Configurazione di NetFlow/IPFIX per l'acquisizione della telemetria sulla SNA

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Configurazione
Campi obbligatori
Campi consigliati
Procedure ottimali
<u>Verifica</u>

Introduzione

Questo documento descrive le best practice e la configurazione di base di Netflow/IPFIX necessarie per Secure Network Analytics (SNA) per il caricamento della telemetria.

Prerequisiti

- Conoscenza SNA Cisco
- Conoscenze NetFlow/IPFIX

Requisiti

- Secure Network Analytics versione 7.2.1 o successive
- Flow Collector in 7.2.1 o versioni successive
- Accesso CLI come root a Flow Collector

Componenti usati

 Ciò dipende completamente dalla progettazione della rete e dai dispositivi selezionati per inviare NetFlow/IPFIX a Secure Network Analytics. La configurazione di NetFlow/IPFIX varia a seconda dell'esportatore. Per informazioni dettagliate sulla configurazione, rivolgersi al team di supporto di ciascun esportatore.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Premesse

Flow Collector è un'appliance SNA incaricata di raccogliere, elaborare e archiviare i flussi che vengono inviati a Secure Network Analytics. Per NetFlow versione 9 o IPFIX, è possibile includere diversi campi nel modello NetFlow/IPFIX per aggiungere ulteriori informazioni relative al traffico di rete. Tuttavia, sono disponibili 9 campi specifici che devono essere inclusi nel modello NetFlow/IPFIX affinché il Flow Collector possa elaborare tali flussi. Flow Collector non elabora i flussi in ingresso che includono un modello non valido, pertanto SNA non visualizza le informazioni sul flusso di tali esportatori sotto interfaccia utente Web o client desktop.

Configurazione

Campi obbligatori

I campi successivi devono essere inclusi nel modello NetFlow/IPFIX per il caricamento della telemetria. Verificare che questi 9 campi siano inclusi nel modello NetFlow/IPFIX per consentire a Secure Network Analytics di elaborare i flussi in ingresso.

- Source IP Address
- Indirizzo IP di destinazione
- Porta di origine
- · Porta di destinazione
- Protocollo di livello 3
- Conteggio byte
- Conteggio pacchetti
- Ora inizio flusso
- Ora fine flusso



Nota: è possibile includere più campi nella configurazione NetFlow/IPFIX, tuttavia i campi precedenti rappresentano i requisiti minimi di Secure Network Analytics per il caricamento della telemetria.

Campi consigliati

Si consiglia di includere i campi successivi nel modello NetFlow/IPFIX per raccogliere informazioni sull'interfaccia. Questa configurazione è necessaria per visualizzare le informazioni sull'interfaccia, ad esempio il nome e la velocità:

- Ingresso interfaccia
- Uscita interfaccia

Procedure ottimali

Inoltre, le impostazioni successive sono consigliate come best practice per garantire le prestazioni corrette di Secure Network Analytics.

- Imposta timeout attivo su 60 secondi
- · Impostare il timeout di inattività su 15 secondi
- Impostare il timeout del modello su 30 secondi



Nota: la porta predefinita per NetFlow è 2055. Tuttavia, è possibile selezionare un'altra porta. Accertarsi di utilizzare la stessa porta durante il processo lc-ast sui Flow Collector.

Verifica

Per convalidare la configurazione del modello NetFlow/IPFIX, è possibile eseguire un'acquisizione di pacchetto tra l'utilità di esportazione e Flow Collector. Accedere al Flow Collector con l'utente root tramite SSH ed eseguire il comando:

tcpdump -nli [Collecting_Interface] host [Exporter_IP_Address] and port [NetFlow_Port] -w /lancope/var/

• Usare uno strumento SCP per esportare l'acquisizione del pacchetto dal Flow Collector (situato in /lancope/var/tcpdump) al computer locale e aprirla su Wireshark

🗖 🔲 🙍	0	•	×	C	্	þ 🔿	2	$\overline{\mathbf{O}}$				⊕ 	e,	€,	••									
📕 Apply a displ	Apply a display filter < 14/>																							
No.	11	Time	Source			Des	tination			Prot	ocol		Info	D										
Г	1 (0.000000	10.1.0	0.253		10.	1.3.31	l I		CFL	OW		IP	FIX 1	flow	(728	bytes)	Obs-D	omain-I	D= 256	6 (Da	ata:260]		
	2	0.000207	10.1.0	0.253		10.	1.4.3			CFL	OW		IP	FIX 1	flow	(728	bytes	Obs-D	omain-I	D= 256	6 [Da	ata:260]		
	3	0.000256	10.1.0	0.253		10.	1.4.32	2		CFL	OW		IP	FIX 1	f LOW	(728	bytes	Obs-D	omain-I	D= 250	6 [Da	ata:260]		
	4	0.865908	10.1.4	0.253		10.	1.3.31			CFL	OW OH		TP		flow (048	bytes	Obs-D	omain-I	D= 250	s (Da	sta:260]		
	6	0.0000//	10.1.0	0.253		10.	1 4 32	,		CEL	0W		TP	ETX 4	flow i	040	bytes	Obs-D	omain_I	D= 250	6 [Da	113:200]		
	7	1.892601	10.1.0	0.253		10.	1.3.31	1		CEL	OW		TP	FTX 1	flow	(436	hytes	Obs-D	omain-T	D= 256	6 [Da	ata:260]		
	8	1.892699	10.1.0	0.253		10.	1.4.3	•		CEL	OW		TP	FTX 1	flow	(436	hytes	Obs-D	omain-T	D= 256	6 [Da	ata:260]		
	9	1.892735	10.1.0	0.253		10.	1.4.32	2		CFL	OW		IP	FIX 1	flow	(436	bytes	Obs-D	omain-I	D= 256	6 [Da	ata:260]		
	10	3.012407	10.1.0	0.253		10.	1.3.31	1		CFL	OW		IP	FIX 1	flow	(256	bytes)	Obs-D	omain-I	D= 256	6 [Da	ata:260]		
	11	3.012688	10.1.0	0.253		10.	1.4.3			CFL	OW		IP	FIX 1	flow	(256	bytes)	0bs-D	omain-I	D= 256	6 (Da	ata:260]		
	12	3.012707	10.1.6	0.253		10.	1.4.32	2		CFL	OW		IP	FIX 1	flow	(256	bytes)	Obs-D	omain-I	D= 256	6 [Da	ata:260]		
11	13	3.880764	10.1.0	0.253		10.	1.3.31	1		CFL	OW		IP	FIX 1	flow	(672	bytes)	Obs-D	omain-I	D= 256	6 [Da	ata:260]		
	14	3.880908	10.1.0	0.253		10.	1.4.3			CFL	OW		IP	FIX 1	flow	(672	bytes)	Obs-D	omain-I	D= 256	6 [Da	ata:260]		
	15	3.880938	10.1.0	0.253		10.	1.4.32	2		CFL	OW		IP	FIX 1	flow	(672	bytes)	Obs-D	omain-I	D= 256	6 [Da	ata:260]		
	16	4.863348	10.1.0	0.253		10.	1.3.31	1		CFL	OW		IP	FIX 1	flow	(612	bytes)	Obs-D	omain-I	D= 256	6 (Da	ata:260]		
	17	4.863496	10.1.0	0.253		10.	1.4.3			CFL	OW		IP	FIX 1	flow	(612	bytes)	Obs-D	omain-I	D= 256	6 [Da	ata:260]		
	18	4.863519	10.1.0	0.253		10.	1.4.32	2		CFL	OW		IP	FIX 1	flow	(612	bytes)	Obs-D	omain-I	D= 256	6 [Da	ata:260]		
	19	5.864222	10.1.0	0.253		10.	1.3.31	1		CFL	OW		IP	FIX 1	flow	(848	bytes	Obs-D	omain-I	D= 256	6 [Da	ata:260]		
	20	5.864379	10.1.0	0.253		10.	1.4.3			CFL	OW		IP	FIX 1	flow ((848	bytes	Obs-D	omain-I	D= 256	5 [Da	ata:260]	_	_
	21	5.864393	10.1.0	9.253		10.	1.4.32				UW		IP		LOW	848	bytes	065=0	omain=1	D= 258	5 105	1121269		
> Frame 1: 7	70 byte	s on wire	(6160	bits),	770 0	ytes ca	ptured	1 (616	0 bit	S)			e	4.60										
> Ethernet J	LI, SFC:	VMware_03	:68:06	(00:5	0:56:0	3:6a:d6	1, UST	21 21	are_b	3:04:	DA (98	1:50:5	6:03:0	14:D9										
> licer Data	> Internet Protocol Version 4, Src: 10.1.0.253, Dst: 10.1.3.31																							
V Cisco Net		TY STC	POIL.	51451	, DSC	FUIL: 2	055																	
Version	: 10	201																						
Length:	728									1														
> Timestamp: Jun 1, 2023 17:40:48.00000000 CST																								
FlowSequence: 24347890																								
Observation Domain Id: 256																								
v Set 1 [id=260] (12 flows)																								
FlowSet Id: (Data) (260)																								
Flows	Set Leng	gth: 712																						
[Temp	plate Fr	rame: 52 (r	eceive	d afte	er this	frame)	1																	
> Flow	1																							
> Flow	2																							

Identificare il frame in cui è stato ricevuto il modello NetFlow/IPFIX e aprirlo per convalidare i campi inclusi nel modello

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



Nota: i nomi dei campi visualizzati possono avere un aspetto diverso in ogni funzione di esportazione. Si tratta solo di un riferimento al modo in cui è possibile convalidare tali campi.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).