Fehlerbehebung bei NetFlow/IPFIX Telemetry Ingest in Secure Network Analytics

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung für Netflow Telemetry Ingest in Secure Network Analytics (SNA) beschrieben.

Voraussetzungen

- Kenntnisse über Cisco SNA
- NetFlow/IPFIX-Kenntnisse

Anforderungen

- Sichere Netzwerkanalysen ab Version 7.5.0
- FlowCollector in Version 7.5.0 oder höher
- CLI-Zugriff als Systemadministrator auf Flow Collector
- Administrator-UI-Zugriff als Administrator für Flow Collector

Konfigurationsanleitungen

- Konfigurieren von NetFlow/IPFIX für Telemetry Ingest für sichere Netzwerkanalysen

Verwendete Komponenten

- SNA Manager und Flow Collector auf 7.5.0
- Wireshark-Software

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

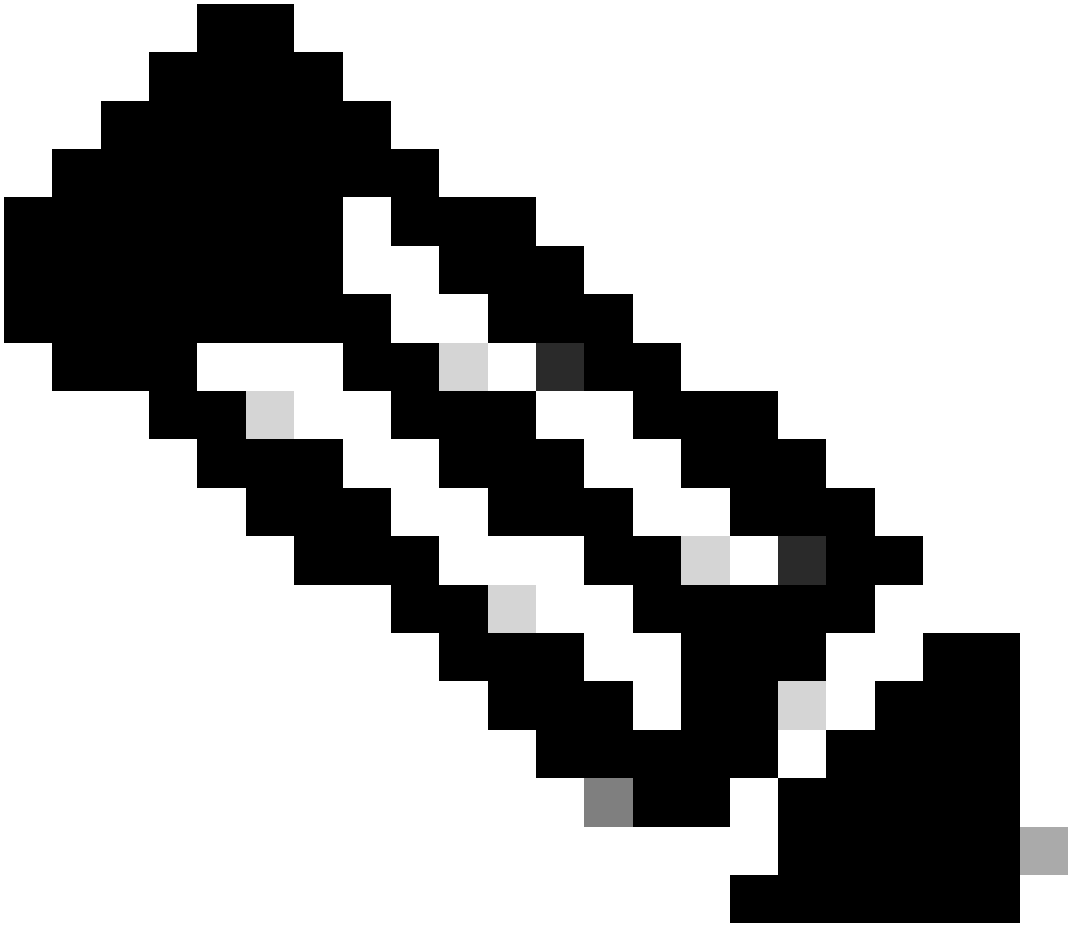
Hintergrundinformationen

Flow Collector ist eine SNA-Appliance, die für das Erfassen, Verarbeiten und Speichern von Flows zuständig ist, die an Secure Network Analytics gesendet werden. Für NetFlow-Version 9 oder IPFIX können mehrere Felder in der NetFlow/IPFIX-Vorlage enthalten sein, um weitere Informationen zum Netzwerkverkehr hinzuzufügen. Es gibt jedoch neun spezifische Felder, die in der NetFlow/IPFIX-Vorlage enthalten sein müssen, damit Flow Collector diese Flows verarbeiten kann. Flow Collector verarbeitet keine eingehenden Datenflüsse, die eine ungültige Vorlage enthalten. Aus diesem Grund zeigt SNA keine Datenflussinformationen dieser Exporteure unter Web UI oder Desktop Client an.

Pflichtfelder

Die nächsten Felder müssen in der NetFlow/IPFIX-Vorlage für die Telemetrie-Erfassung enthalten sein. Stellen Sie sicher, dass diese 9 Felder in der NetFlow/IPFIX-Vorlage enthalten sind, damit Secure Network Analytics eingehende Datenflüsse verarbeiten kann.

- IP-Quelladresse
- Ziel-IP-Adresse
- Quellport
- Zielport
- Layer-3-Protokoll
- Byte Anzahl
- Paketanzahl
- Flow-Startzeit
- Flow-Endzeit



Anmerkung: Die NetFlow/IPFIX-Konfiguration könnte weitere Felder enthalten. Die vorherigen Felder stellen jedoch die Mindestanforderungen für sichere Netzwerkanalysen für Telemetrie-Prüfvorgänge dar.

Fehlerbehebung

Überprüfung von NetFlow/IPFIX Telemetry Ingest

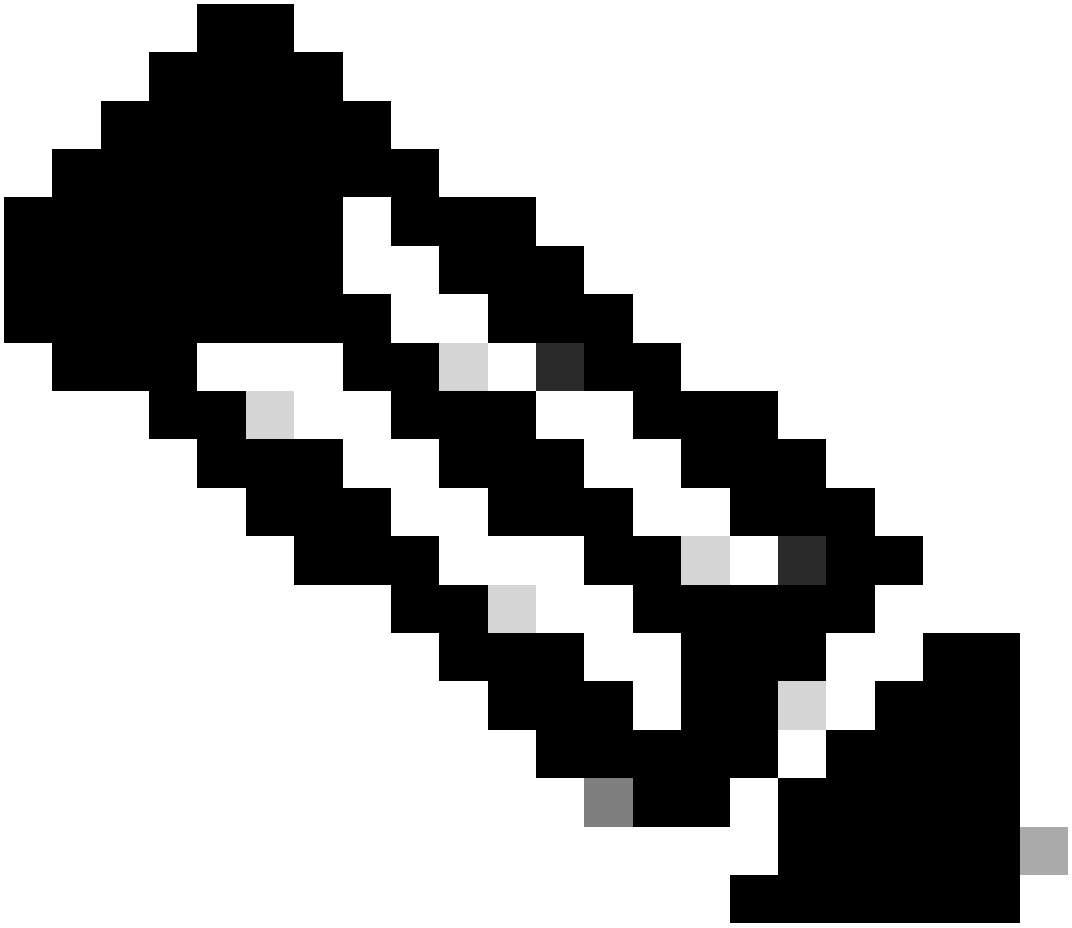
So überprüfen Sie, ob der SNA Flow Collector NetFlow/IPFIX-Telemetriedaten von den Exporteuren empfängt und einfügt:

1. Melden Sie sich bei der SNA Flow Collector-Admin-Benutzeroberfläche mit Admin-Anmeldeinformationen an: https://<IP-Adresse des FlowCollectors>/swa/login.html
2. Navigieren Sie im linken Bereich zu Support > Dateien durchsuchen.
3. Navigieren Sie zum nächsten Ordner: sw > Heute > Protokolle
4. Klicken Sie auf die Datei sw.log, um sie auf Ihren lokalen Computer herunterzuladen und in

einem Texteditor zu öffnen.

5. Suchen Sie am Ende des Protokolls nach diesen Zeilen. Diese Zusammenfassung wird alle fünf Minuten erstellt:

```
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
```



Anmerkung: Zeile 8 gibt an, dass Datenflüsse aufgrund unzureichender Vorlagendaten für den letzten Zeitraum verworfen wurden.

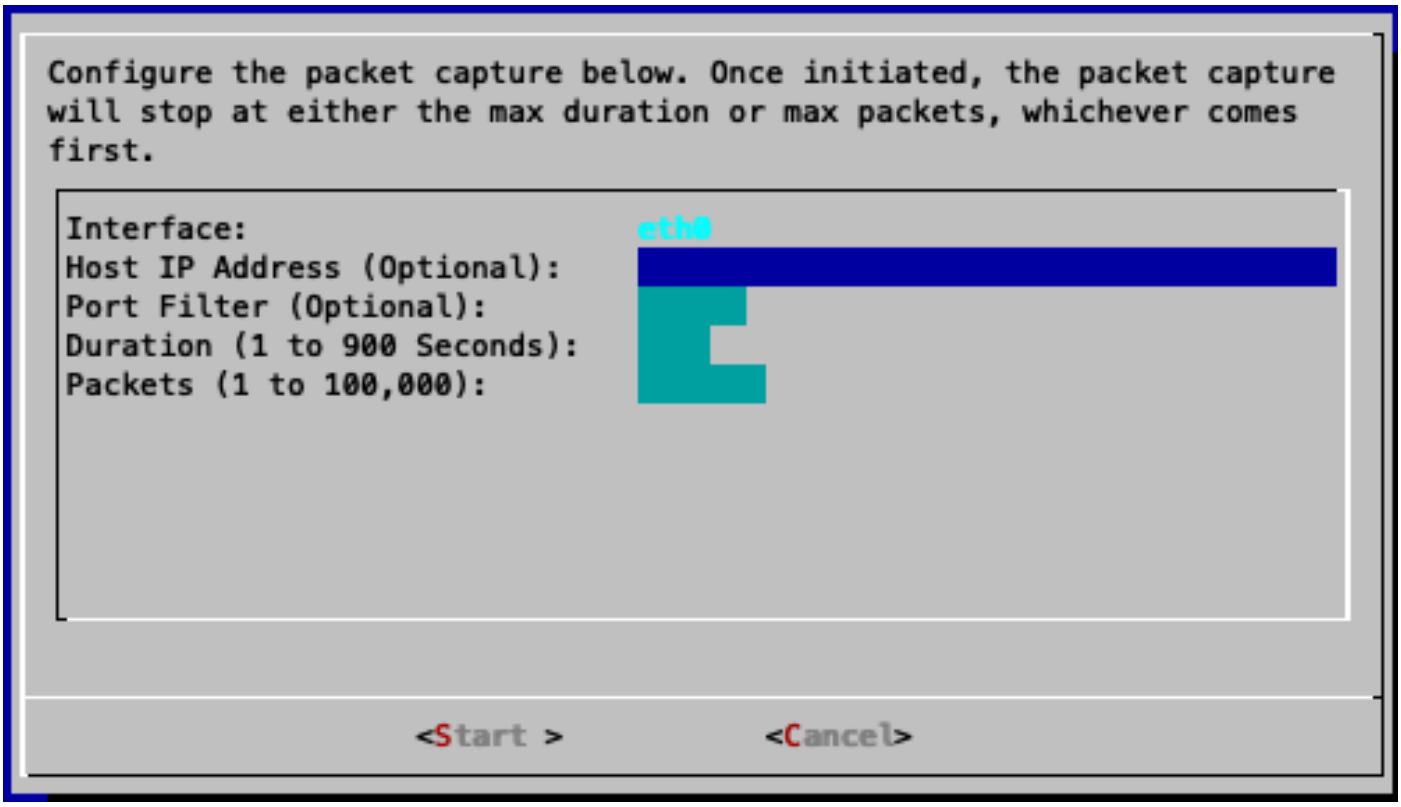
Überprüfung der NetFlow/IPFIX-Vorlage

So bestätigen Sie die in der NetfFlow/IPFIX-Vorlage enthaltenen Felder:

1. Melden Sie sich mit sysadmin-Anmeldeinformationen bei der SNA Flow Collector-CLI an.

2. Navigieren Sie im Menü SystemConfig zu: Erweitert > Paketerfassung

3. Geben Sie die Informationen des Ausführers ein, der keine Zahlungsströme auf der SNA anzeigt:



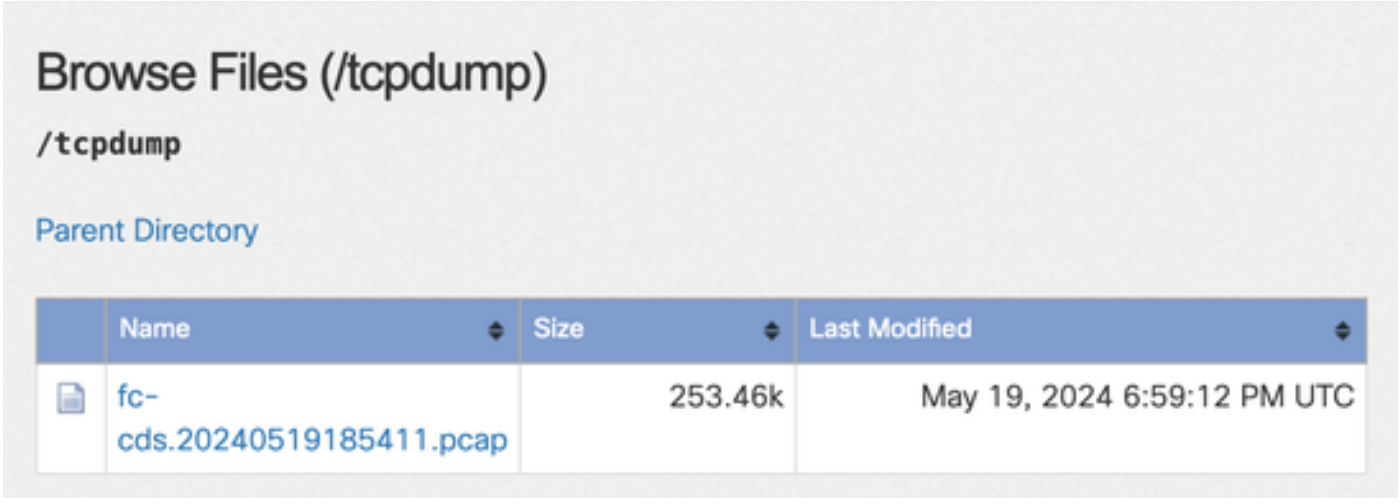
4. Warten Sie, bis der Prozess abgeschlossen ist.

5. Um die Datei herunterzuladen, melden Sie sich bei der SNA Flow Collector-Admin-Benutzeroberfläche mit Admin-Anmeldeinformationen an: https://<IP-Adresse des FlowCollectors>/swa/login.html

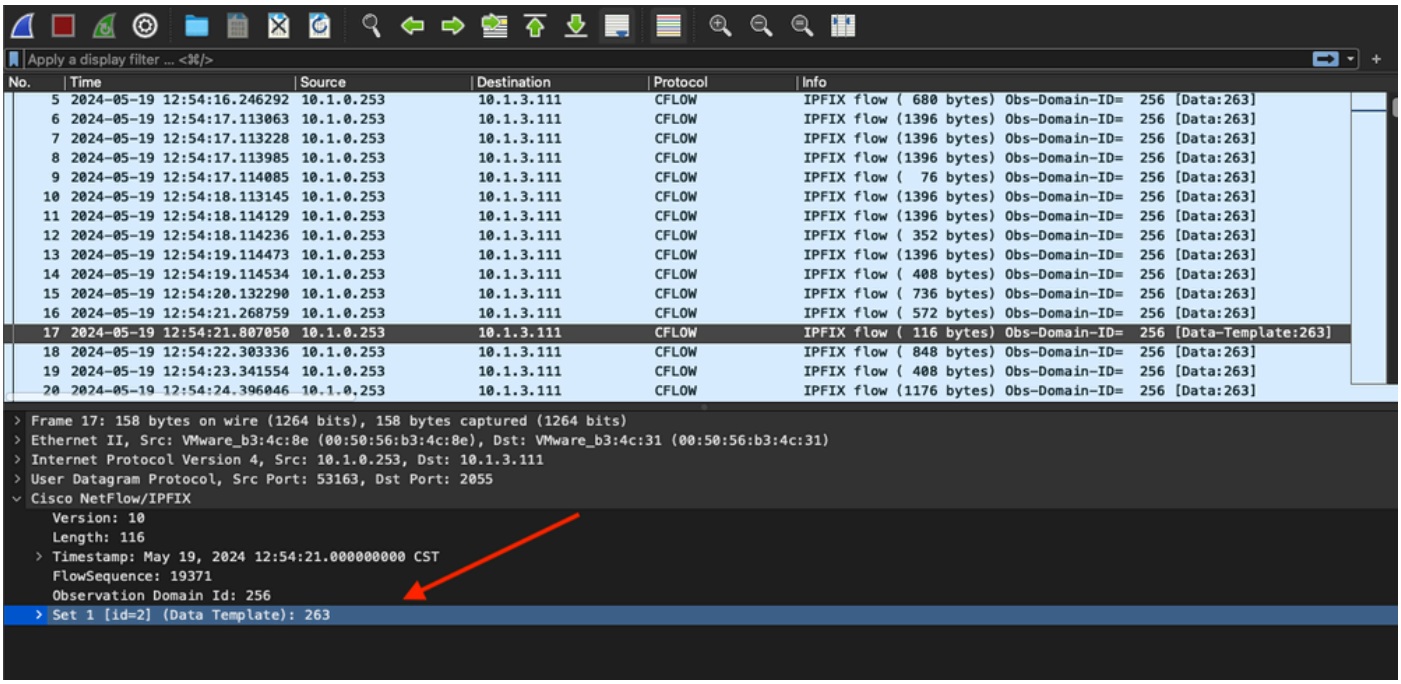
6. Navigieren Sie im linken Bereich zu Support > Dateien durchsuchen.

7. Navigieren Sie zum nächsten Ordner: TCPdump

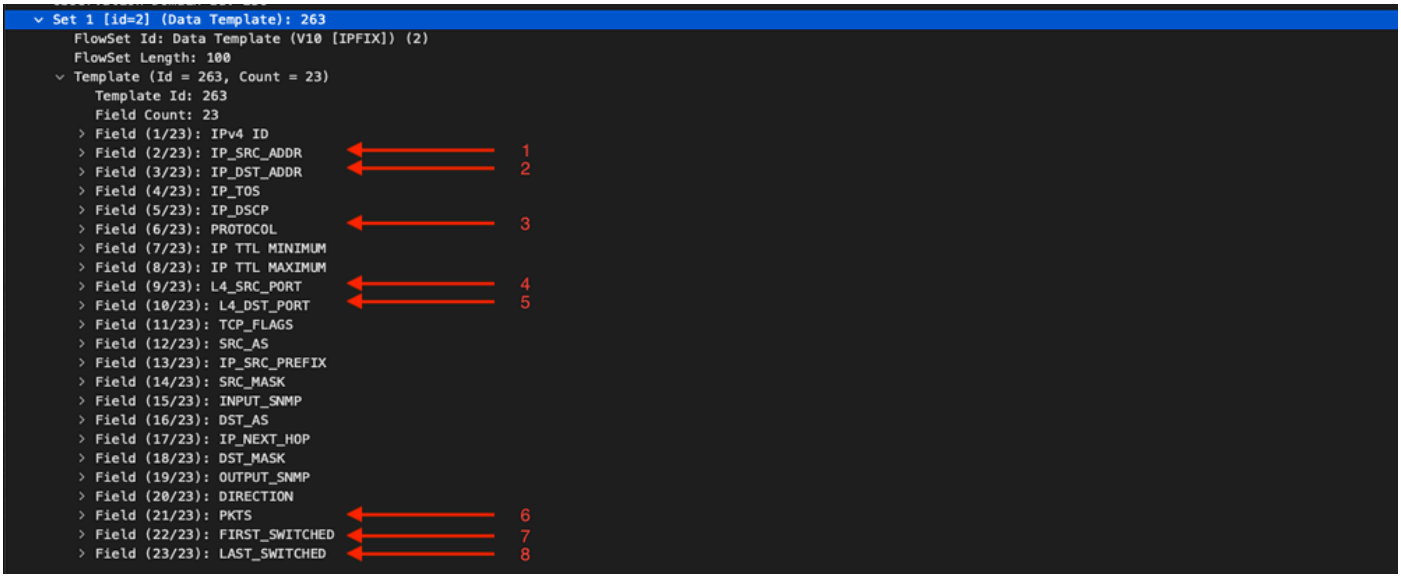
8. Klicken Sie auf die Paketerfassungsdatei, um sie auf Ihren lokalen Computer herunterzuladen, und öffnen Sie sie in Wireshark:

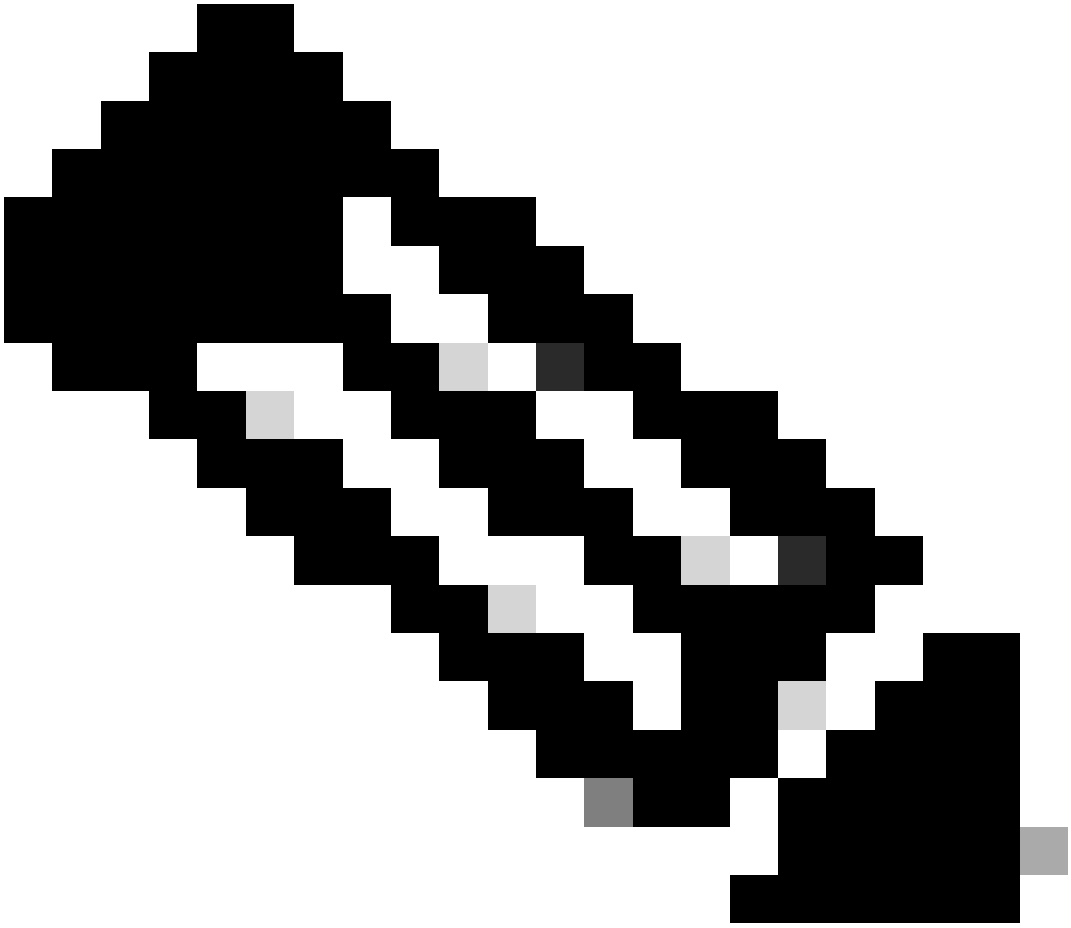


9. Identifizieren Sie den Frame, in dem die NetFlow/IPFIX-Vorlage empfangen wurde.



10. Überprüfen Sie, ob die 9 erforderlichen Felder in der Vorlage angezeigt werden.





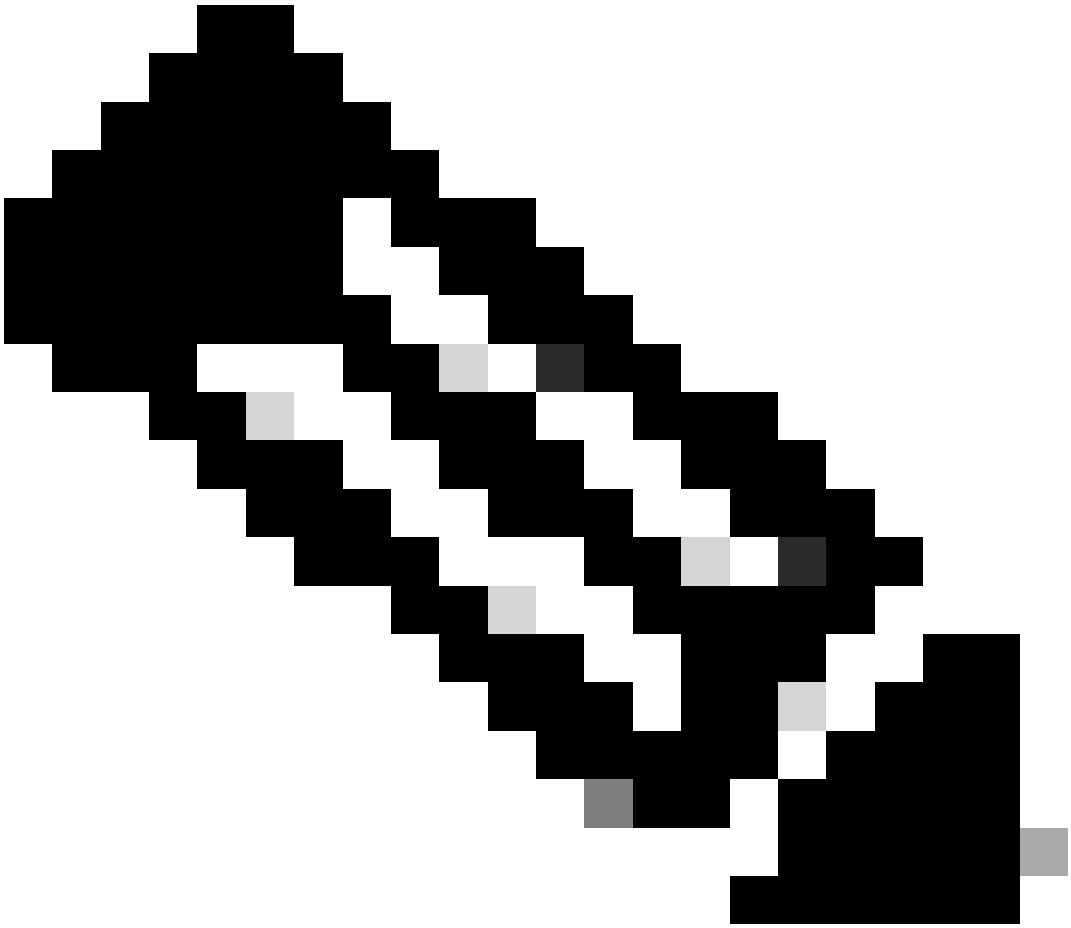
> Anmerkung: Beachten Sie, dass die Vorlage nur acht der neun Pflichtfelder enthält, die SNA für Telemetry Ingest benötigt. In diesem Szenario fehlt das Feld BYTES.

Überprüfen Sie NetFlow/IPFIX Telemetry Ingest nach dem Hinzufügen der fehlenden Felder.

So bestätigen Sie, ob der SNA Flow Collector nach der Änderung NetFlow-/IPFIX-Telemetriedaten vom Exporteur empfängt und einfügt:

1. Melden Sie sich bei der SNA Flow Collector-Admin-Benutzeroberfläche mit Admin-Anmeldeinformationen an: https://<IP-Adresse des FlowCollectors>/swa/login.html
2. Navigieren Sie im linken Bereich zu Support > Dateien durchsuchen.
3. Navigieren Sie zum nächsten Ordner: sw > Heute > Protokolle
4. Klicken Sie auf die Datei sw.log, um sie auf Ihren lokalen Computer herunterzuladen und in einem Texteditor zu öffnen.
5. Nach diesen Zeilen am unteren Rand des Protokolls suchen

```
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
```



Anmerkung: Zeile 8 gibt an, dass in der letzten Periode keine verworfenen Flows

---

vorhanden sind.

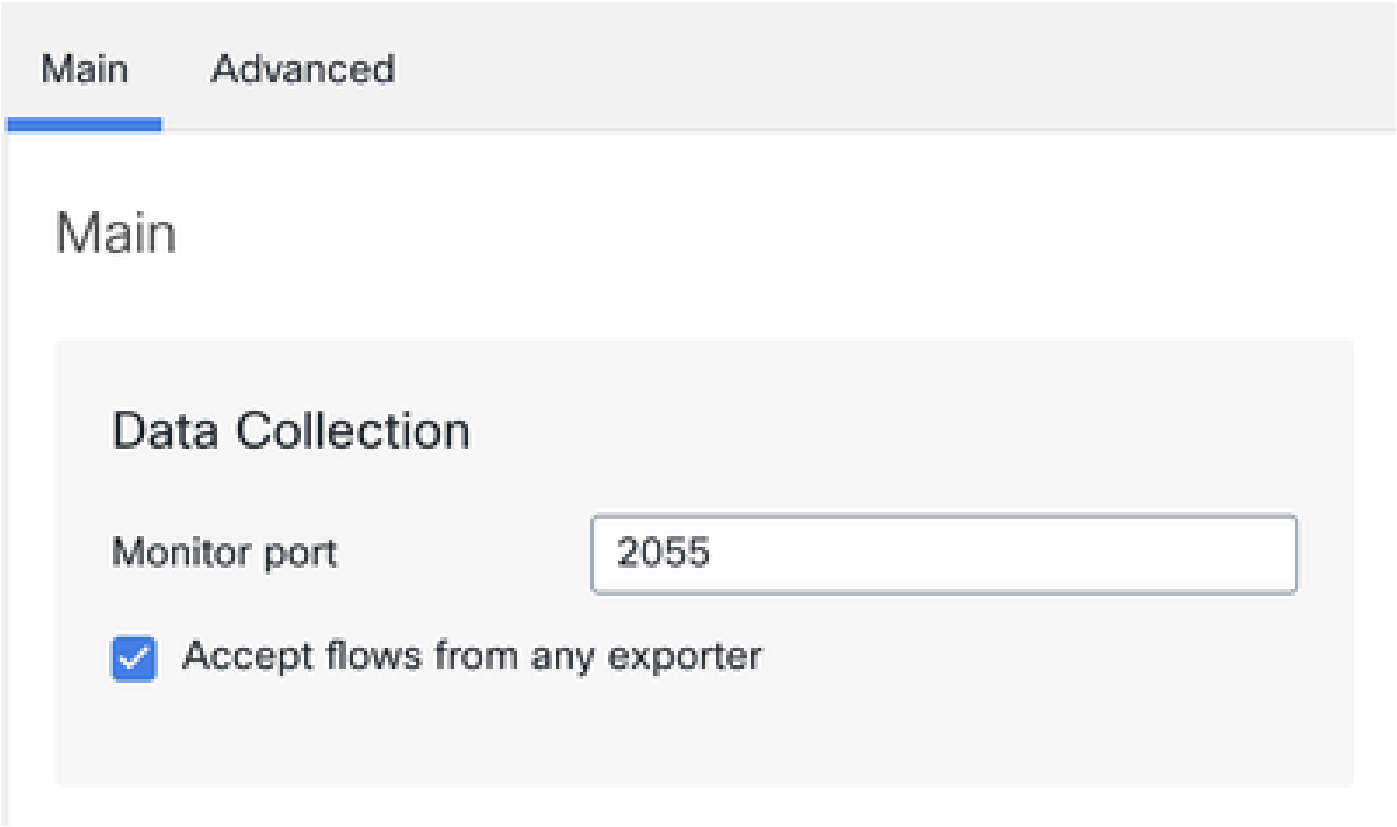
Überprüfen des NetFlow/IPFIX Telemetrie-Eingangsports

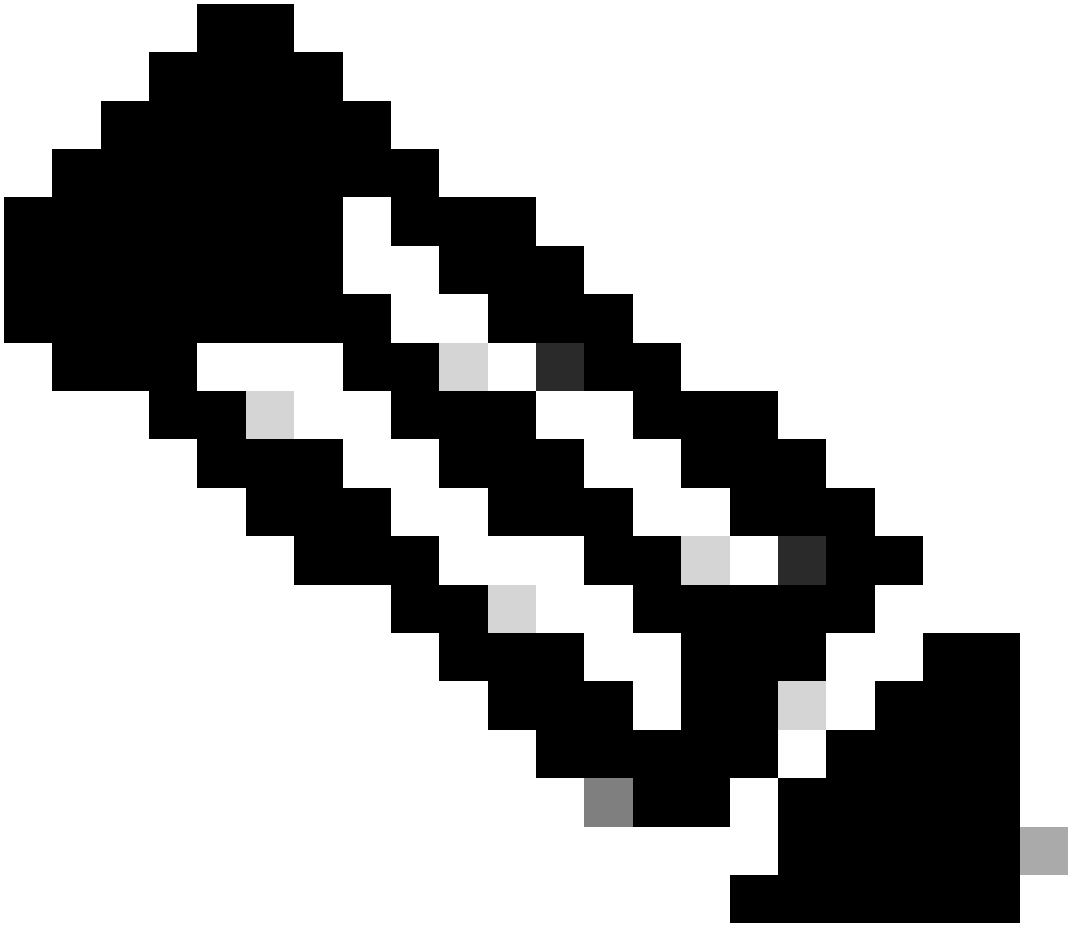
So überprüfen Sie, ob der SNA Flow Collector NetFlow/IPFIX-Telemetrie von den Exporteuren am richtigen Port empfängt:

1. Melden Sie sich bei der SNA-Webbenutzeroberfläche mit einem Benutzer mit Administratorberechtigungen an.

2. Navigieren Sie im oberen Menü zu Konfigurieren, und wählen Sie Flow Collectors aus.

3. Vergewissern Sie sich, dass der SNA Flow Collector den gleichen Port verwendet, den die Exporteure zum Senden von NetFlow/IPFIX konfiguriert haben.





> Anmerkung: Der Standard-Port für NetFlow ist 2055. Sie können jedoch einen anderen Port auswählen. Stellen Sie sicher, dass derselbe Port bei der Ersteinrichtung für Flow Collector(s) verwendet wird.

Überprüfen, ob die NetFlow/IPFIX Telemetry Ingest NetFlow-Option aktiviert ist

So prüfen Sie, ob die SNA Flow Collector-Option für die Telemetrie-Erfassung von NetFlow/IPFIX aktiviert ist:

1. Melden Sie sich mit Administratoranmeldeinformationen bei der SNA Flow Collector-Administrationsoberfläche an: https://<IP-Adresse des FlowCollectors>/swa/login.html
2. Navigieren Sie im linken Bereich zu Support > Erweiterte Einstellungen.
3. Bestätigen Sie, dass die Option enable_netflow auf 1 festgelegt ist:

Zugehörige Informationen

- Weitere Unterstützung erhalten Sie vom Technical Assistance Center (TAC). Ein gültiger Support-Vertrag ist erforderlich: Cisco Worldwide Support Contacts
- Sie können auch die Cisco Security Analytics-Community hier besuchen.
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.