Installeer UTD Security Virtual Image op cEdge-routers

Inhoud

Inleiding

Dit document beschrijft hoe u een virtuele image van Unified Threat Defense (UTD) installeert om beveiligingsfuncties in te schakelen op Cisco IOS XE SD-WAN-apparaten.

Voorwaarden

- Voordat u deze functies gebruikt, kunt u de relevante Security Virtual Image uploaden naar de vManager-opslagplaats.
- cEdge-router moet in de beheermodus staan, met sjabloon vooraf als bijlage.
- Maak een Security Policy Template voor Inbraakpreventiesysteem (IPS), Inbraakdetectiesysteem (IDS), URL-filtering (URL-F) of Advanced Malware Protection (AMP) filtering.

Vereisten

- 4000 geïntegreerde services router Cisco IOS XE SD-WAN (ISR4k)
- 1000 geïntegreerde services router Cisco IOS XE SD-WAN (ISR1k)
- 1000v router voor cloudservices (CSR1kv),

- 1000v geïntegreerde services router (ISRv)
- Randplatforms die 8GB DRAM ondersteunen.

Gebruikte componenten

- Cisco UTD virtuele image
- vManager-controller
- cEdge-routers met controleverbindingen met controllers.

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.

Achtergrondinformatie

Cisco UTD-afbeelding heeft een beveiligingsbeleid nodig met betrekking tot de te installeren apparaatsjabloon, en inbraakpreventiesysteem (IPS), inbraakdetectiesysteem (IDS), URL-filtering (URL-F) en Advanced Malware Protection (AMP) op routers.

De software voor Cisco UTD Snort IP Engine downloaden van Software van Cisco

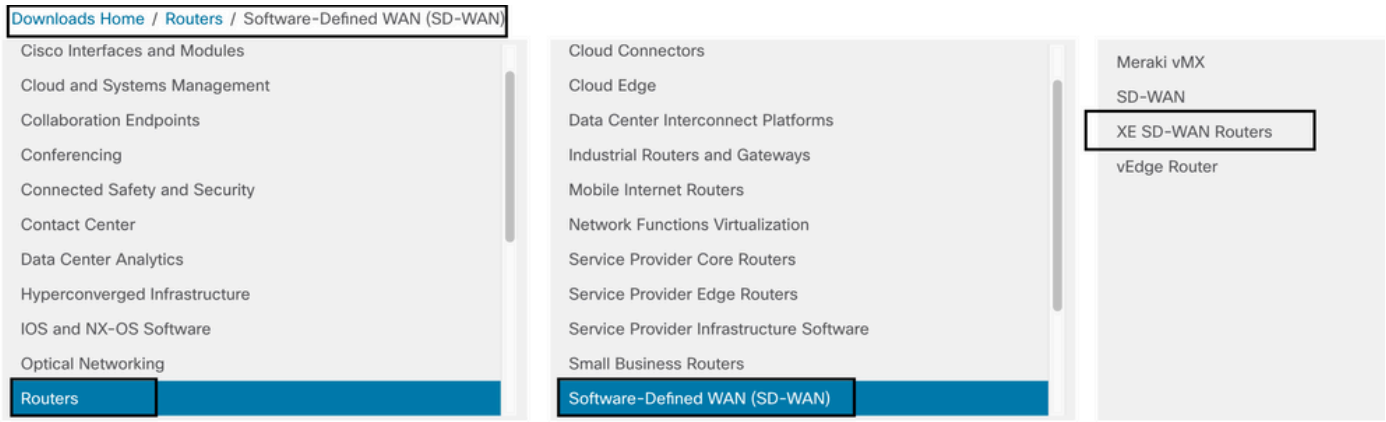
Gebruik het door Cisco UTD virtuele image ondersteunde programma Regex voor de huidige Cisco IOS XE-versie. Gebruik de opdracht **tonen utd motor standaard** versie om de aanbevolen en ondersteunde UTD-afbeelding te valideren.

```
Router01# show utd engine standard version
IOS-XE Recommended UTD Version: 1.0.13_SV2.9.16.1_XE17.3
IOS-XE Supported UTD Regex: ^1\.0\.([0-9]+)_SV(.*)_XE17.3$
```

> **Opmerking** Het pad om de afbeelding te downloaden hangt af van de vraag of de router Cisco IOS XE SDWAN-software (16.x) of Universal Cisco IOS XE-software (17.x) gebruikt.

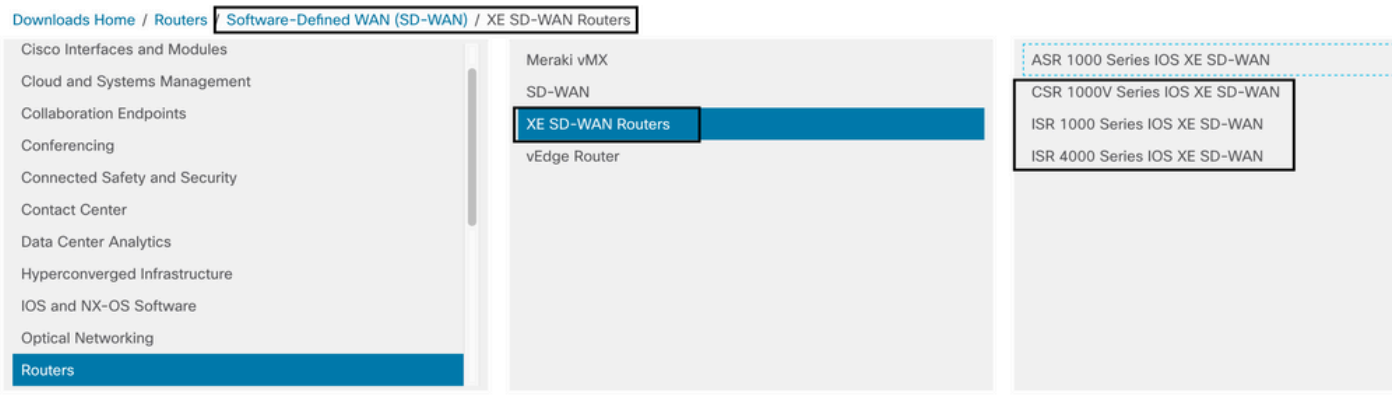
Routers waarop Cisco IOS XE SDWAN-software (16.x) wordt uitgevoerd

Het pad om de Cisco UTD Snel IPS Engine software te krijgen is Routers/ Software-Defined WAN (SD-WAN)/ XE SD-WAN routers / en de Series geïntegreerde router.



Kies het modeltype voor de cEdge-router.

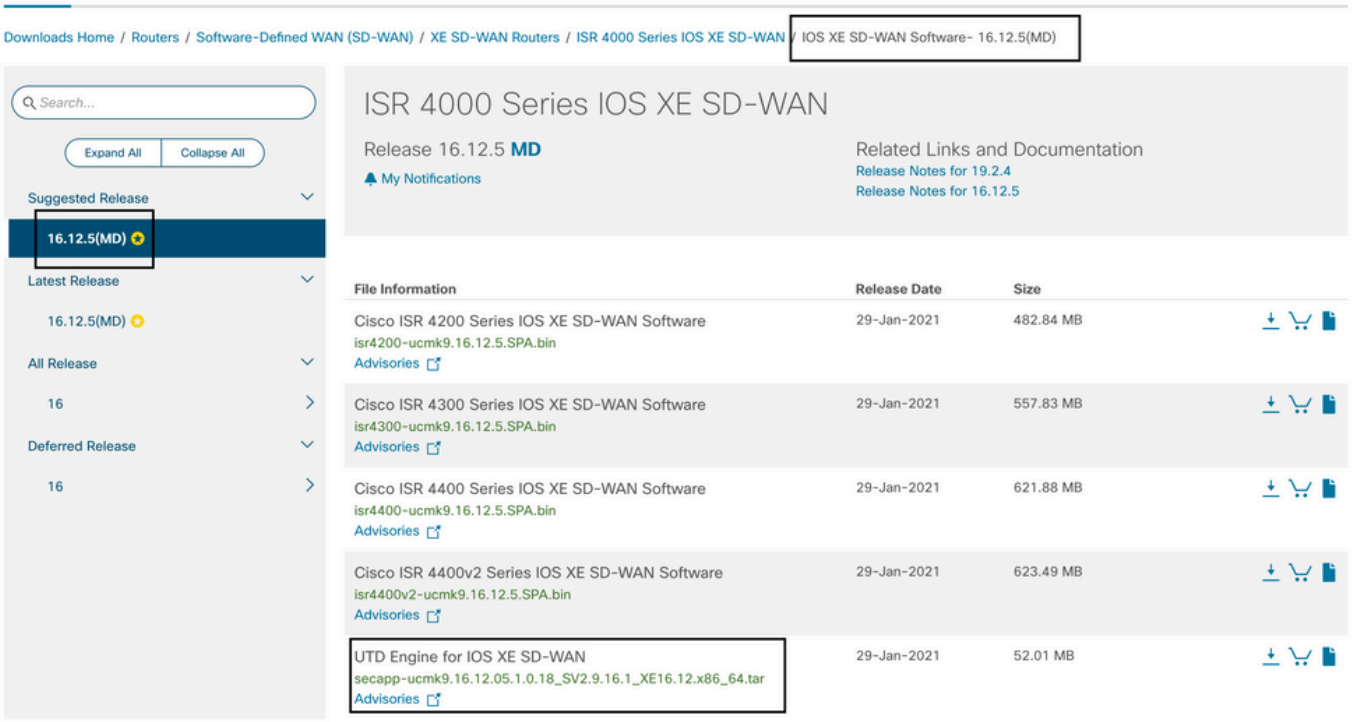
> **Opmerking:** Series Aggregation Services Routers (ASR) zijn niet beschikbaar voor UTD-functies.



Nadat u het type router model kiest, selecteer de **Cisco IOS XE SD-WAN software** optie om het UTD pakket voor cEdge op 16.x versie te krijgen.

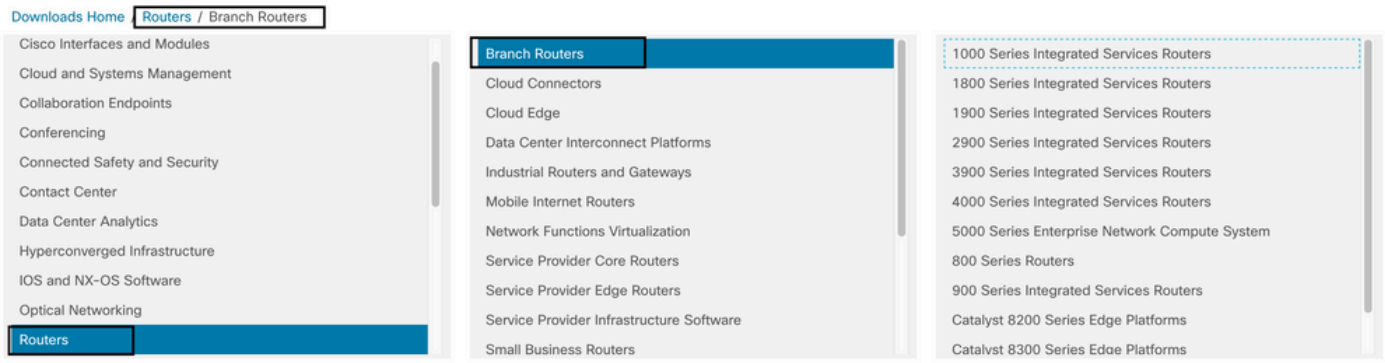
> **Opmerking** Het downloadpad om de virtuele Cisco UTD-afbeelding voor 16.x-code voor cEdge-routers te kiezen, toont ook **Cisco IOS XE-**softwareoptie. Dat is het pad om upgradecodes van cEdge alleen voor 17.x te kiezen, maar er is niet gevonden het UTD virtuele beeld voor versie 17.x. Cisco Unified regular Cisco IOS XE en Cisco IOS XE SDWAN-codes op 17.x en hoger, zodat het pad om de Cisco UTD virtuele afbeelding voor 17.x te verkrijgen, hetzelfde is als de reguliere Cisco IOS XE-codes.

Kies de huidige versie van de cEdge en download het UTD-pakket voor die versie.

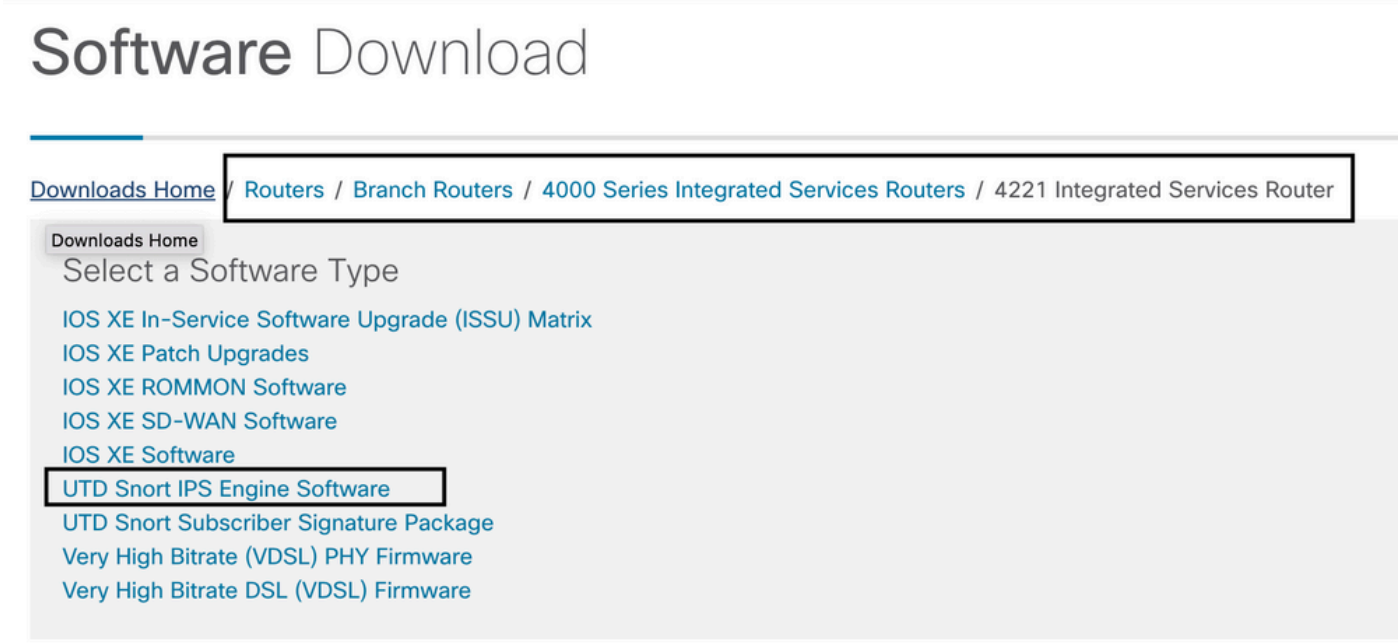


Routers waarop Cisco IOS XE-software (17.x) wordt uitgevoerd

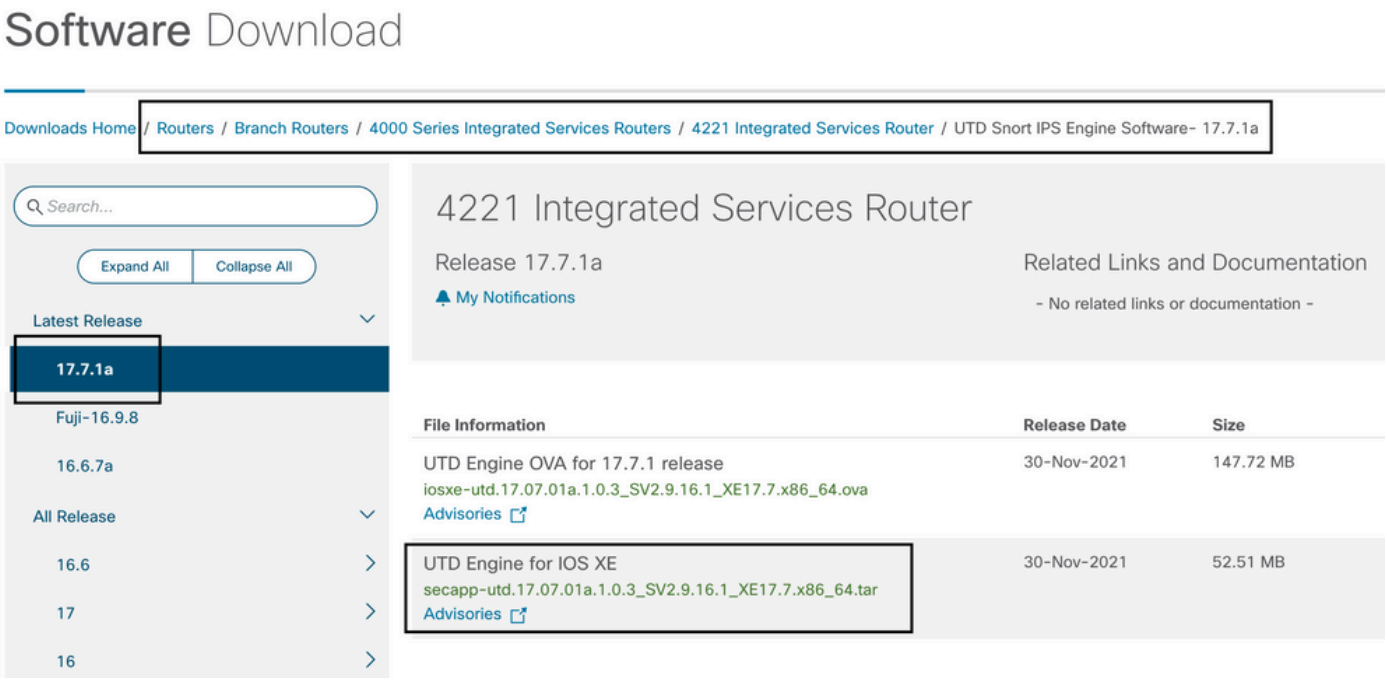
Cisco IOS XE release 17.2.1r en het nieuwste gebruik van het universalk9-image om zowel Cisco IOS XE SD-WAN als Cisco IOS XE op Cisco IOS XE-apparaten te implementeren.
UTD Snort IPS Engine software bevindt zich in **Routers > Branch Routers > Series geïntegreerde router**.



Nadat u het modeltype van de router hebt gekozen, selecteert u de **UTD Snel IPS Engine Software**.



Selecteer de huidige versie van de router en download het UTD-pakket voor de geselecteerde versie.

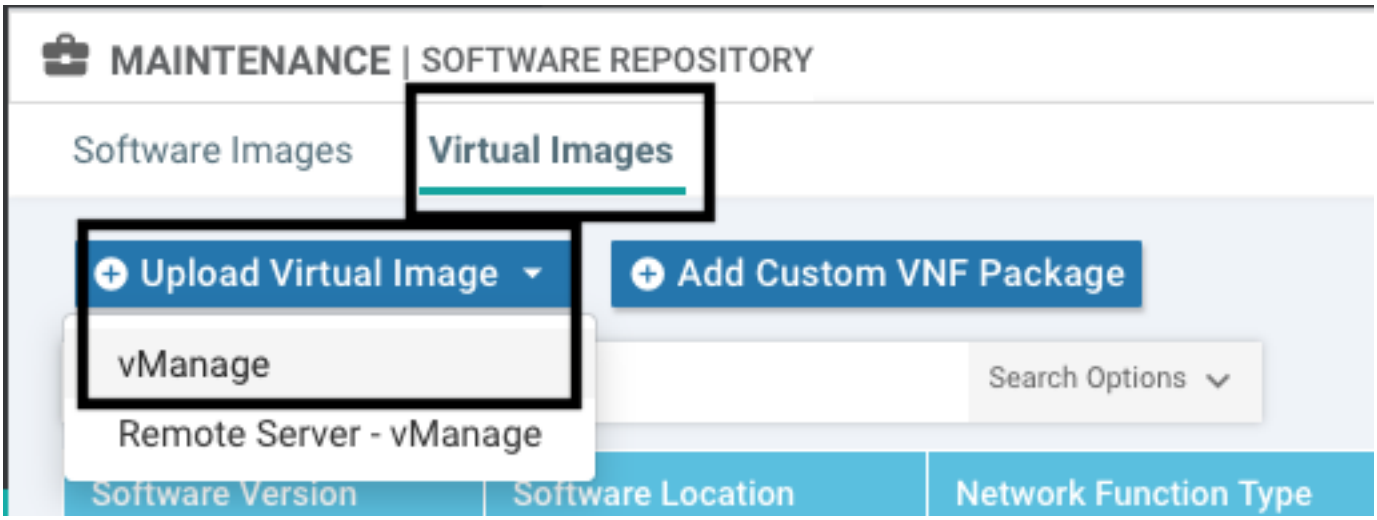


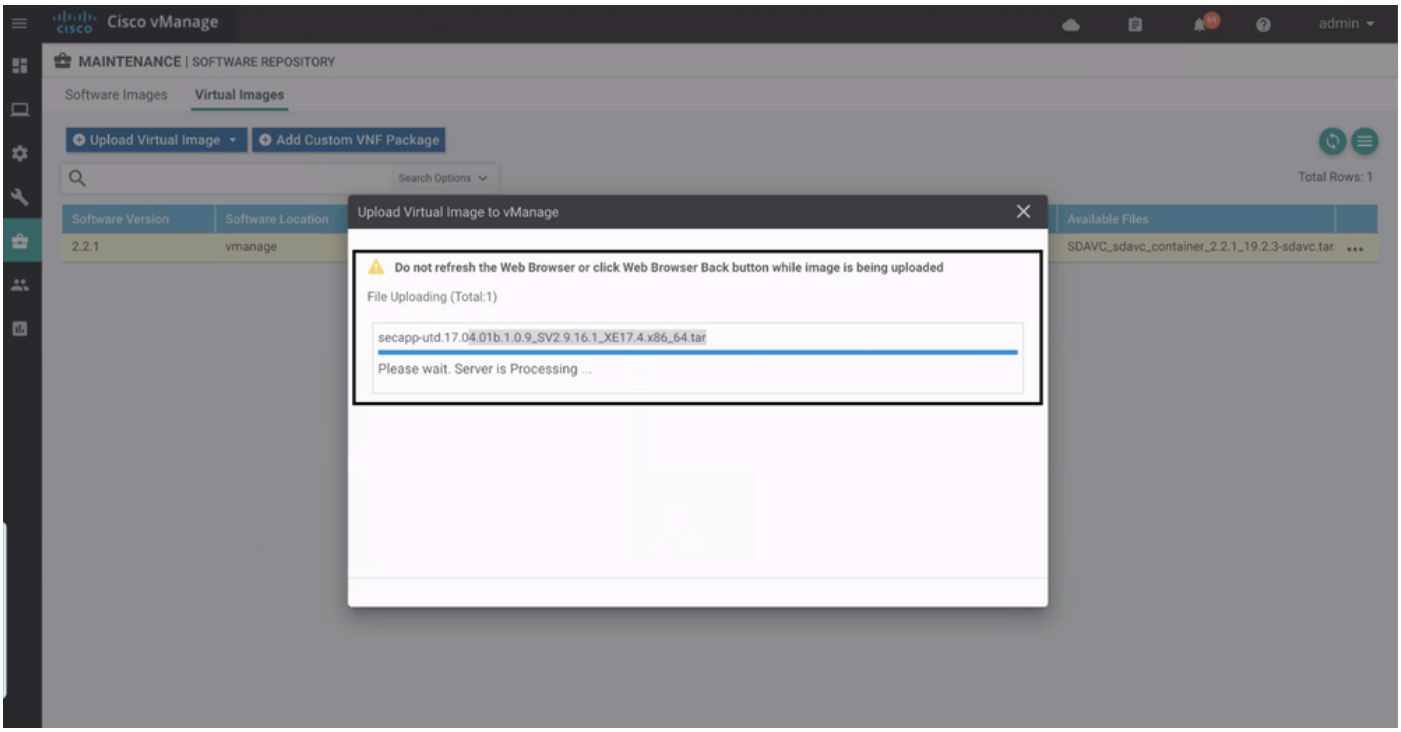
Opmerking: Cisco ISR1100X Series-routers (Cisco Nutella Routers SR1100X-4G/6G) die Cisco IOS XE-software uitvoeren in plaats van Viptela-code zijn gebaseerd op x86_x64. Het virtuele beeld dat Cisco UTD publiceert voor ISR4K kan eraan werken. U kunt dezelfde versie van Cisco UTD-beeldcode installeren die wordt ondersteund door Regex voor de huidige Cisco IOS XE SDWAN-versie op de Nutella-router. Gebruik de opdracht **tonen utd motor standaard versie** om de aanbevolen en ondersteunde regex Cisco UTD-afbeelding te valideren.

Configureren

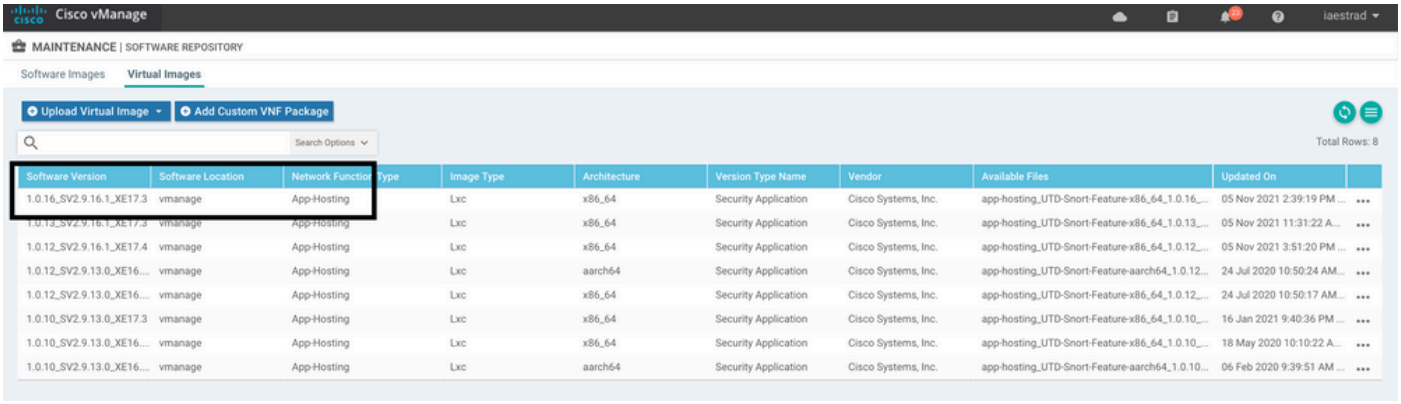
Stap 1. Virtuele afbeelding uploaden

Zorg ervoor dat uw virtuele afbeelding overeenkomt met de huidige Cisco IOS XE SDWAN-code op de cEdge en upload deze naar de opslagplaats.
Ga naar **Onderhoud > Software Repository > Virtual Image > Upload Virtual Image > vManager.**



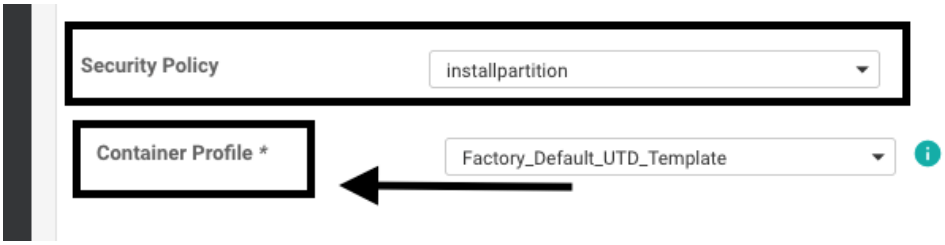


Zodra de virtuele afbeelding van Cisco UTD succesvol is geüpload, controleert u of deze zich in de repository bevindt.



Stap 2. Voeg beveiligingsbeleid en subsjabloon voor containerprofiel toe aan apparaatsjabloon

Voeg het eerder gemaakte beveiligingsbeleid toe aan de apparaatsjabloon. Het beveiligingsbeleid moet een IPS/IDS-, URL-F- of AMP-filteringsbeleid hebben om de apparaatsjabloon aan te passen. Open het containerprofiel automatisch. Gebruik het standaardcontainerprofiel of wijzig het indien nodig.

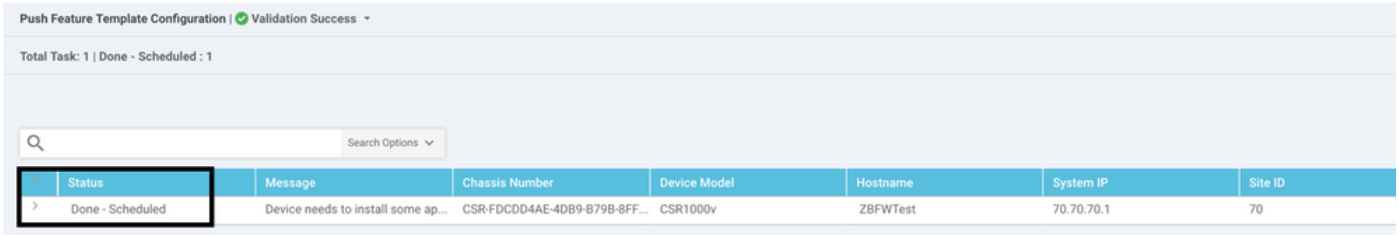


Stap 3. Werk de apparaatsjabloon bij of voeg deze toe met het beveiligingsbeleid en het containerprofiel

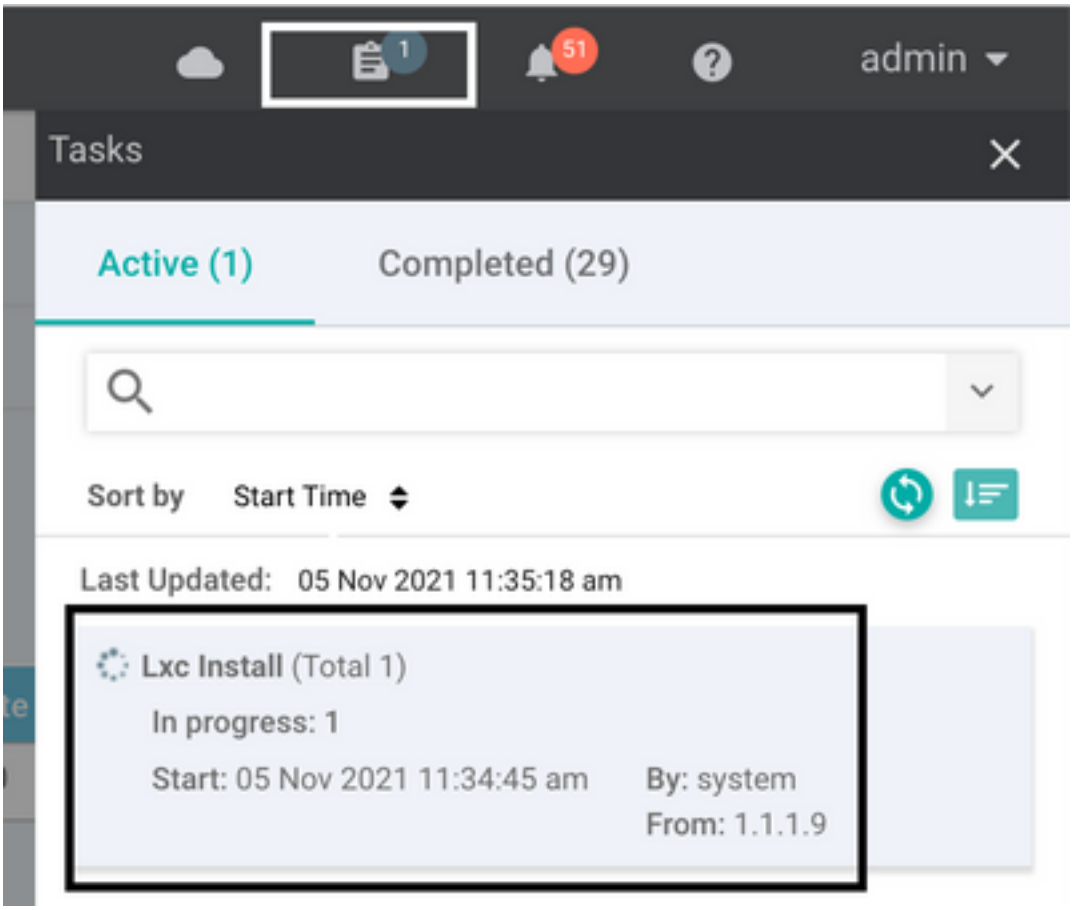
Werk de sjabloon bij of voeg deze toe aan de cEdge-router. Opmerking over het configuratieverschil dat de configuratie van de app en de UTD-engine voor de functie IPS/IDS, URL-F of AMP-filtering zijn geconfigureerd.

```
258  app-hosting appid utd
259   app-resource package-profile cloud-low
260   app-vnic gateway0 virtualportgroup 0 guest-interface 0
261    guest-ipaddress 192.168.1.2 netmask 255.255.255.252
262   !
263   app-vnic gateway1 virtualportgroup 1 guest-interface 1
264    guest-ipaddress 192.0.2.2 netmask 255.255.255.252
265   !
266   start
267  !
258 268  lldp run
259 269  nat64 translation timeout tcp 60
260 270  nat64 translation timeout udp 1
271  utd multi-tenancy
272  utd engine standard multi-tenancy
273   threat-inspection profile GPC_IPS_v06_copy_copy
274    threat detection
275    policy security
276    logging level warning
277   !
278   utd global
279   !
280  !
281  policy
282   no app-visibility
283   no flow-visibility
284   no implicit-acl-logging
285   log-frequency        1000
286  !
```

Sjabloonstatus wijzigen in **Klaar-gepland** omdat vManager opmerkte dat de toegepaste configuratie UTD-motorfuncties heeft, dus vManager bepalen dat de cEdge de virtuele afbeelding nodig heeft die is geïnstalleerd om de UTD-beveiligingsfuncties te gebruiken.



Nadat de sjabloon naar de planningsstatus is verplaatst, wordt een nieuwe taak **in uitvoering** weergegeven in het taakmenu. De nieuwe taak is de **LXC-installatie**, wat betekent dat de beheerder automatisch de installatie van het virtuele beeld naar de cEdge start voordat de nieuwe configuratie wordt geduwd.

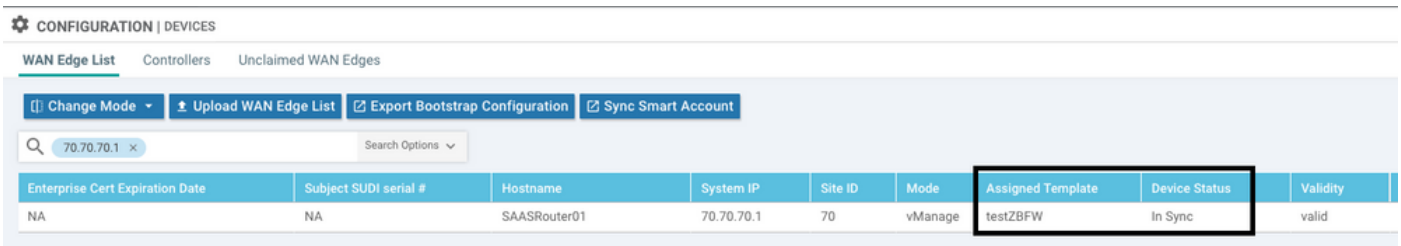


Nadat de LX-container is geïnstalleerd, drukt vManager de configuratie vooraf met de UTD-functies. Er is geen nieuwe taak hiervoor omdat de configuratie eerder was gepland.

Verifiëren

Controleer of de cEdge synchroon is met vManager en de bijbehorende sjabloon.

Navigeren naar **configuratie > Apparaten**



Controleer of de Cisco UTD-versie is geïnstalleerd:

```
Router02# show utd engine standard version
UTD Virtual-service Name: utd
IOS-XE Recommended UTD Version: 1.0.12_SV2.9.16.1_XE17.4
IOS-XE Supported UTD Regex: ^1\.0\.([0-9]+)_SV(.*)_XE17.4$
UTD Installed Version: 1.0.12_SV2.9.16.1_XE17.4         <<<<<<<<<<<<<<<<<<
```

> **Opmerking:** de geïnstalleerde versie van UTD kan niet worden uitgevoerd op **niet-ondersteunde** status.

Controleer of UTD **actief** is met de volgende uitvoer:

```
Router02# show app-hosting list
App id                                   State
---------------------------------------------------------
utd                                      RUNNING      <<<<<<<<<<<<<<<<<<
```

Het volgende bevel vat de vorige bevelen samen en toont de huidige status en de versie:

```
Router02# show app-hosting detail appid utd
App id                 : utd
Owner                  : ioxm
State                  : RUNNING      <<<<<<<<<<<<<<<<<<<<<<<<
Application
  Type                 : LXC
  Name                 : UTD-Snort-Feature
  Version              : 1.0.12_SV2.9.16.1_XE17.4    <<<<<<<<<<<<<<<<<
  Description          : Unified Threat Defense
  Path                 : /bootflash/.UTD_IMAGES/iox-utd_1.0.12_SV2.9.16.1_XE17.4.tar
  URL Path             :
Activated profile name : cloud-low

Resource reservation
  Memory               : 2048 MB
  Disk                 : 861 MB
  CPU                  :
  CPU-percent          : 7 %
  VCPU                 : 0
```

Toon UTD motor standaard status opdracht toont de gezondheidsstatus van de UTD motor en lijst tijd het krijgt de handtekeningupdate.

```
Router02# show utd engine standard status
Engine version       : 1.0.6_SV2.9.13.0_XE17.2
Profile              : Cloud-Low
System memory        :
              Usage  : 20.10 %
              Status : Green
Number of engines    : 1

Engine        Running    Health     Reason
=======================================
Engine(#1):   Yes        Green      None      <<<<<<<<<<<<<<<<<<<<<<<<<<<
=======================================================

Overall system status: Green    <<<<<<<<<<<<<<<<<<<<<<<<<

Signature update status:
========================
```

```
Current signature package version: 29130.156.s
Last update status: Successful
Last successful update time: Wed Nov 25 07:27:35 2020 EDT   <<<<<<<<<<<<<<<<<<<
Last failed update time: None
Last failed update reason: None
Next update scheduled at: None
Current status: Idle
```

Controleer of de functies zijn ingeschakeld en gebruik de volgende opdracht:

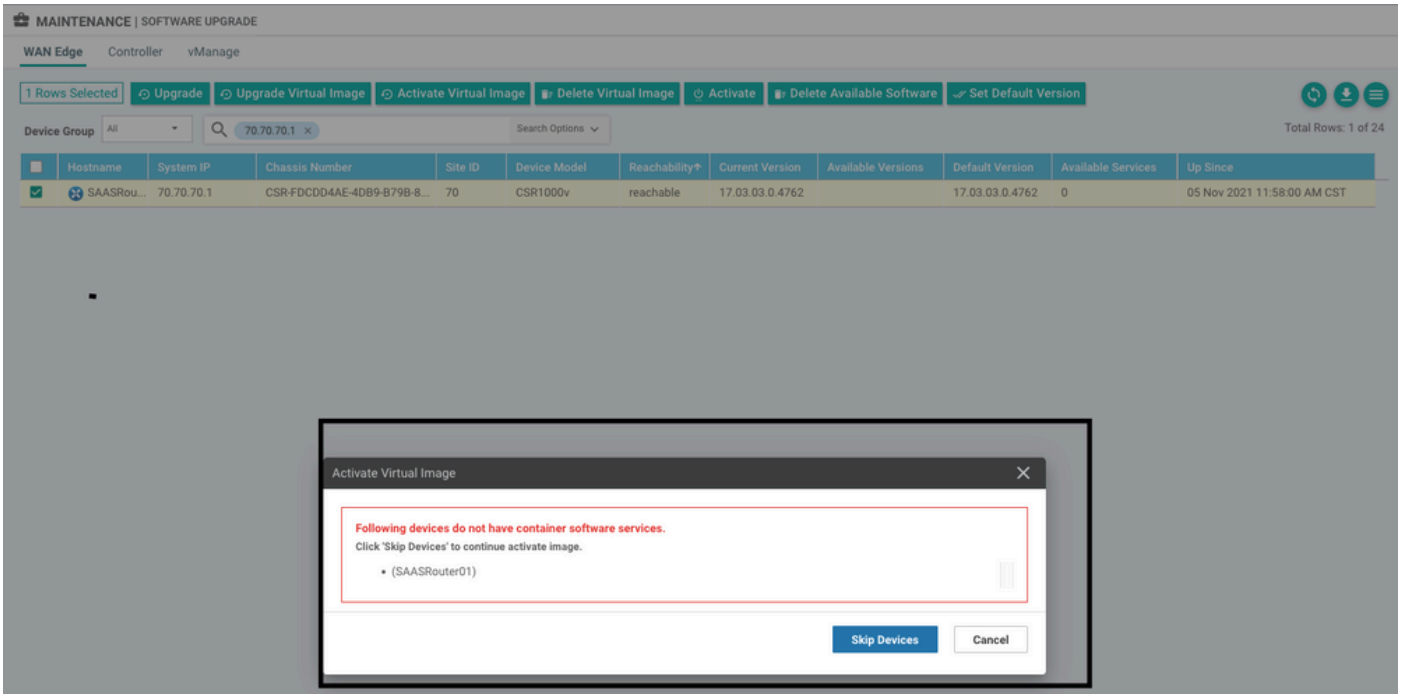
```
Router02# show platform hardware qfp active feature utd config
Global configuration
  NAT64: disabled
  Drop pkts: disabled
  Multi-tenancy: enabled
  Data plane initialized: yes
  TLS Decryption Policy: disabled
  Divert controller mode: enabled
  SN threads: 12
  CFT inst_id 0 feat id 2 fo id 2 chunk id 13
  Max flows: 55000
  SN Health: channel: Threat Defense : Green
  SN Health: channel: Service : Down

  Context Id: 0, Name: Global domain Security Context

   Ctx Flags: (0x1c70001)
        Engine: Standard
        State            : Enabled
        SN Redirect Mode : Fail-open, Divert
        Threat-inspection: Enabled, Mode: IPS
        Domain Filtering : Not Enabled
        URL Filtering    : Enabled   <<<<<<<<<<<
        File Inspection  : Enabled   <<<<<<<<<<<
        All Interfaces   : Enabled
```

Veelvoorkomende problemen

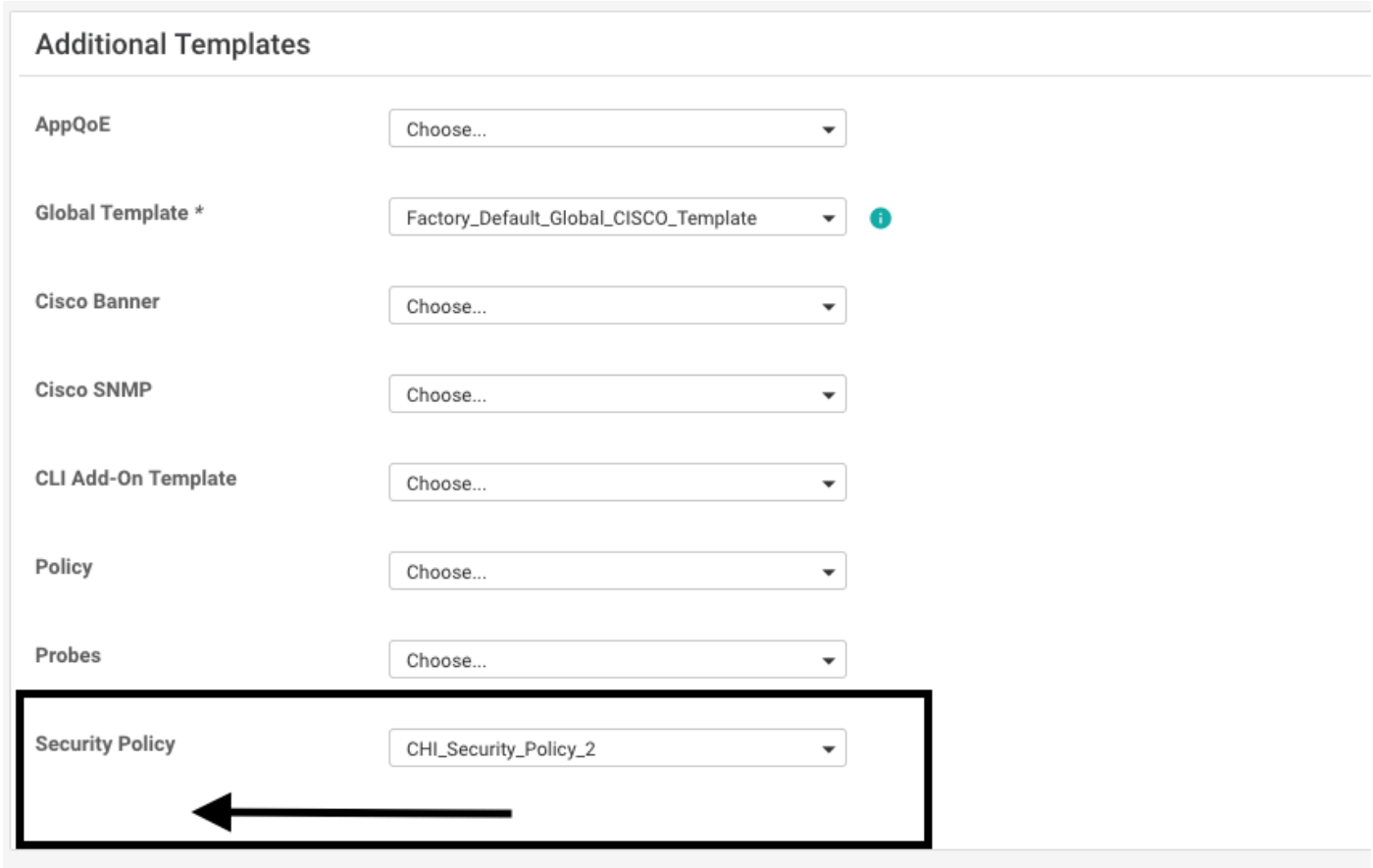
PROBLEEM 1. Fout: Volgende Apparaten hebben geen Container Software Services

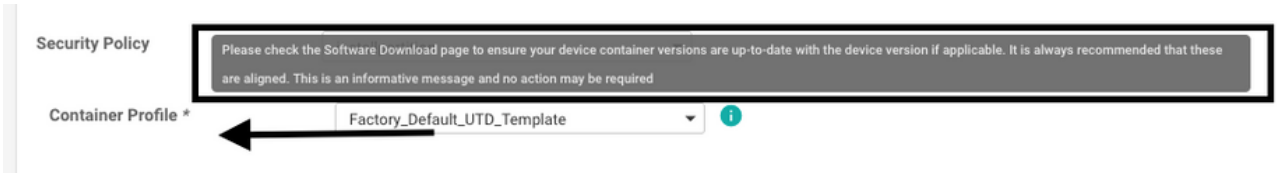
Activeer het virtuele beeld.

Navigeren naar **onderhoud > software > activeren**



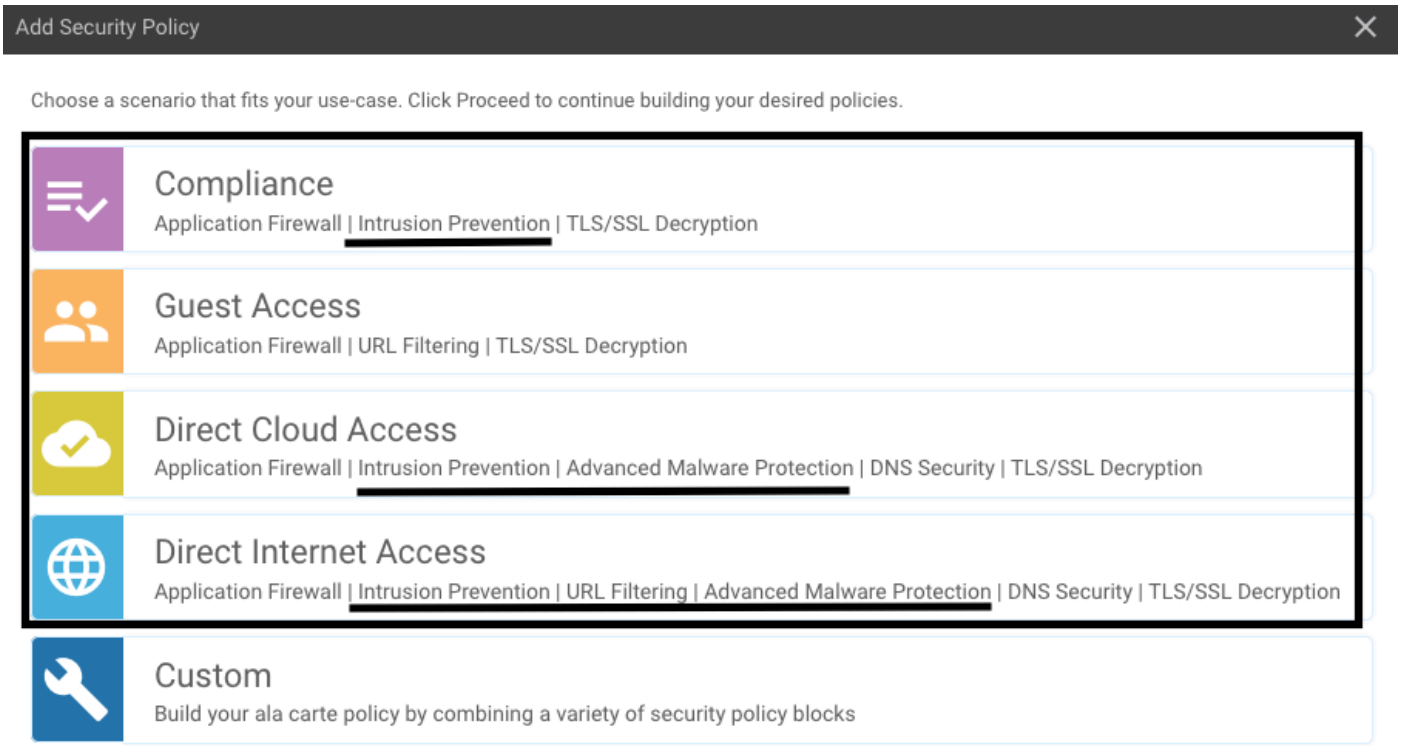
Het virtuele beeld verstuurt een fout: **Apparaten hebben dus geen containersoftware**, Als de geselecteerde cEdge-router geen beveiligingsbeleid heeft met het containerprofiel-subsjabloon.





Deze sjabloon wordt automatisch toegevoegd als u een beveiligingsbeleid gebruikt dat beveiligingsfuncties bevat zoals Inbraakpreventiesysteem (IPS), Inbraakdetectiesysteem (IDS),

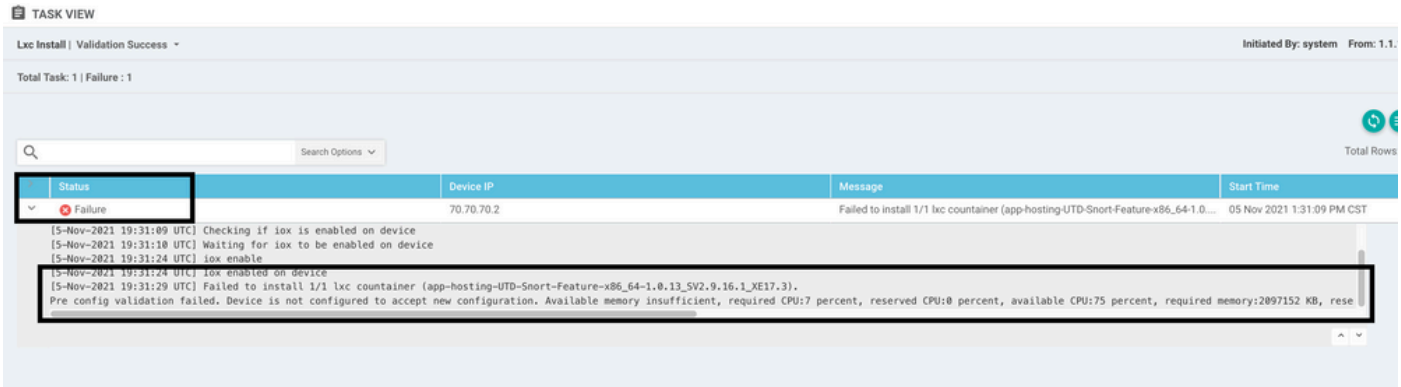
URL-filtering (URL-F) en Advanced Malware Protection (AMP) waarvoor UTD-pakket nodig is. Niet alle beveiligingsfuncties die beschikbaar zijn, hebben UTD-engine nodig, zoals eenvoudige ZBFW-functie.



Zodra u de sjabloon met de subsjabloon van het containerprofiel duwt, installeert de beheerder automatisch de virtuele afbeelding.

PROBLEEM 2. ONVOLDOENDE BESCHIKBAAR GEHEUGEN

Zorg ervoor dat de cEdge router 8 GB DRAM geheugen heeft, als dat niet het geval is, het Lxc Installatie proces verzenden een **apparaat is niet geconfigureerd om nieuwe configuratie te accepteren. Beschikbaar geheugen onvoldoende** fout. De vereisten voor cEdge-routers om UTD-functies te gebruiken, zijn minimaal 8 GB aan DRAM's.



In dit geval heeft de CSRv slechts 4 GB DRAM. Na de upgrade van het geheugen naar 8GB DRAM is de installatie een succes.

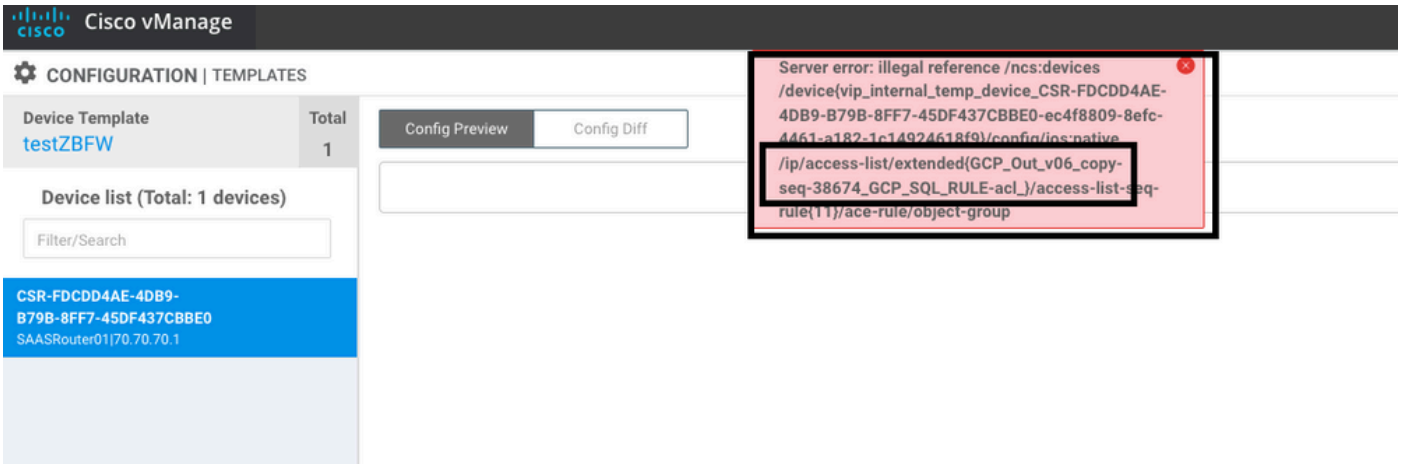
Controleer het huidige totale geheugen met de uitvoer van de **status van het vertragingssysteem**:

```
Router01# show sdwan system status
```

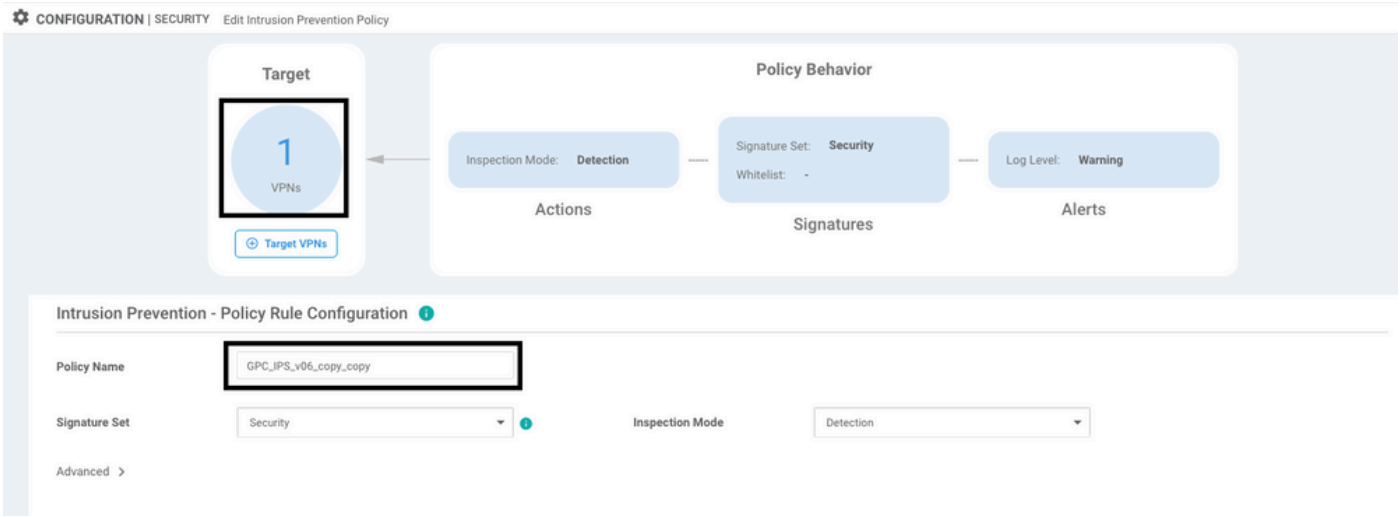
```
Memory usage:            8107024K total,    3598816K used,   4508208K free
                         349492K buffers,  2787420K cache
```

Probleem 3. Onrechtmatige verwijzing

Zorg ervoor dat de VPN's/VRF's die op een van de beveiligingsbeleidsfuncties worden gebruikt, al in de cEdge-router zijn geconfigureerd om een illegale verwijzing voor de beveiligingsbeleidssequenties te voorkomen.



In dit voorbeeld heeft het Beveiligingsbeleid een Inbraakpreventiebeleid voor VPN/VRF 1, maar op de apparaten is geen VRF 1 geconfigureerd. De managers sturen dus een illegale verwijzing naar die beleidsreeks.



Na het configureren van de VRF vermeld op het Beveiligingsbeleid, verschijnt de Illegale referentie niet en wordt de sjabloon met succes gedrukt.

Probleem 4. UTD is geïnstalleerd en actief maar niet ingeschakeld

Het apparaat heeft een beveiligingsbeleid geconfigureerd en UTD is geïnstalleerd en actief, maar is niet ingeschakeld.

Dit probleem houdt verband met probleem nummer 3, maar vManager stond toe dat de configuratie verwijst naar VRF's die niet in het apparaat zijn geconfigureerd en het beleid wordt niet toegepast op een VRF.

Om te bepalen of router met dit probleem te maken heeft, moet u UTD actief zien. UTD niet toegelaten bericht en het beleid maakt geen verwijzing naar enige VRF.

```
Router01# show utd engine standard status

UTD engine standard is not enabled <<<<<<<<<<<


ISR01#show sdwan virtual-application utd

VERSION                                 ACTIVE  PREVIOUS                        TIMESTAMP

---------------------------------------------------------------------------

1.0.16_SV2.9.16.1_XE17.3        true        true            2022-06-10T13:29:43-00:00
```

Controleer voor de resolutie de doel-VPN's en pas het beleid toe op een geconfigureerde VRF.

Gerelateerde informatie

- Routerbeveiliging: Sneltoets IPS op routers
- Cisco SD-WAN security configuratiegids, Cisco IOS XE release
- Technische ondersteuning en documentatie – Cisco Systems

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.