Configurar o NetFlow/IPFIX para a inclusão de telemetria em SNA

Contents

Introdução

Este documento descreve as práticas recomendadas e a configuração básica do Netflow/IPFIX que o Secure Network Analytics (SNA) precisa para a inclusão de telemetria.

Pré-requisitos

- Conhecimento de SNA da Cisco
- Conhecimento de NetFlow/IPFIX

Requisitos

- Análise de rede segura na versão 7.2.1 ou mais recente
- Flow Collector em 7.2.1 ou mais recente
- Acesso CLI como raiz para o Flow Collector

Componentes Utilizados

- Isso depende totalmente do seu projeto de rede e dos dispositivos que você selecionou para enviar o NetFlow/IPFIX para o Secure Network Analytics. A configuração do NetFlow/IPFIX é diferente em cada exportador; para obter uma configuração detalhada, entre em contato com a equipe de suporte de cada exportador.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

Informações de Apoio

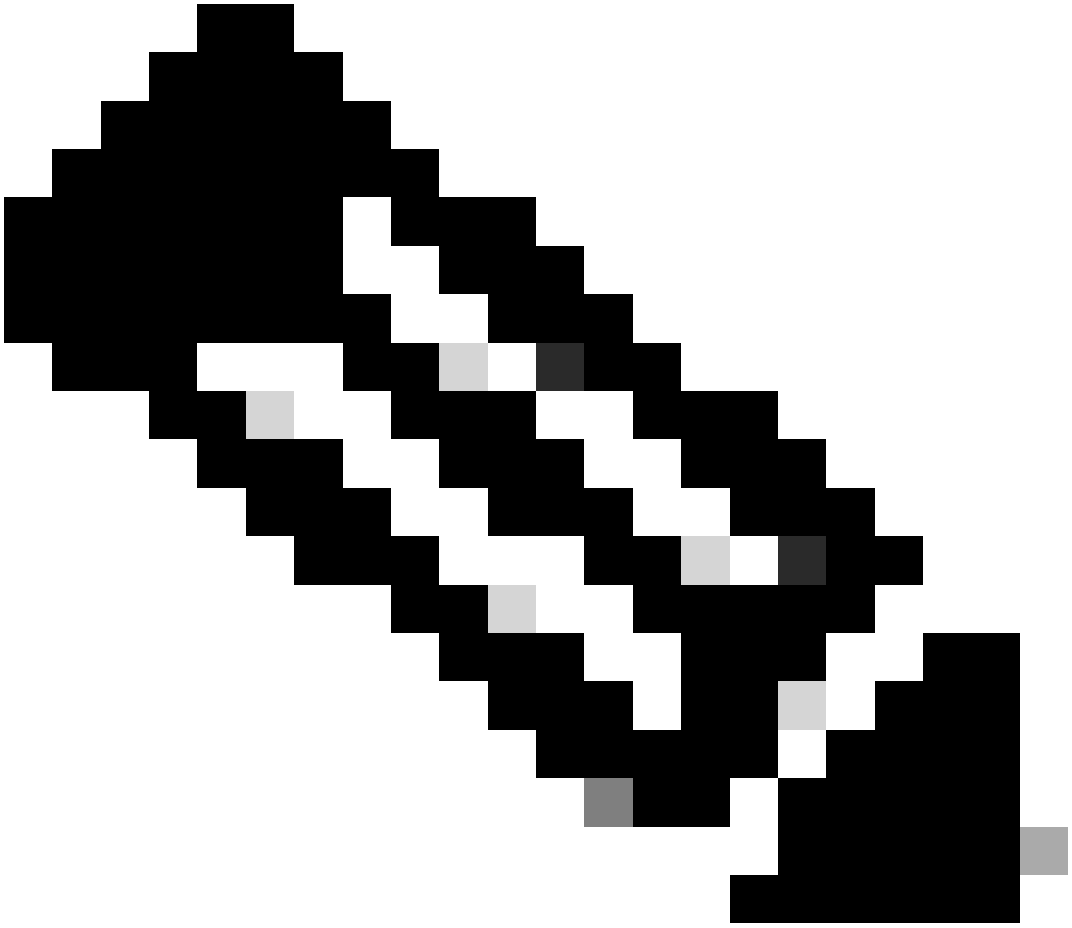
O Flow Collector é um dispositivo SNA encarregado de coletar, processar e armazenar fluxos que são enviados para o Secure Network Analytics. Para o NetFlow versão 9 ou IPFIX, vários campos podem ser incluídos no modelo NetFlow/IPFIX para adicionar mais informações relacionadas ao tráfego de rede. No entanto, há 9 campos específicos que devem ser incluídos no modelo NetFlow/IPFIX para que o Flow Collector processe esses fluxos. O Flow Collector não processa fluxos de entrada que incluam um modelo não válido, portanto, o SNA não exibe informações de fluxo desses exportadores na IU da Web ou no Desktop Client.

Configurar

Campos Obrigatórios

Os próximos campos devem ser incluídos no modelo NetFlow/IPFIX para inclusão de telemetria. Certifique-se de que esses 9 campos estejam incluídos no modelo NetFlow/IPFIX, para que o Secure Network Analytics processe os fluxos de entrada.

- Endereço IP origem
- Endereço IP de destino
- Porta de origem
- Porta de Destino
- Protocolo de Camada 3
- Contagem de Bytes
- Contagem de pacotes
- Hora de início do fluxo
- Hora de término do fluxo



Observação: mais campos podem ser incluídos na configuração NetFlow/IPFIX, no entanto, os campos anteriores são os requisitos mínimos do Secure Network Analytics para Ingestão de Telemetria.

Campos recomendados

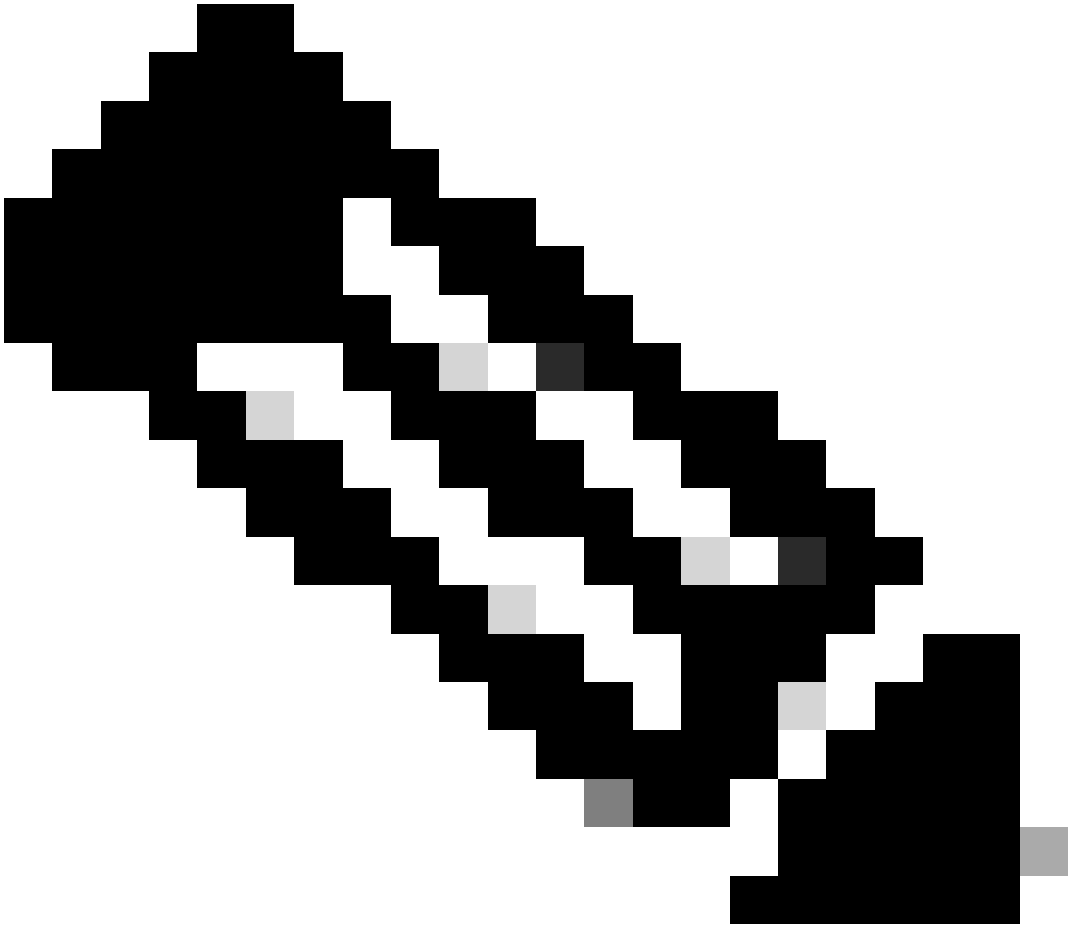
Recomenda-se incluir os próximos campos no modelo NetFlow/IPFIX para coletar informações sobre as informações de interface. Essa configuração é necessária para mostrar informações de interface, como nome e velocidade:

- Entrada de interface
- Saída da interface

Prática recomendada

Além disso, as próximas configurações são recomendadas como práticas recomendadas para garantir um desempenho adequado do Secure Network Analytics.

- Definir o tempo limite ativo como 60 segundos
- Definir o tempo limite inativo para 15 segundos
- Definir o tempo limite do modelo como 30 segundos



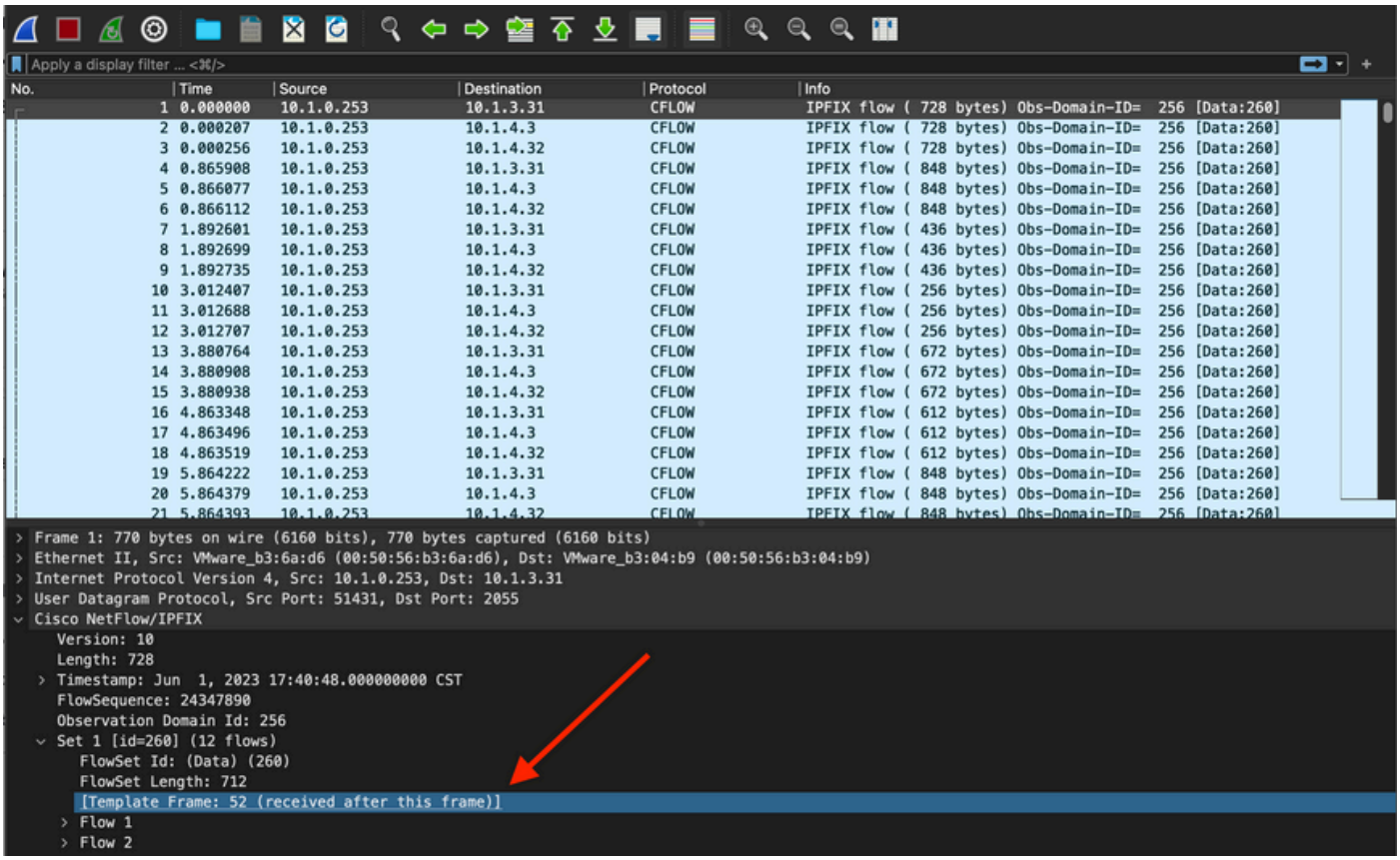
> Observação: a porta padrão do NetFlow é 2055, no entanto, você pode selecionar outra porta. Certifique-se de usar a mesma porta durante o processo lc-ast em Flow Collector(s).

Verificar

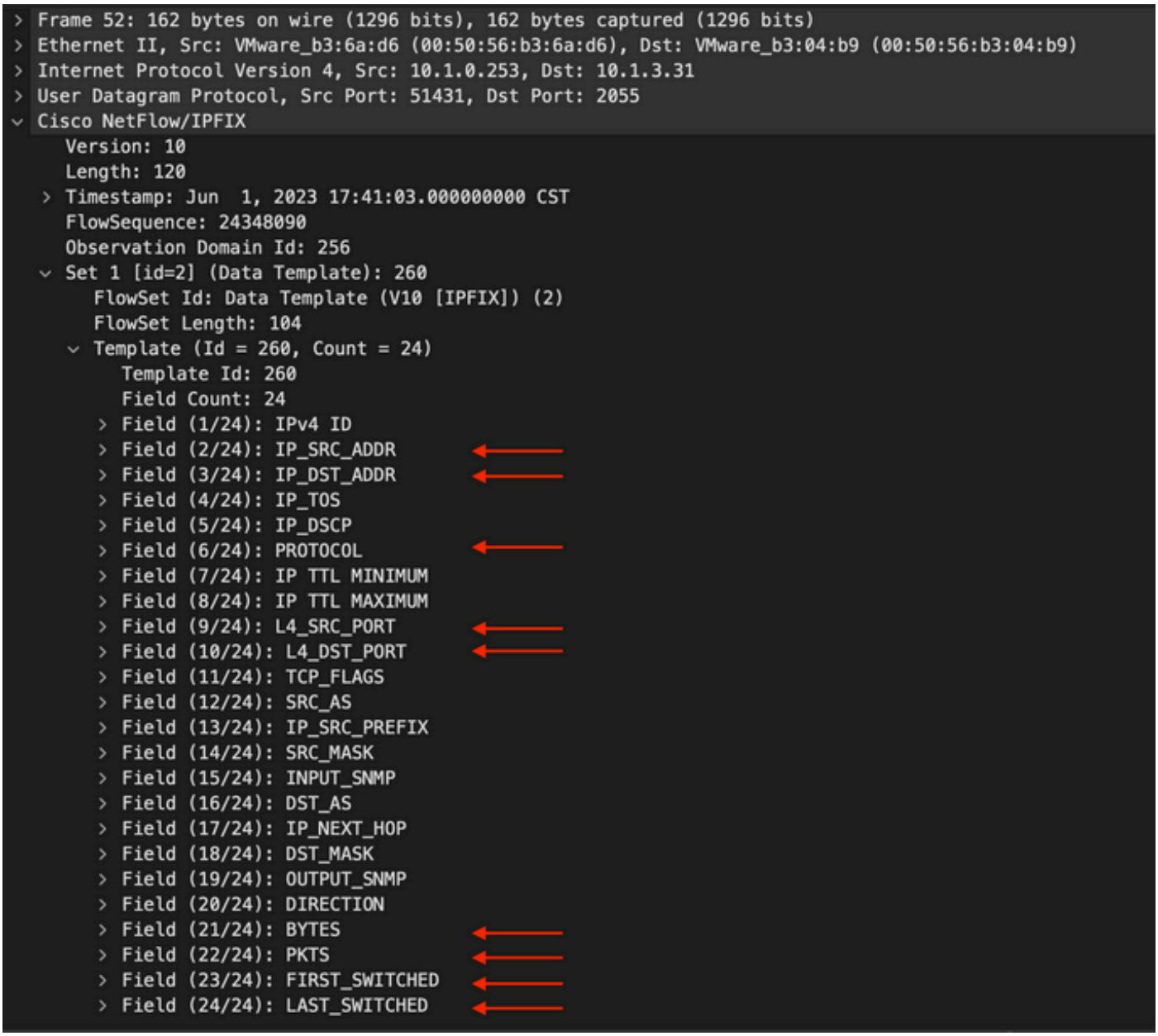
Para validar a configuração do modelo NetFlow/IPFIX, você pode executar uma captura de pacote entre o exportador e o Flow Collector. Faça login no Flow Collector com o usuário root via SSH e execute o comando:

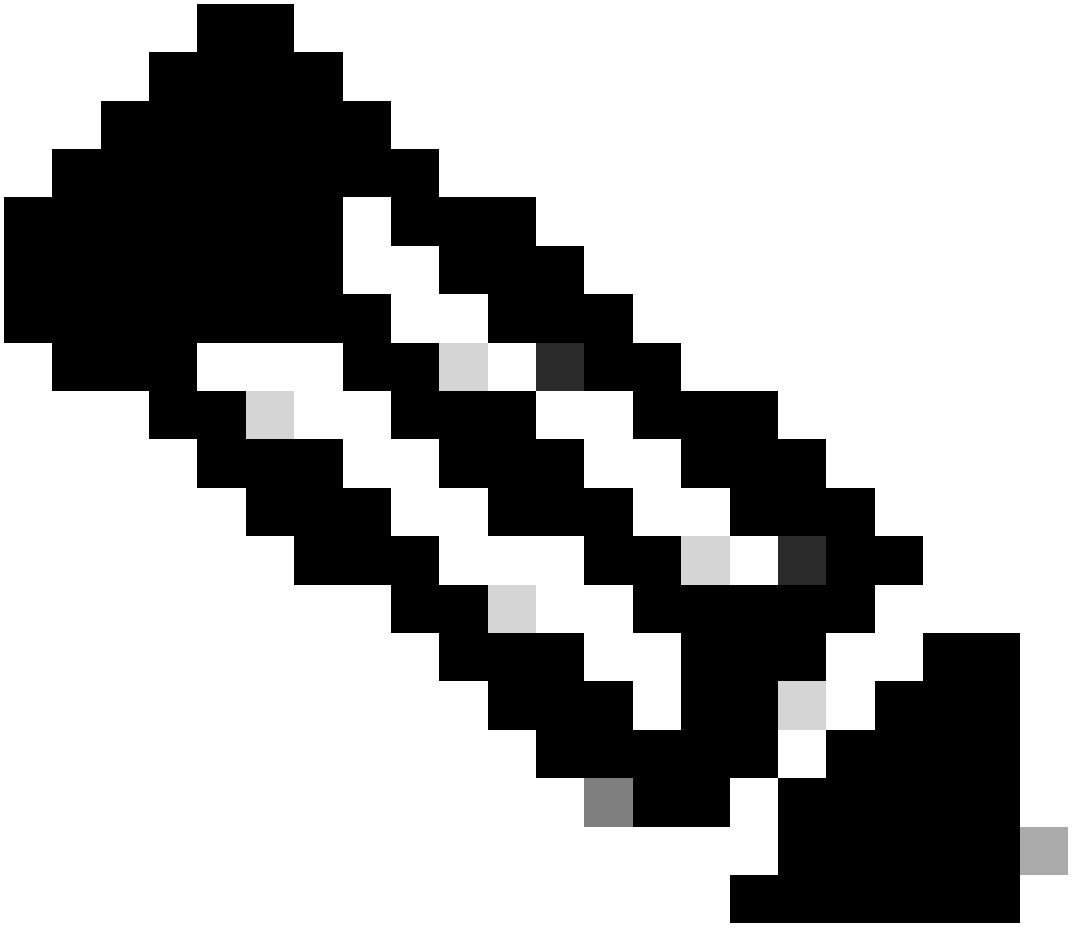
```
tcpdump -nli [Collecting_Interface] host [Exporter_IP_Address] and port [NetFlow_Port] -w /lancope/var/
```

- Use uma ferramenta SCP para exportar a captura de pacotes do Flow Collector (localizado em /lancope/var/tcpdump) para sua máquina local e, em seguida, abra-a no Wireshark



- Identificar o quadro em que o modelo NetFlow/IPFIX foi recebido e abri-lo para validar os campos que o modelo inclui


Frame 52: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits)
Ethernet II, Src: VMware_b3:6a:d6 (00:50:56:b3:6a:d6), Dst: VMware_b3:04:b9 (00:50:56:b3:04:b9)
Internet Protocol Version 4, Src: 10.1.0.253, Dst: 10.1.3.31
User Datagram Protocol, Src Port: 51431, Dst Port: 2055
Cisco NetFlow/IPFIX
Version: 10
Length: 120
Timestamp: Jun 1, 2023 17:41:03.000000000 CST
FlowSequence: 24348090
Observation Domain Id: 256
Set 1 [id=2] (Data Template): 260
FlowSet Id: Data Template (V10 [IPFIX]) (2)
FlowSet Length: 104
Template (Id = 260, Count = 24)
Template Id: 260
Field Count: 24
Field (1/24): IPv4 ID
Field (2/24): IP_SRC_ADDR
Field (3/24): IP_DST_ADDR
Field (4/24): IP_TOS
Field (5/24): IP_DSCP
Field (6/24): PROTOCOL
Field (7/24): IP TTL MINIMUM
Field (8/24): IP TTL MAXIMUM
Field (9/24): L4_SRC_PORT
Field (10/24): L4_DST_PORT
Field (11/24): TCP_FLAGS
Field (12/24): SRC_AS
Field (13/24): IP_SRC_PREFIX
Field (14/24): SRC_MASK
Field (15/24): INPUT_SNMP
Field (16/24): DST_AS
Field (17/24): IP_NEXT_HOP
Field (18/24): DST_MASK
Field (19/24): OUTPUT_SNMP
Field (20/24): DIRECTION
Field (21/24): BYTES
Field (22/24): PKTS
Field (23/24): FIRST_SWITCHED
Field (24/24): LAST_SWITCHED



Observação: os nomes de campo mostrados podem parecer diferentes em cada exportador, essa é apenas uma referência de como você pode validar esses campos.

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.