Configurazione e verifica di Netflow, AVC e ETA sugli switch Catalyst serie 9000

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Esempio di rete](#)
[Configurazione](#)
[Componenti](#)
[Record di flusso](#)
[Esportatore flusso](#)
[Monitoraggio flusso](#)
[Campionatore flusso (facoltativo)](#)
[Restrizioni](#)
[Verifica](#)
[Verifica indipendente dalla piattaforma](#)
[Verifica dipendente dalla piattaforma](#)
[Inizializzazione NetFlow - Tabella delle partizioni NFL](#)
[Monitoraggio flusso](#)
[ACL NetFlow](#)
[Maschera flusso](#)
[Dati offload timestamp e statistiche di flusso](#)
[Visibilità e controllo delle applicazioni (AVC)](#)
[Premesse](#)
[Prestazioni e scalabilità](#)
[Restrizioni per Wired AVC](#)
[Esempio di rete](#)
[Componenti](#)
[BARRA2](#)
[Verifica AVC](#)
[ETA (Encrypted Traffic Analytics)](#)
[Premesse](#)
[Esempio di rete](#)
[Componenti](#)
[Restrizioni](#)
[Configurazione](#)
[Verifica](#)

Introduzione

In questo documento viene descritto come configurare e convalidare NetFlow, Application Visibility and Control (AVC) e Encrypted Traffic Analytics (ETA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- NetFlow
- AVC
- ETA

Componenti usati

Per questo documento, è stato usato uno switch Catalyst 9300 con software Cisco IOS XE versione 16.12.4.

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.

Prodotti correlati

Il presente documento può essere utilizzato anche per le seguenti versioni hardware e software:

- 9200
- 9400
- 9500
- 9600
- Cisco IOS XE 16.12 e versioni successive

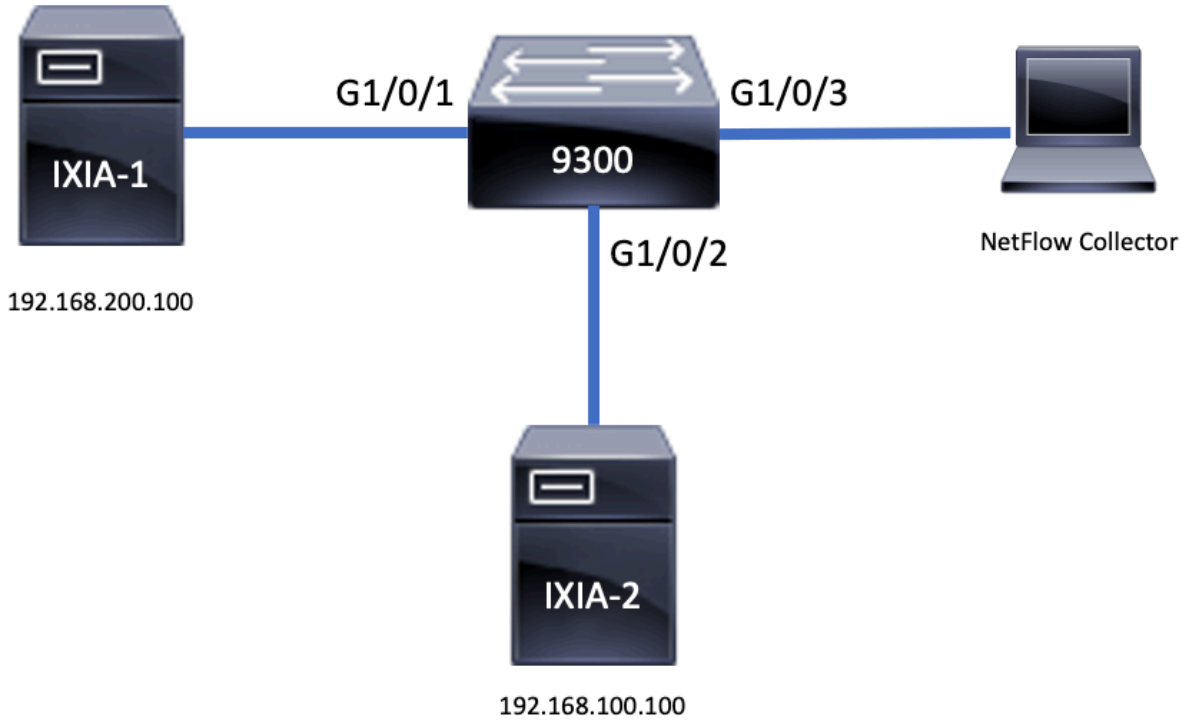
Premesse

- Flexible NetFlow è la tecnologia di flusso di nuova generazione che raccoglie e misura i dati per permettere a tutti i router o switch della rete di diventare una fonte di telemetria.
- Flexible NetFlow consente misurazioni del traffico estremamente granulari e accurate e una raccolta di traffico aggregato di alto livello.
- Flexible NetFlow utilizza i flussi per fornire statistiche per la contabilità, il monitoraggio della rete e la pianificazione della rete.
- Un flusso è un flusso unidirezionale di pacchetti che arriva a un'interfaccia di origine e ha gli stessi valori per le chiavi. Una chiave è un valore identificato per un campo all'interno del pacchetto. È possibile creare un flusso tramite un record di flusso per definire le chiavi univoche per il flusso.

Nota: I comandi della piattaforma (feed) possono variare. Il comando può essere **"show**

platform fed <active|standby>" oppure "**show platform fed switch <active|standby>**". Se la sintassi indicata negli esempi non viene analizzata, provare con la variante.

Esempio di rete



Configurazione

Componenti

La configurazione NetFlow è composta da **tre componenti principali** che possono essere usati insieme: diverse variazioni per eseguire l'analisi del traffico e l'esportazione dei dati.

Record di flusso

- Un record è una combinazione di campi chiave e non chiave. I record Flexible NetFlow vengono assegnati ai monitor di flusso Flexible NetFlow per definire la cache che viene utilizzata per l'archiviazione dei dati di flusso.
- Flexible NetFlow include diversi record predefiniti che possono essere utilizzati per monitorare il traffico.
- Flexible NetFlow consente inoltre di definire record personalizzati per una cache Flexible NetFlow Monitor specificando campi chiave e non chiave per personalizzare la raccolta dei dati in base alle proprie esigenze.

Come mostrato nell'esempio, i dettagli di configurazione del record di flusso sono riportati di seguito.

```
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
```

Esportatore flusso

- Gli esportatori di flusso vengono utilizzati per esportare i dati nella cache del monitor di flusso in un sistema remoto (server che funge da agente di raccolta NetFlow), per l'analisi e l'archiviazione.
- Gli esportatori di flussi vengono assegnati ai monitor di flusso per fornire la capacità di esportazione dei dati per i monitor di flusso.

Come mostrato nell'esempio, i dettagli di configurazione dell'utilità di esportazione del flusso sono:

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

Monitoraggio flusso

- I monitor di flusso sono il componente Flexible NetFlow che viene applicato alle interfacce per eseguire il monitoraggio del traffico di rete.
- I dati di flusso vengono raccolti dal traffico di rete e aggiunti alla cache del monitoraggio del flusso durante l'esecuzione del processo. Il processo si basa sui campi chiave e non chiave nel record di flusso.

Come mostrato nell'esempio, i dettagli di configurazione del monitor di flusso sono:

```
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
```

Campionatore flusso (facoltativo)

- I campionatori di flusso vengono creati come componenti separati nella configurazione di un router.
- I campionatori di flusso limitano il numero di pacchetti selezionati per l'analisi per ridurre il carico sul dispositivo che utilizza Flexible NetFlow.
- I campionatori di flusso vengono utilizzati per ridurre il carico sul dispositivo che utilizza Flexible NetFlow ottenuto tramite il limite del numero di pacchetti selezionati per l'analisi.
- I campionatori di flusso si scambiano l'accuratezza per le prestazioni del router. In caso di riduzione del numero di pacchetti analizzati dal monitor di flusso, è possibile che l'accuratezza delle informazioni archiviate nella cache del monitor di flusso venga compromessa.

Come mostrato nell'esempio, configurazione del campionatore di flusso:

```
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
```

Restrizioni

- Èrichiesta una licenza DNA Addon per Flexible NetFlow completo, altrimenti Sampled NetFlow è disponibile solo.
- Gli esportatori di flussi non possono utilizzare la porta di gestione come origine.

Questo non è un elenco completo. Consultare la guida alla configurazione per la piattaforma e il codice appropriati.

Verifica

Verifica indipendente dalla piattaforma

Verificare la configurazione e confermare che i componenti NetFlow richiesti siano presenti:

1. **Record di flusso**
2. **Esportatore flusso**
3. **Monitoraggio flusso**
4. **Campionatore flusso (facoltativo)**

   Suggerimento: Per visualizzare l'output del record di flusso, dell'utilità di esportazione del flusso e del monitor di flusso in un unico comando, eseguire "**show running-config flow**

monitor <nome monitor flusso> expand"

Come mostrato nell'esempio, il monitor di flusso è collegato alla direzione di input e ai componenti associati:

```
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
!
```

Come mostrato nell'esempio, il monitor di flusso è collegato alla direzione di uscita e ai componenti associati:

```
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
!
```

Eseguire il comando "show flow monitor <nome monitor flusso>" statistics. Questo output è utile per confermare che i dati sono stati registrati:

```
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
```

Eseguire il comando **"show flow monitor <nome monitor flusso> cache** per verificare che la cache NetFlow abbia un output:

```
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
```

Eseguire il comando **"show flow export <nome esportatore> statistics"** per confermare che l'esportatore ha inviato i pacchetti:

```
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
```

Verifica dipendente dalla piattaforma

Inizializzazione NetFlow - Tabella delle partizioni NFL

- Le partizioni NetFlow vengono inizializzate per diverse funzionalità con 16 partizioni per direzione (input vs output).
- La configurazione della tabella di partizione NetFlow è divisa nell'allocazione bancaria globale, ulteriormente suddivisa nelle banche dei flussi in entrata e in uscita.

Campi chiave

- Numero di partizioni

- Stato abilitazione partizione
- Limite di partizione
- Utilizzo corrente della partizione

Per visualizzare la tabella delle partizioni NetFlow, è possibile eseguire il comando "**show platform software fed switch active|standby|member| fnf sw-table-sizes asic <numero di base> shadow 0"**

> **Nota:** I flussi creati sono specifici dello switch e del core di base al momento della creazione. Il numero dell'interruttore (attivo, standby, ecc.) deve essere specificato di conseguenza. Il numero ASIC immesso è associato all'interfaccia corrispondente. Utilizzare "**show platform software fed switch active|standby|member ifm mappings"** per determinare l'ASIC che corrisponde all'interfaccia. Per l'opzione ombra, utilizzare sempre "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
```

Monitoraggio flusso

La configurazione del monitoraggio del flusso include quanto segue:

1. Configurazione di ACL NetFlow, che determina la creazione di una voce nella tabella ACL TCAM.

La voce ACL TCAM è composta da:

- Cerca chiavi corrispondenti
- Parametri dei risultati utilizzati per la ricerca NetFlow, che includono:
  ID profiloID NetFlow

2. Configurazione della maschera di flusso, che determina la creazione di una voce in NflLookupTable e NflFlowMaskTable.

- Indicizzato dai parametri dei risultati ACL NetFlow per trovare la maschera di flusso per la ricerca netflow

ACL NetFlow

Per visualizzare la configurazione degli ACL di NetFlow, eseguire il comando "**show platform hardware fed switch active fwd-asic resource tcam table nfl_acl asic <numero asic>**

> **Suggerimento**: Se è presente un ACL di porta (PACL), la voce viene creata sull'ASIC a cui è mappata l'interfaccia. Nel caso di un ACL del router (RACL), la voce è presente su tutti gli ASIC.

- In questo output ci sono NFCMD0 e NFCMD1, che sono valori a 4 bit. Per calcolare l'ID profilo, convertire i valori in formato binario.
- In questo output, NFCMD0 è 1, NFCMD1 è 2. Quando convertito in formato binario: 000100010
- In Cisco IOS-XE versione 16.12 e successive, all'interno degli 8 bit combinati, i primi 4 bit sono l'ID del profilo e il 7° bit indica che la ricerca è abilitata. Nell'esempio, **0001**0010, l'ID profilo è 1.
- In Cisco IOS XE 16.11 e versioni precedenti del codice, negli 8 bit combinati, i primi 6 bit sono l'ID del profilo e il 7° bit indica che la ricerca è abilitata. Nell'esempio, **000100**10, l'ID profilo è 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

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

Maschera flusso

Eseguire il comando "**show platform software fed switch active|standby|member fnf mask-entry asic <numero di base> voce 1"** per verificare che la maschera di flusso sia installata nell'hardware. Qui è possibile trovare anche il numero di campi chiave.

```
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)
```

Dati offload timestamp e statistiche di flusso

Eseguire il comando "**show platform software fed switch active fnf flow-record asic <numero asic> start-index <numero indice> num-flows <numero di flussi>** per visualizzare le statistiche netflow e i timestamp

```
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
```

Visibilità e controllo delle applicazioni (AVC)

Premesse

- Application Visibility and Control (AVC) è una soluzione che sfrutta le funzionalità di

riconoscimento basato su rete versione 2 (**NBAR2**), **NetFlow V9** e vari strumenti di gestione e report (**Cisco Prime**) per classificare le applicazioni tramite DPI (Deep Packet Inspection).
- AVC può essere configurato su porte di accesso cablate per switch standalone o stack di switch.
- AVC può essere utilizzato anche sui controller wireless Cisco per identificare le applicazioni basate su DPI e quindi contrassegnarle con un valore DSCP specifico. Può inoltre raccogliere varie metriche delle prestazioni wireless, ad esempio l'utilizzo della larghezza di banda in termini di applicazioni e client.

Prestazioni e scalabilità

Prestazioni: ciascun membro dello switch è in grado di gestire 500 connessioni al secondo (CPS) con un utilizzo della CPU inferiore al 50%. Oltre a questa tariffa, il servizio AVC non è garantito.

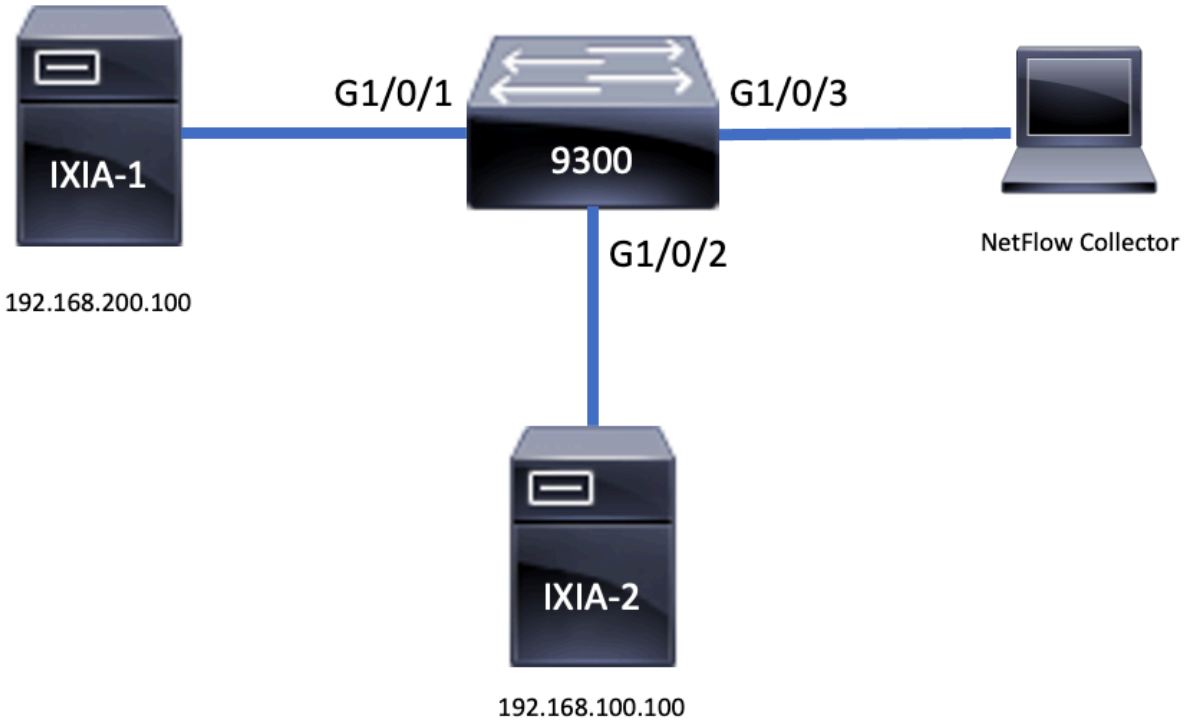
Scalabilità: capacità di gestire fino a 5.000 flussi bidirezionali per 24 porte di accesso (circa 200 flussi per porta di accesso).

Restrizioni per Wired AVC

- Non è possibile configurare contemporaneamente AVC e ETA (Encrypted Traffic Analytics) sulla stessa interfaccia.
- La classificazione dei pacchetti è supportata solo per il traffico IPv4 (TCP/UDP) unicast.
- La configurazione dei criteri QoS basati su NBAR è supportata solo su porte fisiche cablate. Ciò include le porte di accesso e trunk di livello 2 e le porte indirizzate di livello 3.
- La configurazione dei criteri QoS basati su NBAR non è supportata sui membri del canale della porta, sulle interfacce virtuali di switch (SVI) o sulle sottointerfacce.
- I classificatori basati su NBAR2 **(protocollo di corrispondenza),** supportano solo azioni QoS di contrassegno e applicazione di policy.
- Il "protocollo di corrispondenza" è limitato a 255 protocolli diversi in tutte le policy (limitazione hardware a 8 bit)

> **Nota:** Questo non è un elenco esaustivo di tutte le restrizioni. Consultare la guida alla configurazione AVC appropriata per la piattaforma e la versione del codice in uso.

Esempio di rete



Componenti

La configurazione AVC è costituita da **tre** componenti **principali** che costituiscono la soluzione:

Visibilità: Protocol Discovery

- L'individuazione del protocollo viene eseguita tramite NBAR, che fornisce statistiche per interfaccia, direzione e byte/pacchetti dell'applicazione.
- Il rilevamento del protocollo è abilitato per un'interfaccia specifica tramite la configurazione dell'interfaccia **ip nbar protocol-discovery**

Come mostrato nell'output, come abilitare l'individuazione del protocollo:

```
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
```

Controllo: QoS basato su applicazioni

Rispetto alle tradizionali funzionalità QoS che corrispondono all'indirizzo IP e alla porta UDP/TCP, AVC offre un controllo più accurato tramite funzionalità QoS basate sull'applicazione, che consentono di ottenere una corrispondenza con l'applicazione e offrono un controllo più granulare tramite operazioni QoS quali la contrassegno e l'applicazione di policy.

- Le azioni vengono eseguite sul traffico aggregato (non per flusso)
- La funzionalità QoS basata su applicazioni viene ottenuta tramite la creazione di una mappa delle classi, la corrispondenza di un protocollo e quindi la creazione di una mappa dei criteri.
- Il criterio QoS basato su applicazioni è collegato a un'interfaccia.

Come mostrato nell'output, esempio di configurazione per QoS basato su applicazioni:

```
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 basato su applicazioni

Wired AVC FNF supporta due tipi di record di flusso predefiniti: **record di flusso bidirezionale legacy** e nuovi **record di flusso direzionale**.

I record di flusso bidirezionali tengono traccia delle statistiche delle applicazioni client/server.

Come mostrato nell'output, esempio di configurazione di un record di flusso bidirezionale.

```
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
```

I record direzionali sono stati di applicazione per input/output.

Come mostrato nell'output, esempi di configurazione di record direzionali di input e output:

> **Nota**: il comando "**match interface input**" specifica una corrispondenza con l'interfaccia di input. Il comando "**match interface output**" specifica una corrispondenza con l'interfaccia di output. Il comando "**match application name**" è obbligatorio per il supporto di 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
```

Esportatore flusso

Creare un'utilità di esportazione del flusso per definire i parametri di esportazione.

Come mostrato nell'output, esempio di configurazione dell'utilità di esportazione del flusso:

```
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
!
```

Monitoraggio flusso

Creare un monitor di flusso per associarlo a un record di flusso.

Come mostrato nell'output, esempio di configurazione del monitor di flusso:

```
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
```

Associa monitoraggio flusso a un'interfaccia

Èpossibile **collegare** contemporaneamente a un'interfaccia fino a due monitor AVC diversi con diversi record predefiniti.

Come mostrato nell'output, esempio di configurazione del monitor di flusso:

```
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
```

BARRA2

Aggiornamento di NBAR2 Dynamic Hitless Protocol Pack

I pacchetti di protocollo sono pacchetti software che aggiornano il supporto del protocollo NBAR2 su un dispositivo senza sostituire il software Cisco sul dispositivo. Un pacchetto di protocolli contiene informazioni sulle applicazioni ufficialmente supportate da NBAR2 che vengono compilate e compresse insieme. Per ogni applicazione, il pacchetto di protocolli include informazioni sulle firme e sugli attributi dell'applicazione. Ogni versione software è dotata di un pacchetto di protocollo integrato.

- NBAR2 consente di aggiornare il pacchetto-protocollo senza alcuna interruzione del traffico o del servizio e senza la necessità di modificare l'immagine software sui dispositivi
- I pacchetti del protocollo NBAR2 sono disponibili per il download in Cisco Software Center dal seguente URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

Aggiornamento pacchetto protocollo NBAR2

Prima di installare un nuovo pacchetto di protocollo, è necessario copiarlo nella memoria flash su tutti gli switch. Per caricare il nuovo pacchetto di protocollo, usare il comando "**ip nbar protocol-pack flash:<nome pacchetto>**

non è necessario ricaricare gli switch per aggiornare NBAR2.

Come mostrato nell'output, esempio di configurazione per il caricamento di NBAR2 Protocol Pack:

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

Per ripristinare il pacchetto di protocollo incorporato, utilizzare il comando "**default ip nbar protocol-pack**"

Come mostrato nell'output, esempio di configurazione di come ripristinare il pacchetto di protocollo incorporato:

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

Visualizza informazioni su NBAR2 Protocol Pack

Per visualizzare le informazioni sul pacchetto di protocolli, utilizzare i comandi elencati:

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

Come mostrato nell'output, nell'output di esempio di questi comandi:

```
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
```

Applicazioni personalizzate NBAR2

NBAR2 supporta l'utilizzo di protocolli personalizzati per identificare le applicazioni personalizzate. I protocolli personalizzati supportano protocolli e applicazioni attualmente non supportati da NBAR2.

Tra queste vi sono:

- Applicazione specifica a un'organizzazione

- Applicazioni specifiche di un'area geografica

NBAR2 consente di personalizzare manualmente le applicazioni tramite il comando **ip nbar custom<*nomeapp*>**.

Nota: Le applicazioni personalizzate hanno la precedenza sui protocolli incorporati

Esistono diversi tipi di personalizzazione delle applicazioni:

Personalizzazione protocollo generico

- HTTP
- SSL
- DNS

Composito:personalizzazione basata su più protocolli -**nome-server**

Personalizzazione Layer3/Layer4

- Indirizzo IPv4
- Valori DSCP
- porte TCP/UDP
- Direzione origine o destinazione flusso

Offset byte: personalizzazione basata su valori di byte specifici nel payload

Personalizzazione HTTP

La personalizzazione HTTP può essere basata su una combinazione di campi HTTP da:

- **cookie** - Cookie HTTP
- **host** - Nome host del server di origine contenente la risorsa
- **metodo** - metodo HTTP
- **referrer** - Indirizzo da cui è stata ottenuta la richiesta di risorsa
- **url** - Percorso Uniform Resource Locator
- **user-agent**: software utilizzato dall'agente che invia la richiesta
- **version** - Versione HTTP
- **via** - HTTP via campo

Esempio di applicazione personalizzata denominata MYHTTP che utilizza l'host HTTP "*mydomain.com" con ID selettore 10.

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

Personalizzazione SSL

Èpossibile personalizzare il traffico crittografato con SSL tramite le informazioni estratte da SNI (Server Name Indication) SSL o CN (Common Name).

Applicazione personalizzata di esempio denominata MYSSL che utilizza il nome univoco SSL "mydomain.com" con ID selettore 11.

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

Personalizzazione DNS

NBAR2 esamina il traffico di richiesta e risposta DNS e può correlare la risposta DNS a un'applicazione. L'indirizzo IP restituito dalla risposta DNS viene memorizzato nella cache e utilizzato per i flussi di pacchetti successivi associati all'applicazione specifica.

Il comando commandip nbar *customapplication-namednsdomain-nameidapplication*-idis utilizzato per la personalizzazione del DNS. Per estendere un'applicazione, utilizzare il comando commandip nbar *customapplication*-namedns domain-*namedomain-nameextendsexisting-application*.

Esempio di applicazione personalizzata denominata MYDNS che utilizza il nome di dominio DNS "mydomain.com" con ID selettore 12.

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

Personalizzazione composita

NBAR2 consente di personalizzare le applicazioni in base ai nomi di dominio visualizzati in HTTP, SSL o DNS.

Applicazione personalizzata di esempio denominata MYDOMAIN che utilizza il nome di dominio HTTP, SSL o DNS "mydomain.com" con ID selettore 13.

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

Personalizzazione L3/L4

La personalizzazione di layer3/layer4 si basa sulla tupla del pacchetto e viene sempre abbinata al primo pacchetto di un flusso.

Esempio di applicazione personalizzata LAYER4CUSTOM che corrisponde agli indirizzi IP 10.56.1.10 e 10.56.1.11, TCP e DSCP ef con ID selettore 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
```

Monitoraggio applicazioni personalizzate

Per monitorare le applicazioni personalizzate, utilizzare i comandi show elencati:

show ip nbar protocol-id | inc. Personalizzato

```
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 id-protocollo CUSTOM_APP

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

Verifica AVC

Per convalidare la funzionalità di AVC, è necessario eseguire più passaggi. In questa sezione vengono forniti comandi e output di esempio.

Per verificare che NBAR sia attivo, eseguire il comando "**show ip nbar control-plane**"

Aree principali:

- Lo stato NBAR deve essere **attivato** in uno scenario corretto
- Lo stato di configurazione di NBAR deve essere **pronto** in uno scenario corretto

```
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>
```

Verificare che ciascun membro dello switch abbia un piano dati attivo con il comando **show platform software fed switch active|standby|member.wdavc, funzione wdavc_stile_cp_show_info_ui**:

Se DP è attivato, deve essere **VERO** in uno scenario corretto

```
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
```

Utilizzare il comando "**show platform software fed switch active|standby|member wdavc flows** per visualizzare le informazioni principali:

```
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
```

Campi chiave:

CurrFlows: illustra il numero di flussi attivi rilevati da AVC.

Filigrana: Dimostra il maggior numero di flussi tracciati storicamente da AVC

TIMEOUT SEC: Timeout di inattività in base all'applicazione identificata

NOME APP: Applicazione identificata

TIPO DI FLUSSO: Flusso reale indica che è stato creato come risultato di dati in ingresso. Pre Flow indica che il flusso viene creato come risultato dei dati in entrata. I pre-flussi vengono utilizzati per flussi multimediali previsti

TIPO TUPLA: I flussi reali sono sempre tuple complete, i pre-flussi sono tuple piene o mezze tuple

IGNORA: Se impostato su TRUE, indica che il software non richiede altri pacchetti per identificare questo flusso

FINALE: Se impostato su TRUE, indica che l'applicazione non cambia più per questo flusso

IGNORA PKT: Quanti pacchetti erano necessari per arrivare alla classificazione finale

#PKTS: Quanti pacchetti sono stati effettivamente inviati al software per questo flusso

Visualizzare ulteriori dettagli sui flussi correnti, è possibile utilizzare il comando "**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
```

Campi chiave

ID I/F: Specifica l'ID interfaccia

DIR SEG: specifica l'entrata della direzione di uscita

DIR FIF: determina se questa è la direzione dell'iniziatore di flusso

NFL HDL: ID flusso nell'hardware

Per visualizzare la voce nell'hardware, eseguire il comando "**show platform software fed switch active fnf flow-record asic <numero> start-index <numero> num-flows <numero di flussi>**

> **Nota:** Per scegliere l'ASIC, è l'istanza ASIC a cui è mappata la porta. Per identificare l'ASIC, usare il comando "**show platform software fed switch active|standby|member ifm mappings".** L'indice iniziale può essere impostato su "0" se non si è interessati a un flusso specifico. In caso contrario, è necessario specificare l'indice iniziale. Per i num-flow, specifica il numero di flussi visualizzabili, massimo 10.

```
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
```

Cerca vari errori e avvisi nel percorso dati

Utilizzare il comando "**show platform software fed switch active|standby|member wdavc function wdavc_ft_show_stats_ui | inc err|warn|**impossibile visualizzare potenziali errori della tabella di flusso:

```
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
```

Utilizzare il comando "**show platform software fed switch active wdavc function wdavc_stile_stats_show_ui | inc err"** per visualizzare gli eventuali errori 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
```

Verificare che i pacchetti siano clonati sulla CPU

Usare il comando **"show platform software fed switch active punt cpuq 21 | inc received"** per verificare che i pacchetti vengano duplicati sulla CPU per l'elaborazione NBAR:

> **Nota:** In laboratorio questo numero non è stato incrementato.

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

Individuazione congestione CPU

In caso di congestione, i pacchetti possono essere scartati prima di essere inviati al processo WDAVC. Utilizzare il comando **"show platform software fed switch active wdavc function fed_wdavc_show_ots_stats_ui"** per convalidare:

```
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
```

> **Suggerimento**: Per cancellare il contatore di punt drop, usare il comando "**show platform software fed switch active wdavc function fed_wdavc_clear_ots_stats_ui"**

Identificazione dei problemi di scalabilità

Se nell'hardware non sono presenti voci FNF gratuite, il traffico non è soggetto alla classificazione NBAR2. Utilizzare il comando "**show platform software fed switch active fnf sw-table-sizes asic <number> shadow 0"** per confermare:

> **Nota:** I flussi creati sono specifici dello switch e del core di base al momento della creazione. Il numero dell'interruttore (attivo, standby, ecc.) deve essere specificato di conseguenza. Il numero ASIC immesso è associato all'interfaccia corrispondente. Utilizzare "**show platform software fed switch active|standby|member ifm mappings"** per determinare l'ASIC che corrisponde all'interfaccia. Per l'opzione ombra, utilizzare sempre "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
```

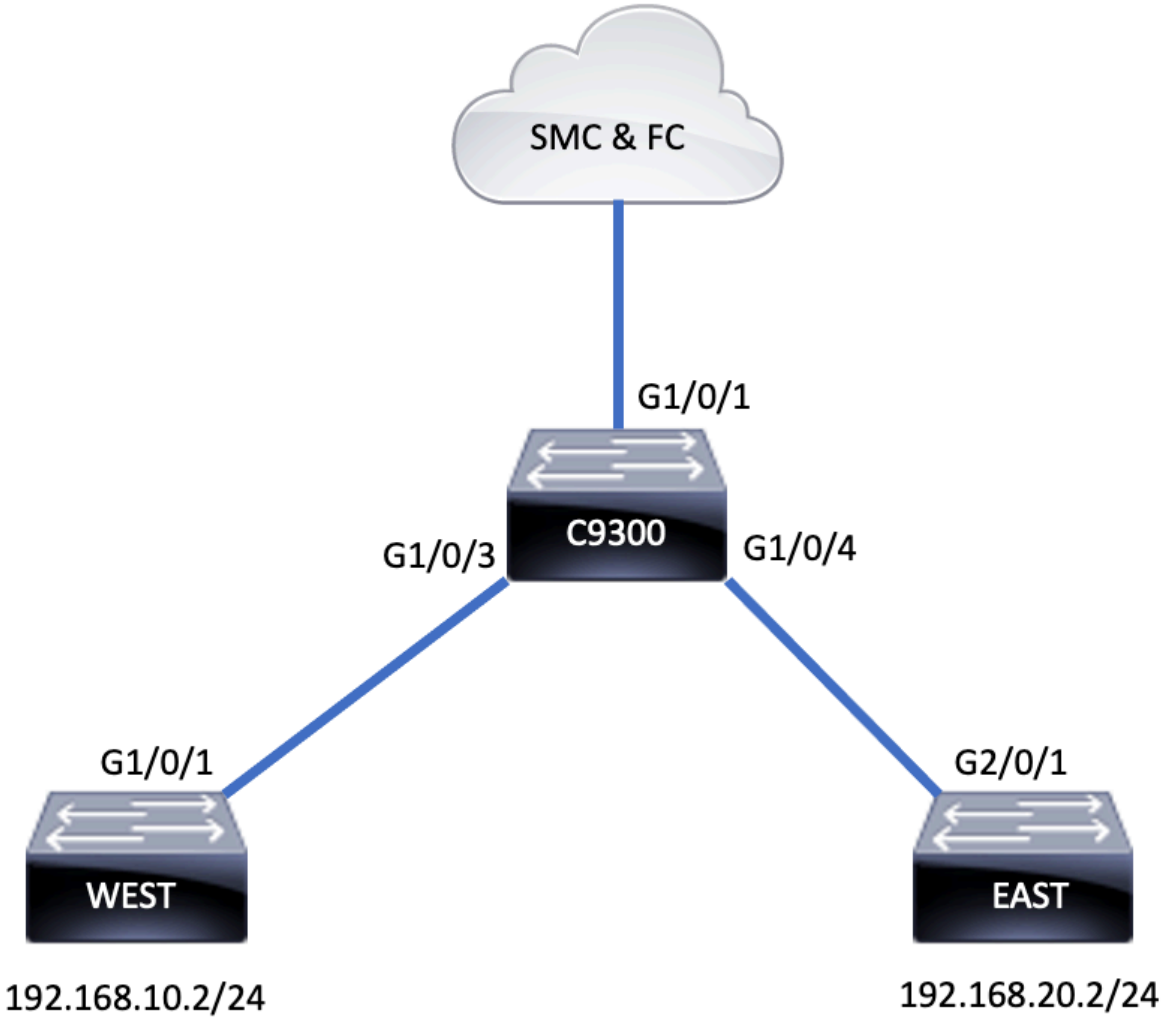
```
EGRESS usedBankEntry 0 usedOvfTcamEntry 0 <-- 256 means TCAM entries are full
--------------------------------
Flows Statistics
INGRESS TotalSeen=1 MaxEntries=1 MaxOverflow=0
EGRESS TotalSeen=0 MaxEntries=0 MaxOverflow=0

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

ETA (Encrypted Traffic Analytics)

Premesse

- L'ETA si concentra sull'identificazione delle comunicazioni malware nel traffico crittografato attraverso il monitoraggio passivo, l'estrazione di elementi di dati rilevanti e una combinazione di modellazione comportamentale e apprendimento automatico con la sicurezza globale basata sul cloud.
- L'ETA sfrutta la telemetria di NetFlow, il rilevamento criptato di malware e la conformità crittografica e invia questi dati a Cisco Stealthwatch.
- L'ETA estrae due dati principali: il pacchetto di dati iniziale (IDP) e la sequenza della lunghezza e dell'ora del pacchetto (SPLT).

Esempio di rete



Componenti

L'ETA è costituito da diversi componenti che vengono utilizzati insieme per creare la soluzione ETA:

- NetFlow: standard che definisce gli elementi dati esportati dai dispositivi di rete che descrivono i flussi sulla rete.
- Cisco Stealthwatch - Sfrutta la potenza della telemetria di rete che include NetFlow, IPFIX, registri proxy e ispezione approfondita dei pacchetti raw per fornire visibilità avanzata della rete, intelligence di sicurezza e analisi.
- Cisco Cognitive Intelligence - Trova attività dannose che hanno ignorato i controlli di sicurezza o sono entrate tramite canali non monitorati e all'interno dell'ambiente di un'organizzazione.
- Encrypted Traffic Analytics: funzionalità di Cisco IOS XE che utilizza algoritmi comportamentali avanzati per identificare modelli di traffico dannosi tramite l'analisi dei metadati di flusso di traffico in entrata del traffico crittografato, rileva le minacce potenziali nascoste nel traffico crittografato.

Nota: Questa parte del documento è dedicata esclusivamente alla configurazione e alla verifica di ETA e NetFlow sugli switch Catalyst serie 9000 e non riguarda l'implementazione di Stealthwatch Management Console (SMC) e Flow Collector (FC) su Cognitive Intelligence Cloud.

Restrizioni

- L'introduzione dell'ETA richiede il funzionamento di DNA Advantage
- L'ETA e un SPAN (Transmission (TX) Switched Port Analyzer non sono supportati sulla stessa interfaccia.

Questo elenco non è completo. Per informazioni sulle restrizioni, consultare la guida alla configurazione dello switch e la versione del codice.

Configurazione

Come mostrato nell'output, abilitare l'ETA sullo switch a livello globale e definire la destinazione dell'esportazione del flusso:

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

> **Suggerimento**: È NECESSARIO utilizzare la porta 2055, non utilizzare un altro numero di porta.

Quindi, configurare Flexible NetFlow come mostrato nell'output:

Configura record di flusso

```
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
```

Configura monitoraggio flusso

```
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
```

Configura record di flusso

```
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
```

Applica monitoraggio flusso

```
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
```

Abilita ETA sulle interfacce dello switch

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

Verifica

Verificare che il monitor ETA-mon sia attivo. Confermare che lo stato sia allocato tramite il comando "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
```

Verificare che la cache ETA sia popolata. Quando NetFlow e ETA sono configurati sulla stessa interfaccia, utilizzare "show flow monitor <nome monitor> cache" anziché "show flow monitor eta-mon cache" poiché l'output di "show flow monitor eta-mon cache" è vuoto:

```
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
```

Verificare che i flussi vengano esportati verso SMC e FC con il comando "**show flow export 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
```

Confermare che lo SPLT e l'IDP vengano esportati nella FC con il comando "**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
```

Convalidare le interfacce configurate per l'analisi della rete con il comando "**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
```

Utilizzare il comando "show platform software et-analytics global" per visualizzare uno stato globale di 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
```

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).