# Konfigurieren von NetFlow/IPFIX für Telemetry Ingest auf SNA

### Inhalt

Einleitung				
Voraussetzungen				
Anforderungen				
Verwendete Komponenten				
Hintergrundinformationen				
Konfigurieren				
Pflichtfelder				
Empfohlene Felder				
Best Practices				
Überprüfung				

### Einleitung

In diesem Dokument werden die Best Practices und die grundlegende Konfiguration von Netflow/IPFIX beschrieben, die Secure Network Analytics (SNA) für die Telemetrie-Erfassung benötigt.

### Voraussetzungen

- Kenntnisse über Cisco SNA
- NetFlow/IPFIX-Kenntnisse

#### Anforderungen

- Sichere Netzwerkanalysen ab Version 7.2.1
- FlowCollector in Version 7.2.1 oder höher
- CLI-Zugriff als Root auf Flow Collector

#### Verwendete Komponenten

 Dies hängt vollständig von Ihrem Netzwerkdesign und den Geräten ab, die Sie ausgewählt haben, um NetFlow/IPFIX an Secure Network Analytics zu senden. Die NetFlow/IPFIX-Konfiguration unterscheidet sich je nach Exporteur. Für eine detaillierte Konfiguration wenden Sie sich bitte an das Support-Team jedes Exporteurs.

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.

### Konfigurieren

### 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



Hinweis: Die NetFlow/IPFIX-Konfiguration könnte weitere Felder enthalten. Die vorherigen Felder stellen jedoch die Mindestanforderungen für Secure Network Analytics für Telemetry Ingest dar.

#### **Empfohlene Felder**

Es wird empfohlen, die nächsten Felder in der NetFlow/IPFIX-Vorlage einzuschließen, um Informationen zu Schnittstelleninformationen zu sammeln. Diese Konfiguration ist erforderlich, um Schnittstelleninformationen wie Name und Geschwindigkeit anzuzeigen:

- Schnittstelleneingang
- Schnittstellenausgang

#### **Best Practices**

Darüber hinaus werden die nächsten Einstellungen als Best Practices empfohlen, um eine ordnungsgemäße Durchführung von Secure Network Analytics sicherzustellen.

- Aktives Timeout auf 60 Sekunden setzen
- Inaktives Timeout auf 15 Sekunden setzen
- Zeitüberschreitung für Vorlage auf 30 Sekunden festlegen



Hinweis: Der Standard-Port für NetFlow ist 2055. Sie können jedoch einen anderen Port auswählen. Stellen Sie sicher, dass derselbe Port während des letzten Prozesses für Flow Collector(s) verwendet wird.

## Überprüfung

Zur Validierung der NetFlow/IPFIX-Vorlagenkonfiguration können Sie eine Paketerfassung zwischen dem Exporter und FlowCollector ausführen. Melden Sie sich bei Flow Collector mit dem Root-Benutzer über SSH an, und führen Sie den folgenden Befehl aus:

tcpdump -nli [Collecting\_Interface] host [Exporter\_IP\_Address] and port [NetFlow\_Port] -w /lancope/var/

 Verwenden Sie ein SCP-Tool, um die Paketerfassung vom Flow Collector (in /lancope/var/tcpdump) auf Ihren lokalen Computer zu exportieren und dann in Wireshark zu öffnen.

	( 🎯 📄 🎬	🛛 🔀 🔄 🤇	수 🗢 曾 🕢 :	🕹 🗔 🔳	e, e, e, ײ			
Apply a display filter < %(>								
No.	Time	Source	Destination	Protocol	Info			
г	1 0.000000	10.1.0.253	10.1.3.31	CFLOW	IPFIX flow ( 728 bytes) Ob	os-Domain-ID= 256 [Data:260]		
	2 0.000207	10.1.0.253	10.1.4.3	CFLOW	IPFIX flow ( 728 bytes) Ob	os-Domain-ID= 256 [Data:260]		
	3 0.000256	10.1.0.253	10.1.4.32	CFLOW	IPFIX flow ( 728 bytes) Ob	os-Domain-ID= 256 [Data:260]		
	4 0.865908	10.1.0.253	10.1.3.31	CFLOW	IPFIX flow ( 848 bytes) Of	os-Domain-ID= 256 [Data:260]		
	5 0.866077	10.1.0.253	10.1.4.3	CFLOW	IPFIX flow ( 848 bytes) Of	os-Domain-ID= 256 [Data:260]		
	6 0.866112	10.1.0.253	10.1.4.32	CFLOW	IPFIX flow ( 848 bytes) Of	os-Domain-ID= 256 [Data:260]		
	7 1.892601	10.1.0.253	10.1.3.31	CFLOW	IPFIX flow ( 436 bytes) Of	s-Domain-ID= 256 [Data:260]		
	8 1.892699	10.1.0.253	10.1.4.3	CFLOW	IPFIX flow ( 436 bytes) Of	us-Domain-ID= 256 [Data:260]		
	9 1.892735	10.1.0.253	10.1.4.32	CFLOW	IPFIX flow (436 bytes) Of	s-Domain-ID= 256 [Data:260]		
11	10 3.012407	10.1.0.253	10.1.3.31	CFLOW	IPFIX flow ( 256 bytes) Of	JS-Domain-ID= 256 [Data:260]		
	11 3.012688	10.1.0.253	10.1.4.3	CFLOW	IPFIX flow ( 256 bytes) Of	Denois TD= 256 [Data:260]		
	12 3.012/0/	10.1.0.253	10.1.4.32	CFLOW	IPFIX flow ( 256 bytes) Of	)S-Domain-ID= 256 [Data:260]		
	13 3.880/04	10.1.0.255	10.1.3.31	CFLOW	TPETX flow ( 672 bytes) Of	Demoin ID= 256 [Data:260]		
	14 3.000900	10.1.0.255	10.1.4.3	CELOW	TPETX flow ( 672 bytes) 0	Demoin-ID= 256 [Data:260]		
	15 3.000930	10.1.0.255	10.1.4.32	CFLOW	TPETX flow ( 612 bytes) Of	Demoin ID= 256 [Data:260]		
	17 4 963406	10.1.0.255	10.1.3.31	CELOW	TPETX flow ( 612 bytes) 0	Domain_ID= 256 [Data:200]		
	18 4 963510	10.1.0.255	10.1.4.3	CELOW	TPETX flow ( 612 bytes) 0	s=Domain=ID= 256 [Data:260]		
	10 5.864222	10.1.0.253	10.1.3.31	CELOW	TPETX flow ( 848 bytes) 0	s=Domain=ID= 256 [Data:260]		
11	20 5.864379	10.1.0.253	10.1.4.3	CELOW	TPETX flow ( 848 bytes) 0	s=Domain=ID= 256 [Data:260]		
	21 5.864393	10.1.0.253	10.1.4.32	CFLOW	IPFIX flow ( 848 bytes) 0	s=Domain=ID= 256 [Data:260]		
Eromo 1. 7	70 huter on wire	a (5150 bitc) 77	9 butes contured (6169	hite)				
7 Finance 1: 776 bytes on while (blob bits), 776 bytes taptured (blob bits). 8 Ethernet TT Strei Mikare Bytes de (blob bits), 176 bytes taptured (blob bits).								
2 Enternet Erit, Stc. wwware_ustatuo (#0:50:50:05:03:00:00), USI: Wwware_ustatuo (00:30:50:03:04:09)								
S liser betaries protocol (1910) 4, 511 Del 2012 5, 511 Del 2012 5								
Cisco NetF	low/IPFIX		51 10111 2055					
Version	: 10							
lenth: 78								
> Timestamp: Jun 1. 2023 17:40:48.000000000 CST								
FlowSequence: 24347890								
Observation Domain Id: 256								
Set 1 [id=260] (12 flows)								
FlowSet Id: (Data) (260)								
FlowSet Length: 712								
[Template Frame: 52 (received after this frame)]								
> Flow	> Flow 1							
> Flow 2								

• Identifizieren Sie den Frame, in dem die NetFlow/IPFIX-Vorlage empfangen wurde, und öffnen Sie sie, um die in der Vorlage enthaltenen Felder zu überprüfen.

~ ~ ~ ~ >	<pre>&gt; Frame 52: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits) &gt; Ethernet II, Src: VMware_b3:6a:d6 (00:50:56:b3:6a:d6), Dst: VMware_b3:04:b9 (00:50:56:b3:04 &gt; Internet Protocol Version 4, Src: 10.1.0.253, Dst: 10.1.3.31 &gt; User Datagram Protocol, Src Port: 51431, Dst Port: 2055 ~ Cisco NetFlow/IPFIX</pre>	1:69)
	<pre>Version: 10 Length: 120 &gt; Timestamp: Jun 1, 2023 17:41:03.00000000 CST FlowSequence: 24348090 Observation Domain Id: 256 &gt; Set 1 [id=2] (Data Template): 260 FlowSet Id: Data Template (V10 [IPFIX]) (2) FlowSet Length: 104 &gt; Template (Id = 260, Count = 24) Template (Id = 260, Count = 24) &gt; Field (1/24): IP_SRC_ADDR &gt; Field (2/24): IP_SRC_ADDR &gt; Field (2/24): IP_DST_ADDR &gt; Field (2/24): IP_DST_ADDR &gt; Field (4/24): IP_DSCP &gt; Field (5/24): IP_DSCP &gt; Field (5/24): IP_DSCP &gt; Field (7/24): IP_TTL MINIMUM &gt; Field (9/24): L4_SRC_PORT &gt; Field (1/24): L4_SRC_PORT &gt; Field (11/24): TCP_FLAGS &gt; Field (11/24): SRC_AS &gt; Field (11/24): SRC_MASK &gt; Field (11/24): INPUT_SNMP &gt; Field (11/24): INPUT_SNMP &gt; Field (11/24): ID_TLMASK &gt; Field (11/24): DST_MASK &gt; Field (11/24): DST_MASK &gt; Field (11/24): DST_MASK &gt; Field (12/24): BYTES &gt; Field (22/24): BYTES &gt; Field (22/24): BYTES &gt; Field (22/24): FKTS_WITCHED</pre>	
	> Field (24/24): LAST_SWITCHED	



Hinweis: Die angezeigten Feldnamen können je nach Exporteur unterschiedlich aussehen. Dies ist nur ein Hinweis darauf, wie Sie diese Felder validieren können.

#### 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.