Entender o AVC no Catalyst 9800 Wireless LAN Controller

Contents

Introdução

Este documento descreve o Application Visibility and Control (AVC) em um Cisco Catalyst 9800 WLC que permite o gerenciamento preciso do tráfego de aplicativos.

Pré-requisito

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do Cisco WLC 9800.
- Conhecimento básico de AP de modo de conexão local e flexível.
- Os pontos de acesso devem ser compatíveis com AVC. (Não aplicável com AP de modo local)
- Para que a parte de controle do AVC (QoS) funcione, o recurso de visibilidade de aplicativo com FNF precisa ser configurado.

Informações sobre Application Visibility and Control (AVC)

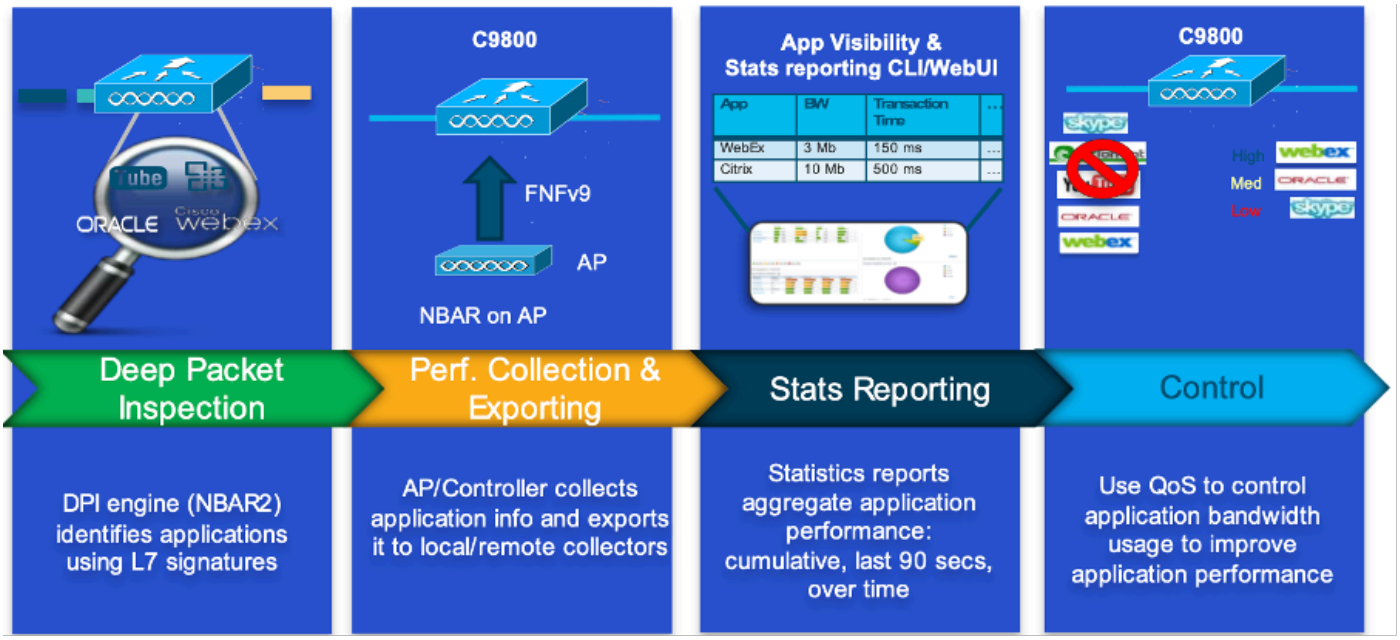
O Application Visibility and Control (AVC) é a abordagem líder da Cisco para a tecnologia de inspeção profunda de pacotes (DPI) em redes com e sem fio. Com o AVC, você pode executar análises em tempo real e criar políticas para reduzir efetivamente o congestionamento da rede, minimizar o dispendioso uso do link de rede e evitar atualizações desnecessárias da infraestrutura. Resumindo, o AVC capacita os usuários a alcançar um nível totalmente novo de reconhecimento e modelagem de tráfego por meio do Network Based Application Recognition (NBAR). Os pacotes NBAR executados no WLC 9800 são usados para DPI e os resultados são relatados usando o Flexible NetFlow (FNF).

Além da visibilidade, o AVC oferece a capacidade de priorizar, bloquear ou acelerar diferentes tipos de tráfego. Por exemplo, os administradores podem criar políticas que priorizem aplicativos de voz e vídeo para garantir a qualidade de serviço (QoS) ou limitar a largura de banda disponível para aplicativos não essenciais durante o horário comercial de pico. Ele também pode ser integrado a outras tecnologias da Cisco, como o Cisco Identity Services Engine (ISE) para políticas de aplicativos baseadas em identidade e o Cisco Catalyst Center para gerenciamento centralizado.

Como o AVC funciona

O AVC utiliza tecnologias avançadas como FNF e mecanismo NBAR2 para DPI. Analisando e identificando fluxos de tráfego usando o mecanismo NBAR2, fluxos específicos são marcados com o protocolo ou aplicativo reconhecido. O controlador coleta todos os relatórios e os apresenta por meio de comandos show, interface do usuário da Web ou mensagens de exportação adicionais do NetFlow para coletores externos do NetFlow, como o Prime.

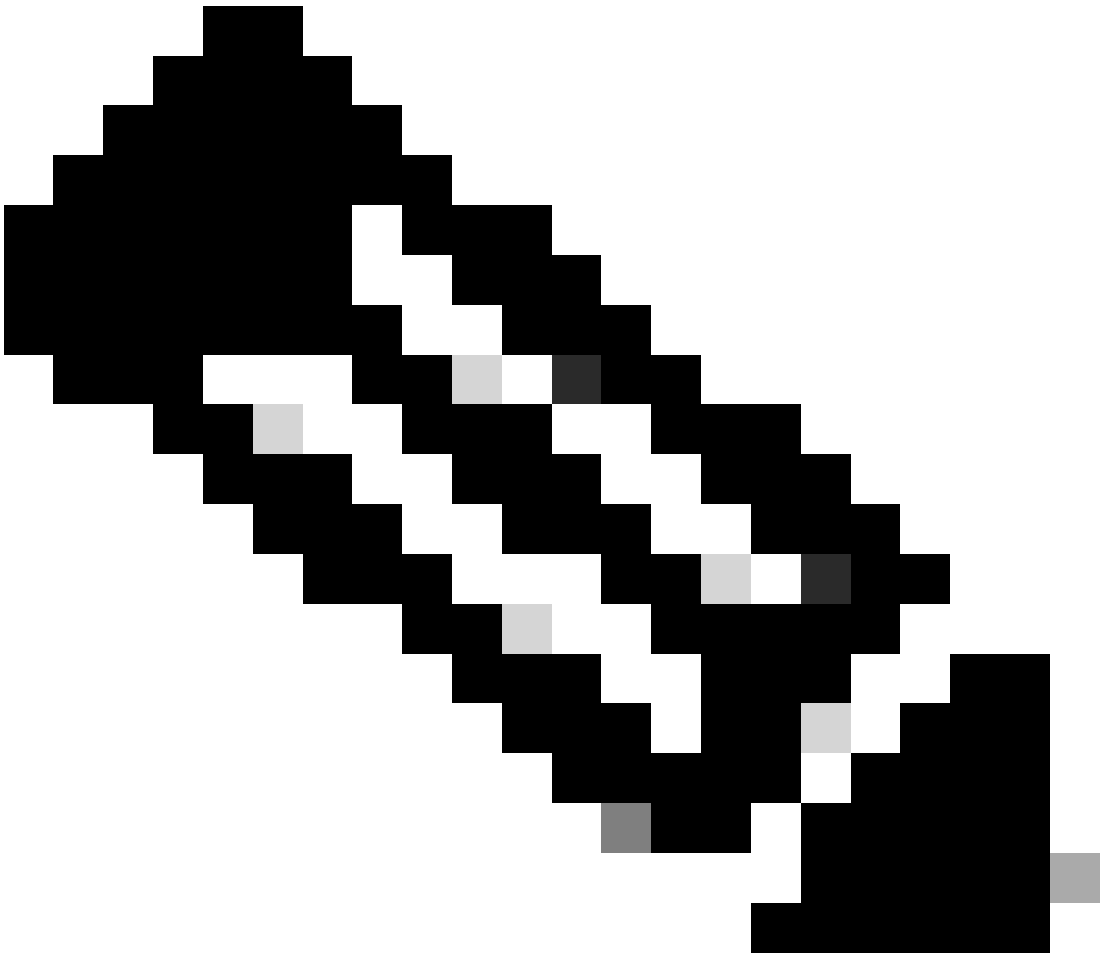
Uma vez estabelecida a visibilidade do aplicativo, os usuários podem criar regras de controle com mecanismos de vigilância para clientes configurando a qualidade de serviço (QOS).



Mecanismo de funcionamento do AVC

Reconhecimento de aplicativo baseado em rede (NBAR)

O NBAR é um mecanismo integrado na WLC 9800, que é usado para executar o DPI para identificar e classificar uma grande variedade de aplicativos executados em uma rede. Ele pode reconhecer e classificar um grande número de aplicativos, incluindo aplicativos criptografados e mapeados dinamicamente por portas, que são geralmente invisíveis às tecnologias tradicionais de inspeção de pacotes.



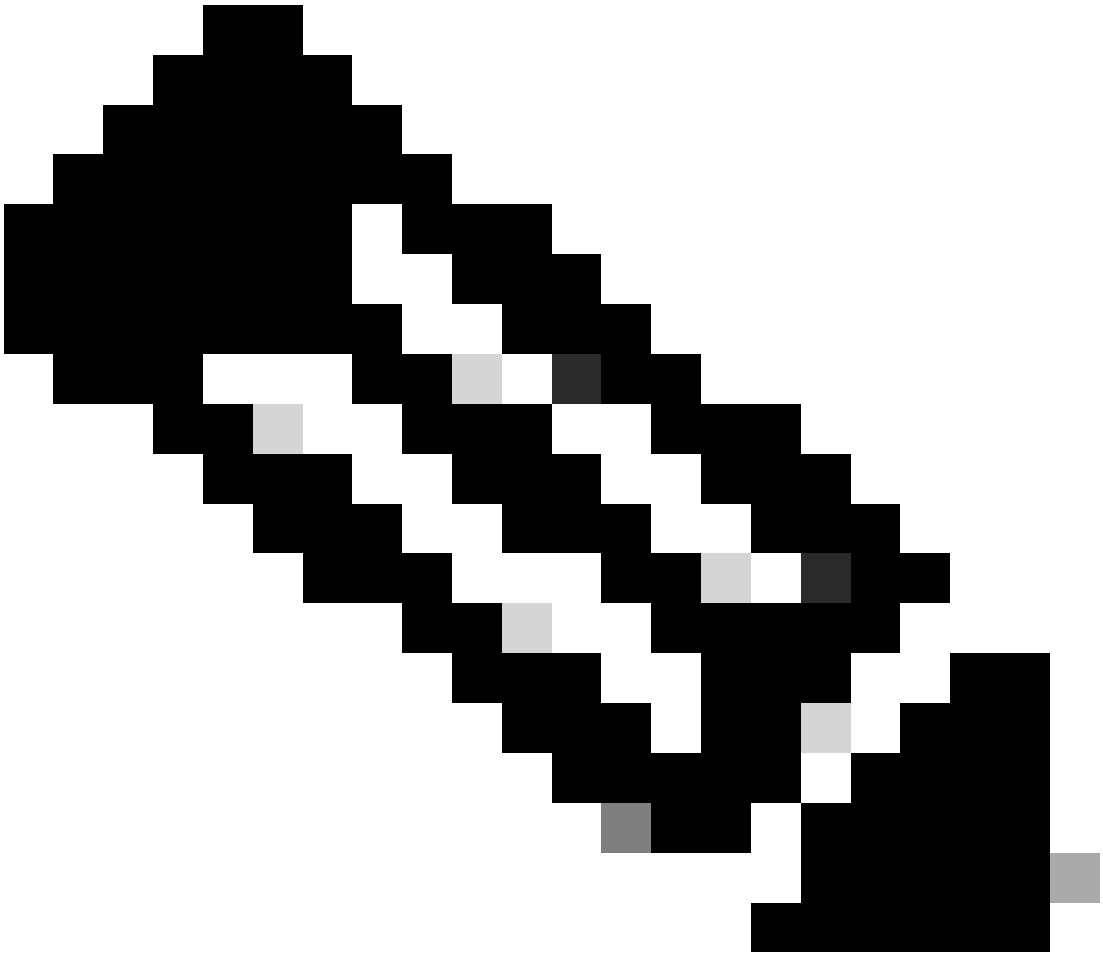
Observação: para aproveitar o NBAR no Catalyst 9800 WLC, é necessário ativá-lo e configurá-lo corretamente, frequentemente em conjunto com perfis AVC específicos que definem as ações apropriadas a serem tomadas com base na classificação do tráfego.

O NBAR continua a ser atualizado periodicamente e é importante manter o software da WLC atualizado para garantir que o conjunto de recursos do NBAR permaneça atualizado e eficaz.

Uma lista completa dos protocolos suportados nas versões mais recentes pode ser encontrada em https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

Habilitar protocolo NBAR no perfil de política

```
9800WLC#configure terminal
9800WLC(config)#wireless profile policy AVC_testing
9800WLC(config-wireless-policy)#ip nbar protocol-discovery
9800WLC(config-wireless-policy)#end
```



Observação: o perfil % Policy precisa ser desabilitado antes da execução desta operação.

```
9800WLC#show wireless profile policy detailed AVC_testing | in NBAR
NBAR Protocol Discovery : Enabled
```

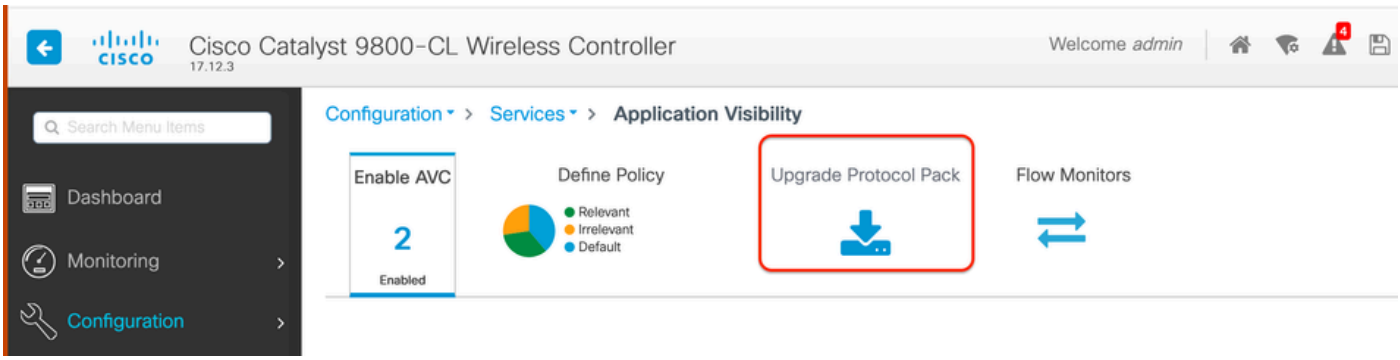
Atualizando o NBAR no 9800 WLC

A WLC 9800 já tem aproximadamente 1.500 aplicativos reconhecíveis. No caso em que um novo aplicativo é lançado, o protocolo para o mesmo será atualizado no NBAR mais recente, que seria necessário fazer o download na página Download de software para o modelo 9800 específico.

Via GUI

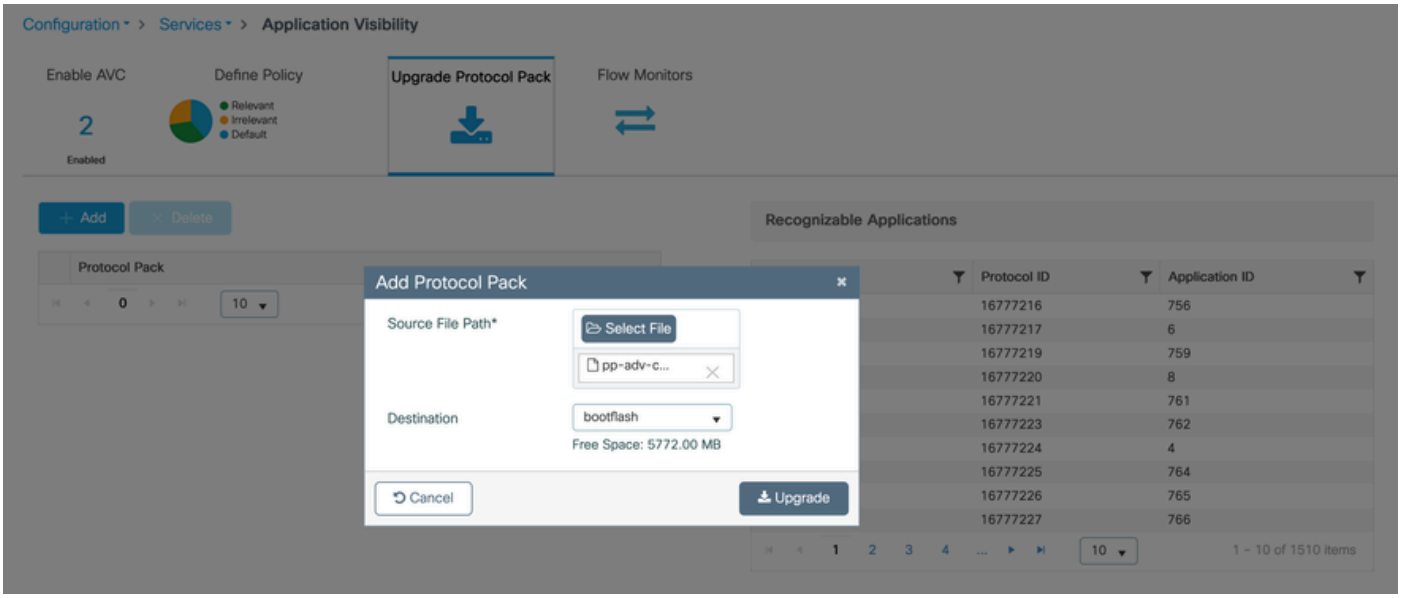
Navegue até Configuration > Services > Application Visibility. Clique em Atualizar Pacote de

Protocolo .



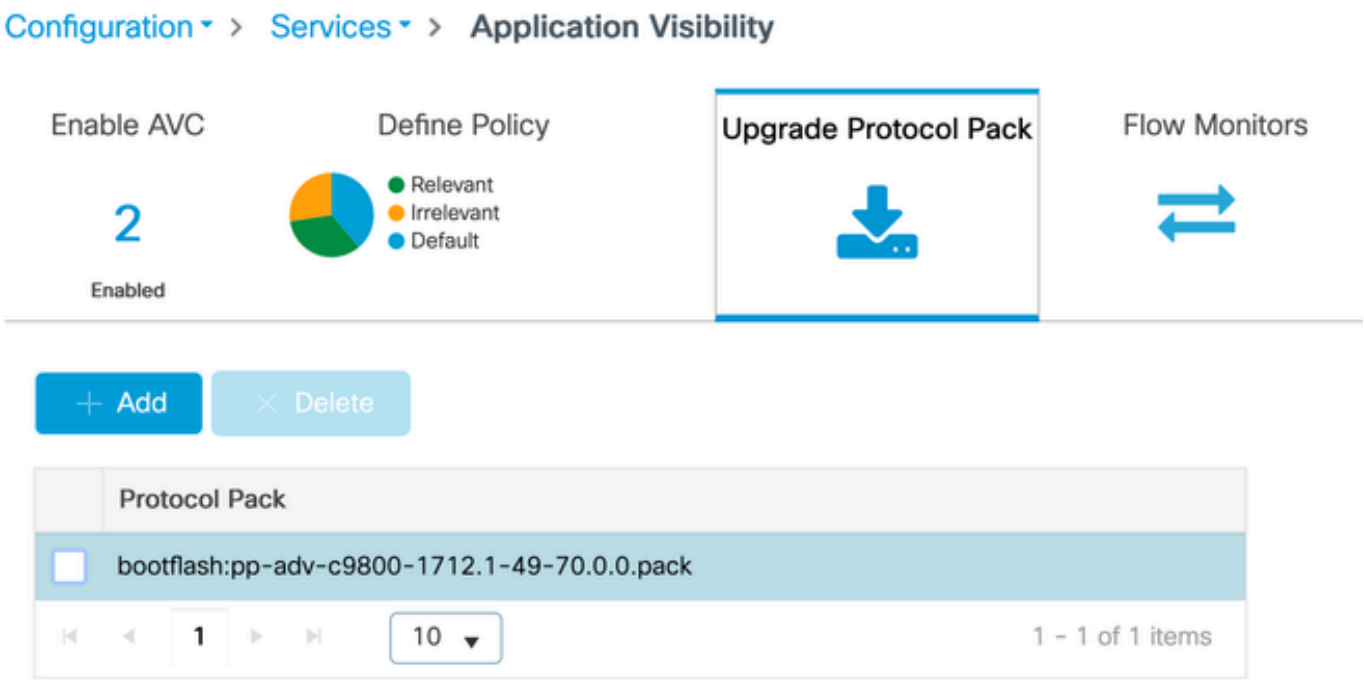
Carregar seção de protocolo no 9800 WLC

Clique em Adicionar, escolha o pacote de protocolos a ser baixado e clique em Atualizar .



Adicionando protocolo NBAR

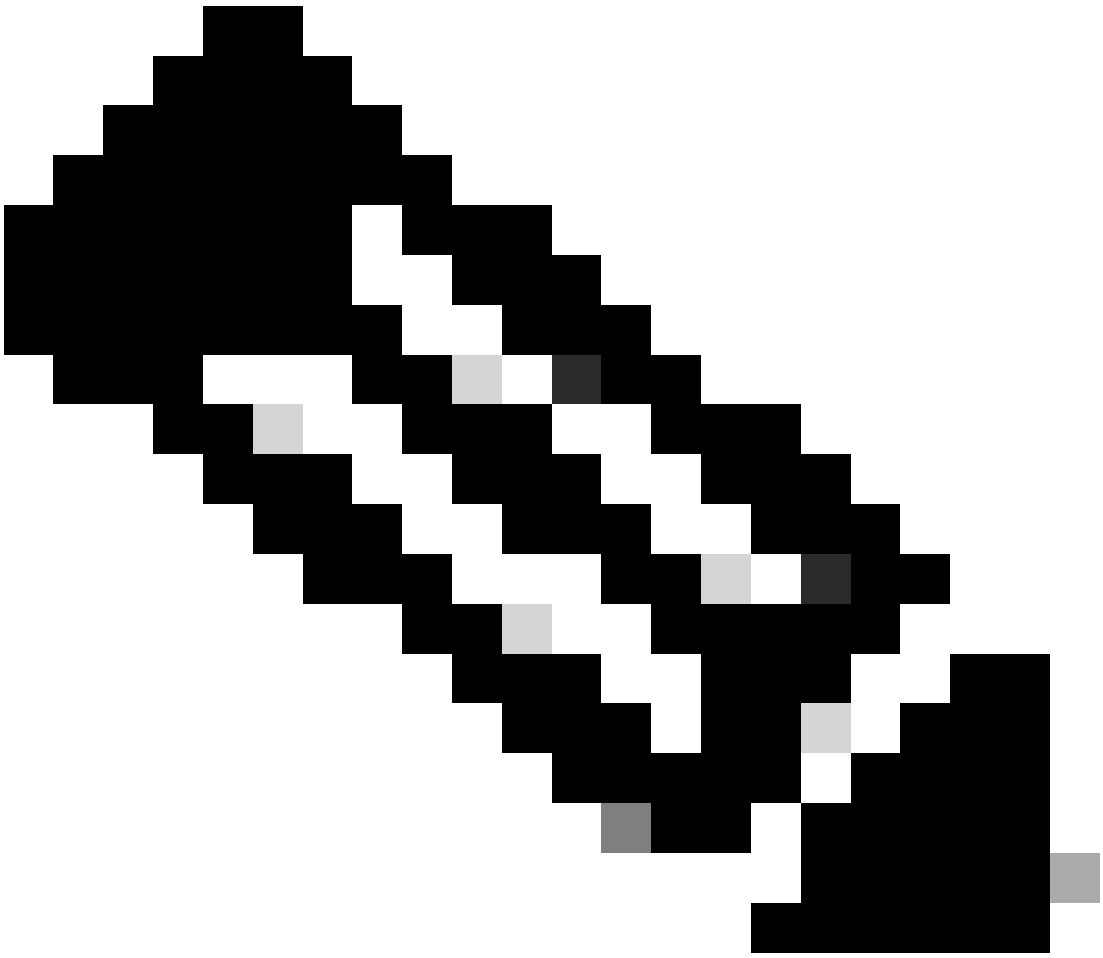
Quando a atualização estiver concluída, você verá o pacote de protocolos adicionado.



Verificação do pacote de protocolo

Via CLI

```
9800WLC#copy tftp://10.10.10.1/pp-adv-c9800-1712.1-49-70.0.0.pack bootflash:
9800WLC#configure terminal
9800WLC(config)#ip nbar protocol-pack bootflash:pp-adv-c9800-1712.1-49-70.0.0.pack

To verify NBAR protocol pack version

9800WLC#show ip nbar protocol-pack active
Active Protocol Pack:
Name: Advanced Protocol Pack
Version: 70.0
Publisher: Cisco Systems Inc.
NBAR Engine Version: 49
Creation time: Tue Jun 4 10:18:09 UTC 2024
File: bootflash:pp-adv-c9800-1712.1-49-70.0.0.pack
State: Active
```



Observação: não haverá interrupção do serviço durante a atualização do pacote de protocolo NBAR.

Netflow

O NetFlow é um protocolo de rede usado para coletar informações de tráfego IP e monitorar dados de fluxo de rede. É usado principalmente para análise de tráfego de rede e monitoramento de largura de banda. Esta é uma visão geral de como o NetFlow funciona nos controladores Cisco Catalyst 9800 Series:

- Coleta de dados: a WLC 9800 coleta dados sobre o tráfego IP que passa por elas. Esses dados incluem informações como endereços IP origem e destino, portas origem e destino, protocolos usados, classe de serviço e a causa do término do fluxo.
- Registros de Fluxo: Os dados coletados são organizados em registros de fluxo. Um fluxo é definido como uma sequência unidirecional de pacotes que compartilham um conjunto de atributos comuns, como o mesmo IP de origem/destino, portas de origem/destino e tipo de

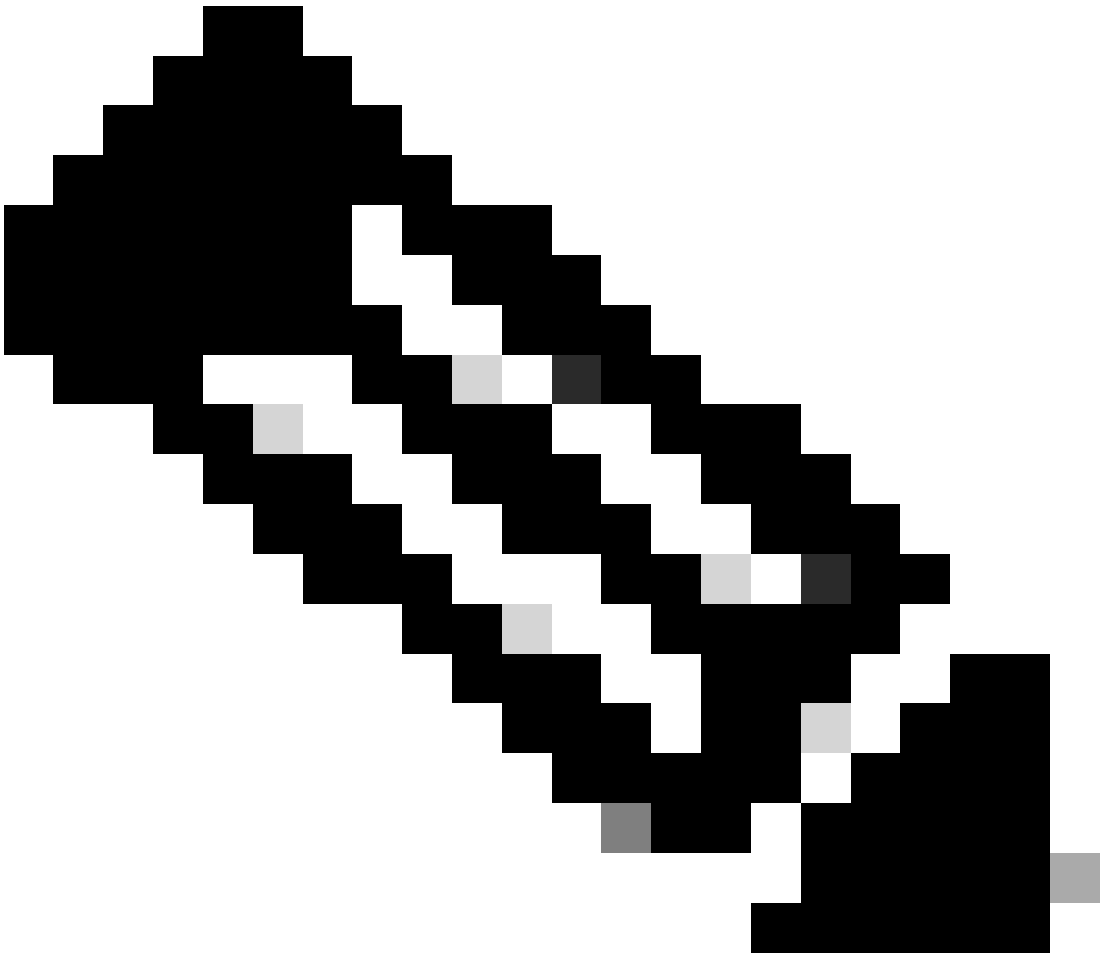
protocolo.
- Exportação de dados: os registros de fluxo são exportados periodicamente do dispositivo habilitado para NetFlow para um coletor NetFlow. O coletor pode ser uma WLC local ou um servidor dedicado ou aplicativo de software que recebe, armazena e processa os dados de fluxo.
- Análise: você pode usar coletores e ferramentas de análise do NetFlow para visualizar padrões de tráfego, identificar largura de banda, detectar fluxos de tráfego incomuns indicativos de violações de segurança, otimizar o desempenho da rede e planejar a expansão da rede.
- Informações específicas de redes sem fio: no contexto de controladores sem fio, o NetFlow pode incluir informações adicionais específicas de redes sem fio, como o SSID, nomes de AP, endereços MAC de clientes e outros detalhes relevantes para o tráfego Wi-Fi.

Flexible Netflow

O Flexible NetFlow (FNF) é uma versão avançada do NetFlow tradicional e é suportado pelos Cisco Catalyst 9800 Series Wireless LAN Controllers (WLCs). Ele fornece mais opções de personalização para rastreamento, monitoramento e análise de padrões de tráfego de rede. Os principais recursos do Flexible NetFlow no Catalyst 9800 WLC incluem:

- Personalização: o FNF permite que os usuários definam quais informações desejam coletar do tráfego de rede. Isso inclui uma ampla gama de atributos de tráfego, como endereços IP, números de porta, carimbos de data/hora, contagens de pacotes e bytes, tipos de aplicativos e muito mais.
- Visibilidade aprimorada: ao aproveitar o FNF, os administradores obtêm visibilidade detalhada dos tipos de tráfego que fluem pela rede, o que é essencial para o planejamento de capacidade, tarifação de rede baseada em uso, análise de rede e monitoramento de segurança.
- Independência de protocolo: o FNF é flexível o suficiente para suportar vários protocolos além do IP, tornando-o adaptável a diferentes tipos de ambientes de rede.

No Catalyst 9800 WLC, o FNF pode ser configurado para exportar registros de fluxo para um coletor NetFlow externo ou um aplicativo de análise. Esses dados podem ser usados para solução de problemas, planejamento de rede e análise de segurança. A configuração FNF envolve a definição de um registro de fluxo (o que coletar), um exportador de fluxo (para onde enviar os dados) e a anexação do monitor de fluxo (que vincula o registro e o exportador) às interfaces apropriadas.



Observação: o FNF pode enviar 17 registros de dados diferentes (conforme definido no RFC 3954) para o coletor Netflow de terceiros externo, como Stealthwatch, Solarwinds e outros, que são: Tag de Aplicativo, Endereço Mac do Cliente, endereço MAC do AP, WlanID, IP de Origem, IP de Destino, Porta de Origem, Porta de Destino, Protocolo, Hora de Início do Fluxo, Hora de Término do Fluxo, Direção, Saída de Pacote, Contagem de Bytes, ID da VLAN (Modo local) - Gerenciamento/Cliente e TOS - Valor DSCP

Monitor de fluxo

Um monitor de fluxo é um componente usado em conjunto com o Flexible NetFlow (FNF) para capturar e analisar dados de tráfego de rede. Ele desempenha um papel crucial no monitoramento e na compreensão dos padrões de tráfego para gerenciamento de rede, segurança e solução de problemas. O monitor de fluxo é essencialmente uma instância aplicada de FNF que coleta e rastreia dados de fluxo com base em critérios definidos. Ele está associado a três elementos principais:

- Registro de Fluxo: define os dados que o monitor de fluxo deve coletar do tráfego de rede.

Ele especifica as chaves (como endereços IP de origem e destino, portas, tipos de protocolo) e os campos não-chave (como contadores de pacotes e bytes, carimbos de data/hora) que serão incluídos nos dados de fluxo.

- Exportador de fluxo: especifica o destino para onde os dados de fluxo coletados devem ser enviados. Ele inclui detalhes como o endereço IP do coletor NetFlow, o protocolo de transporte (geralmente UDP) e o número da porta de destino onde o coletor está escutando.
- Monitor de fluxo: o próprio monitor de fluxo vincula o registro de fluxo e o exportador de fluxo juntos e os aplica a uma interface ou WLAN para realmente iniciar o processo de monitoramento. Determina como os dados de fluxo devem ser coletados e exportados com base nos critérios definidos no registro de fluxo e no destino definido no exportador de fluxo.

Pontos de acesso suportados pelo AVC

O AVC é suportado apenas nestes pontos de acesso:

- Pontos de acesso Cisco Catalyst 9100 Series
- Access point Cisco Aironet 2800 Series
- Access points Cisco Aironet 3800 Series
- Access points Cisco Aironet 4800 Series

Suporte para diferentes modos de implantação do 9800

Modo de Implantação	WLC 9800	Ponto de acesso Wave 1	Ponto de acesso Wave 2	Ponto De Acesso Wifi 6
Modo local (Central Switching)	Tráfego IPV4: AVC suportado FNF suportado Tráfego IPV6: AVC suportado FNF suportado	Processamento no nível da WLC	Processamento no nível da WLC	Processamento no nível da WLC
Modo Flex (Central Switching)	Tráfego IPV4: AVC suportado FNF suportado Tráfego IPV6: AVC suportado FNF suportado	Processamento no nível da WLC	Processamento no nível da WLC	Processamento no nível da WLC
Modo Flex (Switching local)	Processamento no nível do AP	Tráfego IPV4: AVC suportado	Tráfego IPV4: AVC suportado	Tráfego IPV4: AVC suportado

		FNF suportado Tráfego IPV6: AVC suportado FNF Sem Suporte	FNF suportado Tráfego IPV6: AVC suportado FNF suportado	FNF suportado Tráfego IPV6: AVC suportado FNF suportado
Modo local (Malha)	Processamento no nível do AP	Tráfego IPV4: AVC Sem Suporte FNF Sem Suporte Tráfego IPV6: AVC Sem Suporte FNF Sem Suporte	Tráfego IPV4: AVC suportado FNF suportado Tráfego IPV6: AVC suportado FNF suportado	Tráfego IPV4: AVC suportado FNF suportado Tráfego IPV6: AVC suportado FNF suportado

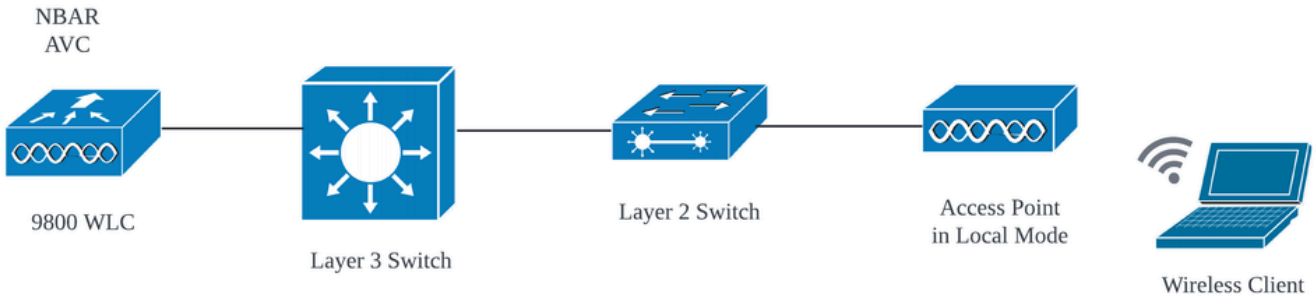
Restrições durante a implementação do AVC no 9800

O Application Visibility and Control (AVC) e o Flexible NetFlow (FNF) são recursos poderosos nos Cisco Catalyst 9800 Series Wireless LAN Controllers que melhoram a visibilidade e o controle da rede. No entanto, há algumas limitações e considerações que devem ser lembradas ao usar esses recursos:

- O roaming de Camada 2 não é suportado nos controladores.
- O tráfego multicast não é suportado.
- Somente os aplicativos reconhecidos com visibilidade de aplicativo podem ser usados para aplicar o controle de QoS.
- Não há suporte para link de dados em campos NetFlow no AVC.
- Não é possível mapear o mesmo perfil de WLAN para o perfil de política não habilitado para AVC e para o perfil de política habilitado para AVC.
- Você não pode usar o perfil de política com mecanismo de comutação diferente para a mesma WLAN para implementar o AVC.
- O AVC não é suportado na porta de gerenciamento (Gig 0/0).
- A configuração da política de QoS baseada em NBAR é permitida apenas em portas físicas com fio. A configuração de política não é suportada em interfaces virtuais, por exemplo, VLAN, canal de porta e outras interfaces lógicas.
- Quando o AVC está ativado, o perfil AVC suporta apenas até 23 regras, o que inclui a regra DSCP padrão. A política AVC não será enviada para o AP, se as regras forem mais de 23.

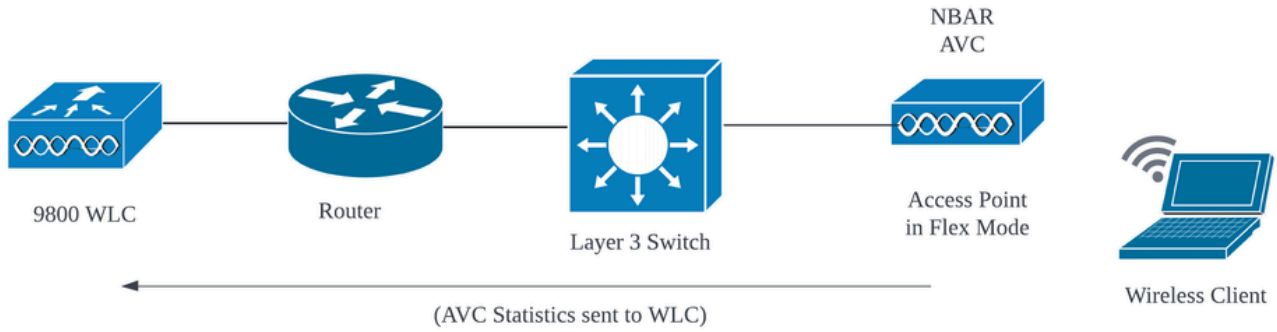
Topologia de rede

AP em modo local



AVC em AP de modo local (switching central)

AP em modo flex



AVC em AP de modo flexível

Configuração do AVC no 9800 WLC

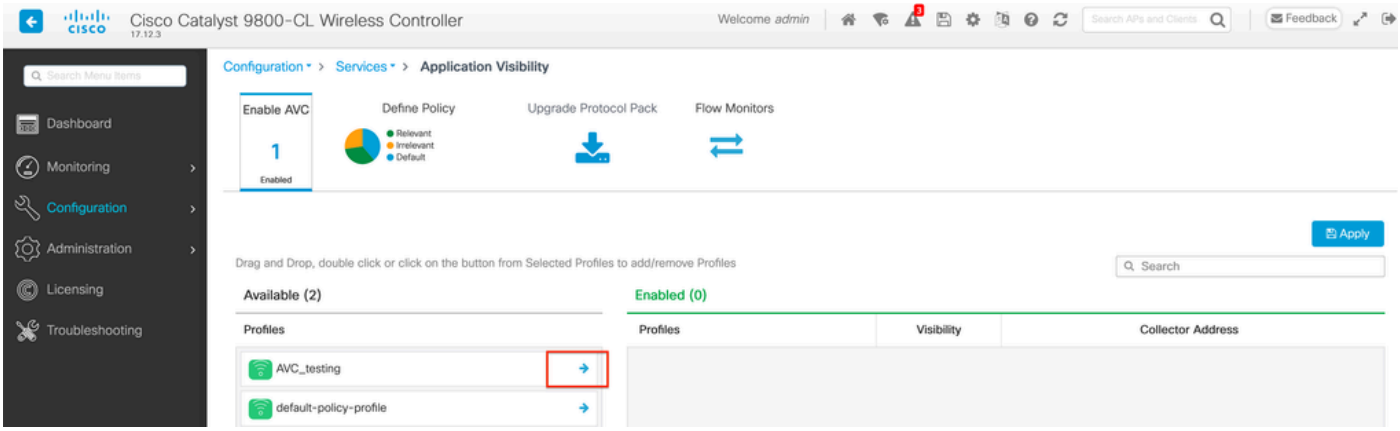
Ao configurar o AVC no 9800 WLC, você pode usá-lo como NetFlow Collector ou pode exportar os dados do NefFlow para o External NetFlow Collector.

Exportador local

Em um Cisco Catalyst 9800 Wireless LAN Controller (WLC), um coletor NetFlow local se refere ao recurso incorporado no WLC que permite coletar e armazenar localmente dados do NetFlow. Esse recurso permite que a WLC execute a análise básica de dados do NetFlow sem a necessidade de exportar os registros de fluxo para um coletor NetFlow externo.

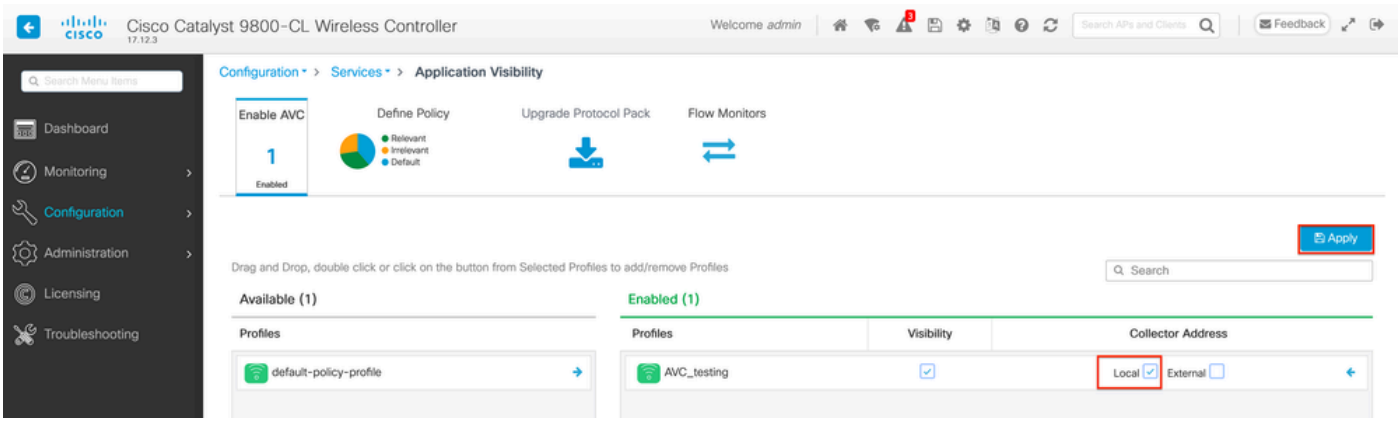
Via GUI

Etapa 1: Para ativar o AVC no SSID específico, navegue até Configuration > Services > Application Visibility. Escolha o perfil de política específico para o qual deseja ativar o AVC.



Ativação do AVC no perfil de política

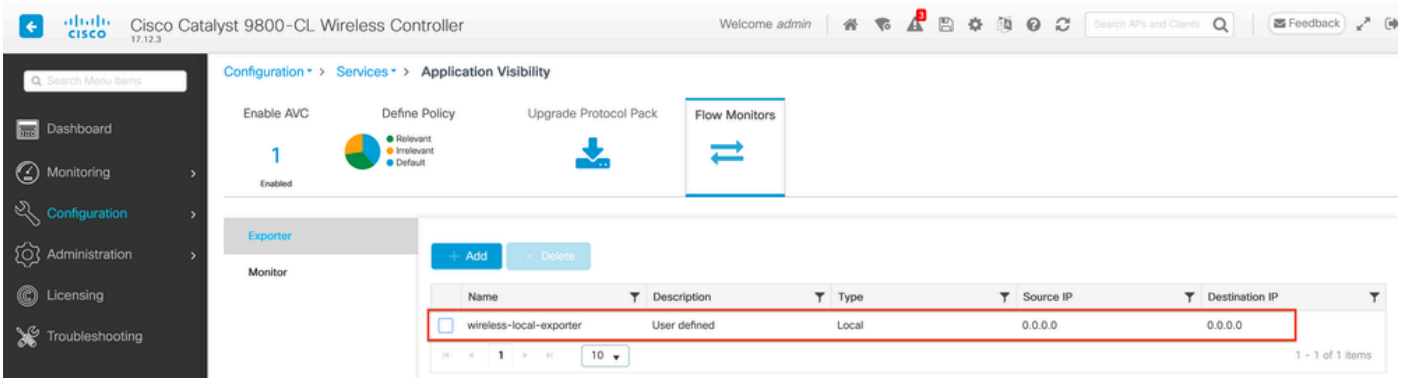
Etapa 2: Selecione Local como o coletor Netflow e clique em Aplicar.



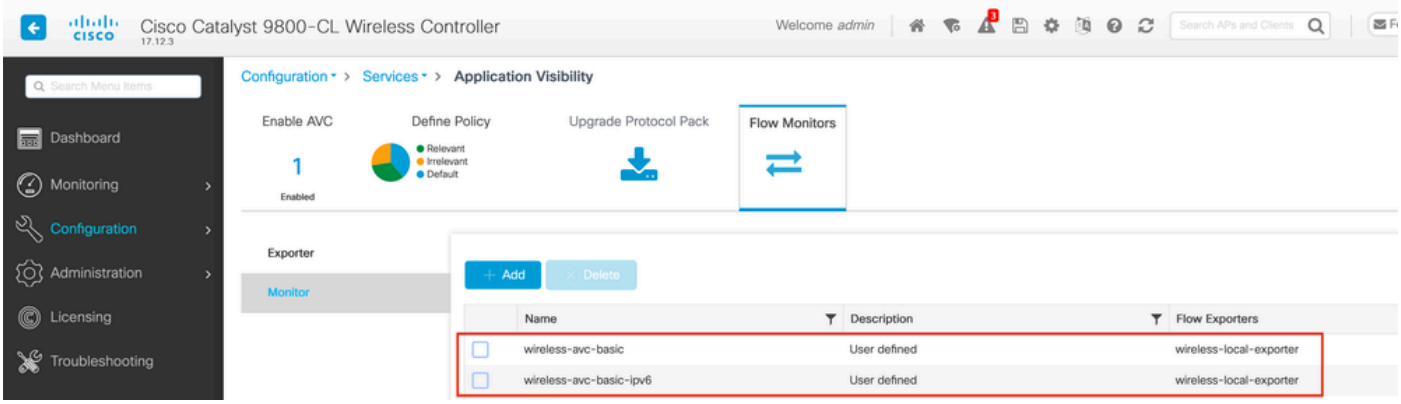
Selecionando o coletor NetFlow local

Observe que as configurações do NetFlow Exporter e do NetFlow foram configuradas automaticamente de acordo com as preferências especificadas depois que você aplica a configuração do AVC.

Você pode validar o mesmo navegando para Configuration > Services > Application Visibility > Flow Monitor > Exporter/Monitor .

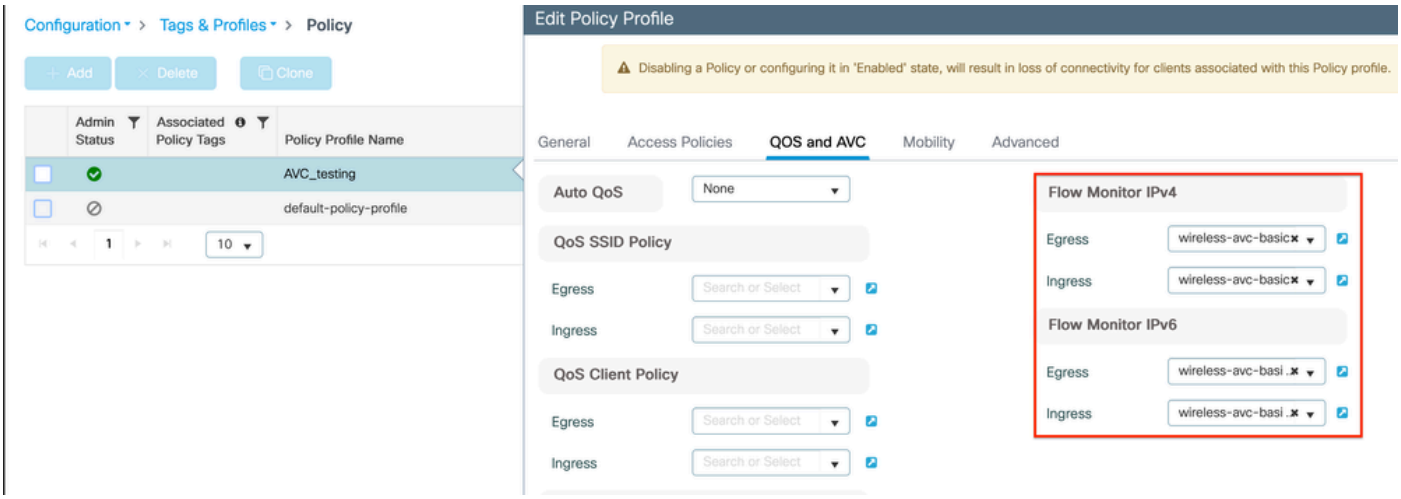


Configuração do coletor de fluxo local no 9800 WLC



Configuração do Monitor de Fluxo com o NetFlow Collector Local

Os monitores de fluxo AVC IPv4 e IPv6 serão associados automaticamente ao perfil de política. Navegue até Configuration > Tags & Profile > Policy . Clique em Policy Profile > AVC e QOS .



Configuração do Monitor de Fluxo no Perfil de Política

Via CLI

Etapa 1: Configure a WLC 9800 como exportador local.

```
9800-Cl-VM#config t
9800-Cl-VM(config)#flow exporter wireless-local-exporter
9800-Cl-VM(config-flow-exporter)#destination local wlc
9800-Cl-VM(config-flow-exporter)#exit
```

Etapa 2: Configure o Monitor de fluxo de rede IPv4 e IPv6 para usar Local(WLC) como NetFlow Exporter.

```
9800-Cl-VM(config)#flow monitor wireless-avc-basic
9800-Cl-VM(config-flow-monitor)#exporter wireless-local-exporter
9800-Cl-VM(config-flow-monitor)#cache timeout active 60
9800-Cl-VM(config-flow-monitor)#record wireless avc ipv4 basic
9800-Cl-VM(config-flow-monitor)#exit
```

```
9800-Cl-VM(config)#flow monitor wireless-avc-basic-ipv6
9800-Cl-VM(config-flow-monitor)#exporter avc_local_exporter
9800-Cl-VM(config-flow-monitor)#cache timeout active 60
9800-Cl-VM(config-flow-monitor)#record wireless avc ipv6 basic
9800-Cl-VM(config-flow-monitor)#exit
```

Etapa 3: Mapeie o Flow Minitor IPv4 e IPv6 no Policy Profile para tráfego de entrada e saída.

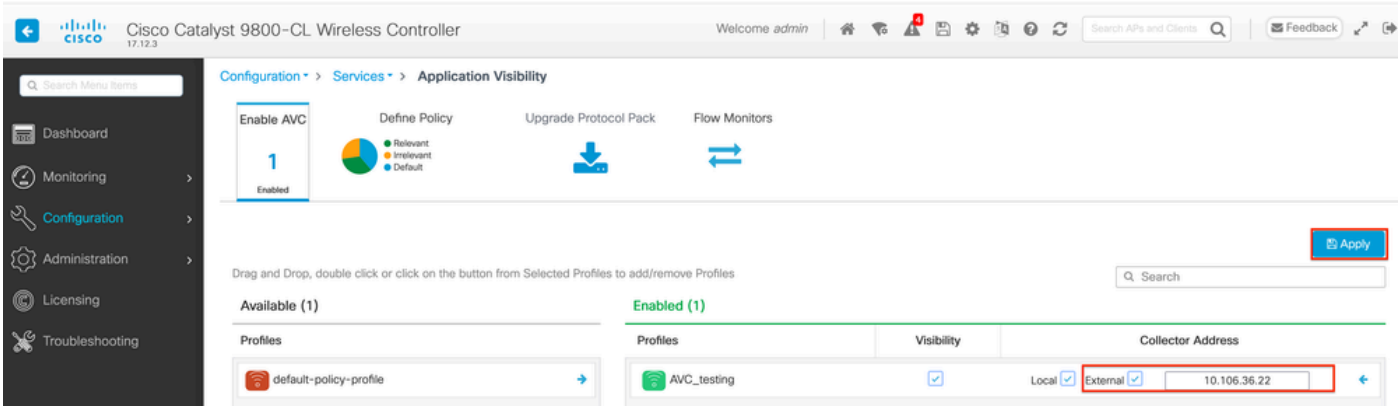
```
9800-Cl-VM(config)#wireless profile policy AVC_Testing
9800-Cl-VM(config-wireless-policy)#shutdown

Disabling policy profile will result in associated AP/Client rejoin

9800-Cl-VM(config-wireless-policy)#ipv4 flow monitor wireless-avc-basic input
9800-Cl-VM(config-wireless-policy)#ipv4 flow monitor wireless-avc-basic output
9800-Cl-VM(config-wireless-policy)#ipv6 flow monitor wireless-avc-basic-ipv6 input
9800-Cl-VM(config-wireless-policy)#ipv6 flow monitor wireless-avc-basic-ipv6 output
9800-Cl-VM(config-wireless-policy)#no shutdown
9800-Cl-VM(config-wireless-policy)#exit
```

Coletor NetFlow externo

Um coletor NetFlow externo, quando usado no contexto de Application Visibility and Control (AVC) em um Cisco Catalyst 9800 Wireless LAN Controller (WLC), é um sistema ou serviço dedicado que recebe, agrega e analisa dados NetFlow exportados do WLC. Você pode Configurar somente o coletor NetFlow externo para monitorar a visibilidade do aplicativo ou pode usá-lo junto com o coletor local também.

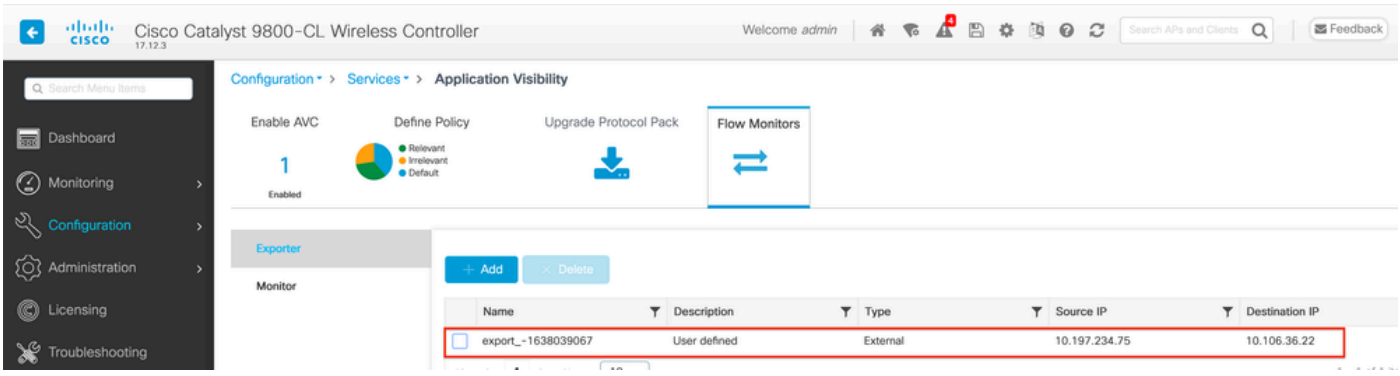
Via GUI

Etapa 1: Para ativar o AVC no SSID específico, navegue até Configuração > Serviços > Visibilidade do aplicativo. Escolha o perfil de política específico para o qual deseja ativar o AVC. Selecione Collector como External e configure o endereço IP do NetFlow Collector como Cisco Prime, SolarWind, StealthWatch e clique em Apply.

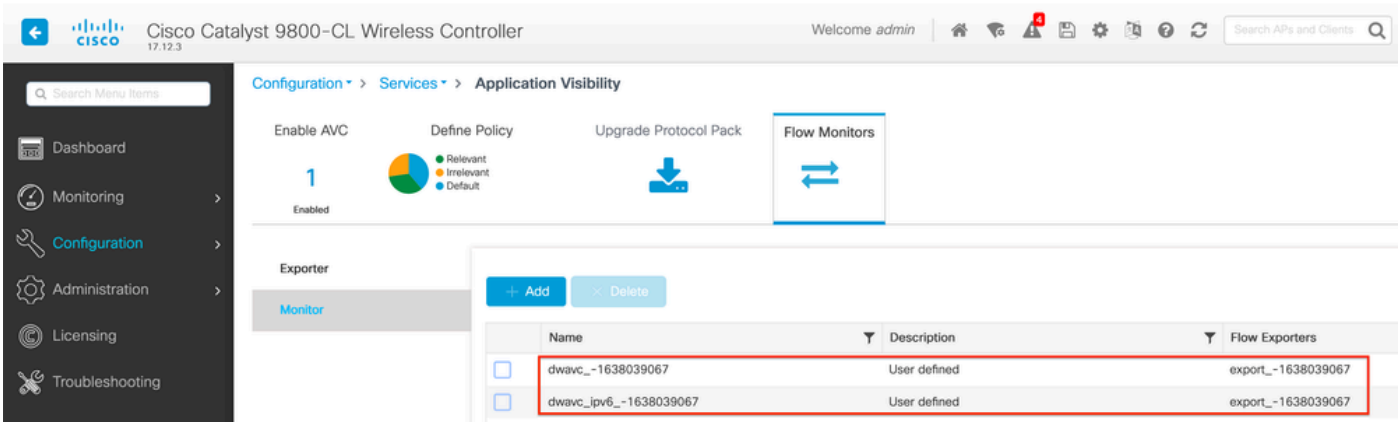


Configuração AVC para coletor NetFlow externo

Observe que, após aplicar a configuração do AVC, as configurações NetFlow Exporter e NetFlow foram automaticamente configuradas com o endereço IP do coletor NetFlow como exportador e o endereço do exportador como 9800 WLC com as configurações de tempo limite padrão e a porta UDP 9995. Você pode validar o mesmo navegando para Configuration > Services > Application Visibility > Flow Monitor > Exporter/Monitor .

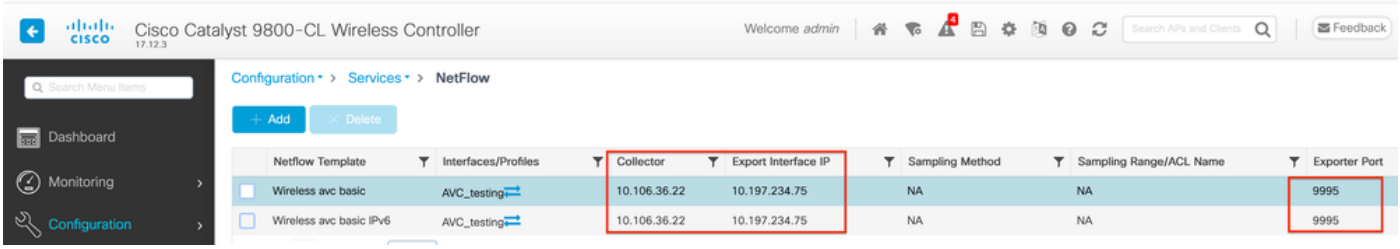


Configuração do coletor NetFlow externo no 9800 WLC



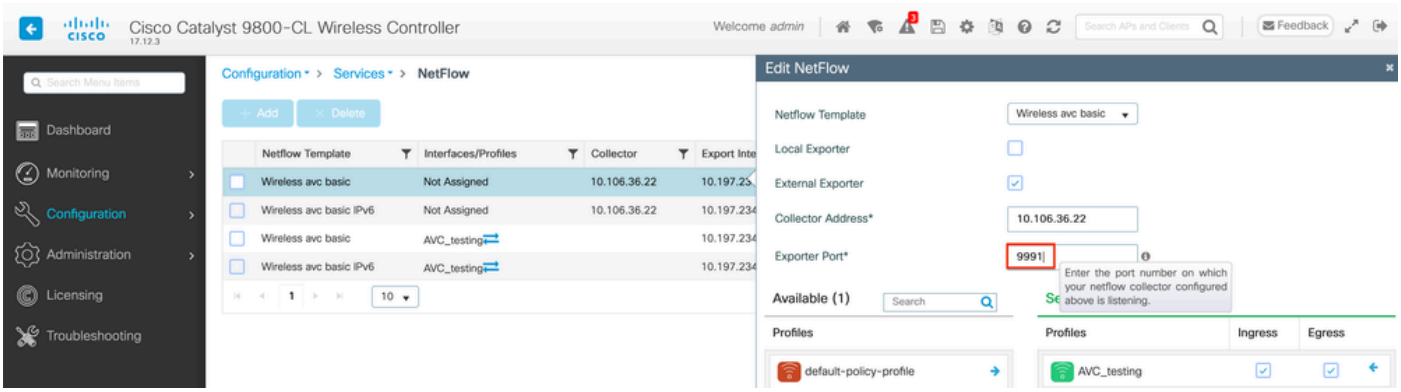
Configuração do Flow Monitor com o NetFlow Collector externo

Você pode verificar a configuração de porta do NetFlow Monitor gerado automaticamente navegando para Configuration > Services > NetFlow .



Observação: se você configurar o AVC via GUI, o NetFlow Exporter gerado automaticamente será configurado para usar a porta UDP 9995. Certifique-se de validar o número de porta que está sendo usado pelo coletor NetFlow.

Por exemplo: se você estiver usando o Cisco Prime como coletor do NetFlow, é essencial definir a porta do exportador como 9991, pois essa é a porta na qual o Cisco Prime escuta o tráfego do NetFlow. Você pode alterar manualmente a Porta do exportador na configuração do NetFlow.



Via CLI

Etapa 1: Configure o endereço IP do coletor NetFlow externo com a interface de origem.

```
9800-Cl-VM#config t
9800-Cl-VM(config)#flow exporter External_Exporter
9800-Cl-VM(config-flow-exporter)#destination 10.106.36.22
9800-Cl-VM(config-flow-exporter)#source $Source_Interface
9800-Cl-VM(config-flow-exporter)#transport udp $Port_Numbet
9800-Cl-VM(config-flow-exporter)#exit
```

Etapa 2: Configure o Monitor de fluxo de rede IPv4 e IPv6 para usar Local(WLC) como NetFlow Exporter.

```
9800-Cl-VM(config)#flow monitor wireless-avc-basic
9800-Cl-VM(config-flow-monitor)#exporter External_Exporter
9800-Cl-VM(config-flow-monitor)#cache timeout active 60
9800-Cl-VM(config-flow-monitor)#record wireless avc ipv4 basic
9800-Cl-VM(config-flow-monitor)#exit

9800-Cl-VM(config)#flow monitor wireless avc ipv6 basic
9800-Cl-VM(config-flow-monitor)#exporter External_Exporter
9800-Cl-VM(config-flow-monitor)#cache timeout active 60
9800-Cl-VM(config-flow-monitor)#record wireless avc ipv6 basic
9800-Cl-VM(config-flow-monitor)#exit
```

Etapa 3: Mapeie o Flow Minitor IPv4 e IPv6 no Policy Profile para tráfego de entrada e saída.

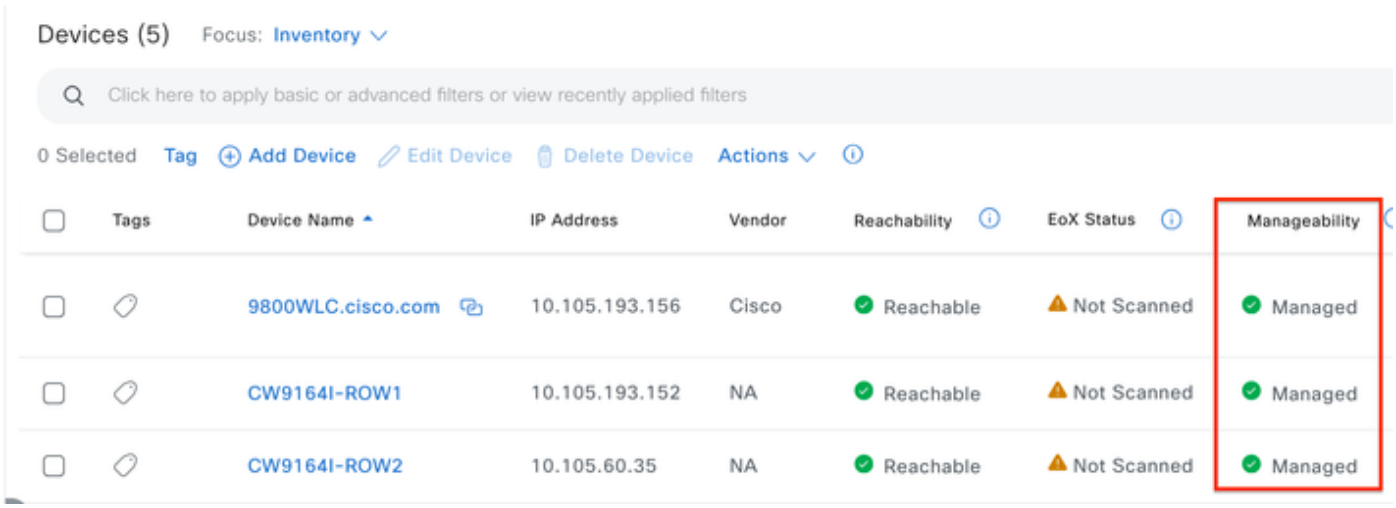
```
9800-Cl-VM(config)#wireless profile policy AVC_Testing
9800-Cl-VM(config-wireless-policy)#shutdown

Disabling policy profile will result in associated AP/Client rejoin

9800-Cl-VM(config-wireless-policy)#ipv4 flow monitor wireless-avc-basic input
9800-Cl-VM(config-wireless-policy)#ipv4 flow monitor wireless-avc-basic output
9800-Cl-VM(config-wireless-policy)#ipv6 flow monitor wireless avc ipv6 basic input
9800-Cl-VM(config-wireless-policy)#ipv6 flow monitor wireless avc ipv6 basic output
9800-Cl-VM(config-wireless-policy)#no shutdown
9800-Cl-VM(config-wireless-policy)#exit
```

Configuração do AVC no 9800 WLC usando o Cisco Catalyst Center

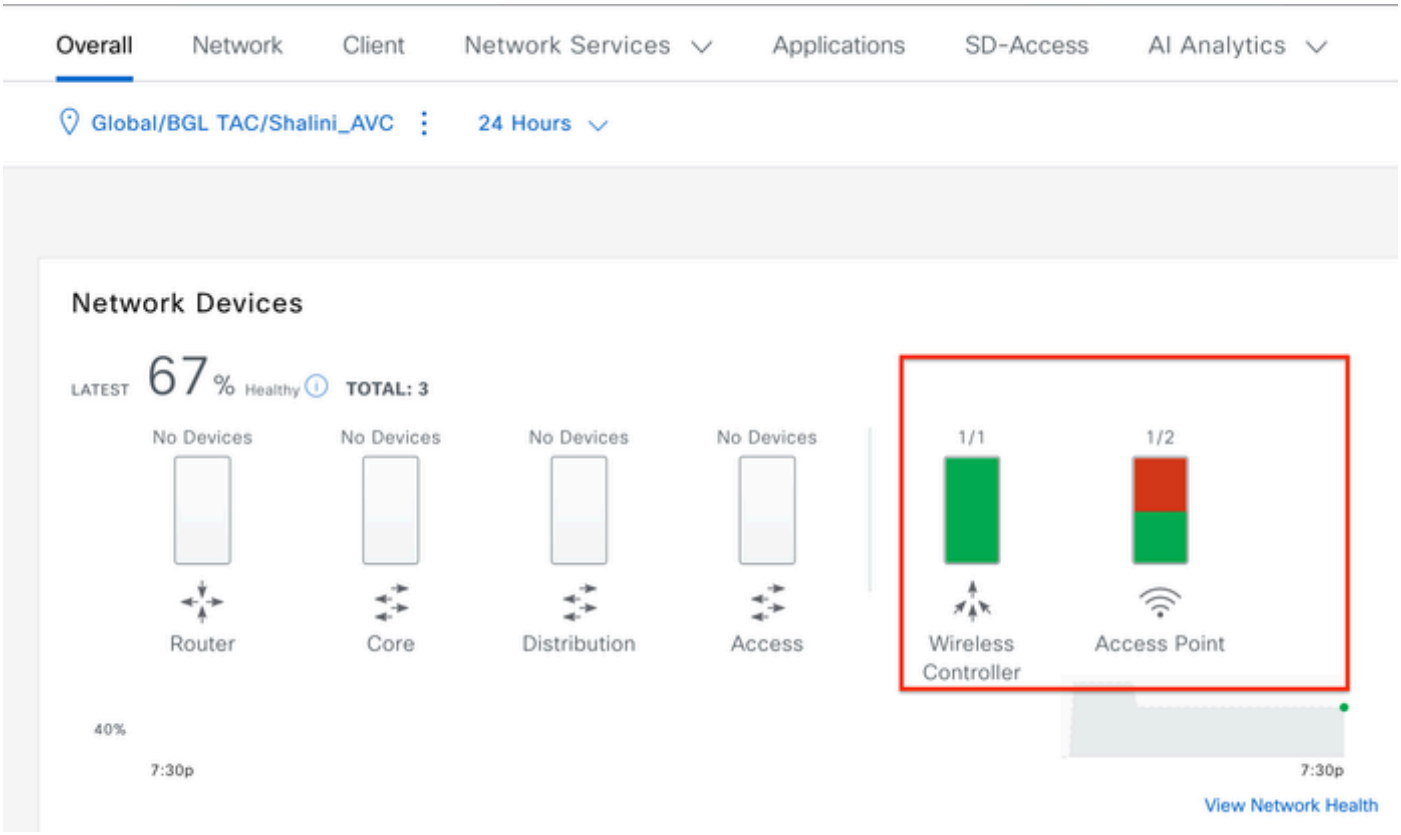
Antes de prosseguir com a configuração do Application Visibility and Control (AVC) em um Cisco Catalyst 9800 Wireless LAN Controller (WLC) através do Cisco Catalyst Center, é importante verificar se a comunicação de telemetria entre o WLC e o Cisco Catalyst Center foi estabelecida com êxito. Certifique-se de que a WLC apareça em um estado gerenciado dentro da interface do Cisco Catalyst Center e que seu status de integridade esteja sendo atualizado ativamente. Além disso, para um monitoramento eficaz do status de integridade, é importante atribuir corretamente a WLC e os pontos de acesso (APs) a seus respectivos locais no Cisco Catalyst Center.

```
9800WLC#show telemetry connection all
Telemetry connections

Index Peer Address              Port  VRF Source Address              State      State Description
----- ------------------------- ----- --- ------------------------- ---------- --------------------
  170 10.78.8.84                25103 0   10.105.193.156            Active     Connection up
```

Verificação de conexão de telemetria no 9800 WLC

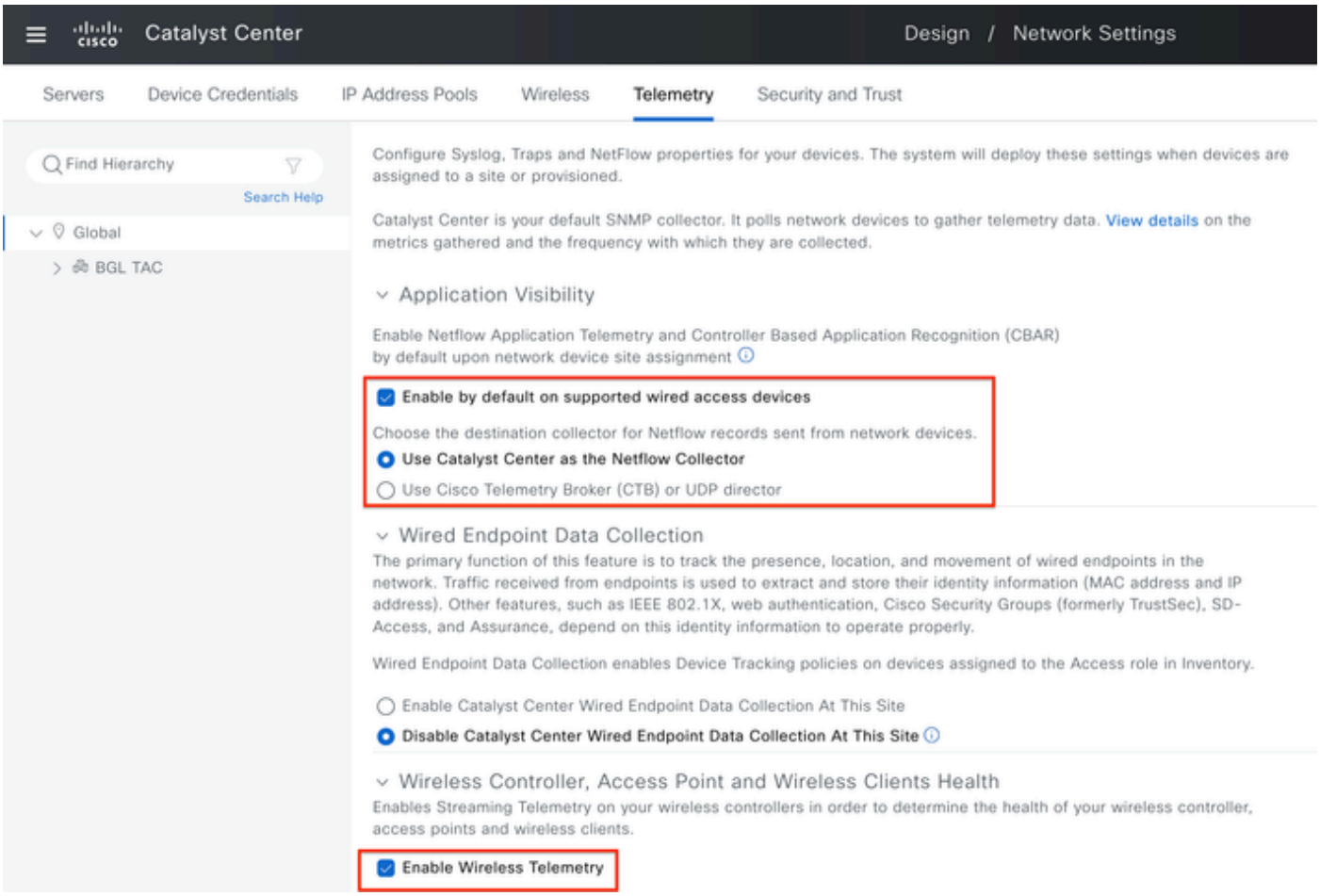


WLC e AP estão em estado gerenciado



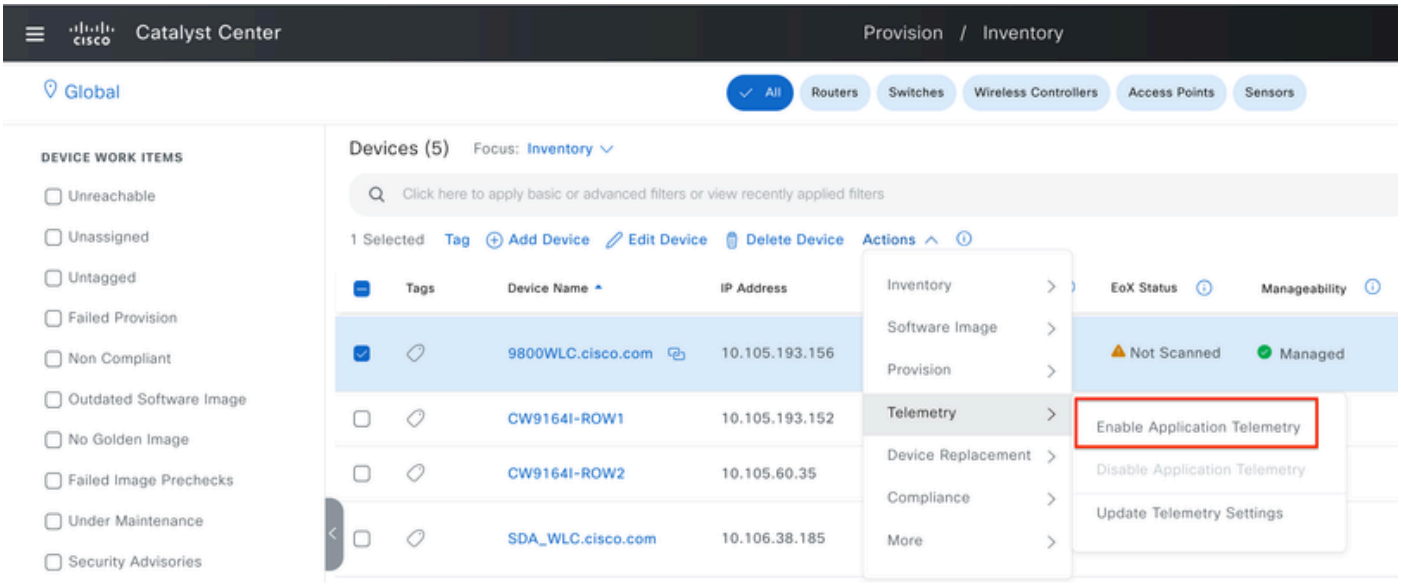
Status de integridade de WLC e AP no Cisco Catalyst Center

Etapa 1: Configure o Cisco Catalyst Center como coletor NetFlow e ative a telemetria sem fio na configuração Global. Navegue até Design > Network Setting > Telemetry e habilite a configuração desejada conforme demonstrado.



Telemetria sem fio e configuração AVC

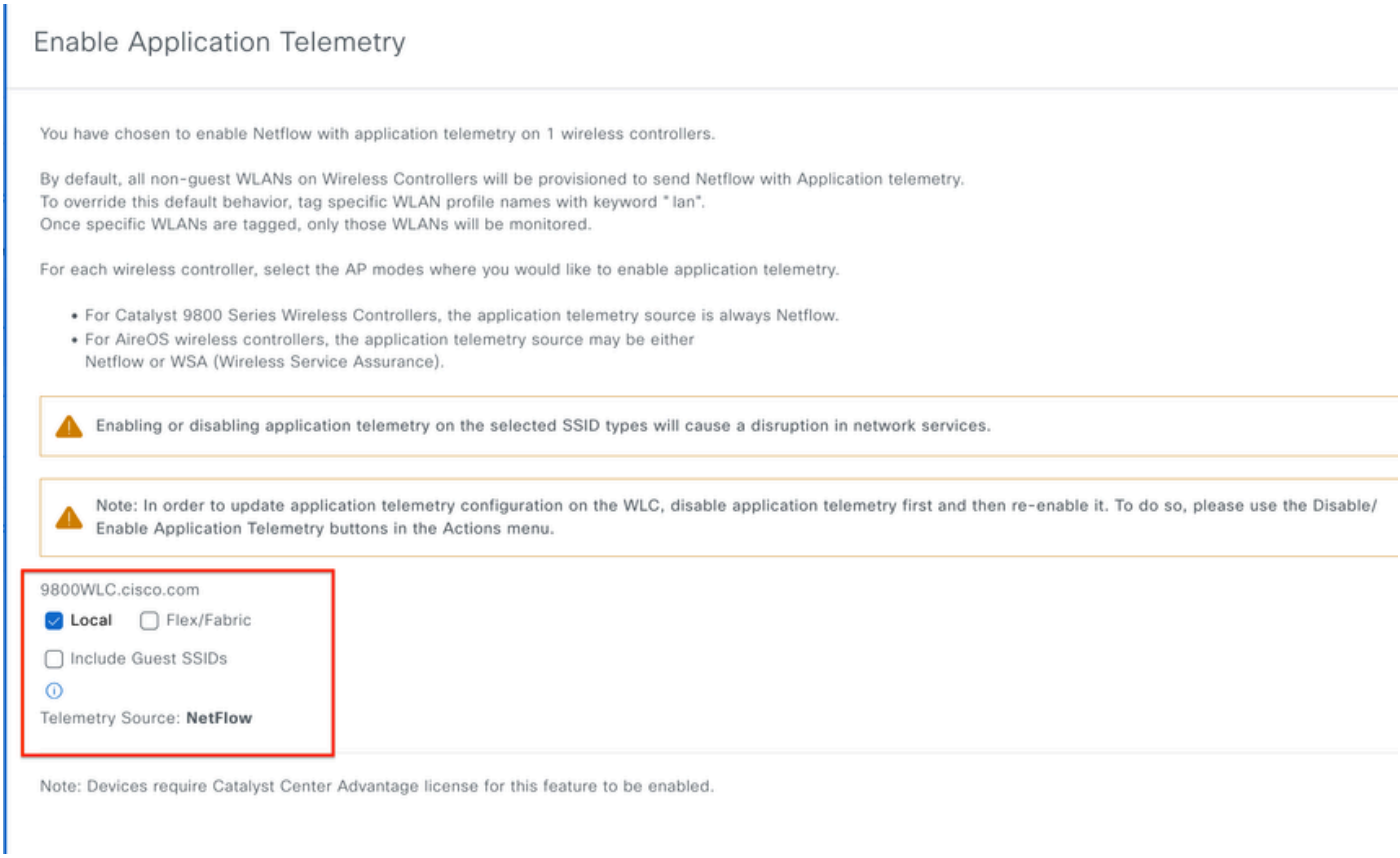
Etapa 2: Ative a telemetria de aplicativos na WLC 9800 desejada para enviar a configuração do AVC na WLC 9800. Para isso, navegue até Provisionar > Dispositivo de rede > Inventário. Escolha a WLC 9800 na qual deseja ativar a Telemetria de Aplicativos e navegue para Ação > Telemetria > Ativar Telemetria de Aplicativos .



Habilitando a telemetria de aplicativos no 9800 WLC

Etapa 3: selecione o Modo de implantação conforme o requisito.
Local: para ativar o AVC no perfil de política local (Central Switching)

Flex/Fabric: para ativar o AVC no perfil de política flexível (switching local) ou SSID baseado em malha.



Seleção do modo de implantação no Cisco Catalyst Center

Etapa 4: Inicia uma tarefa para ativar as configurações do AVC, e a configuração correspondente será aplicada à WLC 9800. Você pode exibir o status navegando até Atividades > Log de auditoria .

Logs de auditoria após habilitar a telemetria no 9800 WLC

O Cisco Catalyst Center implantará as configurações do Flow Exporter e do Flow Monitor, incluindo a porta especificada e outras configurações, e as ativará dentro do perfil de política do modo escolhido, como mostrado abaixo:

```
Configure Cisco Catalyst Center as Flow Exporter:

9800-Cl-VM#config t
9800-Cl-VM(config)#flow exporter avc_exporter
9800-Cl-VM(config-flow-exporter)#destination 10.104.222.201
9800-Cl-VM(config-flow-exporter)#source Vlan10
9800-Cl-VM(config-flow-exporter)#transport udp 6007
9800-Cl-VM(config-flow-exporter)#export-protocol ipfix
9800-Cl-VM(config-flow-exporter)#option vrf-table timeout 300
9800-Cl-VM(config-flow-exporter)#option ssid-table timeout 300
9800-Cl-VM(config-flow-exporter)#option application-table timeout 300
9800-Cl-VM(config-flow-exporter)#option application-attributes timeout 300
9800-Cl-VM(config-flow-exporter)#exit
```

```
Configure 9800 WLC as Local Exporter

9800-Cl-VM#config t
9800-Cl-VM(config)#flow exporter avc_local_exporter
9800-Cl-VM(config-flow-exporter)#destination local wlc
9800-Cl-VM(config-flow-exporter)#exit
```

```
Configure Network Flow Monitor to use both Local(WLC) and Cisco Catalyst Center as Netflow Exporter:

9800-Cl-VM(config)#flow monitor avc_ipv4_assurance
9800-Cl-VM(config-flow-monitor)#exporter avc_exporter
9800-Cl-VM(config-flow-monitor)#exporter avc_local_exporter
9800-Cl-VM(config-flow-monitor)#cache timeout active 60
9800-Cl-VM(config-flow-monitor)#default cache entries
9800-Cl-VM(config-flow-monitor)#record wireless avc ipv4 assurance
9800-Cl-VM(config-flow-monitor)#exit

9800-Cl-VM(config)#flow monitor avc_ipv6_assurance
9800-Cl-VM(config-flow-monitor)#exporter avc_exporter
9800-Cl-VM(config-flow-monitor)#exporter avc_local_exporter
9800-Cl-VM(config-flow-monitor)#cache timeout active 60
9800-Cl-VM(config-flow-monitor)#default cache entries
9800-Cl-VM(config-flow-monitor)#record wireless avc ipv6 assurance
9800-Cl-VM(config-flow-monitor)#exit

9800-Cl-VM(config)#flow monitor avc_ipv4_assurance_rtp
9800-Cl-VM(config-flow-monitor)#exporter avc_exporter
9800-Cl-VM(config-flow-monitor)#cache timeout active 60
9800-Cl-VM(config-flow-monitor)#default cache entries
9800-Cl-VM(config-flow-monitor)#record wireless avc ipv4 assurance-rtp
9800-Cl-VM(config-flow-monitor)#exit

9800-Cl-VM(config)#flow monitor avc_ipv6_assurance_rtp
```

```
9800-Cl-VM(config-flow-monitor)#exporter avc_exporter
9800-Cl-VM(config-flow-monitor)#cache timeout active 60
9800-Cl-VM(config-flow-monitor)#default cache entries
9800-Cl-VM(config-flow-monitor)#record wireless avc ipv6 assurance-rtp
9800-Cl-VM(config-flow-monitor)#exit
```

```
Mapping the IPv4 and IPv6 Flow Minitor in Policy Profile

9800-Cl-VM(config)#wireless profile policy AVC_Testing
9800-Cl-VM(config-wireless-policy)#shutdown

Disabling policy profile will result in associated AP/Client rejoin

9800-Cl-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance input
9800-Cl-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance output
9800-Cl-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance_rtp input
9800-Cl-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance_rtp output
9800-Cl-VM(config-wireless-policy)#ipv6 flow monitor avc_ipv6_assurance input
9800-Cl-VM(config-wireless-policy)#ipv6 flow monitor avc_ipv6_assurance output
9800-Cl-VM(config-wireless-policy)#ipv6 flow monitor avc_ipv6_assurance_rtp input
9800-Cl-VM(config-wireless-policy)#ipv6 flow monitor avc_ipv6_assurance_rtp output
9800-Cl-VM(config-wireless-policy)#no shutdown
9800-Cl-VM(config-wireless-policy)#exit
```

Verificação do AVC

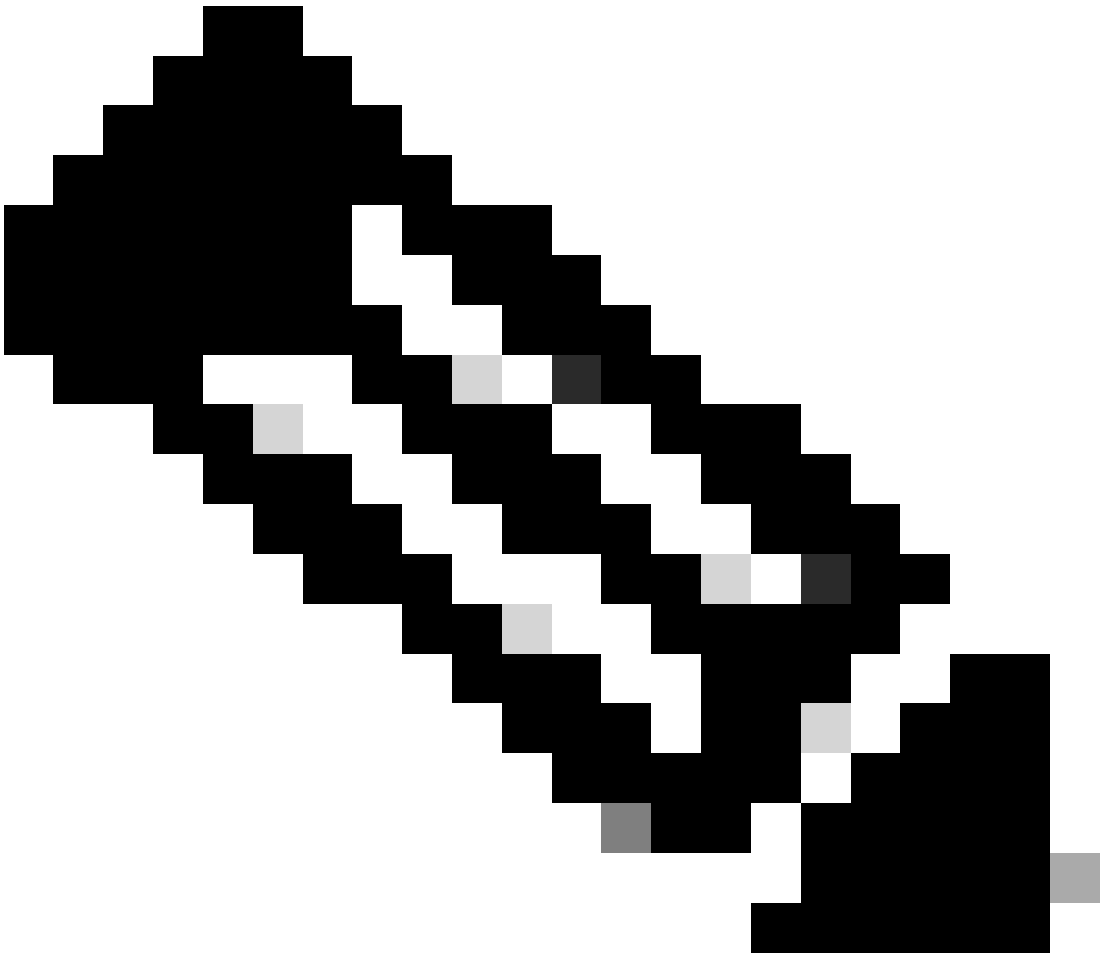
No 9800

Quando a WLC 9800 é utilizada como um exportador de fluxo, estas estatísticas AVC podem ser observadas:

· Visibilidade de aplicativos para clientes conectados em todos os SSIDs.

· Uso de aplicativos individuais para cada cliente.

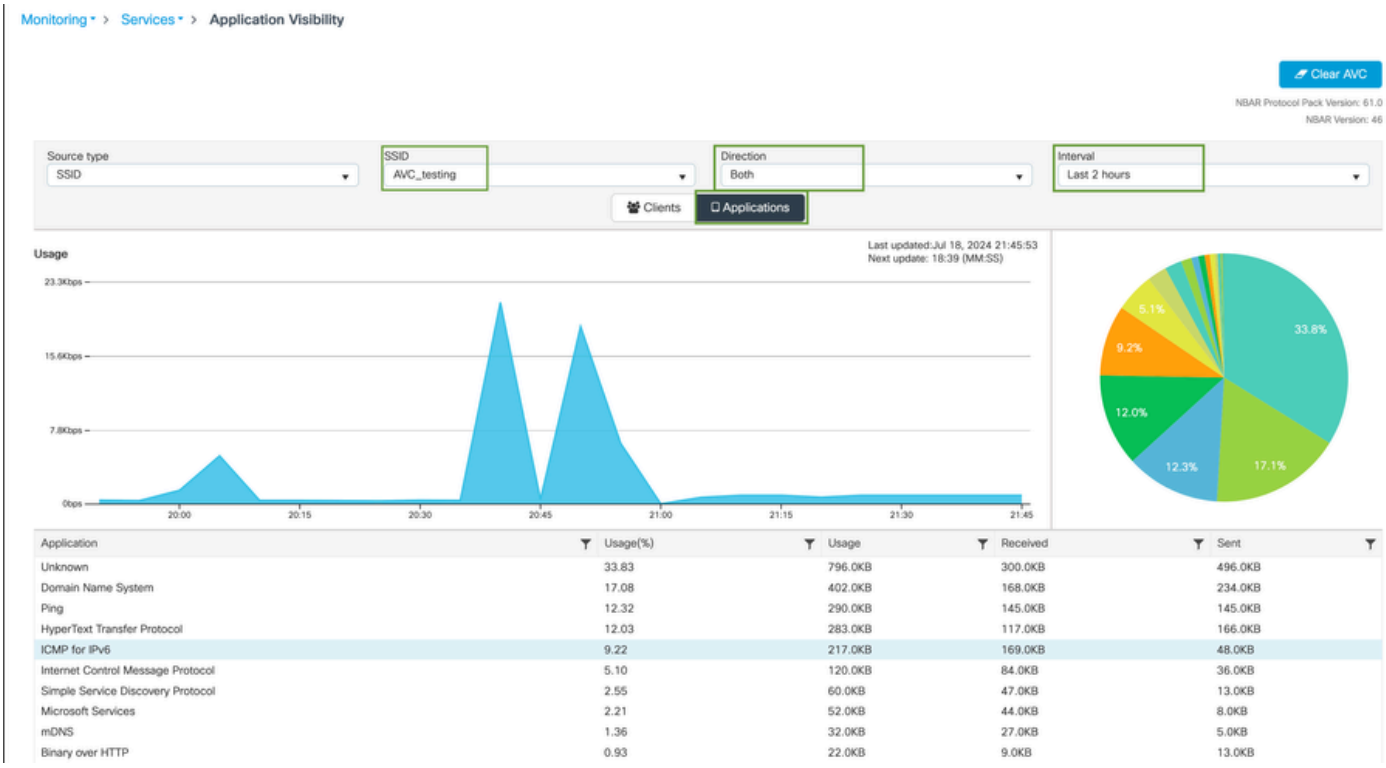
· Uso de aplicativos específicos em cada SSID separadamente.



Observação: você tem a opção de filtrar os dados por direção, abrangendo o tráfego de entrada (entrada) e saída (saída), bem como por intervalo de tempo, com a capacidade de selecionar um intervalo de até 48 horas.

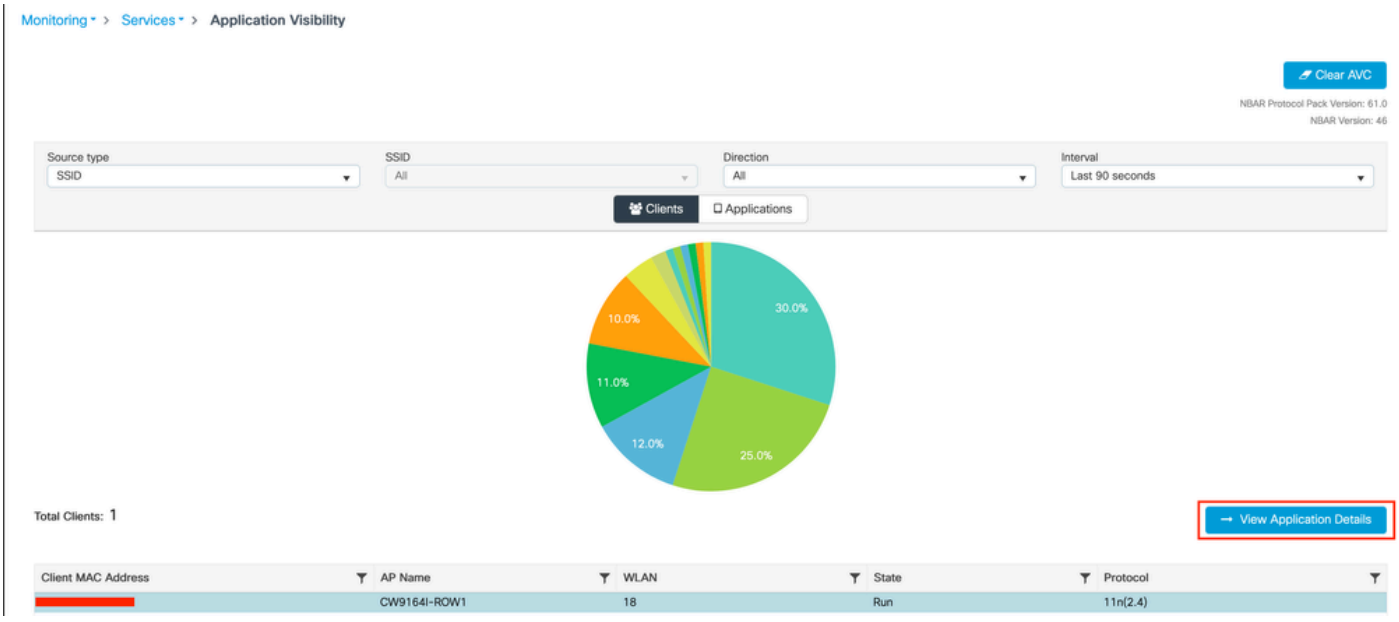
Via GUI

Navegue até Monitoring **>** Services **>** Application Visibility .

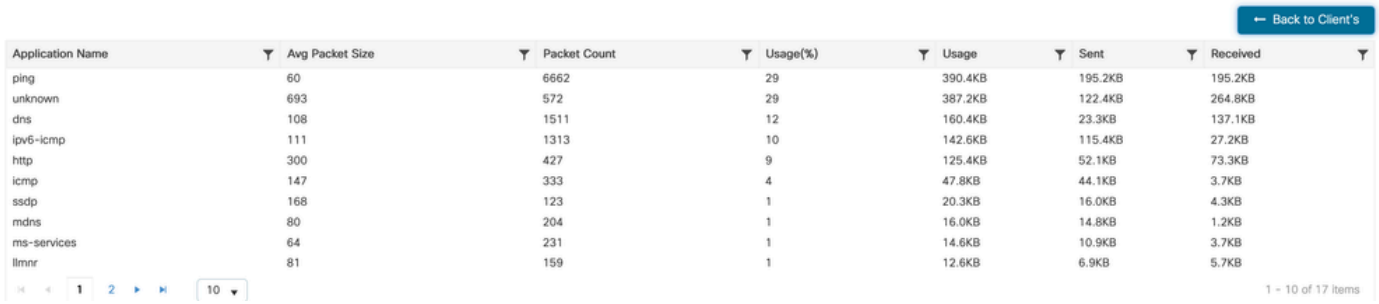


Visibilidade de aplicativos de usuários conectados ao SSID AVC_testing para tráfego de entrada e saída

Para exibir as estatísticas de visibilidade de aplicativos para cada cliente, clique na guia Clientes, escolha um cliente específico e clique em Exibir detalhes do aplicativo.



Visibilidade do aplicativo para o cliente específico - 1



← Back to Client's

Application Name	Avg Packet Size	Packet Count	Usage(%)	Usage	Sent	Received
ping	60	6662	29	390.4KB	195.2KB	195.2KB
unknown	693	572	29	387.2KB	122.4KB	264.8KB
dns	108	1511	12	160.4KB	23.3KB	137.1KB
ipv6-icmp	111	1313	10	142.6KB	115.4KB	27.2KB
http	300	427	9	125.4KB	52.1KB	73.3KB
icmp	147	333	4	47.8KB	44.1KB	3.7KB
ssdp	168	123	1	20.3KB	16.0KB	4.3KB
mdns	80	204	1	16.0KB	14.8KB	1.2KB
ms-services	64	231	1	14.6KB	10.9KB	3.7KB
llmnr	81	159	1	12.6KB	6.9KB	5.7KB

1 2 10 1 - 10 of 17 items

Visibilidade do aplicativo para o cliente específico - 2

Via CLI

Verificar o status do AVC

```
9800WLC#show avc status wlan AVC_testing
WLAN profile name: AVC_testing
------------------------------------------------------------
AVC configuration complete: YES
```

Estatísticas do NetFlow (Cache FNF)

```
9800WLC#show flow monitor $Flow_Monitor_Name cache format table
```

```
9800WLC#show flow monitor  wireless-avc-basic cache format table
  Cache type:                               Normal (Platform cache)
  Cache size:                               200000
  Current entries:                             102
  High Watermark:                              102

  Flows added:                                 102
  Flows aged:                                    0

IPV4 SRC ADDR    IPV4 DST ADDR    TRNS SRC PORT  TRNS DST PORT  FLOW DIRN  WIRELESS SSID                    IP PROT  APP NAME                                bytes long
wireless client mac addr
===============  ===============  =============  =============  =========  ===============================  =======  ==============================  ==================
========================
10.105.193.170   10.105.193.195           5355          61746  Output     AVC_testing                           17  layer7 llmnr                               120
[redacted]
10.105.193.129   10.105.193.195           5355          61746  Output     AVC_testing                           17  port dns                                   120
[redacted]
10.105.193.195   10.105.193.2                0            771  Input      AVC_testing                            1  prot icmp                                  148
[redacted]
10.105.193.195   10.105.193.114              0            771  Input      AVC_testing                            1  prot icmp                                  120
[redacted]
10.105.193.4     10.105.193.195           5355          64147  Output     AVC_testing                           17  layer7 llmnr                               120
[redacted]
10.105.193.169   10.105.193.195           5355          64147  Output     AVC_testing                           17  port dns                                   120
[redacted]
10.105.193.195   10.105.193.52               0            771  Input      AVC_testing                            1  prot icmp                                  148
[redacted]
10.105.193.59    10.105.193.195           5355          64147  Output     AVC_testing                           17  port dns                                   120
```

Verificação do AVC no 9800 CLI

Para examinar individualmente o uso principal do aplicativo para cada WLAN e seus clientes conectados:

```
9800WLC#show avc wlan <SSID> top <n> applications <aggregate|downstream|upstream>
9800WLC#show avc client <mac> top <n> applications <aggregate|downstream|upstream>
where n = <1-30> Enter the number of applications
```

```
9800WLC#show avc wlan <SSID> application <app> top <n> <aggregate|downstream|upstream>
where n =  <1-10> Enter the number of clients
```

Verificar a contagem de pacotes FNFv9 e o status de decodificação apontado para o Plano de Controle (CP)

```
9800WLC#show platform software wlavc status decoder
```

```
9800WLC#show platform software wlavc status decoder
AVC FNFv9 Decoder status:

Pkt Count       Pkt Decoded     Pkt Errors      Data Records    Last decoded time   Last error time
--------------- --------------- --------------- --------------- ------------------- -------------------
25703           25703           0               132480          07/20/2024 14:10:46 01/01/1970 05:30:00
```

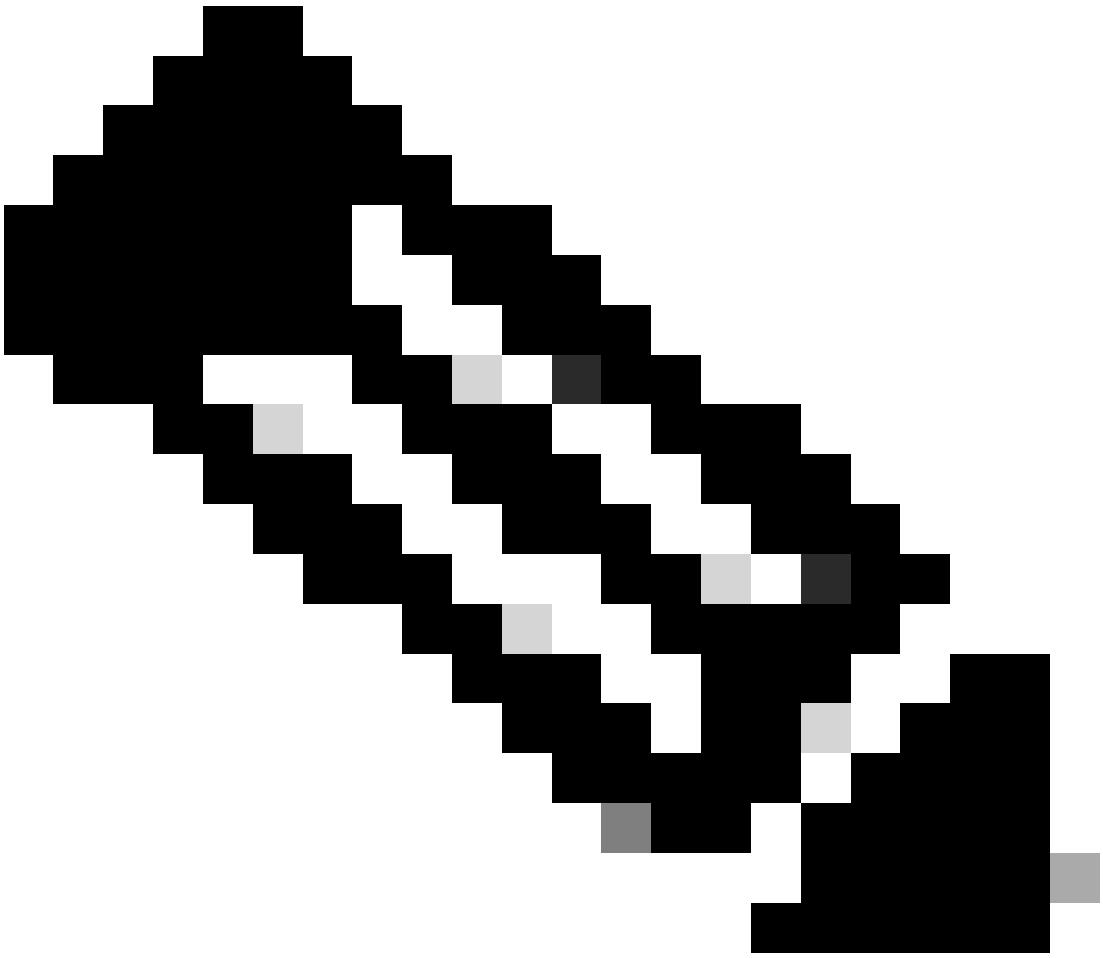
Registro de pacote FNFv9

Você também pode verificar as estatísticas nbar diretamente.

```
9800WLC#show ip nbar protocol-discovery
```

Nos modos Fabric e Flex, você pode obter as estatísticas NBAR do AP por meio de:

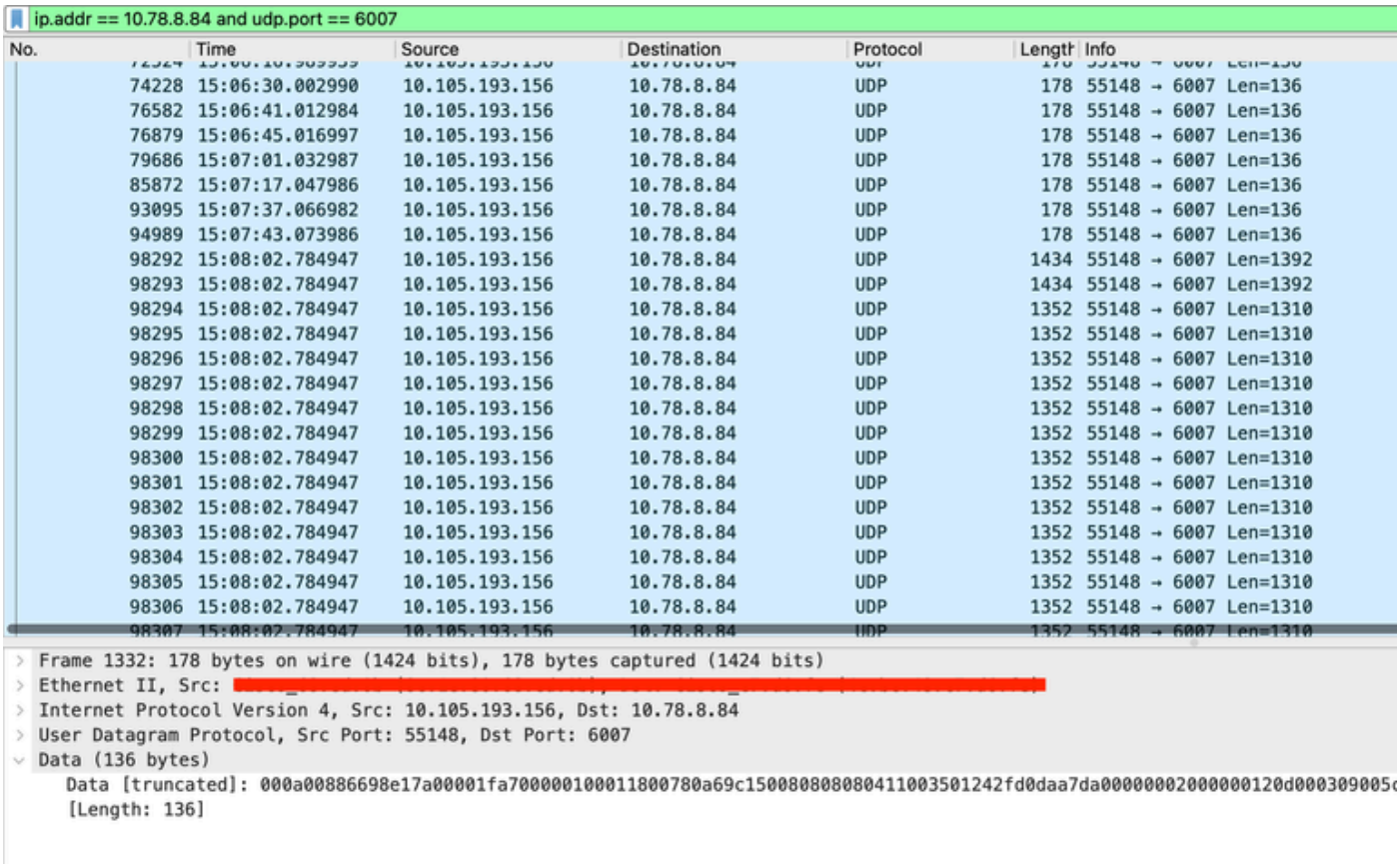
```
AP#show avc nbar statistics
Works on both IOS and ClickOS APs
```



Observação: em uma configuração de âncora externa, a WLC âncora serve como a presença da camada 3 para o cliente, enquanto a WLC externa opera na camada 2. Como o Application Visibility and Control (AVC) opera na camada 3, os dados relevantes são observáveis apenas na WLC âncora.

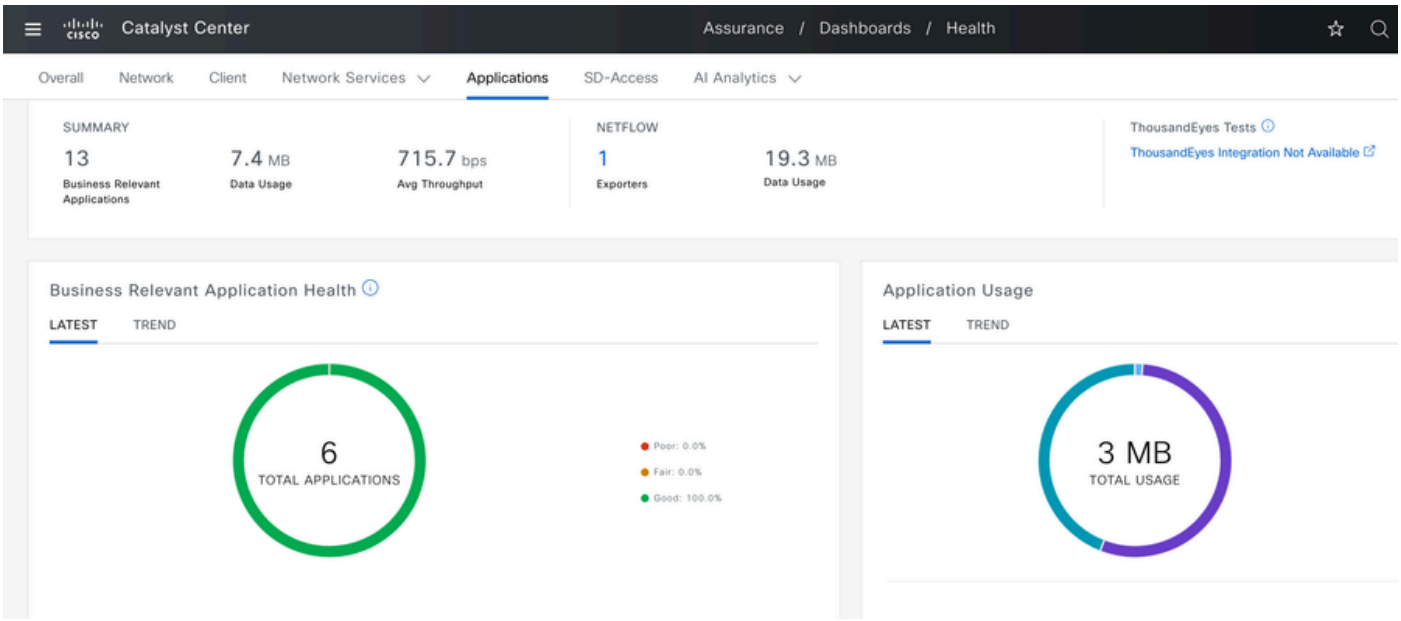
No DNAC

A partir da captura de pacotes feita na WLC 9800, podemos confirmar se ela está enviando dados relativos aos aplicativos e ao tráfego de rede para o Cisco Catalyst Center continuamente.



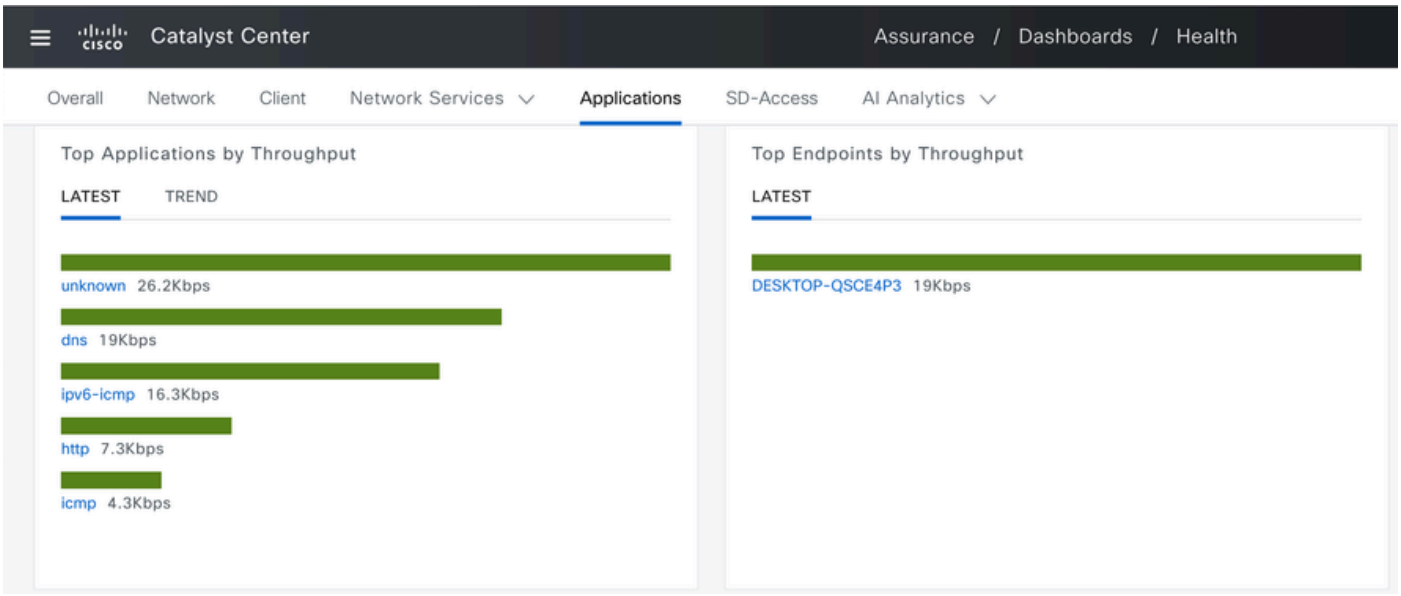
Captura de pacotes em WLC 9800

Para visualizar os dados de aplicativos para clientes conectados a uma WLC específica no Cisco Catalyst Center, navegue para Assurance > Dashboards > Health > Application .



Monitoramento AVC no Cisco Catalyst Center

Podemos rastrear os aplicativos usados com mais frequência por clientes e identificar os consumidores de dados mais altos, como demonstrado aqui.

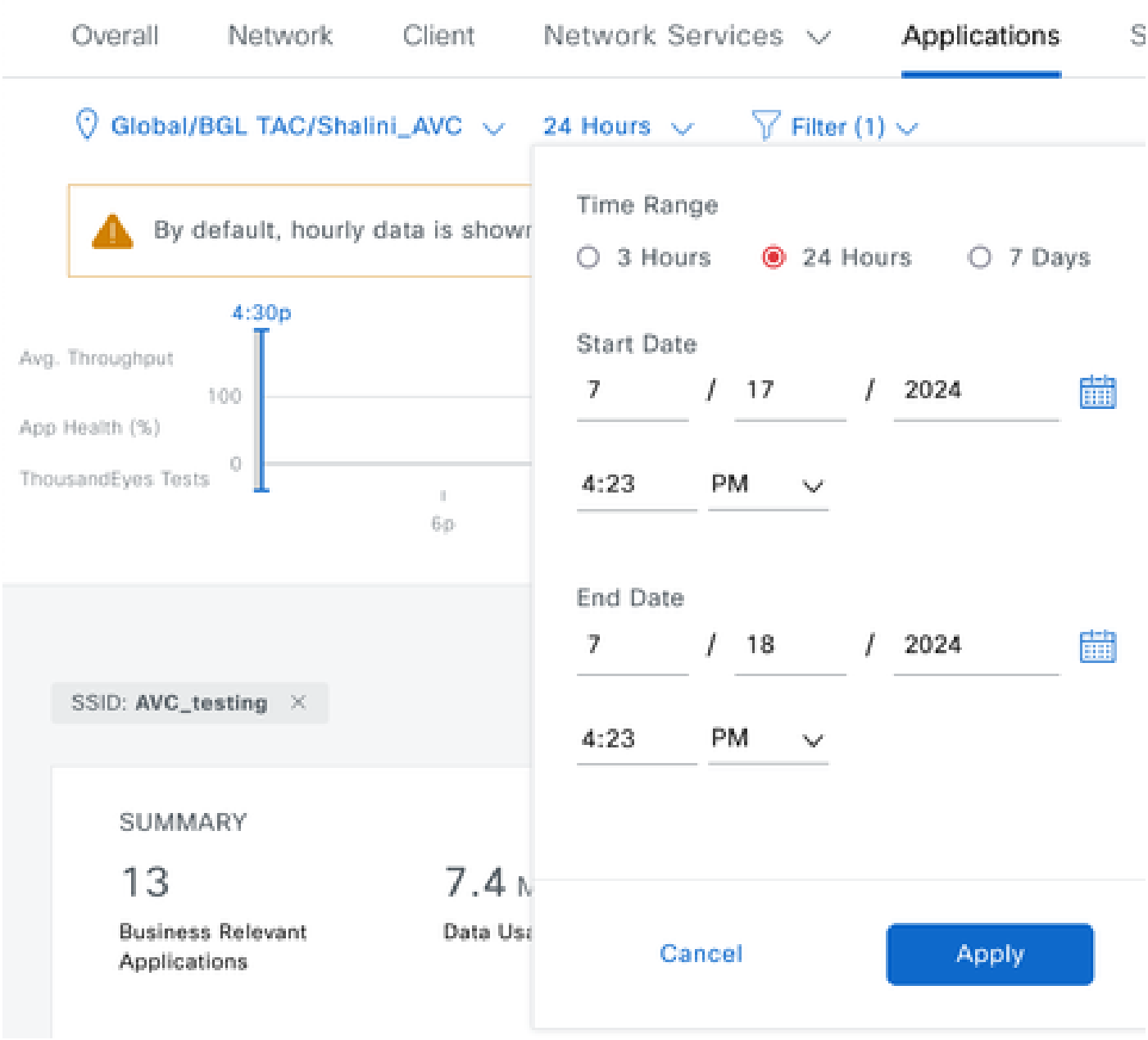


Principais estatísticas de aplicativos e principais estatísticas de usuários de largura de banda

Você pode definir um filtro para um SSID específico, que permite monitorar o throughput geral e o uso do aplicativo dos clientes associados a esse SSID.

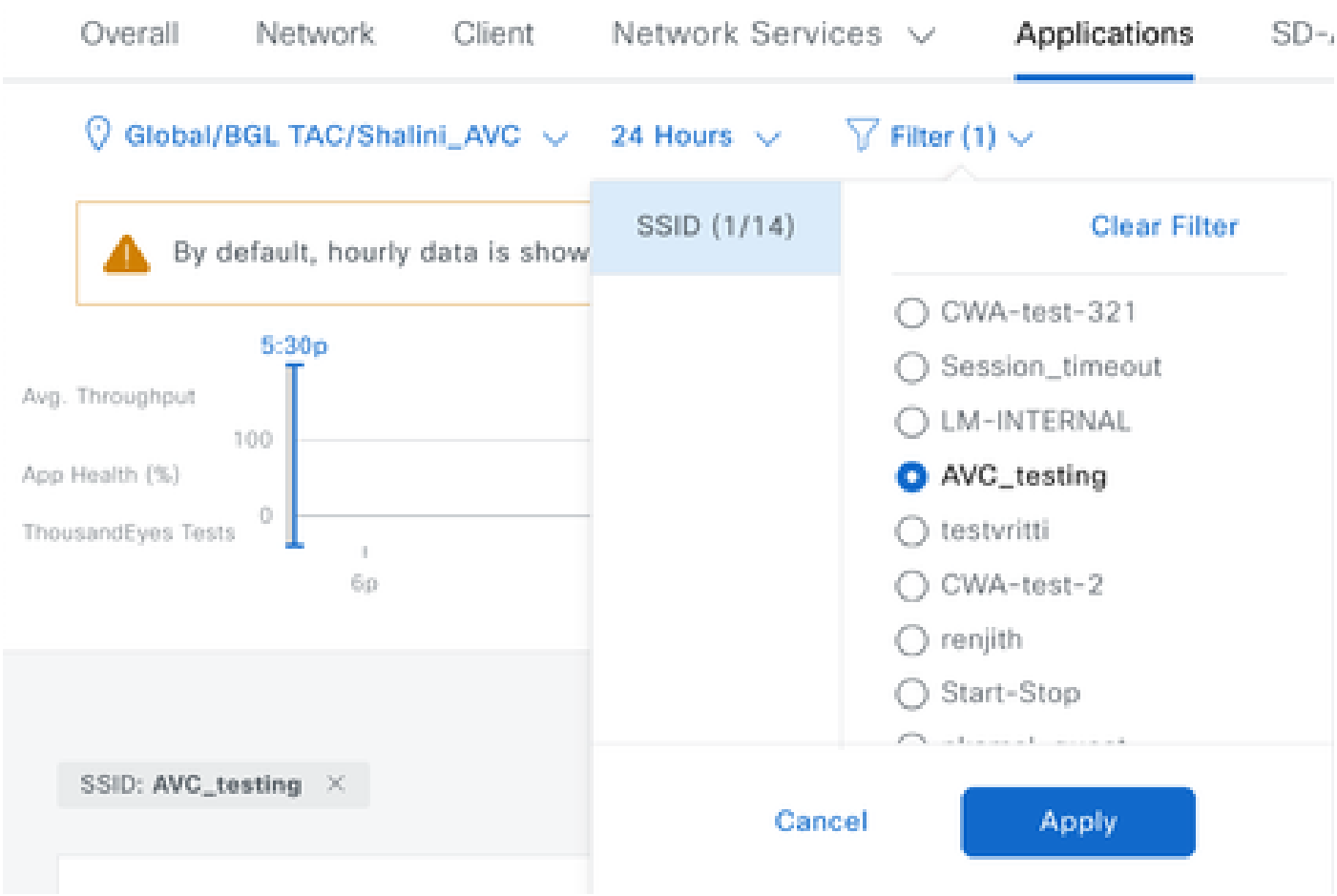
Essa funcionalidade permite identificar os principais aplicativos e os usuários que consomem mais largura de banda na rede.

Além disso, você pode utilizar o recurso Time Filter para examinar esses dados em períodos anteriores, oferecendo insights históricos sobre o uso da rede.



Filtro de Tempo para exibir estatísticas AVC

.



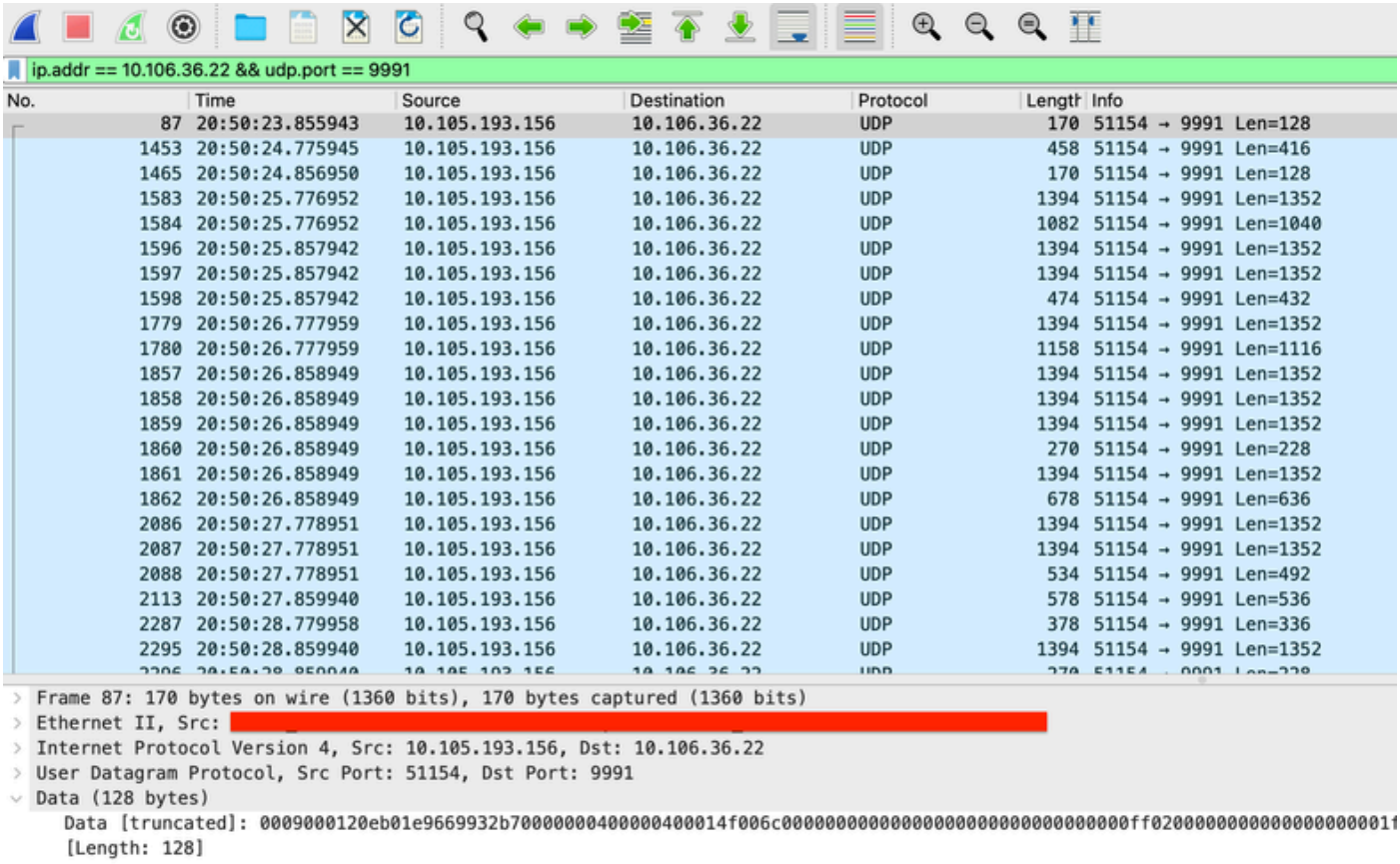
Filtro SSID para exibir Estatísticas AVC

No coletor NetFlow externo

Exemplo 1: Cisco Prime como coletor Netflow

Quando você usa o Cisco Prime como coletor Netflow, a WLC coletada. Você pode ver a WLC 9800 como fonte de dados que envia dados do Netflow, e o modelo do NetFlow será criado automaticamente de acordo com os dados que estão sendo enviados pela WLC 9800.

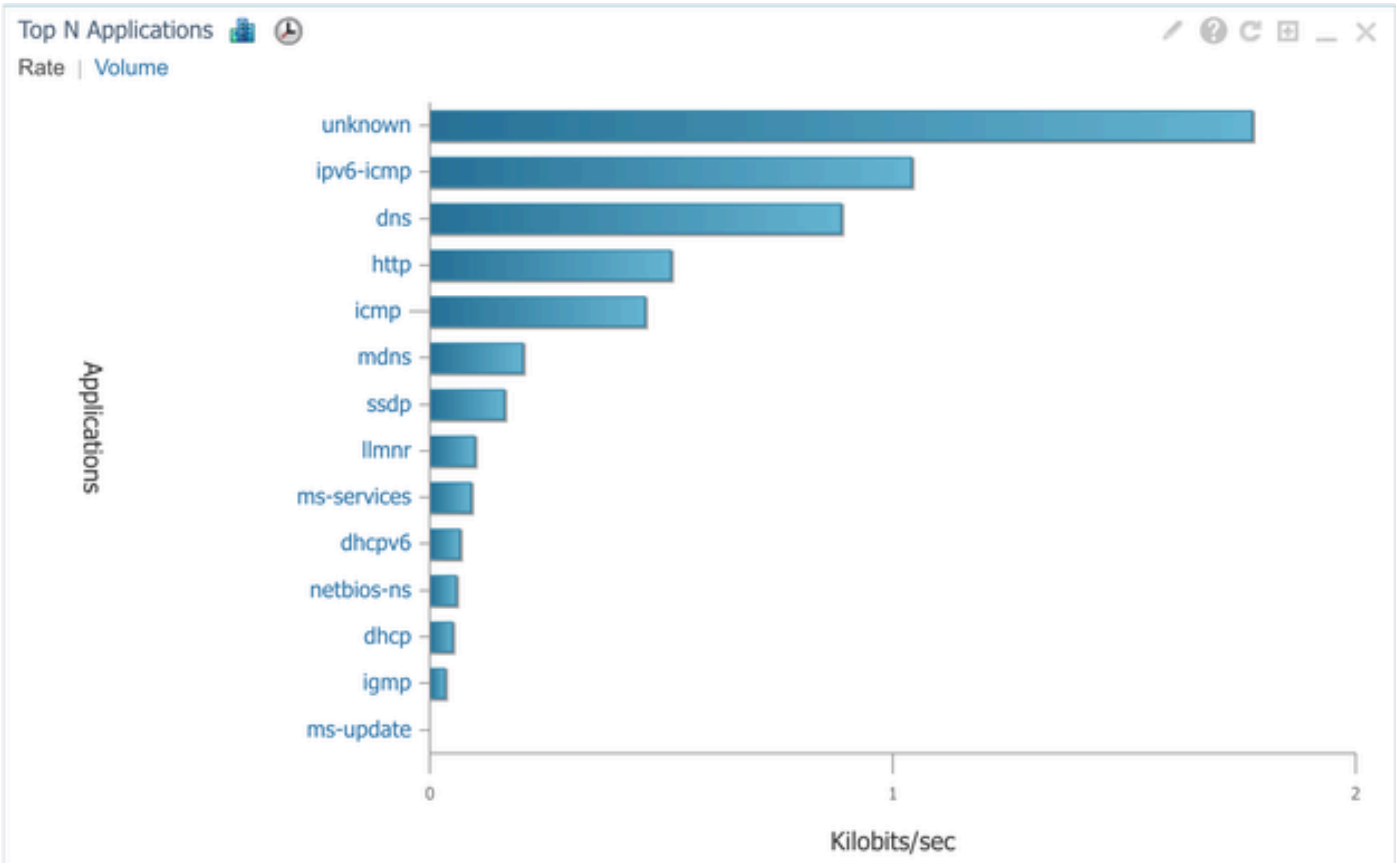
A partir da captura de pacotes feita na WLC 9800, podemos confirmar se ela está enviando dados relativos aos aplicativos e ao tráfego de rede para o Cisco Prime continuamente.



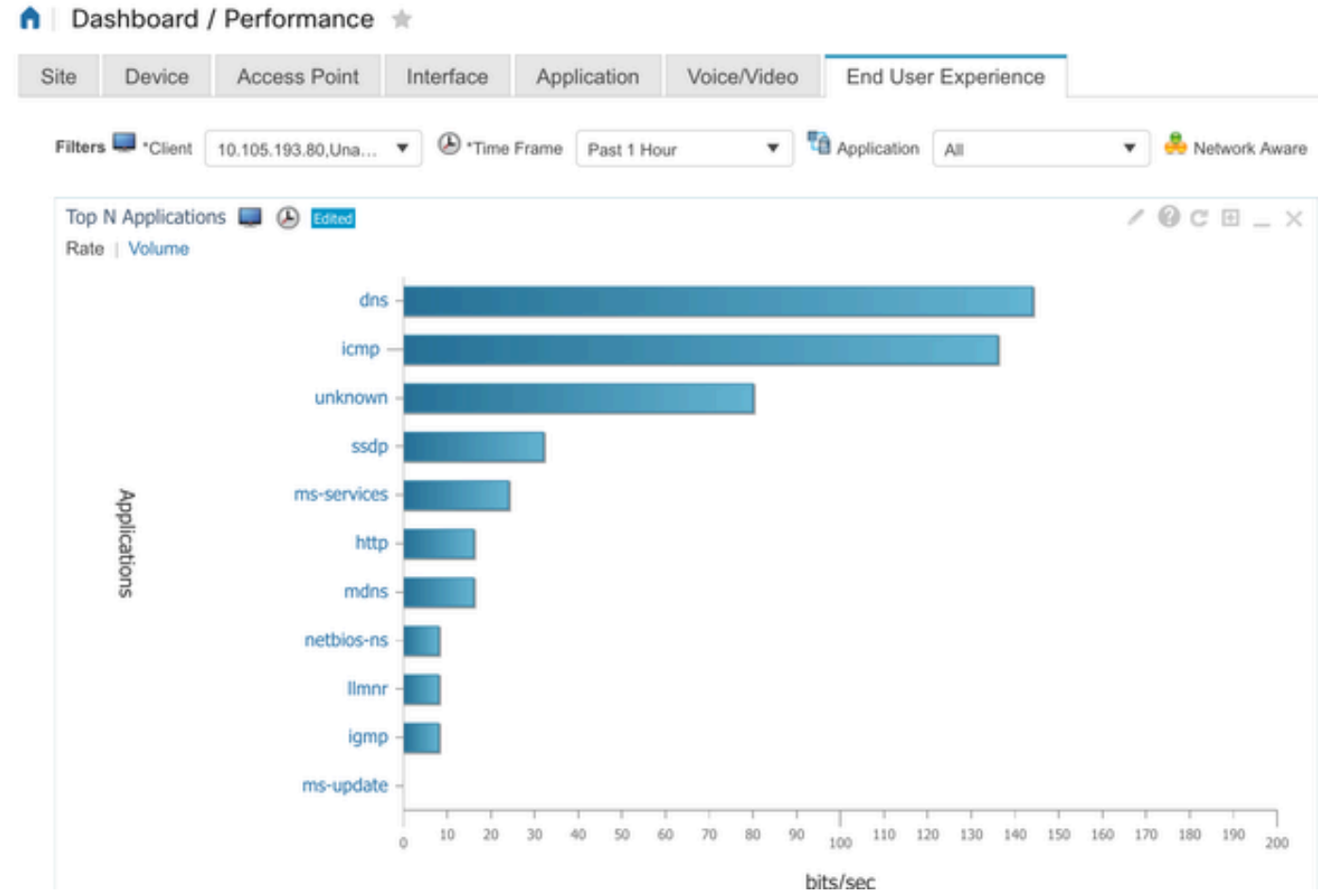
Captura de pacotes realizada em WLC 9800

Cisco Prime Detecting 9800 WLC como fonte de dados Netflow

Você pode definir filtros com base em Aplicativo, Serviços e até mesmo por Cliente, usando o endereço IP para uma análise de dados mais direcionada.



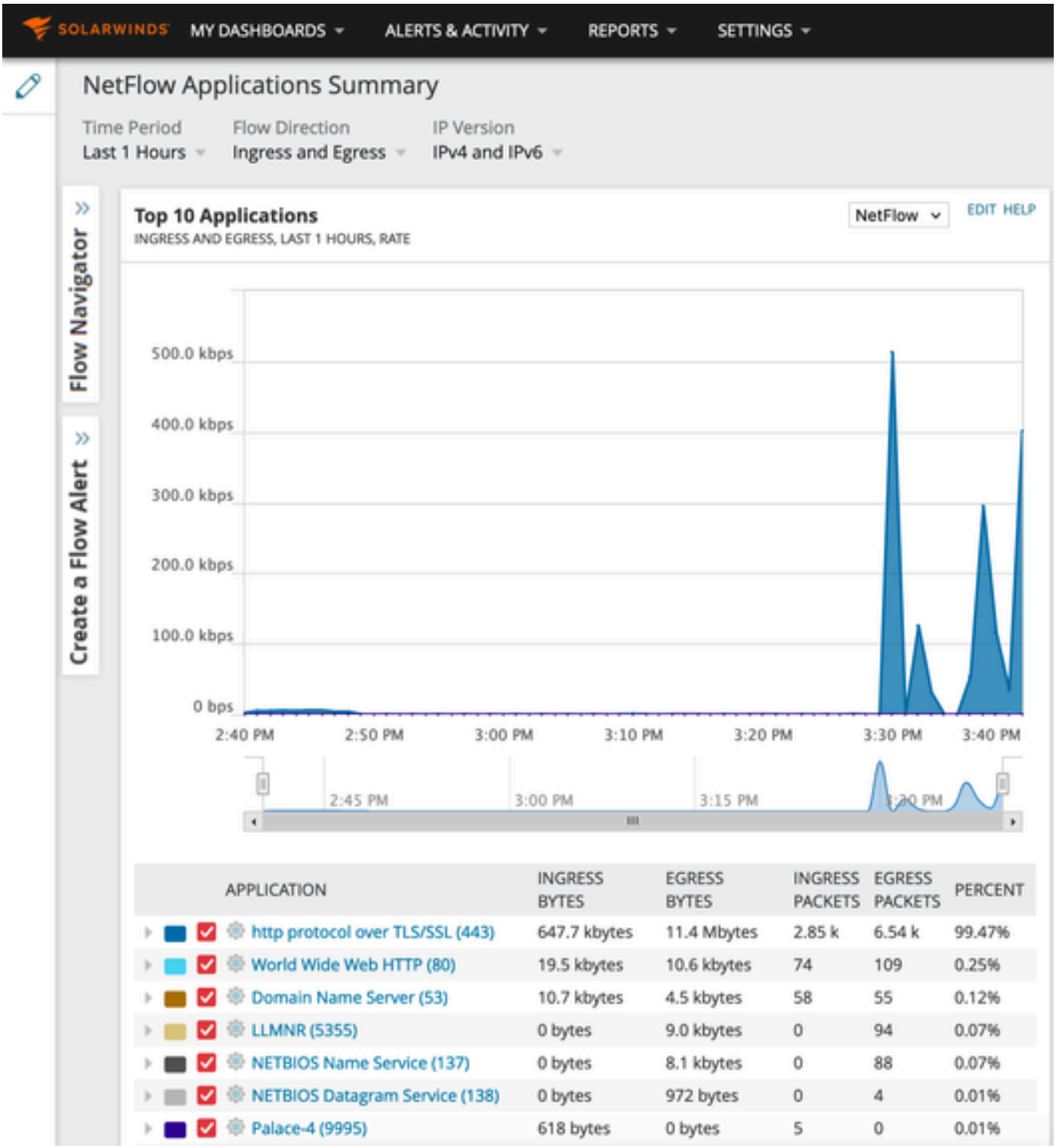
Visibilidade de aplicativos para todos os clientes



Aplicação de cliente específico usando endereço IP

Exemplo 2: Coletor NetFlow de terceiros

Neste exemplo, o coletor NetFlow de terceiros [SolarWinds] é utilizado para coletar estatísticas de aplicativos. A WLC 9800 emprega o Flexible NetFlow (FNF) para transmitir dados abrangentes sobre os aplicativos e o tráfego de rede, que são coletados pela SolarWinds.



Estatísticas de aplicativos Netflow no SolarWind

Controle de tráfego

O controle de tráfego se refere a um conjunto de recursos e mecanismos usados para gerenciar e regular o fluxo do tráfego de rede. Políticas de tráfego ou limitação de taxa são mecanismos usados no controlador sem fio para controlar a quantidade de tráfego transmitido do cliente. Ele monitora a taxa de dados do tráfego de rede e toma medidas imediatas quando um limite de taxa predefinido é excedido. Quando o tráfego excede a taxa especificada, a limitação de taxa pode descartar os pacotes em excesso ou marcá-los para baixo alterando seus valores de Classe de Serviço (CoS) ou Ponto de Código de Serviços Diferenciados (DSCP). Isso pode ser obtido com a configuração de QOS no 9800 WLC. Você pode consultar https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/215441-configure-qos-rate-limiting-on-catalyst.html para obter uma visão geral de como esses componentes funcionam e como podem ser configurados para alcançar resultados diferentes.

Troubleshooting

A solução de problemas do AVC envolve identificar e resolver problemas que possam afetar a capacidade do AVC de identificar, classificar e gerenciar com precisão o tráfego de aplicativos em sua rede sem fio. Os problemas comuns podem incluir problemas com classificação de tráfego, aplicação de políticas ou relatórios. Aqui estão algumas etapas e considerações ao Troubleshoot problemas de AVC em um Catalyst 9800 WLC:

- Verificar a configuração do AVC: verifique se o AVC está configurado corretamente na WLC e associado às WLANs e aos perfis corretos.
- Ao configurar o AVC por meio da GUI, a porta 9995 será automaticamente atribuída como padrão. No entanto, se você estiver usando um coletor externo, verifique em que porta ele está configurado para escutar o tráfego do NetFlow. É crucial configurar com precisão esse número de porta para corresponder às configurações do coletor.
- Verifique o suporte ao modelo do AP e ao modo de implantação.
- Consulte as limitações da WLC 9800 ao implementar o AVC em sua rede sem fio.

Coleta de logs

Logs de WLC

1. Ative o timestamp para ter referência de tempo para todos os comandos.

```
9800WLC#term exec prompt timestamp
```

2. Para revisar a configuração

```
9800WLC#show tech-support wireless
```

3. Você pode verificar o status do avc e as estatísticas do netflow.

Verifique o status da configuração do AVC.

```
9800WLC#show avc status wlan <wlan_name>
```

Verifique a contagem de pacotes FNFv9 e o status de decodificação apontado para o plano de controle (CP).

```
9800WLC#show platform software wlavc status decoder
```

Verifique as estatísticas do NetFlow (cache FNF).

```
9800WLC#show flow monitor <Flow_Monitor_Name>
```

Marque Top n application usage for each wlan, onde n = <1-30> Insira o número de aplicativos.

```
9800WLC#show avc wlan <SSID> top <n> applications <aggregate|downstream|upstream>
```

Marque n principais usos de aplicativos para cada cliente, onde n = <1-30> Insira o número de aplicativos.

```
9800WLC#show avc client <mac> top <n> applications <aggregate|downstream|upstream>
```

Marque os n principais clientes conectados a uma wlan específica usando o aplicativo específico, onde n=<1-10> Insira o número de clientes.

```
9800WLC#show avc wlan <SSID> application <app> top <n> <aggregate|downstream|upstream>
```

Verifique as estatísticas nbar.

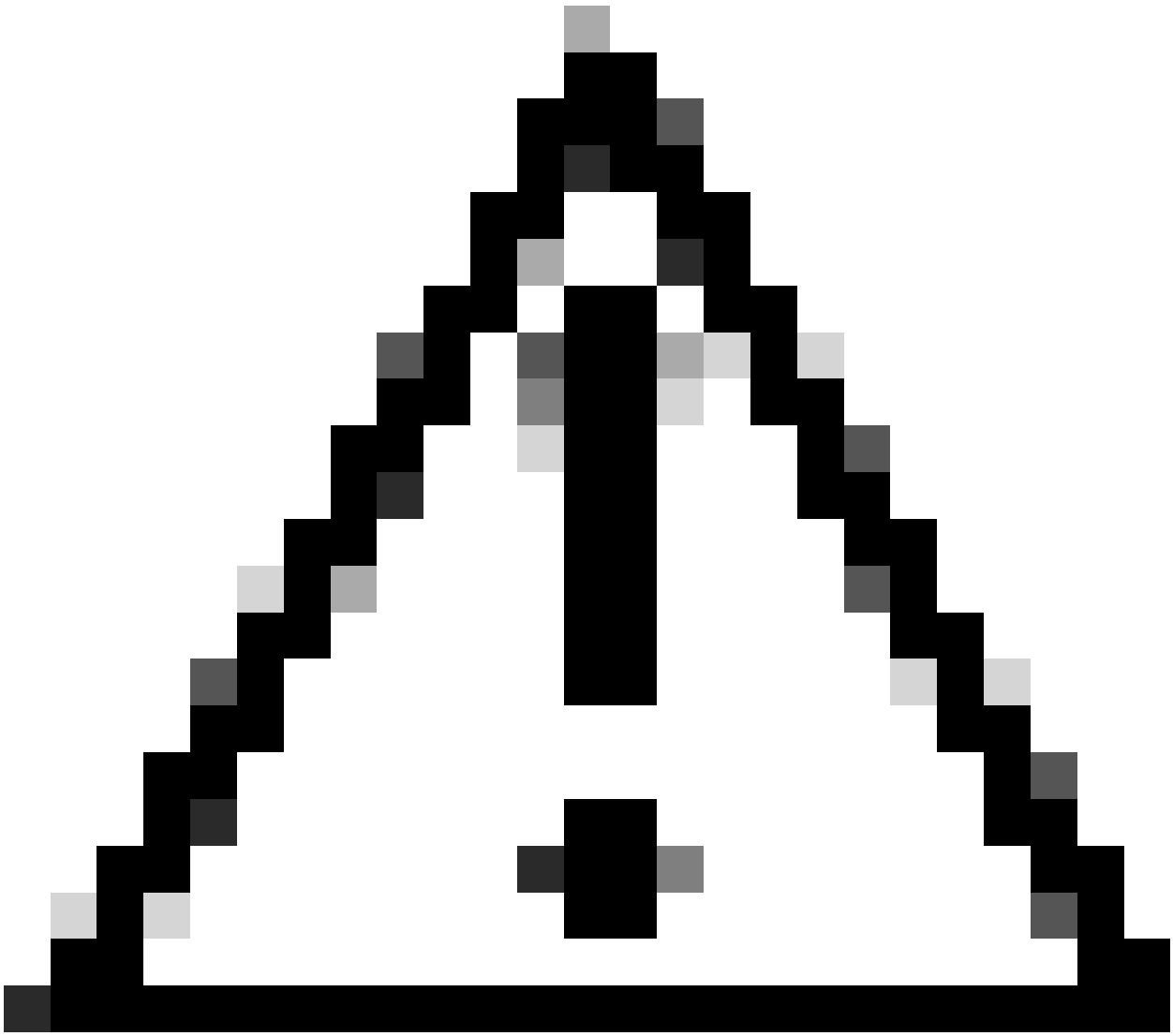
```
9800WLC#show ip nbar protocol-discovery
```

4. Defina o nível de log como debug/verbose.

```
9800WLC#set platform software trace all debug/verbose

!! To View the collected logs
9800WLC#show logging profile wireless internal start last clear to-file bootflash:<File_Name

!!Set logging level back to notice post troubleshooting
9800WLC#set platform software trace wireless all debug/verbose
```

5. Ative o Rastreamento Radioativo (RA) para o endereço MAC do cliente para validar as estatísticas AVC.
Via CLI

```
9800WLLC#debug wireless {mac | ip} {aaaa.bbbb.cccc | x.x.x.x } {monitor-time} {N seconds} !! Setting ti
9800WLC#no debug wireless mac <Client_MAC>
!!WLC generates a debug trace file with Client_info, command to check for debug trace file generated.
9800WLC#dir bootflash: | i debug
```



Cuidado: a depuração condicional habilita o registro em nível de depuração que, por sua vez, aumenta o volume dos logs gerados. Deixar esse item em execução reduz a distância no tempo em que você pode exibir logs. Portanto, é recomendável sempre desabilitar a depuração no final da sessão de solução de problemas.

```
# clear platform condition all
# undebug all
```

Via GUI
Etapa 1. Navegue para Troubleshooting > Radioative Trace .
Etapa 2. Clique em Add e insira um endereço Mac do cliente para o qual você deseja solucionar problemas. Você pode adicionar vários endereços Mac para rastrear.

Etapa 3. Quando estiver pronto para iniciar o rastreamento radioativo, clique em Iniciar. Uma vez iniciado, o registro de depuração é gravado no disco sobre qualquer processamento de plano de

controle relacionado aos endereços MAC rastreados.

Etapa 4. Quando você reproduzir o problema que deseja solucionar, clique em Parar .

Etapa 5. Para cada endereço mac depurado, você pode gerar um arquivo de log que reúne todos os logs referentes a esse endereço mac clicando em Gerar .

Etapa 6. Escolha quanto tempo você deseja que o arquivo de log agrupado volte e clique em Aplicar ao Dispositivo.

Passo 7. Agora você pode fazer o download do arquivo clicando no pequeno ícone ao lado do nome do arquivo. Esse arquivo está presente na unidade flash de inicialização do controlador e também pode ser copiado fora da caixa através da CLI.

Aqui está uma visão geral das depurações AVC em rastreamentos RA

```
2024/07/20 20:15:24.514842337 {wstatsd_RO-0}{2}: [avc-stats] [15736]: (debug): Received stats record fo
2024/07/20 20:15:24.514865665 {wstatsd_RO-0}{2}: [avc-stats] [15736]: (debug): Received stats record fo
2024/07/20 20:15:24.514875837 {wstatsd_RO-0}{2}: [avc-stats] [15736]: (debug): Received stats record fo
2024/07/20 20:15:40.530177442 {wstatsd_RO-0}{2}: [avc-stats] [15736]: (debug): Received stats record fo
```

6. Capturas Incorporadas filtradas pelo endereço MAC do cliente em ambas as direções, filtro MAC interno do cliente disponível após 17.1.

Ele é particularmente útil ao usar um coletor externo, pois ajuda a confirmar se a WLC está transmitindo dados do NetFlow para a porta desejada, como esperado.

Via CLI

```
monitor capture MYCAP clear
monitor capture MYCAP interface <Interface> both
monitor capture MYCAP buffer size 100
monitor capture MYCAP match any
monitor capture MYCAP inner mac CLIENT_MAC@
monitor capture MYCAP start
!! Inititiate different application traffic from user
monitor capture MYCAP stop
monitor capture MYCAP export flash:|tftp:|http:.../filename.pcap
```

Via GUI
Etapa 1. Navegue até Troubleshooting > Captura de Pacotes > +Adicionar .

Etapa 2. Defina o nome da captura do pacote. É permitido um máximo de 8 caracteres.

Etapa 3. Defina filtros, se houver.

Etapa 4. Marque a caixa para Monitorar o tráfego de controle se quiser ver o tráfego apontado para a CPU do sistema e injetado de volta no plano de dados.

Etapa 5. Definir tamanho do buffer. É permitido um máximo de 100 MB.

Etapa 6. Defina o limite, seja pela duração, que permite um intervalo de 1 a 1000000 segundos, ou pelo número de pacotes, que permite um intervalo de 1 a 100000 pacotes, conforme desejado.

Passo 7. Escolha a interface na lista de interfaces na coluna esquerda e selecione a seta para movê-la para a coluna direita.

Etapa 8. Clique em Apply to Device.

Etapa 9. Para iniciar a captura, selecione Start .

Etapa 10. Você pode permitir que a captura seja executada até o limite definido. Para interromper manualmente a captura, selecione Stop.

Etapa 11. Uma vez interrompido, um botão Export fica disponível para clicar com a opção para baixar o arquivo de captura (.pcap) na área de trabalho local via servidor HTTP ou TFTP ou servidor FTP ou disco rígido ou flash do sistema local.

Logs AP

Modos On Fabric e Flex

1. mostre ao técnico para ter todos os detalhes da configuração e estatísticas do cliente para o AP.

2. show avc nbar statistics nbar stats from AP

3. Depurações AVC

```
AP#term mon
AP#debug capwap client avc <all/detail/error/event>
AP#debug capwap client avc netflow <all/detail/error/event/packet>
```

Informações Relacionadas

Guia de configuração do AVC

Limitação de taxa no 9800 WLC

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.