Instalar Imagem Virtual de Segurança UTD em Roteadores cEdge

Contents

Introduction

Este documento descreve como instalar a Imagem Virtual de Segurança do Unified Threat Defense (UTD) para ativar recursos de segurança em dispositivos Cisco IOS XE SD-WAN.

Prerequisites

- Antes de usar esses recursos, carregue a Security Virtual Image relevante no repositório do vManage.
- O roteador cEdge deve estar no modo vmanage com o modelo pré-conectado.
- Crie um Modelo de Política de Segurança para Sistema de Prevenção de Intrusão (IPS), Sistema de Detecção de Intrusão (IDS), Filtragem de URL (URL-F) ou Filtragem de Proteção Avançada contra Malware (AMP).

Requirements

- Roteador de Serviços Integrados série 4000 Cisco IOS XE SD-WAN (ISR4k)
- Roteador de Serviços Integrados série 1000 Cisco IOS XE SD-WAN (ISR1k)

- Roteador de serviços em nuvem 1000v (CSR1kv),
- Roteador de Serviços Integrados (ISRv) 1000v
- Plataformas Edge que suportam DRAM de 8 GB.

Componentes Utilizados

- Imagem virtual do Cisco UTD
- controlador vManage
- Roteadores cEdge com conexões de controle com 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A imagem do Cisco UTD precisa de uma política de segurança no modelo do dispositivo a ser instalado e de recursos de segurança ativados, como o Sistema de prevenção de intrusão (IPS), o Sistema de detecção de intrusão (IDS), a Filtragem de URL (URL-F) e a Proteção avançada contra malware (AMP) nos roteadores de Bordas.

Faça o download do software Cisco UTD Snort IP Engine no Software Cisco

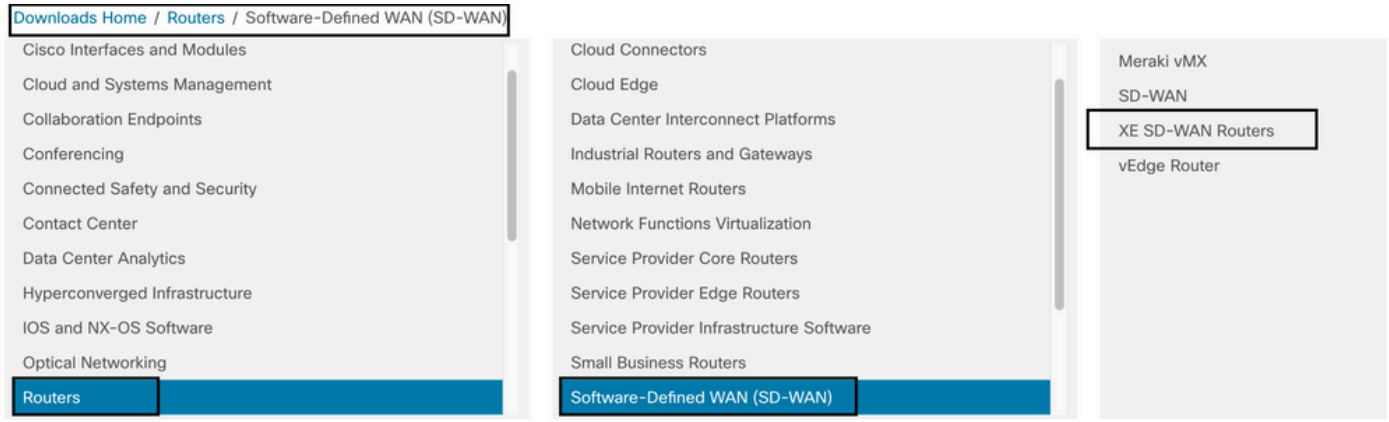
Use o regex suportado pela imagem virtual Cisco UTD para a versão atual do Cisco IOS XE. Use o comando **show utd engine standard** version para validar a imagem UTD recomendada e suportada.

```
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$
```

> **Observação** O caminho para baixar a imagem depende se o roteador executa o software Cisco IOS XE SDWAN (16.x) ou o software Universal Cisco IOS XE (17.x).

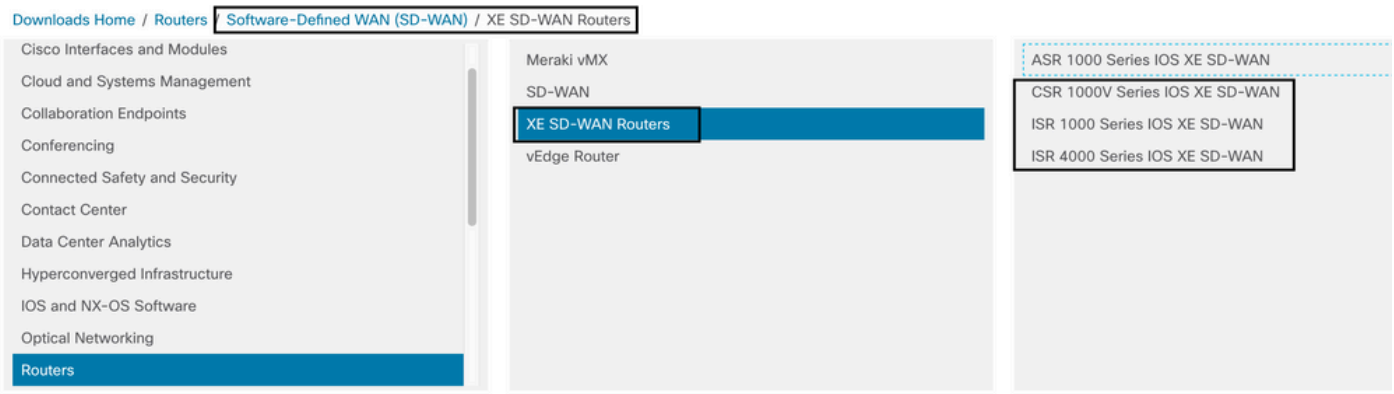
Roteadores que executam o software Cisco IOS XE SDWAN (16.x)

O caminho para obter o software Cisco UTD Snort IPS Engine é Roteadores/ WAN definida por software (SD-WAN)/ Roteadores XE SD-WAN / e o Roteador integrado da série.



Escolha o tipo de modelo para o roteador cEdge.

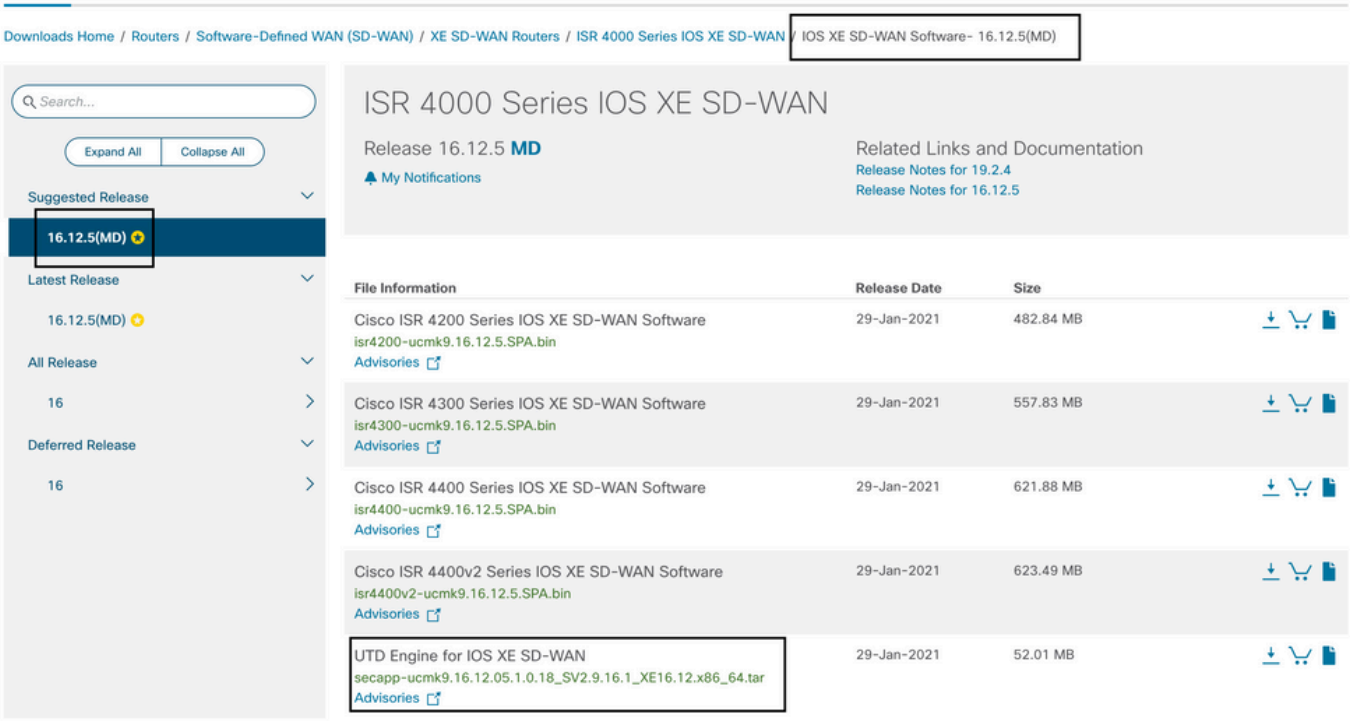
> **Observação** Os Roteadores de Serviços de Agregação (ASR) não estão disponíveis para Recursos UTD.



Depois de escolher o modelo do tipo de roteador, selecione a **opção do software Cisco IOS XE SD-WAN** para obter o pacote UTD para Bordas na versão 16.x.

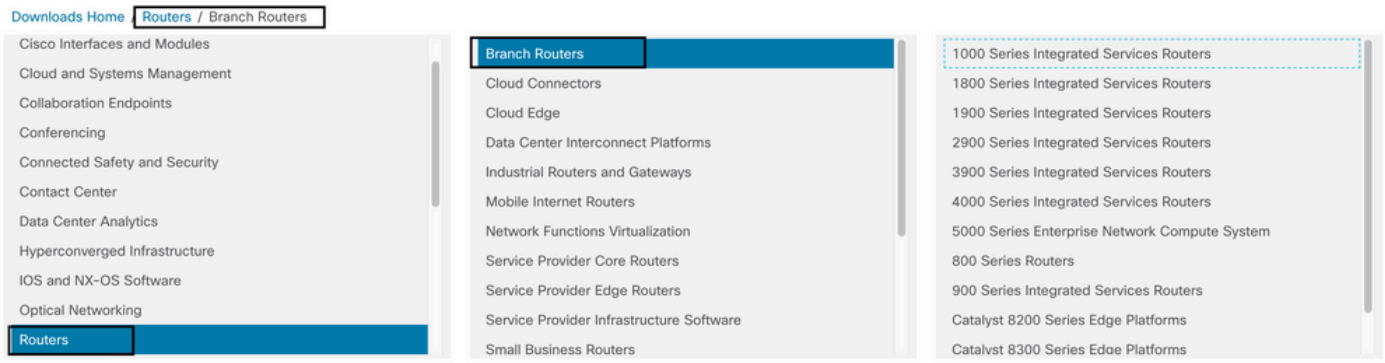
> **Observação** O caminho de download para escolher a imagem virtual do Cisco UTD para o código 16.x para roteadores de Bordas também mostra a **opção do software Cisco IOS XE**. Esse é o caminho para escolher os códigos de atualização do cEdge somente para a versão 17.x, mas a imagem virtual UTD para a versão 17.x não foi localizada. Os códigos Cisco Unified Regular Cisco IOS XE e Cisco IOS XE SDWAN em 17.x e mais recente, portanto, o caminho para obter a imagem virtual Cisco UTD para 17.x é o mesmo que os códigos Cisco IOS XE regulares.

Escolha a versão atual do cEdge e baixe o pacote UTD para essa versão.

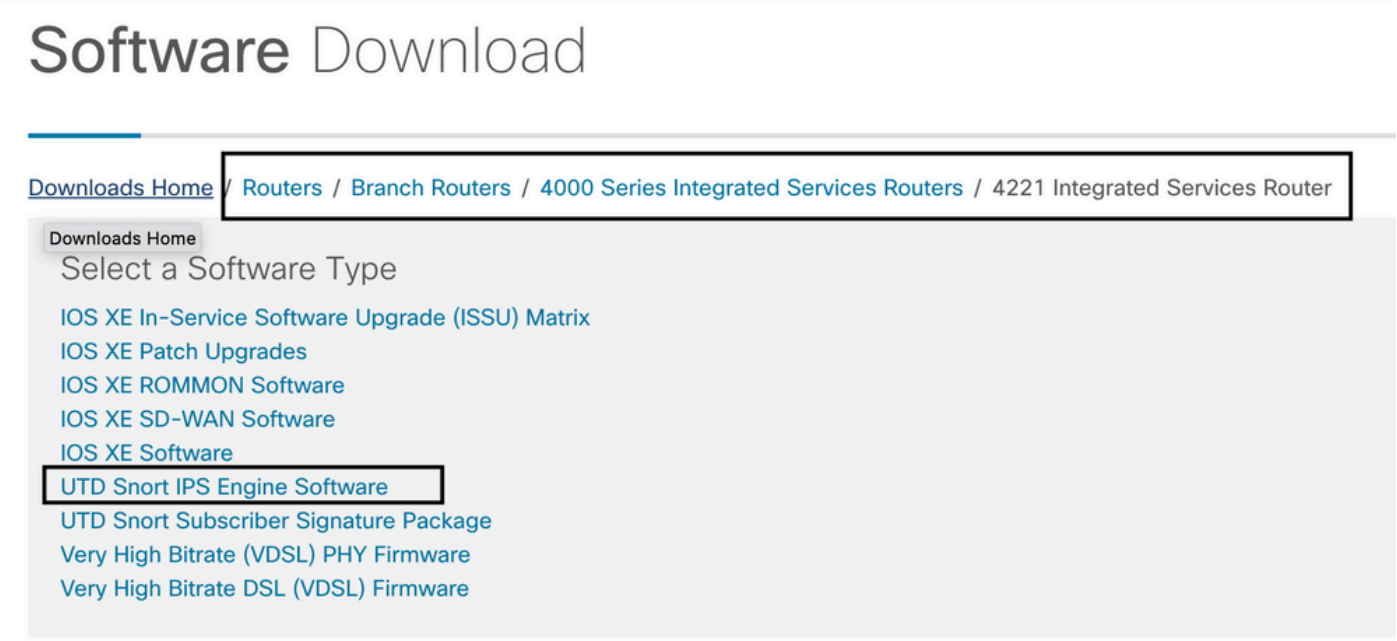


Roteadores que executam o software Cisco IOS XE (17.x)

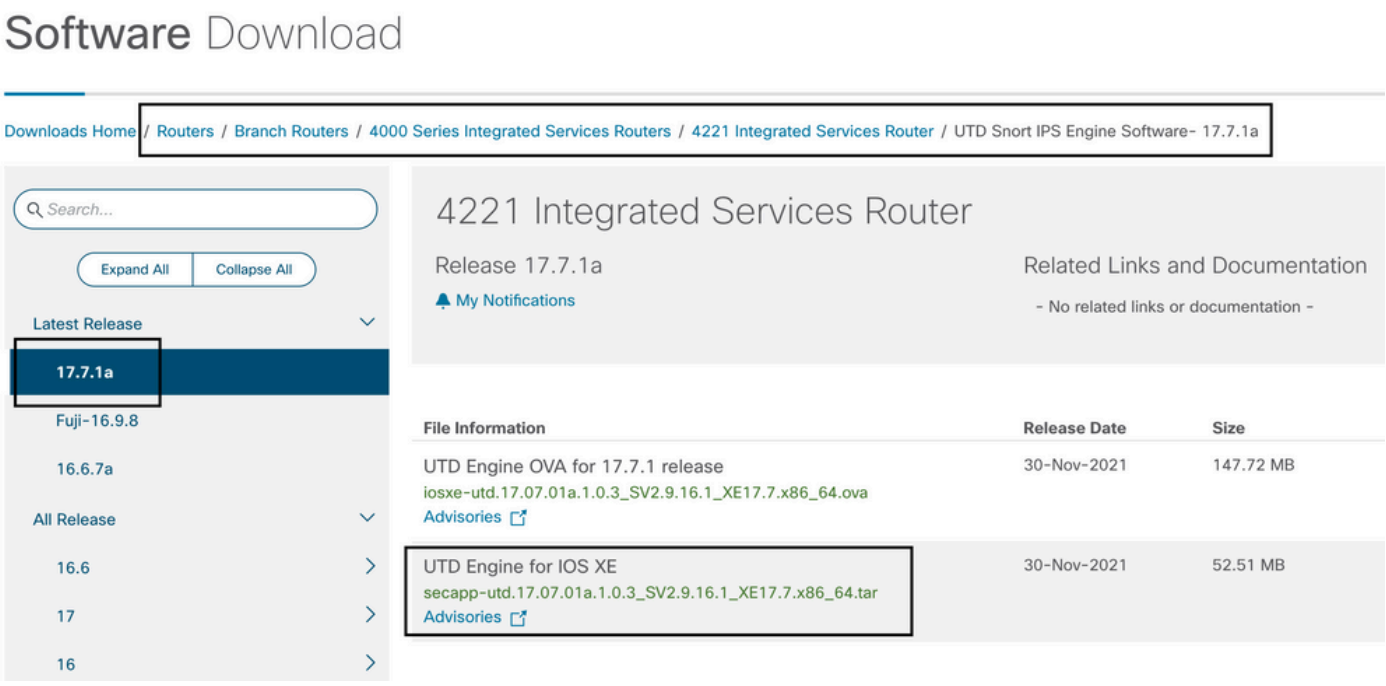
O Cisco IOS XE versão 17.2.1r e o mais recente usam a imagem universalk9 para implantar o Cisco IOS XE SD-WAN e o Cisco IOS XE em dispositivos Cisco IOS XE.
O software UTD Snort IPS Engine está localizado em **Routers > Branch Routers > Series Integrated Router**.



Depois de escolher o tipo de modelo do roteador, selecione o **software UTD Snort IPS Engine**.



Selecione a versão atual do roteador e baixe o pacote UTD para a versão selecionada.



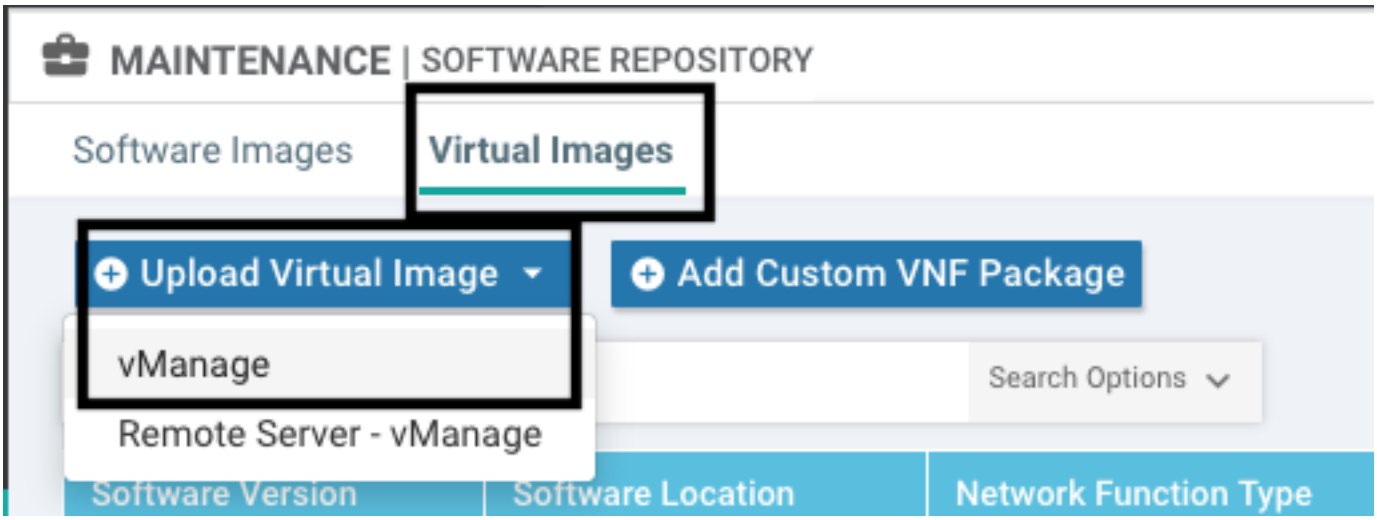
> **Note**: Os Cisco ISR1100X Series Routers (Cisco Nutella Routers SR1100X-4G/6G) que executam o Cisco IOS XE Software em vez do Viptela Code são baseados em x86_x64. A imagem virtual do Cisco UTD publicada para ISR4K pode funcionar neles. Você pode instalar a mesma versão de código de imagem do Cisco UTD com suporte para regex para a versão atual do Cisco IOS XE SDWAN no roteador Nutella. Use o comando **show utd engine standard version** para validar a imagem regex Cisco UTD recomendada e suportada.

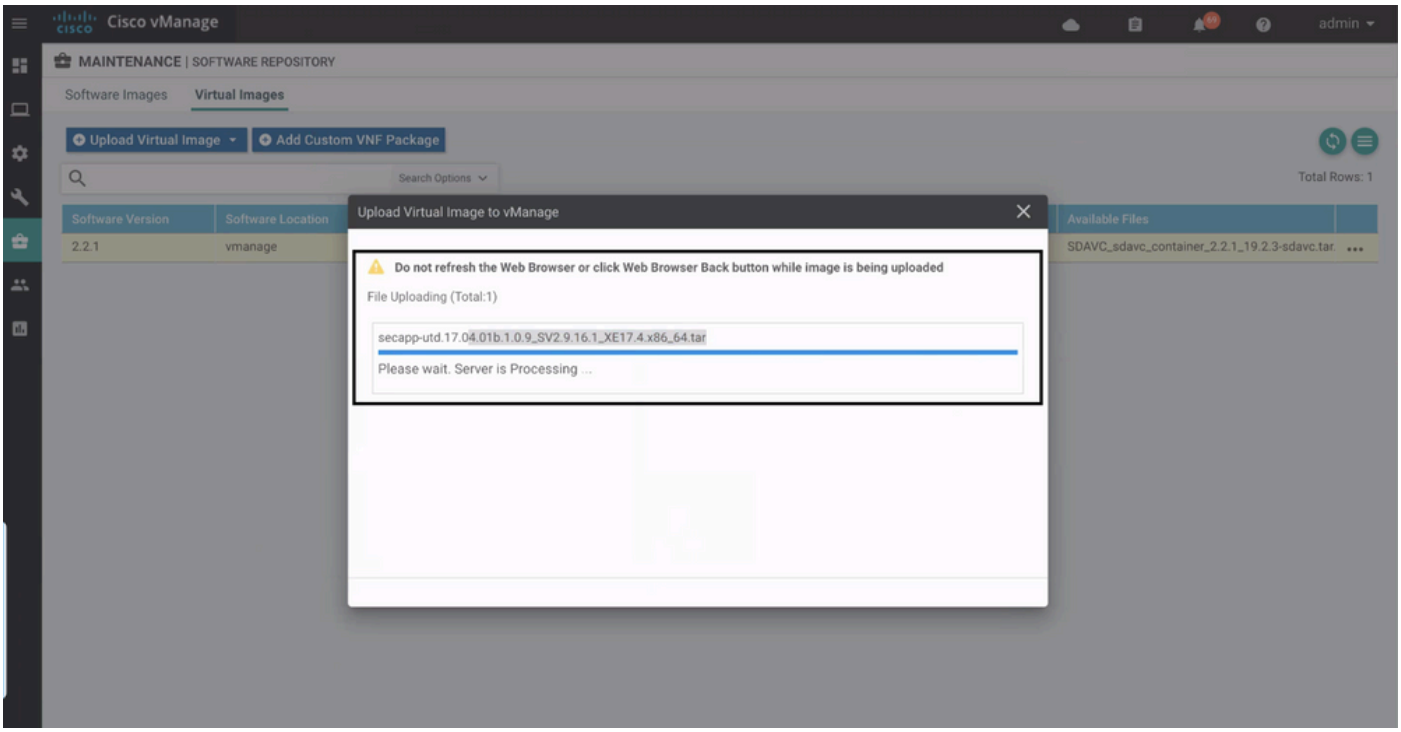
Configurar

Etapa 1. Fazer upload da imagem virtual

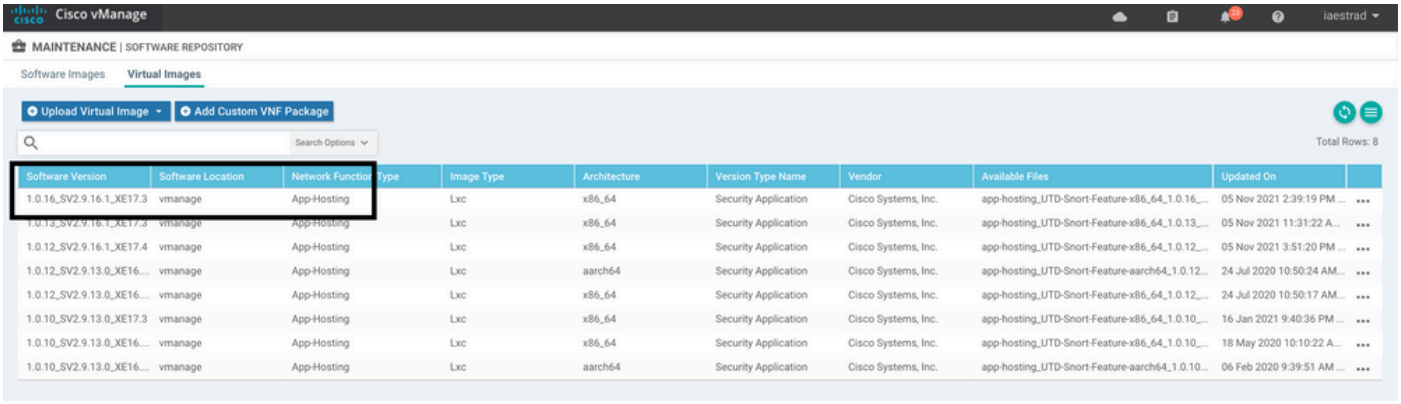
Verifique se a imagem virtual corresponde ao código atual da SDWAN do Cisco IOS XE no cEdge

e carregue-a no repositório vmanage.
Navegue até **Manutenção > Repositório de software > Imagem virtual > Carregar imagem virtual > vManage.**



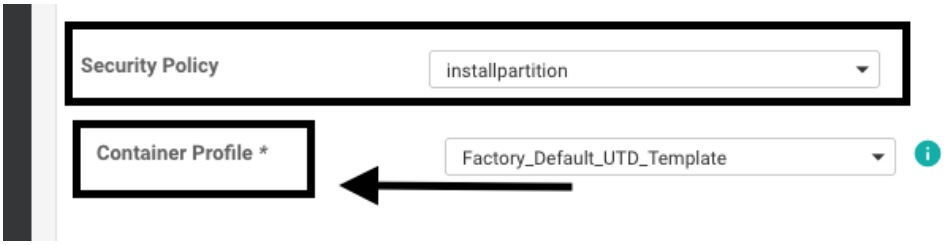


Quando a imagem virtual do Cisco UTD tiver sido carregada com êxito, verifique novamente se ela está no repositório.



Etapa 2. Adicionar política de segurança e submodelo de perfil do contêiner ao modelo do dispositivo

Adicione a política de segurança criada anteriormente ao modelo de dispositivo. A política de segurança deve ter uma política de filtragem IPS/IDS, URL-F ou AMP para o modelo do dispositivo. Abra o perfil do contêiner automaticamente. Use o perfil de contêiner padrão ou modifique-o, se necessário.

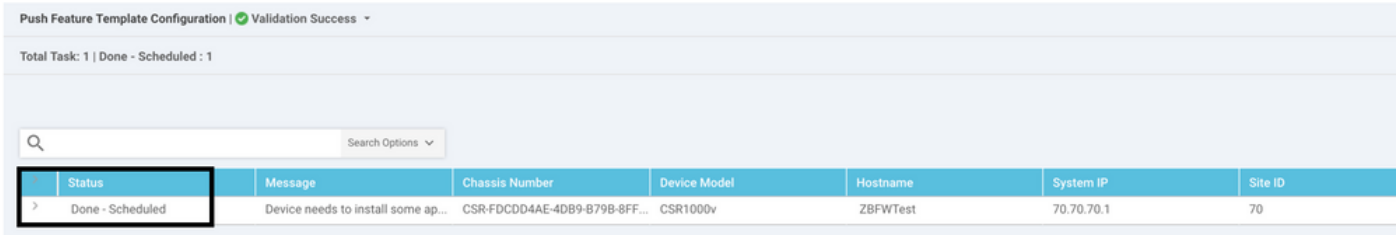


Etapa 3. Atualizar ou anexar o modelo do dispositivo com a política de segurança e o perfil do contêiner

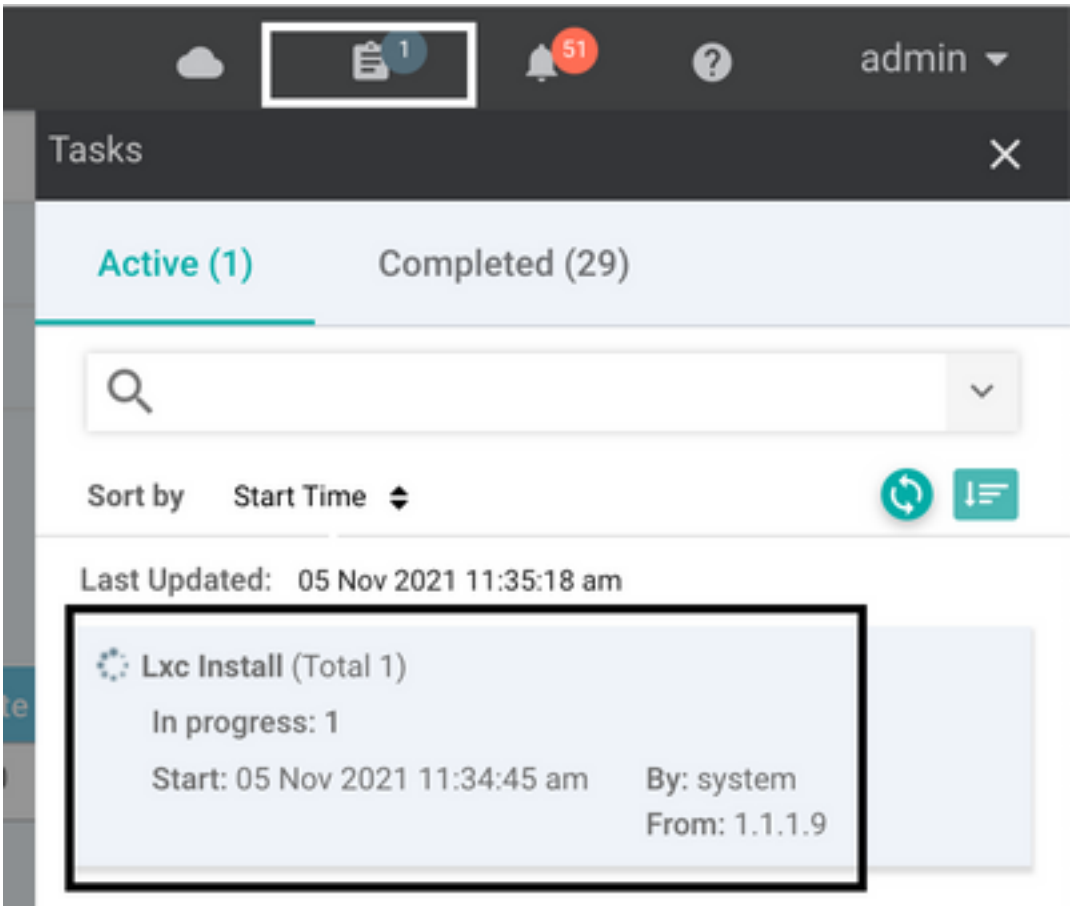
Atualize ou anexe o modelo ao roteador cEdge. Observe na configuração diff que a configuração de hospedagem de aplicativos e o mecanismo UTD para o recurso IPS/IDS, URL-F ou filtragem AMP estão configurados.

```
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
!
```

O status do modelo muda para **Concluído-agendado** porque o vmanage percebeu que a configuração aplicada tem recursos de mecanismo UTD; portanto, o vmanage determina que o cEdge precisa da Imagem Virtual instalada para usar os recursos de segurança UTD.



Depois que o modelo é movido para o estado de agendamento, uma nova tarefa **em andamento** aparece no menu de tarefas**.** A nova tarefa é a **instalação Lxc**, o que significa que o vmanage inicia automaticamente a instalação da imagem virtual no cEdge antes de enviar a nova configuração.

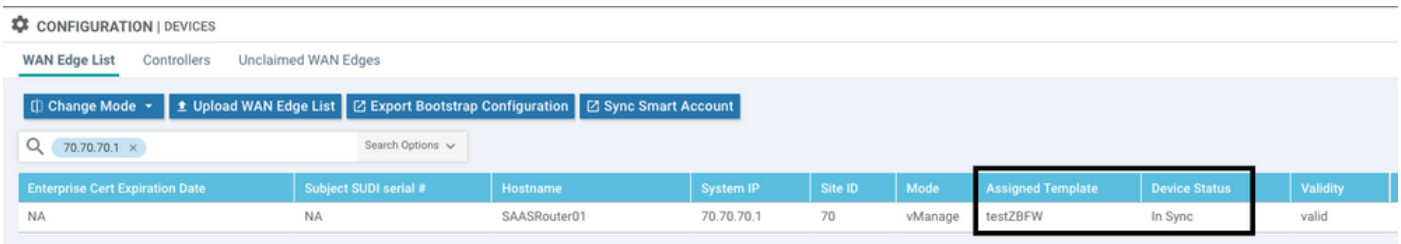


Depois que o contêiner LX for instalado, o vManage enviará a configuração pré-agendada com os recursos de UTD. Não há uma nova tarefa para isso porque a configuração foi agendada anteriormente.

Verificar

Verifique se o cEdge está em sincronia com o vManage e o modelo anexado.

Navegue até **Configuração > Dispositivos**



Verifique se a versão do 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         <<<<<<<<<<<<<<<<<<<
```

Observação A versão instalada do UTD não pode estar no **estado NÃO SUPORTADO**.

Verifique se o UTD está no estado **de execução** com a próxima saída:

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

O próximo comando resume os comandos anteriores e mostra o status e a versão atuais:

```
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
```

O comando **show utd engine standard status** mostra o status de funcionamento do mecanismo UTD e lista o tempo em que ele obtém a atualização da assinatura.

```
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 se os recursos estão ativados usando o próximo comando:

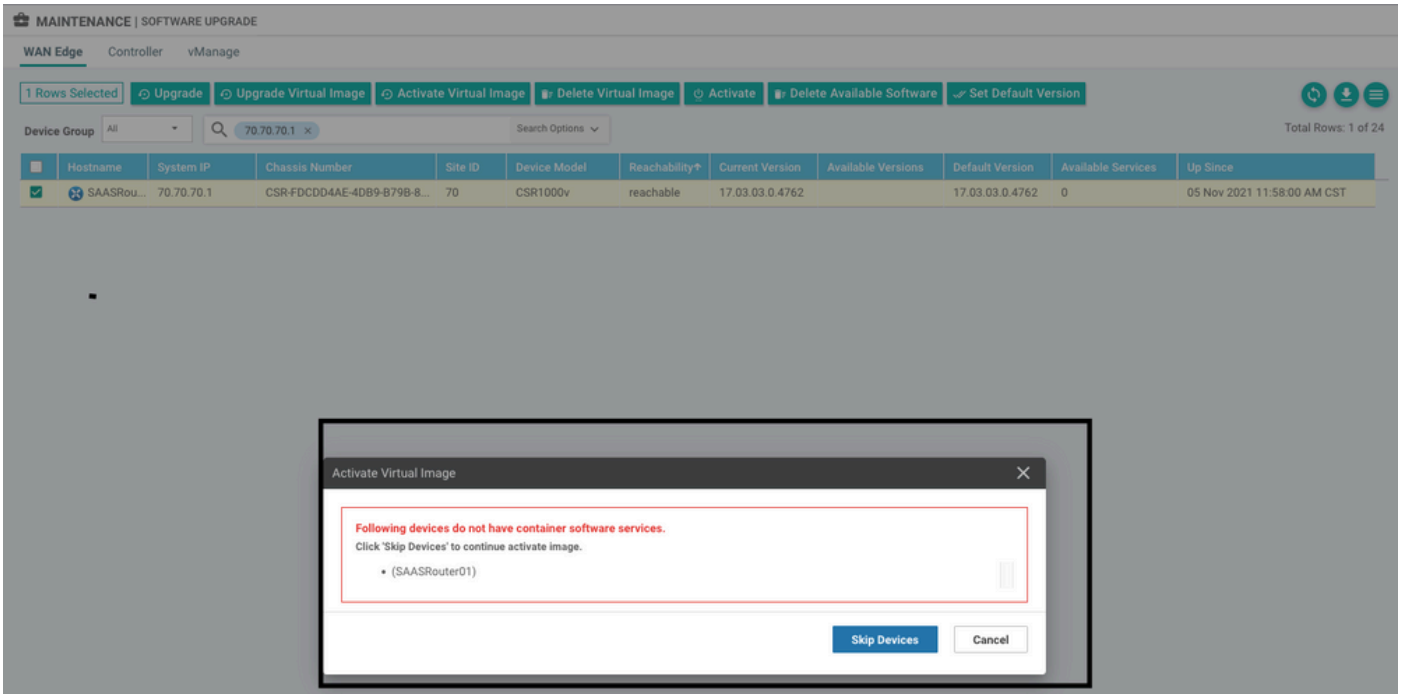
```
Router02# show platform hardware qfp active feature utd config
Global configuration
  NAT64: disabled
  Drop pkts: disabled
  Multi-tenancy: enabled
  Data plane initialized: yes
  TLS Decryption Policy: disabled
  Divert controller mode: enabled
  SN threads: 12
  CFT inst_id 0 feat id 2 fo id 2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

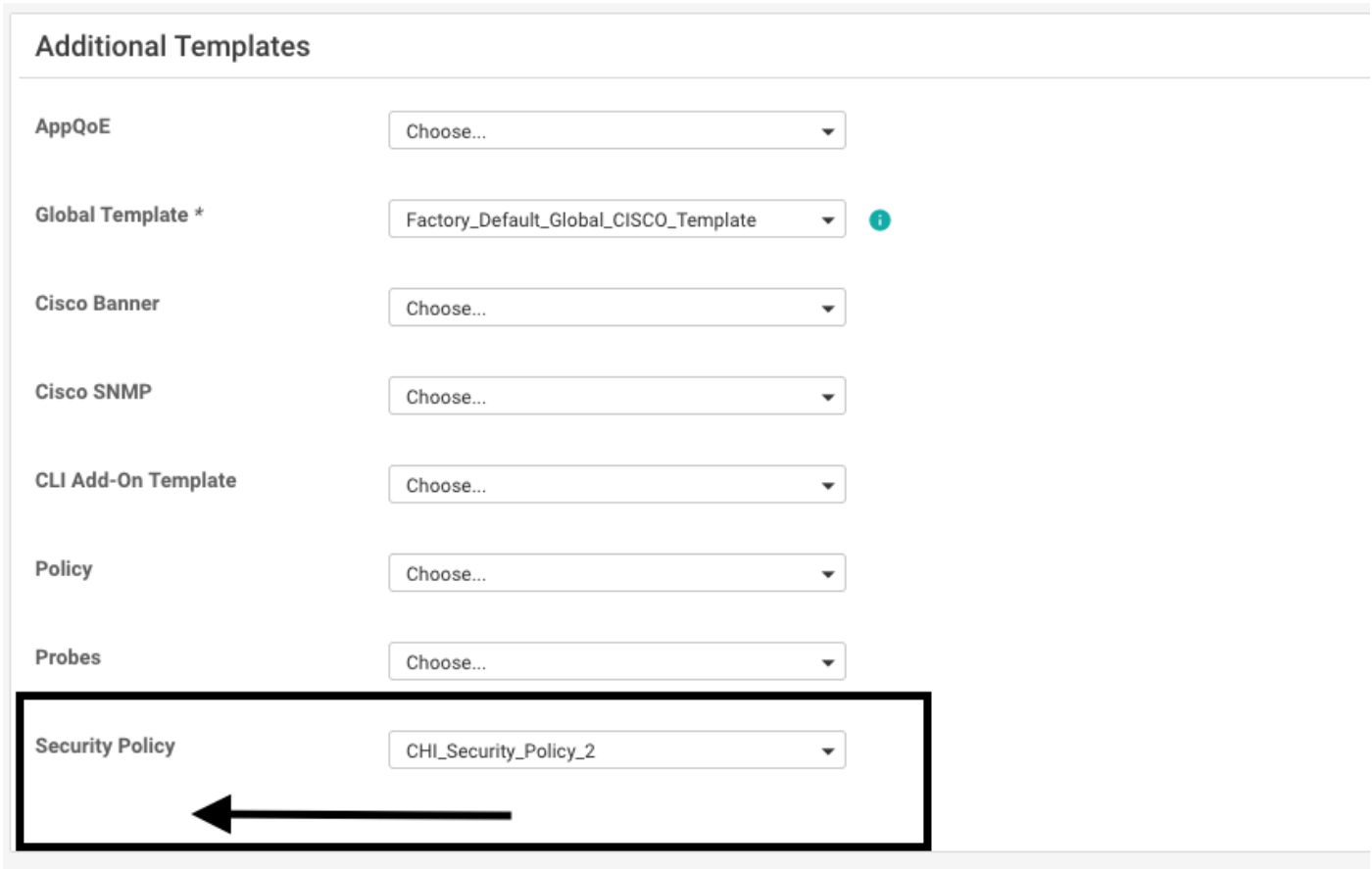
PROBLEMA 1. Erro: Os seguintes dispositivos não têm serviços de software de contêiner

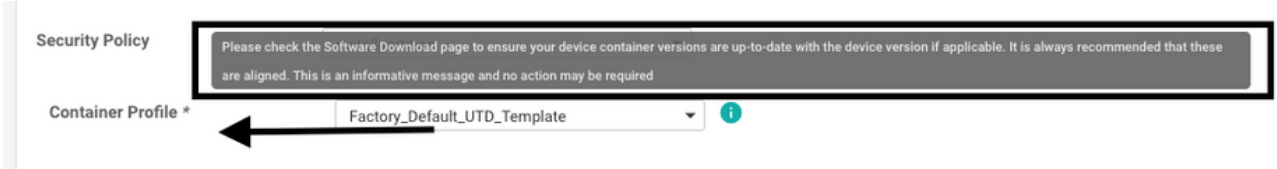
Ative a imagem virtual.

Navegue até **manutenção > software > ativar**



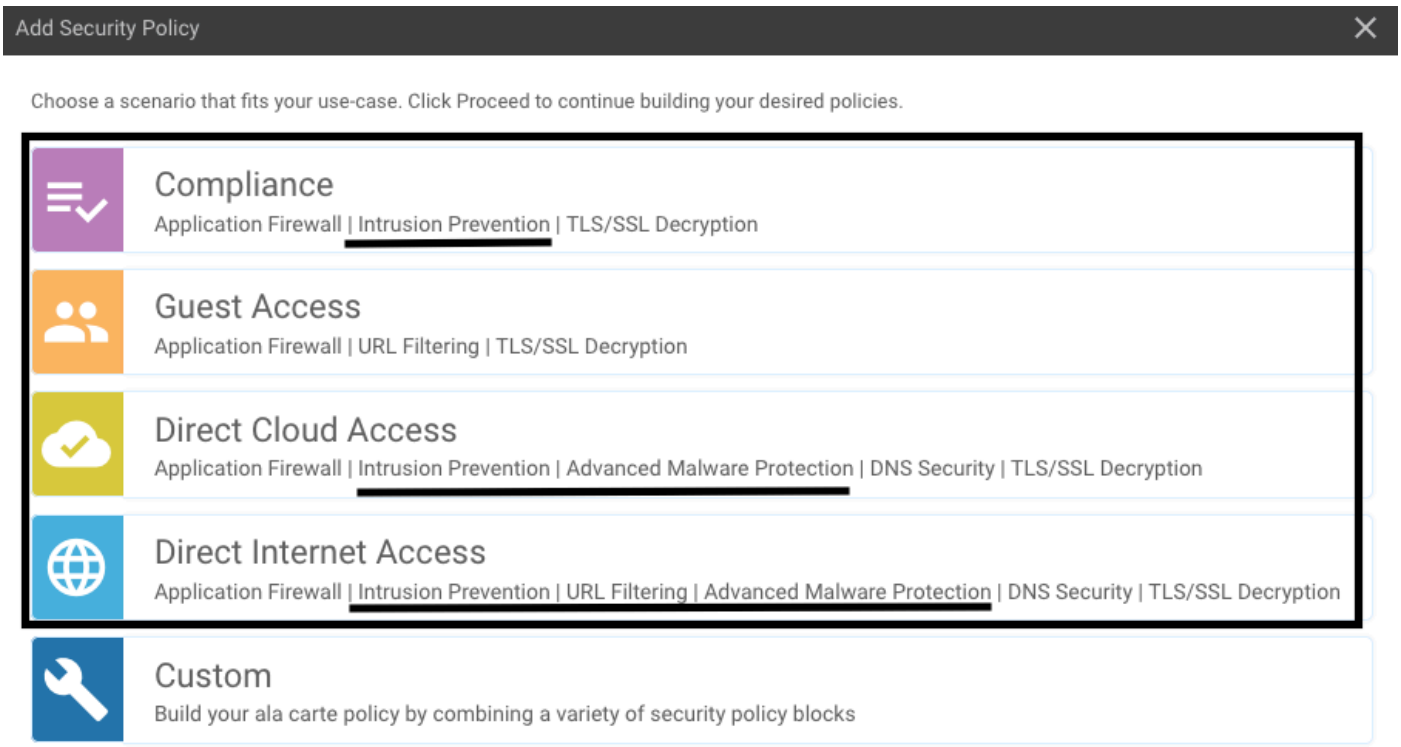
A imagem virtual enviou um erro: **Os dispositivos não têm serviços de software de contêiner**, se o roteador cEdge selecionado não tiver uma política de segurança com o submodelo de perfil de contêiner.





Este modelo será adicionado automaticamente se você usar uma Política de segurança que

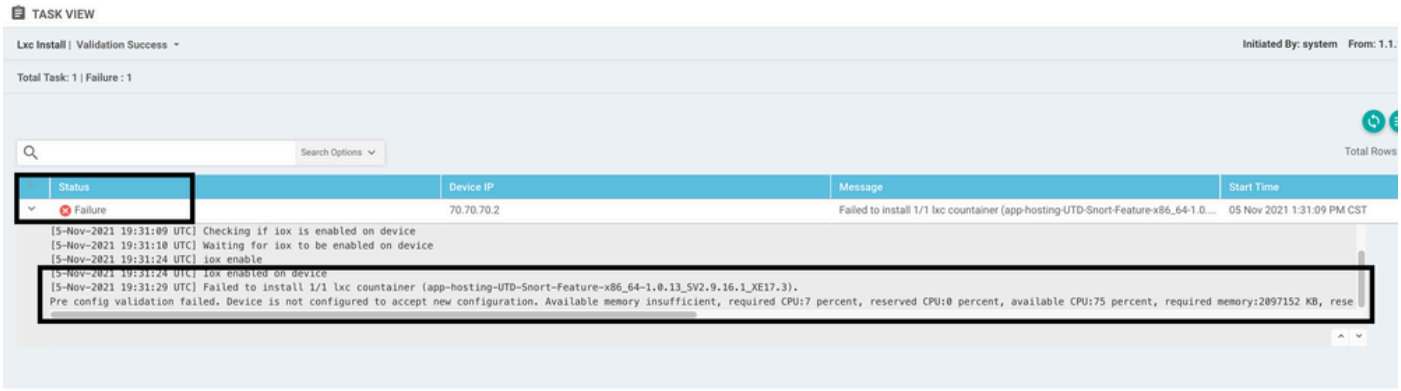
inclua recursos de segurança, como IPS (Sistema de prevenção de intrusão), IDS (Sistema de detecção de intrusão), Filtragem de URL (URL-F) e AMP (Proteção avançada contra malware), que precisam do pacote UTD. Nem todos os recursos de segurança disponíveis precisam do mecanismo UTD, como o recurso ZBFW simples.



Depois de enviar o modelo com o submodelo de perfil de contêiner, o gerenciador instalará automaticamente a imagem virtual.

PROBLEMA 2. Memória disponível insuficiente

Verifique se o roteador cEdge tem 8 GB de memória DRAM; caso contrário, o processo de instalação Lxc envia um **dispositivo não está configurado para aceitar a nova configuração.** Erro **de memória insuficiente**. Os requisitos para que os roteadores cEdge usem recursos UTD são ter no mínimo 8 GB de DRAM.



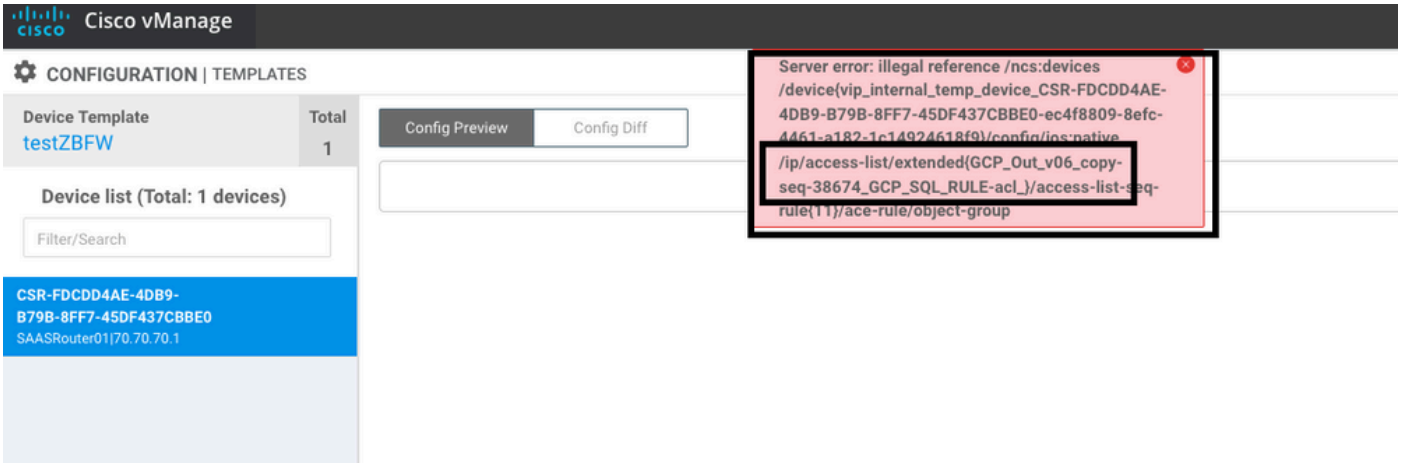
Nesse caso, o CSRv tem apenas 4 GB de DRAM. Após a atualização da memória para DRAM de 8 GB, a instalação é um sucesso.

Verifique a memória total atual com a saída **show sdwan system status**:

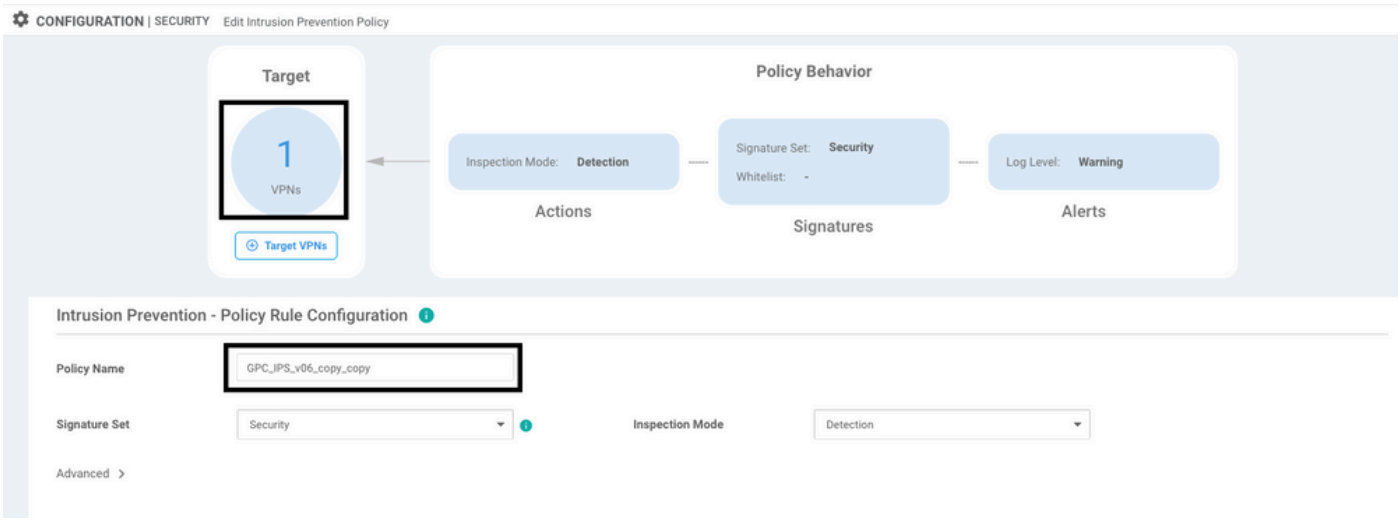
```
Router01# show sdwan system status

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

QUESTÃO 3. Referência ilegal

Certifique-se de que as VPNs/VRFs usadas em qualquer um dos recursos de Política de Segurança já estejam configuradas no roteador de borda para evitar uma referência ilegal para as sequências de Política de Segurança.



Neste exemplo, a política de segurança tem uma política de prevenção de intrusão para VPN/VRF 1, mas os dispositivos não têm nenhum VRF 1 configurado. Portanto, o vmanage envia uma referência ilegal para essa sequência de política.



Após configurar o VRF mencionado nas Políticas de segurança, a referência Ilegal não aparece e o modelo é enviado com êxito.

PROBLEMA 4. O UTD está instalado e ativo, mas não habilitado

O dispositivo tem uma política de segurança configurada e o UTD está instalado e ativo, mas não está habilitado.

Esse problema está relacionado ao problema número 3, no entanto, o vManage permitiu que a configuração fizesse referência a VRFs que não estão configurados no dispositivo e a política não é aplicada a nenhum VRF.

Para determinar se o roteador enfrenta esse problema, você precisa ver o UTD ativo. Mensagem UTD não habilitada e a política não faz referência a nenhum 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 a resolução, verifique as VPNs de destino e certifique-se de aplicar a política a um VRF configurado.

Informações Relacionadas

- Segurança do roteador: Snort IPS em roteadores
- Guia de configuração de segurança Cisco SD-WAN, versão Cisco IOS XE
- Suporte Técnico e Documentação - Cisco Systems

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.