Configuration et vérification de Netflow, AVC et ETA sur les commutateurs de la gamme Catalyst 9000

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Informations générales
Diagramme du réseau
Configuration
Composants
Enregistrement de flux
Exportateur De Flux
Moniteur de flux
Échantillonneur de débit (facultatif)
Restrictions
Vérification
vérification indépendante de la plate-forme
vérification dépendante de la plate-forme
Initialisation NetFlow - Table de partition NFL
Moniteur de flux
ACL NetFlow
Masque de flux
Données de déchargement des statistiques de flux et des horodatages
Visibilité et contrôle des applications (AVC)
Informations générales
Performances et évolutivité
Restrictions AVC filaires
Diagramme du réseau
Composants
NBAR2
Vérifier AVC
Analyse du trafic chiffré (ETA)
Informations générales
Diagramme du réseau
Composants
Restrictions
Configuration
Vérification

Introduction

Ce document décrit comment configurer et valider NetFlow, Application Visibility and Control (AVC) et Encrypted Traffic Analytics (ETA).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Netflow
- AVC
- HAP

Components Used

Les informations de ce document sont basées sur un commutateur Catalyst 9300 qui exécute le logiciel Cisco IOS XE 16.12.4.

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.

Produits connexes

Ce document peut également être utilisé avec les versions de matériel et de logiciel suivantes :

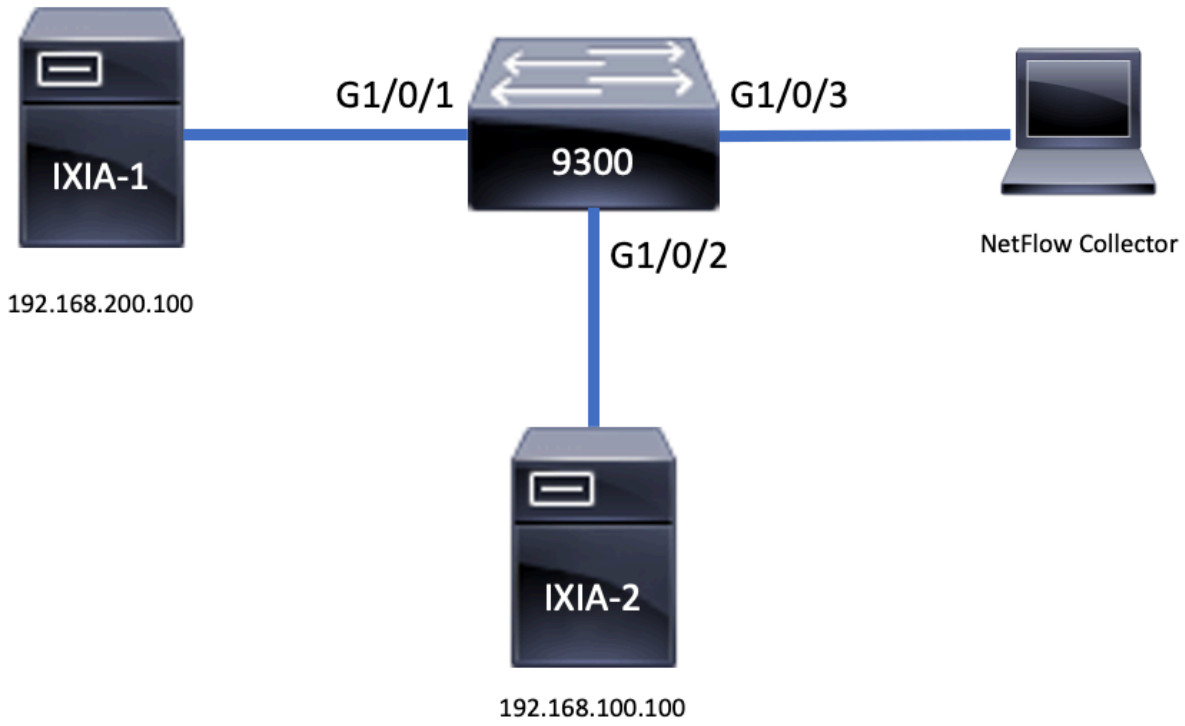
- 9200
- 9400
- 9500
- 9600
- Cisco IOS XE 16.12 et versions ultérieures

Informations générales

- Flexible NetFlow est une technologie de flux de nouvelle génération qui collecte et mesure les données pour permettre à tous les routeurs ou commutateurs du réseau de devenir une source de télémétrie.
- Flexible NetFlow permet des mesures de trafic extrêmement précises et granulaires et une collecte de trafic agrégé de haut niveau.
- Flexible NetFlow utilise des flux pour fournir des statistiques pour la comptabilité, la surveillance du réseau et la planification du réseau.
- Un flux est un flux unidirectionnel de paquets qui arrive sur une interface source et a les mêmes valeurs pour les clés. Une clé est une valeur identifiée pour un champ dans le paquet. Vous créez un flux via un enregistrement de flux pour définir les clés uniques de votre flux.

Note: Les commandes de plate-forme (fed) peuvent varier. La commande peut être "**show platform fed <active|standby>**" ou "**show platform fed switch <active|standby>**". Si la syntaxe notée dans les exemples ne s'analyse pas, essayez la variante.

Diagramme du réseau



Configuration

Composants

La configuration NetFlow se compose de **trois composants principaux** qui peuvent être utilisés ensemble dans plusieurs variantes pour effectuer l'analyse du trafic et l'exportation des données.

Enregistrement de flux

- Un enregistrement est une combinaison de champs clés et non clés. Les enregistrements Flexible NetFlow sont affectés aux moniteurs Flexible NetFlow pour définir le cache utilisé pour le stockage des données de flux.
- Flexible NetFlow inclut plusieurs enregistrements prédéfinis qui peuvent être utilisés pour surveiller le trafic.
- Flexible NetFlow permet également de définir des enregistrements personnalisés pour un cache de surveillance de flux Flexible NetFlow en spécifiant des champs clés et non clés afin de personnaliser la collecte de données selon vos besoins spécifiques.

Comme le montre l'exemple, les détails de configuration des enregistrements de flux :

```
flow record TAC-RECORD-IN
match flow direction
match ipv4 source address
match interface input
match ipv4 destination address
match ipv4 protocol
collect counter packets long
collect counter bytes long
collect timestamp absolute last
collect transport tcp flags

flow record TAC-RECORD-OUT
match flow direction
match interface output
match ipv4 source address
match ipv4 destination address
match ipv4 protocol
collect counter packets long
collect counter bytes long
collect timestamp absolute last
collect transport tcp flags
```

Exportateur De Flux

- Les exportateurs de flux sont utilisés pour exporter les données du cache du moniteur de flux vers un système distant (serveur fonctionnant comme un collecteur NetFlow), à des fins d'analyse et de stockage.
- Des exportateurs de flux sont affectés aux contrôleurs de flux pour fournir une capacité d'exportation de données aux contrôleurs de flux.

Comme indiqué dans l'exemple, les détails de configuration de l'exportateur de flux :

```
flow exporter TAC-EXPORT
destination 192.168.69.2
source Vlan69
```

Moniteur de flux

- Les moniteurs de flux sont le composant Flexible NetFlow qui est appliqué aux interfaces pour effectuer la surveillance du trafic réseau.
- Les données de flux sont collectées à partir du trafic réseau et ajoutées au cache du moniteur de flux pendant l'exécution du processus. Le processus est basé sur les champs clés et non clés de l'enregistrement de flux.

Comme indiqué dans l'exemple, les détails de configuration du moniteur de flux :

```
flow monitor TAC-MONITOR-IN
exporter TAC-EXPORT
record TAC-RECORD-IN

flow monitor TAC-MONITOR-OUT
exporter TAC-EXPORT
record TAC-RECORD-OUT

Switch#show run int g1/0/1
Building configuration...
```

```
Current configuration : 185 bytes
!
interface GigabitEthernet1/0/1
switchport access vlan 42
switchport mode access
ip flow monitor TAC-MONITOR-IN input
ip flow monitor TAC-MONITOR-OUT output
load-interval 30
end
```

Échantillonneur de débit (facultatif)

- Les échantillonneurs de flux sont créés en tant que composants distincts dans la configuration d'un routeur.
- Les échantillonneurs de flux limitent le nombre de paquets sélectionnés pour l'analyse afin de réduire la charge sur le périphérique qui utilise Flexible NetFlow.
- Les échantillonneurs de flux sont utilisés pour réduire la charge sur le périphérique qui utilise Flexible NetFlow, obtenue grâce à la limite du nombre de paquets sélectionnés pour l'analyse.
- Les échantillonneurs de flux échangent la précision pour les performances du routeur. S'il y a une réduction du nombre de paquets qui sont analysés par le moniteur de flux, la précision des informations stockées dans le cache du moniteur de flux peut être affectée.

Comme le montre l'exemple, exemple de configuration d'échantillonneur de flux :

```
sampler SAMPLE-TAC
description Sample at 50%
mode random 1 out-of 2

Switch(config)#interface GigabitEthernet1/0/1
Switch(config-if)#ip flow monitor TAC-MONITOR-IN sampler SAMPLE-TAC input
Switch(config-if)#end
```

Restrictions

- La licence DNA Addon est requise pour Flexible NetFlow complet, sinon Sampled NetFlow est uniquement disponible.
- Les exportateurs de flux ne peuvent pas utiliser le port de gestion comme source.

Cette liste n'est pas exhaustive. Consultez le guide de configuration pour connaître la plate-forme et le code appropriés.

Vérification

vérification indépendante de la plate-forme

Vérifiez la configuration et assurez-vous que les composants NetFlow requis sont présents :

1. **Enregistrement de flux**
2. **Exportateur De Flux**
3. **Moniteur de flux**
4. **Échantillonneur de débit (facultatif)**

   Astuce : Pour afficher l'enregistrement de flux, l'exportateur de flux et le résultat du moniteur de flux en une seule commande, exécutez "**show running-config flow monitor <nom du**

moniteur de flux> expand"

Comme le montre l'exemple, le moniteur de flux est lié à la direction d'entrée et à ses composants associés :

```
Switch#show running-config flow monitor TAC-MONITOR-IN expand
Current configuration:
!
flow record TAC-RECORD-IN
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match interface input
 match flow direction
 collect transport tcp flags
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute last
!
flow exporter TAC-EXPORT
 destination 192.168.69.2
 source Vlan69
!
flow monitor TAC-MONITOR-IN
 exporter TAC-EXPORT
 record TAC-RECORD-IN
!
```

Comme le montre l'exemple, le moniteur de flux est lié à la direction de sortie et à ses composants associés :

```
Switch#show run flow monitor TAC-MONITOR-OUT expand
Current configuration:
!
flow record TAC-RECORD-OUT
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match interface output
 match flow direction
 collect transport tcp flags
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute last
!
flow exporter TAC-EXPORT
 destination 192.168.69.2
 source Vlan69
!
flow monitor TAC-MONITOR-OUT
 exporter TAC-EXPORT
 record TAC-RECORD-OUT
!
```

Exécutez la commande « **show flow monitor <nom du moniteur de flux> » statistics.** Ce résultat est utile pour confirmer que les données sont enregistrées :

```
Switch#show flow monitor TAC-MONITOR-IN statistics
  Cache type:                               Normal (Platform cache)
```

```
  Cache size:                             10000
  Current entries:                            1

  Flows added:                                1
  Flows aged:                                 0
```

Exécutez la commande **"show flow monitor <nom du moniteur de flux> cache** pour confirmer que le cache NetFlow a le résultat suivant :

```
Switch#show flow monitor TAC-MONITOR-IN cache
  Cache type:                           Normal (Platform cache)
  Cache size:                             10000
  Current entries:                            1

  Flows added:                                1
  Flows aged:                                 0

IPV4 SOURCE ADDRESS:       192.168.200.100
IPV4 DESTINATION ADDRESS:  192.168.100.100
INTERFACE INPUT:           Gi1/0/1
FLOW DIRECTION:            Input
IP PROTOCOL:               17
tcp flags:                 0x00
counter bytes long:        4606617470
counter packets long:      25311085
timestamp abs last:        22:44:48.579
```

Exécutez la commande « **show flow exporter <nom de l'exportateur> statistics »** pour confirmer que l'exportateur a envoyé des paquets :

```
Switch#show flow exporter TAC-EXPORT statistics
Flow Exporter TAC-EXPORT:
  Packet send statistics (last cleared 00:08:38 ago):
    Successfully sent:         2                     (24 bytes)

  Client send statistics:
    Client: Flow Monitor TAC-MONITOR-IN
      Records added:           0
      Bytes added:             12
        - sent:                12

    Client: Flow Monitor TAC-MONITOR-OUT
      Records added:           0
      Bytes added:             12
        - sent:                12
```

vérification dépendante de la plate-forme

Initialisation NetFlow - Table de partition NFL

- Les partitions NetFlow sont initialisées pour différentes fonctionnalités avec 16 partitions par direction (entrée/sortie).
- La configuration de la table de partition NetFlow est divisée en allocation de banque globale, qui est subdivisée en banques de flux d'entrée et de sortie.

Champs clés

- Nombre de partitions

- État de partitionnement activé
- Limite de partition
- Utilisation actuelle de la partition

Pour afficher la table de partition NetFlow, vous pouvez exécuter la commande « **show platform software fed switch active|standby|member| fnf sw-table-size asic <numéro de base> shadow 0** »

> **Note**: Les flux créés sont spécifiques au commutateur et au coeur de base lors de leur création. Le numéro de commutateur (actif, en veille, etc.) doit être spécifié en conséquence. Le numéro ASIC entré est lié à l'interface correspondante. Utilisez « **show platform software fed switch active|standby|member ifm mappings »** pour déterminer l'ASIC qui correspond à l'interface. Pour l'option d'ombre, utilisez toujours "0".

```
Switch#show platform software fed switch active fnf sw-table-sizes asic 0 shadow 0

--------------------------------
     Global Bank Allocation
--------------------------------
Ingress Banks : Bank 0 Bank 1
Egress Banks  : Bank 2 Bank 3
--------------------------------
    Global flow table Info                                  <--- Provides the number of entries
used per direction
INGRESS    usedBankEntry           0  usedOvfTcamEntry     0
 EGRESS    usedBankEntry           0  usedOvfTcamEntry     0
--------------------------------
    Flows Statistics
INGRESS    TotalSeen=0 MaxEntries=0 MaxOverflow=0
EGRESS     TotalSeen=0 MaxEntries=0 MaxOverflow=0

--------------------------------
       Partition Table
--------------------------------
## Dir  Limit  CurrFlowCount  OverFlowCount  MonitoringEnabled
 0 ING      0          0               0           0
 1 ING  16640          0               0           1          <-- Current flow count in hardware
 2 ING      0          0               0           0
 3 ING  16640          0               0           0
 4 ING      0          0               0           0
 5 ING   8192          0               0           1
 6 ING      0          0               0           0
 7 ING      0          0               0           0
 8 ING      0          0               0           0
 9 ING      0          0               0           0
10 ING      0          0               0           0
11 ING      0          0               0           0
12 ING      0          0               0           0
13 ING      0          0               0           0
14 ING      0          0               0           0
15 ING      0          0               0           0
 0 EGR      0          0               0           0
 1 EGR  16640          0               0           1          <-- Current flow count in hardware
 2 EGR      0          0               0           0
 3 EGR  16640          0               0           0
 4 EGR      0          0               0           0
 5 EGR   8192          0               0           1
 6 EGR      0          0               0           0
 7 EGR      0          0               0           0
```

```
 8 EGR      0          0              0          0
 9 EGR      0          0              0          0
10 EGR      0          0              0          0
11 EGR      0          0              0          0
12 EGR      0          0              0          0
13 EGR      0          0              0          0
14 EGR      0          0              0          0
15 EGR      0          0              0          0
```

Moniteur de flux

La configuration de Flow Monitor comprend les éléments suivants :

1. Configuration de la liste de contrôle d'accès NetFlow, qui entraîne la création d'une entrée dans la table TCAM de la liste de contrôle d'accès.

L'entrée ACL TCAM se compose des éléments suivants :

- Rechercher les clés correspondantes
- Paramètres de résultat utilisés pour la recherche NetFlow, notamment :
  ID profilID NetFlow

2. Configuration du masque de flux, qui entraîne la création d'une entrée dans NflLookupTable et NflFlowMaskTable.

- Indexé par les paramètres de résultat de la liste de contrôle d'accès NetFlow pour trouver le masque de flux pour la recherche Netflow

ACL NetFlow

Pour afficher la configuration de la liste de contrôle d’accès NetFlow, exécutez la commande « **show platform hardware fed switch active fwd-asic resource tcam table nfl_acl asic <numéro de base>**

> **Astuce** : S'il existe une liste de contrôle d'accès de port (PACL), l'entrée est créée sur l'ASIC auquel l'interface est mappée. Dans le cas d'une liste de contrôle d'accès de routeur (RACL), l'entrée est présente sur tous les ASIC.

- Dans cette sortie, il y a NFCMD0 et NFCMD1, qui sont des valeurs de 4 bits. Afin de calculer l'ID de profil, convertissez les valeurs en binaire.
- Dans cette sortie, NFCMD0 est 1, NFCMD1 est 2. Lors de la conversion en binaire : 000100010
- Dans Cisco IOS-XE 16.12 et versions ultérieures, dans les 8 bits combinés, les 4 premiers bits correspondent à l'ID de profil et le 7 indique que la recherche est activée. Dans l'exemple, **0001**0010, l'ID de profil est 1.
- Dans Cisco IOS XE 16.11 et les versions antérieures du code, dans les 8 bits combinés, les 6 premiers bits correspondent à l'ID de profil et le 7 indique que la recherche est activée. Dans cet exemple, **00010010**, l'ID de profil est donc 4.

```
Switch#show platform hardware fed switch active fwd-asic resource tcam table nfl_acl asic 0
Printing entries for region INGRESS_NFL_ACL_CONTROL (308) type 6 asic 0
=======================================================
Printing entries for region INGRESS_NFL_ACL_GACL (309) type 6 asic 0
=======================================================
Printing entries for region INGRESS_NFL_ACL_PACL (310) type 6 asic 0
=======================================================
TAQ-2 Index-32 (A:0,C:0) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Input IPv4 NFL PACL

Labels  Port   Vlan   L3If   Group
M:      00ff   0000   0000   0000
V:      0001   0000   0000   0000

   vcuResults l3Len l3Pro l3Tos SrcAddr  DstAddr  mtrid vrfid  SH
M:  00000000   0000  00    00  00000000 00000000  00   0000   0000
V:  00000000   0000  00    00  00000000 00000000  00   0000   0000

   RMAC RA MEn IPOPT MF NFF DF SO DPT TM DSEn  l3m
M:  0    0  0    0    0  0   0  0  0   0  0  0
V:  0    0  0    0    0  0   0  0  0   0  0  0

   SrcPort DstPortIITypeCode TCPFlags TTL ISBM QosLabel ReQOS S_P2P D_P2P
M:  0000    0000              00    00    0000    00      0     0     0
V:  0000    0000              00    00    0000    00      0     0     0

   SgEn SgLabel    AuthBehaviorTag  l2srcMiss  l2dstMiss ipTtl SgaclDeny
M:  0    000000    0  0   0 0     0
V:  0    000000    0  0   0 0     0

NFCMD0 NFCMD1 SMPLR LKP1 LKP2 PID QOSPRI MQLBL MPLPRO LUT0PRI CPUCOPY
     1      2     0    1    0   0       0     0       0 0x0000f       0
Start/Skip Word: 0x00000003
Start Feature, Terminate

---------------------------------------
Printing entries for region INGRESS_NFL_ACL_VACL (311) type 6 asic 0
=======================================================
Printing entries for region INGRESS_NFL_ACL_RACL (312) type 6 asic 0
=======================================================
Printing entries for region INGRESS_NFL_ACL_SSID (313) type 6 asic 0
=======================================================
Printing entries for region INGRESS_NFL_CATCHALL (314) type 6 asic 0
=======================================================
TAQ-2 Index-224 (A:0,C:0) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Input IPv4 NFL RACL

Labels  Port   Vlan   L3If   Group
M:      0000   0000   0000   0000
V:      0000   0000   0000   0000

   vcuResults l3Len l3Pro l3Tos SrcAddr  DstAddr  mtrid vrfid  SH
M:  00000000   0000  00    00  00000000 00000000  00   0000   0000
V:  00000000   0000  00    00  00000000 00000000  00   0000   0000

   RMAC RA MEn IPOPT MF NFF DF SO DPT TM DSEn  l3m
M:  0    0  0    0    0  0   0  0  0   0  0  0
V:  0    0  0    0    0  0   0  0  0   0  0  0

   SrcPort DstPortIITypeCode TCPFlags TTL ISBM QosLabel ReQOS S_P2P D_P2P
M:  0000    0000              00    00    0000    00      0     0     0
V:  0000    0000              00    00    0000    00      0     0     0
```

```
   SgEn SgLabel    AuthBehaviorTag  l2srcMiss  l2dstMiss ipTtl SgaclDeny
M:  0    000000    0  0   0 0     0
V:  0    000000    0  0   0 0     0

NFCMD0 NFCMD1 SMPLR LKP1 LKP2 PID QOSPRI MQLBL MPLPRO LUT0PRI CPUCOPY
     0      0     0    0    0   0      0     0      0 0x00000       0
Start/Skip Word: 0x00000003
Start Feature, Terminate

----------------------------------------
TAQ-2 Index-225 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Input IPv4 NFL PACL

Labels  Port   Vlan   L3If   Group
M:      0000   0000   0000   0000
V:      0000   0000   0000   0000

   vcuResults l3Len l3Pro l3Tos SrcAddr  DstAddr  mtrid vrfid  SH
M:  00000000   0000  00    00  00000000 00000000  00   0000   0000
V:  00000000   0000  00    00  00000000 00000000  00   0000   0000

   RMAC RA MEn IPOPT MF NFF DF SO DPT TM DSEn  l3m
M:  0    0  0    0    0  0   0  0  0   0  0  0
V:  0    0  0    0    0  0   0  0  0   0  0  0

   SrcPort DstPortIITypeCode TCPFlags TTL ISBM QosLabel ReQOS S_P2P D_P2P
M:  0000    0000              00    00    0000    00      0     0     0
V:  0000    0000              00    00    0000    00      0     0     0

   SgEn SgLabel    AuthBehaviorTag  l2srcMiss  l2dstMiss ipTtl SgaclDeny
M:  0    000000    0  0   0 0     0
V:  0    000000    0  0   0 0     0

NFCMD0 NFCMD1 SMPLR LKP1 LKP2 PID QOSPRI MQLBL MPLPRO LUT0PRI CPUCOPY
     0      0     0    0    0   0      0     0      0 0x00000       0
Start/Skip Word: 0x00000000
No Start, Terminate

----------------------------------------
TAQ-2 Index-226 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Input IPv6 NFL PACL

Labels  Port   Vlan   L3If   Group
Mask    0x0000 0x0000 0x0000 0x0000
Value   0x0000 0x0000 0x0000 0x0000

vcuResult dstAddr0 dstAddr1 dstAddr2 dstAddr3 srcAddr0
00000000  00000000 00000000 00000000 00000000 00000000
00000000  00000000 00000000 00000000 00000000 00000000

srcAddr1 srcAddr2 srcAddr3 TC HL l3Len fLabel vrfId toUs
00000000 00000000 00000000 00 00  0000  00000  000   0
00000000 00000000 00000000 00 00  0000  00000  000   0

l3Pro mtrId AE FE RE HE MF NFF SO IPOPT RA MEn RMAC DPT TMP l3m
 00    00   0  0  0  0  0   0  0    0   0   0   0    0   0    0
 00    00   0  0  0  0  0   0  0    0   0   0   0    0   0    0

DSE srcPort dstPortIITypeCode tcpFlags IIPresent cZId dstZId
 0   0000    0000      00      00     00     00
 0   0000    0000      00      00     00     00

v6RT AH ESP mREn ReQOS QosLabel PRole VRole  AuthBehaviorTag
```

```
M: 0   0   0    0    0      00         0     0 0
V: 0   0   0    0    0      00         0     0 0

   SgEn SgLabel
M:  0    000000
V:  0    000000

NFCMD0 NFCMD1 SMPLR LKP1 LKP2 PID QOSPRI MQLBL MPLPRO LUT0PRI CPUCOPY
     0      0     0    0    0   0      0     0      0 0x00000       0
Start/Skip Word: 0x00000000
No Start, Terminate

----------------------------------------
TAQ-2 Index-228 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
conversion to string vmr l2p not supported
----------------------------------------
TAQ-2 Index-230 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Input MAC NFL PACL

Labels  Port   Vlan   L3If   Group
M:      0000   0000   0000   0000
V:      0000   0000   0000   0000

   arpSrcHwAddr  arpDestHwAddr  arpSrcIpAddr  arpTargetIp  arpOperation
M: 000000000000  000000000000   00000000       00000000     0000
V: 000000000000  000000000000   00000000       00000000     0000


   TRUST  SNOOP  SVALID  DVALID
M:    0     0      0      0
V:    0     0      0      0


   arpHardwareLength  arpHardwareType  arpProtocolLength  arpProtocolType
M:   00000000          00000000            00000000          00000000
V:   00000000          00000000            00000000          00000000


   VlanId l2Encap l2Protocol cosCFI   srcMAC      dstMAC    ISBM  QosLabel
M:  000    0        0000     0     000000000000 000000000000 00     00
V:  000    0        0000     0     000000000000 000000000000 00     00


  ReQOS isSnap  isLLC  AuthBehaviorTag
M:  0     0      0       0
V:  0     0      0        0

NFCMD0 NFCMD1 SMPLR LKP1 LKP2 PID QOSPRI MQLBL MPLPRO LUT0PRI CPUCOPY
     0      0     0    0    0   0      0     0      0 0x00000       0
Start/Skip Word: 0x00000000
No Start, Terminate

----------------------------------------
```

Masque de flux

Exécutez la commande « **show platform software fed switch active|standby|member fnf fmask-entry asic <numéro de base> entry 1 »** pour vérifier que le masque de flux est installé dans le matériel. Le nombre de champs clés est également indiqué ici.

```
Switch#show platform software fed switch active fnf fmask-entry asic 1 entry 1
```

```
--------------------------------
mask0_valid : 1
Mask hdl0   : 1
Profile ID  : 0
Feature 0   : 148
Fmsk0 RefCnt: 1
Mask M1     :
[511:256] => :00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
[255:000] => :FFFFFFFF 00000000 FFFFFFFF 03FF0000 00000000 00FF0000 00000000 C00000FF

Mask M2     :

Key Map     :

Source   Field-Id   Size   NumPFields   Pfields
 002       090       04        01       (0 1 1 1)
 002       091       04        01       (0 1 1 0)
 002       000       01        01       (0 1 0 7)
 000       056       08        01       (0 0 2 4)
 001       011       11        04       (0 0 0 1) (0 0 0 0) (0 1 0 6) (0 0 2 0)
 000       067       32        01       (0 1 12 0)
 000       068       32        01       (0 1 12 2)
```

Données de déchargement des statistiques de flux et des horodatages

Exécutez la commande "**show platform software fed switch active fnf flow-record asic <numéro de base> start-index <numéro d'index> num-flows <nombre de flux>** pour afficher les statistiques netflow ainsi que les horodatages

```
Switch#show platform software fed switch active fnf flow-record asic 1 start-index 1 num-flows 1
1 flows starting at 1 for asic 1:--------------------------------------------------
Idx 996 :
{90, ALR_INGRESS_NET_FLOW_ACL_LOOKUP_TYPE1 = 0x01}
{91, ALR_INGRESS_NET_FLOW_ACL_LOOKUP_TYPE2 = 0x01}
{0, ALR_INGRESS_NFL_SPECIAL1 = 0x00}
{56, PHF_INGRESS_L3_PROTOCOL = 0x11}
{11 PAD-UNK = 0x0000}
{67, PHF_INGRESS_IPV4_DEST_ADDRESS = 0xc0a86464}
{68, PHF_INGRESS_IPV4_SRC_ADDRESS = 0xc0a8c864}
FirstSeen = 0x4b2f, LastSeen = 0x4c59, sysUptime = 0x4c9d
PKT Count = 0x000000000102d5df, L2ByteCount = 0x00000000ca371638
```

```
Switch#show platform software fed switch active fnf flow-record asic 1 start-index 1 num-flows 1
1 flows starting at 1 for asic 1:--------------------------------------------------
Idx 996 :
{90, ALR_INGRESS_NET_FLOW_ACL_LOOKUP_TYPE1 = 0x01}
{91, ALR_INGRESS_NET_FLOW_ACL_LOOKUP_TYPE2 = 0x01}
{0, ALR_INGRESS_NFL_SPECIAL1 = 0x00}
{56, PHF_INGRESS_L3_PROTOCOL = 0x11}
{11 PAD-UNK = 0x0000}
{67, PHF_INGRESS_IPV4_DEST_ADDRESS = 0xc0a86464}
{68, PHF_INGRESS_IPV4_SRC_ADDRESS = 0xc0a8c864}
FirstSeen = 0x4b2f, LastSeen = 0x4c5b, sysUptime = 0x4c9f
PKT Count = 0x0000000001050682, L2ByteCount = 0x00000000cbed1590
```

Visibilité et contrôle des applications (AVC)

Informations générales

- Application Visibility and Control (AVC) est une solution qui tire parti de Network-Based Recognition Version 2 (**NBAR2**), de **NetFlow V9**, et de divers outils de rapport et de gestion (**Cisco Prime**) pour aider à classer les applications via Deep Packet Inspection (DPI).
- AVC peut être configuré sur des ports d'accès câblés pour des commutateurs autonomes ou des piles de commutateurs.
- AVC peut également être utilisé sur les contrôleurs sans fil Cisco pour identifier les applications en fonction de la DPI, puis les marquer avec une valeur DSCP spécifique. Il peut également collecter diverses mesures de performances sans fil, telles que l'utilisation de la bande passante en termes d'applications et de clients.

Performances et évolutivité

Performances : chaque membre du commutateur est capable de gérer 500 connexions par seconde (CPS) à moins de 50 % d'utilisation du processeur. Au-delà de ce tarif, le service AVC n'est pas garanti.

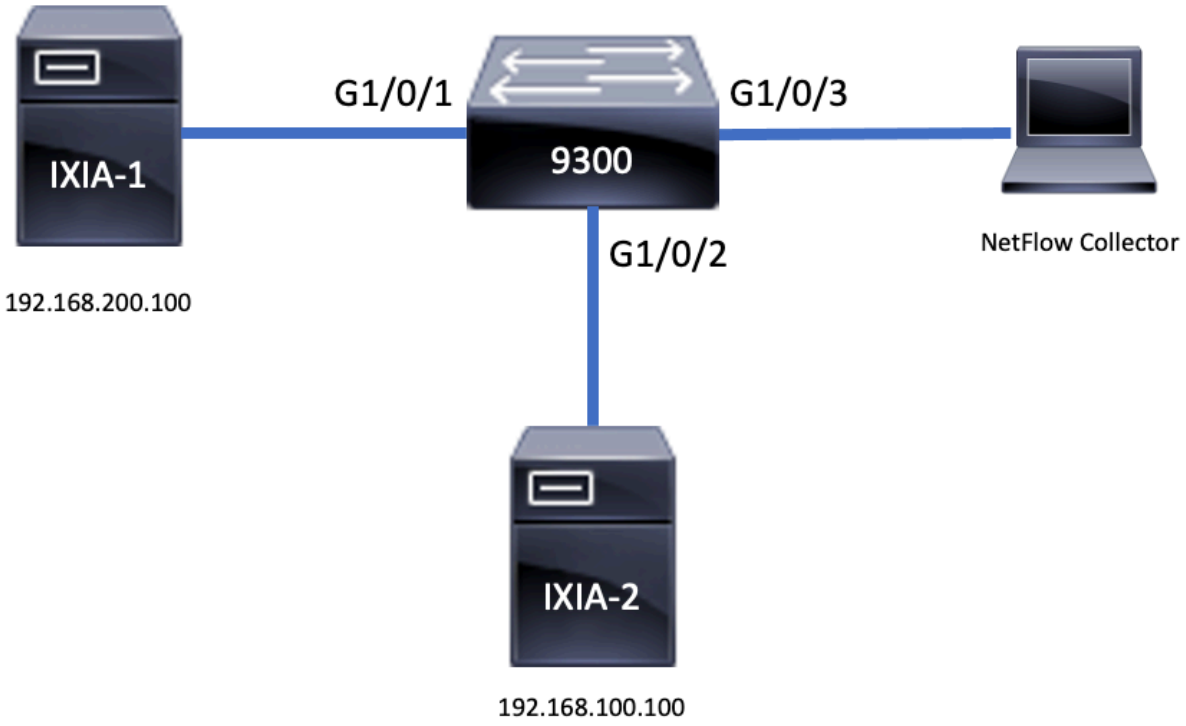
Évolutivité : possibilité de gérer jusqu'à 5 000 flux bidirectionnels par 24 ports d'accès (environ 200 flux par port d'accès).

Restrictions AVC filaires

- AVC et ETA (Encrypted Traffic Analytics) ne peuvent pas être configurés simultanément sur la même interface.
- La classification des paquets est uniquement prise en charge pour le trafic IPv4 monodiffusion (TCP/UDP).
- La configuration de stratégie QoS basée sur NBAR est uniquement prise en charge sur les ports physiques filaires. Cela inclut les ports d'accès et d'agrégation de couche 2 et les ports routés de couche 3.
- La configuration de la stratégie QoS basée sur NBAR n'est pas prise en charge sur les membres port-channel, les interfaces SVI (Switch Virtual Interfaces) ou les sous-interfaces.
- Les classificateurs basés sur NBAR2 **(protocole de correspondance),** prennent uniquement en charge les actions QoS de marquage et de réglementation.
- Le « protocole de correspondance » est limité à 255 protocoles différents dans toutes les stratégies (limitation matérielle de 8 bits)

> **Note**: Il ne s'agit pas d'une liste exhaustive de toutes les restrictions, consultez le guide de configuration AVC approprié pour votre plate-forme et votre version de code.

Diagramme du réseau



Composants

La configuration AVC se compose de **trois** composants **principaux** qui constituent la solution :

Visibilité : Détection de protocole

- La découverte de protocoles est effectuée par le biais de NBAR, qui fournit des statistiques par interface, direction et octets/paquets d'application.
- La détection de protocole est activée pour une interface spécifique via la configuration d'interface : **ip nbar protocol-discovery**

Comme indiqué dans le résultat, comment activer la détection de protocole :

```
Switch(config)#interface fi4/0/5
Switch(config-if)#ip nbar protocol-discovery
Switch(config-if)#exit

Switch#show run int fi4/0/5
Building configuration...

Current configuration : 70 bytes
!
interface FiveGigabitEthernet4/0/5
ip nbar protocol-discovery
end
```

Contrôle : QoS basée sur les applications

Par rapport à la QoS traditionnelle, qui correspond à l'adresse IP et au port UDP/TCP, AVC offre un contrôle plus précis grâce à la QoS basée sur les applications, qui vous permet de faire correspondre une application, et fournit un contrôle plus granulaire grâce à des actions de QoS telles que le marquage et la réglementation.

- Les actions sont effectuées sur le trafic agrégé (pas par flux)
- La qualité de service basée sur les applications est obtenue par la création d'une carte de classe, d'une correspondance de protocole, puis d'une carte de stratégie.
- La stratégie QoS basée sur les applications est associée à une interface.

Comme indiqué dans le résultat, exemple de configuration pour la QoS basée sur les applications :

```
Switch(config)#class-map WEBEX
Switch(config-cmap)#match protocol webex-media
Switch(config)#end

Switch(config)#policy-map WEBEX
Switch(config-pmap)#class WEBEX
Switch(config-pmap-c)#set dscp af41
Switch(config)#end

Switch(config)#interface fi4/0/5
Switch(config-if)#service-policy input WEBEX
Switch(config)#end

Switch#show run int fi4/0/5
Building configuration...

Current configuration : 98 bytes
!
interface FiveGigabitEthernet4/0/5
service-policy input WEBEX
ip nbar protocol-discovery
end
```

Flexible NetFlow basé sur les applications

La fonction FNF AVC filaire prend en charge deux types d'enregistrements de flux prédéfinis : **les anciens enregistrements de flux bidirectionnels** et les nouveaux **enregistrements de flux directionnels**.

Les enregistrements de flux bidirectionnels permettent de suivre les statistiques des applications client/serveur.

Comme le montre le résultat, exemple de configuration d'un enregistrement de flux bidirectionnel.

```
Switch(config)#flow record BIDIR-1
Switch(config-flow-record)#match ipv4 version
Switch(config-flow-record)#match ipv4 protocol
Switch(config-flow-record)#match application name
Switch(config-flow-record)#match connection client ipv4 address
Switch(config-flow-record)#match connection server ipv4 address
Switch(config-flow-record)#match connection server transport port
Switch(config-flow-record)#match flow observation point
Switch(config-flow-record)#collect flow direction
Switch(config-flow-record)#collect connection initiator
Switch(config-flow-record)#collect connection new-connections
Switch(config-flow-record)#collect connection client counter packets long
Switch(config-flow-record)#connection client counter bytes network long
Switch(config-flow-record)#collect connection server counter packets long
Switch(config-flow-record)#connection server counter bytes network long
Switch(config-flow-record)#collect timestamp absolute first
Switch(config-flow-record)#collect timestamp absolute last
```

```
Switch(config-flow-record)#end

Switch#show flow record BIDIR-1
flow record BIDIR-1:
Description: User defined
No. of users: 0
Total field space: 78 bytes
Fields:
match ipv4 version
match ipv4 protocol
match application name
match connection client ipv4 address
match connection server ipv4 address
match connection server transport port
match flow observation point
collect flow direction
collect timestamp absolute first
collect timestamp absolute last
collect connection initiator
collect connection new-connections
collect connection server counter packets long
collect connection client counter packets long
collect connection server counter bytes network long
collect connection client counter bytes network long
```

Les enregistrements directionnels sont des statistiques d'application pour les entrées/sorties.

Comme le montre le résultat, exemples de configuration des enregistrements directionnels d'entrée et de sortie :

> **Remarque** : la commande "**match interface input**" spécifie une correspondance avec l'interface d'entrée. La commande "**match interface output**" spécifie une correspondance avec l'interface de sortie. La commande « **match application name** » est obligatoire pour la prise en charge d'AVC.

```
Switch(config)#flow record APP-IN
Switch(config-flow-record)#match ipv4 version
Switch(config-flow-record)#match ipv4 protocol
Switch(config-flow-record)#match ipv4 source address
Switch(config-flow-record)#match ipv4 destination address
Switch(config-flow-record)#match transport source-port
Switch(config-flow-record)#match transport destination-port
Switch(config-flow-record)#match interface input
Switch(config-flow-record)#match application name
Switch(config-flow-record)#collect interface output
Switch(config-flow-record)#collect counter bytes long
Switch(config-flow-record)#collect counter packets long
Switch(config-flow-record)#collect timestamp absolute first
Switch(config-flow-record)#collect timestamp absolute last
Switch(config-flow-record)#end

Switch#show flow record APP-IN
flow record APP-IN:
Description: User defined
No. of users: 0
Total field space: 58 bytes
Fields:
match ipv4 version
match ipv4 protocol
match ipv4 source address
```

```
match ipv4 destination address
match transport source-port
match transport destination-port
match interface input
match application name
collect interface output
collect counter bytes long
collect counter packets long
collect timestamp absolute first
collect timestamp absolute last

Switch(config)#flow record APP-OUT
Switch(config-flow-record)#match ipv4 version
Switch(config-flow-record)#match ipv4 protocol
Switch(config-flow-record)#match ipv4 source address
Switch(config-flow-record)#match ipv4 destination address
Switch(config-flow-record)#match transport source-port
Switch(config-flow-record)#match transport destination-port
Switch(config-flow-record)#match interface output
Switch(config-flow-record)#match application name
Switch(config-flow-record)#collect interface input
Switch(config-flow-record)#collect counter bytes long
Switch(config-flow-record)#collect counter packets long
Switch(config-flow-record)#collect timestamp absolute first
Switch(config-flow-record)#collect timestamp absolute last
Switch(config-flow-record)#end

Switch#show flow record APP-OUT
flow record APP-OUT:
Description: User defined
No. of users: 0
Total field space: 58 bytes
Fields:
match ipv4 version
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match interface output
match application name
collect interface input
collect counter bytes long
collect counter packets long
collect timestamp absolute first
collect timestamp absolute last
```

Exportateur De Flux

Créez un exportateur de flux pour définir les paramètres d'exportation.

Comme indiqué dans le résultat, exemple de configuration de l'exportateur de flux :

```
Switch(config)#flow exporter AVC
Switch(config-flow-exporter)#destination 192.168.69.2
Switch(config-flow-exporter)#source vlan69
Switch(config-flow-exporter)#end

Switch#show run flow exporter AVC
Current configuration:
!
```

```
flow exporter AVC
destination 192.168.69.2
source Vlan69
!
```

Moniteur de flux

Créez un moniteur de flux pour l'associer à un enregistrement de flux.

Comme indiqué dans le résultat, exemple de configuration du moniteur de flux :

```
Switch(config)#flow monitor AVC-MONITOR
Switch(config-flow-monitor)#record APP-OUT
Switch(config-flow-monitor)#exporter AVC
Switch(config-flow-monitor)#end

Switch#show run flow monitor AVC-MONITOR
Current configuration:
!
flow monitor AVC-MONITOR
exporter AVC
record APP-OUT
```

Associer Flow Monitor à une interface

Vous pouvez connecter simultanément à une interface deux moniteurs AVC différents avec des enregistrements prédéfinis différents.

Comme indiqué dans le résultat, exemple de configuration du moniteur de flux :

```
Switch(config)#interface fi4/0/5
Switch(config-if)#ip flow monitor AVC-MONITOR out
Switch(config-if)#end

Switch#show run interface fi4/0/5
Building configuration...
Current configuration : 134 bytes
!
interface FiveGigabitEthernet4/0/5
ip flow monitor AVC-MONITOR output
service-policy input WEBEX
ip nbar protocol-discovery
end
```

NBAR2

Mise à niveau NBAR2 Dynamic Hitless Protocol Pack

Les packs de protocoles sont des packages logiciels qui mettent à jour la prise en charge du protocole NBAR2 sur un périphérique sans remplacer le logiciel Cisco sur le périphérique. Un pack de protocoles contient des informations sur les applications officiellement prises en charge par NBAR2 qui sont compilées et compressées ensemble. Pour chaque application, le pack de protocoles inclut des informations sur les signatures et les attributs d'application. Chaque version logicielle est accompagnée d'un pack de protocoles intégré.

- NBAR2 permet de mettre à jour le paquet de protocole sans interruption de trafic ou de service et sans avoir à modifier l'image logicielle sur le ou les périphériques

- Les paquets de protocole NBAR2 peuvent être téléchargés sur Cisco Software Center à l'adresse suivante : https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

Mise à niveau du pack de protocoles NBAR2

Avant d'installer un nouveau pack de protocoles, vous devez copier le paquet de protocoles dans la mémoire flash de tous les commutateurs. Pour charger le nouveau pack de protocoles, utilisez la commande "**ip nbar protocol-pack flash:<Nom du pack>**

Vous n'avez pas besoin de recharger les commutateurs pour que la mise à niveau NBAR2 se produise.

Comme indiqué dans le résultat, exemple de configuration du chargement du pack de protocoles NBAR2 :

```
Switch(config)#ip nbar protocol-pack flash:newProtocolPack
```

Pour revenir au pack de protocoles intégré, utilisez la commande « **default ip nbar protocol-pack »**

Comme indiqué dans le résultat, exemple de configuration de la façon de revenir au pack de protocole intégré :

```
Switch(config)#default ip nbar protocol-pack
```

Afficher les informations du pack de protocoles NBAR2

Pour afficher les informations du pack de protocoles, utilisez les commandes suivantes :

- **show ip nbar version**
- **show ip nbar protocol-pack active detail**

Comme le montre le résultat, exemple de résultat de ces commandes :

```
Switch#show ip nbar version
NBAR software version: 37
NBAR minimum backward compatible version: 37
NBAR change ID: 293126

Loaded Protocol Pack(s):
Name: Advanced Protocol Pack
Version: 43.0
Publisher: Cisco Systems Inc.
NBAR Engine Version: 37
State: Active

Switch#show ip nbar protocol-pack active detail
Active Protocol Pack:
Name: Advanced Protocol Pack
Version: 43.0
Publisher: Cisco Systems Inc.
NBAR Engine Version: 37
State: Active
```

Applications personnalisées NBAR2

NBAR2 prend en charge l'utilisation de protocoles personnalisés pour identifier les applications

personnalisées. Les protocoles personnalisés prennent en charge des protocoles et des applications que NBAR2 ne prend pas actuellement en charge.

Il peut s'agir des éléments suivants :

- Application spécifique à une organisation
- Applications spécifiques à une zone géographique

NBAR2 permet de personnaliser manuellement les applications à l'aide de la commande **ip nbar custom<*myappname*>**.

Note: Les applications personnalisées ont priorité sur les protocoles intégrés

Il existe différents types de personnalisation des applications :

Personnalisation de protocole générique

- HTTP
- SSL
- DNS

Composite : personnalisation basée sur plusieurs protocoles -**nom-serveur**

Personnalisation de couche 3/couche 4

- Adresse IPv4
- Valeurs DSCP
- Ports TCP/UDP
- Direction source ou de destination du flux

Décalage d'octet : personnalisation basée sur des valeurs d'octet spécifiques dans la charge utile

Personnalisation HTTP

La personnalisation HTTP peut être basée sur une combinaison de champs HTTP provenant de :

- **cookie** - Cookie HTTP
- **host** : nom d'hôte du serveur d'origine contenant la ressource
- **method** - méthode HTTP
- **referrer** - Adresse à laquelle la demande de ressource a été obtenue
- **url** - Chemin d'accès Uniform Resource Locator
- **user-agent** - Logiciel utilisé par l'agent qui envoie la requête
- **version** - version HTTP
- **via** - Champ HTTP via

Exemple d'application personnalisée appelée MYHTTP qui utilise l'hôte HTTP « *mondomaine.com » avec l'ID de sélecteur 10.

```
Switch(config)#ip nbar custom MYHTTP http host *mydomain.com id 10
```

Personnalisation SSL

La personnalisation peut être effectuée pour le trafic chiffré SSL via des informations extraites de l'indication de nom de serveur SSL (SNI) ou du nom commun (CN).

Exemple d'application personnalisée appelée MYSSL qui utilise le nom unique SSL « mondomaine.com » avec l'ID de sélecteur 11.

```
Switch(config)#ip nbar custom MYSSL ssl unique-name *mydomain.com id 11
```

Personnalisation DNS

NBAR2 examine le trafic de requête et de réponse DNS et peut corréler la réponse DNS à une application. L'adresse IP renvoyée par la réponse DNS est mise en cache et utilisée pour les flux de paquets ultérieurs associés à cette application spécifique.

Le commandip nbar *customapplication-namednsdomain-nameidapplication-*id est utilisé pour la personnalisation DNS. Pour étendre une application, utilisez commandip nbar customapplication-namends domain-*namedomain-nameextendsexisting-application*.

Exemple d'application personnalisée appelée MYDNS qui utilise le nom de domaine DNS « mydomain.com » avec l'ID de sélecteur 12.

```
Switch(config)#ip nbar custom MYDNS dns domain-name *mydomain.com id 12
```

Personnalisation composite

NBAR2 permet de personnaliser les applications en fonction des noms de domaine apparaissant dans HTTP, SSL ou DNS.

Exemple d'application personnalisée appelée MYDOMAIN qui utilise le nom de domaine HTTP, SSL ou DNS « mondomaine.com » avec l'ID de sélecteur 13.

```
Switch(config)#ip nbar custom MYDOMAIN composite server-name *mydomain.com id 13
```

Personnalisation C3/C4

La personnalisation de couche 3/couche 4 est basée sur le tuple de paquets et est toujours associée au premier paquet d'un flux.

Exemple d'application personnalisée LAYER4CUSTOM qui correspond aux adresses IP 10.56.1.10 et 10.56.1.11, TCP et DSCP ef avec l'ID de sélecteur 14.

```
Switch(config)#ip nbar custom LAYER4CUSTOM transport tcp id 14
Switch(config-custom)#ip address 10.56.1.10 10.56.1.11
Switch(config-custom)#dscp ef
Switch(config-custom)#end
```

Surveiller les applications personnalisées

Pour surveiller les applications personnalisées, utilisez les commandes show répertoriées :

show ip nbar protocol-id | inc Personnalisé

```
Switch#show ip nbar protocol-id | inc Custom
LAYER4CUSTOM             14            Custom
MYDNS                    12            Custom
MYDOMAIN                 13            Custom
MYHTTP                   10            Custom
MYSSL                    11            Custom
```

show ip nbar protocol-id CUSTOM_APP

```
Switch#show ip nbar protocol-id MYSSL
Protocol Name             id            type
-------------------------------------------
MYSSL                    11            Custom
```

Vérifier AVC

La validation de la fonctionnalité d'AVC s'effectue en plusieurs étapes. Cette section fournit des commandes et des exemples de résultats.

Pour valider que NBAR est actif, vous pouvez exécuter la commande "**show ip nbar control-plane"**

Domaines clés :

- L'état NBAR doit être **activé** dans un scénario correct
- L'état de configuration NBAR doit être **prêt** dans un scénario correct

```
Switch#show ip nbar control-plane
NGCP Status:
============

graph sender info:
NBAR state is ACTIVATED
NBAR config send mode is ASYNC
NBAR config state is READY

NBAR update ID 3
NBAR batch ID ACK 3
NBAR last batch ID ACK clients 1 (ID: 4)
Active clients 1 (ID: 4)
NBAR max protocol ID ever 1935
NBAR Control-Plane Version: 37

<snip>
```

Vérifiez que chaque membre du commutateur possède un plan de données actif à l'aide de la commande **show platform software fed switch active|standby|member wdavc function wdavc_stile_cp_show_info_ui** :

Si DP activé doit être **TRUE** dans un scénario correct

```
Switch#show platform software fed switch active wdavc function wdavc_stile_cp_show_info_ui

Is DP activated : TRUE
MSG ID : 3
Maximum number of flows: 262144
Current number of graphs: 1
```

```
Requests queue state : WDAVC_STILE_REQ_QUEUE_STATE_UP
Number of requests in queue : 0
Max number of requests in queue (TBD): 1
Counters:
activate_msgs_rcvd : 1
graph_download_begin_msgs_rcvd : 3
stile_config_msgs_rcvd : 1584
graph_download_end_msgs_rcvd : 3
deactivate_msgs_rcvd : 0
intf_proto_disc_msgs_rcvd : 1
intf_attach_msgs_rcvd : 2
cfg_response_msgs_sent : 1593
num_of_handle_msg_from_fmanfp_events : 1594
num_of_handle_request_from_queue : 1594
num_of_handle_process_requests_events : 1594
```

Utilisez la commande « **show platform software fed switch active|standby|member wdavc flows** to display key information :

```
Switch#show platform software fed switch active wdavc flows

CurrFlows=1, Watermark=1

IX |IP1 |IP2 |PORT1|PORT2|L3 |L4 |VRF |TIMEOUT|APP |TUPLE|FLOW |IS FIF |BYPASS|FINAL |#PKTS
|BYPASS
  | | | | |PROTO|PROTO|VLAN|SEC |NAME |TYPE |TYPE |SWAPPED | | | |PKT
-------------------------------------------------------------------------------------
1 |192.168.100.2 |192.168.200.2 |68 |67 |1 |17 |0 |360 |unknown |Full |Real Flow|Yes |True |True
|40 |40
```

Champs clés :

CurrFlows : illustre le nombre de flux actifs suivis par AVC

Filigrane : Démontre le plus grand nombre de flux historiquement suivis par AVC

DÉLAI SEC : Délai d'inactivité basé sur l'application identifiée

NOM DE L'APPLICATION : Application identifiée

TYPE DE FLUX : Real Flow indique que ce flux a été créé à la suite de données entrantes. Pre Flow indique que ce flux est créé à la suite de données entrantes. Les pré-flux sont utilisés pour les flux de médias anticipés

TYPE DE TUPLE : Les flux réels sont toujours des tuples complets, les pré-flux sont des tuples complets ou des demi-tuples

CONTOURNER : Si la valeur est TRUE, indique qu'aucun paquet supplémentaire n'est requis par le logiciel pour identifier ce flux

FINAL : Si la valeur est TRUE, indique que l'application ne change plus pour ce flux

CONTOURNER PKT : Combien de paquets étaient nécessaires pour parvenir à la classification finale ?

#PKTS : Combien de paquets ont été réellement envoyés au logiciel pour ce flux ?

Pour afficher des détails supplémentaires sur les flux actuels, vous pouvez utiliser la commande **"show platform software fed switch active wdavc function wdavc_ft_show_all_flows_seg_ui"**

```
Switch#show platform software fed switch active wdavc function wdavc_ft_show_all_flows_seg_ui
CurrFlows=1, Watermark=1

IX |IP1 |IP2 |PORT1|PORT2|L3 |L4 |VRF |TIMEOUT|APP |TUPLE |FLOW |IS FIF |BYPASS|FINAL |#PKTS
|BYPASS
| | | | |PROTO|PROTO|VLAN|SEC |NAME |TYPE |TYPE |SWAPPED | | | |PKT
-----------------------------------------------------------------------------------------------
-----------------------------------------------------------------
1 |192.168.100.2 |192.168.200.2|68 |67 |1 |17 |0 |360 |unknown |Full |Real Flow|Yes |True |True
|40 |40

SEG IDX |I/F ID |OPST I/F |SEG DIR |FIF DIR |Is SET |DOP ID |NFL HDL |BPS PND |APP PND |FRST TS
|LAST TS |BYTES |PKTS |TCP FLGS
-----------------------------------------------------------------------------------------------
-----------------------------------
0 |9 |---- |Ingress |True |True |0 |50331823 |0 |0 |177403000|191422000|24252524|70094 |0
```

Champs clés

ID E/F : Spécifie l'ID d'interface

SEG DIR : spécifie la direction d'entrée de sortie

FIF DIR : détermine s'il s'agit ou non de la direction de l'initiateur de flux

NFL HDL : ID de flux dans le matériel

Pour afficher l'entrée dans le matériel, exécutez la commande « **show platform software fed switch active fnf flow-record asic <number> start-index <number> num-flows <number of flows>**

> **Note**: Pour choisir l'ASIC, il s'agit de l'instance ASIC à laquelle le port est mappé. Pour identifier l'ASIC, utilisez la commande **"show platform software fed switch active|standby|member ifm mappings"** L'index de démarrage peut être défini sur "0" si vous n'êtes pas intéressé par un flux spécifique. Sinon, l'index de début doit être spécifié. Pour les flux num, qui spécifie le nombre de flux pouvant être visualisés, 10 maximum.

```
Switch#show platform software fed switch active fnf flow-record asic 3 start-index 0 num-flows 1
1 flows starting at 0 for asic 3:-----------------------------------------------
Idx 175 :
{90, ALR_INGRESS_NET_FLOW_ACL_LOOKUP_TYPE1 = 0x01}
{91, ALR_INGRESS_NET_FLOW_ACL_LOOKUP_TYPE2 = 0x01}
{0, ALR_INGRESS_NFL_SPECIAL1 = 0x00}
{11 PAD-UNK = 0x0000}
{94, PHF_INGRESS_DEST_PORT_OR_ICMP_OR_IGMP_OR_PIM_FIRST16B = 0x0043}
{93, PHF_INGRESS_SRC_PORT = 0x0044}
{67, PHF_INGRESS_IPV4_DEST_ADDRESS = 0xc0a8c802}
{68, PHF_INGRESS_IPV4_SRC_ADDRESS = 0xc0a86402}
{56, PHF_INGRESS_L3_PROTOCOL = 0x11}
FirstSeen = 0x2b4fb, LastSeen = 0x2eede, sysUptime = 0x2ef1c
PKT Count = 0x000000000001216f, L2ByteCount = 0x0000000001873006
```

Recherchez diverses erreurs et avertissements dans le chemin de données

Utilisez la commande "**show platform software fed switch active|standby|member wdavc function wdavc_ft_show_stats_ui | inc err|warn|fail** to view potential flow table errors :

```
Switch#show platform software fed switch active wdavc function wdavc_ft_show_stats_ui | inc
err|warn|fail
Bucket linked exceed max error : 0
extract_tuple_non_first_fragment_warn : 0
ft_client_err_alloc_fail : 0
ft_client_err_detach_fail : 0
ft_client_err_detach_fail_intf_attach : 0
ft_inst_nfl_clock_sync_err : 0
ft_ager_err_invalid_timeout : 0
ft_intf_err_alloc_fail : 0
ft_intf_err_detach_fail : 0
ft_inst_err_unreg_client_all : 0
ft_inst_err_inst_del_fail : 0
ft_flow_seg_sync_nfl_resp_pend_del_warn : 0
ager_sm_cb_bad_status_err : 0
ager_sm_cb_received_err : 0
ft_ager_to_time_no_mask_err : 0
ft_ager_to_time_latest_zero_ts_warn : 0
ft_ager_to_time_seg_zero_ts_warn : 0
ft_ager_to_time_ts_bigger_curr_warn : 0
ft_ager_to_ad_nfl_resp_error : 0
ft_ager_to_ad_req_all_recv_error : 0
ft_ager_to_ad_req_error : 0
ft_ager_to_ad_resp_error : 0
ft_ager_to_ad_req_restart_timer_due_err : 0
ft_ager_to_flow_del_nfl_resp_error : 0
ft_ager_to_flow_del_all_recv_error : 0
ft_ager_to_flow_del_req_error : 0
ft_ager_to_flow_del_resp_error : 0
ft_consumer_timer_start_error : 0
ft_consumer_tw_stop_error : 0
ft_consumer_memory_error : 0
ft_consumer_ad_resp_error : 0
ft_consumer_ad_resp_fc_error : 0
ft_consumer_cb_err : 0
ft_consumer_ad_resp_zero_ts_warn : 0
ft_consumer_ad_resp_zero_pkts_bytes_warn : 0
ft_consumer_remove_on_count_zero_err : 0
ft_ext_field_ref_cnt_zero_warn : 0
ft_ext_gen_ref_cnt_zero_warn : 0
```

Utilisez la commande "**show platform software fed switch active wdavc function wdavc_stile_stats_show_ui | inc err"** pour afficher les éventuelles erreurs NBAR :

```
Switch#show platform software fed switch active wdavc function wdavc_stile_stats_show_ui | inc
err
find_flow_error : 0
add_flow_error : 0
remove_flow_error : 0
detach_fo_error : 0
is_forward_direction_error : 0
set_flow_aging_error : 0
ft_process_packet_error : 0
sys_meminfo_get_error : 0
```

Vérifier que les paquets sont clonés sur le processeur

Utilisez la commande **"show platform software fed switch active punt cpuq 21 | inc received"** pour

vérifier que les paquets sont clonés sur le processeur pour le traitement NBAR :

> **Note**: Au cours des travaux pratiques, ce numéro n'a pas été incrémenté.

```
Switch#show platform software fed switch active punt cpuq 21 | inc received
Packets received from ASIC : 63
```

Identifier la congestion du processeur

En cas de congestion, les paquets peuvent être abandonnés avant d'être envoyés au processus WDAVC. Utilisez la commande **"show platform software fed switch active wdavc function fed_wdavc_show_ots_stats_ui"** pour valider :

```
Switch#show platform software fed switch active wdavc function fed_wdavc_show_ots_stats_ui
OTS Limits
-------------------------------------------
ots_queue_max : 20000
emer_bypass_ots_queue_stress : 4000
emer_bypass_ots_queue_normal : 200
OTS Statistics
-------------------------------------------
total_requests : 40
total_non_wdavc_requests : 0
request_empty_field_data_error : 0
request_invalid_di_error : 0
request_buf_coalesce_error : 0
request_invalid_format_error : 0
request_ip_version_error : 0
request_empty_packet_error : 0
memory_allocation_error : 0
emergency_bypass_requests_warn : 0
dropped_requests : 0
enqueued_requests : 40
max_ots_queue : 0
```

> **Astuce** : Pour effacer le compteur de points de chute, utilisez la commande "**show platform software fed switch active wdavc function fed_wdavc_clear_ots_stats_ui"**

Identifier les problèmes d'évolutivité

S'il n'y a aucune entrée FNF libre dans le matériel, le trafic n'est pas soumis à la classification NBAR2. Utilisez la commande « **show platform software fed switch active fnf sw-table-size asic <number> shadow 0 »** pour confirmer :

> **Note**: Les flux créés sont spécifiques au commutateur et au coeur de base lors de leur création. Le numéro de commutateur (actif, en veille, etc.) doit être spécifié en conséquence. Le numéro ASIC entré est lié à l'interface correspondante. Utilisez « **show platform software fed switch active|standby|member ifm mappings »** pour déterminer l'ASIC qui correspond à l'interface. Pour l'option d'ombre, utilisez toujours "0".

```
Switch#show platform software fed switch active fnf sw-table-sizes asic 3 shadow 0

--------------------------------
```

```
Global Bank Allocation
--------------------------------
Ingress Banks : Bank 0
Egress Banks : Bank 1
--------------------------------
Global flow table Info
INGRESS usedBankEntry 1 usedOvfTcamEntry 0
EGRESS usedBankEntry 0 usedOvfTcamEntry 0 <-- 256 means TCAM entries are full
--------------------------------
Flows Statistics
INGRESS TotalSeen=1 MaxEntries=1 MaxOverflow=0
EGRESS TotalSeen=0 MaxEntries=0 MaxOverflow=0

--------------------------------
Partition Table
--------------------------------
## Dir Limit CurrFlowCount OverFlowCount MonitoringEnabled
0 ING 0 0 0 0
1 ING 16640 1 0 1
2 ING 0 0 0 0
3 ING 16640 0 0 0
4 ING 0 0 0 0
5 ING 8192 0 0 1
6 ING 0 0 0 0
7 ING 0 0 0 0
8 ING 0 0 0 0
9 ING 0 0 0 0
10 ING 0 0 0 0
11 ING 0 0 0 0
12 ING 0 0 0 0
13 ING 0 0 0 0
14 ING 0 0 0 0
15 ING 0 0 0 0
0 EGR 0 0 0 0
1 EGR 16640 0 0 1
2 EGR 0 0 0 0
3 EGR 16640 0 0 0
4 EGR 0 0 0 0
5 EGR 8192 0 0 1
6 EGR 0 0 0 0
7 EGR 0 0 0 0
8 EGR 0 0 0 0
9 EGR 0 0 0 0
10 EGR 0 0 0 0
11 EGR 0 0 0 0
12 EGR 0 0 0 0
13 EGR 0 0 0 0
14 EGR 0 0 0 0
15 EGR 0 0 0 0
```

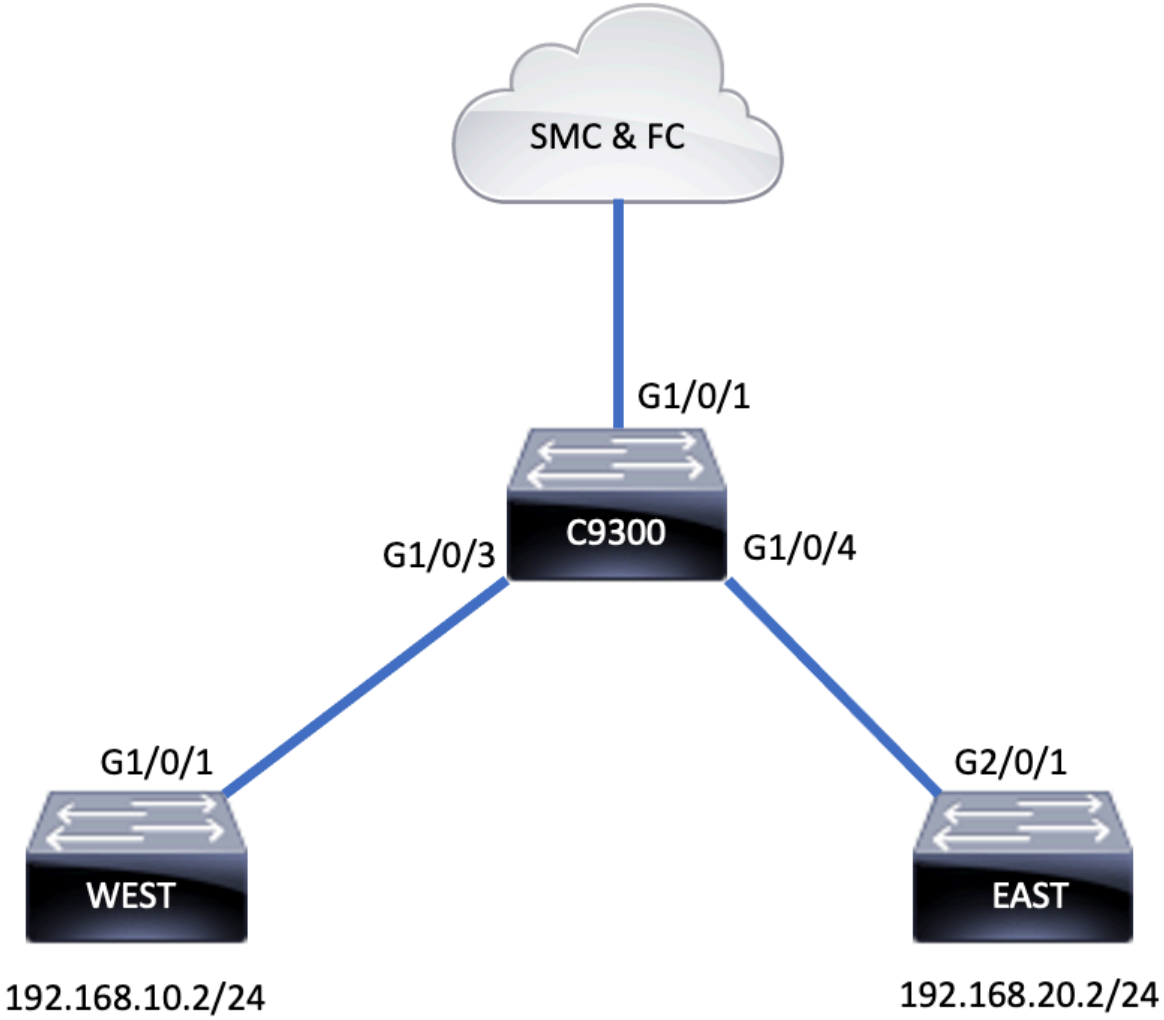
Analyse du trafic chiffré (ETA)

Informations générales

- L'ETA se concentre sur l'identification de la communication de programmes malveillants dans le trafic chiffré via la surveillance passive, l'extraction d'éléments de données pertinents et une combinaison de modélisation comportementale et d'apprentissage automatique avec une sécurité globale basée sur le cloud.
- ETA exploite la télémétrie de NetFlow ainsi que la détection des programmes malveillants chiffrés et la conformité cryptographique et envoie ces données à Cisco StealthWatch.

- ETA extrait deux éléments de données principaux : le Paquet de données initial (IDP) et la Séquence de longueur et de durée du paquet (SPLT).

Diagramme du réseau



Composants

L'ETA se compose de plusieurs composants différents utilisés conjointement pour créer la solution ETA :

- NetFlow : norme définissant les éléments de données exportés par les périphériques réseau qui décrivent les flux sur le réseau.
- Cisco StealthWatch - Exploite la puissance de la télémétrie du réseau, notamment NetFlow, IPFIX, les journaux de proxy et l'inspection approfondie des paquets bruts, pour fournir une visibilité réseau avancée, des informations de sécurité et des analyses.
- Cisco Cognitive Intelligence - Détecte les activités malveillantes qui ont contourné les contrôles de sécurité ou sont entrées par des canaux non surveillés et dans l'environnement d'une entreprise.
- Analyse du trafic chiffré : la fonctionnalité Cisco IOS XE, qui utilise des algorithmes comportementaux avancés pour identifier les modèles de trafic malveillant via l'analyse des métadonnées d'entrée du trafic chiffré, détecte les menaces potentielles cachées dans le

trafic chiffré.

Note: Cette partie du document se concentre uniquement sur la configuration et la vérification de l'ETA et de NetFlow sur le commutateur de la gamme Catalyst 9000 et ne couvre pas le déploiement de la console de gestion StealthWatch (SMC) et du collecteur de flux (FC) sur le cloud Cognitive Intelligence.

Restrictions

- Le déploiement de l'ETA nécessite DNA Advantage pour fonctionner
- ETA et un analyseur de port commuté (SPAN) de transmission (TX) ne sont pas pris en charge sur la même interface.

Cette liste n'est pas exhaustive. Consultez le guide de configuration approprié pour le commutateur et la version du code pour toutes les restrictions.

Configuration

Comme le montre la sortie, activez l'ETA sur le commutateur globalement et définissez la destination d'exportation de flux :

```
C9300(config)#et-analytics
C9300(config-et-analytics)#ip flow-export destination 172.16.18.1 2055
```

Astuce : Vous DEVEZ utiliser le port 2055, n'utilisez pas un autre numéro de port.

Configurez ensuite Flexible NetFlow comme indiqué dans le résultat :

Configurer l'enregistrement de flux

```
C9300(config)#flow record FNF-RECORD
C9300(config-flow-record)#match ipv4 protocol
C9300(config-flow-record)#match ipv4 source address
C9300(config-flow-record)#match ipv4 destination address
C9300(config-flow-record)#match transport source-port
C9300(config-flow-record)#match transport destination-port
C9300(config-flow-record)#collect counter bytes long
C9300(config-flow-record)#collect counter packets long
C9300(config-flow-record)#collect timestamp absolute first
C9300(config-flow-record)#collect timestamp absolute last
```

Configurer Flow Monitor

```
C9300(config)#flow exporter FNF-EXPORTER
C9300(config-flow-exporter)#destination 172.16.18.1
C9300(config-flow-exporter)#transport udp 2055
C9300(config-flow-exporter)#template data timeout 30
C9300(config-flow-exporter)#option interface-table
C9300(config-flow-exporter)#option application-table timeout 10
C9300(config-flow-exporter)#exit
```

Configurer l'enregistrement de flux

```
C9300(config)#flow monitor FNF-MONITOR
C9300(config-flow-monitor)#exporter FNF-EXPORTER
C9300(config-flow-monitor)#record FNF-RECORD
C9300(config-flow-monitor)#end
```

Appliquer le moniteur de flux

```
C9300(config)#int range g1/0/3-4
C9300(config-if-range)#ip flow mon FNF-MONITOR in
C9300(config-if-range)#ip flow mon FNF-MONITOR out
C9300(config-if-range)#end
```

Activer ETA sur les interfaces de commutateur

```
C9300(config)#interface range g1/0/3-4
C9300(config-if-range)#et-analytics enable
```

Vérification

Vérifiez que le moniteur ETA « eta-mon » est actif. Vérifiez que l'état est alloué via la commande "show flow monitor eta-mon"

```
C9300#show flow monitor eta-mon
Flow Monitor eta-mon:
Description: User defined
Flow Record: eta-rec
Flow Exporter: eta-exp
Cache:
Type: normal (Platform cache)
Status: allocated
Size: 10000 entries
Inactive Timeout: 15 secs
Active Timeout: 1800 secs
```

Vérifiez que le cache ETA est rempli. Lorsque NetFlow et ETA sont configurés sur la même interface, utilisez « show flow monitor <nom du moniteur> cache » au lieu de « show flow monitor eta-mon cache » car le résultat de « show flow monitor eta-mon cache » est vide :

```
C9300#show flow monitor FNF-MONITOR cache
Cache type: Normal (Platform cache)
Cache size: 10000
Current entries: 4

Flows added: 8
Flows aged: 4
- Inactive timeout ( 15 secs) 4

IPV4 SOURCE ADDRESS: 192.168.10.2
IPV4 DESTINATION ADDRESS: 192.168.20.2
TRNS SOURCE PORT: 0
TRNS DESTINATION PORT: 0
IP PROTOCOL: 1
counter bytes long: 500
counter packets long: 5
timestamp abs first: 21:53:23.390
timestamp abs last: 21:53:23.390

IPV4 SOURCE ADDRESS: 192.168.20.2
```

```
IPV4 DESTINATION ADDRESS: 192.168.10.2
TRNS SOURCE PORT: 0
TRNS DESTINATION PORT: 0
IP PROTOCOL: 1
counter bytes long: 500
counter packets long: 5
timestamp abs first: 21:53:23.390
timestamp abs last: 21:53:23.390

IPV4 SOURCE ADDRESS: 192.168.20.2
IPV4 DESTINATION ADDRESS: 192.168.10.2
TRNS SOURCE PORT: 0
TRNS DESTINATION PORT: 0
IP PROTOCOL: 1
counter bytes long: 500
counter packets long: 5
timestamp abs first: 21:53:23.390
timestamp abs last: 21:53:23.390

IPV4 SOURCE ADDRESS: 192.168.10.2
IPV4 DESTINATION ADDRESS: 192.168.20.2
TRNS SOURCE PORT: 0
TRNS DESTINATION PORT: 0
IP PROTOCOL: 1
counter bytes long: 500
counter packets long: 5
timestamp abs first: 21:53:23.390
timestamp abs last: 21:53:23.390
```

Validez que les flux sont exportés vers SMC et FC avec la commande "**show flow exporter eta-exp statistics**"

```
C9300#show flow exporter eta-exp statistics
Flow Exporter eta-exp:
Packet send statistics (last cleared 03:05:32 ago):
Successfully sent: 3 (3266 bytes)

Client send statistics:
Client: Flow Monitor eta-mon
Records added: 4
- sent: 4
Bytes added: 3266
- sent: 3266
```

Vérifiez que le SPLT et l'IDP sont exportés vers la carte FC à l'aide de la commande « **show platform software fed switch active fnf et-analytics-flows** »

```
C9300#show platform software fed switch active fnf et-analytics-flows

ET Analytics Flow dump

=================
Total packets received : 20
Excess packets received : 0
Excess syn received : 0
Total eta records added : 4
Current eta records : 0
Total eta splt exported : 2
Total eta IDP exported : 2
```

Validez quelles interfaces sont configurées pour et-analytics avec la commande "**show platform software et-analytics interfaces**"

```
C9300#show platform software et-analytics interfaces
ET-Analytics interfaces
GigabitEthernet1/0/3
GigabitEthernet1/0/4

ET-Analytics VLANs
```

Utilisez la commande "show platform software et-analytics global" pour afficher un état global d'ETA :

```
C9300#show plat soft et-analytics global
ET-Analytics Global state
=========================
All Interfaces : Off
IP Flow-record Destination : 10.31.126.233 : 2055
Inactive timer : 15

ET-Analytics interfaces
GigabitEthernet1/0/3
GigabitEthernet1/0/4

ET-Analytics VLANs
```

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.