Ingebouwde NFVIS WAN Edge-apparaten

Inhoud

Inleiding

In dit document wordt het proces beschreven van systemen die geschikt zijn voor NFVIS en die worden aangesloten op een Catalyst™ SD-WAN-omgeving voor beheer en gebruik.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Aangenomen wordt dat:

- SD-WAN controllers (vManager, vBond en vSmart) worden al met geldige certificaten geïmplementeerd.
- Cisco WAN Edge (NFVIS in deze case) heeft bereikbaarheid met de vBond-orchestrator en andere SD-WAN-controllers die via openbare IP-adressen kunnen worden bereikt via de WAN-transport(en)

- De NFVIS-versie moet compatibel zijn met de Control Components Compatibility Guide.

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Hardware

- C8300-UCPE-1N20 (Maar kan worden toegepast op elk platform dat NFVIS ondersteunt)

in Cisco IOS®-software

- vManager 20.14.1
- vSmart & vBond 20.14.1
- NFVIS 4.14.1

PnP-werkstroom

Vertrouwen op de WAN Edge-apparaten gebeurt met behulp van de basiskettingcertificaten die vooraf worden geladen in de productie, handmatig worden geladen, automatisch worden gedistribueerd door vManager, of worden geïnstalleerd tijdens het geautomatiseerde implementatieproces van PnP of ZTP.

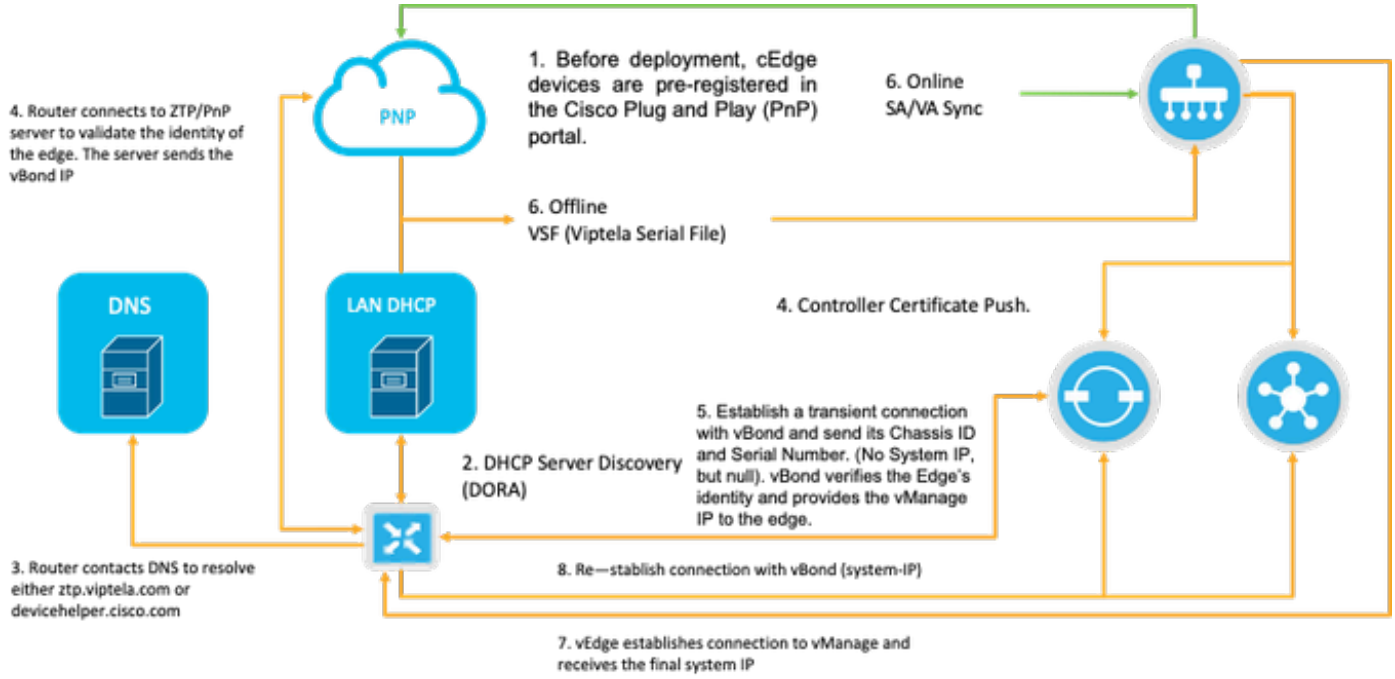
De SD-WAN oplossing maakt gebruik van een toestemmingslijstmodel, wat betekent dat de WAN Edge-apparaten die zich bij het SDWAN-overlay-netwerk mogen aansluiten, vooraf bekend moeten zijn bij alle SD-WAN-controllers. Dit gebeurt door de WAN Edge-apparaten toe te voegen aan het Plug-and-Play connect-portal (PnP) op https://software.cisco.com/software/pnp/devices

Voor deze procedure moet het apparaat altijd worden geïdentificeerd, vertrouwd en in hetzelfde overlay-netwerk op een acceptabele lijst geplaatst. Voor alle SD-WAN componenten dient wederzijdse verificatie plaats te vinden alvorens beveiligde controleverbindingen tot stand te brengen tussen SD-WAN componenten in hetzelfde overlay netwerk. De identiteit van het WAN Edge-apparaat wordt uniek geïdentificeerd aan de hand van het serienummer van het chassis-ID en het certificaat. Afhankelijk van de WAN Edge-router worden certificaten op verschillende manieren geleverd:

- Op hardware gebaseerde vEdge: Certificaat wordt opgeslagen in de ingebouwde Tamper Proof Module (TPM)-chip die tijdens de productie is geïnstalleerd.
- Op hardware gebaseerde Cisco IOS®-XE SD-WAN: het certificaat wordt opgeslagen in de ingebouwde SUDI-chip die tijdens de fabricage is geïnstalleerd.
- Virtueel platform voor Cisco IOS-XE SD-WAN apparaten: geen basiscertificaten (zoals het ASR1002-X-platform) vooraf op het apparaat zijn geïnstalleerd. Voor deze apparaten wordt door vManager een eenmalig wachtwoord (One-Time Password, OTP) verstrekt om het

apparaat te verifiëren met de SD-WAN-controllers.

Om Zero Touch Provisioning (ZTP) uit te voeren, moet een DHCP-server beschikbaar zijn. Als dit niet het geval is, kan een IP-adres handmatig worden toegewezen om verder te gaan met de resterende stappen van het Plug and Play (PnP)-proces.



Afbeelding 1. Werkstroomdiagram van PnP- en WAN Edge-apparaatvertrouwen.

Beveiligd instappen van het NFVIS-compatibele apparaat

SN- en serienummer van certificaat ophalen

De op hardware gebaseerde SUDI (Secure Unique Device Identifier) chip van de voor NFVIS geschikte hardware wordt gebruikt om er zeker van te zijn dat alleen geautoriseerde apparaten een beveiligde TLS of DTLS-besturings-vlakke tunnel kunnen opzetten naar de SD-WAN Manager orchestrator. Verzamel het corresponderende serienummer met behulp van de opdracht voor uitvoerend niveau van het chassis van de support show:

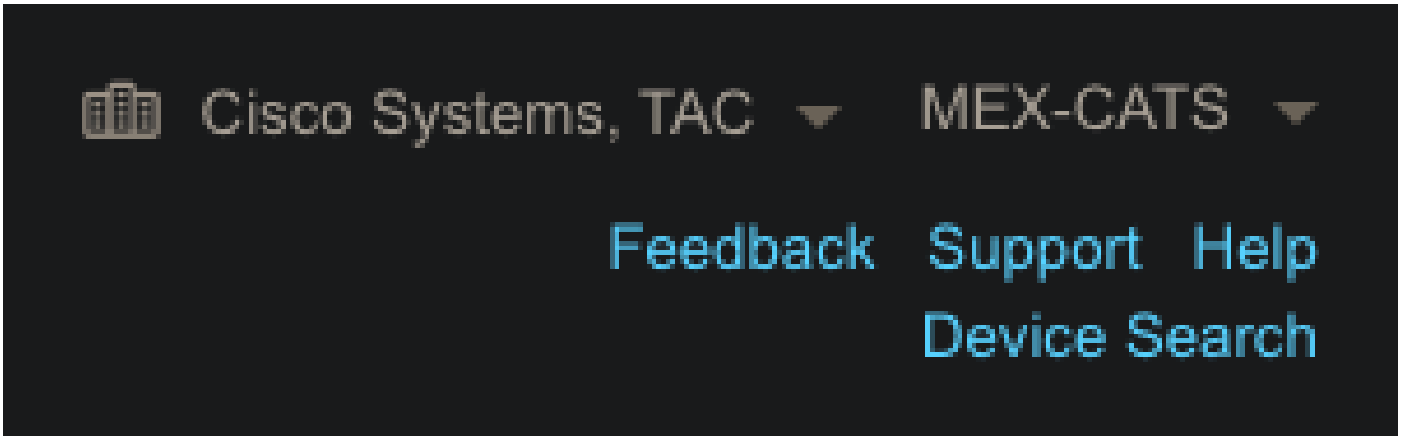
```
C8300-UCPE-NFVIS# support show chassis
Product Name              : C8300-UCPE-1N20
Chassis Serial Num        : XXXXXXXXX
Certificate Serial Num    : XXXXXXXXXXXXXXXXX
```

Het apparaat toevoegen aan de PnP-portal

Navigeer naar https://software.cisco.com/software/pnp/devices en selecteer de juiste Smart Account en Virtual Account voor uw gebruiker of lab omgeving. (als meerdere Smart Accounts

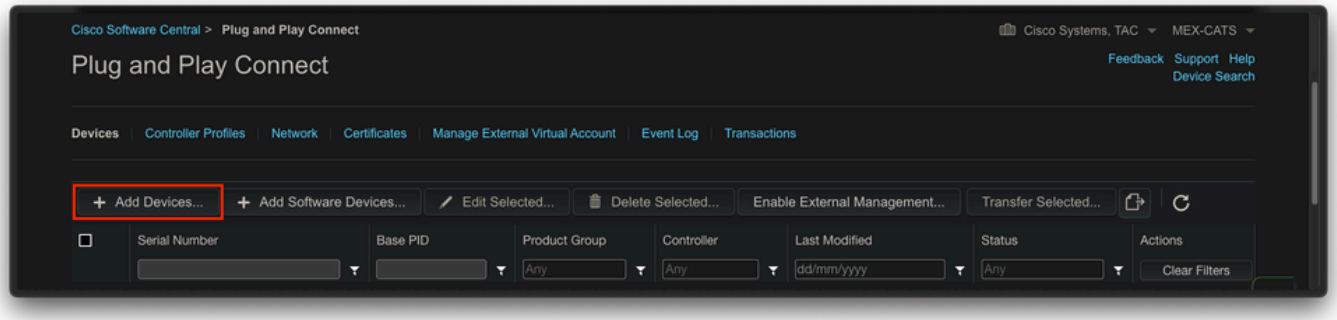
samenvallen in de naam, kunt u ze onderscheiden met de domeinidentificatie).

Als u of uw gebruiker niet weet met welke Smart Account (SA) / Virtual Account (VA) te werken, kunt u altijd zoeken en bestaand/onboarded serienummer in de tekstlink "Apparaatzoeken" om te zien tot welke SA/VA het behoort.



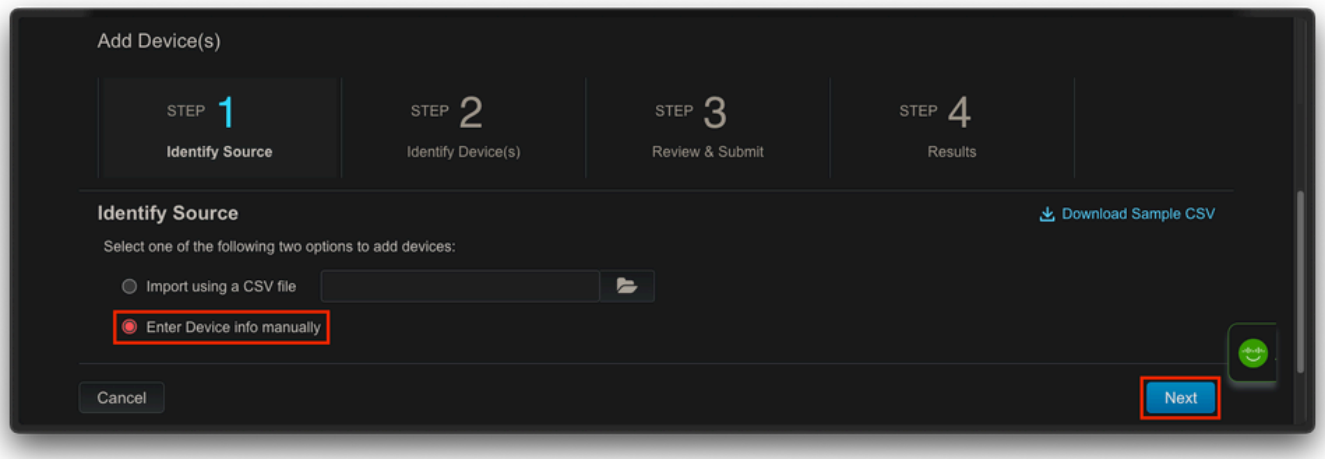
Afbeelding 2. Knop SA/VA-selectie en apparaatzoeken.

Zodra de juiste SA/VA is geselecteerd, klikt u op "Apparaten toevoegen.":



Afbeelding 3. "Apparaten toevoegen..." Knop om te klikken voor fysieke apparaatregistratie.

In dit specifieke geval is slechts één apparaat aan boord, zodat een handmatige invoer volstaat:



Afbeelding 4. "Apparaten toevoegen...", alternatief voor apparaatinformatie-invoer, handmatig (afzonderlijk) of CSV (meervoudig).

Klik voor stap 2 op de knop "+ Identificeer apparaat...". Er verschijnt een formuliermodel. Vul de details in met de informatie die op de ondersteuning wordt getoond toon chassis output van NFVIS en selecteer het corresponderende vBond controller profiel.

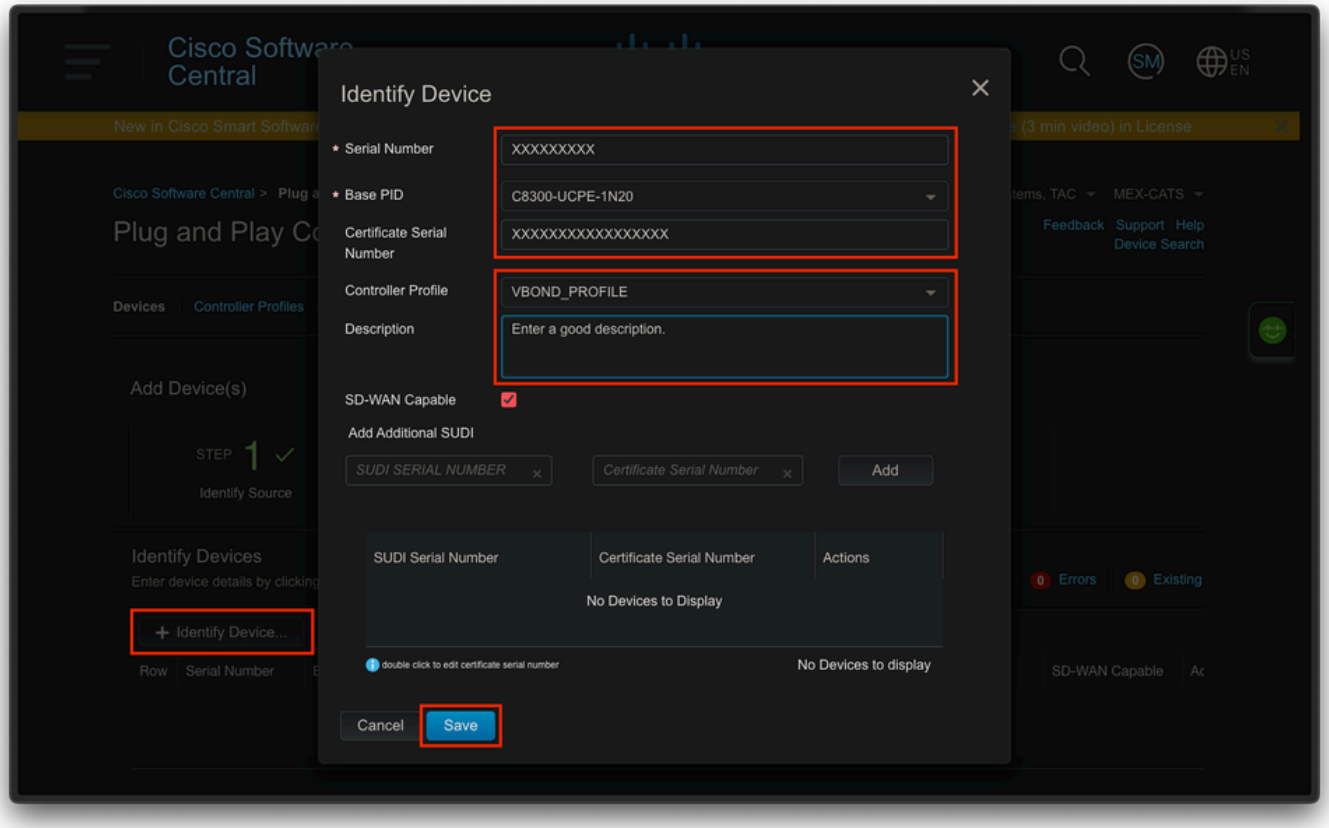


Fig. 5. Identificatieformulier apparaat.

Zodra het is opgeslagen, klikt u op Volgende voor stap 3 en ten slotte op Indienen voor stap 4.

PnP in NFVIS

Raadpleeg voor meer informatie over de verschillende configuratie-instellingen voor PnP binnen NFVIS, voor zowel automatische als statische modi, de bron: [NFVIS PnP Commands.]

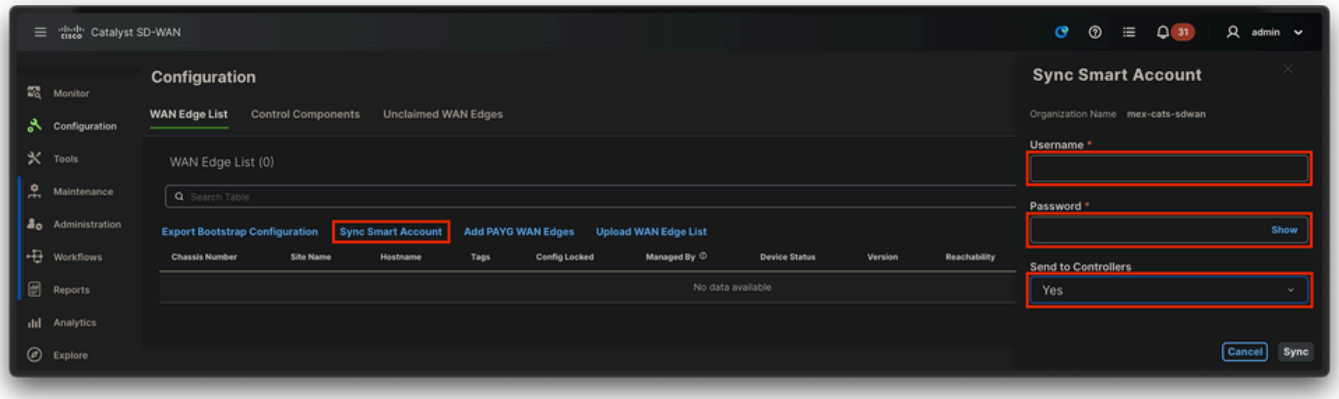
Opgemerkt moet worden dat PnP standaard op alle NFVIS-versies is ingeschakeld.

vManager-synchronisatie met PnP

Online modus

Als vManager internet en het PnP-portal kan bereiken, moet u gewoon een SA/VA sync kunnen uitvoeren. Ga hiervoor naar Configuration > Devices en klik op een tekstknop die Sync Smart Account aangeeft. Er zijn referenties vereist die worden gebruikt om in te loggen op Cisco

Software Central. Zorg ervoor dat het certificaat duw naar alle controllers.



Afbeelding 6. Update van WAN Edge-router via SA/VA-synchronisatie.

Offline modus

Als vManager zich in een laboratoriumomgeving bevindt of geen internettoegang heeft, kunt u handmatig een provisioningbestand van PnP uploaden dat de SN moet bevatten die aan de apparaatlijst is toegevoegd. Dit bestand is van het type .viptela (Viptela Serial File), dat kan worden verkregen van het tabblad "Controllerprofielen":

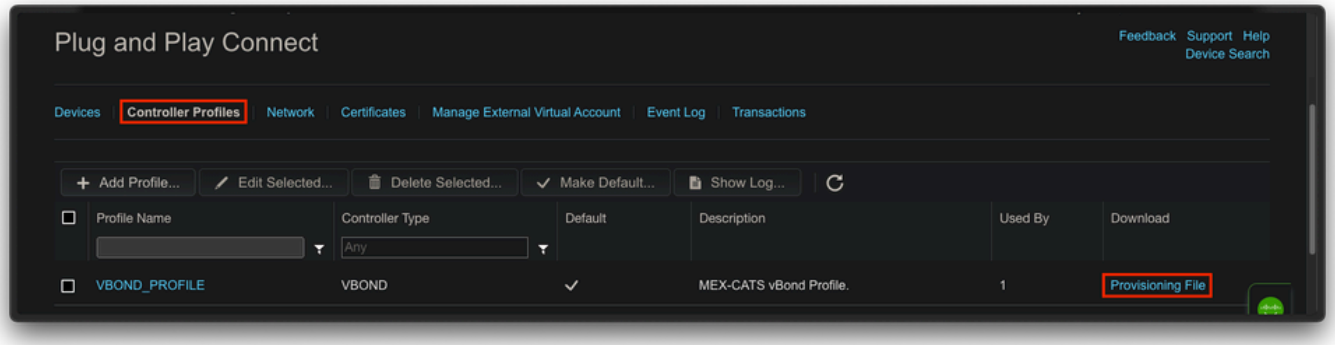


Fig. 7. Provisioning bestand downloaden voor CEdge WAN lijst update.

Voor het handmatig uploaden van het provisioningbestand navigeer je naar Configuration > Devices en klik je op een tekstknop die aangeeft dat WAN Edge List wordt geüpload. Er verschijnt een knoppenbalk waar u het betreffende bestand kunt slepen en neerzetten (als de knop Upload niet markeert nadat deze handelingen zijn uitgevoerd, klikt u op Kies een bestand en zoekt u handmatig naar het bestand in het venster voor pop-upbestandsverkenner). Zorg ervoor dat het certificaat duw naar alle controllers.

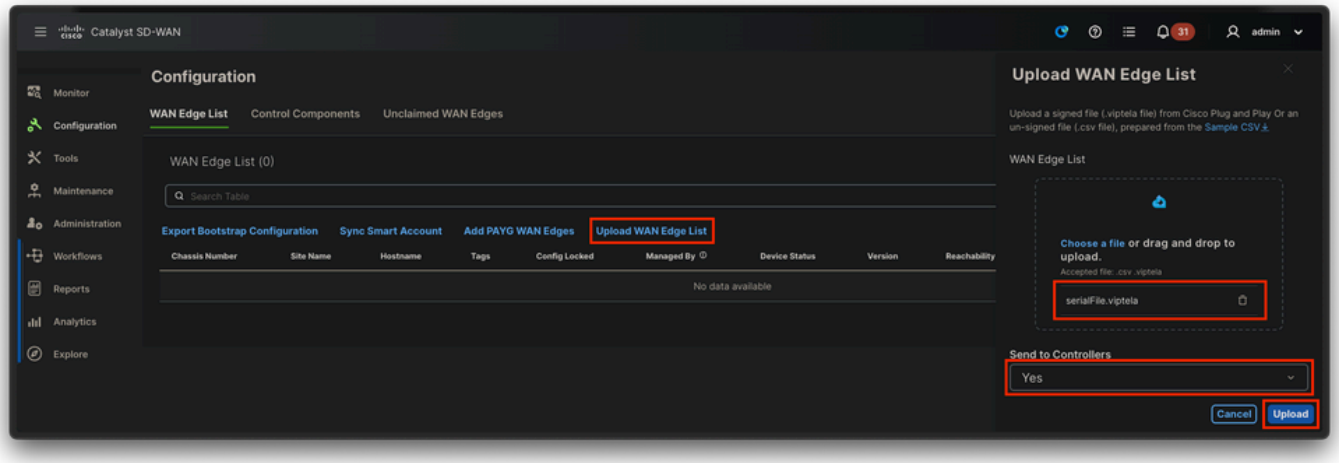
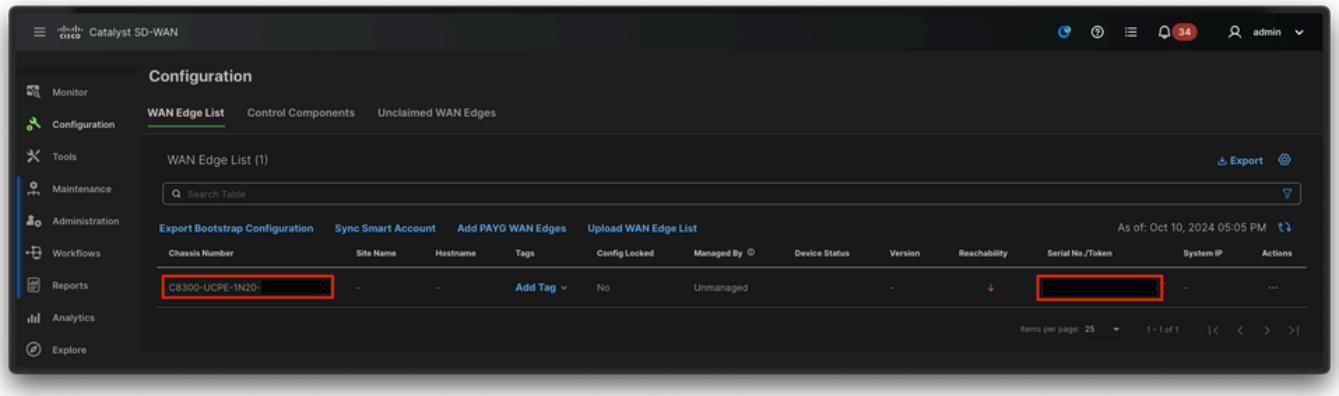


Fig. 8. WAN-lijstupdate met behulp van het provisioningbestand (VSF, Viptela Serial File) dat is gedownload van het PnP-portaal.

Na de voltooiing van de Online of Offline methode, moet u een apparateningang in de lijst van de Lijst van de Rand van WAN kunnen zien die met SN van het apparaat beantwoordt dat in PnP wordt geregistreerd:

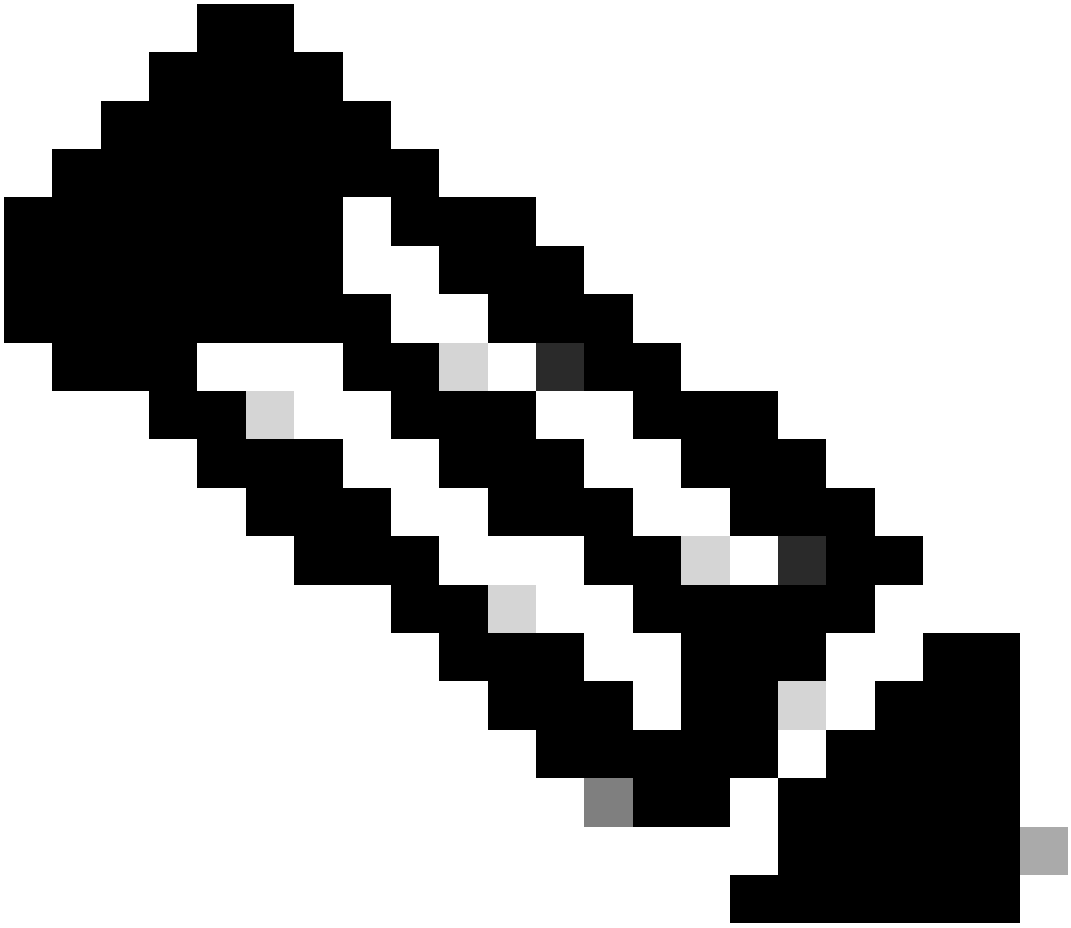


Afbeelding 9. 8300 apparaat in de randlijst.

NFVIS-verbindingen voor automatisch aan boord gaan en controle

Als NFVIS devicehelper.cisco.com (bereik PnP via internet) kan oplossen, wordt onboarding automatisch uitgevoerd. Een onboardsysteem NFVIS presenteert automatisch een viptela-systeem:system en vpn 0 configuratie die basiscontrollerinformatie bevat.

Vanaf Cisco NFVIS release 4.9.1 wordt het opzetten van een besturingsverbinding met het beheervliegtuig via de beheerpoort ondersteund. De beheerpoort moet bereikbaar zijn met SD-WAN Manager voor een succesvolle verbinding met het besturingsplane.



Opmerking: Elke opdracht met het "systeem" sleutelwoord moet worden geschreven als system:system. Als de Tab -toets wordt gebruikt voor voltooiing, past deze automatisch aan deze nieuwe standaard.

```
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 is het vooraf gedefinieerde transport VPN van de SD-WAN oplossing. Dit kan niet worden verwijderd of gewijzigd. Het doel van dit VPN is het afdwingen van een scheiding tussen de WAN transportnetwerken (de onderlaag) en netwerkservices (de overlay):

```
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
  !
 !
!
```

Control connecties zijn DTLS-sessies tussen verschillende knooppunten (controllers en randrouters) van de SD-WAN-fabric. Aangezien NFVIS geen routeringsplatform is dat verantwoordelijk is voor het routeren van beslissingen, vormt het geen controleverbindingen met de vSmarts. Vanuit het vak kunt u een "challenge"-status voor vManager waarnemen:

```
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.
```

Dit duidt er doorgaans op dat er geen systeemip is en/of de organisatienaam verkeerd of helemaal niet is geconfigureerd. Het PnP-portaal en vBond moeten de organisatienaam vaststellen en zodra de controle-verbinding met vManager tot stand is gebracht. Anders, duw deze informatie binnen een NFV Config-Group (Ondersteund vanaf 20.14.1) met respectieve systeem-ip en site-id in het malplaatje, of vorm het statisch binnen viptela-systeem:systeem subconfiguratie:

```
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.
```

Deze items zijn te vinden binnen vManager:

- Naam van de organisatie: Beheer > Instellingen > Systeem > Naam van organisatie
- IP-validator en poort: Beheer > Instellingen > Systeem > Validator

Nadat de resterende configuratie is ingevoerd binnen het viptela-systeem:system subconfiguratie, hebt u actieve/ingestelde besturingsverbindingen nodig.

```
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.
```

NFVIS niet beheren

Als u NFVIS wilt terugbrengen naar de status "niet beheerd", dient u deze handelingen uit te voeren:

1. Verwijder de apparaatingang uit het PnP-portaal:

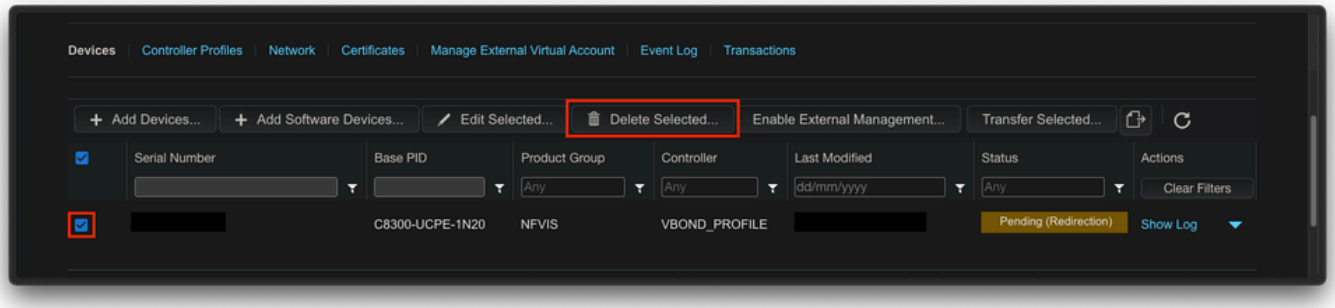


Fig. 10. 8300 apparaatverwijdering van het PnP-portaal.

2. Fabrieksinstellingen van NFVIS hersteld.

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

3. Optionele stappen: Verwijder het apparaat uit de lijst met vManager Edge:

3.1 Het apparaatcertificaat ongeldig maken.

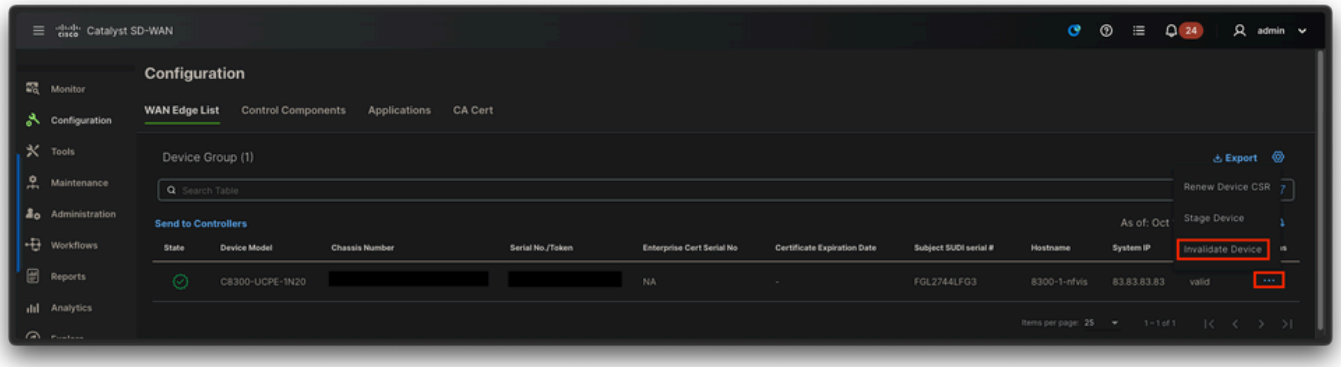
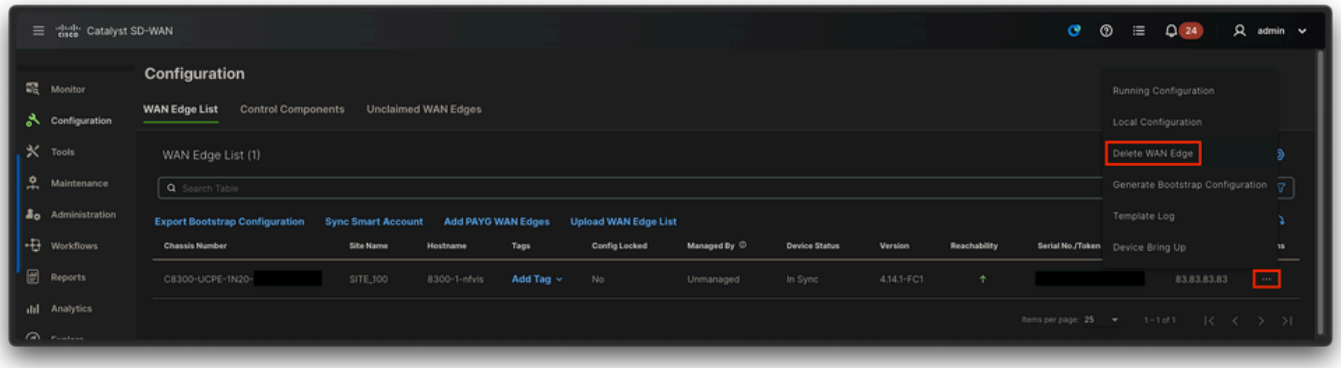


Fig. 11. 8300 ongeldigverklaring van het certificaat.

3.2 Verwijdert het apparaat uit de lijst van WAN Edge.



Afbeelding 12. 8300 verwijderen van de WAN Edge-lijst.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.