Dispositivos de borda de WAN NFVIS onboard

Contents

Introdução

Este documento descreve o processo de integração de sistemas com capacidade NFVIS em um ambiente Catalyst™ SD-WAN para gerenciamento e operação.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco SDWAN
- NFVIS
- Plug and Play (PNP)

Presume-se que:

- Os controladores SD-WAN (vManage, vBond e vSmart) já estão implantados com certificados válidos.
- O Cisco WAN Edge (NFVIS, neste caso) tem acessibilidade para o orquestrador vBond e outros controladores SD-WAN que podem ser acessados por meio de endereços IP públicos nos transportes da WAN

- A versão do NFVIS deve ser compatível com o Guia de compatibilidade de componentes de controle.

Componentes Utilizados

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.

Hardware

- C8300-UCPE-1N20 (mas pode ser aplicado a qualquer plataforma compatível com NFVIS)

Software

- vManage 20.14.1
- vSmart e vBond 20.14.1
- NFVIS 4.14.1

Fluxo de Trabalho PnP

A confiança nos dispositivos de borda da WAN é feita usando os certificados da cadeia raiz que são pré-carregados na fabricação, carregados manualmente, distribuídos automaticamente pelo vManage ou instalados durante o processo de provisionamento de implantação automatizada PnP ou ZTP.

A solução de SD-WAN usa um modelo de lista de permissões, o que significa que os dispositivos de borda da WAN que têm permissão para se unir à rede de sobreposição de SDWAN precisam ser conhecidos por todos os controladores de SD-WAN com antecedência. Isso é feito adicionando-se os dispositivos de borda da WAN no portal de conexão Plug-and-Play (PnP) em https://software.cisco.com/software/pnp/devices

Este procedimento sempre requer que o dispositivo seja identificado, confiável e com permissão listado na mesma rede de sobreposição. A autenticação mútua precisa ocorrer em todos os componentes da SD-WAN antes de estabelecer conexões de controle seguras entre os componentes da SD-WAN na mesma rede de sobreposição. A identidade do dispositivo de borda da WAN é identificada exclusivamente pela ID do chassi e pelo número de série do certificado. Dependendo do roteador de borda da WAN, os certificados são fornecidos de diferentes maneiras:

- vEdge baseado em hardware: O certificado é armazenado no chip TPM (Módulo à prova de adulteração) instalado durante a fabricação.
- Cisco IOS®-XE SD-WAN baseado em hardware: certificado é armazenado no chip SUDI instalado durante a fabricação.
- Plataforma virtual ou dispositivos Cisco IOS-XE SD-WAN: não têm certificados raiz (como a

plataforma ASR1002-X) pré-instalados no dispositivo. Para esses dispositivos, uma OTP (One-Time Password, senha única) é fornecida pelo vManage para autenticar o dispositivo com os controladores SD-WAN.

Para executar o ZTP (Zero Touch Provisioning), um servidor DHCP deve estar disponível. Caso contrário, um endereço IP pode ser atribuído manualmente para prosseguir com as etapas restantes do processo Plug and Play (PnP).

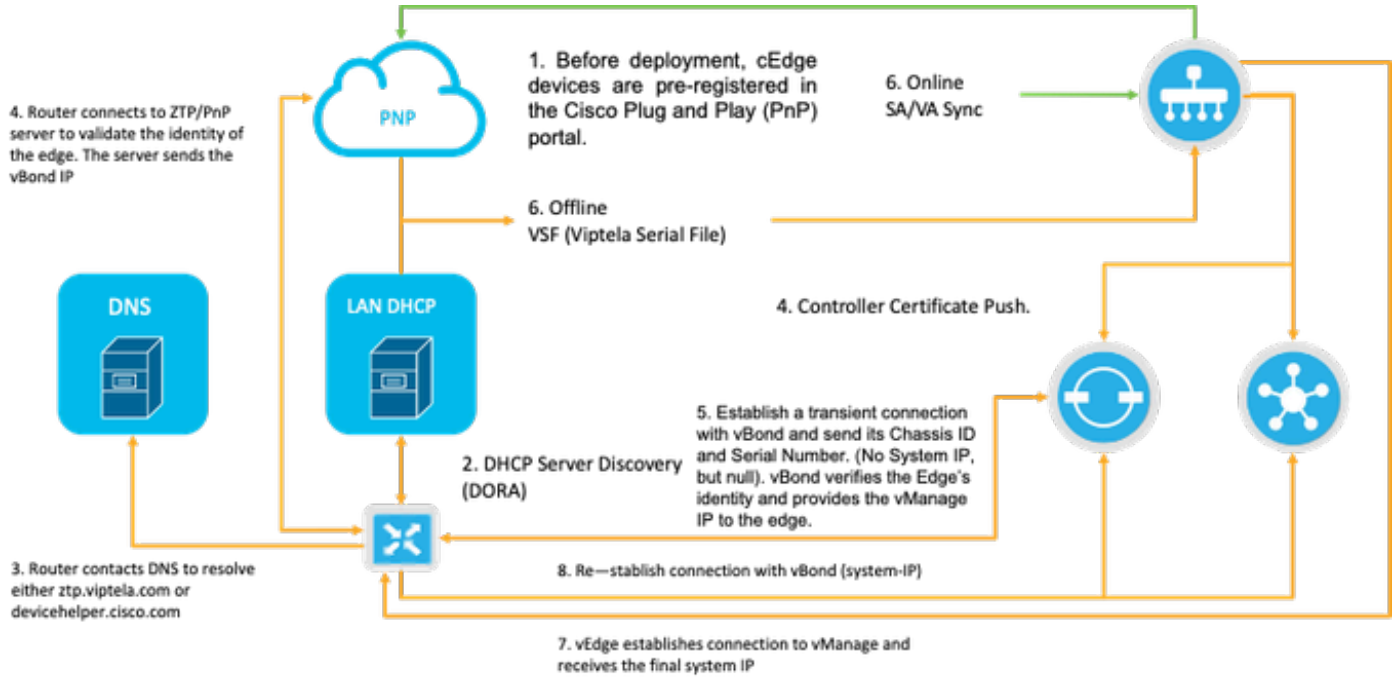


Fig. 1. Diagrama do fluxo de trabalho de confiança do dispositivo de Borda PnP e WAN.

Integração segura do dispositivo compatível com NFVIS

Recuperar Número de Série do Certificado e SN

O chip SUDI (Secure Unique Device Identifier) baseado em hardware do hardware compatível com NFVIS é usado para garantir que apenas dispositivos autorizados possam estabelecer um controle TLS ou DTLS seguro — túnel plano para o orquestrador do SD-WAN Manager. Colete o número de série correspondente usando o comando de nível executivo support show chassis:

```
C8300-UCPE-NFVIS# support show chassis
Product Name              : C8300-UCPE-1N20
Chassis Serial Num        : XXXXXXXXX
Certificate Serial Num    : XXXXXXXXXXXXXXXX
```

Adicionar o dispositivo ao portal PnP

Navegue até https://software.cisco.com/software/pnp/devices e selecione a Smart Account e a

Virtual Account corretas para seu ambiente de usuário ou laboratório. (se várias Smart Accounts coincidirem no nome, você poderá distingui-las com o identificador de domínio).

Se você ou seu usuário não souber com qual Smart Account (SA)/Virtual Account (VA) trabalhar, você sempre poderá pesquisar um número de série existente/integrado no link de texto "Pesquisa de dispositivo" para ver a qual SA/VA ele pertence.

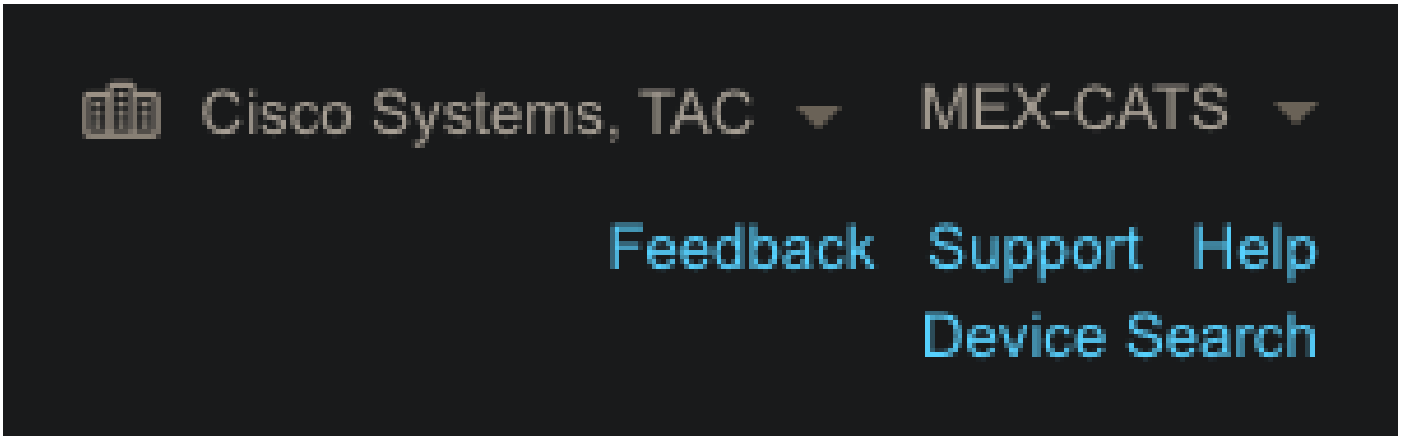


Fig. 2. Seleção de SA/VA e botão Pesquisa de dispositivo.

Quando o SA/VA correto for selecionado, clique em "Adicionar dispositivos...":

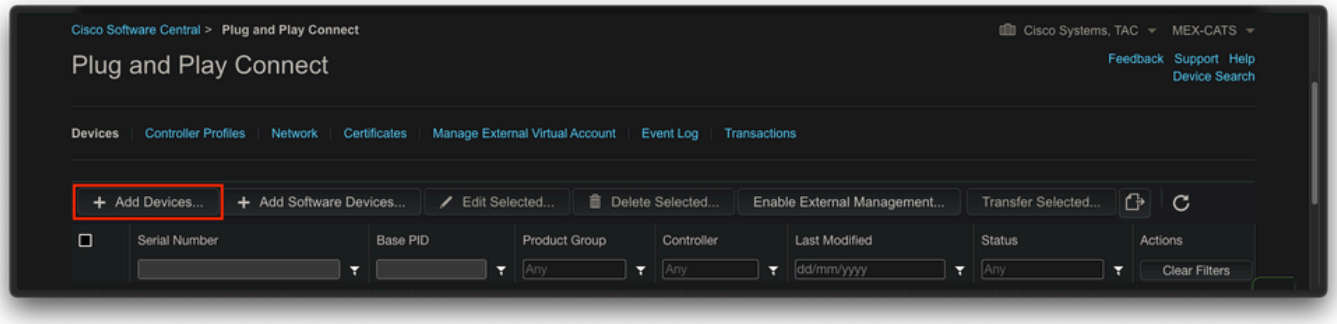


Figura 3. "Adicionar dispositivos..." Botão para clicar para registrar o dispositivo físico.

Para esse caso específico, basta colocar um dispositivo na placa, de modo que uma entrada manual é suficiente:

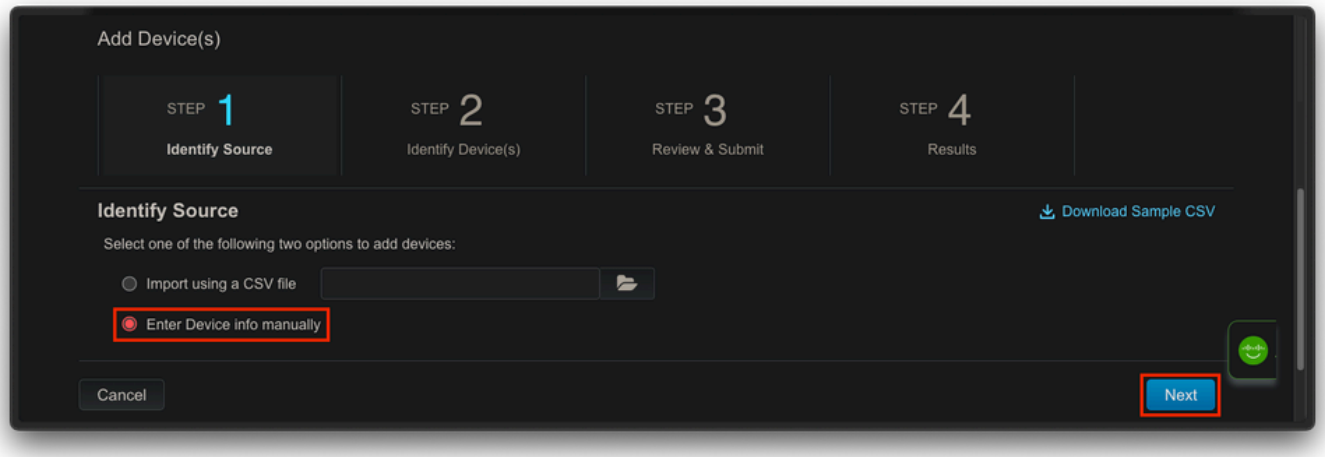


Fig. 4. "Adicionar dispositivos..." alternativa para entrada de informações do dispositivo, manual (individual) ou CSV (múltiplo).

Para a etapa 2, clique no botão "+ Identificar dispositivo...". Um modo Formulário é exibido. Preencha os detalhes com as informações mostradas na saída do suporte show chassis do NFVIS e selecione o perfil do controlador vBond correspondente.

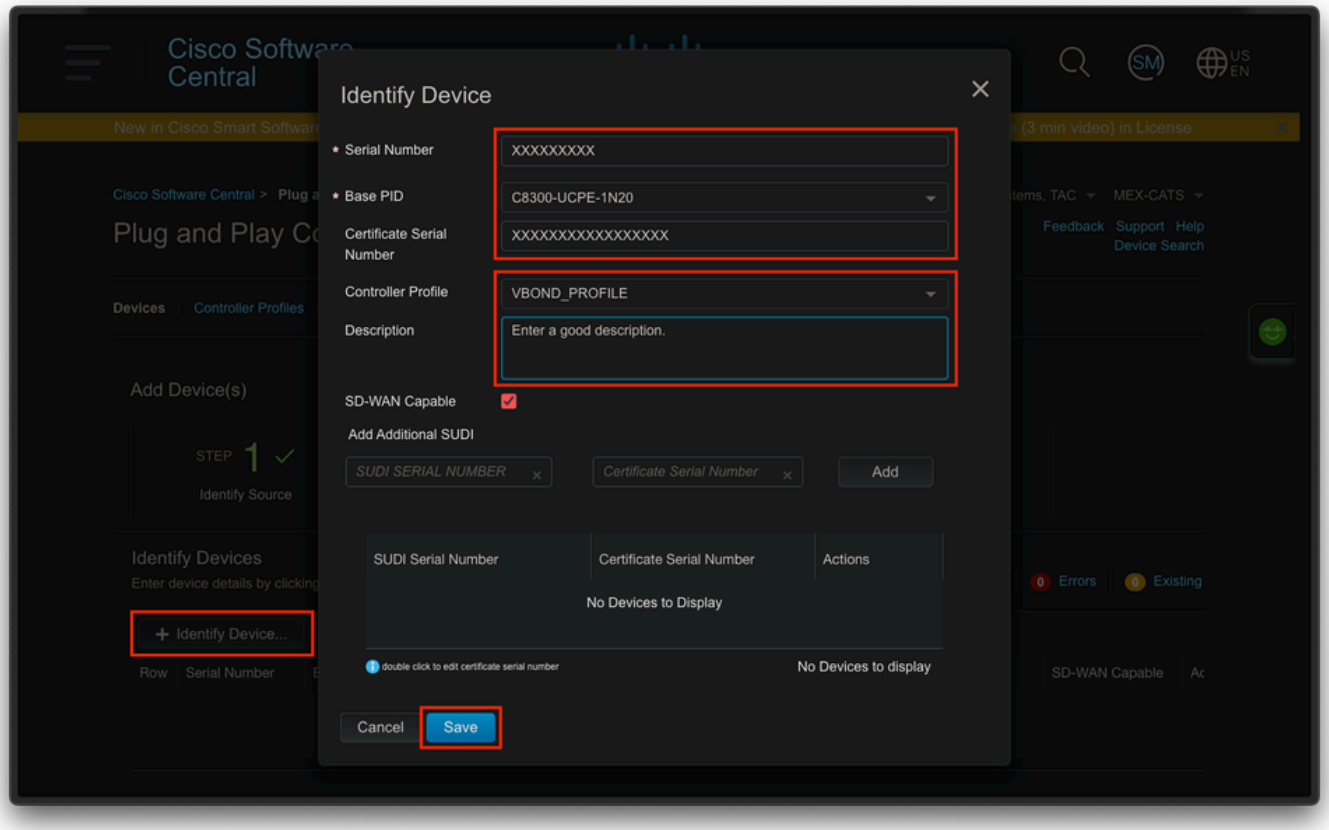


Figura 5. Formulário de identificação do dispositivo.

Depois de salvá-lo, clique em Next para a Etapa 3 e, finalmente, em Submit para a Etapa 4.

PnP em NFVIS

Para obter mais informações sobre as diversas definições de configuração para PnP no NFVIS, abrangendo os modos automático e estático, consulte o recurso: Comandos NFVIS PnP.

Observe que o PnP é habilitado por padrão em todas as versões do NFVIS.

Sincronização do vManage com PnP

Modo on-line

Se o vManage puder acessar a Internet e o portal PnP, você deverá ser capaz de apenas executar uma sincronização SA/VA. Para isso, navegue até Configuration > Devices e clique em um botão de texto que indique Sync Smart Account. As credenciais usadas para fazer login na Cisco Software Central são necessárias. Certifique-se de enviar o push de certificado para todos os controladores.

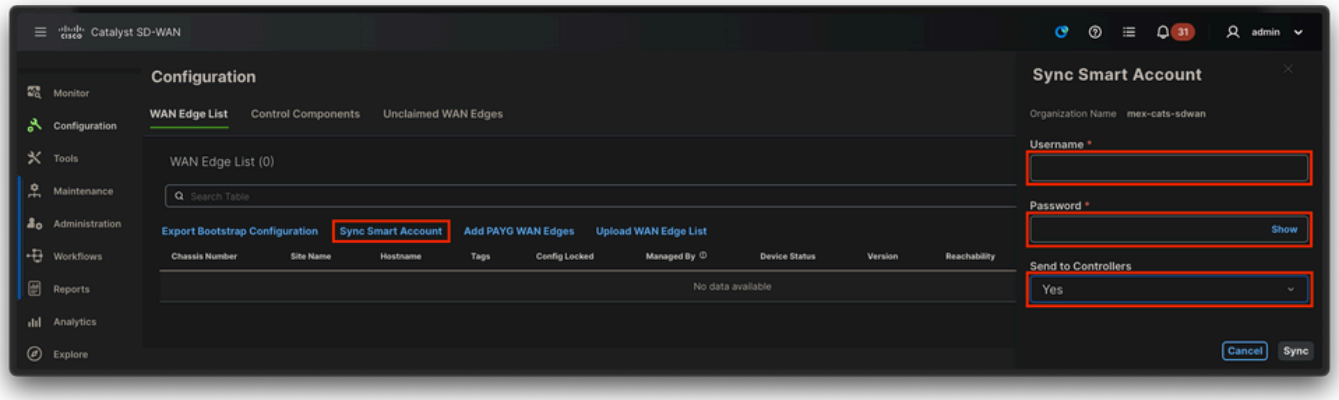


Figura 6. Atualização do Roteador de Borda WAN via sincronização SA/VA.

Modo Offline

Se o vManage estiver em um ambiente de laboratório ou não tiver acesso à Internet, você poderá carregar manualmente um arquivo de provisionamento do PnP que deve conter o SN adicionado à lista de dispositivos. Este arquivo é do tipo .viptela (Viptela Serial File), que pode ser obtido na guia "Controller Profiles":

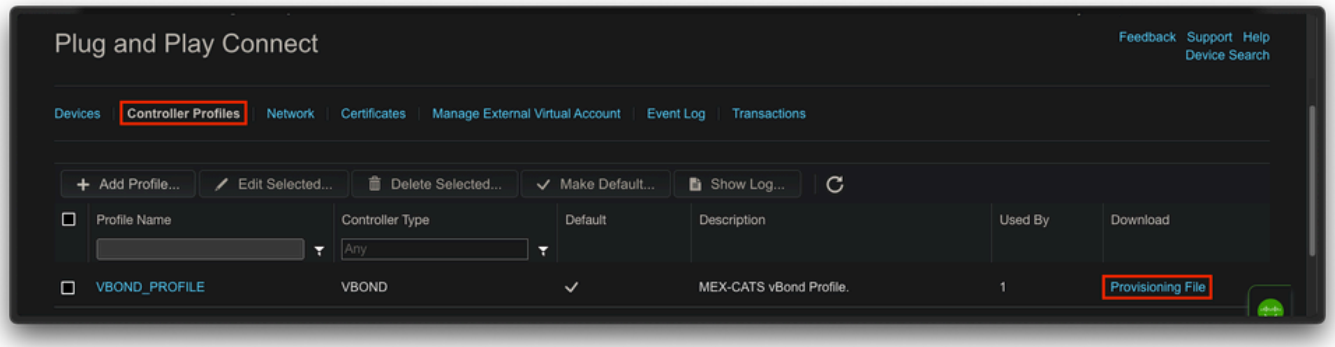


Figura 7. Download do arquivo de provisionamento para atualização da lista de WAN do CEdge.

Para carregar manualmente o arquivo de provisionamento, navegue para Configuration > Devices e clique em um botão de texto que indique Upload WAN Edge List. Uma barra lateral aparece onde você pode arrastar e soltar o respectivo arquivo (se o botão Upload não realçar depois que essas ações foram feitas, clique em Escolha um arquivo e procure o arquivo manualmente dentro da janela pop-up explorador de arquivos). Certifique-se de enviar o push de certificado para todos os controladores.

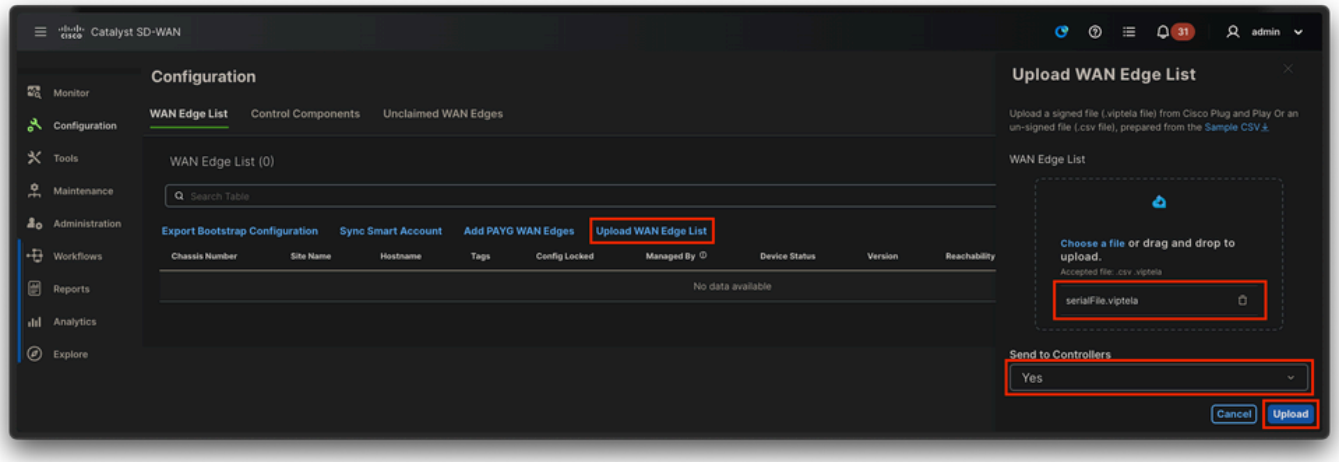


Figura 8. Atualização da lista de WAN usando o arquivo de provisionamento (VSF, Viptela Serial File) baixado do portal PnP.

Após concluir o método Online ou Offline, você deverá ser capaz de ver uma entrada de dispositivo na tabela Lista de Borda da WAN que corresponde ao SN do dispositivo registrado no PnP:

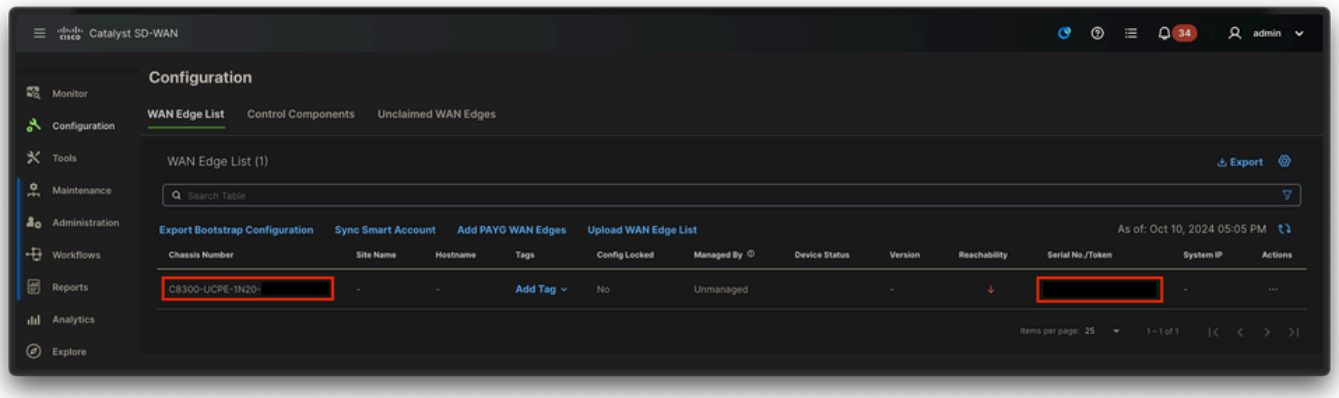
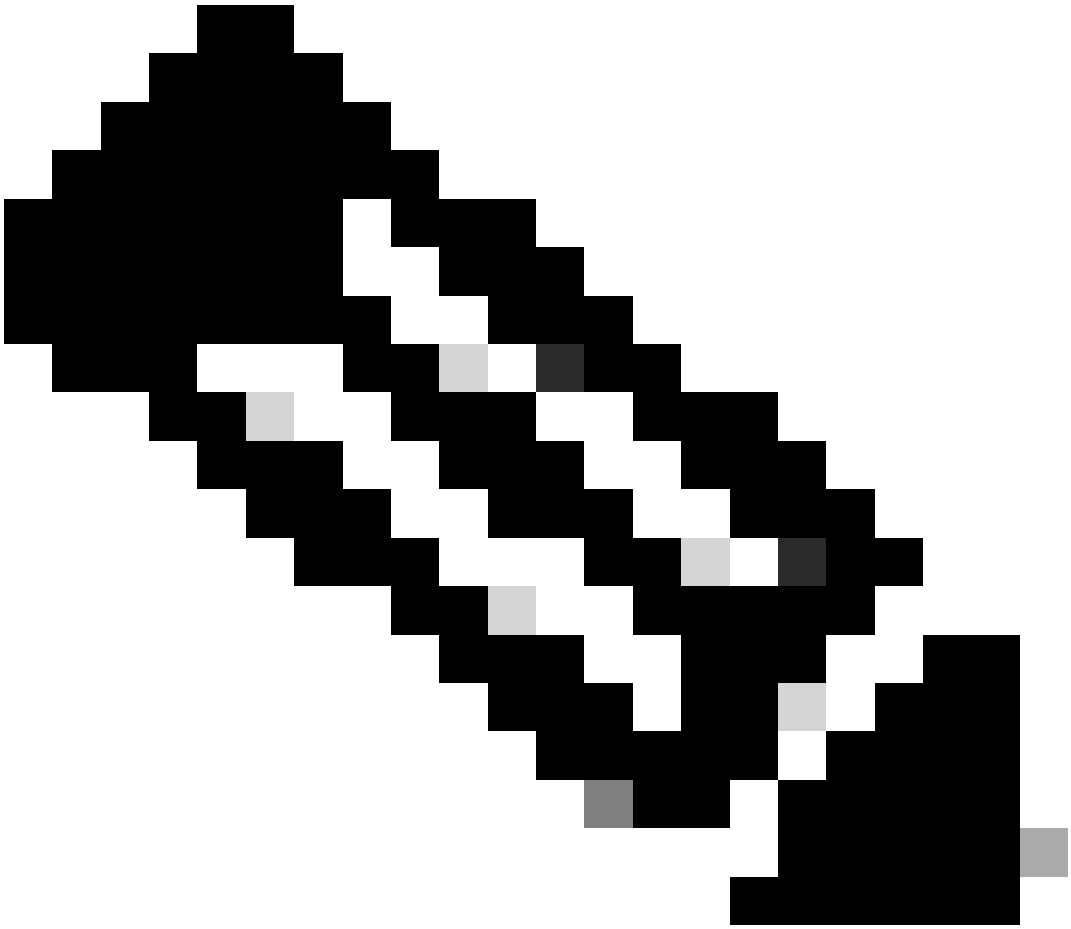


Figura 9. Dispositivo 8300 na lista de borda.

Conexões NFVIS Automáticas de Onboarding e Controle

Se o NFVIS puder resolver devicehelper.cisco.com (acessar o PnP pela Internet), a integração será executada automaticamente. Um sistema NFVIS integrado apresenta automaticamente uma configuração de viptela-system:system e vpn 0 que contém informações básicas do controlador.

A partir do Cisco NFVIS versão 4.9.1, é possível estabelecer uma conexão de controle com o plano de gerenciamento através da porta de gerenciamento. A porta de gerenciamento precisa estar acessível com o SD-WAN Manager para uma conexão bem-sucedida com o plano de controle.



> Note: Cada comando que contém a palavra-chave "system" precisa ser escrito como system:system. Se a tecla Tab for usada para completar, ela se adapta automaticamente a este novo padrão.

```
C8300-UCPE-NFVIS# show running-config viptela-system:system
viptela-system:system
 admin-tech-on-failure
 no vrrp-advt-with-phymac
 sp-organization-name "Cisco Systems"
 organization-name "Cisco Systems"
 vbond
```

```
      port 12346 logging disk enable ! ! ntp parent no enable stratum 5 exit ! !
```

VPN 0 é a VPN de transporte predefinida da solução SD-WAN. Ele não pode ser excluído nem modificado. A finalidade dessa VPN é aplicar uma separação entre as redes de transporte da WAN (a camada subjacente) e os serviços de rede (a camada):

```
C8300-UCPE-NFVIS# show running-config vpn 0
vpn 0
 interface wan-br
  no shutdown
  tunnel-interface
   color gold
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   encapsulation ipsec
  !
 !
!
```

As conexões de controle são sessões DTLS estabelecidas entre diferentes nós (controladores e roteadores de borda) da malha SD-WAN. Como o NFVIS não é uma plataforma de roteamento responsável pelas decisões de roteamento, ele não forma conexões de controle com o vSmarts. Você pode observar um estado de "desafio" para o vManage:

```
C8300-UCPE-NFVIS# show control connection
                                                                                    PEER
PEER    PEER PEER            SITE       DOMAIN PEER                                PRIV  PEER
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                          PORT  PUBLIC IP
-------------------------------------------------------------------------------------------------
vbond   dtls 0.0.0.0         0          0      10.88.247.79                        12346 10.88.247.
vmanage dtls 10.10.10.10     100        0      10.88.247.71                        12946 10.88.247.
```

Isso geralmente indica que não há system-ip, e/ou organization-name está incorretamente ou não

está configurado. O portal PnP e o vBond devem estabelecer o nome da organização e uma vez que a conexão de controle com o vManage tenha sido estabelecida. Caso contrário, empurre essas informações em um NFV Config-Group (suportado a partir de 20.14.1) com o respectivo system-ip e site-id no modelo, ou configure-o estaticamente na subconfiguração viptela-system:system:

```
C8300-UCPE-NFVIS#(config)# viptela-system:system
C8300-UCPE-NFVIS#(config-viptela-system:system)# system-ip
```

```
C8300-UCPE-NFVIS#(config-viptela-system:system)# site-id
```

```
C8300-UCPE-NFVIS#(config-viptela-system:system)# organization-name
```

```
C8300-UCPE-NFVIS#(config-viptela-system:system)# commit Commit complete.
```

Esses itens podem ser encontrados no vManage:

- Nome da organização: Administração > Configurações > Sistema > Nome da Organização
- IP e porta do validador: Administração > Configurações > Sistema > Validador

Depois que a configuração restante for inserida na subconfiguração viptela-system:system, você precisará de conexões de controle ativas/estabelecidas.

```
C8300-UCPE-NFVIS# show control connections
                                                                                    PEER
PEER    PEER PEER            SITE       DOMAIN PEER                                 PRIV  PEER
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                           PORT  PUBLIC IP
-------------------------------------------------------------------------------------------------
vbond   dtls 0.0.0.0         0          0      10.88.247.79                         12346 10.88.247.
vmanage dtls 10.10.10.10     100        0      10.88.247.71                         12946 10.88.247.
```

Não gerenciando NFVIS

Caso deseje retornar o NFVIS ao seu estado "Não gerenciado", você precisará executar estas ações:

1. Remova a entrada do dispositivo do portal PnP:

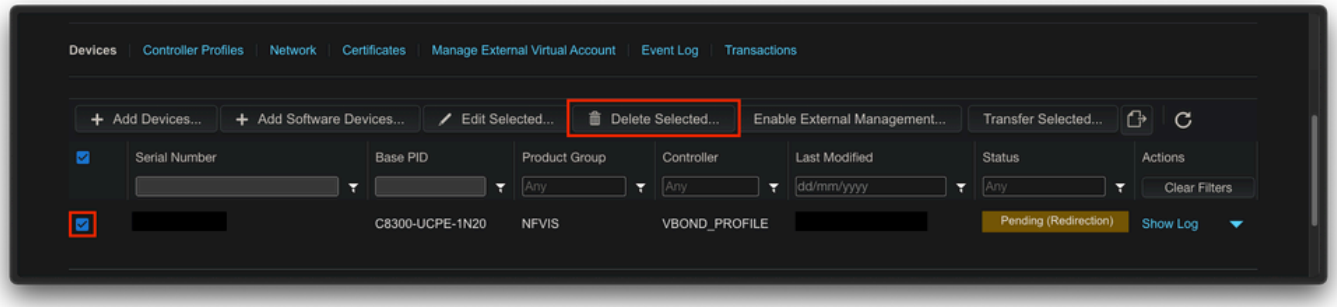


Figura 10. Remoção do dispositivo 8300 do portal PnP.

2. NFVIS de redefinição de fábrica.

```
C8300-UCPE-NFVIS# factory-default-reset all
```

3. Etapas opcionais: Remova o dispositivo da lista vManage Edge:

3.1 Invalide o certificado do dispositivo.

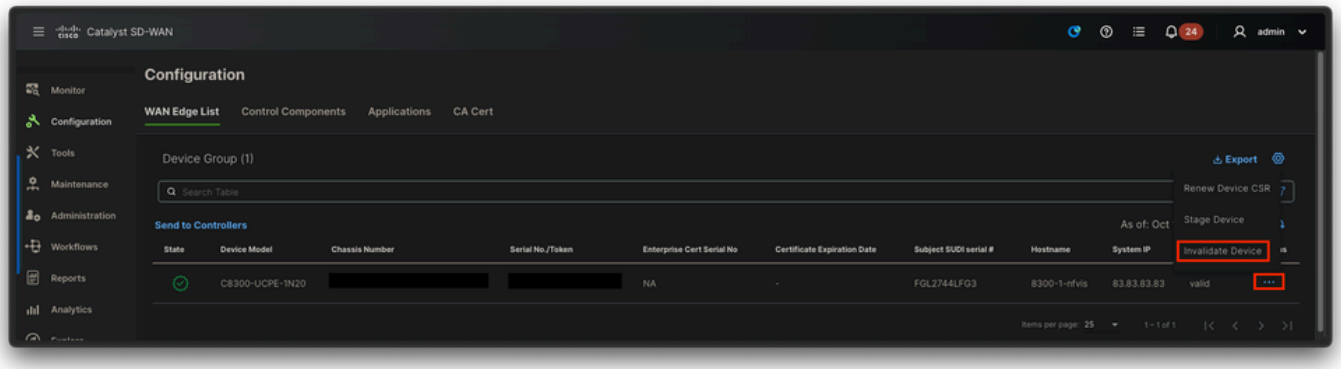


Fig. 11. 8300 invalidação do certificado.

3.2 Exclua o dispositivo da lista de Borda da WAN.

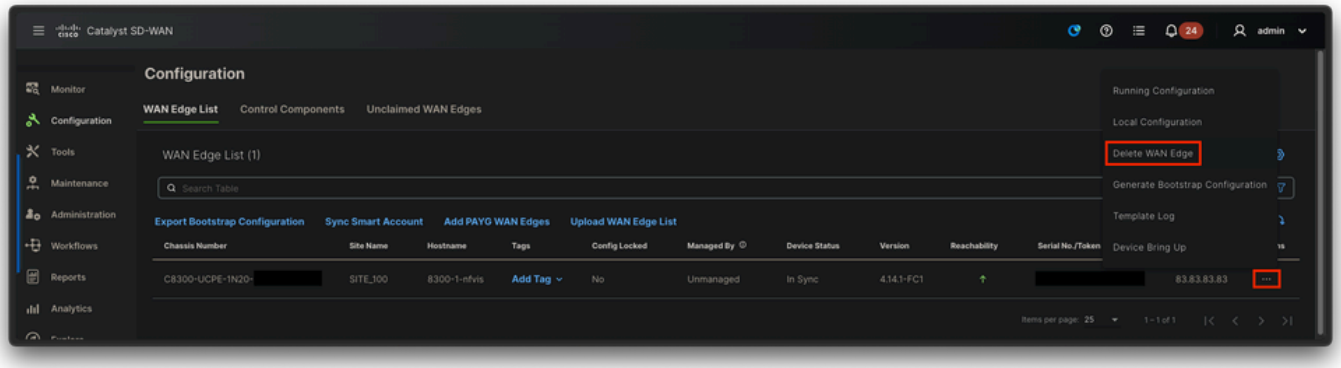


Figura 12. Remoção do 8300 da lista de Borda da WAN.

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.