Instalación de la imagen virtual de seguridad UTD en routers cEdge

Contenido

Introducción

Este documento describe cómo instalar la imagen virtual de seguridad de Unified Threat Defence (UTD) para habilitar las funciones de seguridad en los dispositivos SD-WAN de Cisco IOS XE.

Prerequisites

- Antes de utilizar estas funciones, cargue la imagen virtual de seguridad correspondiente en el repositorio de vManage.
- El router cEdge debe estar en modo vmanage con la plantilla previamente conectada.
- Cree una plantilla de políticas de seguridad para el sistema de prevención de intrusiones (IPS), el sistema de detección de intrusiones (IDS), el filtrado de URL (URL-F) o el filtrado de protección frente a malware avanzado (AMP).

Requirements

- 4000 Router de servicios integrados Cisco IOS XE SD-WAN (ISR4k)
- Router de servicios integrados 1000 Cisco IOS XE SD-WAN (ISR1k)

- Router para servicios basados en la nube 1000v (CSR1kv),
- Router de servicios integrados (ISRv) 1000v
- Plataformas periféricas que admiten 8 GB de DRAM.

Componentes Utilizados

- Imagen virtual de Cisco UTD
- vManage controller
- Routers cEdge con conexiones de control con controladores.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La imagen de Cisco UTD necesita una política de seguridad en la plantilla del dispositivo que se va a instalar, así como funciones de seguridad activadas, como el sistema de prevención de intrusiones (IPS), el sistema de detección de intrusiones (IDS), el filtrado de URL (URL-F) y la protección frente a malware avanzado (AMP) en los routers de Bordes.

Descargue el software Cisco UTD Snort IP Engine del software Cisco

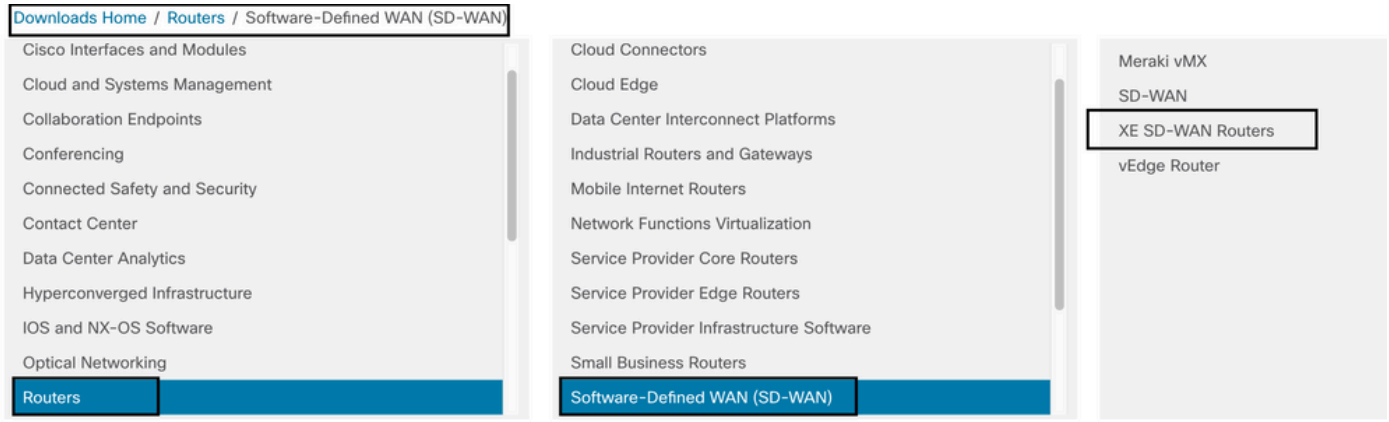
Utilice el regex compatible con la imagen virtual de Cisco UTD para la versión actual de Cisco IOS XE. Utilice el comando **show utd engine standard** version para validar la imagen UTD recomendada y admitida.

```
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$
```

> **Nota** La ruta para descargar la imagen depende de si el router ejecuta Cisco IOS XE SDWAN Software (16.x) o Cisco IOS XE Software Universal (17.x).

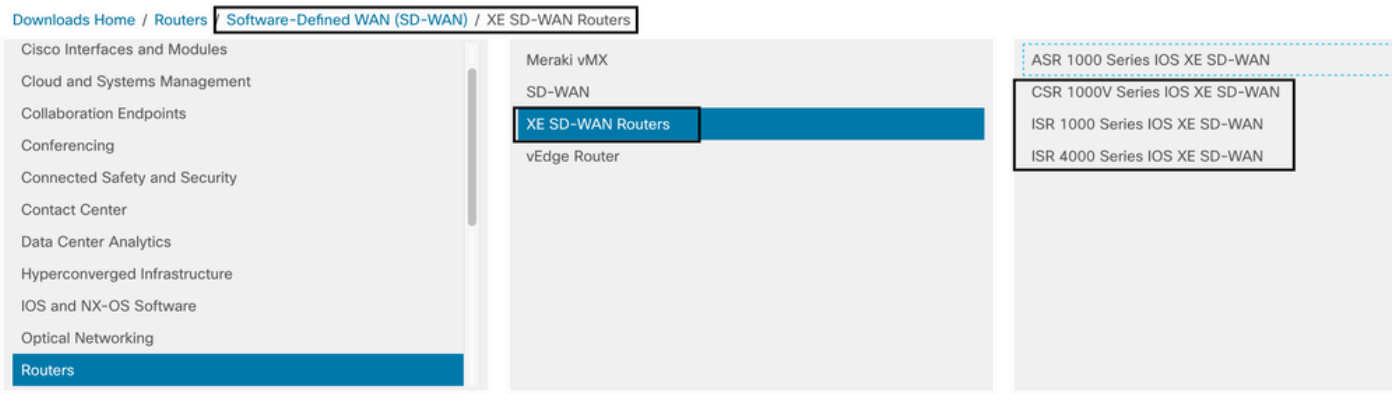
Routers que ejecutan el software SDWAN Cisco IOS XE (16.x)

La ruta para obtener el software Cisco UTD Snort IPS Engine es Routers/WAN definida por software (SD-WAN)/routers XE SD-WAN/y el router integrado de la serie.



Elija el tipo de modelo para el router cEdge.

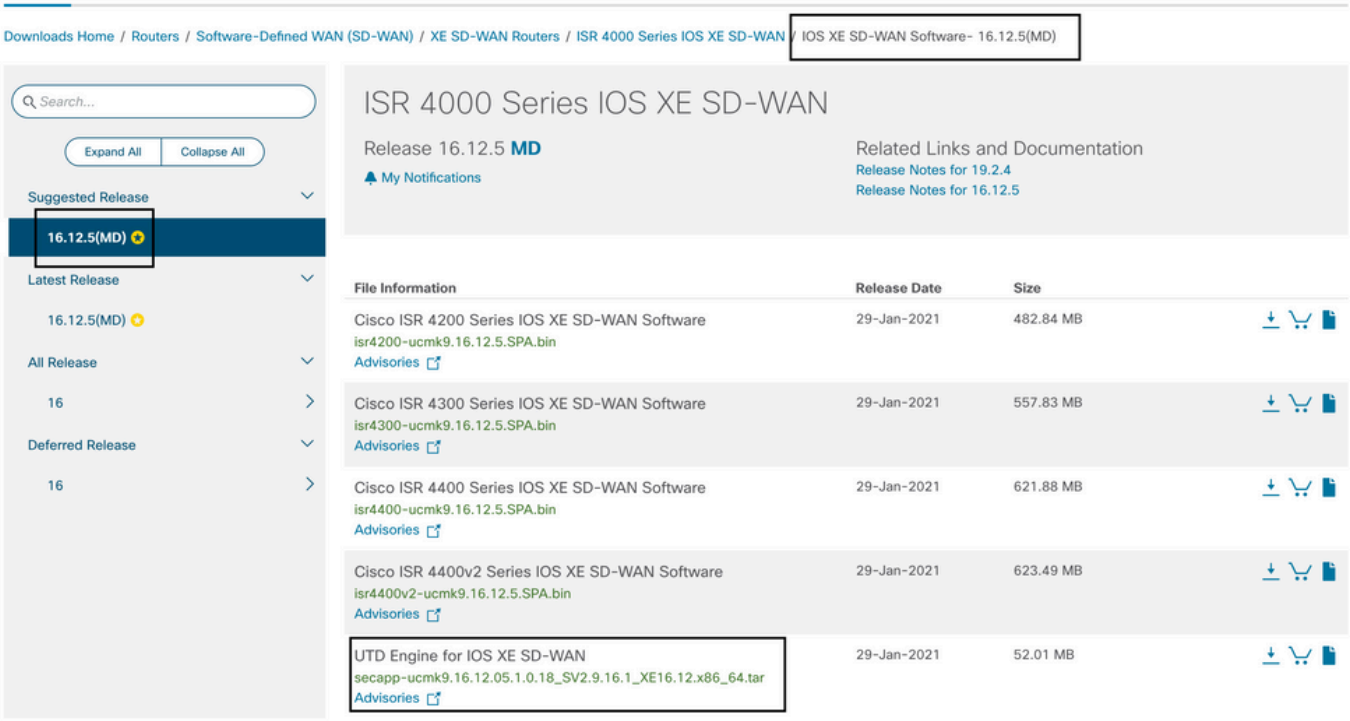
> **Nota** Los routers de servicios de agregación (ASR) de la serie no están disponibles para las funciones de UTD.



Después de elegir el tipo de modelo de router, seleccione la opción de **software Cisco IOS XE SD-WAN** para obtener el paquete UTD para cEdges en la versión 16.x.

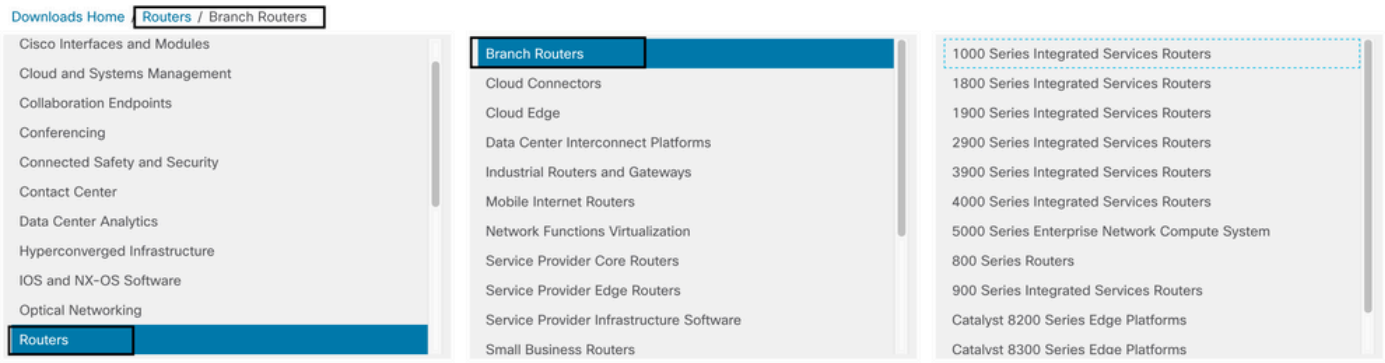
> **Nota** La ruta de descarga para elegir la imagen virtual de Cisco UTD para el código 16.x para los routers de cEdge también muestra la opción de **software Cisco IOS XE**. Esa es la ruta para elegir los códigos de actualización de cEdge para 17.x solamente, pero no se encuentra la imagen virtual UTD para la versión 17.x. Los códigos SDWAN de Cisco IOS XE y Cisco IOS XE normales unificados en 17.x y versiones más recientes, por lo que la ruta para obtener la imagen virtual de Cisco UTD para 17.x es la misma que la de los códigos normales de Cisco IOS XE.

Elija la versión actual de cEdge y descargue el paquete UTD para esa versión.

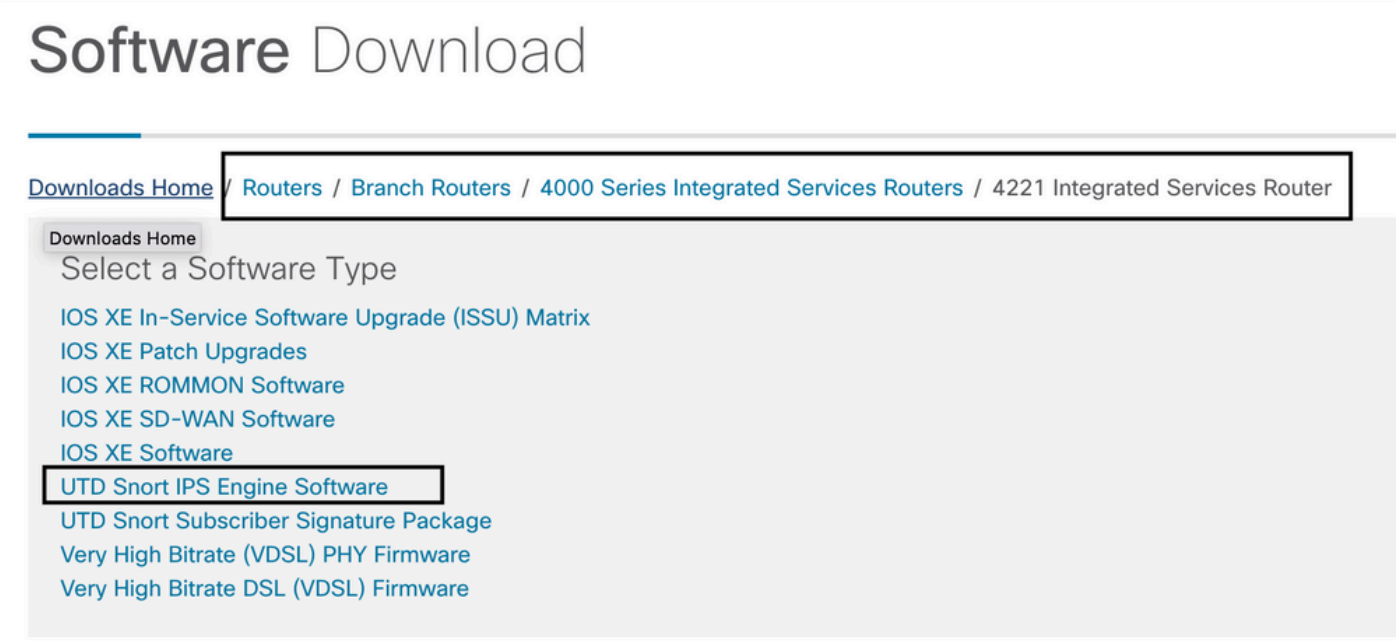


Routers que ejecutan el software Cisco IOS XE (17.x)

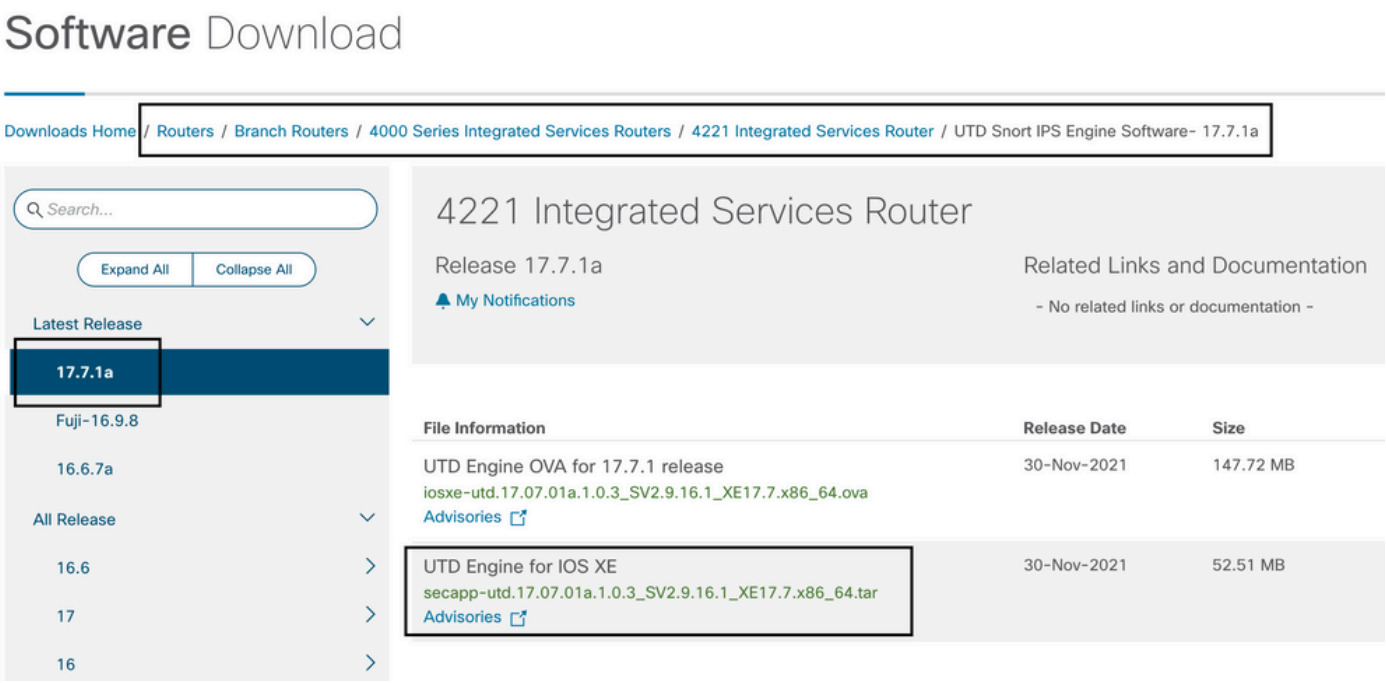
Cisco IOS XE Release 17.2.1r y la versión más reciente utilizan la imagen universalk9 para implementar tanto Cisco IOS XE SD-WAN como Cisco IOS XE en dispositivos Cisco IOS XE. **El software UTD Snort IPS Engine** se encuentra en **Routers > Branch Routers > Series Integrated Router**.



Después de elegir el tipo de modelo del router, seleccione el **software UTD Snort IPS Engine**.



Seleccione la versión actual del router y descargue el paquete UTD para la versión seleccionada.

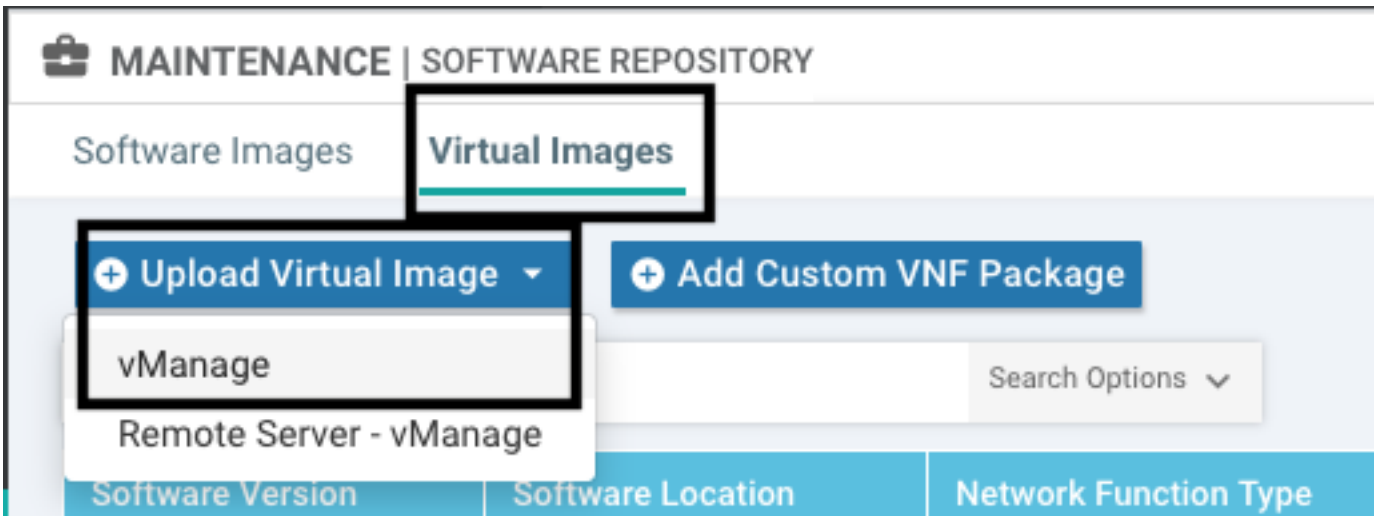


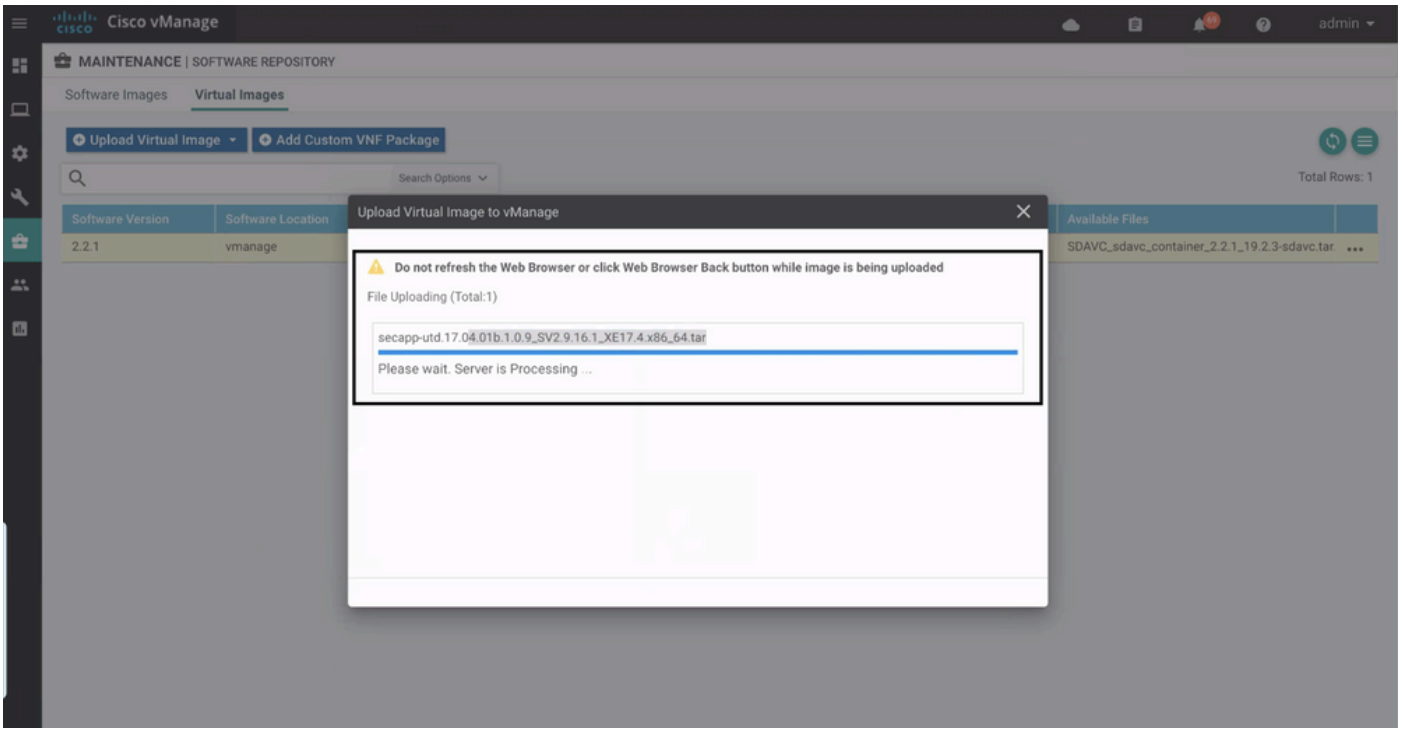
Nota: Los routers Cisco ISR1100X Series (routers Cisco Nutella SR1100X-4G/6G) que ejecutan el software Cisco IOS XE en lugar del código de Viptela se basan en x86_x64. La imagen virtual de Cisco UTD publicada para ISR4K puede funcionar con ellos. Puede instalar la misma versión de código de imagen UTD de Cisco compatible con regex para la versión SDWAN actual de Cisco IOS XE en el router Nutella. Utilice el comando **show utd engine standard version** para validar la imagen regex UTD de Cisco recomendada y admitida.

Configurar

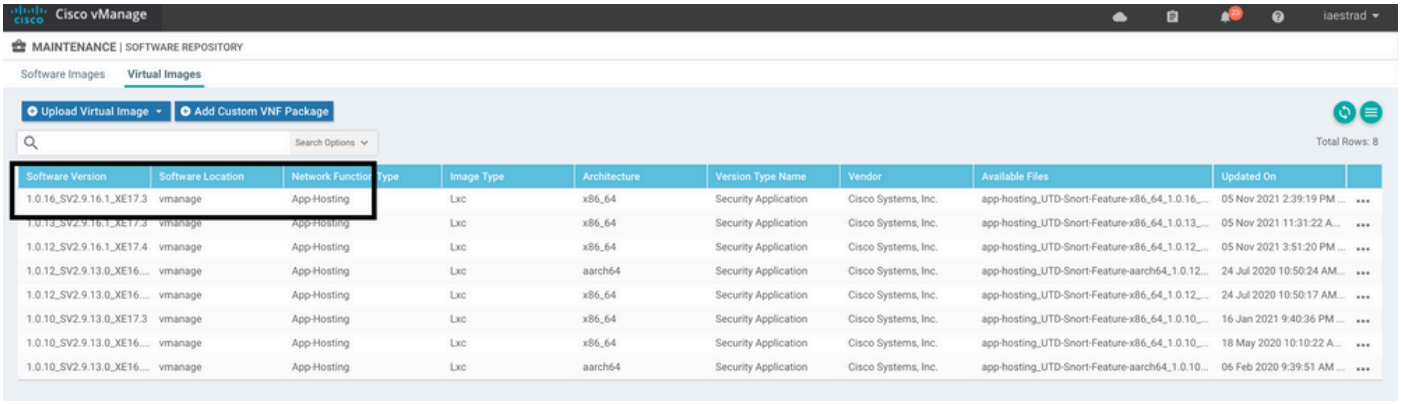
Paso 1. Cargar imagen virtual

Asegúrese de que la imagen virtual coincida con el código SDWAN actual de Cisco IOS XE en el cEdge y cárguela en el repositorio vmanage.
Vaya a **Mantenimiento > Repositorio de software > Imagen virtual > Cargar imagen virtual > vManage.**



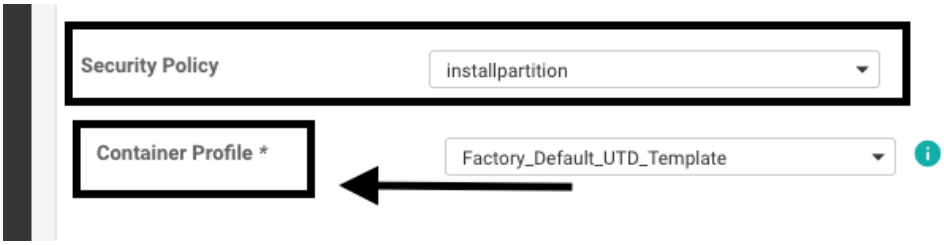


Una vez que la imagen virtual de Cisco UTD se haya cargado correctamente, vuelva a comprobar que está en el repositorio.



Paso 2. Agregar subplantilla de política de seguridad y perfil de contenedor a plantilla de dispositivo

Agregue la política de seguridad creada anteriormente a la plantilla de dispositivo. La política de seguridad debe tener una política IPS/IDS, URL-F o de filtrado de AMP en la plantilla de dispositivo. Abra el perfil del contenedor automáticamente. Utilice el perfil de contenedor predeterminado o modifíquelo si es necesario.

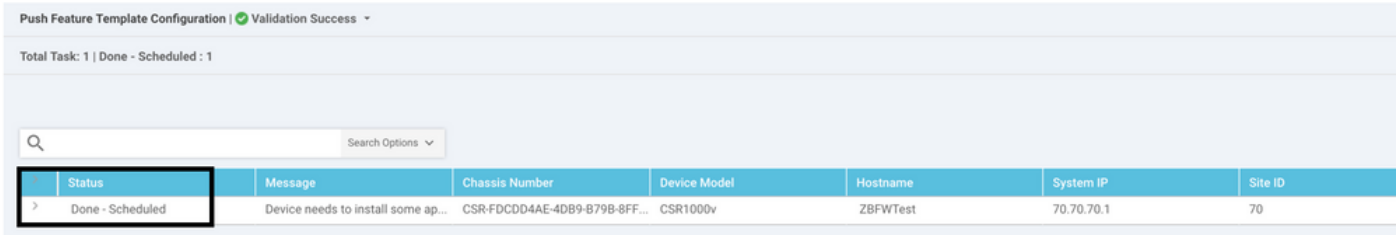


Paso 3. Actualice o adjunte la plantilla de dispositivo con la política de seguridad y el perfil del contenedor

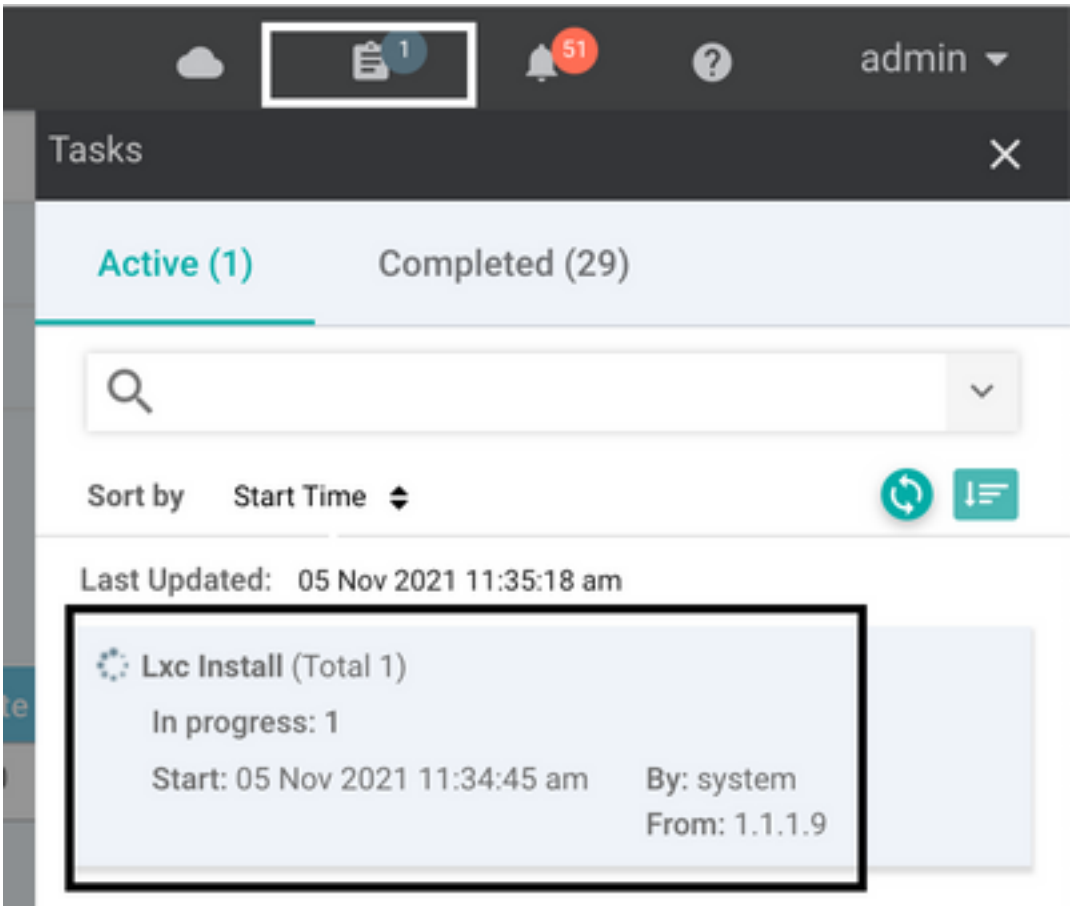
Actualice o adjunte la plantilla al router cEdge. Observe en config diff que la configuración de alojamiento de aplicaciones y el motor UTD para la función IPS/IDS, URL-F o AMP Filtering están configurados.

```
app-hosting appid utd
 app-resource package-profile cloud-low
 app-vnic gateway0 virtualportgroup 0 guest-interface 0
  guest-ipaddress 192.168.1.2 netmask 255.255.255.252
 !
 app-vnic gateway1 virtualportgroup 1 guest-interface 1
  guest-ipaddress 192.0.2.2 netmask 255.255.255.252
 !
 start
!
lldp run
nat64 translation timeout tcp 60
nat64 translation timeout udp 1
utd multi-tenancy
utd engine standard multi-tenancy
 threat-inspection profile GPC_IPS_v06_copy_copy
  threat detection
  policy security
  logging level warning
 !
 utd global
 !
!
policy
 no app-visibility
 no flow-visibility
 no implicit-acl-logging
 log-frequency        1000
!
```

El estado de la plantilla cambia a **Finalizado-programado** debido a que vmanage observó que la configuración aplicada tiene funciones de motor UTD, por lo que vmanage determina que cEdge necesita la imagen virtual instalada para utilizar las funciones de seguridad UTD.



Después de mover la plantilla al estado de programación, aparece una nueva tarea **en curso** en el menú de tareas**.** La nueva tarea es la **instalación Lxc**, lo que significa que vmanage inicia automáticamente la instalación de la imagen virtual en el cEdge antes de enviar la nueva configuración.

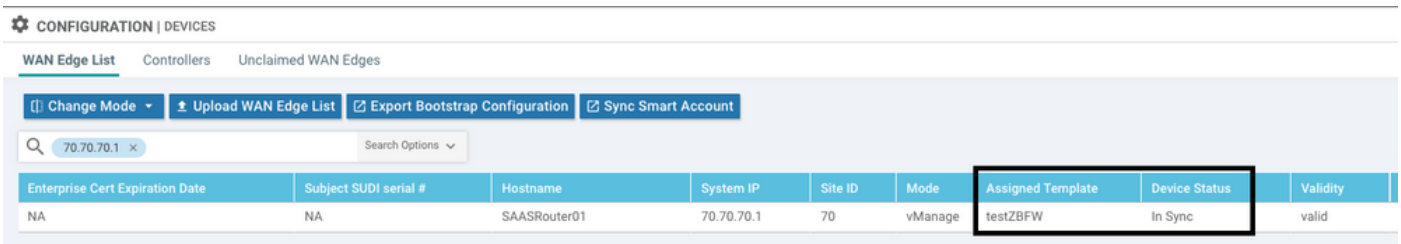


Una vez instalado el contenedor LX, vManage realiza la configuración previa a la programación con las funciones UTD. No hay ninguna tarea nueva para esto debido a que la configuración se programó anteriormente.

Verificación

Verifique si cEdge está sincronizado con vManage y la plantilla adjunta.

Vaya a **Configuration > Devices**



Verifique si la versión de Cisco UTD está instalada:

```
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         <<<<<<<<<<<<<<<<<<<
```

Nota La versión instalada de UTD no puede tener el estado **UNSUPPORTED**.

Compruebe si UTD está en estado **en ejecución** con el siguiente resultado:

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

El siguiente comando resume los comandos anteriores y muestra el estado y la versión actuales:

```
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
```

El comando **Show utd engine standard status** muestra el estado del motor UTD y la hora de la lista para obtener la actualización de la firma.

```
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
```

Verifique las funciones habilitadas mediante el siguiente comando:

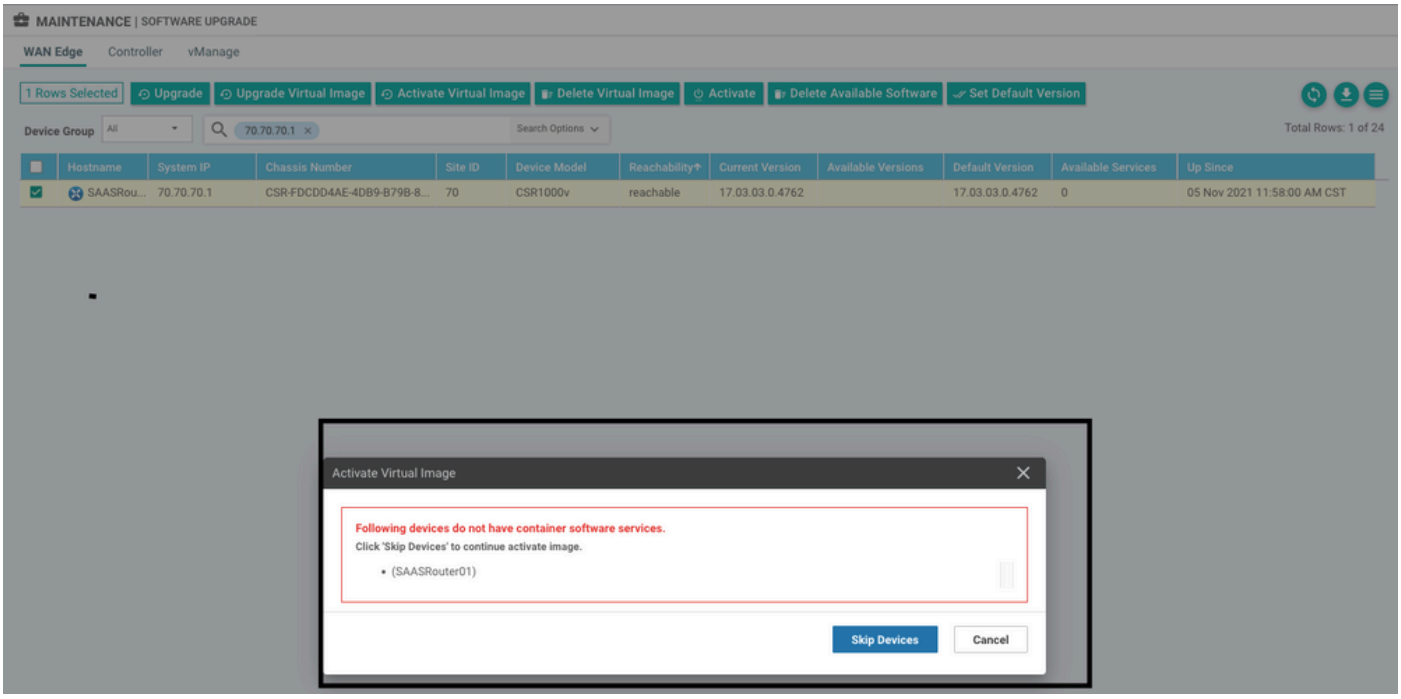
```
Router02# show platform hardware qfp active feature utd config
Global configuration
  NAT64: disabled
  Drop pkts: disabled
  Multi-tenancy: enabled
  Data plane initialized: yes
  TLS Decryption Policy: disabled
  Divert controller mode: enabled
  SN threads: 12
  CFT inst_id 0 feat id 2 fo id 2 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
```

Problemas comunes

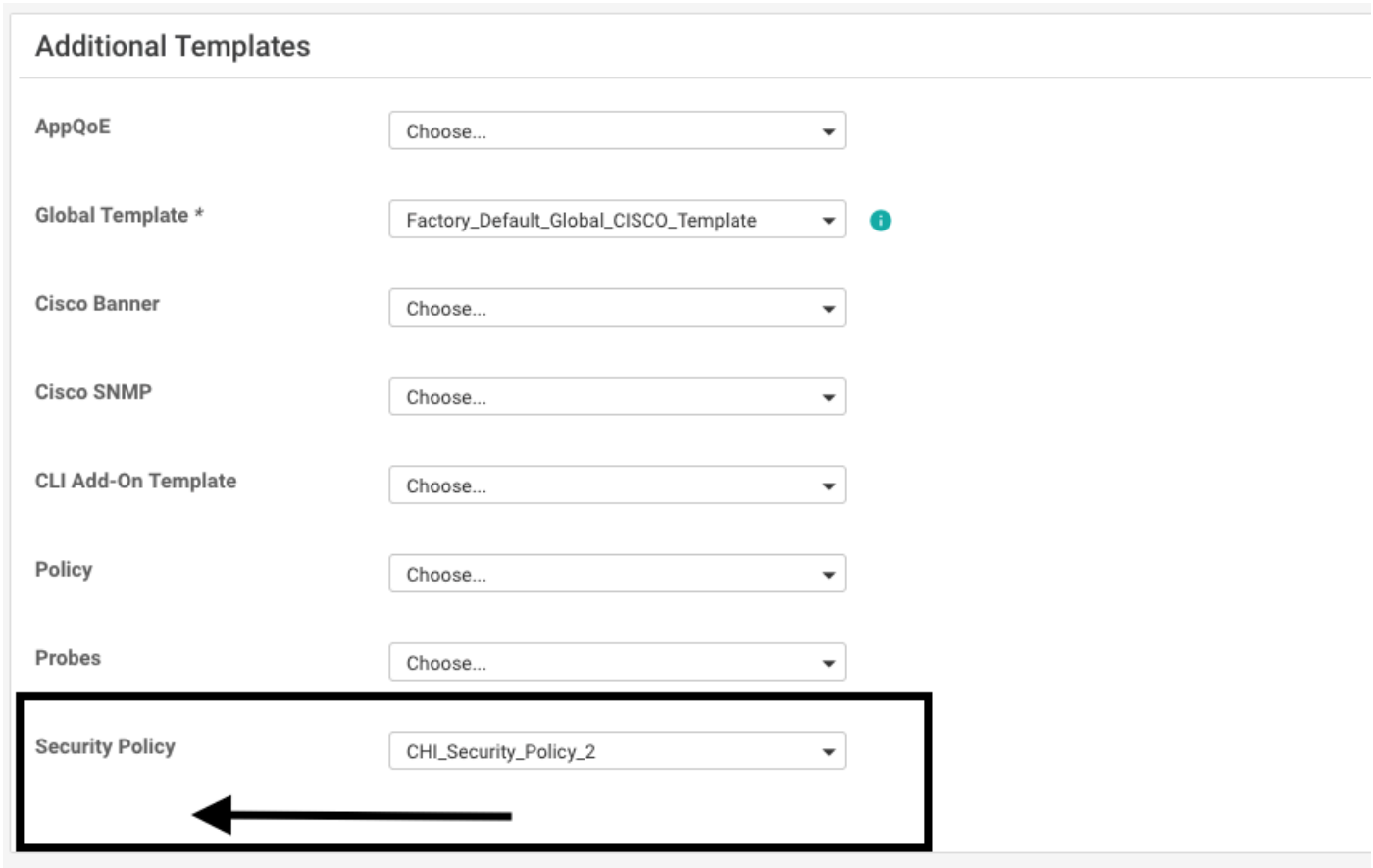
PROBLEMA 1. Error: Los siguientes dispositivos no tienen servicios de software de contenedor

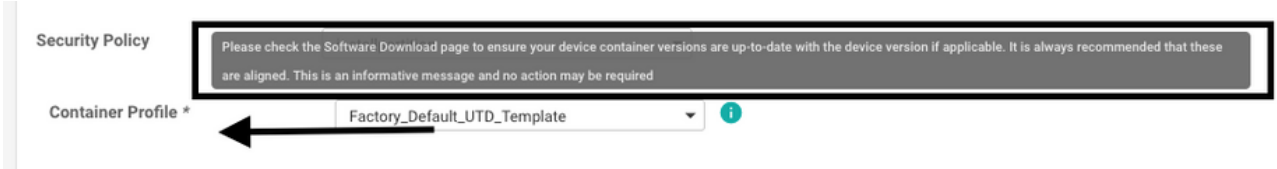
Active la imagen virtual.

Vaya a **mantenimiento > software > activar**



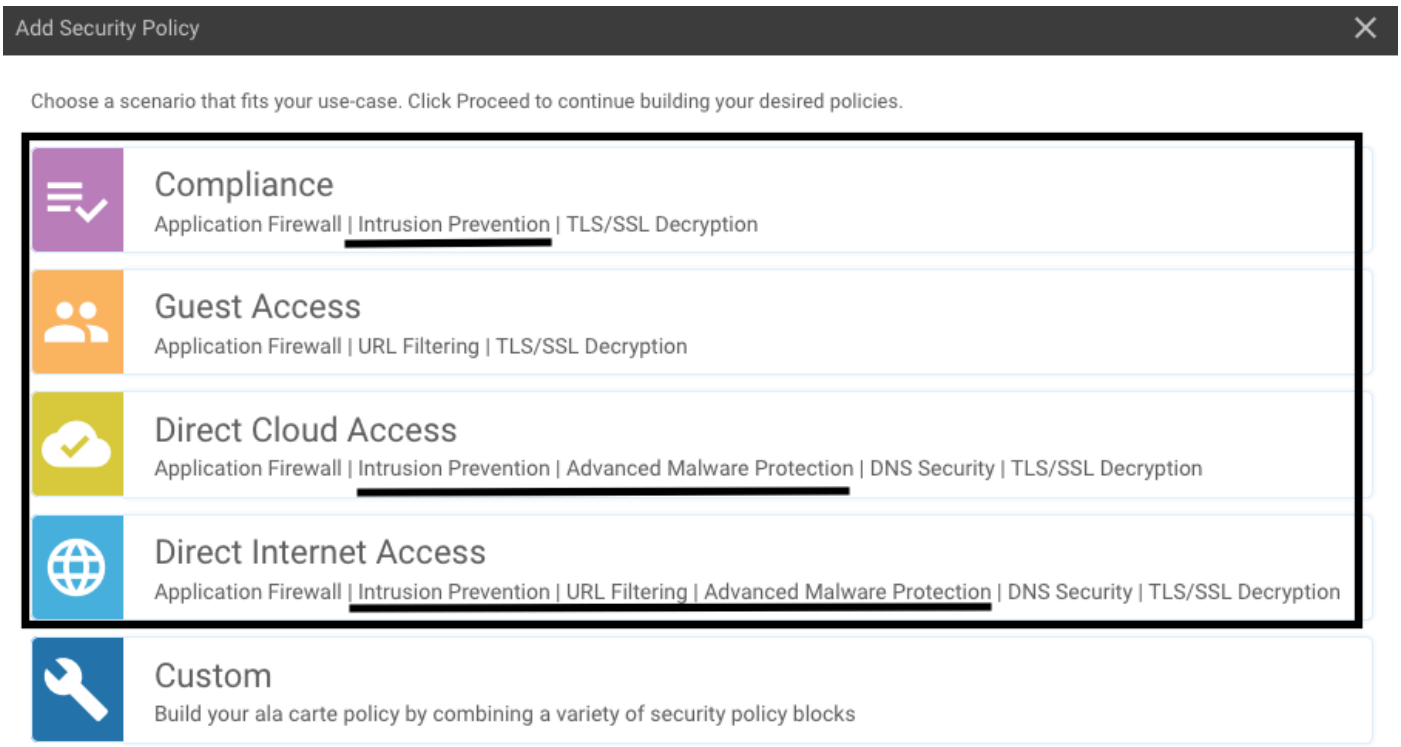
La imagen virtual envía un error: **Los dispositivos no tienen servicios de software de contenedor**, si el router cEdge seleccionado no tiene una política de seguridad con la subplantilla de perfil de contenedor.





Esta plantilla se agrega automáticamente si utiliza una directiva de seguridad que incluya

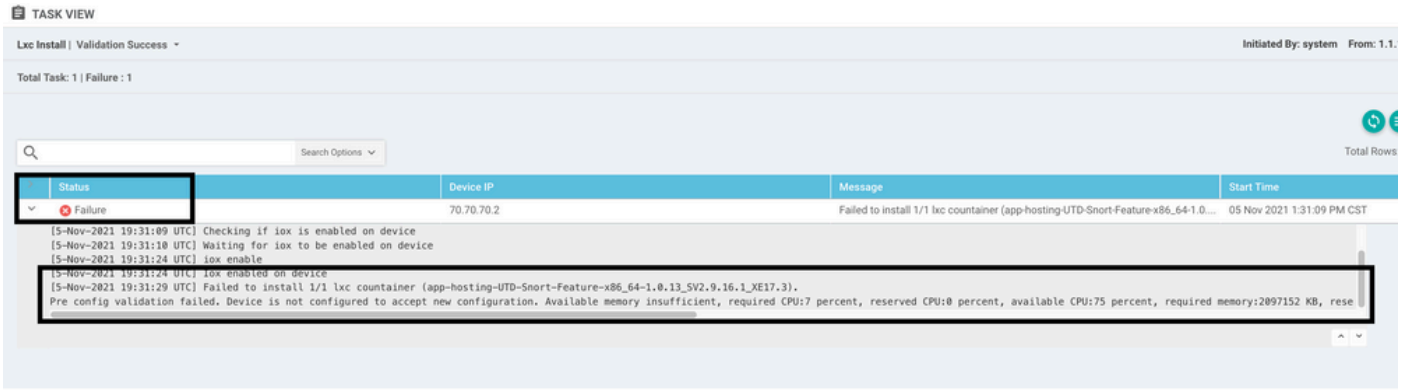
funciones de seguridad como el sistema de prevención de intrusiones (IPS), el sistema de detección de intrusiones (IDS), el filtrado de URL (URL-F) y la protección frente a malware avanzado (AMP) que necesite el paquete UTD. No todas las funciones de seguridad disponibles necesitan un motor UTD como una simple función ZBFW.



Una vez que se inserta la plantilla con la subplantilla de perfil de contenedor, vmanage instala automáticamente la imagen virtual.

PROBLEMA 2. Memoria disponible insuficiente

Asegúrese de que el router cEdge tenga una memoria DRAM de 8 GB; de lo contrario, el proceso de instalación Lxc send a **Device no está configurado para aceptar la nueva configuración.** Error **de memoria insuficiente disponible**. Los requisitos para que los routers cEdge utilicen funciones UTD es tener un mínimo de 8 GB de DRAM.



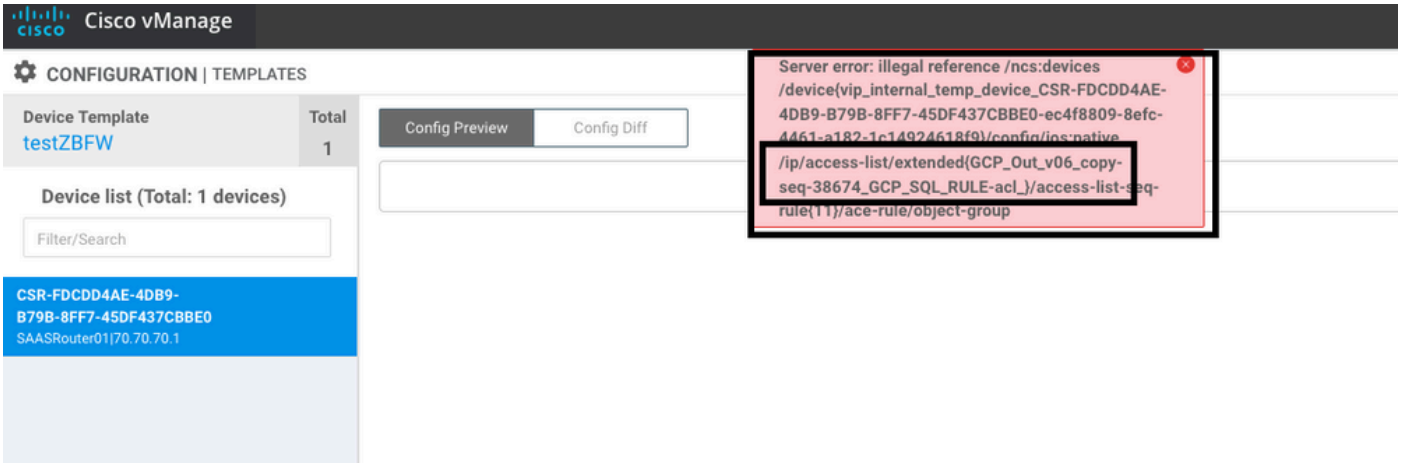
En este caso, el CSRv solo tiene 4 GB de DRAM. Después de actualizar la memoria a 8GB de DRAM, la instalación es un éxito.

Verifique la memoria total actual con el resultado de **show sdwan system status**:

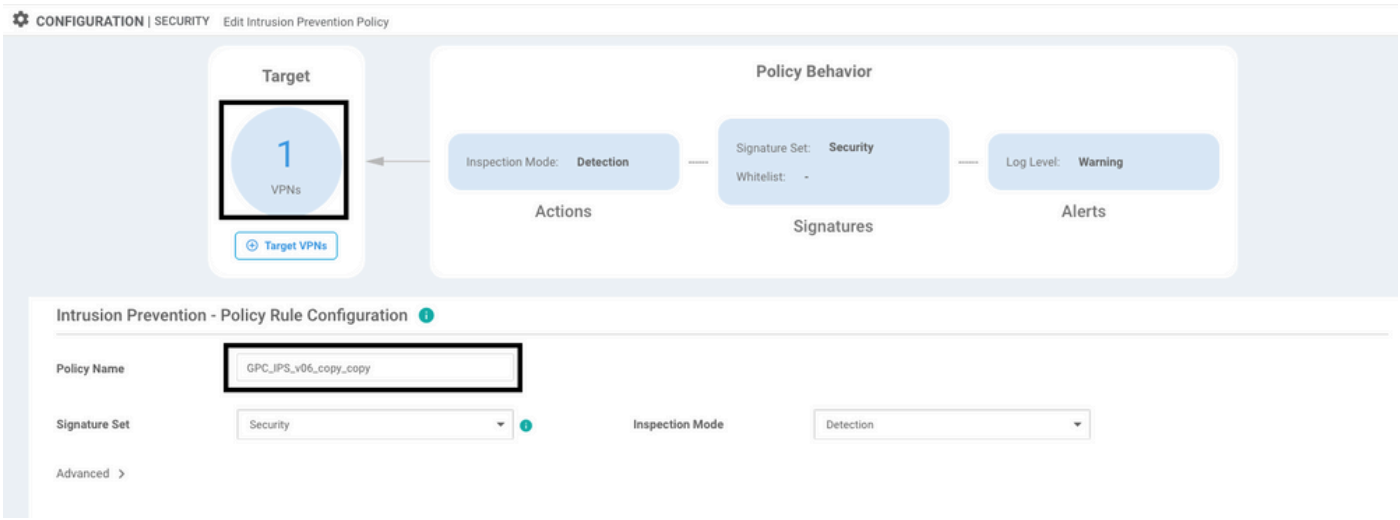
```
Router01# show sdwan system status

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

CUESTIÓN 3. Referencia ilegal

Asegúrese de que las VPNs/VRFs utilizadas en cualquiera de las funciones de la política de seguridad ya estén configuradas en el router cEdge para evitar una referencia ilegal para las secuencias de la política de seguridad.



En este ejemplo, la política de seguridad tiene una política de prevención de intrusiones para VPN/VRF 1, pero los dispositivos no tienen ningún VRF 1 configurado. Por lo tanto, vmanage envía una referencia ilegal para esa secuencia de políticas.



Después de configurar el VRF mencionado en las políticas de seguridad, la referencia Illegal no aparece y la plantilla se envía correctamente.

PROBLEMA 4. UTD está instalado y activo pero no habilitado

El dispositivo tiene una política de seguridad configurada y UTD está instalado y activo, pero no está habilitado.

Este problema está relacionado con el número 3; sin embargo, vManage permitió que la configuración hiciera referencia a VRF que no están configurados en el dispositivo y la política no se aplica a ningún VRF.

Para determinar si el router enfrenta este problema, debe ver el UTD activo. mensaje UTD not enabled y la política no hace referencia a ningún 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
```

Para la resolución, verifique las VPNs de destino y asegúrese de aplicar la política a un VRF configurado.

Información Relacionada

- Seguridad del router: Snort IPS en routers
- Guía de Configuración de Seguridad SD-WAN de Cisco, Cisco IOS XE Release
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).