Configuration de NetFlow/IPFIX pour l'accès de télémétrie sur SNA

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Configurer

- Champs obligatoires
- Champs recommandés
- Meilleure pratique

Vérifier

Introduction

Ce document décrit les meilleures pratiques et la configuration de base de Netflow/IPFIX dont Secure Network Analytics (SNA) a besoin pour l'acquisition de la télémétrie.

Conditions préalables

- Connaissances de Cisco SNA
- Connaissances NetFlow/IPFIX

Exigences

- Secure Network Analytics dans la version 7.2.1 ou ultérieure
- Collecteur de flux de la version 7.2.1 ou ultérieure
- Accès CLI en tant que racine au collecteur de flux

Composants utilisés

- Cela dépend entièrement de la conception de votre réseau et des périphériques que vous avez sélectionnés pour envoyer NetFlow/IPFIX à Secure Network Analytics. La configuration NetFlow/IPFIX est différente pour chaque exportateur. Pour obtenir une configuration détaillée, contactez l'équipe d'assistance de chaque exportateur.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

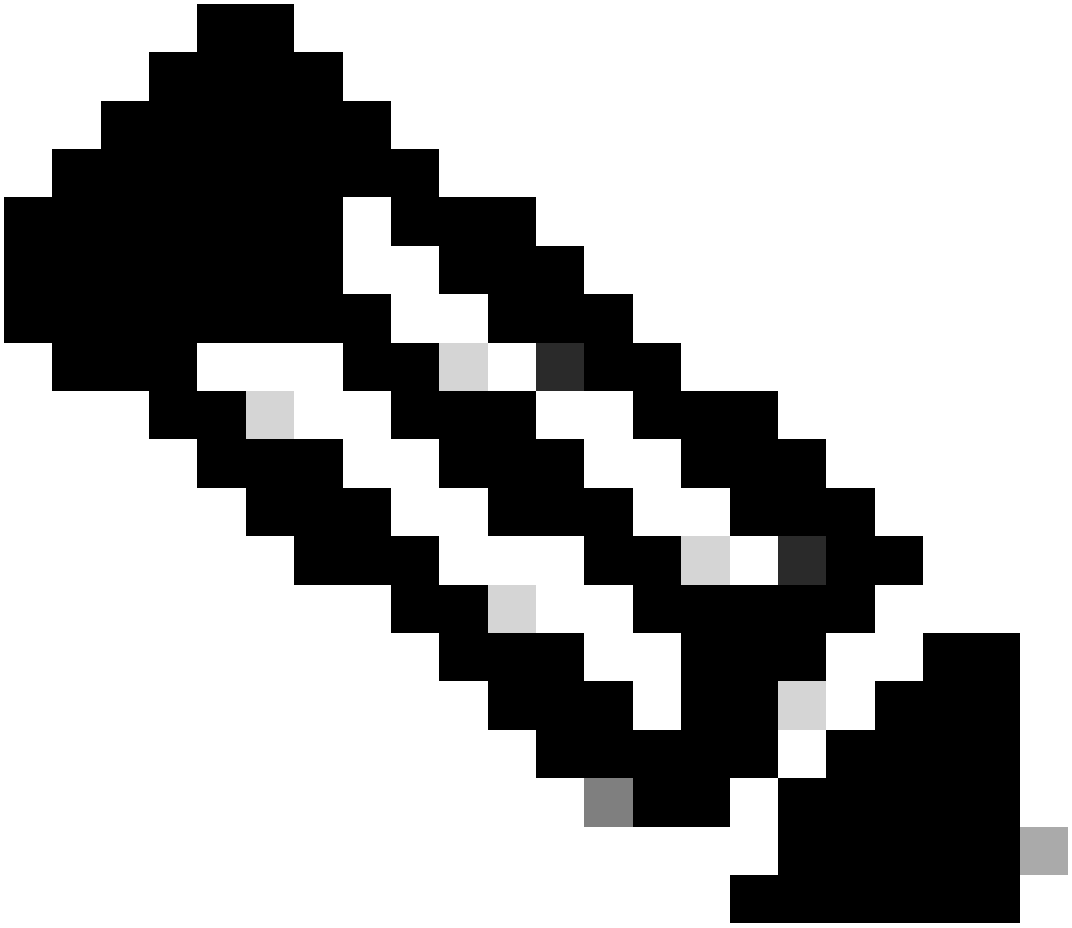
Le collecteur de flux est une appliance SNA chargée de collecter, traiter et stocker les flux envoyés à Secure Network Analytics. Pour NetFlow version 9 ou IPFIX, plusieurs champs peuvent être inclus dans le modèle NetFlow/IPFIX pour ajouter des informations relatives au trafic réseau. Toutefois, 9 champs spécifiques doivent être inclus dans le modèle NetFlow/IPFIX pour que le collecteur de flux puisse traiter ces flux. Le collecteur de flux ne traite pas les flux entrants qui incluent un modèle non valide. Par conséquent, SNA n'affiche pas les informations de flux de ces exportateurs sous l'interface utilisateur Web ou le client Desktop.

Configurer

Champs obligatoires

Les champs suivants doivent être inclus dans le modèle NetFlow/IPFIX pour l'acquisition de télémétrie. Assurez-vous que ces 9 champs sont inclus dans le modèle NetFlow/IPFIX, afin que Secure Network Analytics traite les flux entrants.

- adresse IP source
- adresse IP de destination
- Port source
- Port de destination
- Protocole de couche 3
- Nombre d'octets
- Nombre de paquets
- Heure de début du flux
- Heure de fin du flux



Remarque : d'autres champs peuvent être inclus dans la configuration NetFlow/IPFIX. Toutefois, les champs précédents correspondent aux exigences minimales de Secure Network Analytics pour l'accès de télémétrie.

Champs recommandés

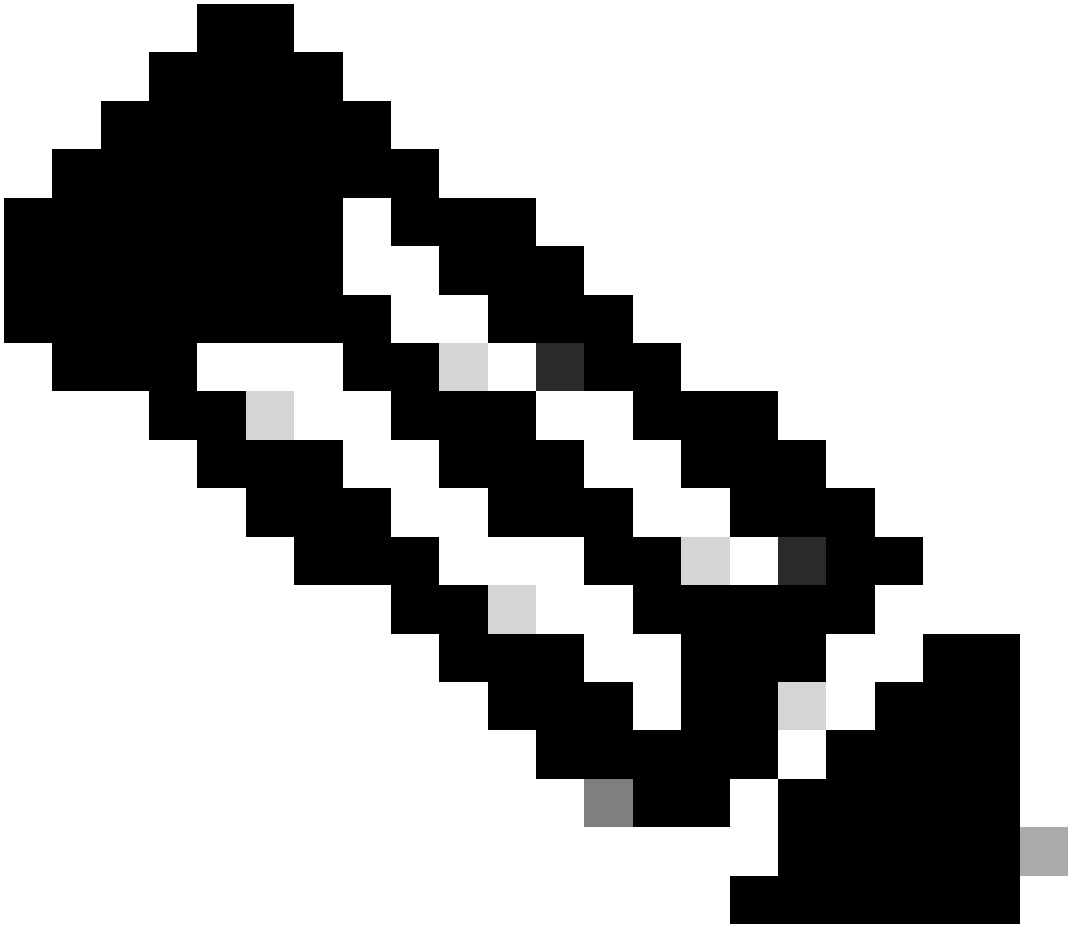
Il est recommandé d'inclure les champs suivants dans le modèle NetFlow/IPFIX pour collecter des informations sur les informations d'interface. Cette configuration est requise pour afficher les informations d'interface telles que le nom et la vitesse :

- Entrée interface
- Sortie interface

Meilleure pratique

En outre, les paramètres suivants sont recommandés comme meilleures pratiques pour garantir des performances correctes de Secure Network Analytics.

- Définir le délai d'attente actif à 60 secondes
- Définir le délai d'inactivité sur 15 secondes
- Définir le délai d'attente du modèle sur 30 secondes



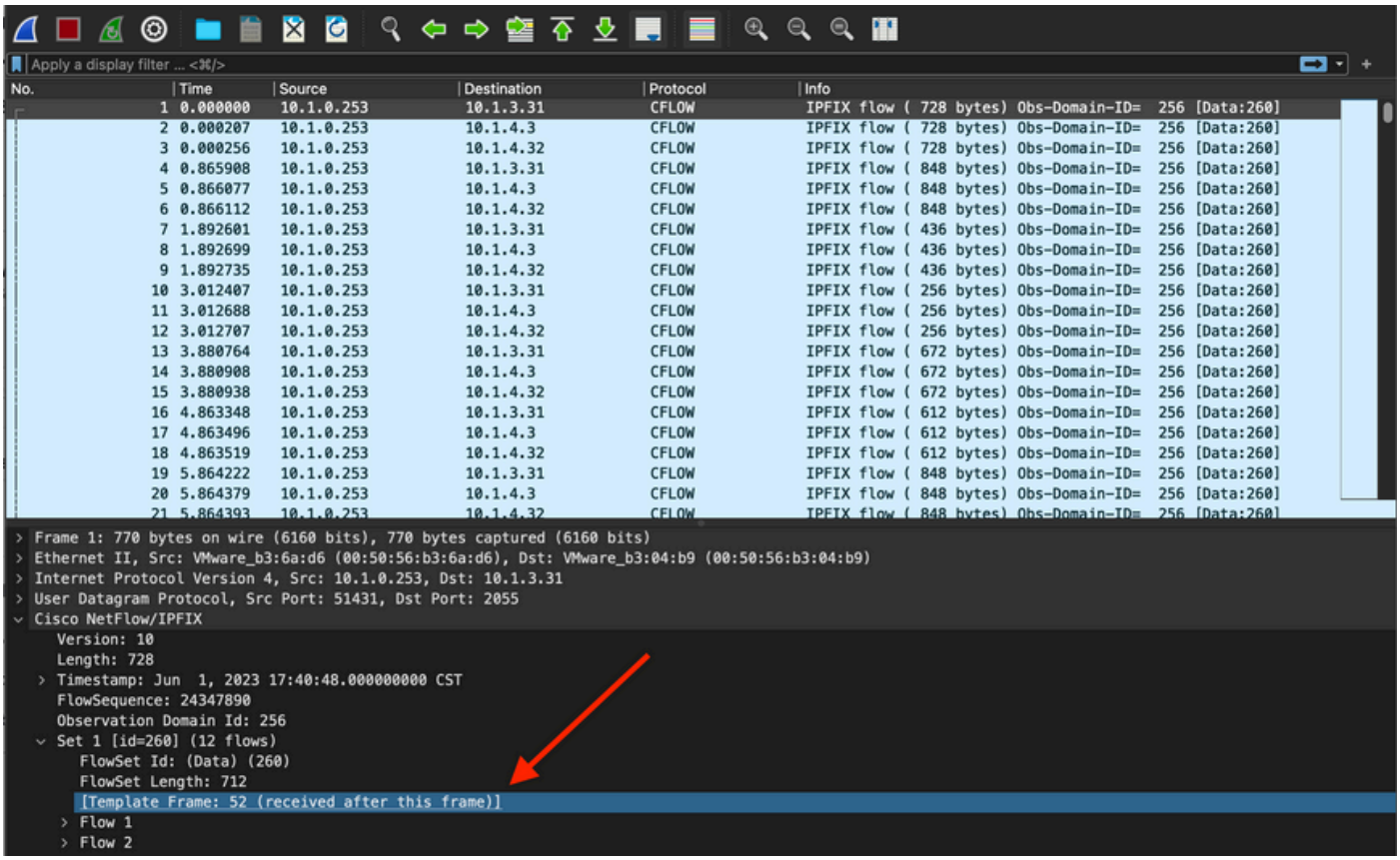
Remarque : le port par défaut pour NetFlow est 2055. Toutefois, vous pouvez sélectionner un autre port. Veillez à utiliser le même port pendant le processus lc-ast sur les collecteurs de flux.

Vérifier

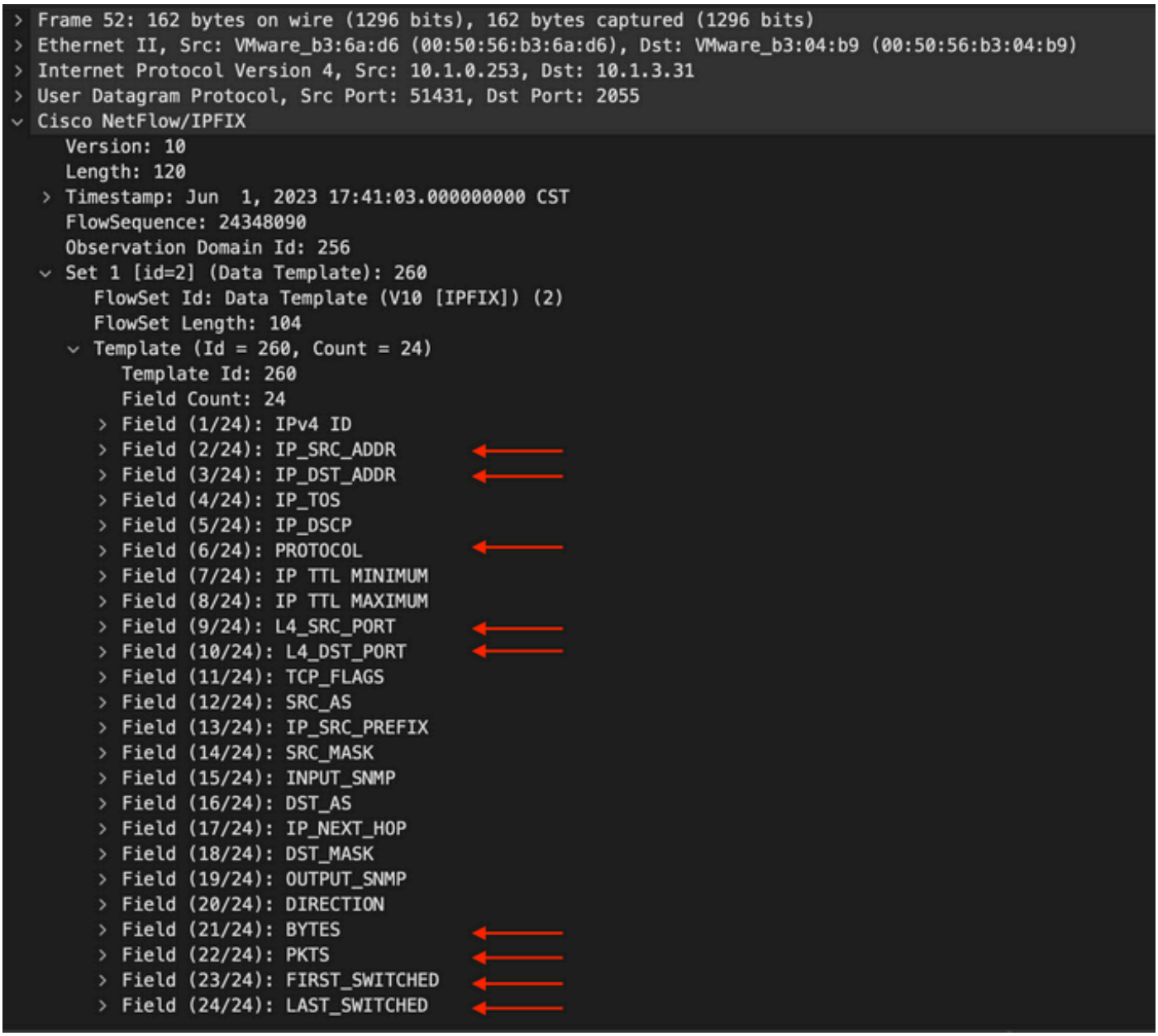
Pour valider la configuration du modèle NetFlow/IPFIX, vous pouvez exécuter une capture de paquets entre l'exportateur et le collecteur de flux. Connectez-vous au collecteur de flux avec l'utilisateur racine via SSH et exécutez la commande :

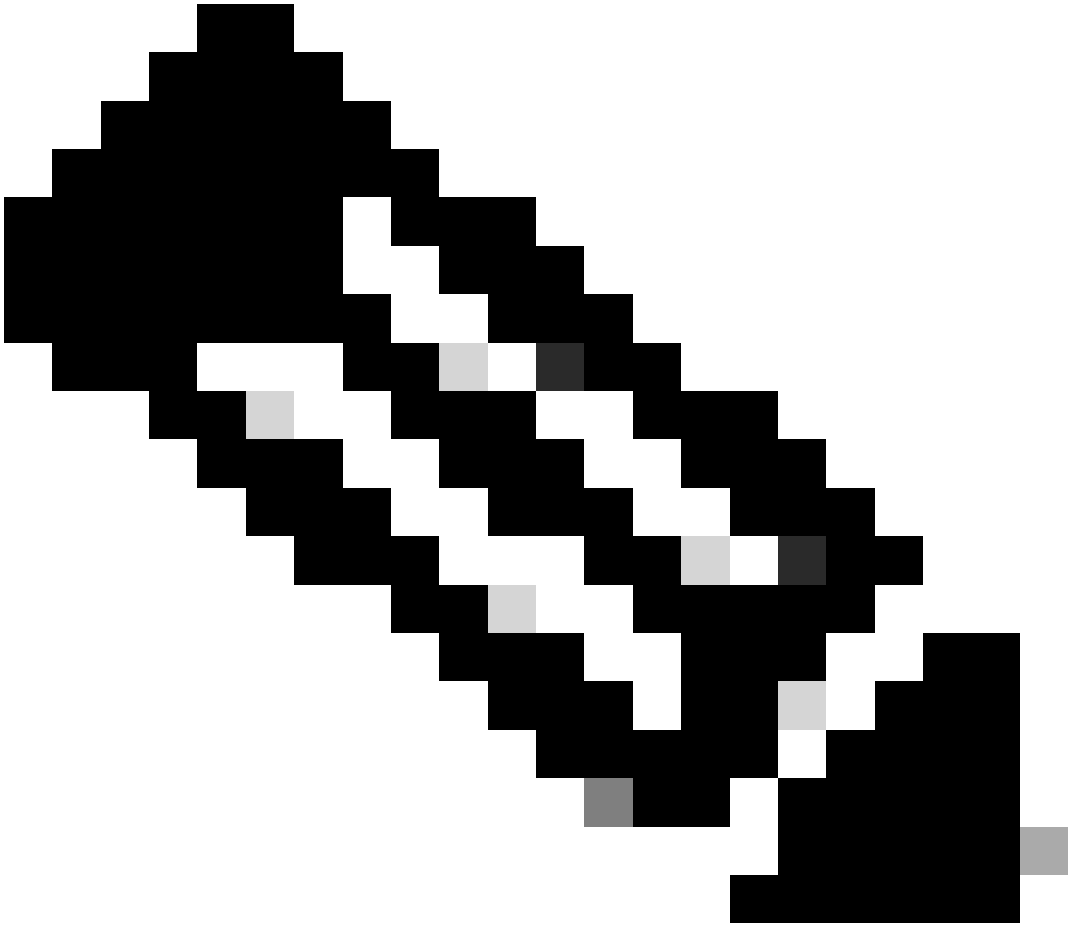
```
tcpdump -nli [Collecting_Interface] host [Exporter_IP_Address] and port [NetFlow_Port] -w /lancope/var/
```

- Utilisez un outil SCP pour exporter la capture de paquets du collecteur de flux (situé dans /lancope/var/tcpdump) vers votre machine locale, puis ouvrez-la sur Wireshark



- Identifiez la trame dans laquelle le modèle NetFlow/IPFIX a été reçu et ouvrez-la pour valider les champs inclus dans le modèle


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:b9)
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
Version: 10
Length: 120
Timestamp: Jun 1, 2023 17:41:03.000000000 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
Field Count: 24
Field (1/24): IPv4 ID
Field (2/24): IP_SRC_ADDR
Field (3/24): IP_DST_ADDR
Field (4/24): IP_TOS
Field (5/24): IP_DSCP
Field (6/24): PROTOCOL
Field (7/24): IP TTL MINIMUM
Field (8/24): IP TTL MAXIMUM
Field (9/24): L4_SRC_PORT
Field (10/24): L4_DST_PORT
Field (11/24): TCP_FLAGS
Field (12/24): SRC_AS
Field (13/24): IP_SRC_PREFIX
Field (14/24): SRC_MASK
Field (15/24): INPUT_SNMP
Field (16/24): DST_AS
Field (17/24): IP_NEXT_HOP
Field (18/24): DST_MASK
Field (19/24): OUTPUT_SNMP
Field (20/24): DIRECTION
Field (21/24): BYTES
Field (22/24): PKTS
Field (23/24): FIRST_SWITCHED
Field (24/24): LAST_SWITCHED



Remarque : les noms de champs affichés peuvent être différents sur chaque exportateur, ce n'est qu'une référence sur la façon dont vous pouvez valider ces champs.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.