

Configurar e verificar a filtragem de URL

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar Componentes para Política de Filtragem de URL](#)

[Criar listas de URL de interesse](#)

[Criar Política de Segurança](#)

[Aplicar uma política de segurança a um dispositivo](#)

[Modificar filtragem de URL](#)

[Excluir filtragem de URL](#)

[Verificar](#)

[Monitore a filtragem de URL a partir da GUI do vManage](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar e verificar a filtragem de URL em roteadores Cisco IOS-XE® usando a GUI do Cisco Catalyst Manager.

Pré-requisitos

Carregue a imagem virtual do software UTD compatível com o código atual do Cisco IOS-XE no vManage. Consulte a seção Informações relacionadas para obter instruções sobre como instalar a imagem virtual de segurança UTD em roteadores cEdge.

O roteador Cisco Edge deve estar no modo vManaged com o modelo pré-conectado.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- O Cisco SD-WAN Overlay traz a configuração inicial.
- Configuração da filtragem de URL GUI do Cisco Catalyst Manager.

Componentes Utilizados

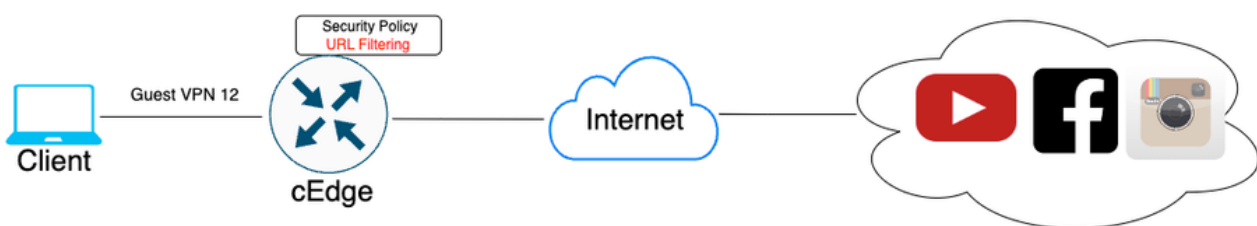
Este documento é baseado nestas versões de software e hardware:

- Cisco Catalyst SD-WAN Manager versão 20.14.1.
- Controlador Cisco Catalyst SD-WAN versão 20.14.1.
- Cisco Edge Router versão 17.14.1.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede



Configurar Componentes para Política de Filtragem de URL

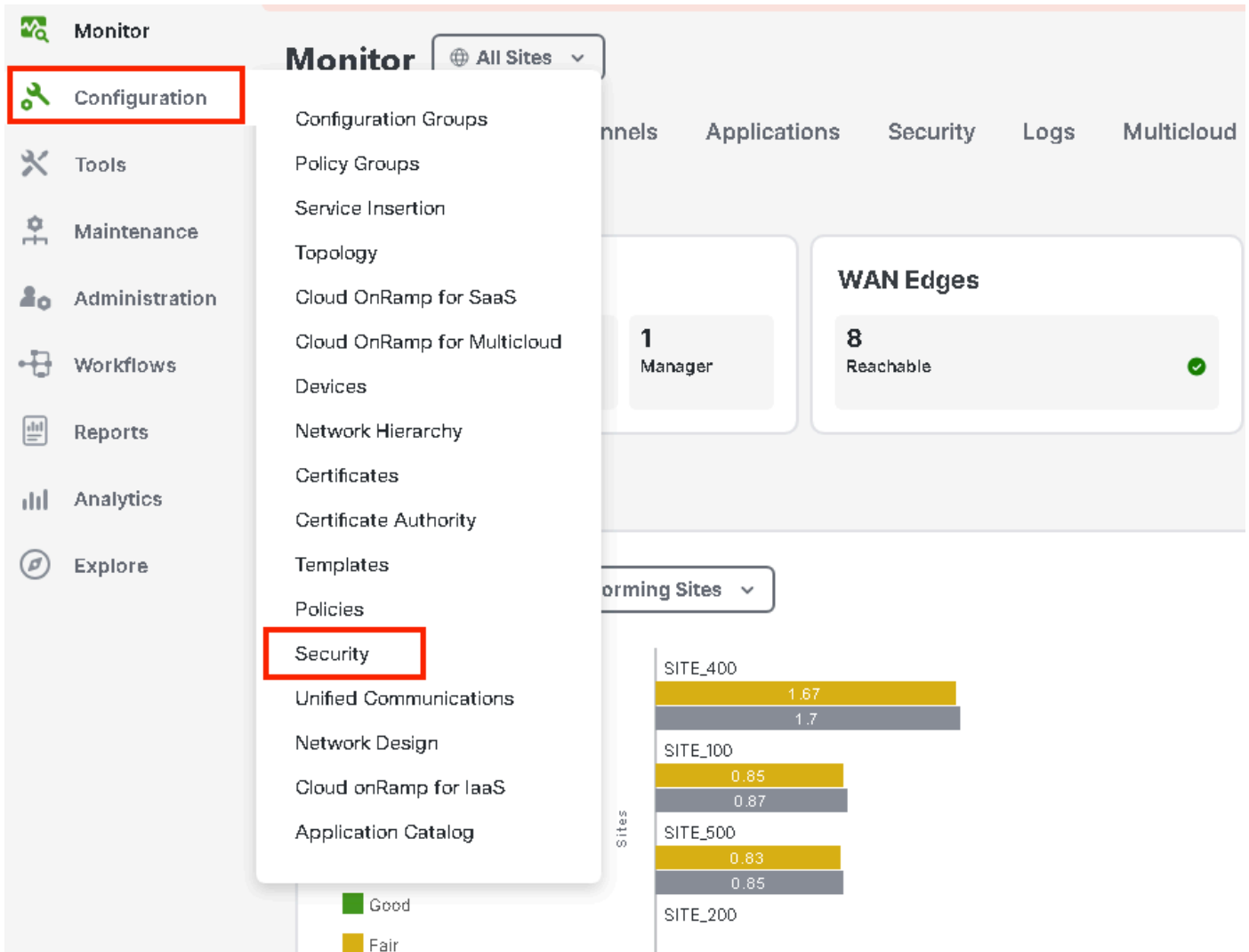
Este artigo explica como configurar a filtragem de URL para bloquear/permitir o tráfego HTTPS de determinados clientes com base na categoria, reputação ou por listas de bloqueio/permissão de domínio, considerando estes requisitos de exemplo:

- Bloquear estas solicitações HTTPS de clientes nas categorias da Web de VPN convidado:
 - Jogos
 - Jogos de azar
 - Hacking
 - Drogas ilegais
- Qualquer solicitação de URL HTTPS para sites do cliente na VPN convidada com reputação da Web menor ou igual a 60 deve ser bloqueada.
- As solicitações de HTTP(s) para sites de clientes no VPN convidado bloqueiam Facebook, Instagram e YouTube, ao mesmo tempo em que permitem acesso a google.com e yahoo.com.

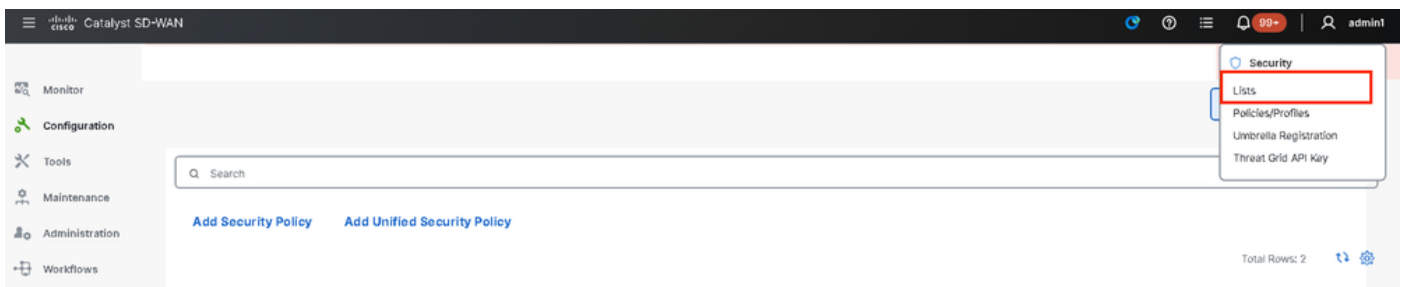
Para configurar a filtragem de URL:

Criar listas de URL de interesse

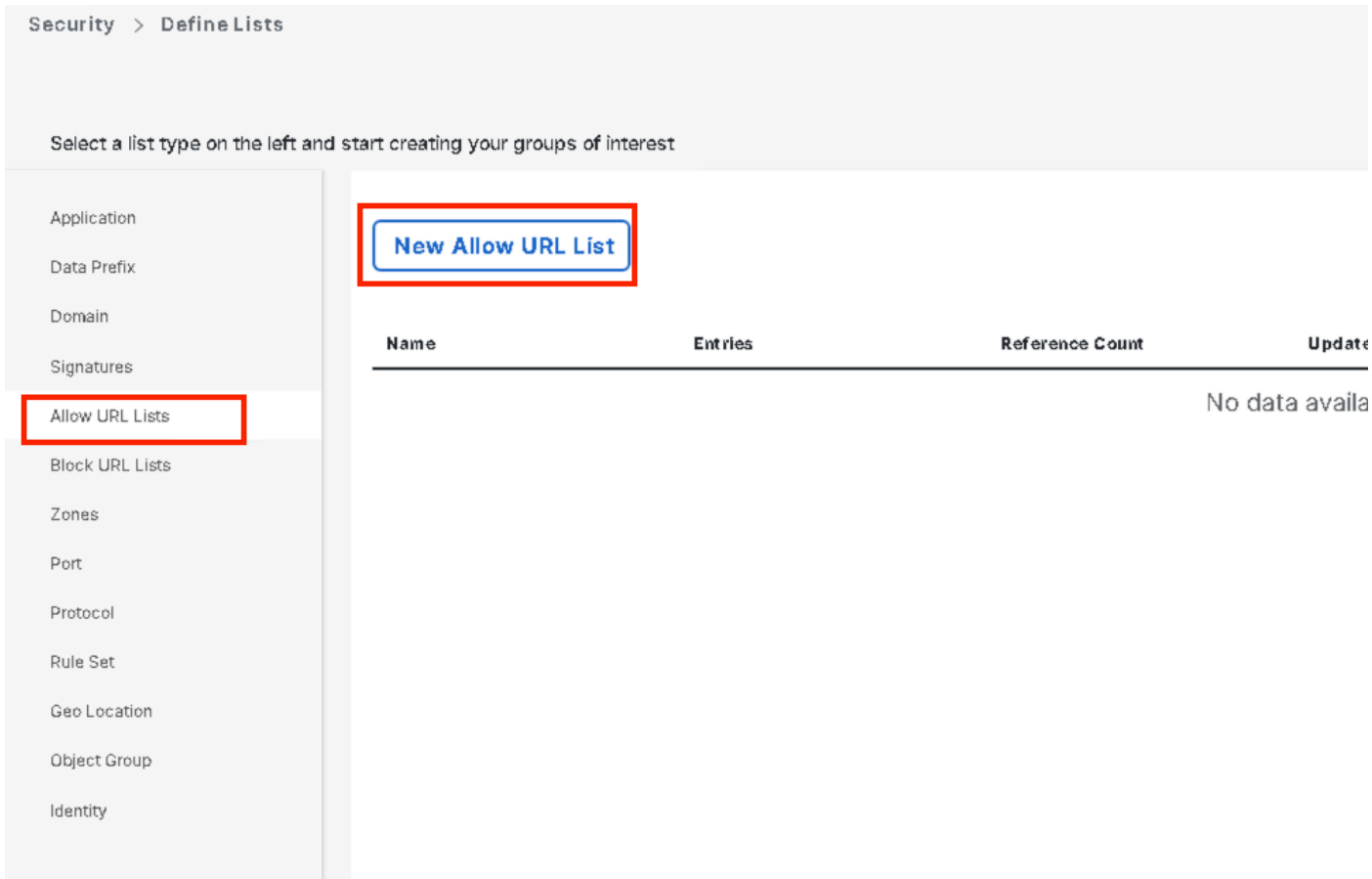
1. No menu Cisco SD-WAN Manager, navegue para a guia Configuration > Security no painel do lado esquerdo.



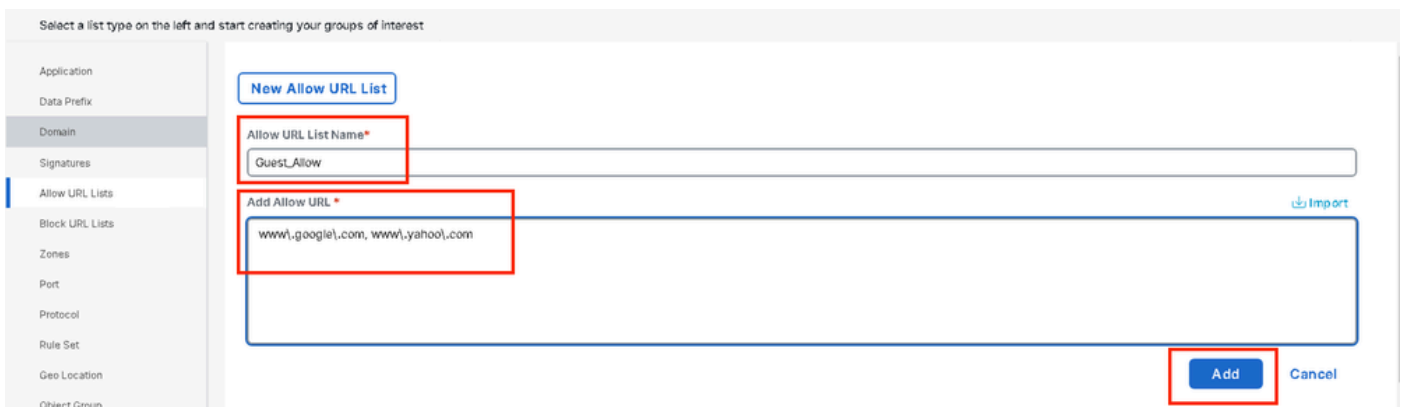
Para criar ou gerenciar Lista de URLs da lista de permissão ou Lista de URLs da lista de bloqueio, selecione Listas no menu suspenso Opções personalizadas na parte superior direita da página.



Clique em Allow URLs Lists no painel esquerdo e crie New Allow URL List.



- No campo Nome da lista de URLs, insira um nome de lista que contenha até 32 caracteres (somente letras, números, hífen e sublinhados).
- No campo URL, digite os URLs a serem incluídos na lista, separados por vírgulas. Você também pode usar o botão Importar para adicionar listas de um local de armazenamento acessível.
- Clique em Adicionar quando concluir.

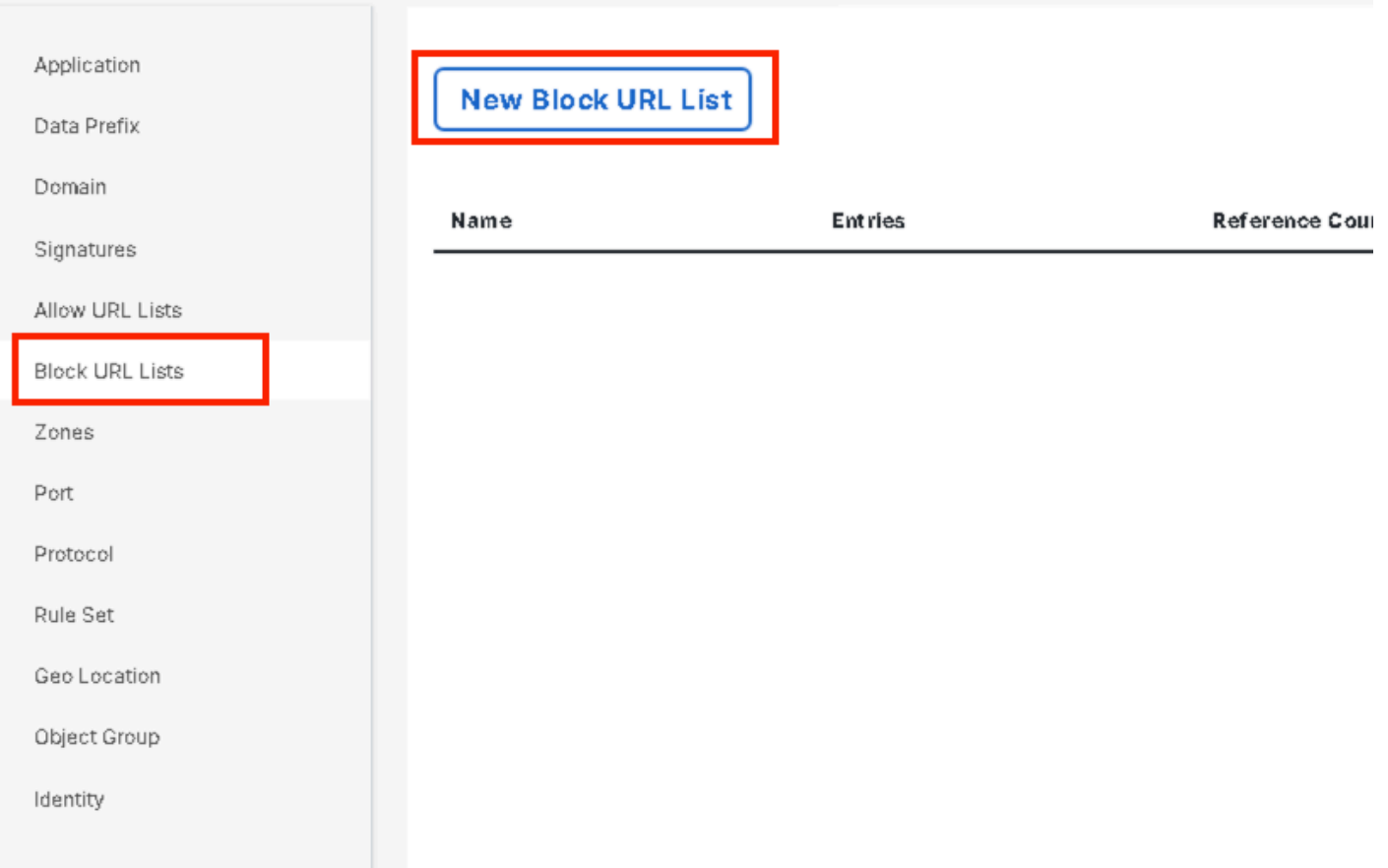




Observação: você pode considerar o uso de um padrão regex para o nome de domínio nas listas de permissão e bloqueio

Clique em Block URLs Lists no painel esquerdo e crie New Block URL List.

Select a list type on the left and start creating your groups of interest



Application

Data Prefix

Domain

Signatures

Allow URL Lists

Block URL Lists

Zones

Port

Protocol

Rule Set

Geo Location

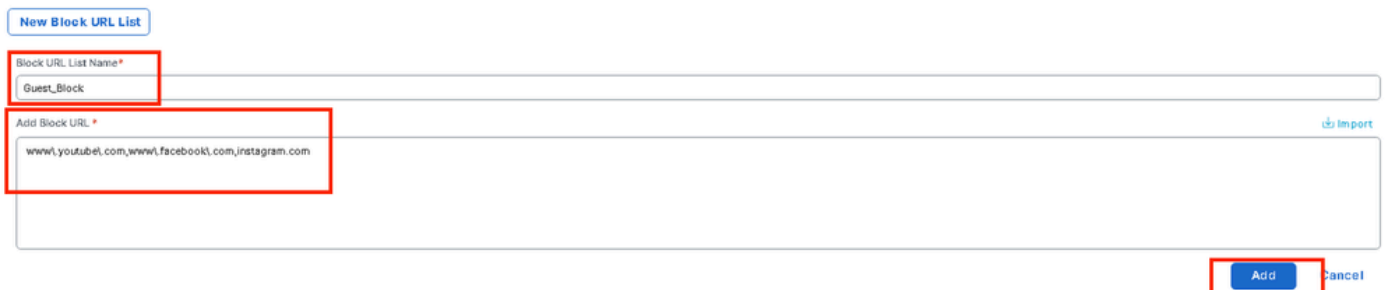
Object Group

Identity

New Block URL List

Name	Entries	Reference Count
------	---------	-----------------

- No campo Nome da lista de URLs, insira um nome de lista que contenha até 32 caracteres (somente letras, números, hífen e sublinhados)
- No campo URL, digite os URLs a serem incluídos na lista, separados por vírgulas. Você também pode usar o botão Importar para adicionar listas de um local de armazenamento acessível.
- Clique em Adicionar quando concluir.



New Block URL List

Block URL List Name*

Guest_Block

Add Block URL

www1.youtubel.com,www1.facebook.com,instagram.com

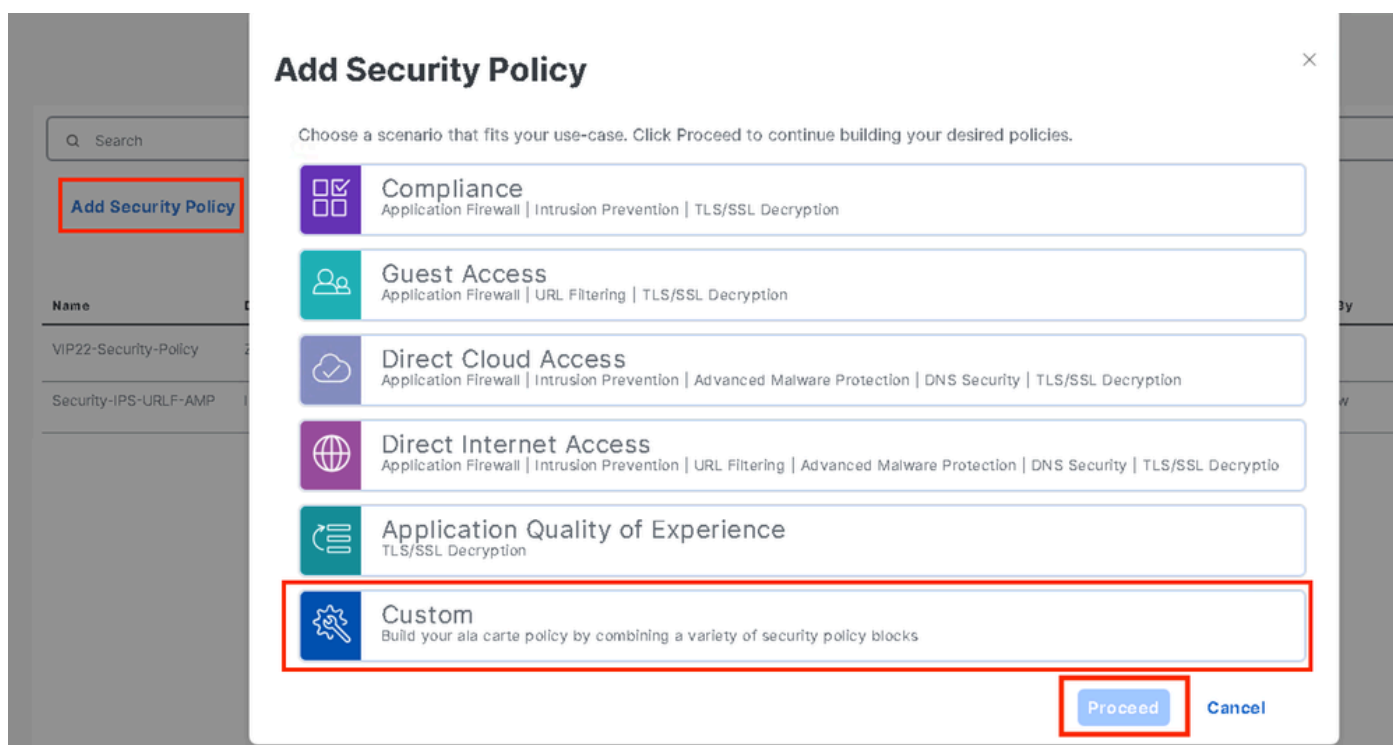
Import

Add Cancel

Criar Política de Segurança

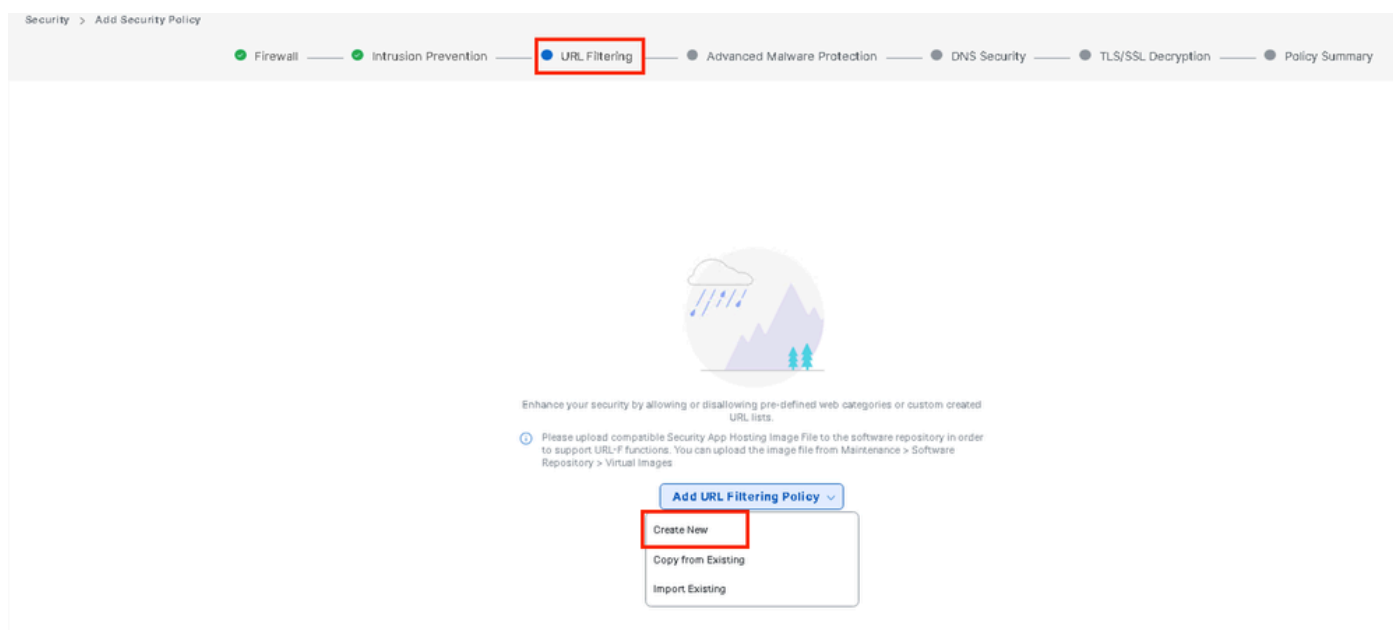
2. No menu do Cisco SD-WAN Manager, navegue para Configuração > Segurança Clique em Adicionar nova política de segurança. O assistente Adicionar política de segurança é aberto e

vários cenários de caso de uso são exibidos ou usam a política existente na lista. Selecione personalizado, clique em Continuar para adicionar uma política de filtragem de URL no assistente.



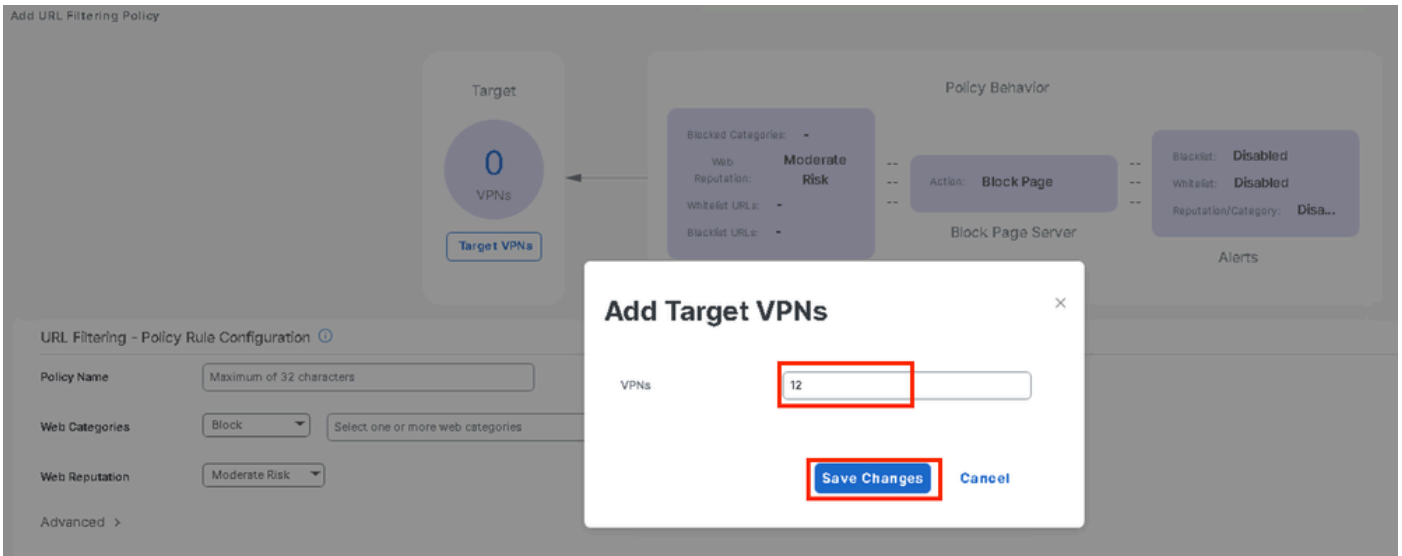
Observação: em Adicionar política de segurança, escolha um cenário que suporte a filtragem de URL (Acesso de convidado, Acesso direto à Internet ou Personalizado).

No Assistente Adicionar política de segurança, clique em Avançar até que a janela Filtragem de URL seja exibida. Agora, crie uma política de filtragem de URL indo para Filtragem de URL > Adicionar política de filtragem de URL > Criar novo. Clique em Next



Clique em Target VPNs para adicionar o número necessário de VPNs no assistente Add Target

VPNs.



- Insira um nome de política no campo Policy Name.
- Escolha uma dessas opções no menu suspenso Categorias da Web, selecione Bloquear e os sites que corresponderem às categorias escolhidas serão bloqueados.

Bloquear — Bloqueia sites da Web que correspondam às categorias selecionadas.

Permitir — Permitir sites que correspondam às categorias selecionadas.

Escolha um Web Reputation no menu suspenso e defina como Risco moderado. Qualquer URL que tenha uma pontuação de reputação 60 ou inferior será bloqueada.

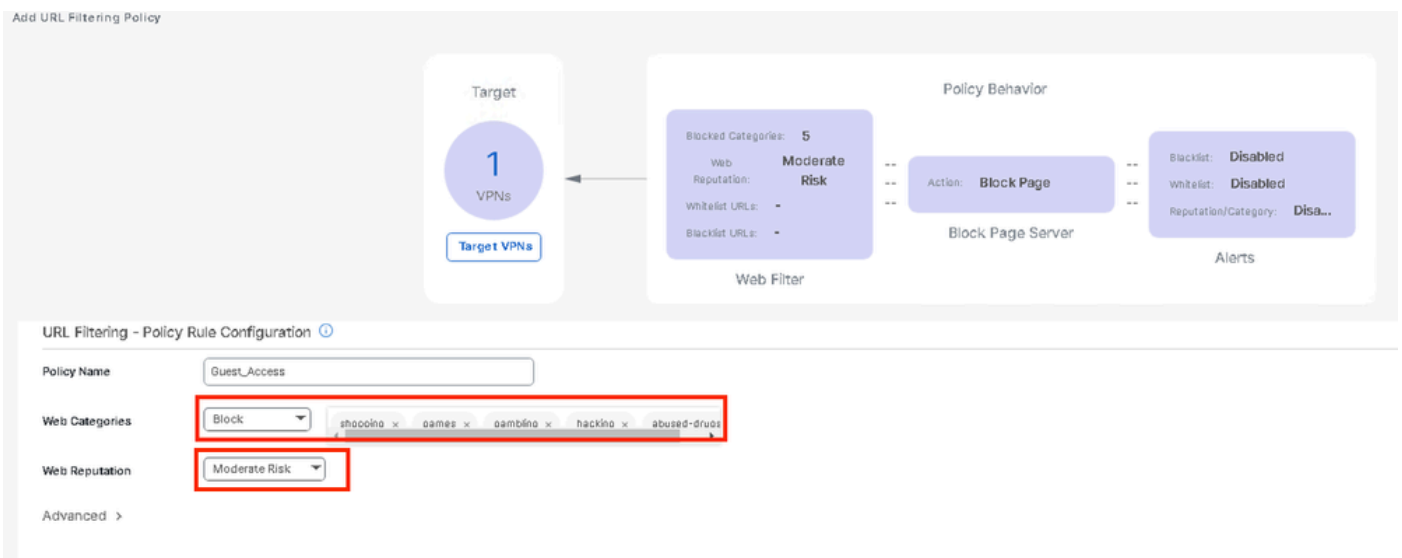
Alto risco: pontuação de reputação de 0 a 20.

Suspeito: pontuação de reputação de 0 a 40.

Risco moderado: pontuação de reputação de 0 a 60.

Risco baixo: pontuação de reputação de 0 a 80.

Confiável: pontuação de reputação de 0 a 100.



Em Advanced, escolha listas existentes ou crie uma nova lista conforme necessário no menu

suspensa Allowlist URL List ou blacklist URL List.

Advanced ▾

Whitelist URL List

Select a whitelist url list

Search

Guest_Allow

www\.google\.com
www\.yahoo\.com

Block Page Server

Block Page Content

Default Content Header

New Allow URL List

Content Body

Blacklist URL List

Select a blacklist url list

Search

Guest_Block

www\.youtube\.com
www\.facebook\.com
instagram.com

Block Page Server

Block Page Content

Default Content Header

Content Body

Redirect URL ⓘ

New Block URL List

Se necessário, altere o corpo do conteúdo em Bloquear conteúdo da página e verifique se todos os Alertas estão selecionados.

Clique em Save URL filtering Policy para adicionar uma política de filtragem de URL.

URL Filtering - Policy Rule Configuration ⓘ

Advanced ▾

Whitelist URL List

Guest_Allow ×

Blacklist URL List

Guest_Block ×

Block Page Server

Block Page Content

Default Content Header

Access to the requested page has been denied

Content Body

Please contact your Network Administrator

Redirect URL ⓘ

Enter URL

Alerts and Logs ⓘ

Alerts



Blacklist



Whitelist



Reputation/Category

Save URL Filtering Policy

Cancel

Clique em Avançar até que a página Resumo da política seja exibida.

Insira Security Policy Name (Nome da política de segurança) e Security Policy Description (Descrição da política de segurança) nos respectivos campos.

● Firewall —● Intrusion Prevention —● URL Filtering —● Advanced Malware Protection —● DNS Security —● TLS/SSL Decryption —● Policy Summary

Provide a name and description for your security master policy and configure additional security settings. Click Save Policy to save the security master policy configuration.

Security Policy Name

Security Policy Description

Additional Policy Settings

Intrusion Prevention and/or URL Filtering and/or Advanced Malware Protection

External Syslog Server

VPN ⓘ Server IP

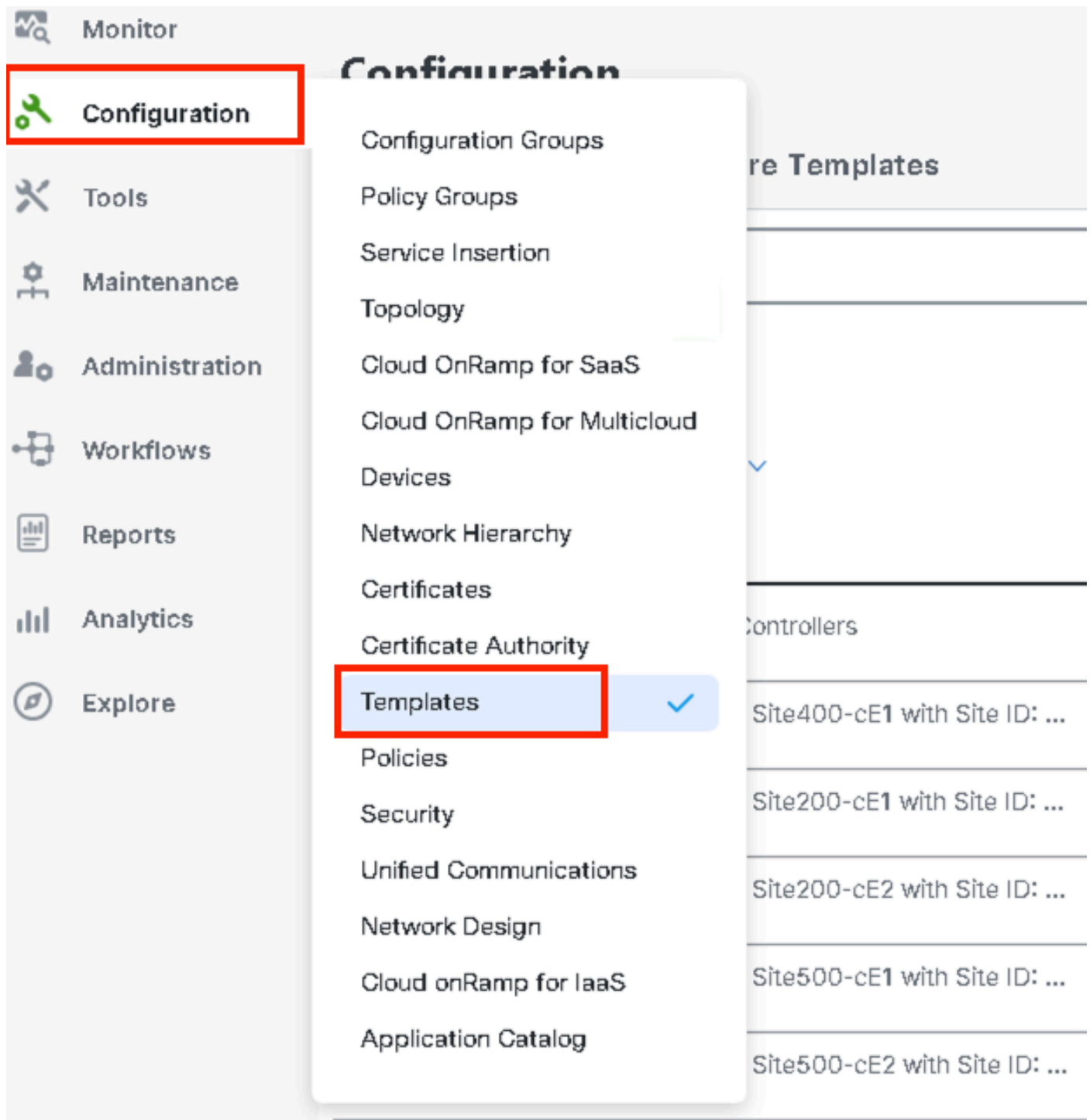
Failure Mode

Back Cancel

Aplicar uma política de segurança a um dispositivo

Para aplicar uma política de segurança a um dispositivo:

No menu do Cisco SD-WAN Manager, escolha Configuration > Templates.



Clique em Device Templates e clique em Edit em Device Template.

Configuration

Device Templates Feature Templates

Q 300 x Search

Create Template v

Template Type Non-Default v

Total Rows: 1 of 9

Name	Description	Type	Device Model ...	Device Role	Feature Templates	Draft Mode	Devices Attached	Updated By	Last Updated	common.templateStatus
fc862ea4-e57e-4618-8bc7-88d2d2978...	Device template of Site300-cE1 w...	Feature	C8000v	SDWAN Edge	25	Disabled	1	admin	24 Jul 2024 11...	In Sync

Edit
View
Delete
Copy
Enable Draft Mode
Attach Devices
Detach Devices
Export CSV
Change Device Values

Clique em Modelos Adicionais.

Configuration

Device Templates Feature Templates

Device Model* C8000v

Device Role* SDWAN Edge

Template Name* fc862ea4-e57e-4618-8bc7-88d2d2978089

Description* Device template of Site300-cE1 with Site ID: 300

Basic Information Transport & Management VPN Service VPN Cellular **Additional Templates** Switchport

- Na lista suspensa Security Policy, escolha o nome da política que você configura em Guest_URL_Policy anteriormente e clique em Update.

Policy VIP07_DPI_Visibility v

Probes Choose... v

Tenant Choose... v

Security Policy Guest_URL_Policy v

Container Profile * Factory_Default_UTD_Template v ⓘ

Switch Port + Switch Port v

Update Cancel

Clique nos dispositivos e verifique se a configuração está correta e clique em Config Diff e Side by

Side Diff. Clique em Configure Devices.

The screenshot displays the vManage configuration interface. At the top, there are buttons for 'Config Preview', 'Config Diff', 'Side by Side Diff', and 'Intent'. The 'Config Diff' button is highlighted with a red box. Below this, the 'Local Configuration vs. New Configuration' section shows a list of configuration items. The 'Configure Devices' button is also highlighted with a red box.

The configuration diff shows the following changes:

```
389 parameter-map type regex Guest_Allow-wl_
390 pattern www.google.com
391 pattern www.yahoo.com
392 |
393 parameter-map type regex Guest_Block-bl_
394 pattern instagram.com
395 pattern www.facebook.com
396 pattern www.youtube.com
397 |
444 web-filter block page profile block-Guest_Access
445 text Access to the requested page has been denied. Please contact your Network
Administrator
446 exit
447 web-filter url profile Guest_Access
448 alert blacklist categories-reputation whitelist
449 blacklist
450 parameter-map regex Guest_Block-bl_
451 exit
452 categories block
453 abused-drugs
454 gambling
455 games
456 hacking
457 shopping
458 exit
459 block page-profile block-Guest_Access
460 log level error
461 reputation
462 block-threshold moderate-risk
463 exit
464 whitelist
465 parameter-map regex Guest_Allow-wl_
466 exit
467 exit
468 utd global
469 exit
470 policy utd-policy-vrf-12
471 all-interfaces
472 vrf 12
473 web-filter url profile Guest_Access
474 exit
```

O vManage configurou com êxito o modelo de dispositivo com a política de segurança e instalou o pacote UTD no dispositivo Edge.

Push Feature Template Configuration | ● Validation success

Total Task: 1 | Success : 1

Device Group (1)

Q Search Table

Status	Message	Chassis Number
● Success	Template successfully atta...	C8K-C16B1FE2-C89F-A311-DEA7-46...

View Logs

Host: Site300-cE1(11.30.1)
 Site ID: 300
 Device: C8000v
 Model:

[26-Jul-2024 13:55:55 PDT] Configuring device with feature template: fc862ee4-e57e-4616-8bc7-88d2d2978089
 [26-Jul-2024 13:55:56 PDT] Checking and creating device in Manager
 [26-Jul-2024 13:55:57 PDT] Generating configuration from template
 [26-Jul-2024 13:56:06 PDT] Device is online
 [26-Jul-2024 13:56:06 PDT] Updating device configuration in Manager
 [26-Jul-2024 13:56:06 PDT] Sending configuration to device
 [26-Jul-2024 13:56:12 PDT] Successfully notified device to pull configuration
 [26-Jul-2024 13:56:14 PDT] Device has pulled the configuration
 [26-Jul-2024 13:56:21 PDT] Device: Configured IOX
 [26-Jul-2024 13:56:35 PDT] Device: Started IOX
 [26-Jul-2024 13:56:58 PDT] Device: Successfully downloaded package for appid utd
 [26-Jul-2024 13:57:40 PDT] Device: Successfully installed appid utd
 [26-Jul-2024 13:59:07 PDT] Device: Verified appid utd in running state
 [26-Jul-2024 13:59:07 PDT] Device: Successfully verified appids: utd
 [26-Jul-2024 13:59:08 PDT] Device: Config applied successfully
 [26-Jul-2024 13:59:08 PDT] Template successfully attached to device

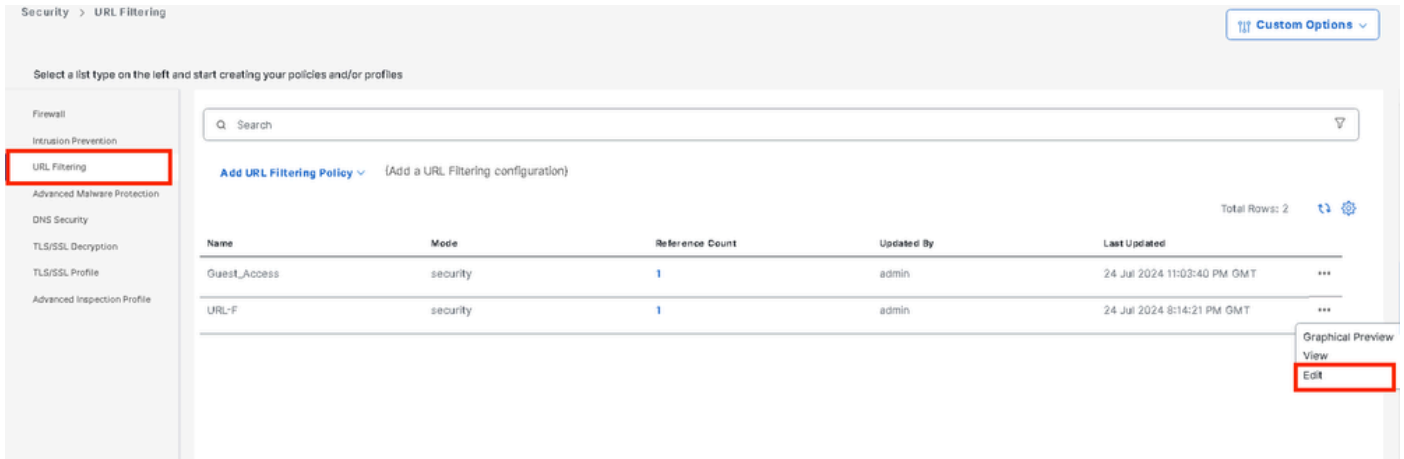
Modificar filtragem de URL

Para modificar uma política de filtragem de URL, siga estas etapas:

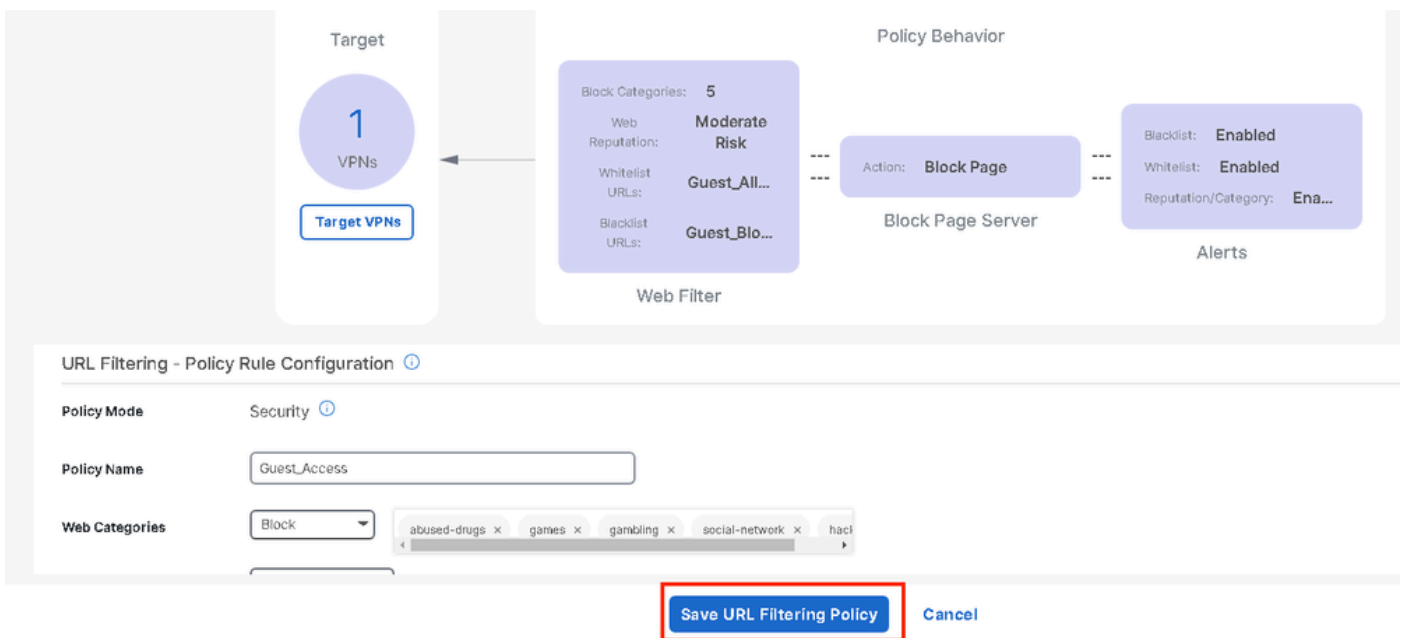
1. No menu Cisco SD-WAN Manager, escolha Configuration > Security.
2. Na tela Security, clique no menu suspenso Custom Options , selecione Policies/Profiles.

The screenshot shows the Cisco SD-WAN Manager interface. On the left, there is a navigation menu with options: Monitor, Configuration, Tools, Maintenance, Administration, Workflows, Reports, and Analytics. The main content area is titled 'Security' and contains a search bar and two buttons: 'Add Security Policy' and 'Add Unified Security Policy'. Below these is a table with columns: Name, Description, Use Case, Policy Mode, Devices Attached, DeviceTemplates/ConfigGroups, Updated By, and Last Updated. The table contains one row: 'VIP22-Security-Policy' with description 'ZBFW policy for DIA', use case 'Custom', policy mode 'security', 0 devices attached, 0 templates, updated by 'adminh', and last updated '12 Apr 2024 8:32:39 PM'. On the right side, a dropdown menu is open, showing options: Security, Lists, Policies/Profiles (highlighted with a red box), Umbrella Registration, and Threat Grid API Key.

Clique em Filtragem de URL na guia esquerda, para a política desejada que você deseja modificar, clique em 3 pontos (...)e escolha Editar.



Modifique a política conforme necessário e clique em Save URL Filtering Policy.



Excluir filtragem de URL

Para excluir uma política de filtragem de URL, primeiro desanexe a política da política de segurança:

No menu do Cisco SD-WAN Manager, escolha Configuration > Security.

Para desanexar a política de filtragem de URL da política de segurança:

- Para a política de segurança que contém a política de filtragem de URL, clique em 3 pontos (...) e em Editar.

Name	Description	Use Case	Policy Mode	Devices Attached	DeviceTemplates/ConfigGroups	Updated By	Last Updated
VIP22-Security-Policy	ZBFW policy for DIA	Custom	security	0	0	admin	12 Apr 2024 9:32:39 PM
Security-IPS-URLF-AMP	IPS, URL-F, AMP	Custom	security	0	0	admin	24 Jul 2024 8:49:01 PM
Guest_URL_Policy	Guest_URL_Policy	Custom	security	1	1	admin	24 Jul 2024 11:03:25 PM

- View
- Preview
- Edit**
- Delete

A página Resumo da política é exibida. Clique na guia Filtragem de URL.

Para a diretiva que você deseja excluir, clique em 3 pontos (...) e escolha Desanexar.

Clique em Save Policy Changes (Salvar alterações de política).

[Firewall](#) |
 [Intrusion Prevention](#) |
 [URL Filtering](#) |
 [Advanced Malware Protection](#) |
 [DNS Security](#) |
 [TLS/SSL Decryption](#) |
 [Policy Summary](#)

Q Search

Name	Type	Reference Count	Updated By	Last Updated
Guest_Access	urlFiltering	1	admin	24 Jul 2024 11:03:40 PM GMT

- Graphical Preview
- View
- Edit
- Detach**

[Preview](#) |
 [Save Policy Changes](#) |
 [Cancel](#)

Para excluir a política de filtragem de URL:

Na tela Security, clique no menu suspenso Custom Options , selecione Policies/Profiles e escolha URL Filtering.

The network is out of compliance due to licensing, please [click here](#) for more actions.

- Monitor
- Configuration
- Tools
- Maintenance
- Administration
- Workflows
- Reports
- Analytics
- Explore

[Add Security Policy](#) |
 [Add Unified Security Policy](#)

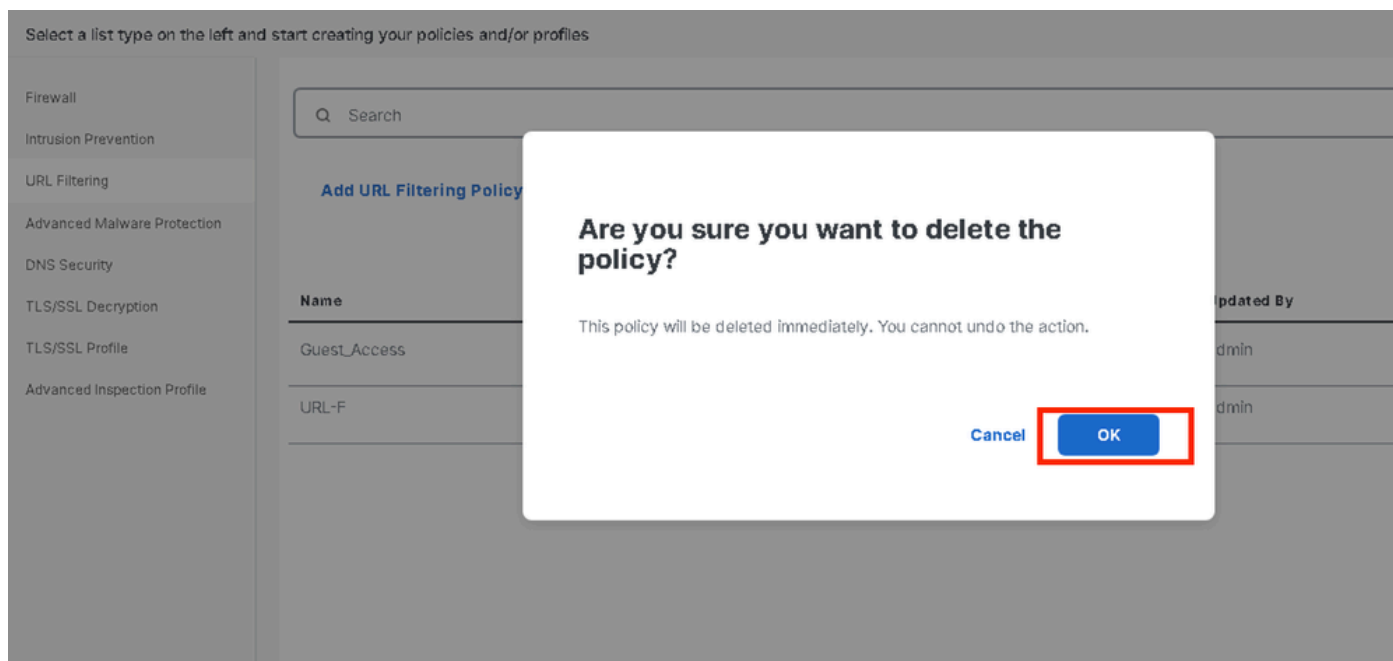
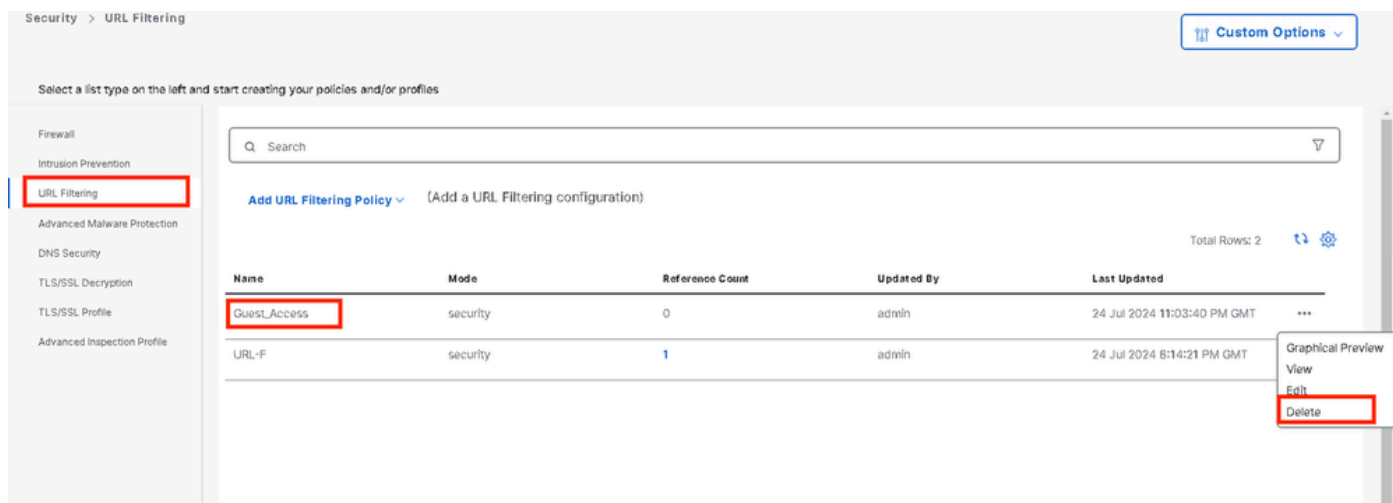
Total Rows: 3

Name	Description	Use Case	Policy Mode	Devices Attached	DeviceTemplates/ConfigGroups	Updated By	Last Updated
VIP22-Security-Policy	ZBFW policy for DIA	Custom	security	0	0	admin	12 Apr 2024 9:32:39
Security-IPS-URLF-A...	IPS, URL-F, AMP	Custom	security	0	0	admin	24 Jul 2024 8:49:01
GuestURL_Policy	GuestURL_Policy	Custom	security	1	1	admin	25 Jul 2024 4:23:52

- Security
- Lists
- Policies/Profiles**
- Umbrella Registration
- Threat Grid API Key

Para a diretiva que deseja excluir, clique em 3 pontos (...) e em Excluir.

Clique em OK.



Verificar

Verifique se a versão do Cisco UTD está instalada.

<#root>

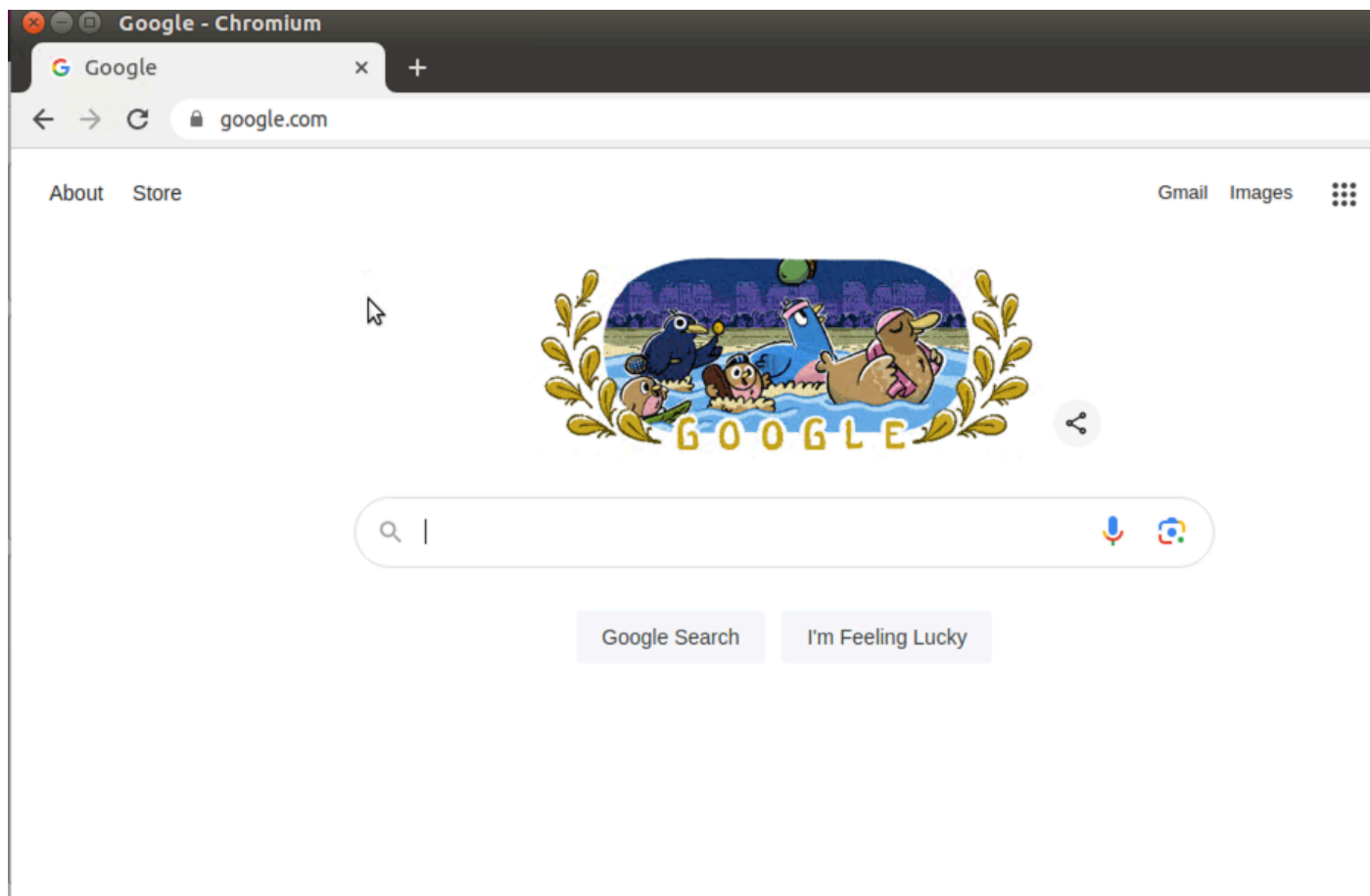
```
Site300-cE1#show utd engine standard version
UTD Virtual-service Name: utd
IOS-XE Recommended UTD Version: 1.0.2_SV3.1.67.0_XE17.14
```

IOS-XE Supported UTD Regex: ^1\.0\.[0-9]+_SV(.*)_XE17.14\$

UTD Installed Version:

1.0.2_SV3.1.67.0_XE17.14

No PC cliente localizado na VPN de convidado, se você tentar abrir google.com e yahoo.com, eles serão permitidos.



<#root>

Site300-cE1#show utd engine standard logging events | in google

2024/07/24-13:22:38.900508 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Pass

[**]

UTD WebFilter Allowlist

[**] [

URL: www.google.com

] [VRF: 12] {TCP} 10.32.1.10:55310 -> 142.250.189.196:443

2024/07/24-13:24:03.429964 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Pass

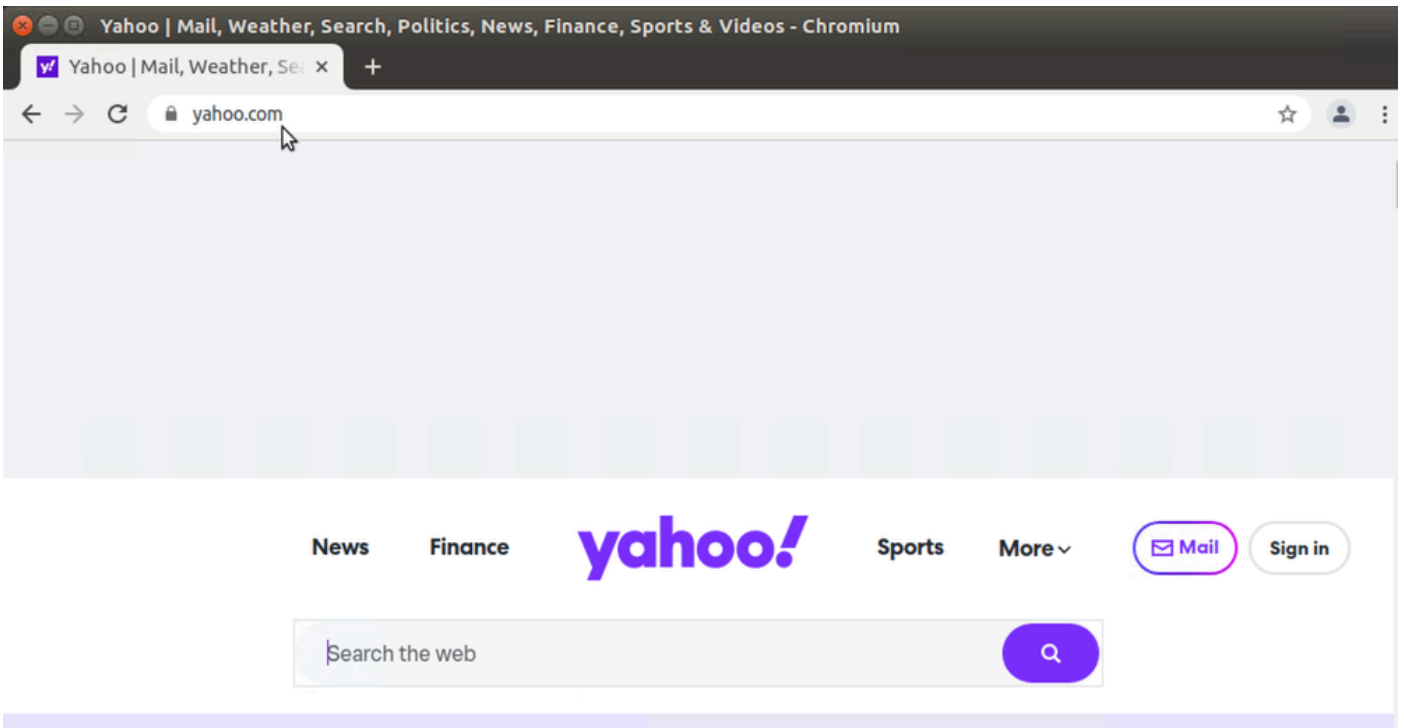
[**]

UTD WebFilter Allowlist

[**] [

URL: www.google.com

] [VRF: 12] {TCP} 10.32.1.10:55350 -> 142.250.189.196:443



<#root>

Site300-cE1#show utd engine standard logging events | in yahoo

2024/07/24-13:20:45.238251 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Pass [

**]

UTD WebFilter Allowlist

[**] [

URL: www.yahoo.com

] [VRF: 12] {TCP} 10.32.1.10:48714 -> 69.147.88.8:443

2024/07/24-13:20:45.245446 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Pass

[**]

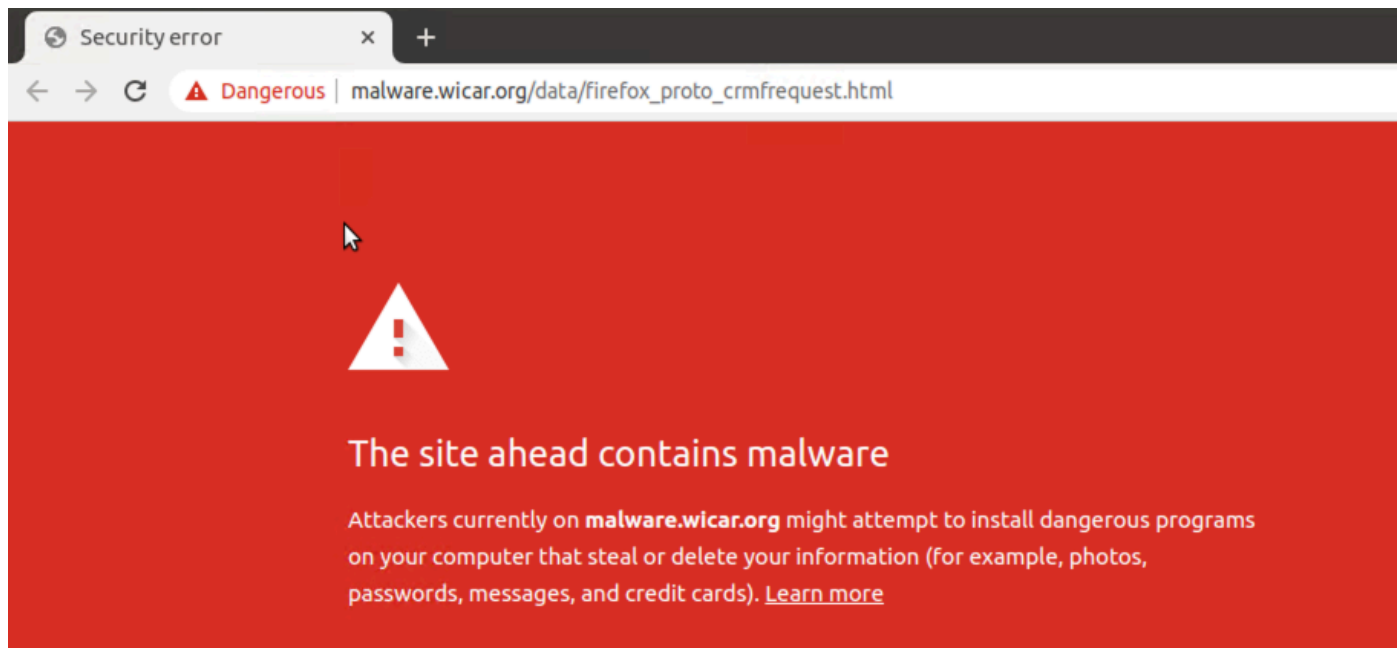
UTD WebFilter Allowlist

[**] [

URL: www.yahoo.com

] [VRF: 12] {TCP} 10.32.1.10:48716 -> 69.147.88.8:443

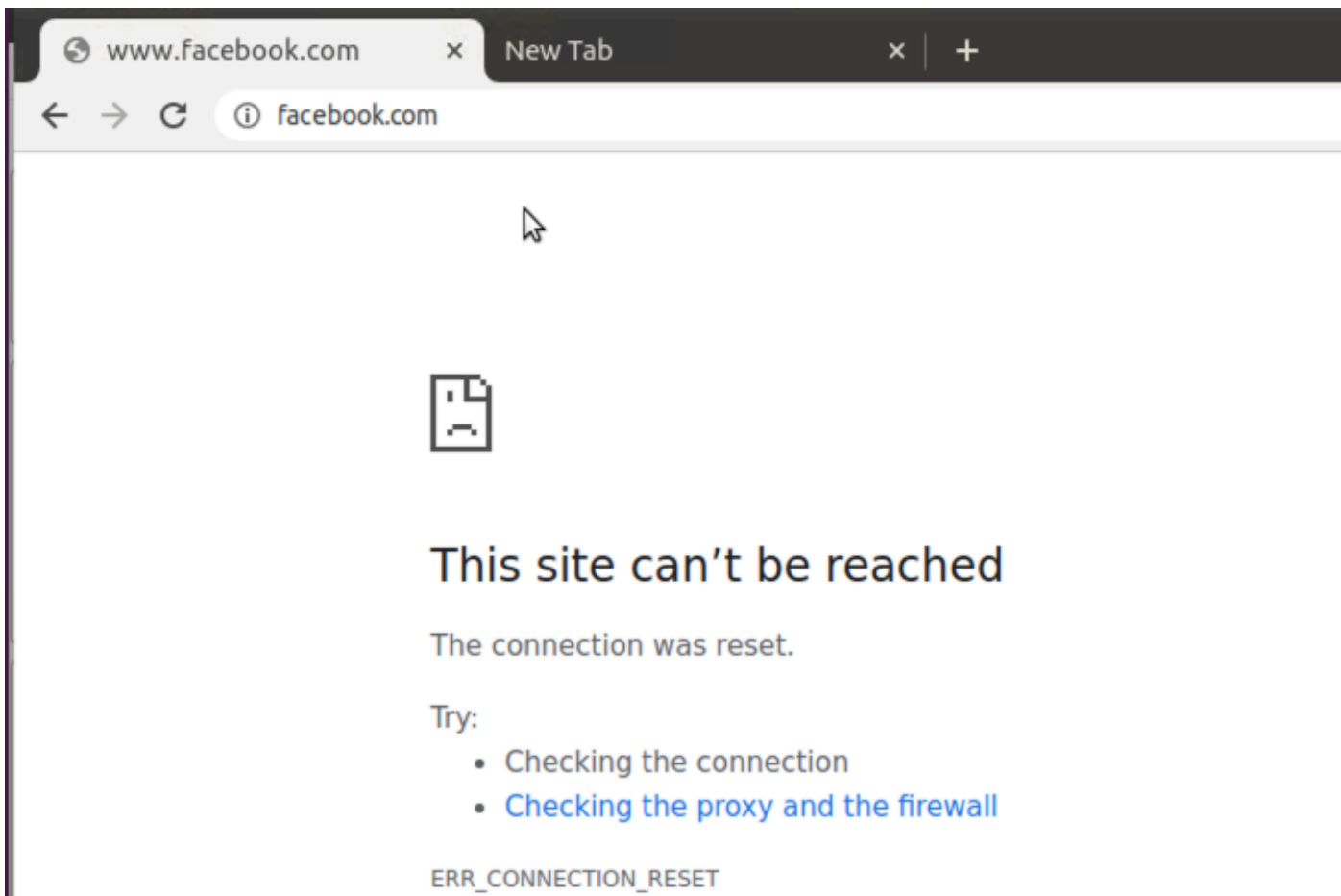
No PC cliente localizado na VPN de convidado, se você tentar abrir páginas da Web com baixa pontuação de reputação ou em uma das categorias da Web bloqueadas, o mecanismo de filtragem de URL negará a solicitação HTTPs.



<#root>

```
Site300-cE1#show utd engine standard logging events | in ma  
2024/07/24-13:32:18.475318 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID  
Drop  
[**]  
UTD WebFilter Category/Reputation  
[**] [  
URL: malware.wicar.org/data/firefox_proto_crmfrequest.html  
] ** [Category: Malware Sites] ** [Reputation: 10] [VRF: 12] {TCP} 10.32.1.10:40154 -> 208.94.116.246:8
```

No PC cliente localizado na VPN de convidado, se você tentar abrir o facebook, o instagram e o youtube serão bloqueados.



<#root>

Site300-cE1#show utd engine standard logging events | in face

2024/07/24-13:05:25.622746 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Drop

[**]

UTD WebFilter blacklist

[**] [

URL: www.facebook.com

] [VRF: 12] {TCP} 10.32.1.10:55872 -> 157.240.22.35:443

2024/07/24-13:05:25.638612 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Drop

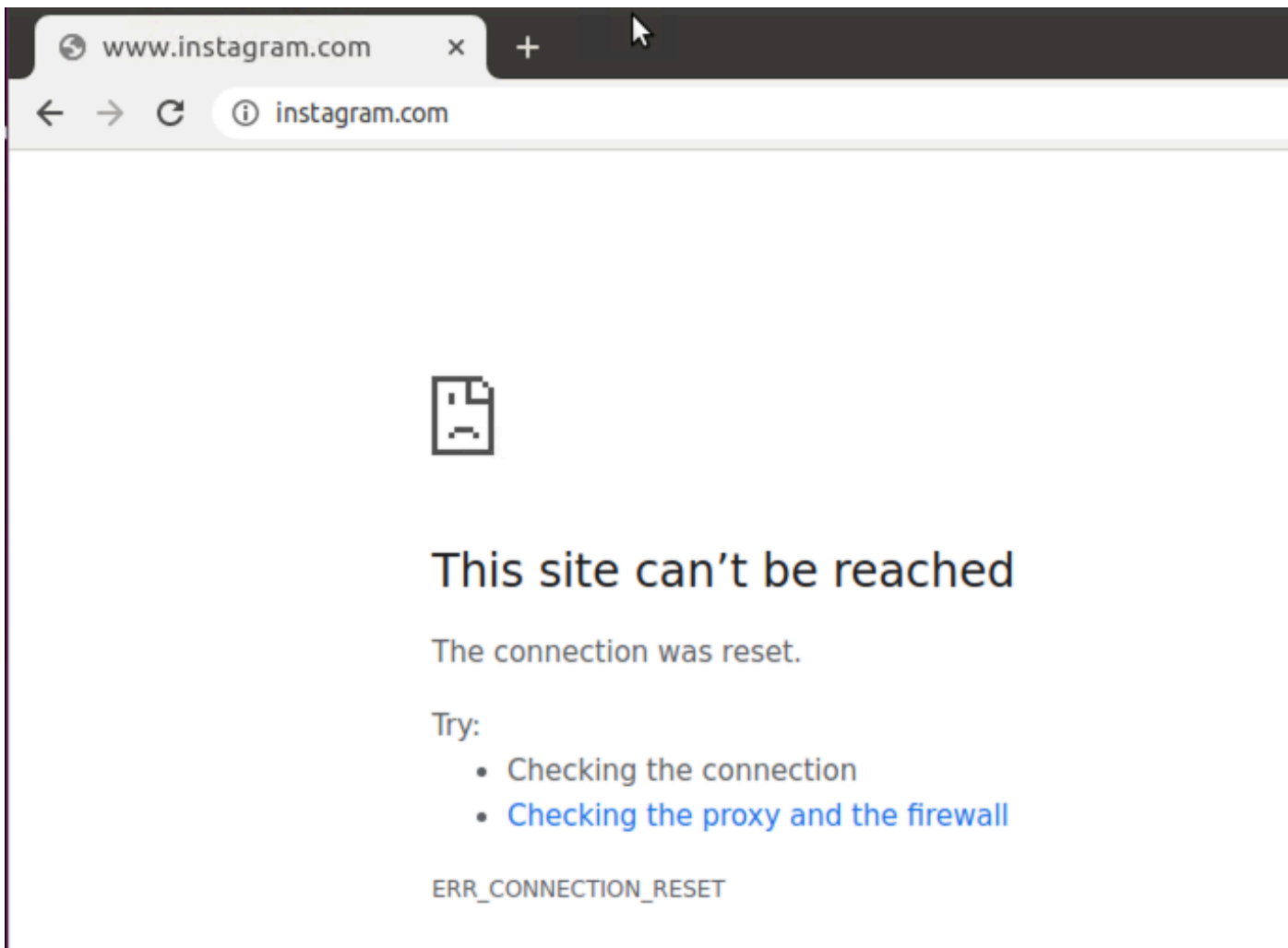
[**]

UTD WebFilter blacklist

[**] [

URL: www.facebook.com

] [VRF: 12] {TCP} 10.32.1.10:55876 -> 157.240.22.35:443



<#root>

```
Site300-cE1#show utd engine standard logging events | in insta
2024/07/24-13:09:07.027559 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
Drop
[**]
UTD WebFilter blacklist
[**] [
URL: www.instagram.com
] [VRF: 12] {TCP} 10.32.1.10:58496 -> 157.240.22.174:443
2024/07/24-13:09:07.030067 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
Drop
[**]
UTD WebFilter blacklist
[**] [
URL: www.instagram.com
] [VRF: 12] {TCP} 10.32.1.10:58498 -> 157.240.22.174:443
2024/07/24-13:09:07.037384 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
```

Drop

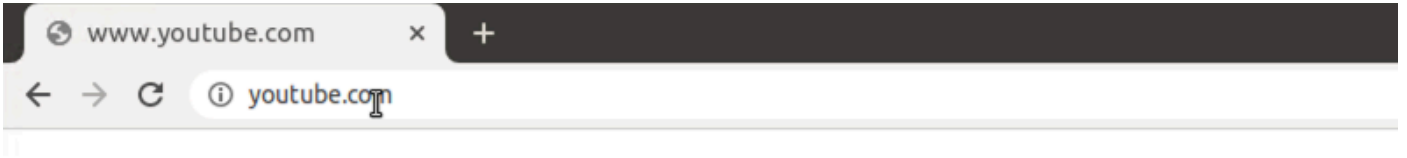
[**]

UTD WebFilter blocklist

[**] [

URL: www.instagram.com

] [VRF: 12] {TCP} 10.32.1.10:58500 -> 157.240.22.174:443



This site can't be reached

The connection was reset.

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)

ERR_CONNECTION_RESET

<#root>

Site300-cE1#show utd engine standard logging events | in youtube

2024/07/24-13:10:01.712501 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Drop

[**]

UTD WebFilter blocklist

[**] [

URL: www.youtube.com

] [VRF: 12] {TCP} 10.32.1.10:54292 -> 142.250.72.206:443

2024/07/24-13:10:01.790521 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Drop

[**]

UTD WebFilter blocklist

[**] [

URL: www.youtube.com

] [VRF: 10] {TCP} 10.30.1.10:37988 -> 142.250.72.206:443

2024/07/24-13:11:11.400417 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Drop

[**]

UTD WebFilter blocklist

[**] [

URL: www.youtube.com

] [VRF: 12] {TCP} 10.32.1.10:54352 -> 142.250.72.206:443

Monitore a filtragem de URL a partir da GUI do vManage

Você pode monitorar a filtragem de URL em tempo real ou historicamente para cada dispositivo por categorias da Web usando essas etapas.

Para monitorar os URLs que estão bloqueados ou permitidos em um dispositivo Cisco IOS XE Catalyst SD-WAN:

1. No menu Cisco SD-WAN Manager, escolha Monitor > Dispositivos > Selecionar dispositivo

The screenshot shows a network management interface. On the left, a sidebar menu is visible with the following items: Monitor (highlighted with a red box), Configuration, Tools, Maintenance, Administration, Workflows, Reports, Analytics, and Explore. A dropdown menu is open under 'Monitor', listing: Overview, Devices (highlighted with a red box and a blue checkmark), Tunnels, Applications, Security, VPN, Logs, Multicloud, SD-AVC Cloud Connector, and Compliance. The main content area shows a table with the following columns: Hostname, Device Model, Site Name, System IP, and Health. The table contains three rows of data:

Hostname	Device Model	Site Name	System IP	Health
vManage	Manager	SITE_1	1.1.1.1	✓
vBond	Validator	SITE_1	1.1.1.2	✓
vSmart-1	Controller	SITE_1	1.1.1.3	✓

2. No painel esquerdo, em Monitoramento de segurança, clique em Filtragem de URL. As informações de filtragem de URL são exibidas no painel direito.

- Clique em Bloqueado. A contagem de sessões em uma URL bloqueada é exibida.
- Clique em Allowed. A contagem de sessão em URLs permitidas é exibida.

Observação: a versão instalada do UTD não pode estar no estado NÃO SUPORTADO.

Verifique se o UTD está no estado em execução.

```
Site300-cE1#show app-hosting list
App id                               State
-----
utd                                   RUNNING
```

O status de integridade de Validar UTD está em VERDE.

<#root>

```
Site300-cE1#show utd engine standard status
Engine version      : 1.0.2_SV3.1.67.0_XE17.14
Profile             : Cloud-Low
```

System memory :
Usage : 11.70 %
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: 29.0.c
Last update status: None
Last successful update time: None
Last failed update time: None
Last failed update reason: None
Next update scheduled at: None
Current status: Idle

Verifique se o recurso Filtragem de URLs está habilitado.

<#root>

Site300-cE1#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
Unified Policy mode: disabled
SN threads: 12

CFT inst_id 0 feat id 4 fo id 4 chunk id 19

Max flows: 165000
SN Health: channel: Threat Defense : Green
SN Health: channel: Service : Down

Flow-logging Information:

State : disabled

Context Id: 3, Name: 3 : 12

Ctx Flags: (0xc50001)
Engine: Standard
State : Enabled
SN Redirect Mode : Fail-open, Divert
Threat-inspection: Not Enabled

Domain Filtering : Not Enabled

URL Filtering : Enabled

File Inspection : Not Enabled

All Interfaces : Enabled

Para exibir os logs de filtragem de URL, execute o comando `show utd engine standard logging events url-filtering`.

```
Site300-cE1#show utd engine standard logging events url-filtering
```

```
2024/07/24-20:36:58.833237 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID  
2024/07/24-20:37:59.000400 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID  
2024/07/24-20:37:59.030787 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID  
2024/07/24-20:38:59.311304 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID  
2024/07/24-20:38:59.343273 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
```

Observação: execute o comando `clear utd engine standard logging events` para limpar eventos antigos.

Verificar pacotes de entrada/saída no contêiner UTD, atraso na pesquisa.

```
Site300-cE1#show utd engine standard statistics url-filtering vrf name 12 internal
```

UTM Preprocessor URLF Statistics

```
-----  
URL Filter Requests Sent:          50  
URL Filter Response Received:      50  
blocklist Hit Count:               27  
Allowlist Hit Count:               0  
Reputation Lookup Count:           50  
Reputation Action Block:           0  
Reputation Action Pass:            50  
Reputation Action Default Pass:    0  
Reputation Action Default Block:   0  
Reputation Score None:             0
```

Reputation Score Out of Range:	0
Category Lookup Count:	50
Category Action Block:	15
Category Action Pass:	35
Category Action Default Pass:	0
Category Action Default Block:	0
Category None:	0
Category Out of Range:	0

UTM Preprocessor URLF Internal Statistics

```
-----
Total Packets Received:          1335
SSL Packet Count:                56
HTTP Header Count:              22
Action Drop Flow:                69
Action Reset Session:           0
Action Block:                    42
Action Pass:                     503
Action Offload Session:         0
Invalid Action:                  0
No UTM Tenant Persona:          0
No UTM Tenant Config:           0
URL Lookup Response Late:       150
URL Lookup Response Very Late:  21
URL Lookup Response Extremely Late: 0
URL Lookup Response Status Invalid: 0
Response Does Not Match Session: 0
No Response When Freeing Session: 0
First Packet Not From Initiator: 0
No HTTP Header:                 0
Invalid Action:                  0
Send Error Fail Open Count:     0
Send Error Fail Close Count:    0
Lookup Error Fail Open Count:   0
Lookup Error Fail Close Count:  0
Lookup Timeout Fail Open Count: 0
Lookup Timeout Fail Close Count: 0
```

Informações Relacionadas

- [Guia de configuração de segurança do Cisco Catalyst SD-WAN](#)
- [Instalar Imagem Virtual de Segurança UTD em Roteadores cEdge](#)
- [Identificar e Solucionar Problemas de Tratamento de Datapath por UTD e Filtragem de URL](#)

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.