配置和验证URL过滤

目录

简介

本文档介绍如何使用Cisco Catalyst Manager GUI在Cisco IOS-XE®路由器上配置和验证URL过滤。

先决条件

在vManage中上传与当前思科IOS-XE代码兼容的UTD软件虚拟映像。有关在cEdge路由器上安装UTD安全虚拟映像的说明，请查看相关信息部分。

云翼路由器必须处于vManaged模式，并且必须预先附加模板。

要求

Cisco 建议您了解以下主题：

- Cisco SD-WAN Overlay将启动初始配置。
- URL过滤配置Cisco Catalyst Manager GUI。

使用的组件

本文档基于以下软件和硬件版本：

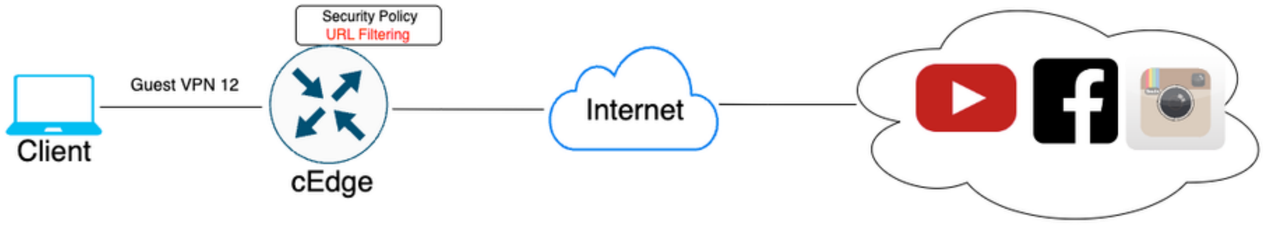
- Cisco Catalyst SD-WAN Manager版本20.14.1。

- 思科Catalyst SD-WAN控制器版本20.14.1。
- Cisco Edge路由器17.14.1版。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图



配置URL过滤策略的组件

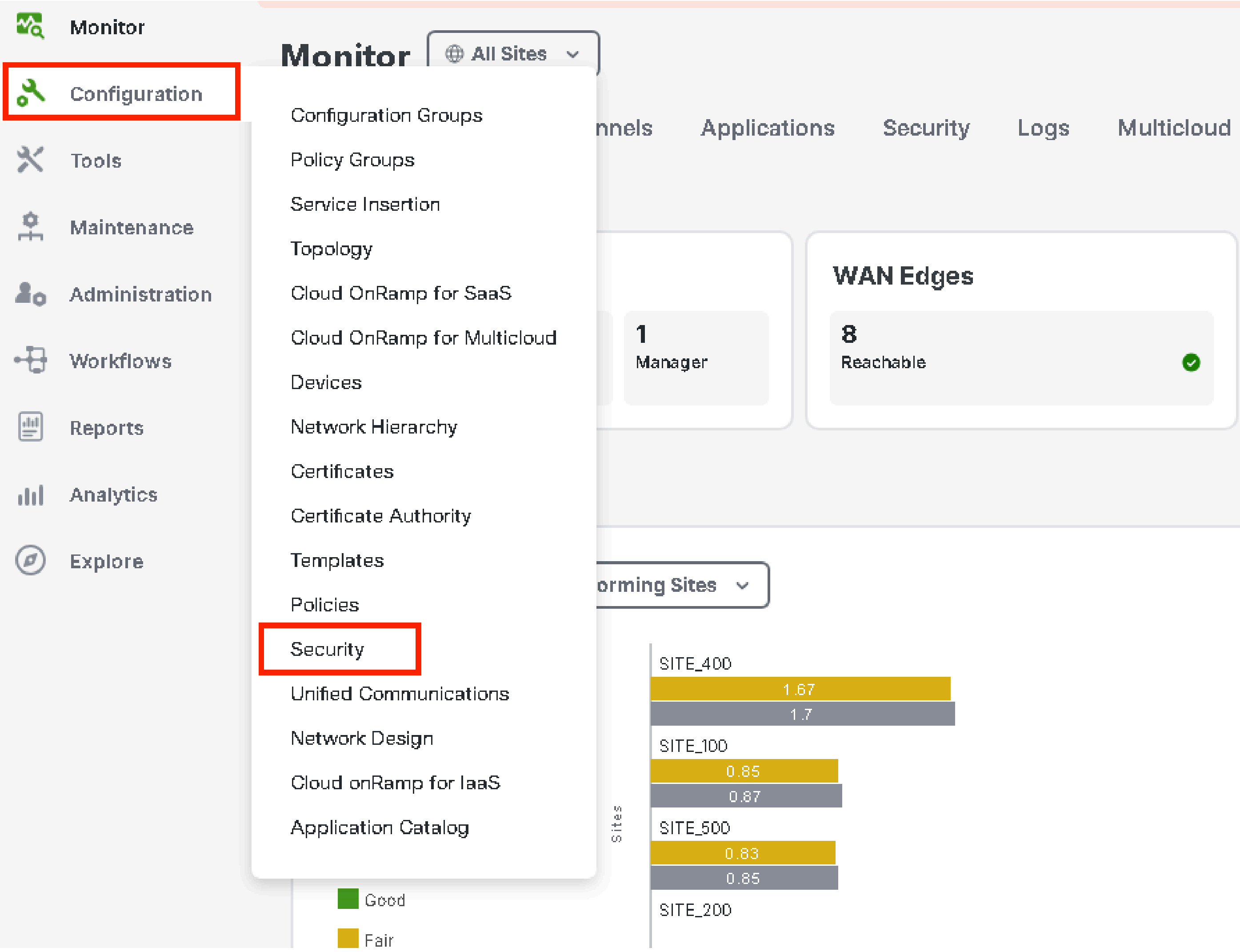
本文解释如何根据类别、信誉或域阻止/允许列表将URL过滤配置为阻止/允许特定客户端HTTPS流量，并提供以下示例要求：

- 阻止来自访客VPN Web类别上的客户端的此HTTPS请求：
  - 游戏
  - 赌博
  - 黑客攻击
  - 非法毒品
- 必须阻止Web信誉小于或等于60的访客VPN上的客户端向网站发出的任何HTTPS URL请求。
- 访客VPN上的客户端向网站发出的HTTP(s)请求阻止了Facebook、Instagram和YouTube，同时允许访问google.com和yahoo.com。

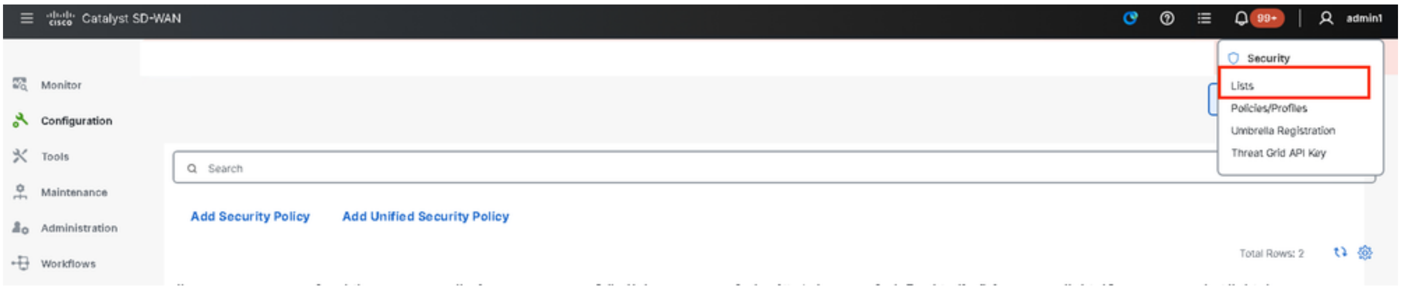
要配置URL过滤：

创建感兴趣的URL列表

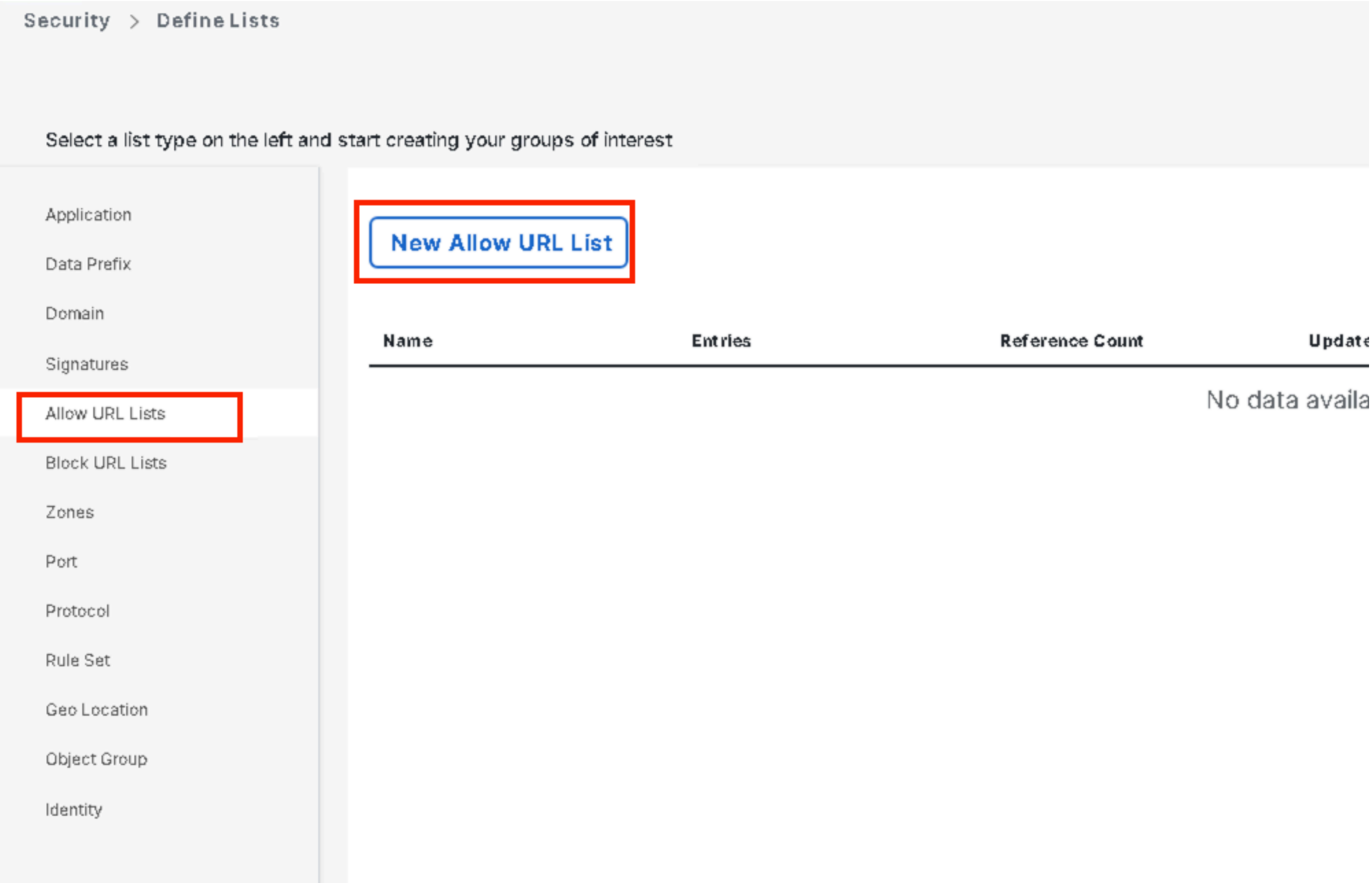
1. 在Cisco SD-WAN Manager菜单上，导航到左侧面板中的Configuration > Security选项卡。



要创建或管理Allowlist URL List或Blocklist URL List，请从页面右上方的Custom Options下拉菜单中选择Lists。



在左侧窗格中单击Allow URLs Lists，然后创建New Allow URLs List。

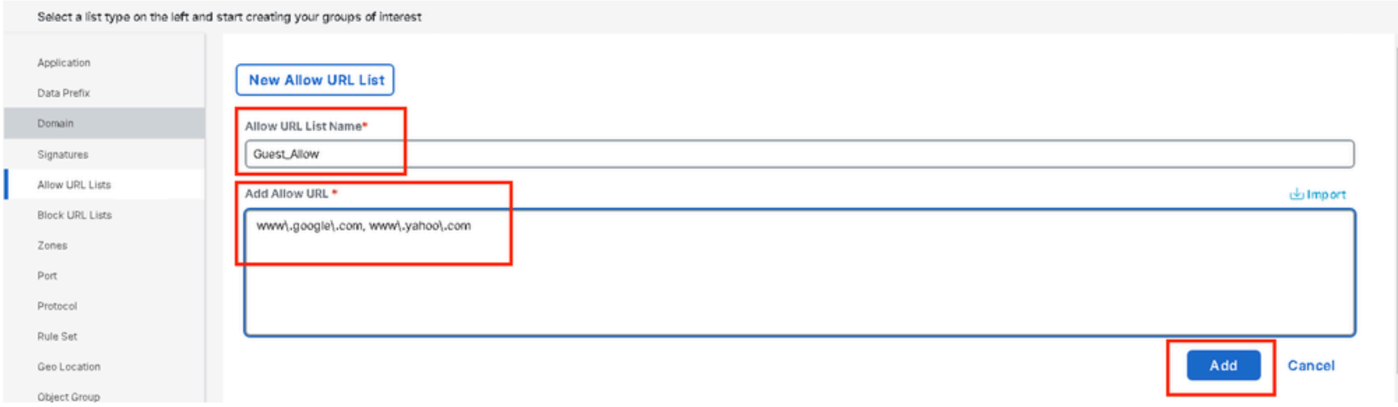


Select a list type on the left and start creating your groups of interest

Name	Entries	Reference Count	Update

No data availa

- 在URL List Name字段中，输入最多包含32个字符（仅包括字母、数字、连字符和下划线）的列表名称。
- 在URL字段中，输入要包括在列表中的URL，以逗号分隔。您还可以使用导入按钮从可访问的存储位置添加列表。
- 完成后，单击Add。



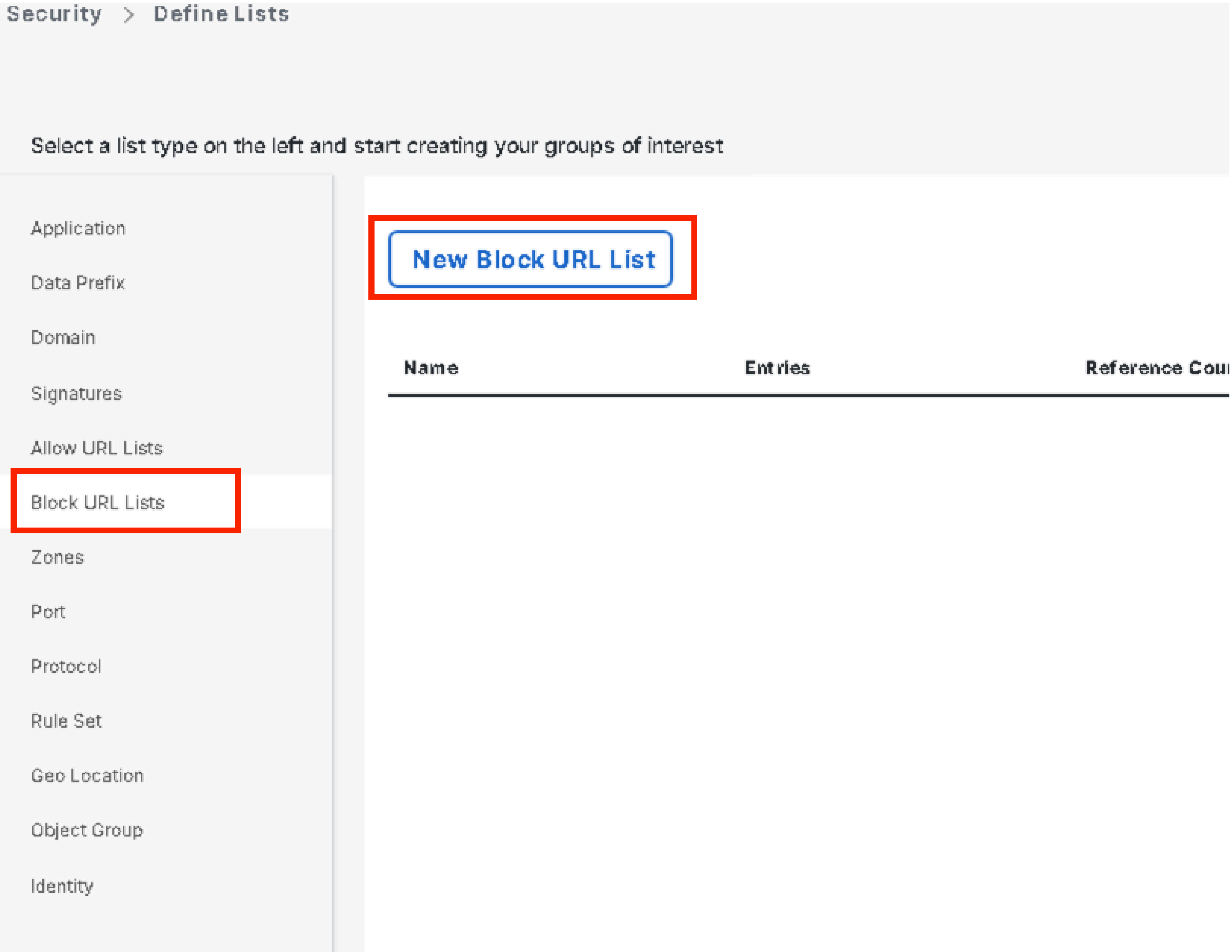
Select a list type on the left and start creating your groups of interest

Allow URL List Name*
Guest_Allow

Add Allow URL *
www\.google\.com, www\.yahoo\.com

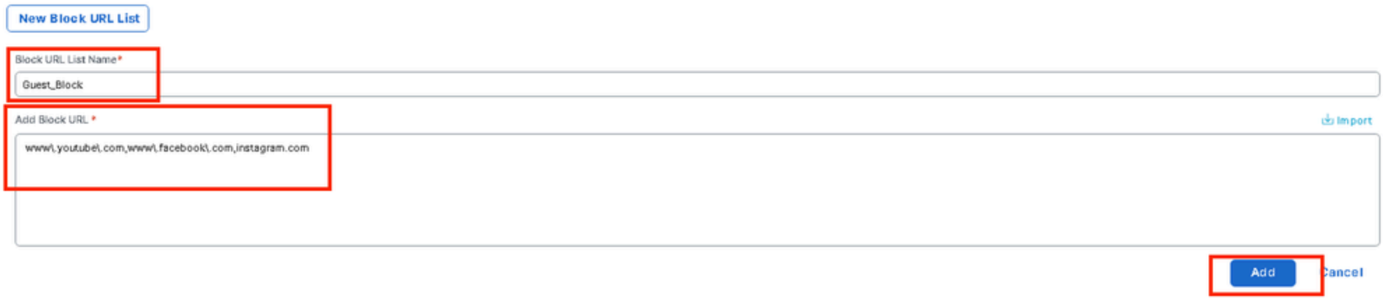
注意：可以考虑对允许和阻止列表中的域名使用正则表达式模式

在左侧窗格中单击Block URLs Lists，然后创建New Block URLs List。


Security > Define Lists

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

- 在URL List Name字段中，输入最多包含32个字符（仅字母、数字、连字符和下划线）的列表名称
- 在URL字段中，输入要包括在列表中的URL，以逗号分隔。您还可以使用导入按钮从可访问的存储位置添加列表。
- 完成后，单击Add。

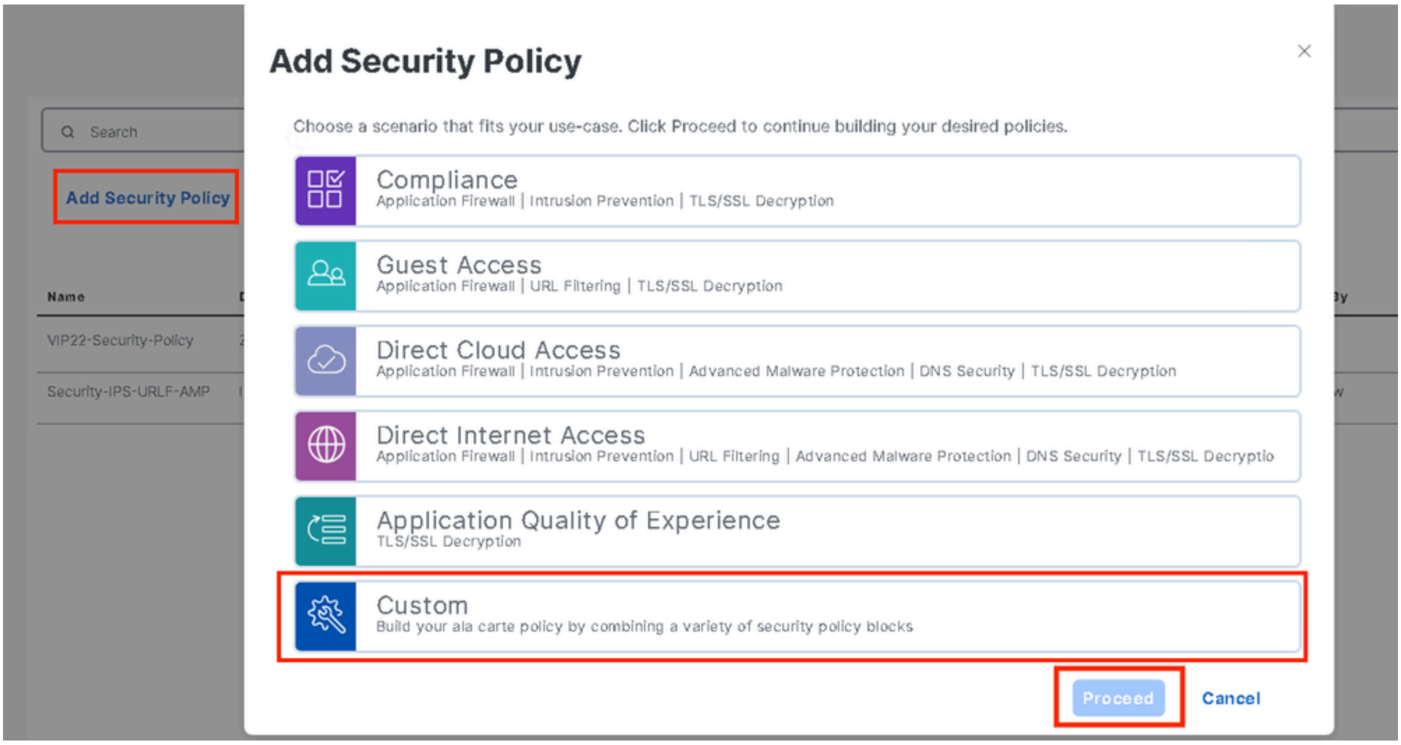

New Block URL List

Block URL List Name*: Guest_Block

Add Block URL *: www\.youtube\.com,www\.facebook\.com,instagram.com

创建安全策略

2. 在Cisco SD-WAN Manager菜单上，导航到配置>安全，然后单击添加新安全策略。系统将打开“添加安全策略”(Add Security Policy)向导，并显示各种使用案例场景或使用列表中的现有策略。选择custom，然后单击Proceed在向导中添加URL过滤策略。



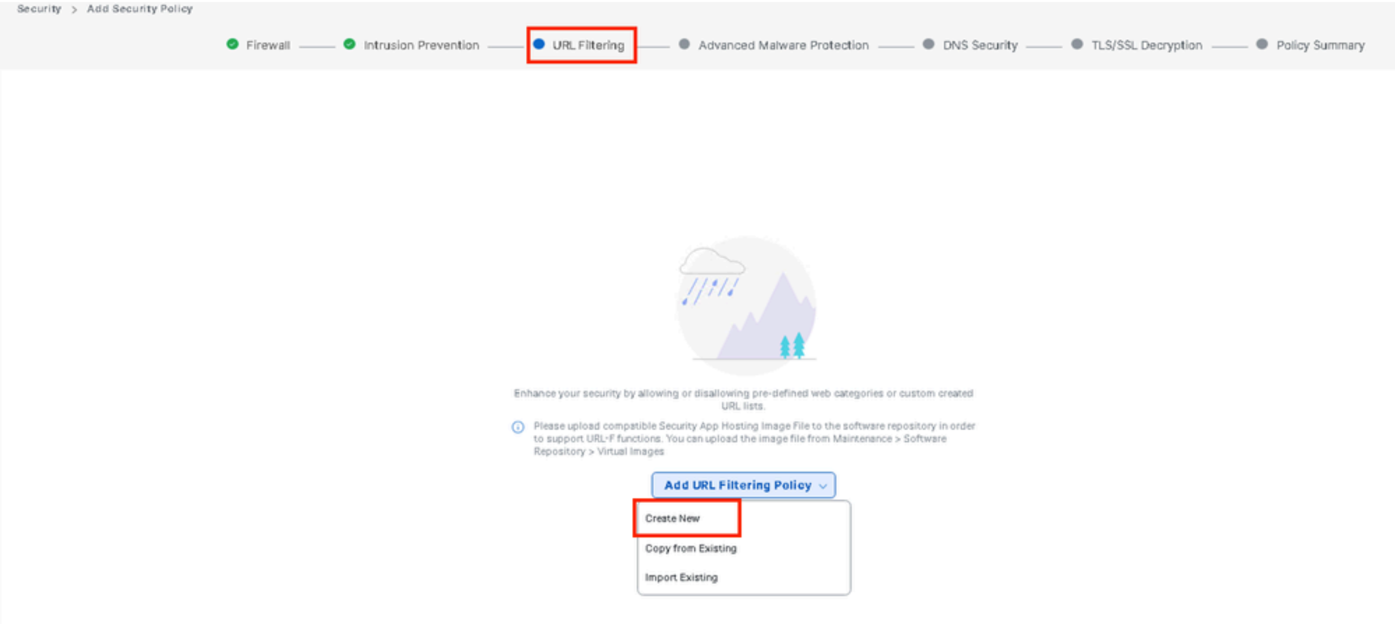
Add Security Policy

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 Decryptio
- Application Quality of Experience
  TLS/SSL Decryption
- Custom
  Build your ala carte policy by combining a variety of security policy blocks

注意：在“添加安全策略”(Add Security Policy)中，选择支持URL过滤的方案（访客访问、直接互联网访问或自定义）。

在添加安全策略向导中，单击Next，直到显示URL Filtering窗口。 现在请转到URL Filtering > Add URL Filtering Policy > Create New以创建URL过滤策略。单击“下一步”

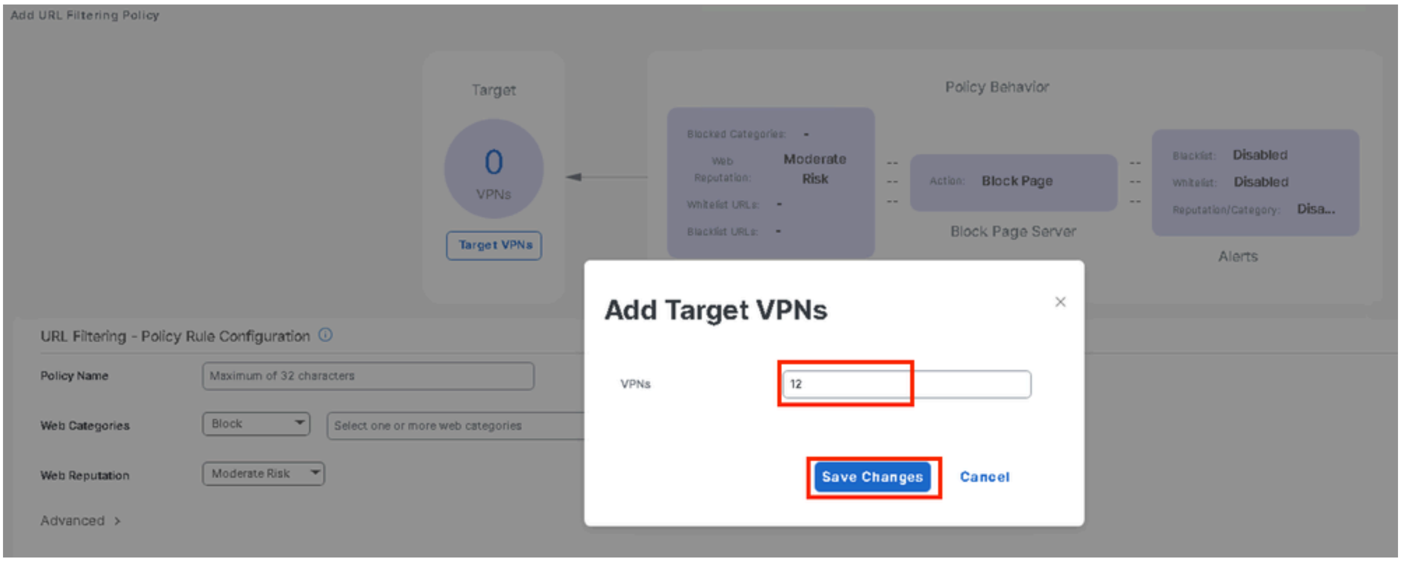


Security > Add Security Policy

Enhance your security by allowing or disallowing pre-defined web categories or custom created URL lists.

Please upload compatible Security App Hosting Image File to the software repository in order to support URL-F functions. You can upload the image file from Maintenance > Software Repository > Virtual Images

单击Target VPNs可在“Add Target VPNs”向导中添加所需的VPN数量。



Add URL Filtering Policy

URL Filtering - Policy Rule Configuration

Policy Name: Maximum of 32 characters

Web Categories: Block | Select one or more web categories

Web Reputation: Moderate Risk

Advanced >

Add Target VPNs

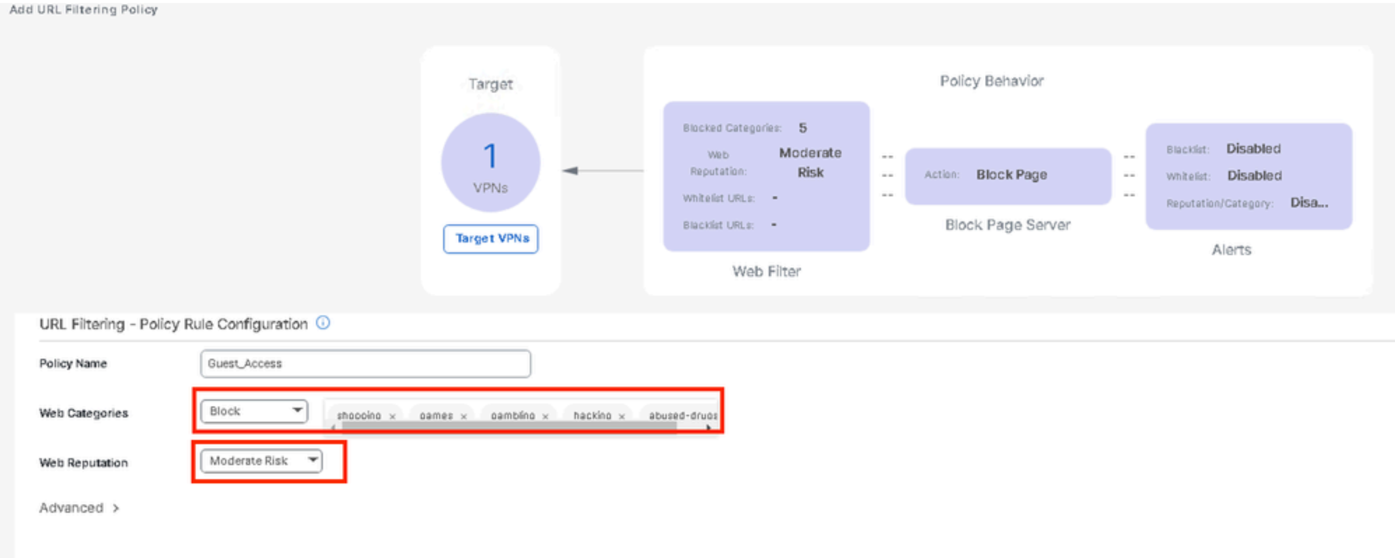
VPNs: 12

- 在Policy Name字段中输入策略名称。
- 从Web Categories下拉列表中选择以下选项之一，选择Block，并且会阻止与您选择的类别匹配的网站。

  Block -阻止与您选择的类别匹配的网站。
  Allow -允许与您选择的类别匹配的网站。

从下拉菜单中选择Web Reputation（Web信誉），并设置为Moderate Risk（中度风险）。 信誉得分等于或低于60的所有URL都将被阻止。

高风险：信誉得分为0到20。
可疑：信誉得分为0到40。
中等风险：信誉得分为0到60。
低风险：信誉得分为0到80。
值得信赖：信誉得分为0到100。



Add URL Filtering Policy

URL Filtering - Policy Rule Configuration

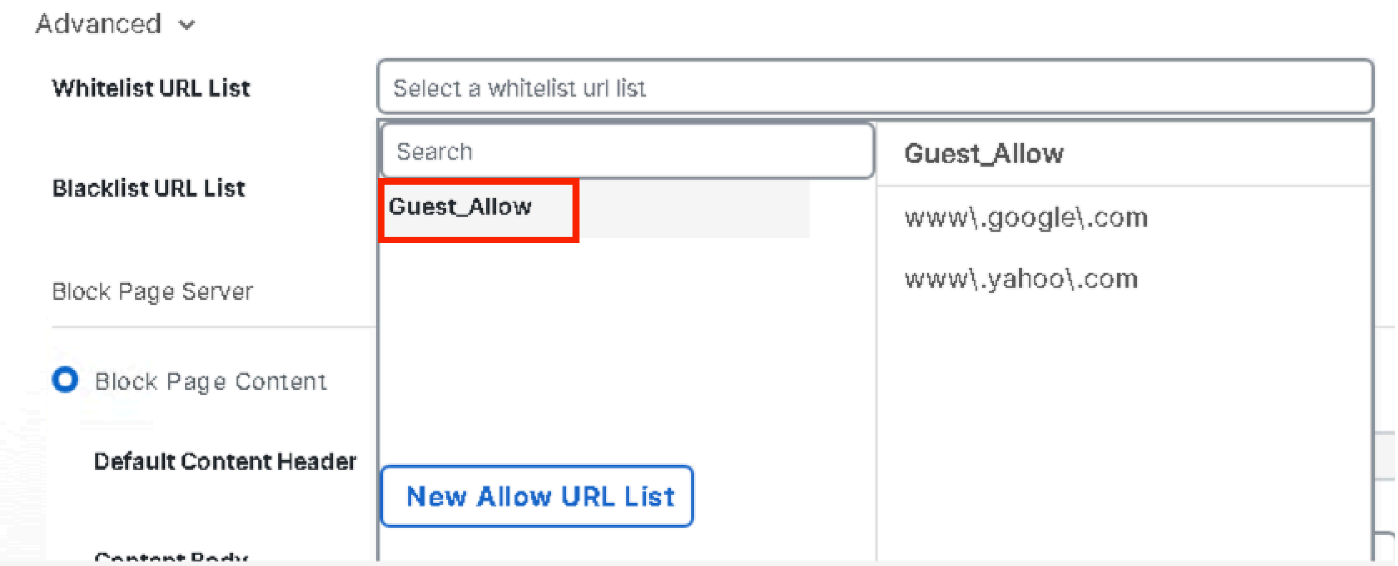
Policy Name: Guest_Access

Web Categories: Block | shopping × games × gambling × hacking × abused-drugs

Web Reputation: Moderate Risk

Advanced >

在高级中，根据需要从Allowlist URL List或blocklist URL List下拉菜单中选择现有列表或创建新列表。



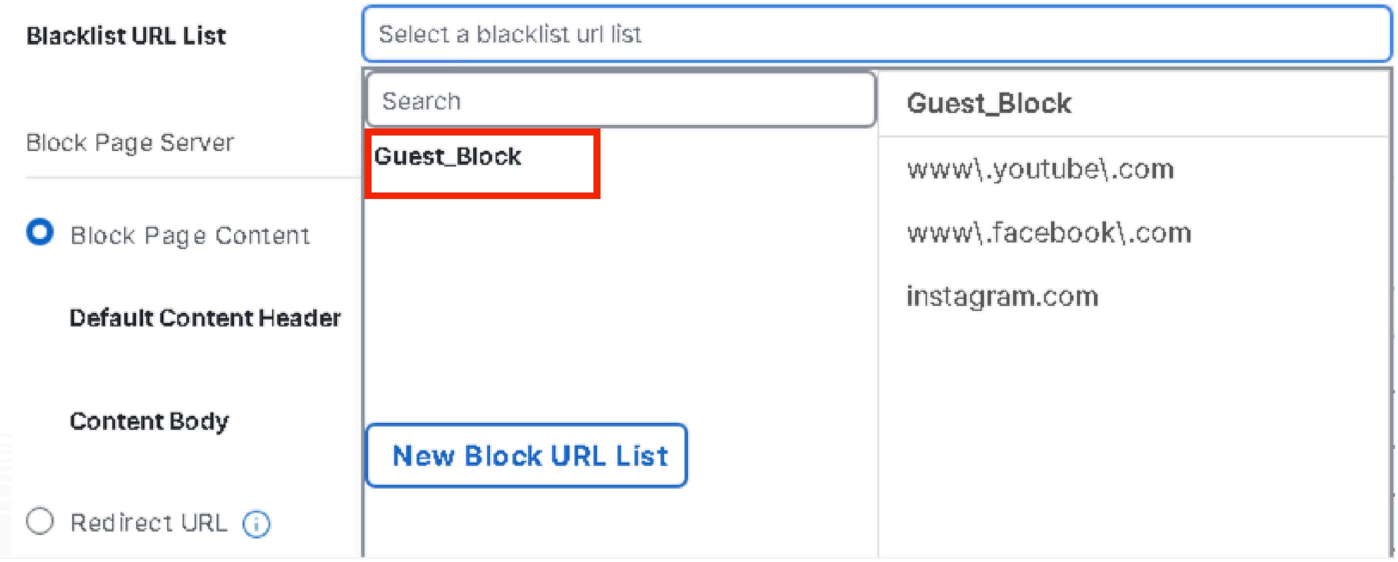
Advanced

Whitelist URL List: Select a whitelist url list

Guest_Allow

www\.google\.com

www\.yahoo\.com



Blacklist URL List: Select a blacklist url list

Guest_Block

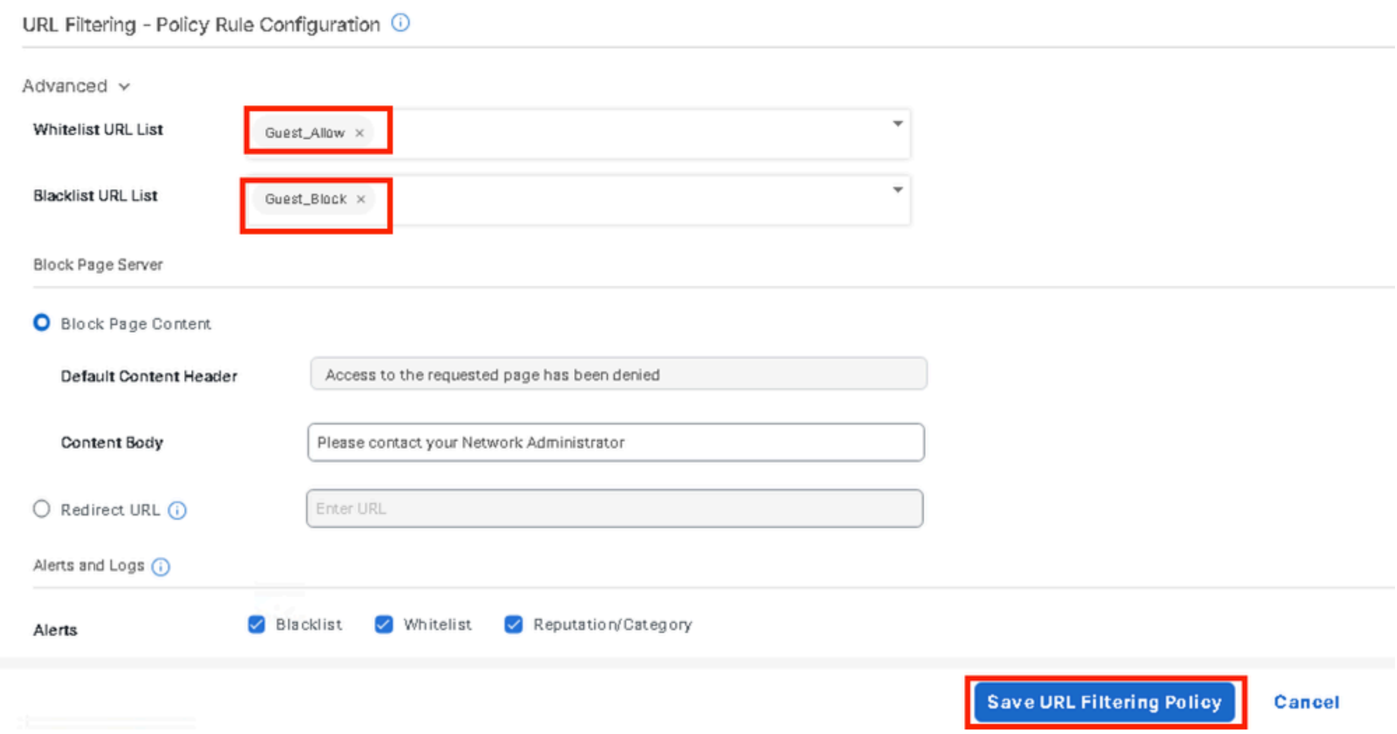
www\.youtube\.com

www\.facebook\.com

instagram.com

如果需要，请更改Block Page Content下的内容正文，并确保已选择所有警报。

单击Save URL filtering策略以添加URL过滤策略。



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

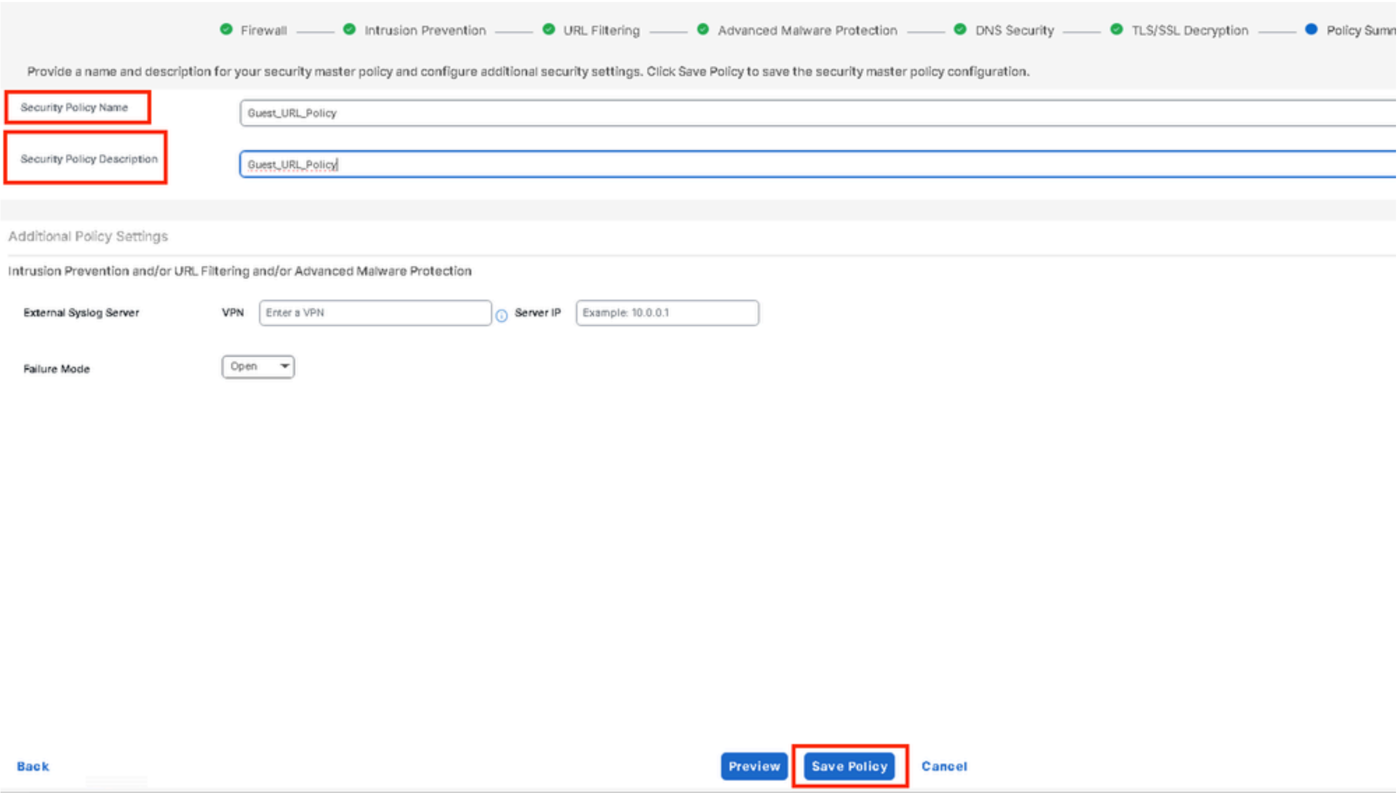
○ Redirect URL: Enter URL

Alerts and Logs

Alerts: ☑ Blacklist ☑ Whitelist ☑ Reputation/Category

单击Next，直到显示Policy Summary页。

在相应字段中输入安全策略名称和安全策略说明。



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: Guest_URL_Policy

Security Policy Description: Guest_URL_Policy

Additional Policy Settings

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

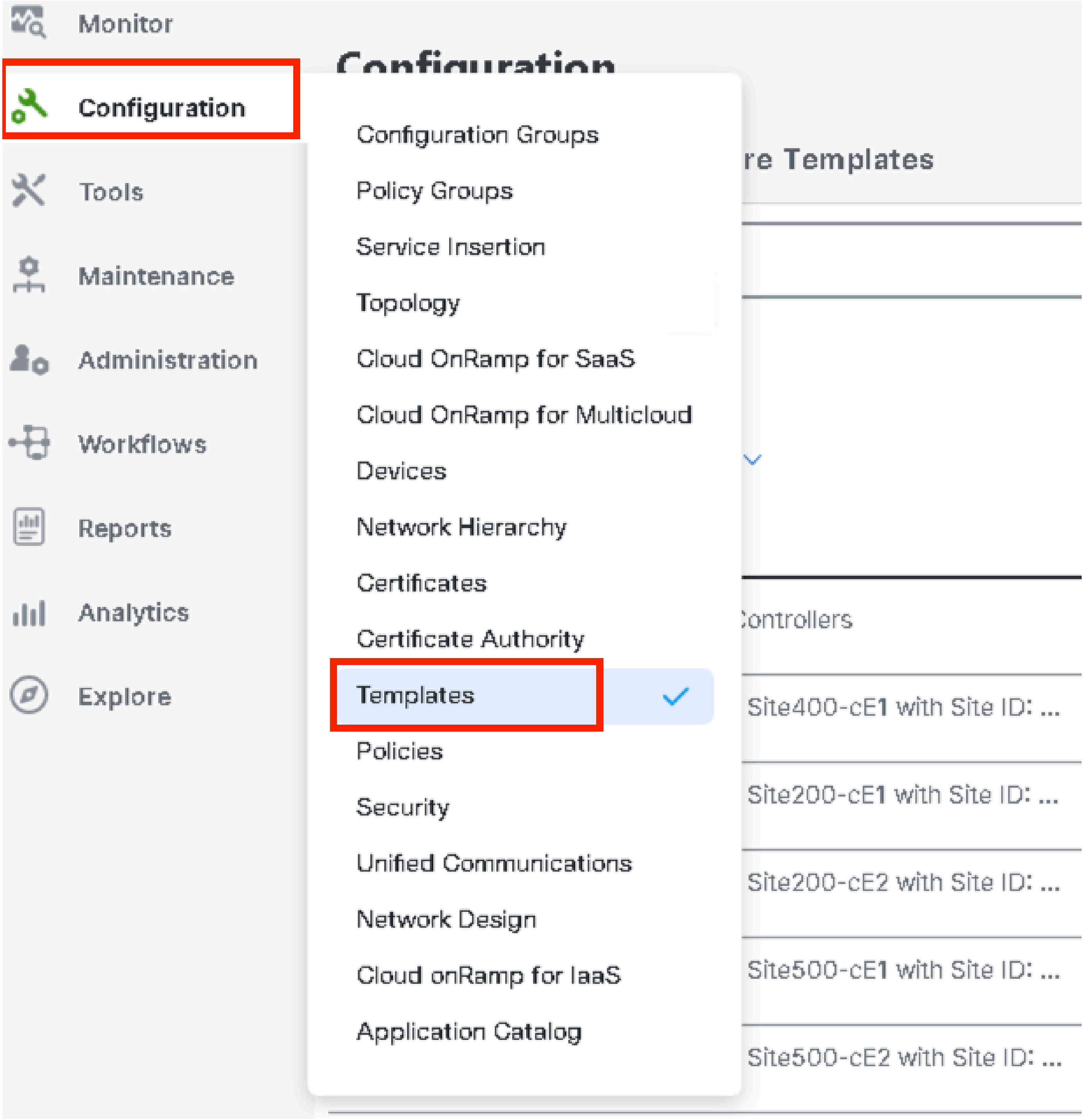
External Syslog Server: VPN: Enter a VPN Server IP: Example: 10.0.0.1

Failure Mode: Open

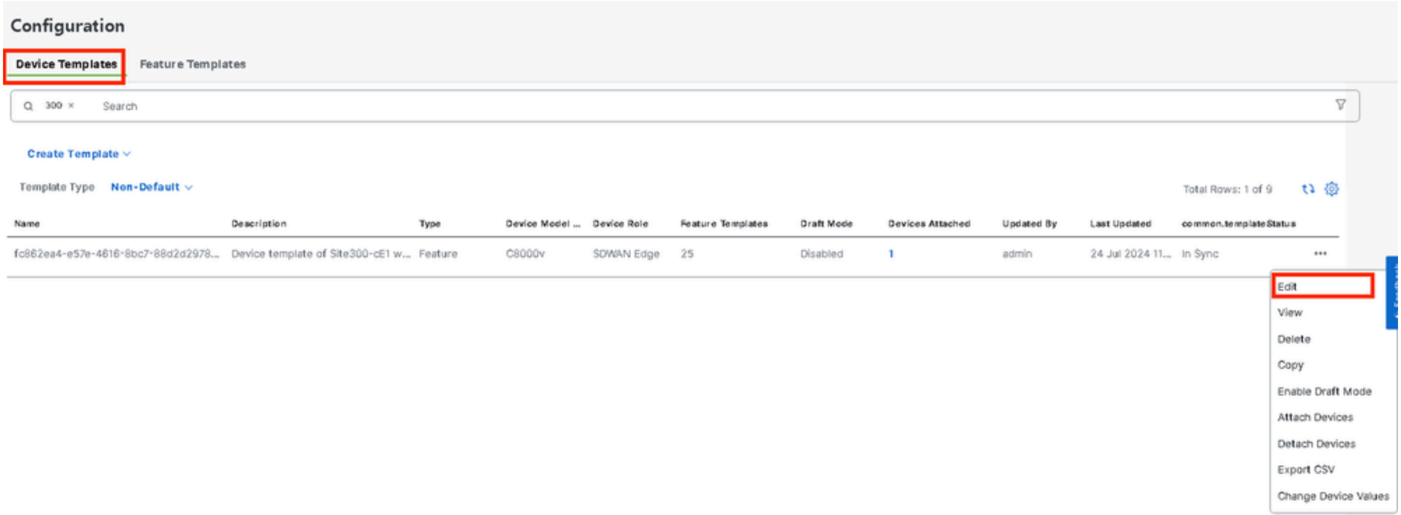
将安全策略应用于设备

要将安全策略应用到设备，请执行以下操作：

从Cisco SD-WAN Manager菜单中，选择Configuration > Templates。



依次点击设备模板和编辑设备模板。



Configuration

Device Templates | Feature Templates

300 × Search

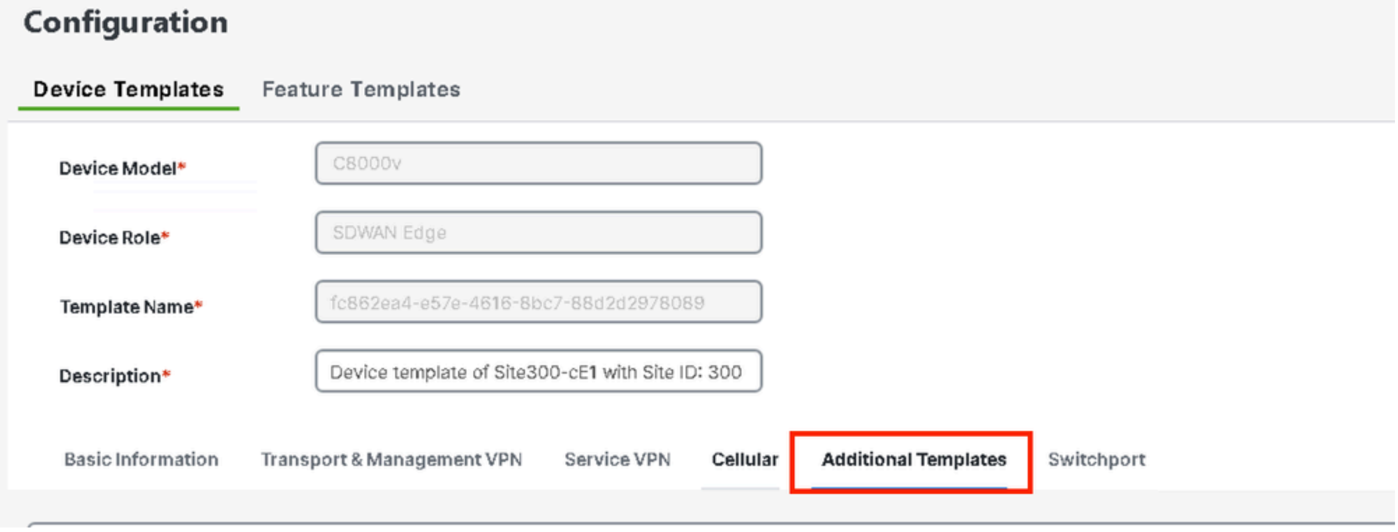
Create Template

Template Type: Non-Default

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-4616-8bc7-88d2d2978...	Device template of Site300-cE1 w...	Feature	C8000v	SDWAN Edge	25	Disabled	1	admin	24 Jul 2024 11...	In Sync

单击Additional Templates。

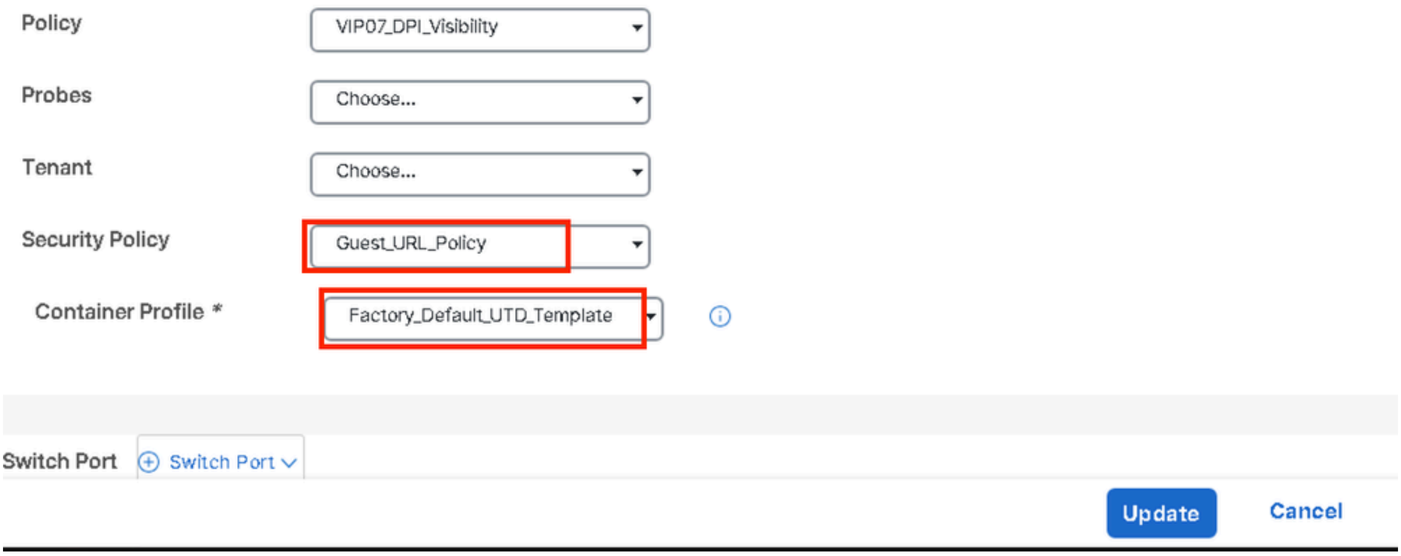


Configuration

Device Templates | Feature Templates

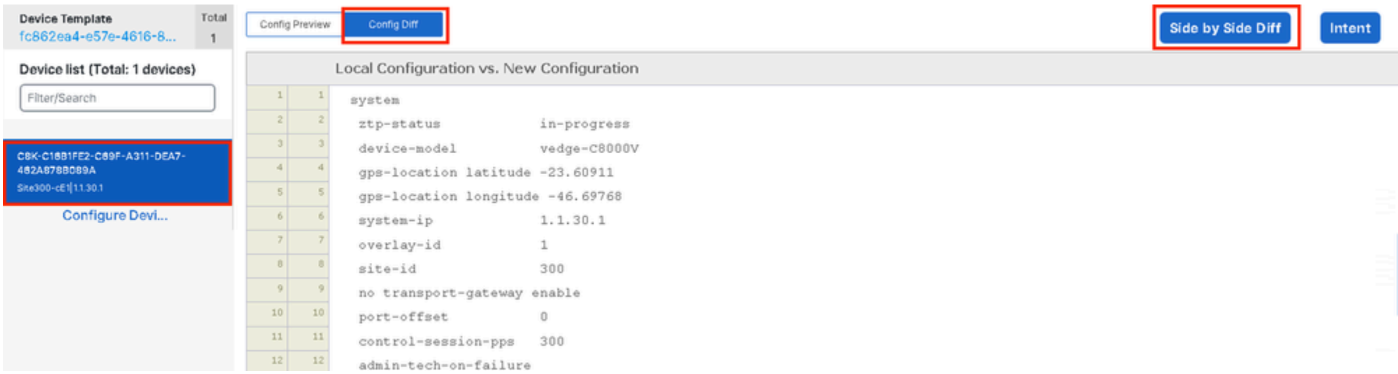
Device Model*	C8000v
Device Role*	SDWAN Edge
Template Name*	fc862ea4-e57e-4616-8bc7-88d2d2978089
Description*	Device template of Site300-cE1 with Site ID: 300

- 从Security Policy下拉列表中，选择之前在Guest_URL_Policy下配置的策略名称，然后单击Update。

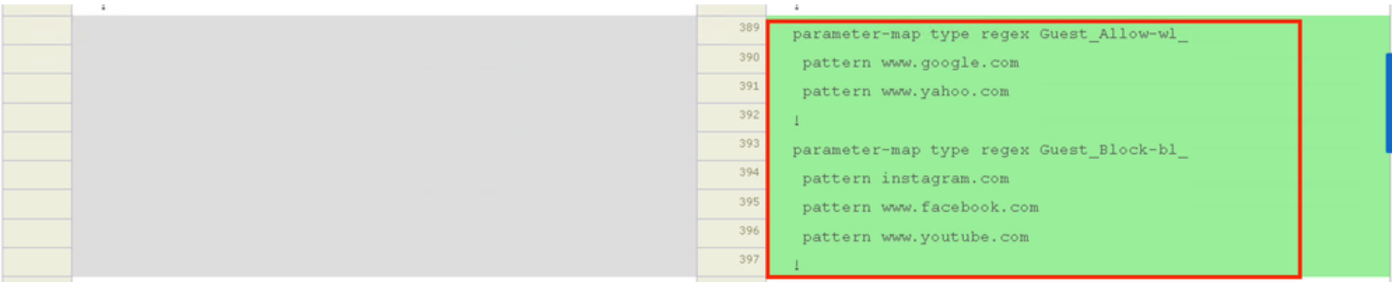


Policy	VIP07_DPI_Visibility
Probes	Choose...
Tenant	Choose...
Security Policy	Guest_URL_Policy
Container Profile *	Factory_Default_UTD_Template

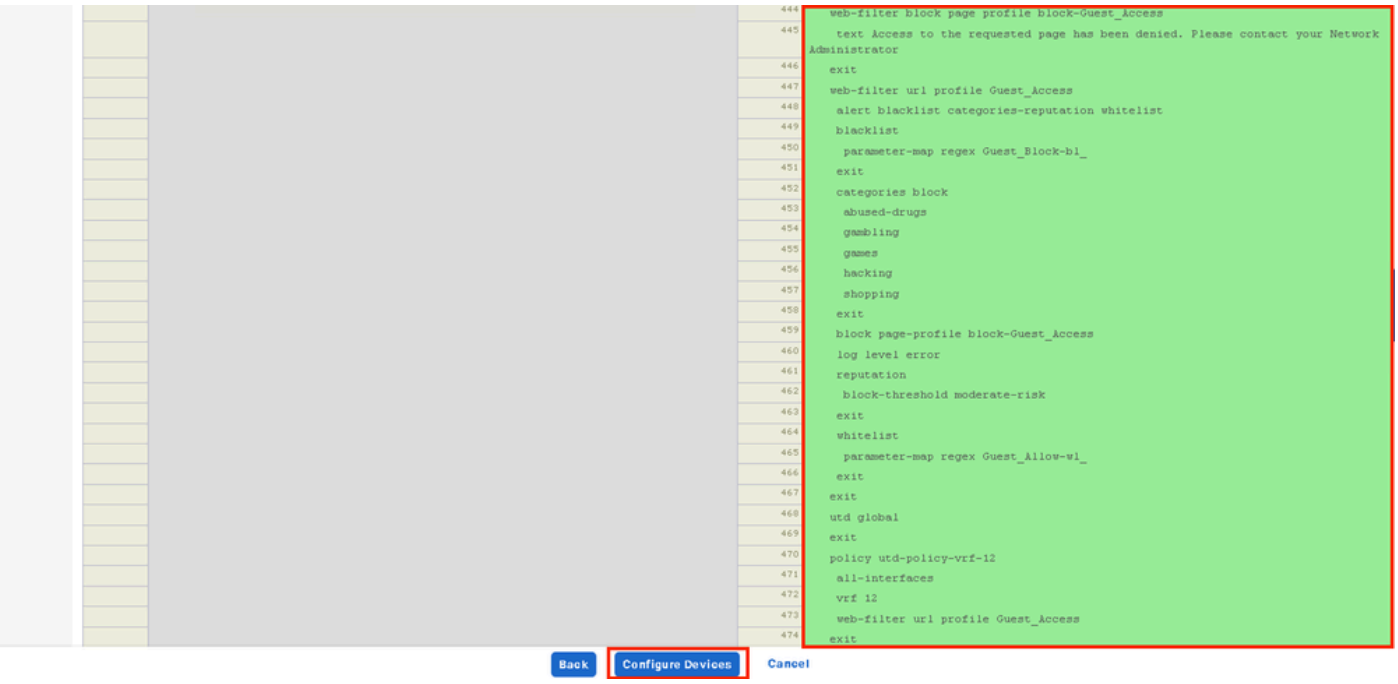
单击设备，确保配置正确，然后单击Config Diff和Side Diff。点击配置设备。



```
system
 ztp-status            in-progress
 device-model          vedge-C8000V
 gps-location latitude -23.60911
 gps-location longitude -46.69768
 system-ip             1.1.30.1
 overlay-id            1
 site-id               300
 no transport-gateway enable
 port-offset           0
 control-session-pps   300
 admin-tech-on-failure
```

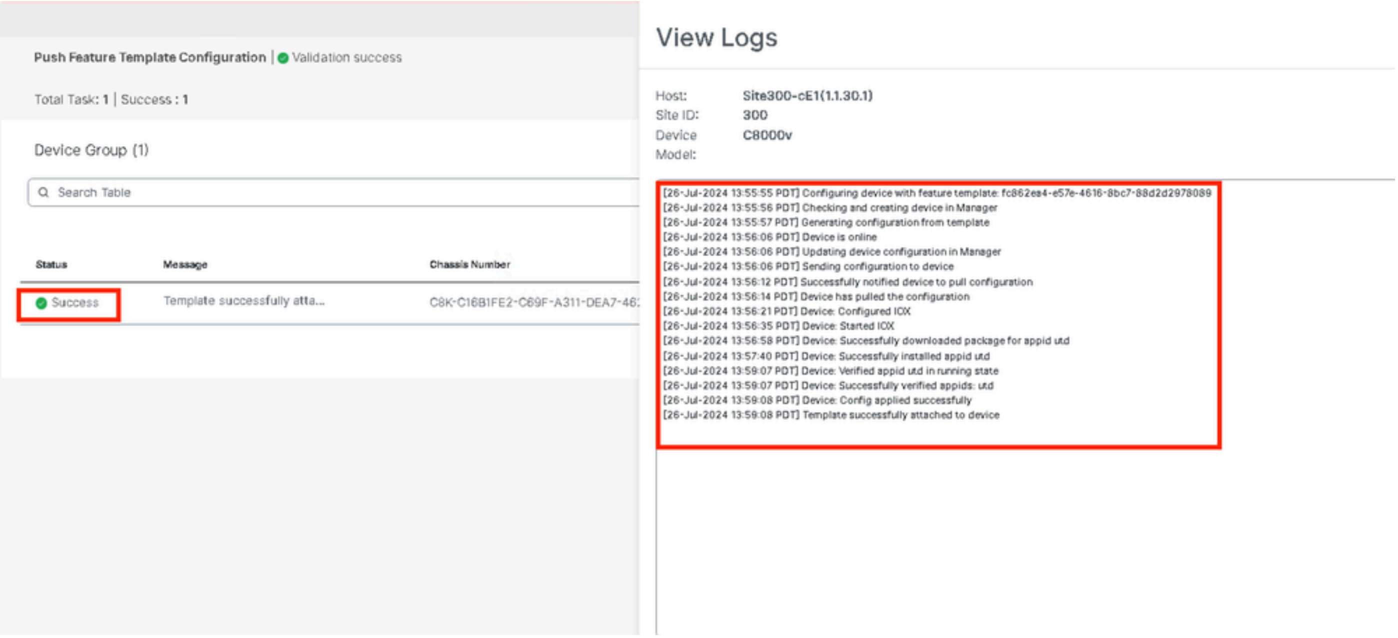


```
!
parameter-map type regex Guest_Allow-wl_
 pattern www.google.com
 pattern www.yahoo.com
!
parameter-map type regex Guest_Block-bl_
 pattern instagram.com
 pattern www.facebook.com
 pattern www.youtube.com
!
```



```
  web-filter block page profile block-Guest_Access
   text Access to the requested page has been denied. Please contact your Network Administrator
  exit
  web-filter url profile Guest_Access
   alert blacklist categories-reputation whitelist
   blacklist
    parameter-map regex Guest_Block-bl_
   exit
   categories block
    abused-drugs
    gambling
    games
    hacking
    shopping
   exit
   block page-profile block-Guest_Access
   log level error
   reputation
    block-threshold moderate-risk
   exit
   whitelist
    parameter-map regex Guest_Allow-wl_
   exit
  exit
  utd global
  exit
  policy utd-policy-vrf-12
   all-interfaces
   vrf 12
   web-filter url profile Guest_Access
  exit
```

vManage已成功使用安全策略配置设备模板，并在边缘设备上安装UTD软件包。



Push Feature Template Configuration | ● Validation success

Total Task: 1 | Success : 1

Device Group (1)

Status	Message	Chassis Number
● Success	Template successfully atta...	C8K-C16B1FE2-C69F-A311-DEA7-46:

View Logs

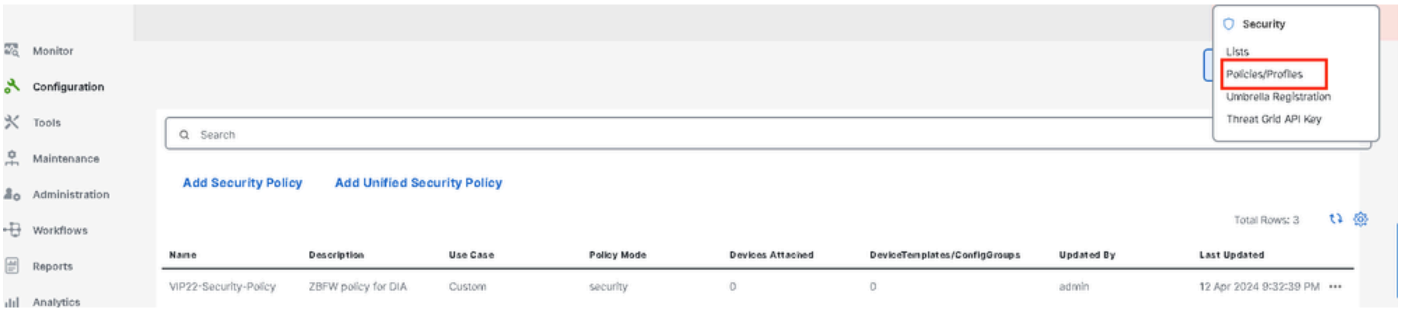
Host: Site300-cE1(1.1.30.1)
Site ID: 300
Device Model: C8000v

```
[26-Jul-2024 13:55:55 PDT] Configuring device with feature template: fc862ea4-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
```

修改URL过滤

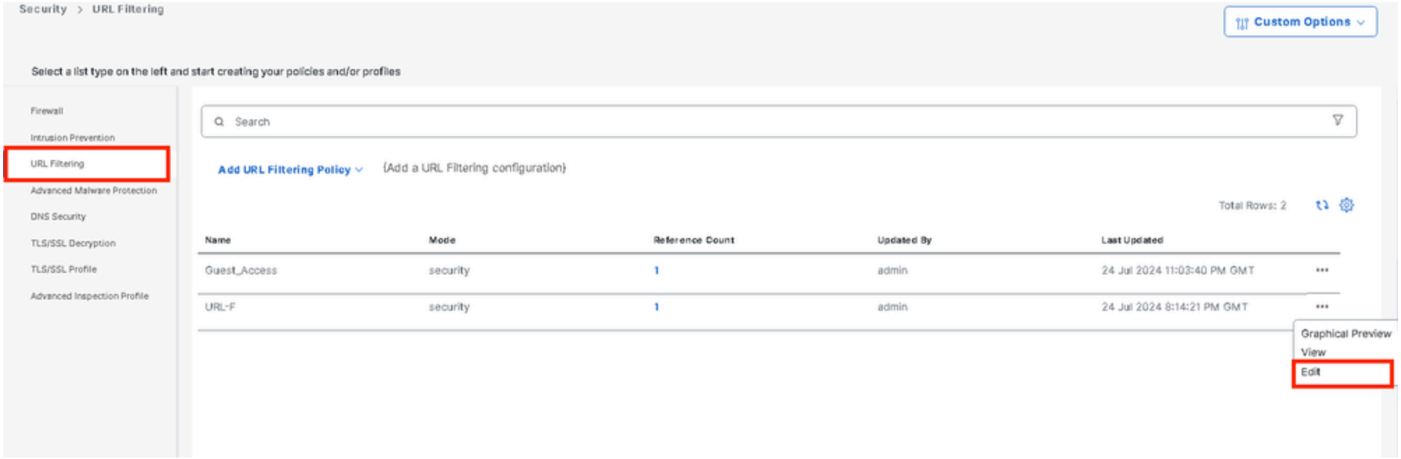
要修改URL过滤策略，请执行以下步骤：

1. 从Cisco SD-WAN Manager菜单中选择Configuration > Security。
2. 在“Security”屏幕中，单击Custom Options下拉菜单（在“Controller/Profiles”窗口中），然后选择Policies/Profiles。



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 •••

单击左侧选项卡上的URL Filtering，针对要修改的所需策略，单击3个点(...)，然后选择Edit。

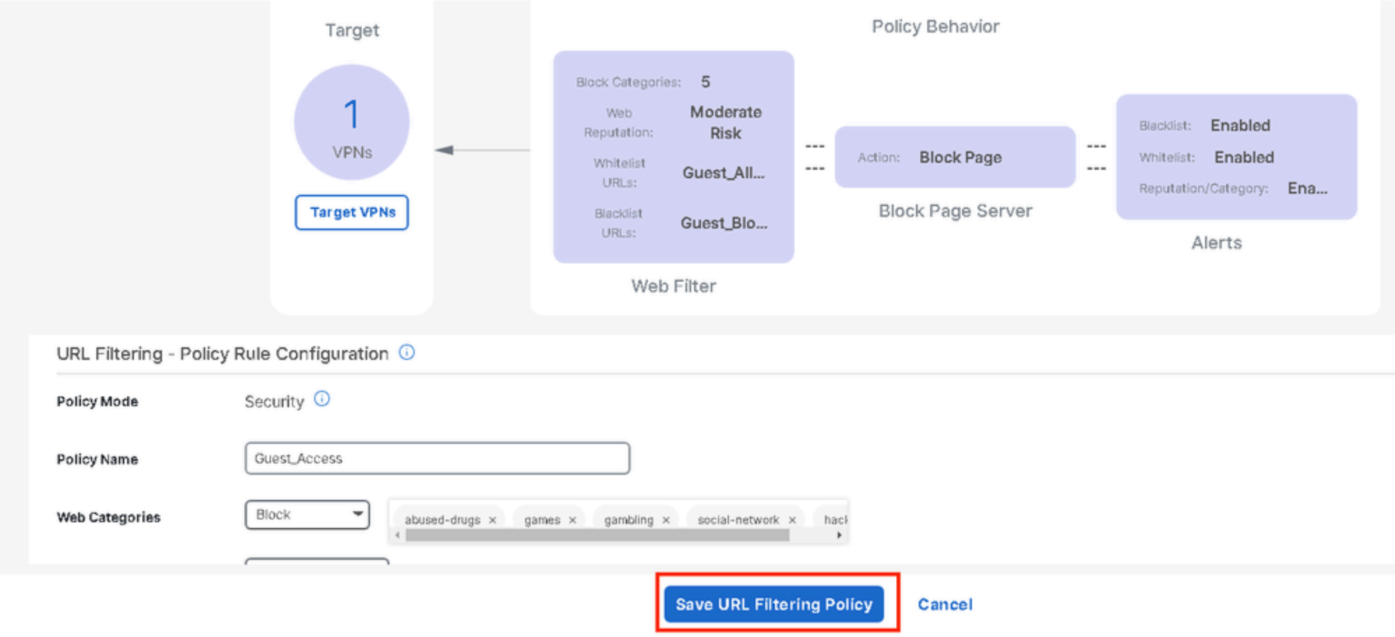


Select a list type on the left and start creating your policies and/or profiles

(Add a URL Filtering configuration)

Name	Mode	Reference Count	Updated By	Last Updated
Guest_Access	security	1	admin	24 Jul 2024 11:03:40 PM GMT
URL-F	security	1	admin	24 Jul 2024 8:14:21 PM GMT

根据需要修改策略，然后单击Save URL Filtering Policy。



Block Categories: 5
Web Reputation: Moderate Risk
Whitelist URLs: Guest_All...
Blacklist URLs: Guest_Blo...

Action: Block Page

Blacklist: Enabled
Whitelist: Enabled
Reputation/Category: Ena...

URL Filtering - Policy Rule Configuration

Policy Mode: Security

Policy Name: Guest_Access

Web Categories: Block — abused-drugs, games, gambling, social-network, hacl

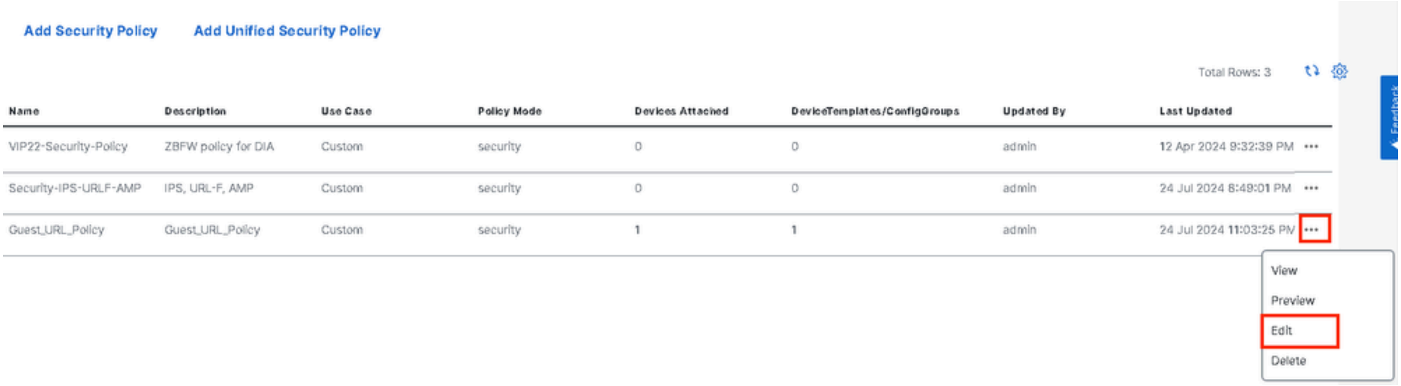
删除URL过滤

要删除URL过滤策略，必须首先从安全策略分离策略：

从Cisco SD-WAN Manager菜单中，选择Configuration > Security。

要将URL过滤策略与安全策略分离，请执行以下操作：

- 对于包含URL过滤策略的安全策略，请点击3个点(...)，然后点击Edit。

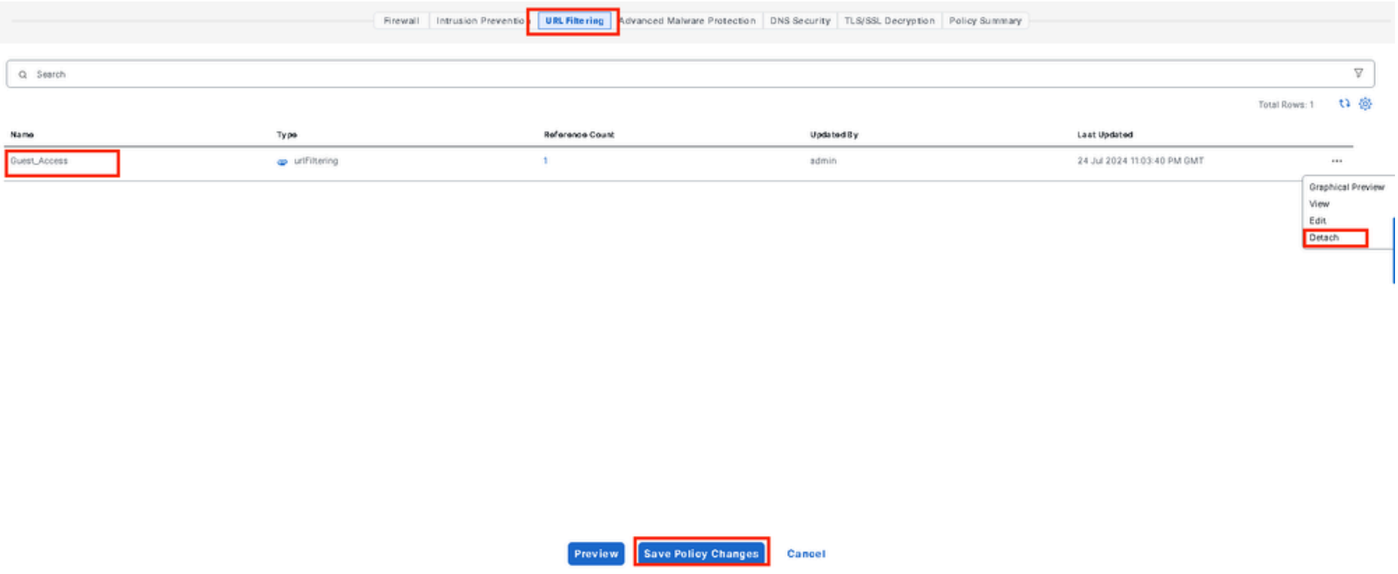


Name	Description	Use Case	Policy Mode	Devices Attached	DeviceTemplates/ConfigGroups	Updated By	Last Updated
VIP22-Security-Policy	ZBFW policy for DIA	Custom	security	0	0	admin	12 Apr 2024 9:32:39 PM
Security-IPS-URLF-AMP	IPS, URL-F, AMP	Custom	security	0	0	admin	24 Jul 2024 8:49:01 PM
Guest_URL_Policy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

系统将显示Policy Summary页面。点击URL Filtering选项卡。

对于要删除的策略，请点击3点(...)，然后选择分离(Detach)。

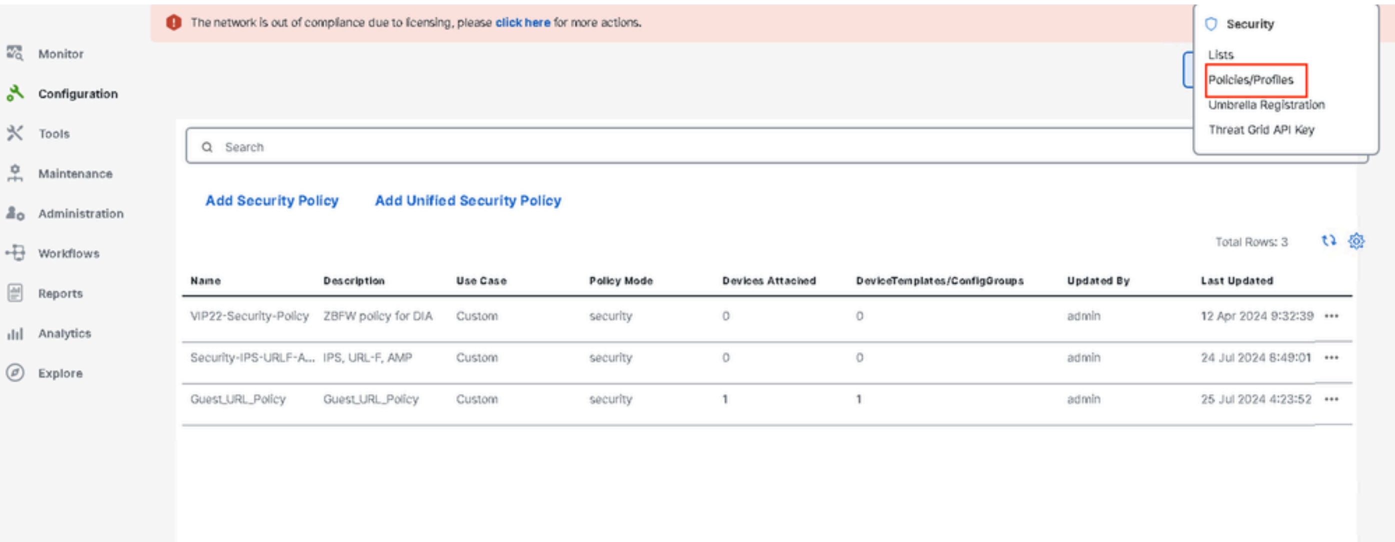
单击Save Policy Changes。



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

要删除URL过滤策略，请执行以下操作：

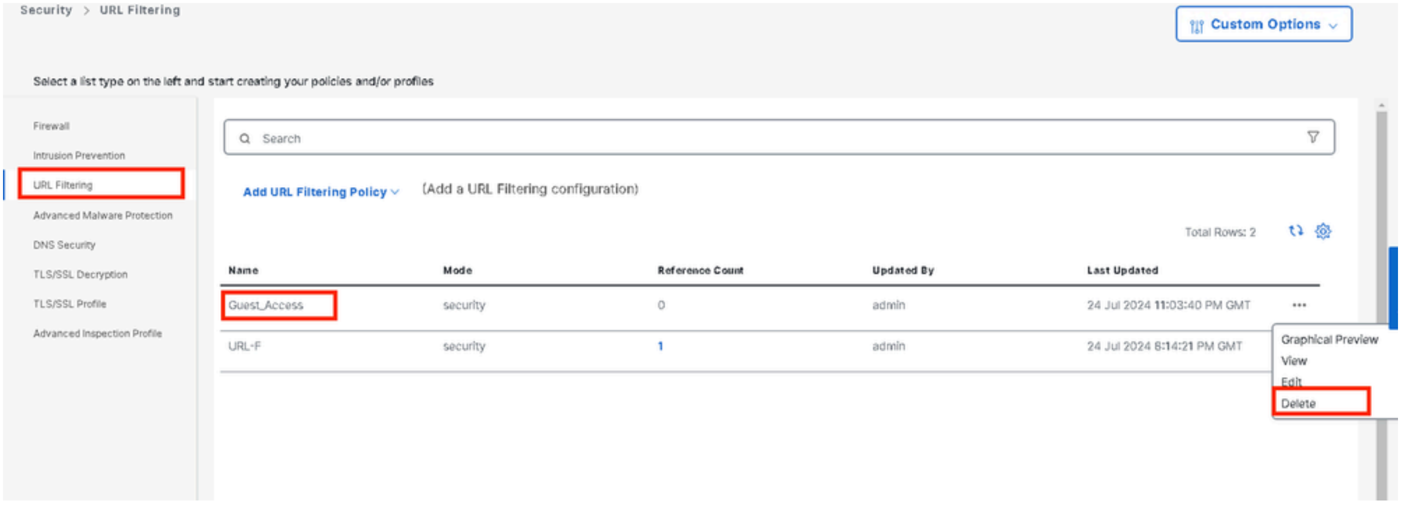
在Security屏幕中，点击Custom Options下拉菜单(Policies/Profiles)，然后选择URL Filtering。


The network is out of compliance due to licensing, please click here for more actions.

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
Guest_URL_Policy	Guest_URL_Policy	Custom	security	1	1	admin	25 Jul 2024 4:23:52

对于要删除的策略，请点击3个点(...)，然后点击删除。

单击OK。



Security > URL Filtering

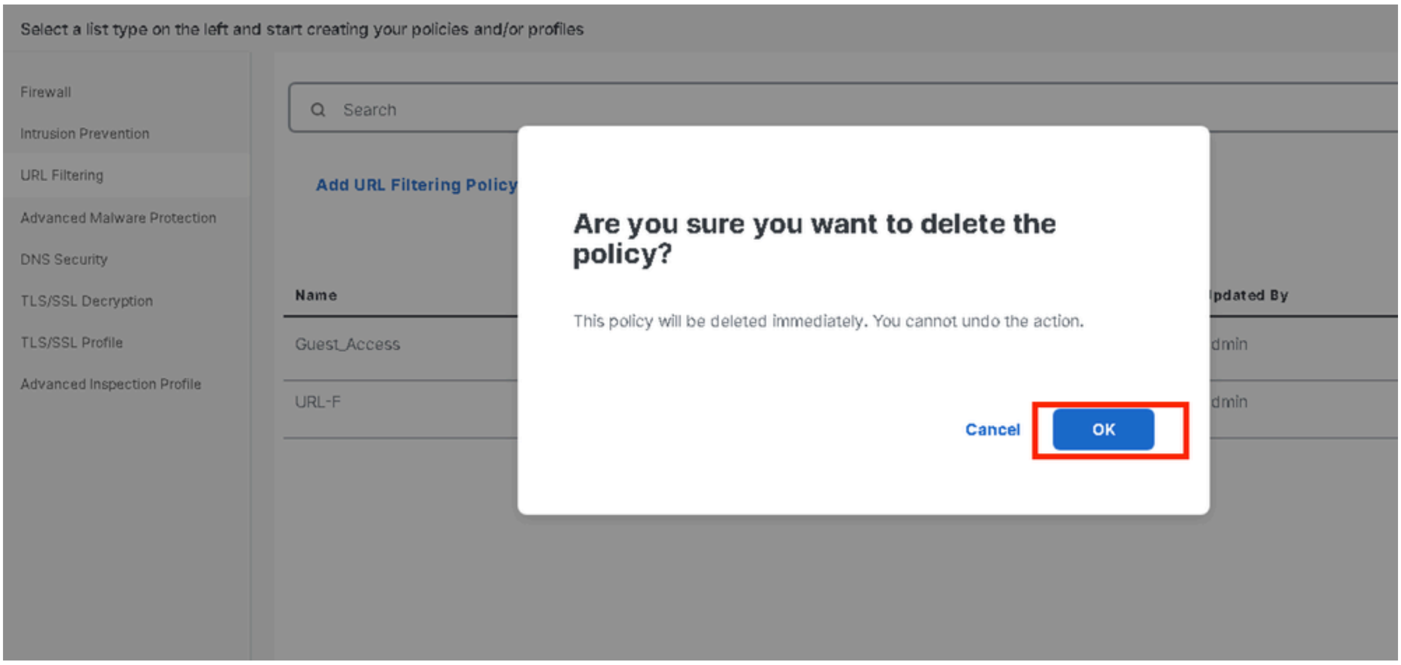
Custom Options

Select a list type on the left and start creating your policies and/or profiles

(Add a URL Filtering configuration)

Total Rows: 2

Name	Mode	Reference Count	Updated By	Last Updated
Guest_Access	security	0	admin	24 Jul 2024 11:03:40 PM GMT
URL-F	security	1	admin	24 Jul 2024 8:14:21 PM GMT



Select a list type on the left and start creating your policies and/or profiles

Are you sure you want to delete the policy?

This policy will be deleted immediately. You cannot undo the action.

验证

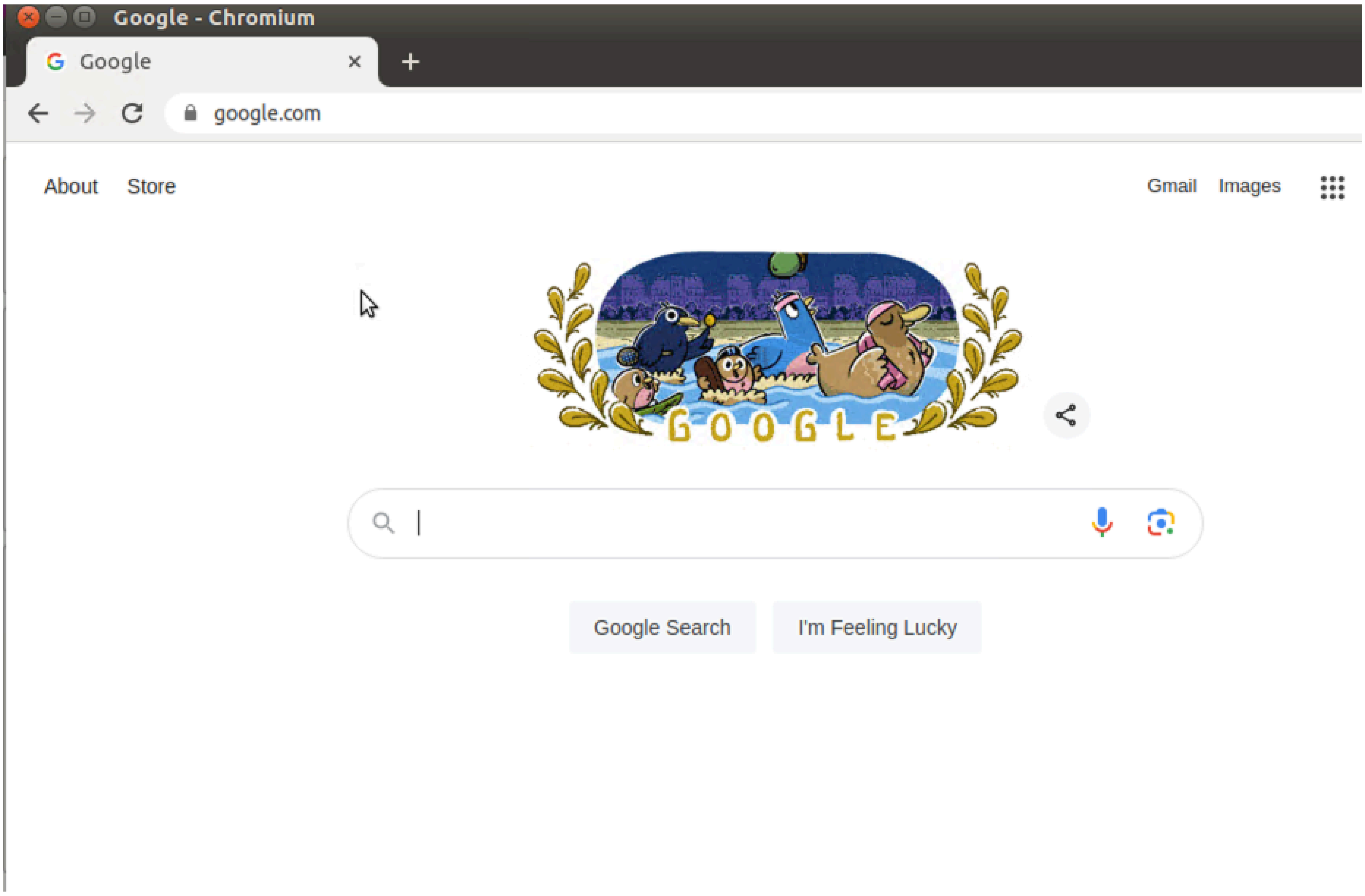
验证是否安装了Cisco UTD版本。

<#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
```

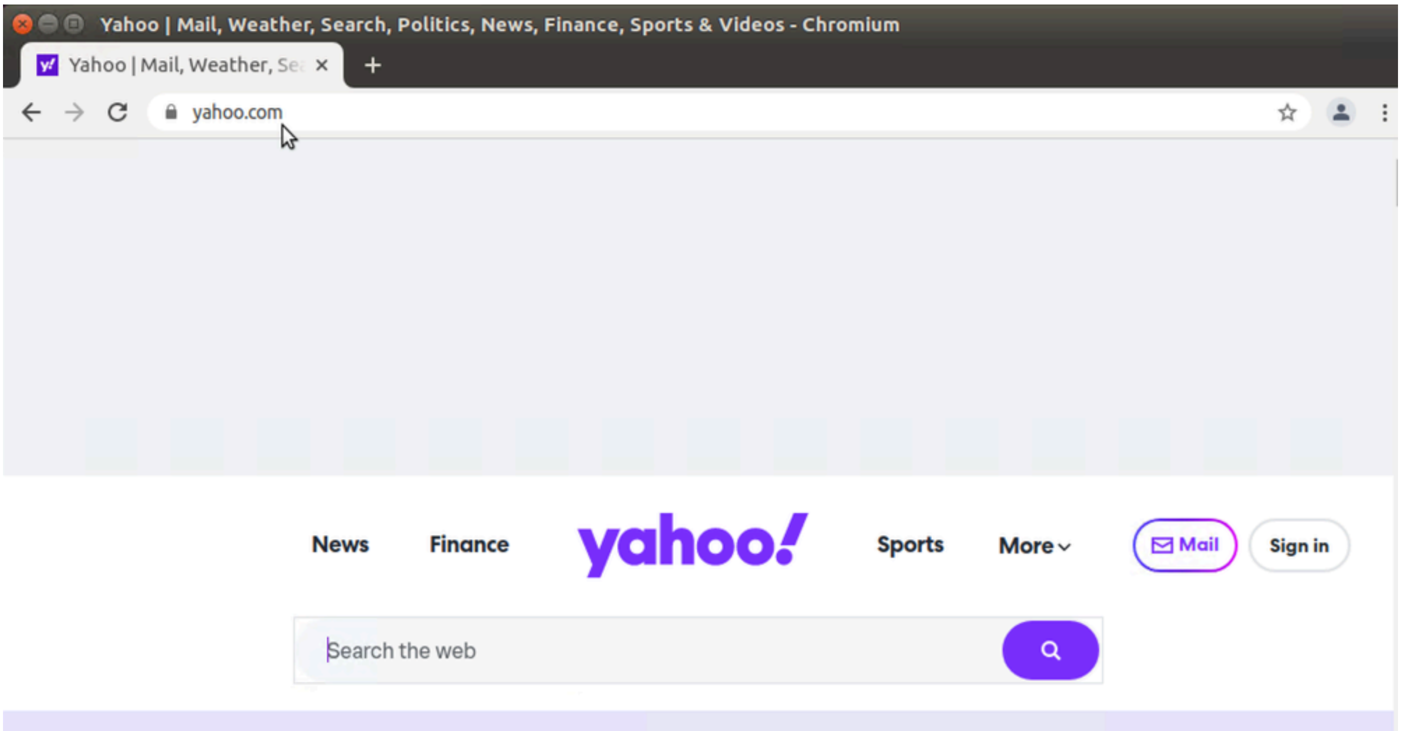
```
IOS-XE Supported UTD Regex: ^1\.0\.([0-9]+)_SV(.*)_XE17.14$
UTD Installed Version:

1.0.2_SV3.1.67.0_XE17.14
```

在位于访客VPN上的客户端PC上，如果您尝试打开google.com和yahoo.com，则允许这些访问。



<#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
```

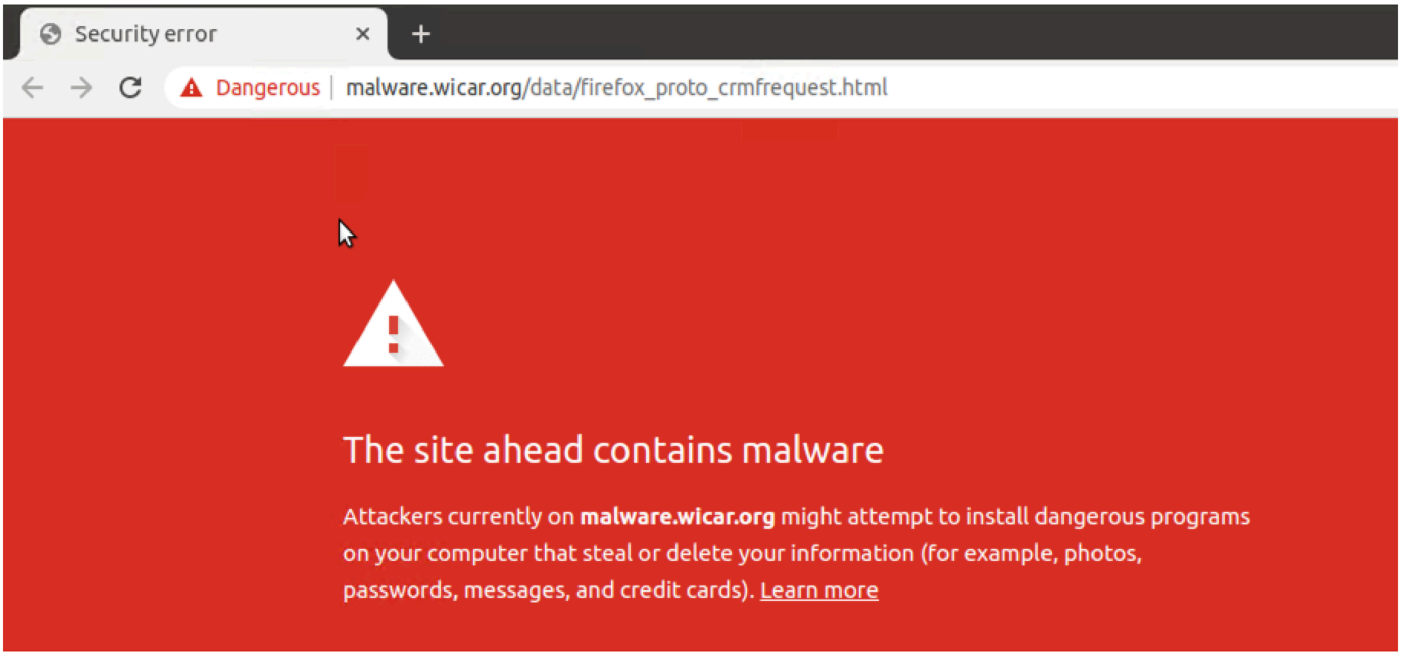


Yahoo | Mail, Weather, Search, Politics, News, Finance, Sports & Videos - Chromium
Yahoo | Mail, Weather, Se
yahoo.com
News
Finance
yahoo!
Sports
More
Mail
Sign in
Search the web

<#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
```

在位于访客VPN上的客户端PC上，如果您尝试打开信誉得分较低的网页或来自其中一个被阻止的网络类别，URL过滤引擎将拒绝HTTPs请求。



The site ahead contains malware

Attackers currently on **malware.wicar.org** might attempt to install dangerous programs on your computer that steal or delete your information (for example, photos, passwords, messages, and credit cards). Learn more

<#root>

```
Site300-cE1#show utd engine standard logging events | in mal
2024/07/24-13:32:18.475318 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
```

Drop

```
 [**]
```

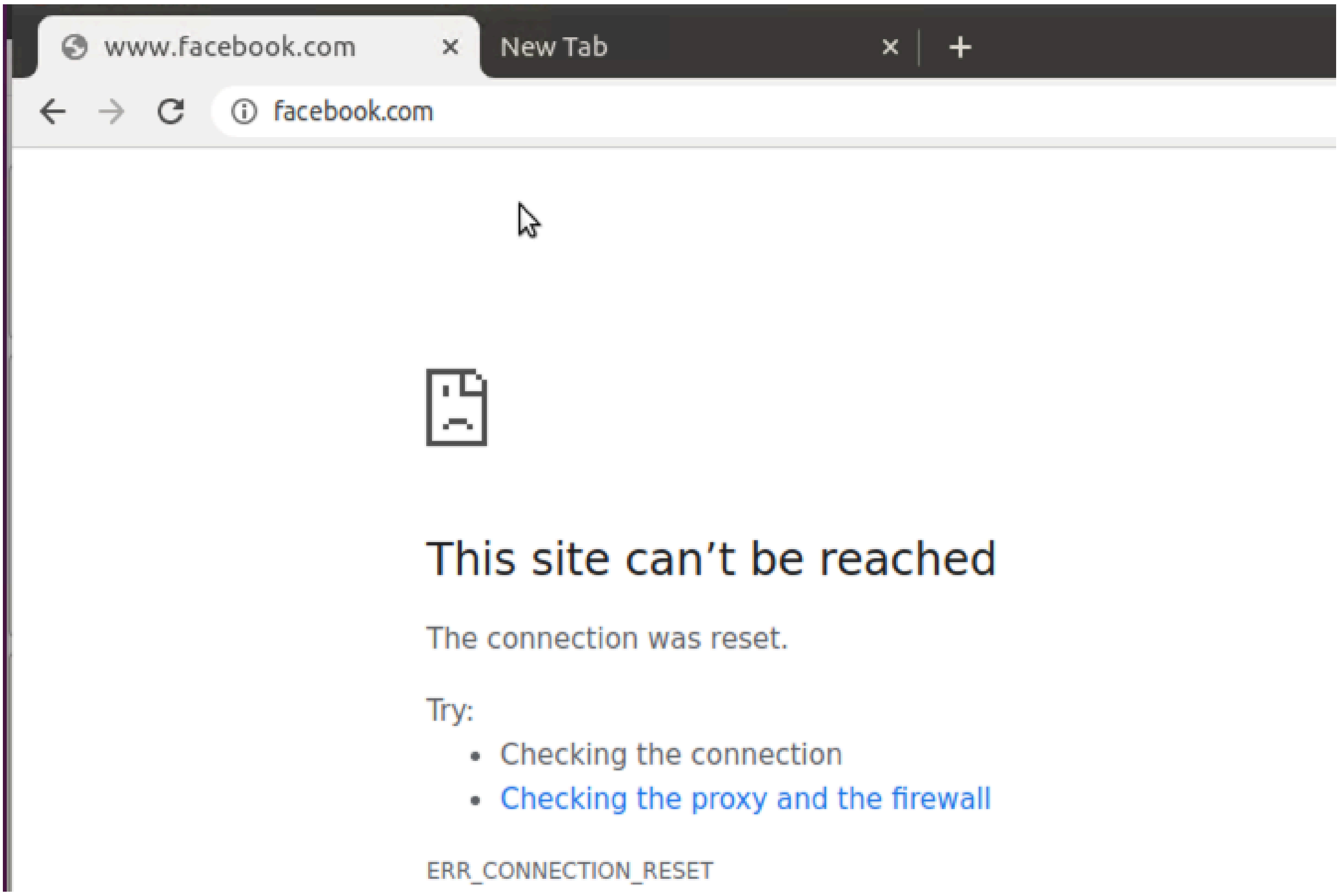
UTD WebFilter Category/Reputation

```
 [**] [
```

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
```

如果您尝试打开facebook、instagram和youtube，从位于访客VPN上的客户端PC上会阻止访问。



This site can’t be reached

The connection was reset.

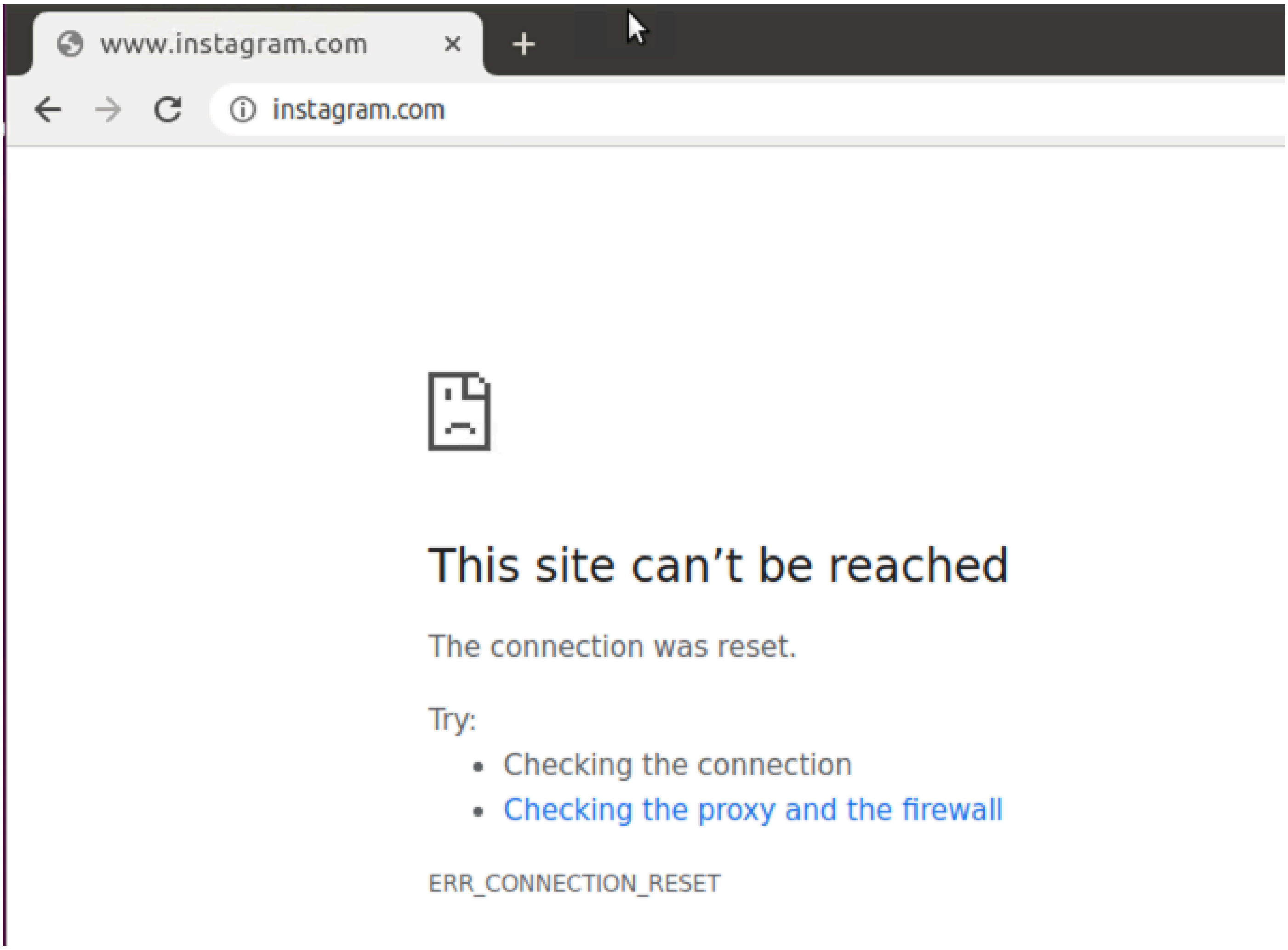
Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_RESET

<#root>

```
Site300-cE1#show utd engine standard logging events | in face
2024/07/24-13:05:25.622746 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID

Drop

 [**]

UTD WebFilter blocklist

 [**] [

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 blocklist

 [**] [

URL: www.facebook.com

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



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 insta
2024/07/24-13:09:07.027559 PDT [**] [Hostname: site300-ce1] [**] [System_IP: x.x.x.x] [**] [Instance_ID
```

Drop

```
 [**]
```

UTD WebFilter blocklist

```
 [**] [
```

URL: www.instagram.com

```
] [VRF: 12] {TCP} 10.32.1.10:58496 -> 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

```
 [**]
```

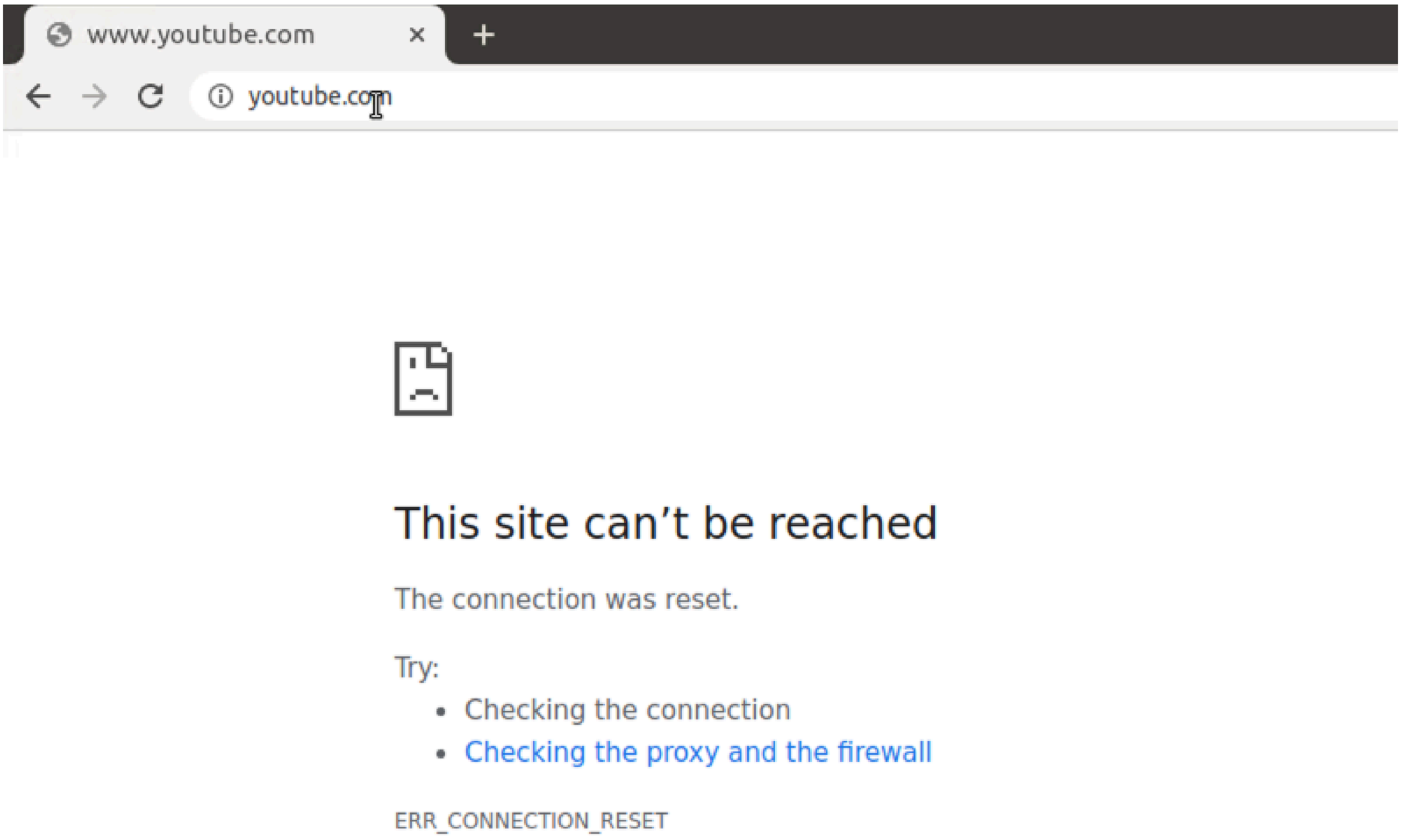
UTD WebFilter blocklist

```
 [**] [
```

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

 [**]
```

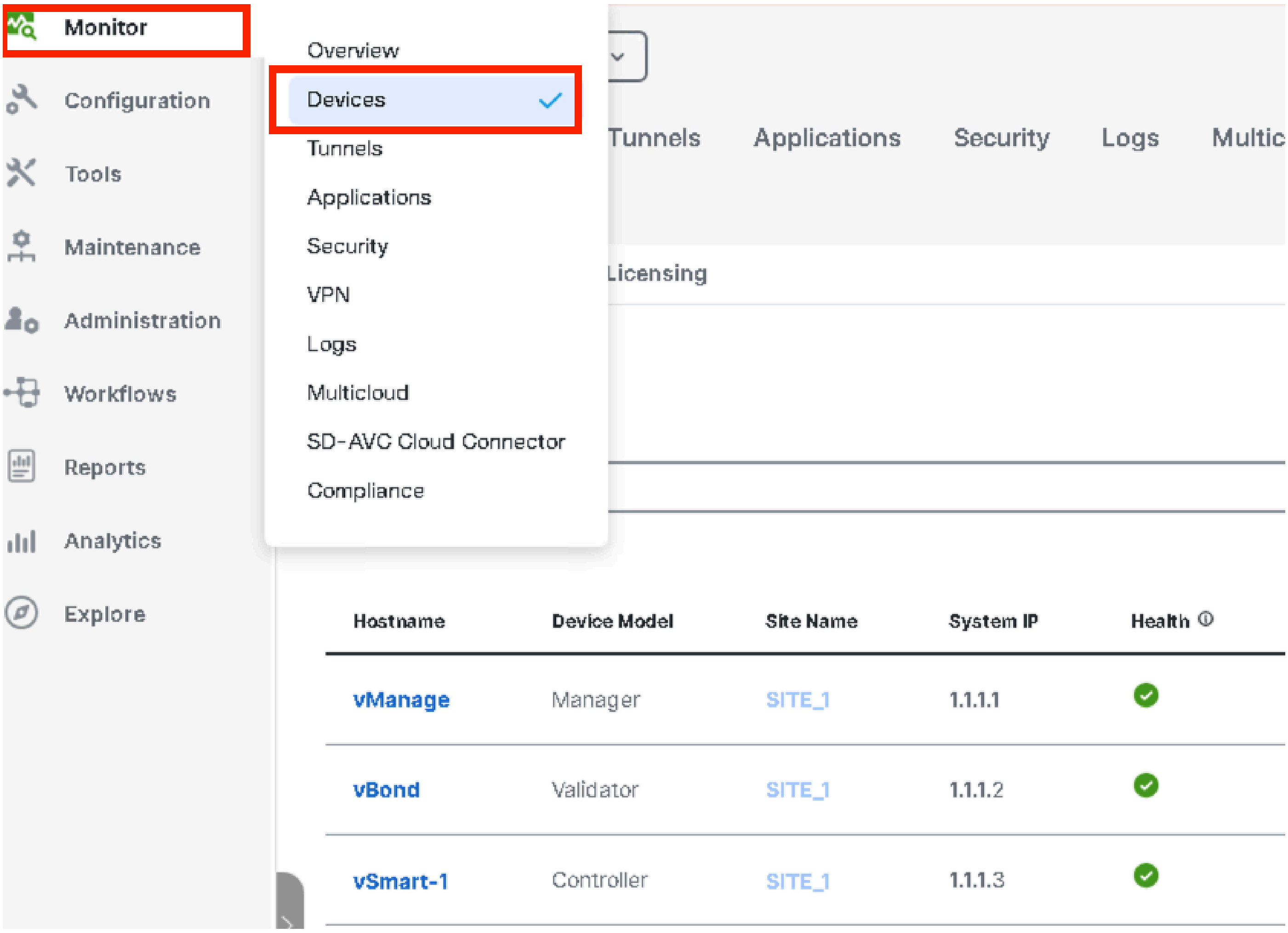
```
UTD WebFilter blocklist

 [**] [

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
```

从vManage GUI监控URL过滤

您可以使用这些步骤，按网络类别实时或历史地监控每个设备的URL过滤。

要在Cisco IOS XE Catalyst SD-WAN设备上监控阻止或允许的URL，请执行以下操作：

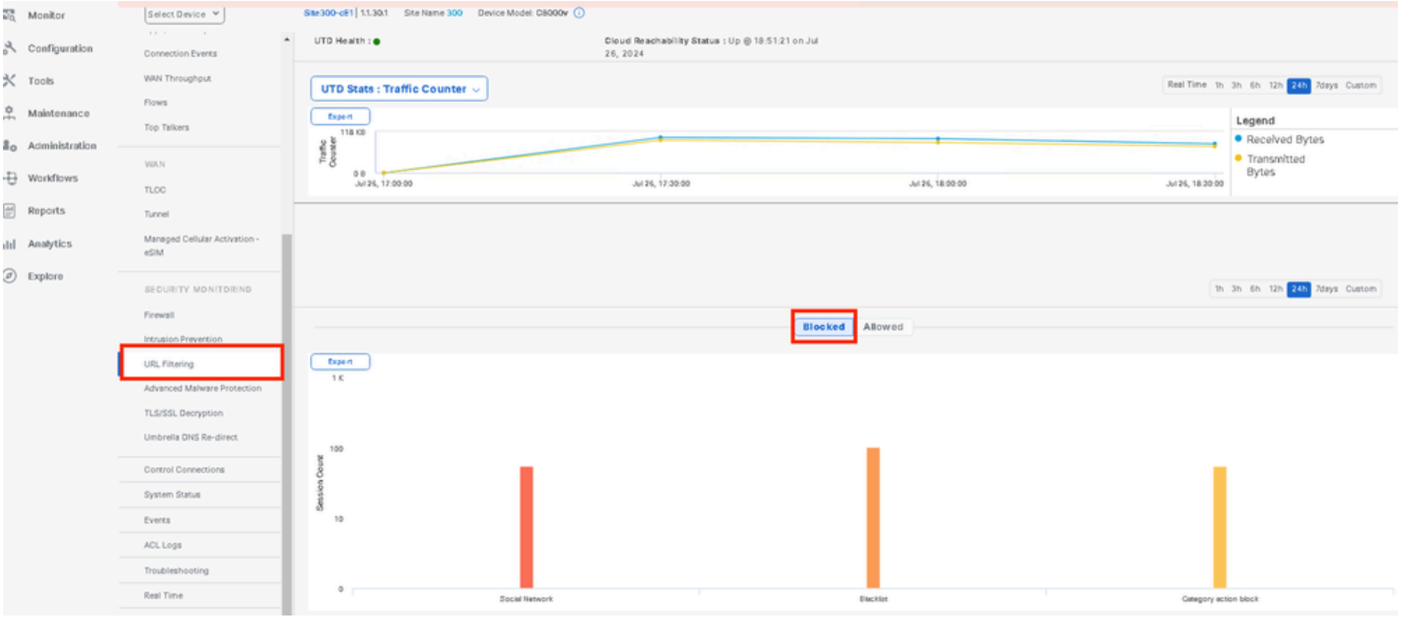
1. 在Cisco SD-WAN Manager菜单中，选择Monitor > Devices >Select Device

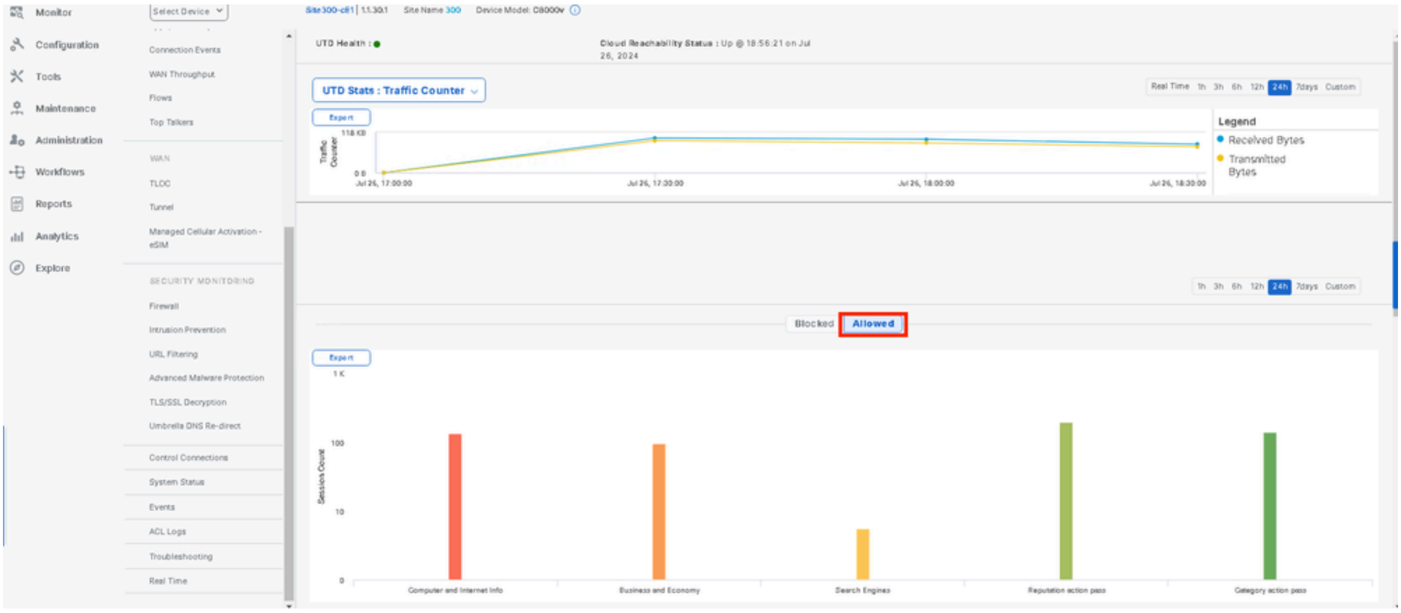


Hostname	Device Model	Site Name	System IP	Health ⓘ
vManage	Manager	SITE_1	1.1.1.1	✓
vBond	Validator	SITE_1	1.1.1.2	✓
vSmart-1	Controller	SITE_1	1.1.1.3	✓

2. 在左侧窗格中的“安全监控”下，单击“URL过滤”。URL过滤信息将显示在右窗格中。

- 单击Blocked。系统将显示受阻URL上的会话计数。
- 单击Allowed。系统将显示允许的URL上的会话计数。





故障排除

验证是否安装了受支持的UTD版本：

<#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 <<<<<<<<<<<<<<<<

注意：UTD安装的版本不能处于不支持的状态。

检查UTD是否处于onrunning状态。

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

验证UTD运行状况处于绿色。

<#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
```

验证是否已启用URL过滤功能。

<#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
```

要显示URL过滤日志，请运行show utd engine standard logging events url-filtering命令。

```
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
```

注意：运行clear utd engine standard logging events命令以清除旧事件。

检查进入UTD容器的入口/出口数据包，查询延迟。

```
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
```

相关信息

- Cisco Catalyst SD-WAN安全配置指南
- 在cEdge路由器上安装UTD安全虚拟映像
- 通过UTD和URL过滤排除数据路径处理故障