Configurar e verificar Netflow, AVC e ETA nos switches Catalyst 9000 Series

Contents

Introduction

Este documento descreve como configurar e validar o NetFlow, Application Visibility and Control (AVC) e Encrypted Traffic Analytics (ETA).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Netflow
- AVC
- ETA

Componentes Utilizados

As informações neste documento são baseadas em um switch Catalyst 9300 que executa o software 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Produtos Relacionados

Este documento também pode ser usado com as seguintes versões de hardware e software:

- 9200
- 9400
- 9500
- 9600
- Cisco IOS XE 16.12 e posterior

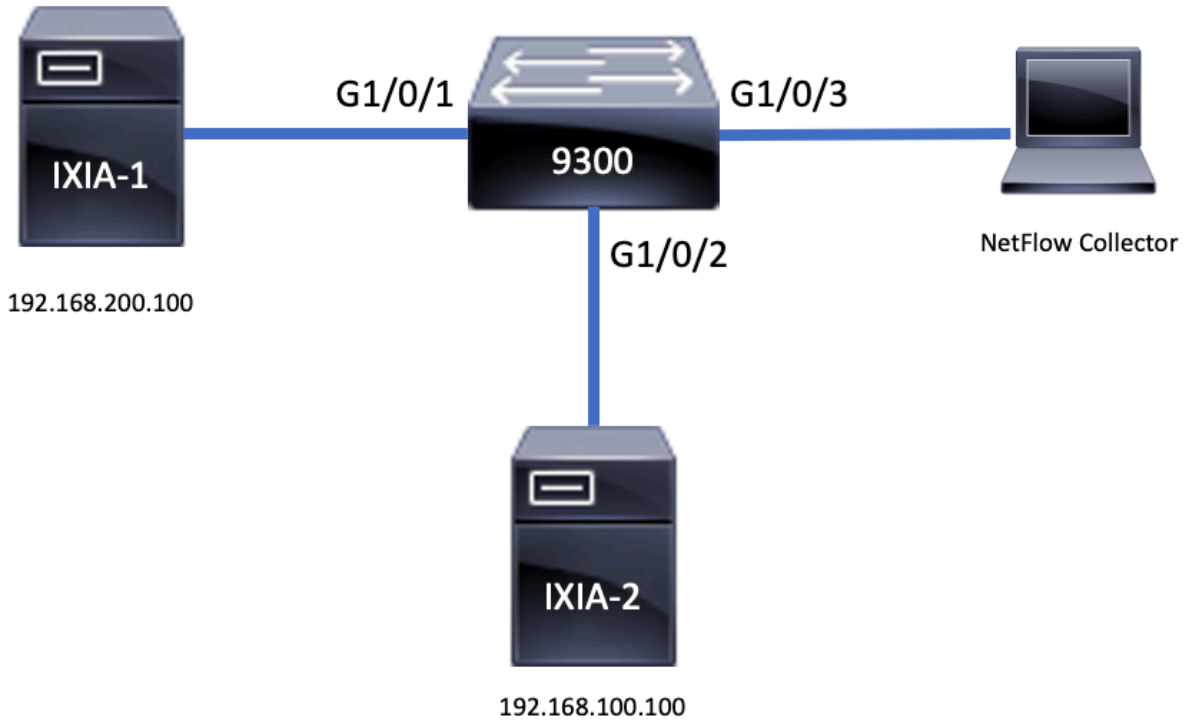
Informações de Apoio

- O Flexible NetFlow é a tecnologia de fluxo de próxima geração que coleta e mede dados para permitir que todos os roteadores ou switches na rede se tornem uma fonte de telemetria.
- O Flexible NetFlow permite medições de tráfego extremamente granulares e precisas e coleta de tráfego agregada de alto nível.
- O Flexible NetFlow usa fluxos para fornecer estatísticas para contabilidade, monitoramento de rede e planejamento de rede.
- Um fluxo é um fluxo unidirecional de pacotes que chega em uma interface de origem e tem os mesmos valores para as chaves. Uma chave é um valor identificado para um campo dentro do pacote. Você cria um fluxo por meio de um registro de fluxo para definir as chaves exclusivas do fluxo.

> **Note**: Os comandos de plataforma (feed) podem variar. O comando pode ser "**show platform fed <ative|standby>**" versus "**show platform fed switch <ative|standby>**". Se a sintaxe

anotada nos exemplos não for analisada, tente a variante.

Diagrama de Rede



Configurar

Componentes

A configuração do NetFlow é composta de **três componentes principais** que podem ser usados juntos, com várias variações para executar a análise de tráfego e a exportação de dados.

Registro de fluxo

- Um registro é uma combinação de campos-chave e não-chave. Os registros do Flexible NetFlow são atribuídos aos monitores de fluxo do Flexible NetFlow para definir o cache usado para o armazenamento de dados de fluxo.
- O Flexible NetFlow inclui vários registros predefinidos que podem ser usados para monitorar o tráfego.
- O Flexible NetFlow também permite que registros personalizados sejam definidos para um cache de monitor de fluxo do Flexible NetFlow por especificação de campos-chave e não-chave para personalizar a coleta de dados de acordo com seus requisitos específicos.

Como mostrado no exemplo, os detalhes da configuração do registro de fluxo:

```
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
```

Exportador de fluxo

- Os exportadores de fluxo são usados para exportar os dados no cache do monitor de fluxo para um sistema remoto (servidor que funciona como coletor NetFlow), para análise e armazenamento.
- Os exportadores de fluxo são atribuídos a monitores de fluxo para fornecer recursos de exportação de dados para os monitores de fluxo.

Como mostrado no exemplo, os detalhes de configuração do exportador de fluxo:

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

Monitor de fluxo

- Os monitores de fluxo são o componente Flexible NetFlow aplicado às interfaces para executar o monitoramento de tráfego de rede.
- Os dados de fluxo são coletados do tráfego da rede e adicionados ao cache do monitor de fluxo enquanto o processo é executado. O processo é baseado nos campos chave e não chave no registro de fluxo.

Como mostrado no exemplo, os detalhes da configuração do monitor de fluxo:

```
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
```

Amostrador de caudais (facultativo)

- Os amostradores de fluxo são criados como componentes separados na configuração de um roteador.
- Os amostradores de fluxo limitam o número de pacotes selecionados para análise para reduzir a carga no dispositivo que usa o Flexible NetFlow.
- Os Flow samplers são usados para reduzir a carga no dispositivo que usa o Flexible NetFlow obtida por meio do limite do número de pacotes selecionados para análise.
- Os amostradores de fluxo trocam precisão pelo desempenho do roteador. Se houver uma redução no número de pacotes analisados pelo monitor de fluxo, a precisão das informações armazenadas no cache do monitor de fluxo poderá ser afetada.

Como mostrado no exemplo, exemplo de configuração do amostrador de fluxo:

```
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
```

Restrições

- A licença do DNA Addon é necessária para o Flexible NetFlow completo, caso contrário, o Sampled NetFlow está disponível apenas.
- Os exportadores de fluxo não podem usar a porta de gerenciamento como origem.

Esta não é uma lista inclusiva. Consulte o guia de configuração para obter a plataforma e o código apropriados.

Verificar

Verificação independente de plataforma

Verifique a configuração e confirme se os componentes do NetFlow necessários estão presentes:

1. **Registro de fluxo**
2. **Exportador de fluxo**
3. **Monitor de fluxo**
4. **Amostrador de caudais (facultativo)**

> **Tip**: Para exibir o registro de fluxo, o exportador de fluxo e a saída do monitor de fluxo em um comando, execute "**show running-config flow monitor <flow monitor name> expand**"

Como mostrado no exemplo, o monitor de fluxo é ligado à direção de entrada e seus

componentes associados:

```
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
!
```

Como mostrado no exemplo, o monitor de fluxo é ligado à direção de saída e seus componentes associados:

```
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
!
```

Execute o comando "**show flow monitor <flow monitor name>" statistics.** Esta saída é útil para confirmar que os dados estão registrados:

```
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
```

Execute o comando **"show flow monitor <flow monitor name> cache para confirmar se o cache do NetFlow tem saída:**

```
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
```

Execute o comando **"show flow export <nome do exportador> statistics" para confirmar se o exportador enviou pacotes:**

```
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
```

Verificação dependente de plataforma

Inicialização do NetFlow - Tabela de Partição NFL

- As partições do NetFlow são inicializadas para recursos diferentes com 16 partições por direção (entrada vs saída).
- A configuração da tabela de partição do NetFlow é dividida em alocação de banco global, que é subdividida em bancos de fluxo de entrada e saída.

Campos-chave

- Número de partições
- Status de habilitação de partição
- Limite de partição
- Uso da partição atual

Para exibir a Tabela de Partição do NetFlow, você pode executar o comando "**show platform software fed switch ative|standby|member| fnf sw-table-size asic <asic number> shadow 0"**

> **Note**: Os fluxos criados são específicos do switch e do núcleo básico quando são criados. O número do switch (ativo, standby etc.) precisa ser especificado de acordo. O número ASIC inserido está vinculado à respectiva interface. Use "**show platform software fed switch ative|standby|member ifm mappings"** para determinar o ASIC que corresponde à interface. Para a opção de sombra, sempre use "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
```

Monitor de fluxo

A configuração do monitor de fluxo inclui o seguinte:

1. Configuração da ACL NetFlow, que resulta na criação de uma entrada na tabela TCAM da ACL.

A entrada TCAM da ACL é composta de:

- Pesquisar chaves correspondentes
- Parâmetros de resultado usados para pesquisa do NetFlow, que inclui o seguinte:
  ID do perfilID do NetFlow

2. Configuração de Máscara de Fluxo, que resulta na criação de uma entrada em NflLookupTable e NflFlowMaskTable.

- Indexado pelos parâmetros de resultado da ACL do NetFlow para encontrar a máscara de fluxo para pesquisa de Netflow

ACL NetFlow

Para visualizar a configuração da ACL do NetFlow, execute o comando "**show platform hardware fed switch ative fwd-asic resource tcam table nfl_acl asic <asic number>**

> **Tip**: Se houver uma ACL de porta (PACL), a entrada será criada no ASIC para o qual a interface está mapeada. No caso de uma ACL de roteador (RACL), a entrada está presente em todos os ASICs.

- Nesta saída, há NFCMD0 e NFCMD1, que são valores de 4 bits. Para calcular a ID do perfil, converta os valores em binários.
- Nesta saída, NFCMD0 é 1, NFCMD1 é 2. Quando convertido em binário: 000100010
- No Cisco IOS-XE 16.12 e posteriores dentro dos 8 bits combinados, os primeiros 4 bits são o ID do perfil e o sétimo bit indica que a pesquisa está ativada. Assim, no exemplo, **0001**0010, o ID do perfil é 1.
- No Cisco IOS XE 16.11 e em versões mais antigas do código, dentro dos 8 bits combinados, os primeiros 6 bits são o ID do perfil e o sétimo bit indica que a pesquisa está ativada. Neste exemplo, **000100**10, a ID do perfil é 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

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

Máscara de fluxo

Execute o comando "**show platform software fed switch ative|standby|member fnf fmask-entry asic <asic number> entry 1" para verificar se a máscara de fluxo está instalada no hardware.** O número de campos-chave também pode ser encontrado aqui.

```
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)
```

Dados de estatísticas de fluxo e descarga de carimbo de data/hora

Execute o comando "**show platform software fed switch ative fnf flow-record asic <asic number> start-index <index number> num-flows <number of flows> para exibir estatísticas de netflow, bem como carimbos de data/hora**

```
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
```

Visibilidade e controle de aplicativo (AVC)

Informações de Apoio

- O Application Visibility and Control (AVC) é uma solução que aproveita o Network-Based Recognition Version 2 (**NBAR2**), o **NetFlow V9** e várias ferramentas de relatório e gerenciamento (**Cisco Prime**) para ajudar a classificar aplicativos por meio da inspeção detalhada de pacotes (DPI).
- O AVC pode ser configurado em portas de acesso com fio para switches autônomos ou

pilhas de switches.
- O AVC também pode ser usado em controladores sem fio da Cisco para identificar aplicativos baseados em DPI e marcá-lo com um valor de DSCP específico. Ele também pode coletar várias métricas de desempenho sem fio, como uso de largura de banda em termos de aplicativos e clientes.

Desempenho e escala

Desempenho: cada membro do switch pode lidar com 500 conexões por segundo (CPS) a menos de 50% de utilização da CPU. Além dessa taxa, o serviço AVC não é garantido.

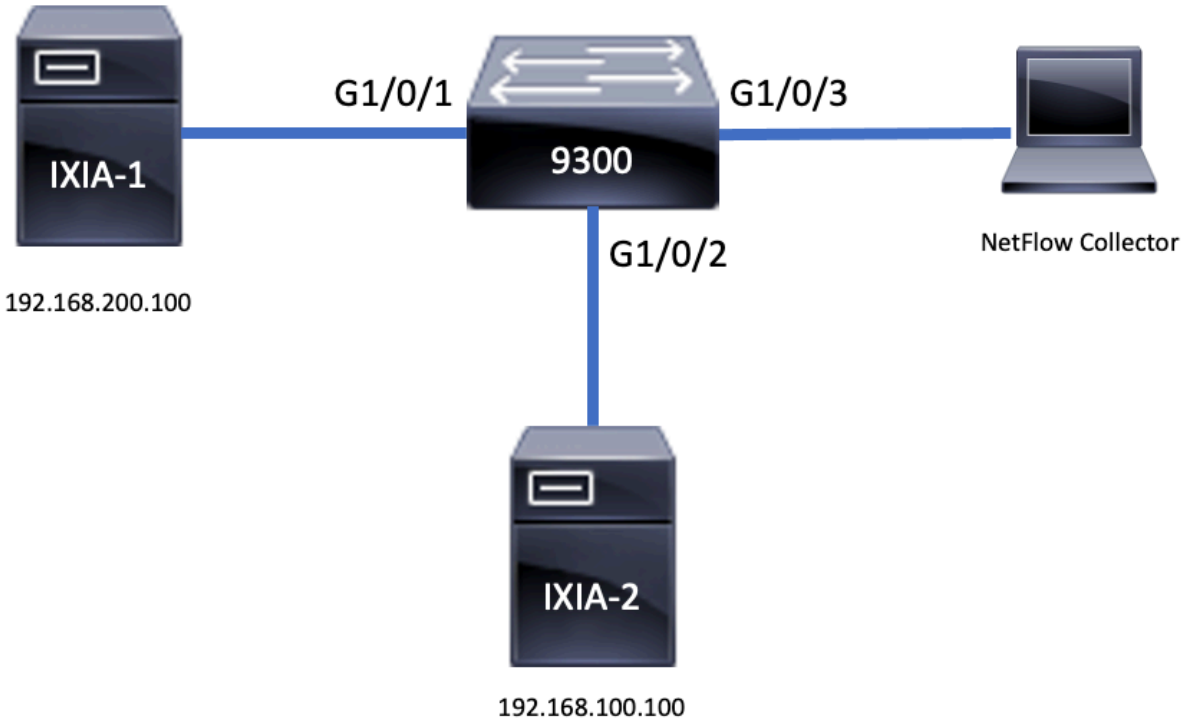
Escala: capacidade de lidar com até 5.000 fluxos bidirecionais por 24 portas de acesso (aproximadamente 200 fluxos por porta de acesso).

Restrições de AVC com fio

- O AVC e o Encrypted Traffic Analytics (ETA) não podem ser configurados juntos ao mesmo tempo na mesma interface.
- A classificação de pacote só é suportada para tráfego IPv4 unicast (TCP/UDP).
- A configuração de política de QoS baseada em NBAR só é suportada em portas físicas com fio. Isso inclui portas de acesso e tronco da camada 2 e portas roteadas da camada 3.
- A configuração de política de QoS baseada em NBAR não é suportada em membros do canal de porta, interfaces virtuais do switch (SVIs) ou subinterfaces.
- Classificadores baseados em NBAR2 **(protocolo de correspondência),** suportam apenas ações de QoS de marcação e vigilância.
- O "protocolo correspondente" é limitado a 255 protocolos diferentes em todas as políticas (limitação de hardware de 8 bits)

> **Note**: Esta não é uma lista completa de todas as restrições, consulte o guia de configuração AVC apropriado para sua plataforma e versão de código.

Diagrama de Rede



Componentes

A configuração do AVC é composta de **três** componentes principais que compõem a solução:

Visibilidade: Descoberta de protocolo

- A descoberta de protocolo é obtida por meio do NBAR, que fornece estatísticas por interface, direção e bytes/pacotes de aplicativo.
- A descoberta de protocolo é habilitada para uma interface específica através da configuração de interface: **ip nbar protocol-discovery**

Como mostrado na saída, como habilitar a descoberta de protocolo:

```
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
```

Controle: QoS baseada em aplicativo

Quando comparado ao QoS tradicional que corresponde ao endereço IP e à porta UDP/TCP, o AVC obtém melhor controle por meio de QoS baseado em aplicativo, o que permite que você corresponda ao aplicativo e fornece um controle mais granular por meio de ações de QoS, como marcação e vigilância.

- As ações são executadas em tráfego agregado (não por fluxo)
- A QoS baseada em aplicativo é obtida pela criação de um mapa de classe, correspondência de um protocolo e, em seguida, criação de um mapa de política.
- A política de QoS baseada em aplicativo é anexada a uma interface.

Como mostrado na saída, exemplo de configuração para QoS baseada em aplicativo:

```
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 baseado em aplicativo

O FNF AVC com fio suporta dois tipos de registros de fluxo predefinidos: **registros de fluxo bidirecional herdados** e novos **registros de fluxo direcional**.

Os registros de fluxo bidirecional controlam as estatísticas de aplicativos cliente/servidor.

Como mostrado na saída, exemplo de configuração de um registro de fluxo bidirecional.

```
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
```

Os registros direcionais são estatísticas de aplicativo para entrada/saída.

Como mostrado na saída, exemplos de configuração de registros direcionais de entrada e saída:

> **Observação**: o comando "**match interface input**" especifica uma correspondência para a interface de entrada. O comando "**match interface output**" especifica uma correspondência para a interface de saída. O comando "**match application name**" é obrigatório para suporte a 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
```

Exportador de fluxo

Crie um exportador de fluxo para definir parâmetros de exportação.

Como mostrado na saída, exemplo de configuração do exportador de fluxo:

```
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
!
```

Monitor de fluxo

Crie um monitor de fluxo para associá-lo a um registro de fluxo.

Como mostrado na saída, exemplo de configuração do monitor de fluxo:

```
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
```

Associar o Monitor de Fluxo a uma Interface

Você pode **anexar** até dois monitores AVC diferentes com registros predefinidos diferentes a uma interface ao mesmo tempo.

Como mostrado na saída, exemplo de configuração do monitor de fluxo:

```
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

Atualização do pacote de protocolo NBAR2 Dynamic Hitless

Pacotes de protocolo são pacotes de software que atualizam o suporte ao protocolo NBAR2 em um dispositivo sem substituição do software Cisco no dispositivo. Um pacote de protocolos contém informações sobre aplicativos oficialmente suportados pelo NBAR2 que são compilados e empacotados juntos. Para cada aplicativo, o pacote de protocolos inclui informações sobre assinaturas de aplicativos e atributos de aplicativos. Cada versão de software tem um pacote de protocolo integrado incluído.

- O NBAR2 fornece uma maneira de atualizar o pacote de protocolo sem qualquer tráfego ou interrupção de serviço e sem a necessidade de modificar a imagem de software nos dispositivos
- Os pacotes de protocolo NBAR2 estão disponíveis para download no Cisco Software Center neste URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

Atualização do pacote de protocolo NBAR2

Antes da instalação de um novo pacote de protocolo, você deve copiar o pacote de protocolo para a memória flash em todos os switches. Para carregar o novo pacote de protocolos, use o comando "**ip nbar protocol-pack flash:<Pack Name>**

Você não precisa recarregar o(s) switch(es) para que a atualização NBAR2 ocorra.

Como mostrado na saída, exemplo de configuração de como carregar o pacote de protocolo NBAR2:

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

Para reverter para o pacote de protocolo interno, use o comando "**default ip nbar protocol-pack**"

Como mostrado na saída, exemplo de configuração de como reverter de volta para o pacote de protocolo interno:

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

Exibir informações do pacote de protocolo NBAR2

Para exibir informações sobre pacotes de protocolos, use os comandos listados:

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

Como mostrado na saída, exemplo de saída desses comandos:

```
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
```

Aplicativos personalizados NBAR2

O NBAR2 suporta o uso de protocolos personalizados para identificar aplicativos personalizados. Protocolos personalizados suportam protocolos e aplicativos que NBAR2 não suporta atualmente.

Eles podem incluir o seguinte:

- Aplicativo específico para uma organização

- Aplicativos específicos de uma região

O NBAR2 fornece uma maneira de personalizar manualmente aplicativos por meio do comando **ip nbar custom<*myappname*>**.

Note: Os aplicativos personalizados têm precedência sobre os protocolos incorporados

Há vários tipos de personalização de aplicativos:

Personalização de protocolo genérico

- HTTP
- SSL
- DNS

Composto: Personalização baseada em vários protocolos -**server-name**

Personalização de Camada 3/Camada 4

- endereço IPv4
- Valores de DSCP
- Portas TCP/UDP
- Direção de origem ou destino do fluxo

Deslocamento de Byte: Personalização baseada em valores de byte específicos no payload

Personalização de HTTP

A personalização de HTTP pode ser baseada em uma combinação de campos HTTP de:

- **cookie** - Cookie HTTP
- **host** - Nome do host do Servidor de Origem que contém o recurso
- **método** - método HTTP
- **referenciador** - Endereço do qual a solicitação de recurso foi obtida
- **url** - Caminho Uniform Resource Locator
- **user-agent** - Software usado pelo agente que envia a solicitação
- **versão** - versão HTTP
- **via** - HTTP via campo

Exemplo de aplicação personalizada chamada MYHTTP que usa o host HTTP "*mydomain.com" com ID de seletor 10.

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

Personalização de SSL

A personalização pode ser feita para tráfego criptografado SSL por meio de informações extraídas da SNI (Indicação de Nome de Servidor) ou do CN (Nome Comum) SSL.

Exemplo de aplicativo personalizado chamado MYSSL que usa nome exclusivo SSL "mydomain.com" com ID de seletor 11.

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

Personalização de DNS

O NBAR2 examina o tráfego de solicitação e resposta DNS e pode correlacionar a resposta DNS a uma aplicação. O endereço IP retornado da resposta DNS é armazenado em cache e usado para fluxos de pacotes posteriores associados a esse aplicativo específico.

O comando **nbar** *customapplication*-**namednsdomain-***nameidapplication*-**idé usado para personalização DNS.** Para estender um aplicativo, use o comando **nbar** *customapplication*-**namedns domain-***nameddomain*-**nameextendsexisting-application**.

Exemplo de aplicativo personalizado chamado MYDNS que usa o nome de domínio DNS "mydomain.com" com ID de seletor 12.

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

Personalização composta

O NBAR2 fornece uma maneira de personalizar aplicativos com base em nomes de domínio que aparecem em HTTP, SSL ou DNS.

Exemplo de aplicativo personalizado chamado MYDOMAIN que usa o nome de domínio HTTP, SSL ou DNS "mydomain.com" com ID de seletor 13.

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

Personalização de L3/L4

A personalização da Camada 3/Camada 4 é baseada na tupla de pacotes e sempre é combinada no primeiro pacote de um fluxo.

Exemplo de aplicação personalizada LAYER4CUSTOM que combina endereços IP 10.56.1.10 e 10.56.1.11, TCP e DSCP ef com ID de seletor 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
```

Monitorar aplicativos personalizados

Para monitorar aplicativos personalizados, utilize os comandos show listados:

show ip nbar protocol-id | inc Personalizado

```
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
```

Verificar AVC

Há várias etapas para validar a funcionalidade do AVC, esta seção fornece comandos e exemplo de saída.

Para validar se o NBAR está ativo, você pode executar o comando "**show ip nbar control-plane**"

Áreas principais:

- O estado NBAR deve ser **ativado** em um cenário correto
- O estado de configuração NBAR deve estar **pronto** em um cenário correto

```
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>
```

Valide se cada membro do switch tem um plano de dados ativo com o comando **show platform software fed switch ative|standby|member wdavc function wdavc_stile_cp_show_info_ui**:

O DP ativado deve ser **TRUE** em um cenário correto

```
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
```

Utilize o comando "**show platform software fed switch ative|standby|member wdavc flows** para exibir informações importantes:

```
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
```

Campos-chave:

CurrFlows: Demonstra quantos fluxos ativos são rastreados pelo AVC

Marca d'água: Demonstra o maior número de fluxos historicamente rastreados pelo AVC

TEMPO LIMITE S: Tempo limite de inatividade com base no aplicativo identificado

NOME DO APLICATIVO: Aplicativo identificado

TIPO DE FLUXO: Real Flow indica que ele foi criado como resultado de dados de entrada. Pre Flow indica que esse fluxo é criado como resultado de dados de entrada. Os pré-fluxos são usados para fluxos de mídia antecipados

TIPO DE TUPLA: Os fluxos reais são sempre tuplas cheias. Os pré-fluxos são tuplas cheias ou semituplas

DESVIO: Se definido como TRUE, indica que não são necessários mais pacotes pelo software para identificar esse fluxo

FINAL: Se definido como TRUE, indica que o aplicativo não muda mais para esse fluxo

IGNORAR PKT: Quantos pacotes foram necessários para chegar à classificação final

#PKTS: Quantos pacotes foram realmente lançados para o software para esse fluxo

Ver detalhes adicionais sobre os fluxos atuais, você pode utilizar o comando "**show platform software fed switch ative 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
```

Campos-chave

ID de I/F: Especifica o ID da interface

SEG DIR: especifica a direção de entrada da saída

DIR FIF: determina se esta é ou não a direção do iniciador de fluxo

NFL HDL: ID de fluxo em hardware

Para visualizar a entrada no hardware execute o comando "**show platform software fed switch ative fnf flow-record asic <number> start-index <number> num-flows <number of flows>**

> **Note**: Para escolher o ASIC, é a instância do ASIC para a qual a porta está mapeada. Para identificar o ASIC, utilize o comando "**show platform software fed switch ative|standby|member ifm mappings**" O índice inicial pode ser definido como "0" se você não estiver interessado em um fluxo específico. Caso contrário, o índice inicial precisa ser especificado. Para núm-fluxos, que especifica o número de fluxos que podem ser exibidos, máximo de 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
```

Procurar vários erros e avisos no caminho de dados

Utilize o comando "**show platform software fed switch ative|standby|member wdavc function wdavc_ft_show_stats_ui | inc err|warn|não** exibir possíveis erros da tabela de fluxo:

```
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
```

Utilize o comando **"show platform software fed switch ative wdavc function wdavc_stile_stats_show_ui | inc err"** para visualizar todos os possíveis erros de 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
```

Verifique se os pacotes são clonados para a CPU

Utilize o comando **"show platform software fed switch ative punt cpuq 21 | inc received"** para verificar se os pacotes são clonados para a CPU para processamento NBAR:

> **Note**: No laboratório, esse número não foi incrementado.

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

Identificar o congestionamento da CPU

Em momentos de congestionamento, os pacotes podem ser descartados antes de serem enviados ao processo WDAVC. Utilize o comando **"show platform software fed switch ative wdavc function fed_wdavc_show_ots_stats_ui"** para validar:

```
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
```

> **Tip**: Para limpar o contador punt drop, utilize o comando "**show platform software fed switch ative wdavc function fed_wdavc_clear_ots_stats_ui"**

Identificar problemas de escala

Se não houver entradas FNF livres no hardware, o tráfego não estará sujeito à classificação NBAR2. Utilize o comando "**show platform software fed switch ative fnf sw-table-size asic <number> shadow 0"** para confirmar:

> **Note**: Os fluxos criados são específicos do switch e do núcleo básico quando são criados. O número do switch (ativo, standby etc.) precisa ser especificado de acordo. O número ASIC inserido está vinculado à respectiva interface. Use "**show platform software fed switch ative|standby|member ifm mappings"** para determinar o ASIC que corresponde à interface. Para a opção de sombra, sempre use "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
```

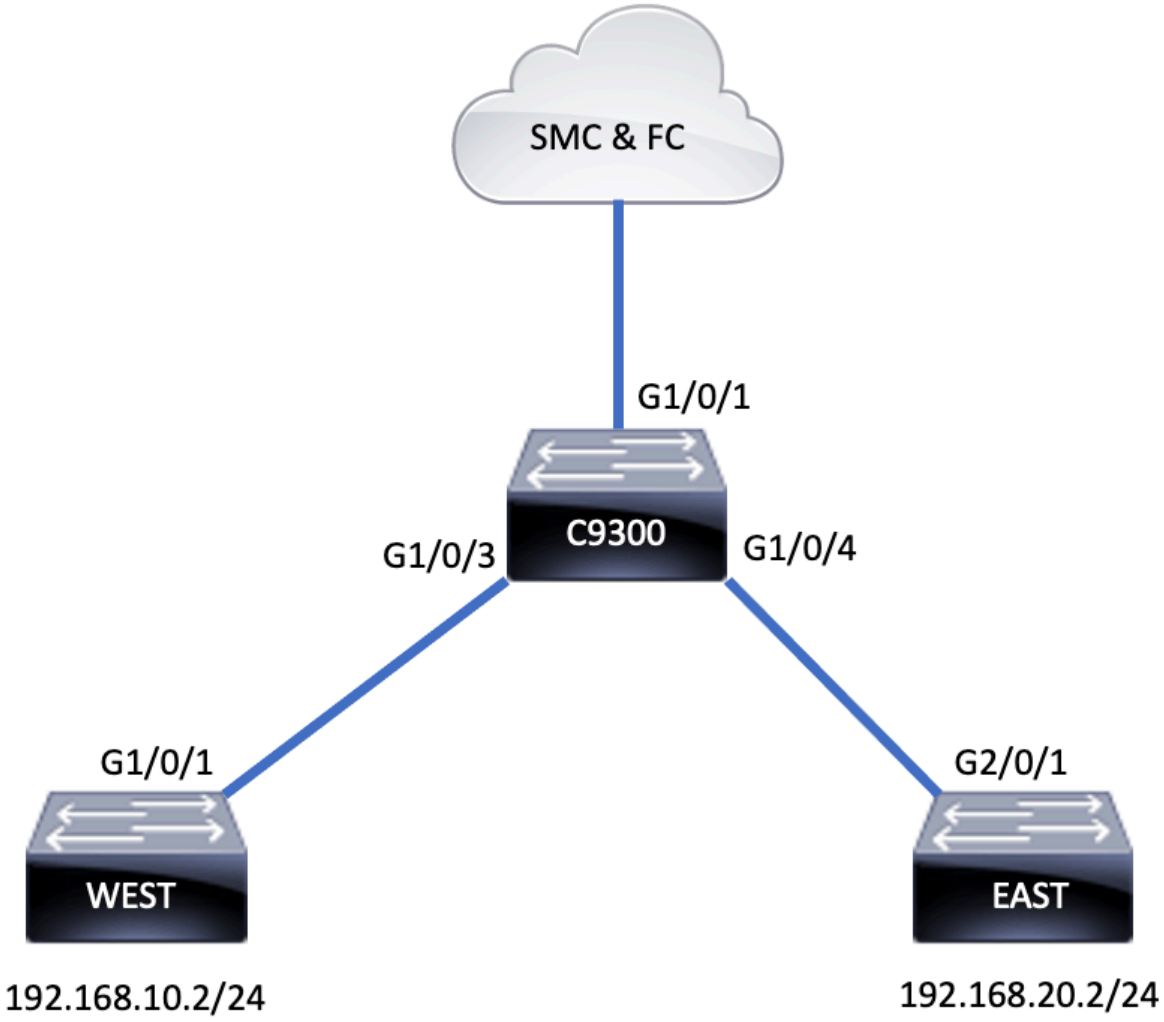
```
INGRESS TotalSeen=1 MaxEntries=1 MaxOverflow=0
EGRESS TotalSeen=0 MaxEntries=0 MaxOverflow=0

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

Análise de tráfego criptografado (ETA)

Informações de Apoio

- O ETA se concentra na identificação da comunicação de malware em tráfego criptografado por meio de monitoramento passivo, extração de elementos de dados relevantes e uma combinação de modelagem comportamental e aprendizagem automática com segurança global baseada em nuvem.
- O ETA aproveita a telemetria do NetFlow, bem como a detecção de malware criptografado e a conformidade criptográfica, e envia esses dados para o Cisco Stealthwatch.
- A ETA extrai dois elementos de dados principais: o Pacote de dados inicial (IDP - Initial Data Packet) e a Sequência de comprimento e hora do pacote (SPLT - Sequence of Packet Length and Time).

Diagrama de Rede



Componentes

O ETA é composto por vários componentes diferentes que são usados em conjunto para criar a solução ETA:

- NetFlow - padrão que define os elementos de dados exportados pelos dispositivos de rede que descrevem os fluxos na rede.
- Cisco Stealthwatch - Aproveita o poder da telemetria de rede que inclui NetFlow, IPFIX, logs de proxy e inspeção profunda de pacotes brutos - para fornecer visibilidade de rede avançada, inteligência de segurança e análise.
- Cisco Cognitive Intelligence - Localiza atividades mal-intencionadas que passaram pelos controles de segurança ou foram inseridas por canais não monitorados e dentro do ambiente de uma empresa.
- Encrypted Traffic Analytics - O recurso Cisco IOS XE que usa algoritmos comportamentais avançados para identificar padrões de tráfego mal-intencionados por meio da análise de metadados de fluxo de entrada de tráfego criptografado, detecta possíveis ameaças ocultas no tráfego criptografado.

Note: Esta parte do documento se concentra apenas na configuração e verificação de ETA e NetFlow no switch da série Catalyst 9000 e não cobre a implantação do Stealthwatch Management Console (SMC) e do Flow Collector (FC) no Cognitive Intelligence Cloud.

Restrições

- A implantação do ETA requer o DNA Advantage para funcionar
- O ETA e um analisador de porta comutada (SPAN) de transmissão (TX) não são suportados na mesma interface.

Esta não é uma lista inclusiva, consulte o guia de configuração apropriado para o switch e a versão do código para todas as restrições.

Configuração

Como mostrado na saída, ative o ETA no switch globalmente e defina o destino de exportação do fluxo:

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

Tip: Você DEVE usar a porta 2055, não use outro número de porta.

Em seguida, configure o Flexible NetFlow como mostrado na saída:

Configurar registro de fluxo

```
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
```

Configurar o Monitor de Fluxo

```
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
```

Configurar registro de fluxo

```
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
```

Aplicar Monitor de Fluxo

```
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
```

Ativar ETA nas interfaces do switch

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

Verificar

Verifique se o monitor ETA "eta-mon" está ativo. Confirme se o status está alocado através do 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
```

Verifique se o cache ETA está preenchido. Quando o NetFlow e o ETA estiverem configurados na mesma interface, utilize "show flow monitor <nome do monitor> cache" em vez de "show flow monitor eta-mon cache", pois a saída de "show flow monitor eta-mon cache" está vazia:

```
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
```

Valide se os fluxos são exportados para o SMC e FC com o 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
```

Confirme se o SPLT e o IDP são exportados para o FC com o comando "**show platform software fed switch ative 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
```

Valide quais interfaces estão configuradas para et-analytics com o 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
```

Use o comando "**show platform software et-analytics global**" para exibir um estado global de 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
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.