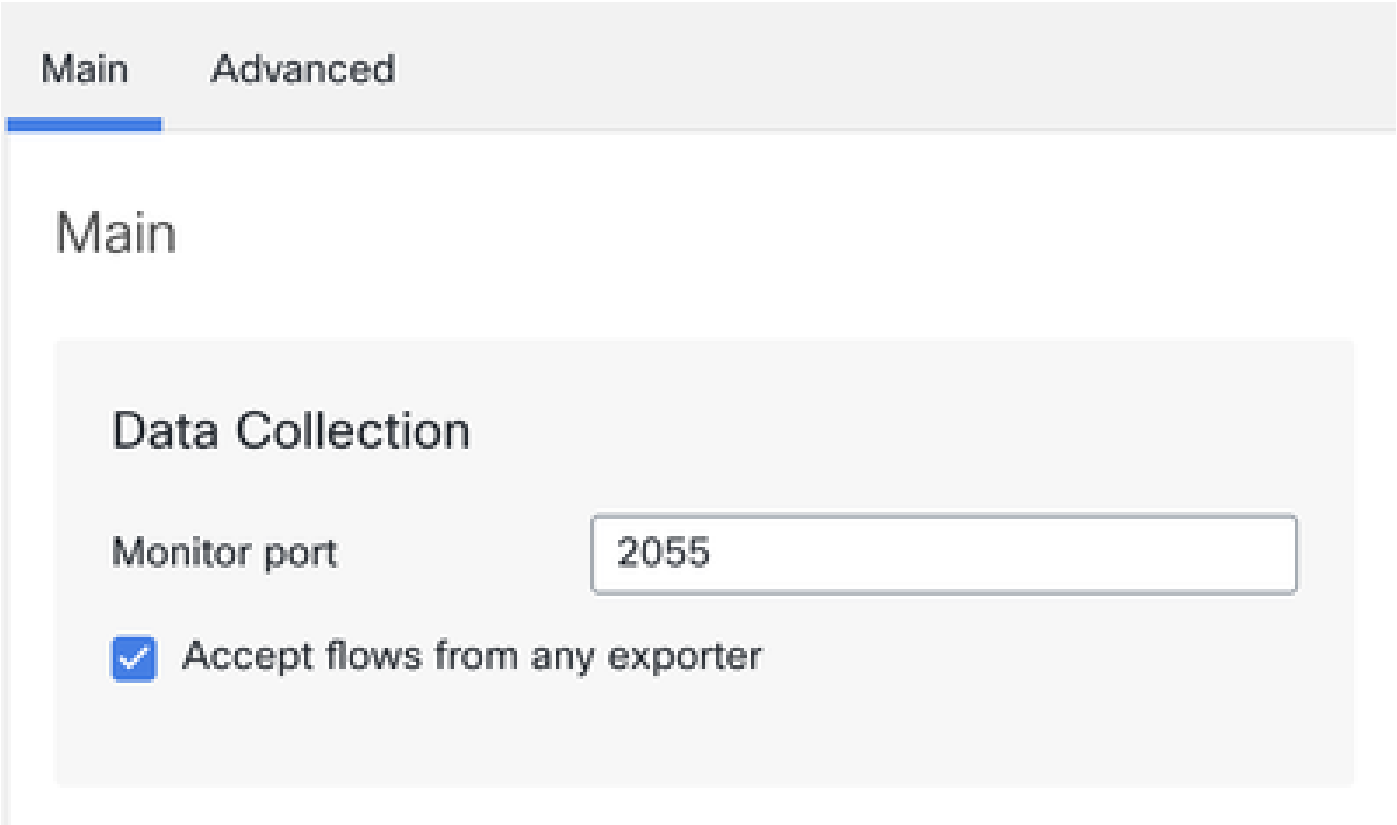
Inzetpoort voor NetFlow/IPFIX-telemetrie controleren

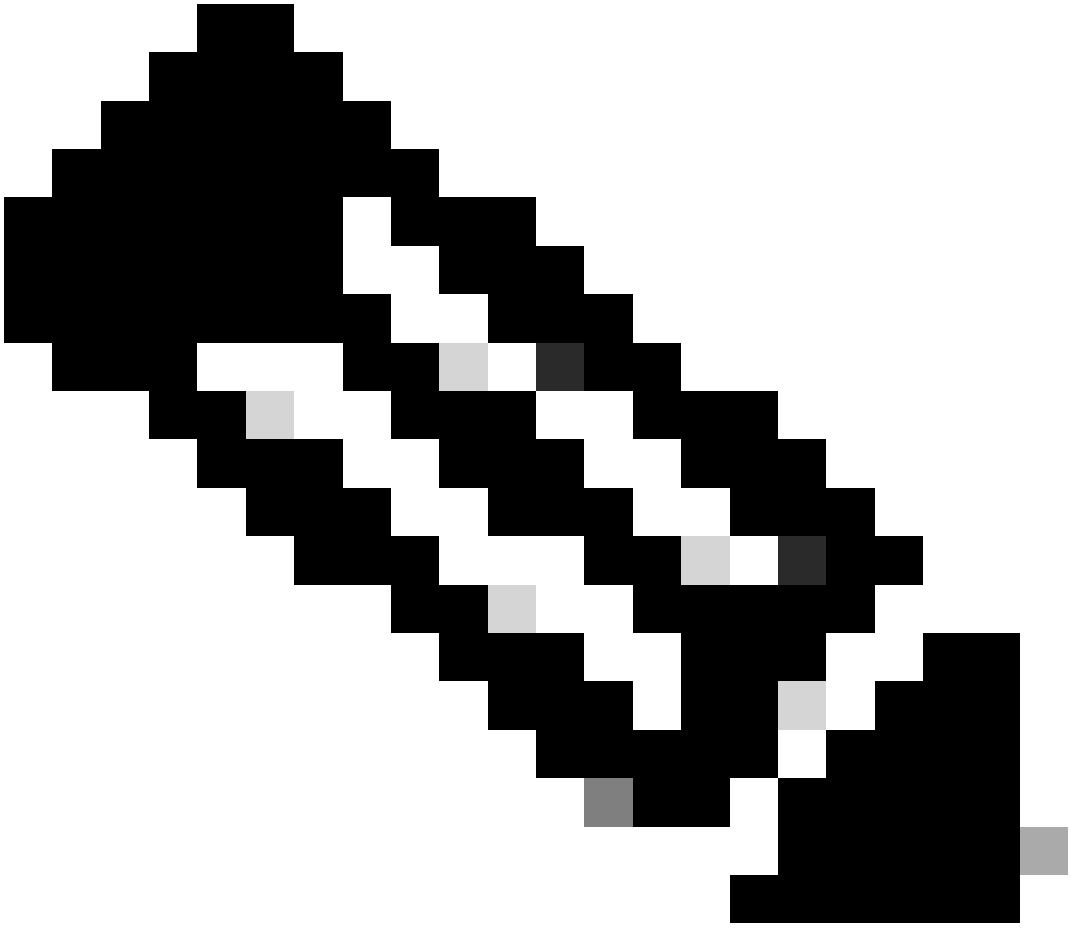
Om te bevestigen of de SNA Flow Collector NetFlow/IPFIX-telemetrie ontvangt van de exporteurs op de juiste poort:

1. Meld u aan bij de SNA Web UI met een gebruiker met beheerdersrechten.

2. Navigeer in het bovenste menu naar Configureren en kies Stroomverzamelaars

3. Bevestig dat de SNA Flow Collector dezelfde poort gebruikt die de exporteurs hebben geconfigureerd om NetFlow/IPFIX te verzenden





> Opmerking: de standaardpoort voor NetFlow is 2055, maar u kunt een andere poort selecteren. Zorg ervoor dat u dezelfde poort gebruikt tijdens het proces voor de eerste keer instellen op de stroomverzamelaar(s).

Controleer of de optie NetFlow/IPFIX Telemetry Ingest NetFlow is ingeschakeld

Om te bevestigen of de optie SNA Flow Collector voor telemetrie-inname van NetFlow/IPFIX is ingeschakeld:

1. Meld u aan bij de beheerdersinterface van SNA Flow Collector met beheerdersreferenties: https://<Flow Collector IP Address>/swa/login.html
2. Navigeer in het linkerdeelvenster naar Ondersteuning > Geavanceerde instellingen
3. Bevestig dat optie enable_netflow is ingesteld op 1:

Gerelateerde informatie

- Neem voor meer hulp contact op met het Technical Assistance Centre (TAC). Een geldig supportcontract is vereist: Cisco Worldwide Support Contacts.
- U kunt ook de Cisco Security Analytics Community hier bezoeken.
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.