

Instalar Imagem Virtual de Segurança UTD em Roteadores cEdge

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Roteadores que executam o software Cisco IOS XE SDWAN \(16.x\)](#)

[Roteadores que executam o software Cisco IOS XE \(17.x\)](#)

[Configurar](#)

[Etapa 1. Fazer upload da imagem virtual](#)

[Etapa 2. Adicionar política de segurança e submodelo de perfil do contêiner ao modelo do dispositivo](#)

[Etapa 3. Atualizar ou anexar o modelo do dispositivo com a política de segurança e o perfil do contêiner](#)

[Verificar](#)

[Problemas comuns](#)

[PROBLEMA 1. Erro: Os seguintes dispositivos não têm serviços de software de contêiner](#)

[PROBLEMA 2. Memória disponível insuficiente](#)

[QUESTÃO 3. Referência ilegal](#)

[PROBLEMA 4. O UTD está instalado e ativo, mas não habilitado](#)

[Informações Relacionadas](#)

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](#)

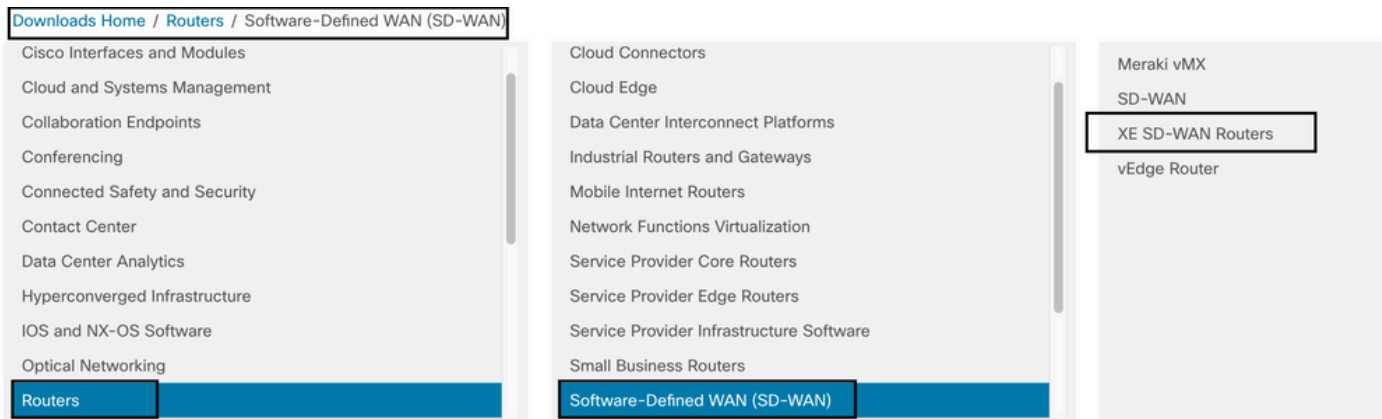
Use o regex suportado pela imagem virtual Cisco UTD para a versão atual do Cisco IOS XE. Use o comando **show utd engine standard** version para validar a imagem UTD recomendada e suportada.

```
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).

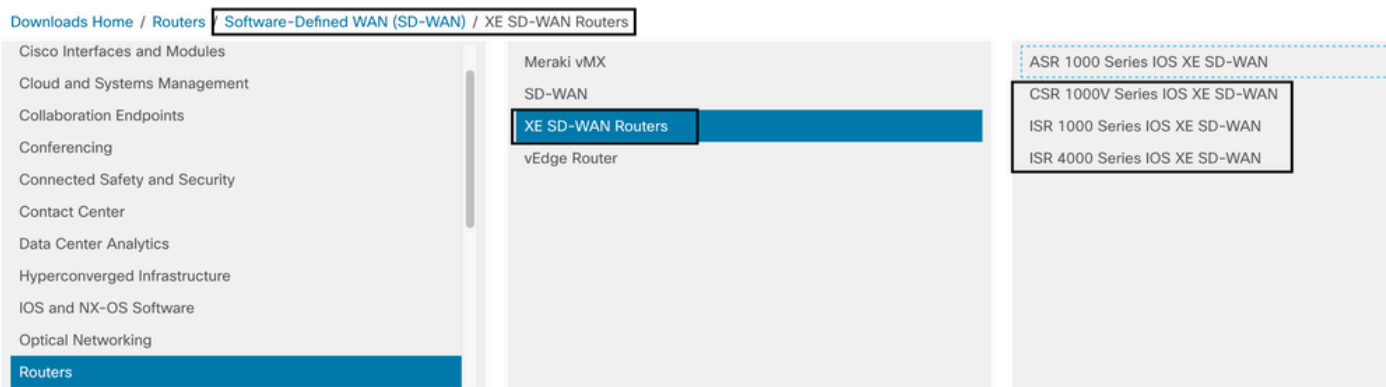
Roteadores que executam o software Cisco IOS XE SDWAN (16.x)

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.

[Downloads Home](#) / [Routers](#) / [Software-Defined WAN \(SD-WAN\)](#) / [XE SD-WAN Routers](#) / [ISR 4000 Series IOS XE SD-WAN](#)

Select a Software Type

[IOS XE In-Service Software Upgrade \(ISSU\) Matrix](#)

[IOS XE SD-WAN Software](#)

[IOS XE Software](#)

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.

Q Search...

Expand All Collapse All

Suggested Release

16.12.5(MD)

Latest Release

16.12.5(MD)

All Release

16

Deferred Release

16

ISR 4000 Series IOS XE SD-WAN

Release 16.12.5 **MD**

▲ My Notifications

Related Links and Documentation

[Release Notes for 19.2.4](#)

[Release Notes for 16.12.5](#)

File Information	Release Date	Size	
Cisco ISR 4200 Series IOS XE SD-WAN Software isr4200-ucmk9.16.12.5.SPA.bin Advisories	29-Jan-2021	482.84 MB	↓ 🛒 📄
Cisco ISR 4300 Series IOS XE SD-WAN Software isr4300-ucmk9.16.12.5.SPA.bin Advisories	29-Jan-2021	557.83 MB	↓ 🛒 📄
Cisco ISR 4400 Series IOS XE SD-WAN Software isr4400-ucmk9.16.12.5.SPA.bin Advisories	29-Jan-2021	621.88 MB	↓ 🛒 📄
Cisco ISR 4400v2 Series IOS XE SD-WAN Software isr4400v2-ucmk9.16.12.5.SPA.bin Advisories	29-Jan-2021	623.49 MB	↓ 🛒 📄
UTD Engine for IOS XE SD-WAN secapp-ucmk9.16.12.05.1.0.18_SV2.9.16.1_XE16.12.x86_64.tar Advisories	29-Jan-2021	52.01 MB	↓ 🛒 📄

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**.

Downloads Home **Routers / Branch Routers**

- Cisco Interfaces and Modules
- Cloud and Systems Management
- Collaboration Endpoints
- Conferencing
- Connected Safety and Security
- Contact Center
- Data Center Analytics
- Hyperconverged Infrastructure
- IOS and NX-OS Software
- Optical Networking
- Routers**

Branch Routers

- Cloud Connectors
- Cloud Edge
- Data Center Interconnect Platforms
- Industrial Routers and Gateways
- Mobile Internet Routers
- Network Functions Virtualization
- Service Provider Core Routers
- Service Provider Edge Routers
- Service Provider Infrastructure Software
- Small Business Routers

- 1000 Series Integrated Services Routers**
- 1800 Series Integrated Services Routers
- 1900 Series Integrated Services Routers
- 2900 Series Integrated Services Routers
- 3900 Series Integrated Services Routers
- 4000 Series Integrated Services Routers
- 5000 Series Enterprise Network Compute System
- 800 Series Routers
- 900 Series Integrated Services Routers
- Catalyst 8200 Series Edge Platforms
- Catalyst 8300 Series Edge Platforms

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

Software Download

[Downloads Home](#) / [Routers](#) / [Branch Routers](#) / [4000 Series Integrated Services Routers](#) / [4221 Integrated Services Router](#)

Downloads Home

Select a Software Type

[IOS XE In-Service Software Upgrade \(ISSU\) Matrix](#)

[IOS XE Patch Upgrades](#)

[IOS XE ROMMON Software](#)

[IOS XE SD-WAN Software](#)

[IOS XE Software](#)

[UTD Snort IPS Engine Software](#)

[UTD Snort Subscriber Signature Package](#)

[Very High Bitrate \(VDSL\) PHY Firmware](#)

[Very High Bitrate DSL \(VDSL\) Firmware](#)

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

Software Download

[Downloads Home](#) / [Routers](#) / [Branch Routers](#) / [4000 Series Integrated Services Routers](#) / [4221 Integrated Services Router](#) / [UTD Snort IPS Engine Software- 17.7.1a](#)

[Expand All](#) [Collapse All](#)

Latest Release

- 17.7.1a**
- Fuji-16.9.8
- 16.6.7a

All Release

- 16.6
- 17
- 16

4221 Integrated Services Router

Release 17.7.1a

[My Notifications](#)

Related Links and Documentation
- No related links or documentation -

File Information	Release Date	Size
UTD Engine OVA for 17.7.1 release iosxe-utd.17.07.01a.1.0.3_SV2.9.16.1_XE17.7.x86_64.ova Advisories	30-Nov-2021	147.72 MB
UTD Engine for IOS XE secapp-utd.17.07.01a.1.0.3_SV2.9.16.1_XE17.7.x86_64.tar Advisories	30-Nov-2021	52.51 MB

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.

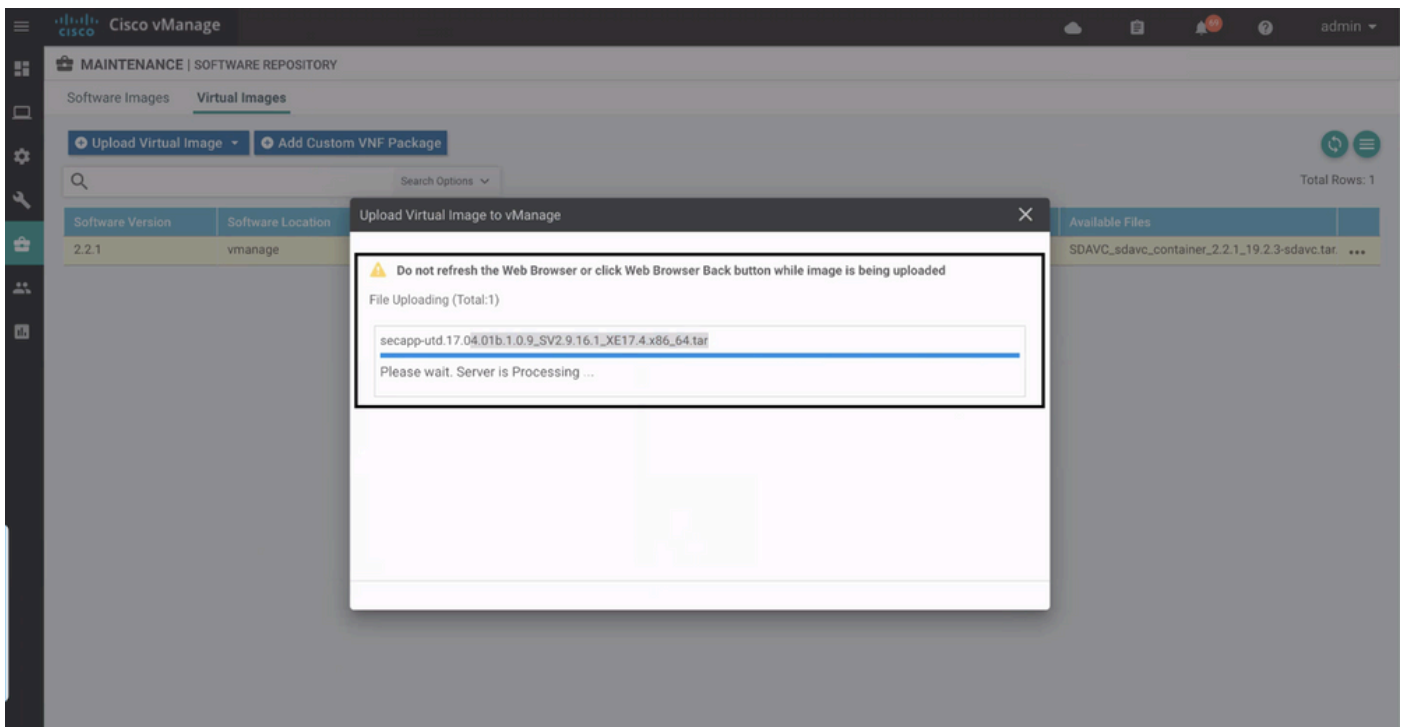
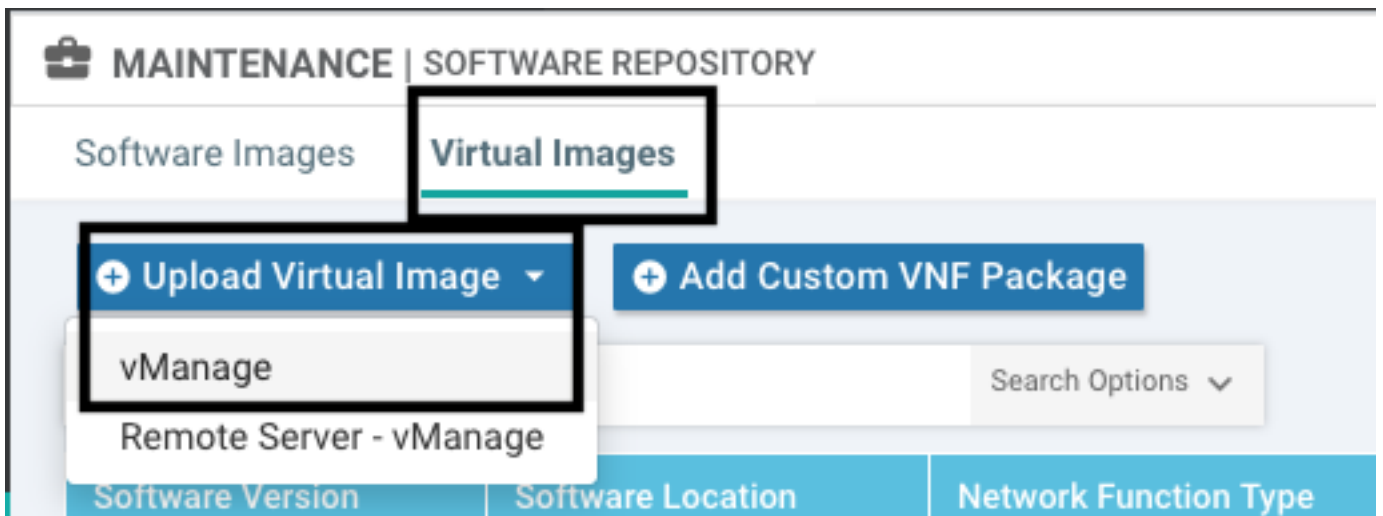
Configurar

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.



Cisco vManage MAINTENANCE | SOFTWARE REPOSITORY

Software Images Virtual Images

Upload Virtual Image Add Custom VNF Package

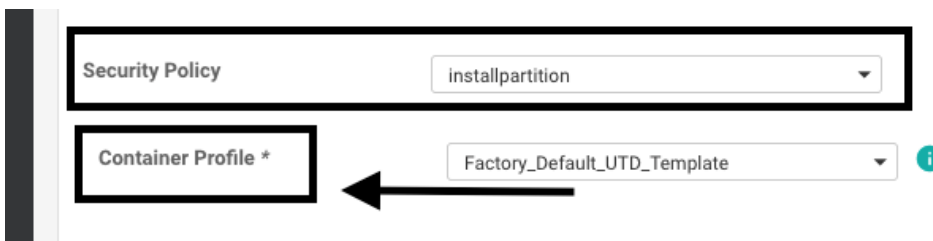
Search Options

Total Rows: 8

Software Version	Software Location	Network Function	Type	Image Type	Architecture	Version Type Name	Vendor	Available Files	Updated On
1.0.16_SV2.9.16.1_XE17.3	vmanage	App-Hosting	Lxc	x86_64	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.16...	05 Nov 2021 2:39:19 PM ...
1.0.13_SV2.9.16.1_XE17.2	vmanage	App-Hosting	Lxc	x86_64	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.13...	05 Nov 2021 11:31:22 A...
1.0.12_SV2.9.16.1_XE17.4	vmanage	App-Hosting	Lxc	x86_64	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.12...	05 Nov 2021 3:51:20 PM ...
1.0.12_SV2.9.13.0_XE16...	vmanage	App-Hosting	Lxc	aarch64	aarch64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-aarch64_1.0.12...	24 Jul 2020 10:50:24 AM...
1.0.12_SV2.9.13.0_XE16...	vmanage	App-Hosting	Lxc	x86_64	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.12...	24 Jul 2020 10:50:17 AM...
1.0.10_SV2.9.13.0_XE17.3	vmanage	App-Hosting	Lxc	x86_64	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.10...	16 Jan 2021 9:40:36 PM ...
1.0.10_SV2.9.13.0_XE16...	vmanage	App-Hosting	Lxc	x86_64	x86_64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-x86_64_1.0.10...	18 May 2020 10:10:22 A...
1.0.10_SV2.9.13.0_XE16...	vmanage	App-Hosting	Lxc	aarch64	aarch64	Security Application	Cisco Systems, Inc.	app-hosting_UTD-Snort-Feature-aarch64_1.0.10...	06 Feb 2020 9:39:51 AM ...

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.

```
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 !ldp run
259 269 nat64 translation timeout tcp 60
260 270 nat64 translation timeout udp 1
271
272 utd multi-tenancy
273 utd engine standard multi-tenancy
274   threat-inspection profile GPC_IPS_v06_copy_copy
275     threat detection
276     policy security
277     logging level warning
278   !
279 utd global
280 !
281 !
282 policy
283   no app-visibility
284   no flow-visibility
285   no implicit-acl-logging
286   log-frequency 1000
287 !
```

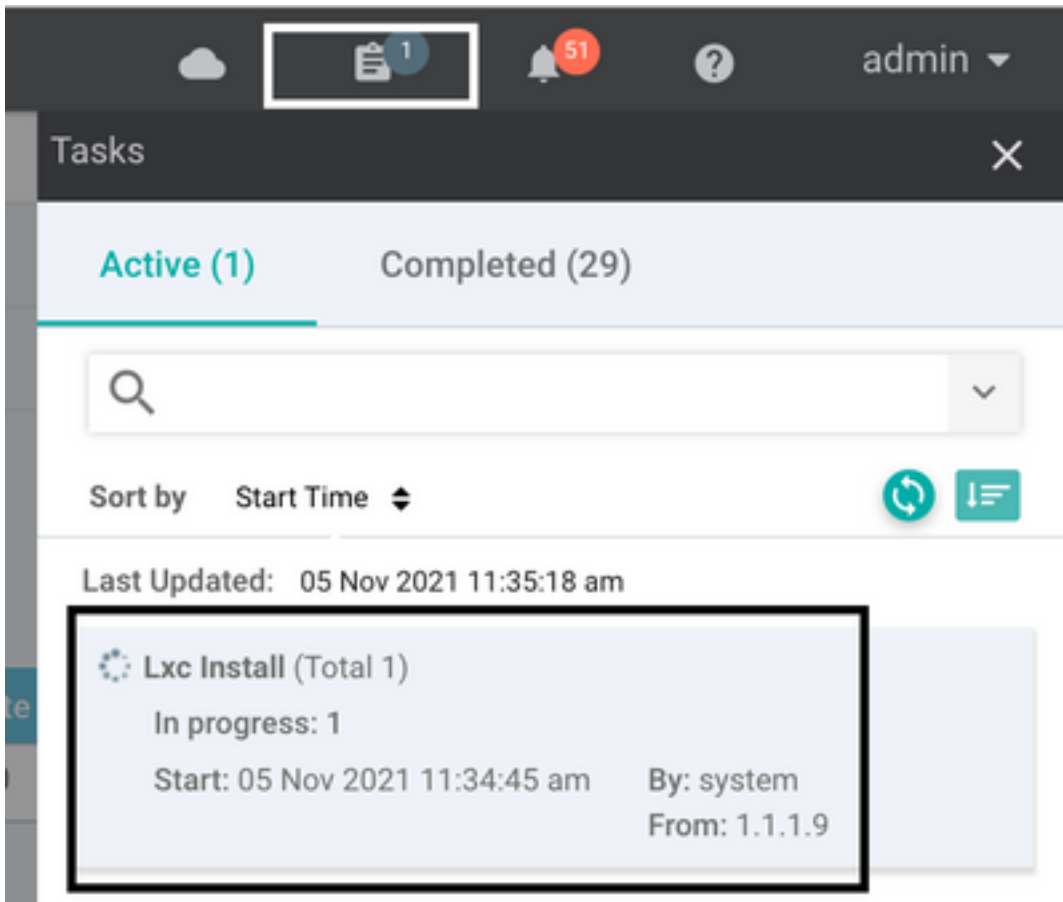
O status do modelo muda para **Concluído-agendado** porque o vmanage percebeu que a configuração aplicada tem recursos de mecanismo UTD; portanto, o vmanage determina que o cEdge precisa da Imagem Virtual instalada para usar os recursos de segurança UTD.

Push Feature Template Configuration | Validation Success

Total Task: 1 | Done - Scheduled : 1

Status	Message	Chassis Number	Device Model	Hostname	System IP	Site ID
Done - Scheduled	Device needs to install some ap...	CSR-FDCDD4AE-4DB9-B79B-8FF...	CSR1000v	ZBFWTest	70.70.70.1	70

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.



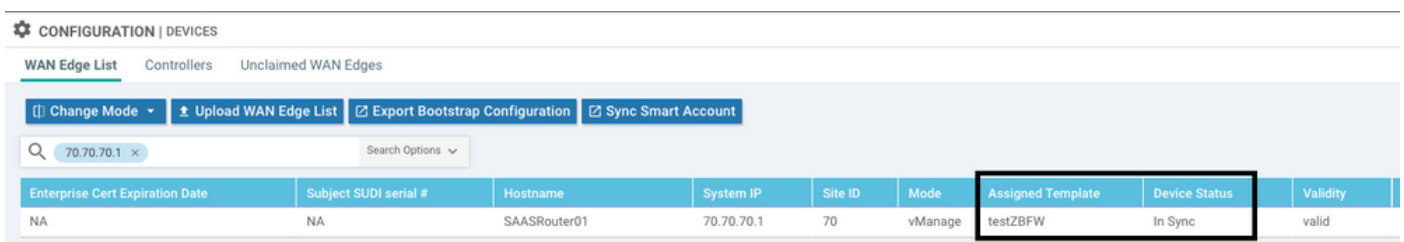
Depois que o contêiner LX for instalado, o vManage enviará a configuração pré-agendada com os recursos de UTD. Não há uma nova tarefa para isso porque a configuração foi agendada anteriormente.



Verificar

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

Navegue até **Configuração > Dispositivos**



MAINTENANCE | SOFTWARE UPGRADE

WAN Edge Controller vManage

1 Rows Selected Upgrade Upgrade Virtual Image Activate Virtual Image Delete Virtual Image Activate Delete Available Software Set Default Version

Device Group All 70.70.70.1 Search Options Total Rows: 1 of 24

Hostname	System IP	Chassis Number	Site ID	Device Model	Reachability*	Current Version	Available Versions	Default Version	Available Services	Up Since
SAASRou...	70.70.70.1	CSR-FDCDD4AE-4DB9-B798-8...	70	CSR1000v	reachable	17.03.03.0.4762		17.03.03.0.4762	0	05 Nov 2021 11:58:00 AM CST

Activate Virtual Image

Following devices do not have container software services.
Click 'Skip Devices' to continue activate image.

- (SAASRouter01)

Skip Devices Cancel

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.

Additional Templates

AppQoE Choose...

Global Template * Factory_Default_Global_CISCO_Template ⓘ

Cisco Banner Choose...

Cisco SNMP Choose...

CLI Add-On Template Choose...

Policy Choose...

Probes Choose...

Security Policy CHI_Security_Policy_2

Security Policy

Please check the Software Download page to ensure your device container versions are up-to-date with the device version if applicable. It is always recommended that these are aligned. This is an informative message and no action may be required

Container Profile * Factory_Default_UTD_Template ⓘ

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.

Add Security Policy [X]

Choose a scenario that fits your use-case. Click Proceed to continue building your desired policies.

- Compliance**
Application Firewall | Intrusion Prevention | TLS/SSL Decryption
- Guest Access**
Application Firewall | URL Filtering | TLS/SSL Decryption
- Direct Cloud Access**
Application Firewall | Intrusion Prevention | Advanced Malware Protection | DNS Security | TLS/SSL Decryption
- Direct Internet Access**
Application Firewall | Intrusion Prevention | URL Filtering | Advanced Malware Protection | DNS Security | TLS/SSL Decryption
- Custom**
Build your ala carte policy by combining a variety of security policy blocks

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.

TASK VIEW

Lxc Install | Validation Success - [Initiated By: system From: 1.1.]

Total Task: 1 | Failure: 1

status	Device IP	Message	Start Time
Failure	70.70.70.2	Failed to install 1/1 lxc container (app-hosting-UTD-Snort-Feature-x86_64-1.0...)	05 Nov 2021 1:31:09 PM CST

```
[5-Nov-2021 19:31:09 UTC] Checking if iox is enabled on device
[5-Nov-2021 19:31:10 UTC] Waiting for iox to be enabled on device
[5-Nov-2021 19:31:24 UTC] iox enable
[5-Nov-2021 19:31:24 UTC] iox enabled on device
[5-Nov-2021 19:31:29 UTC] Failed to install 1/1 lxc container (app-hosting-UTD-Snort-Feature-x86_64-1.0.13_SV2.9.16.1_XE17.3).
Pre config validation failed. Device is not configured to accept new configuration. Available memory insufficient, required CPU:7 percent, reserved CPU:0 percent, available CPU:75 percent, required memory:2097152 KB, rese...
```

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

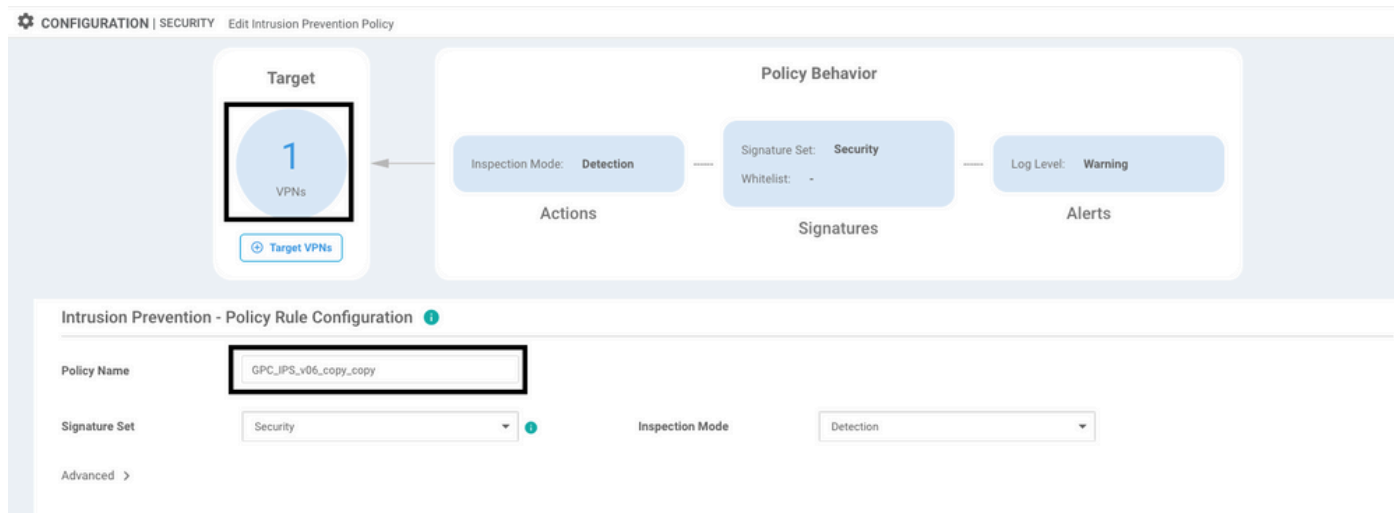
Memory usage: 8107024K total, 3598816K used, 4508208K free
349492K buffers, 2787420K cache

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 seqüências 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 seqüência 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.