

# URLフィルタリングの設定と確認

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[URLフィルタリングポリシーのコンポーネントの設定](#)

[対象のURLリストの作成](#)

[セキュリティポリシーの作成](#)

[デバイスへのセキュリティポリシーの適用](#)

[URLフィルタの変更](#)

[URLフィルタリングの削除](#)

[確認](#)

[vManage GUIからのURLフィルタリングのモニタ](#)

[トラブルシューティング](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、Cisco Catalyst Manager GUIを使用して、CISCO IOS-XE®ルータでURLフィルタリングを設定および確認する方法について説明します。

## 前提条件

vManageの現在のCisco IOS-XEコードと互換性のあるUTDソフトウェア仮想イメージをアップロードします。cEdgeルータにUTDセキュリティ仮想イメージをインストールする方法については、「[関連情報](#)」セクションを参照してください。

Ciscoエッジルータは、テンプレートがプリアタッチされたvManagedモードである必要があります。

## 要件

次の項目に関する知識があることが推奨されます。

- Cisco SD-WANオーバーレイが初期設定で起動します。
- URLフィルタリングの設定：Cisco Catalyst Manager GUI

## 使用するコンポーネント

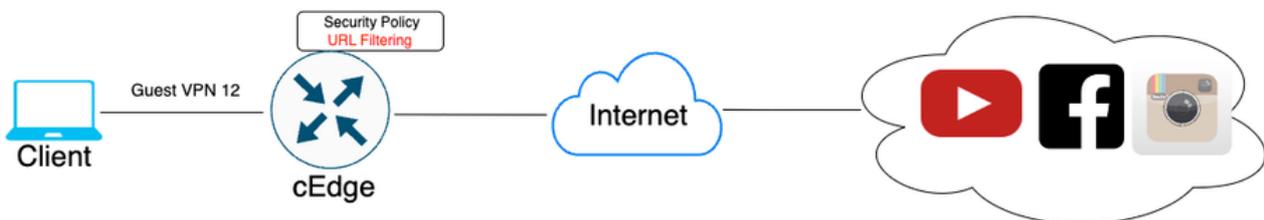
このドキュメントは、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Catalyst SD-WAN Managerバージョン20.14.1
- Cisco Catalyst SD-WANコントローラバージョン20.14.1
- Ciscoエッジルーターバージョン17.14.1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 設定

### ネットワーク図



### URLフィルタリングポリシーのコンポーネントの設定

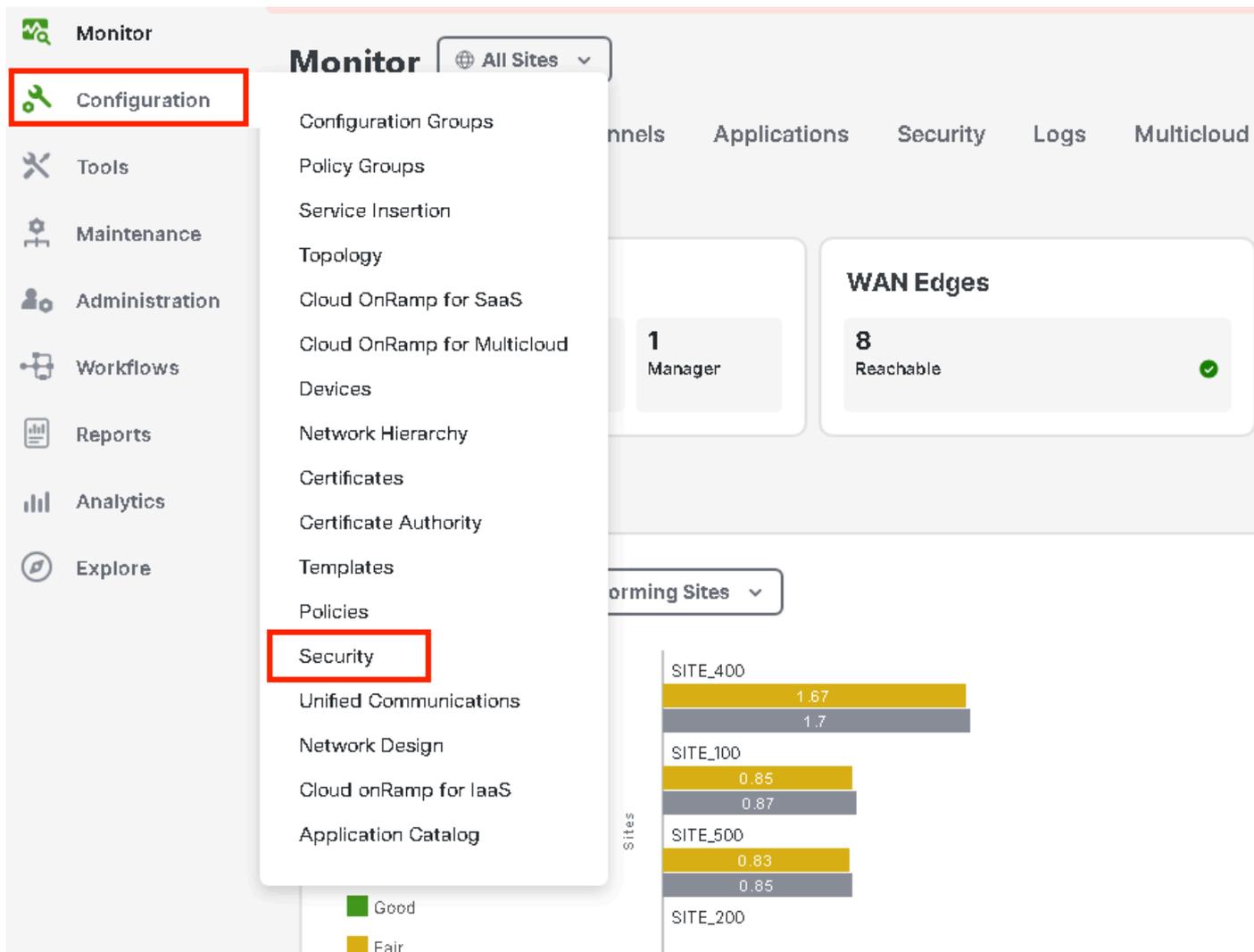
この記事では、カテゴリ、レピュテーション、または次の例の要件を満たすドメインのブロック/許可リストに基づいて、特定のクライアントのHTTPSトラフィックをブロック/許可するようにURLフィルタリングを設定する方法について説明します。

- ゲストVPN Webカテゴリのクライアントからの次のHTTPS要求をブロックします。
  - ゲーム
  - ギャンブル
  - ハッキング
  - 違法薬物
- Webレピュテーションが60以下のゲストVPN上のクライアントからWebサイトへのHTTPS URL要求はすべてブロックする必要があります。
- ゲストVPN上のクライアントからWebサイトへのHTTP(s)要求は、Facebook、Instagram、およびYouTubeをブロックし、google.comおよびyahoo.comへのアクセスは許可します。

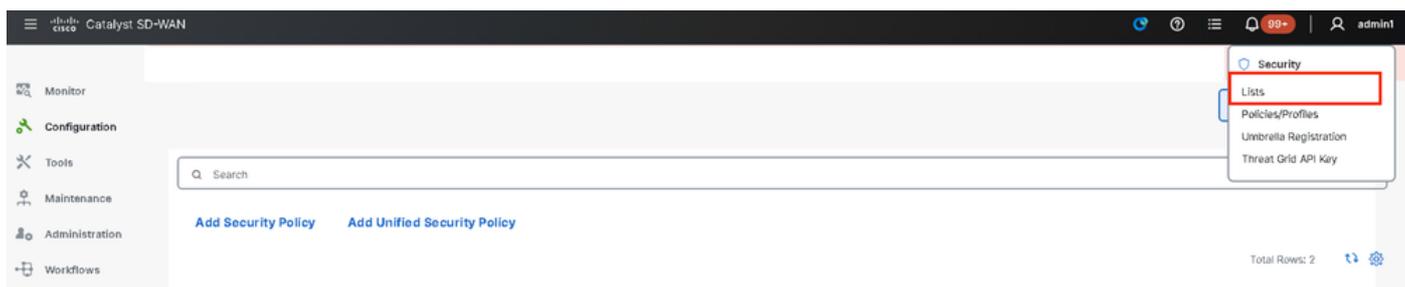
URLフィルタリングを設定するには：

#### 対象のURLリストの作成

1. Cisco SD-WAN Managerメニューで、左側のパネルにあるConfiguration > Securityタブに移動します。



Allowlist URL ListまたはBlocklist URL Listを作成または管理するには、ページ右上のCustom OptionsドロップダウンメニューからListsを選択します。



左側のペインでAllow URLs Listsをクリックし、New Allow URLs Listを作成します。

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 Allow URL List](#)

Name	Entries	Reference Count	Update
No data available			

- 「URLリスト名」フィールドに、最大32文字（文字、数字、ハイフン、アンダースコアのみ）で構成されるリスト名を入力します。
- URLフィールドに、リストに含めるURLをカンマで区切って入力します。Importボタンを使用して、アクセス可能な保存場所からリストを追加することもできます。
- 終了したら Add をクリックします。

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

[New Allow URL List](#)

Allow URL List Name\*

Guest\_Allow

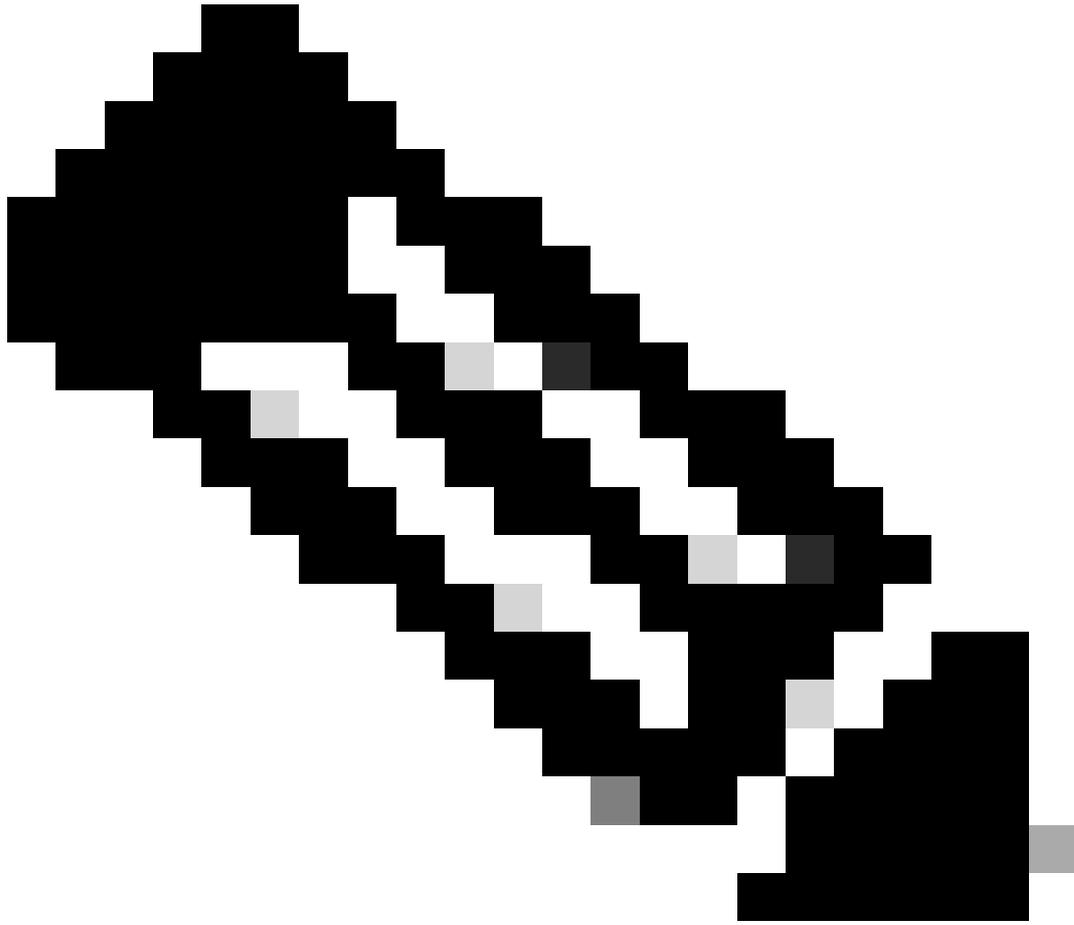
Add Allow URL \*

www.google.com, www.yahoo.com

[Import](#)

Add

Cancel



注：許可リストとブロックリストのドメイン名に正規表現パターンを使用することを検討できます

---

左側のペインでBlock URLs Listsをクリックし、New Block URL Listを作成します。

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
------	---------	-----------------

- 「URLリスト名」フィールドに、最大32文字（文字、数字、ハイフン、アンダースコアのみ）で構成されるリスト名を入力します
- URLフィールドに、リストに含めるURLをカンマで区切って入力します。Importボタンを使用して、アクセス可能な保存場所からリストを追加することもできます。
- 終了したら Add をクリックします。

**New Block URL List**

Block URL List Name\*

Guest\_Block

Add Block URL \*

www.youtube.com,www.facebook.com,instagram.com

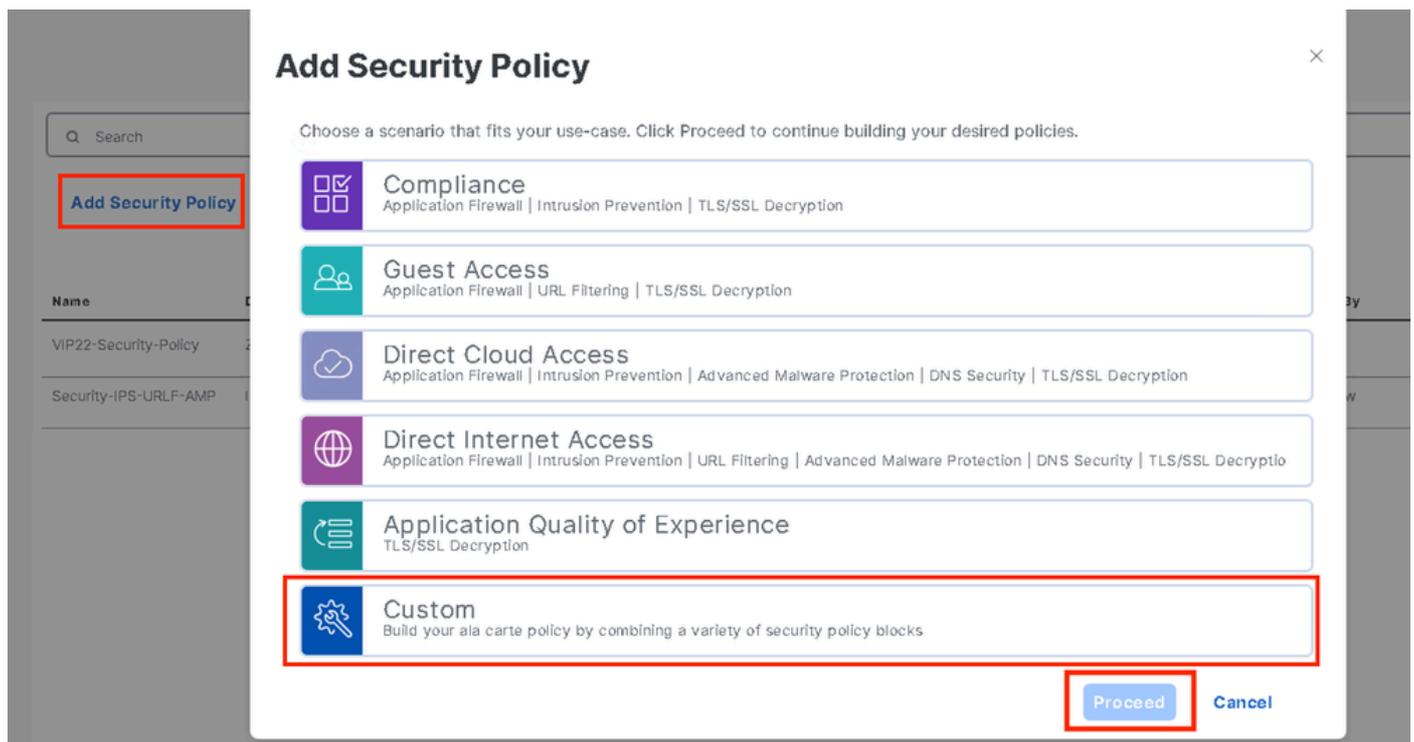
Import

Add Cancel

## セキュリティポリシーの作成

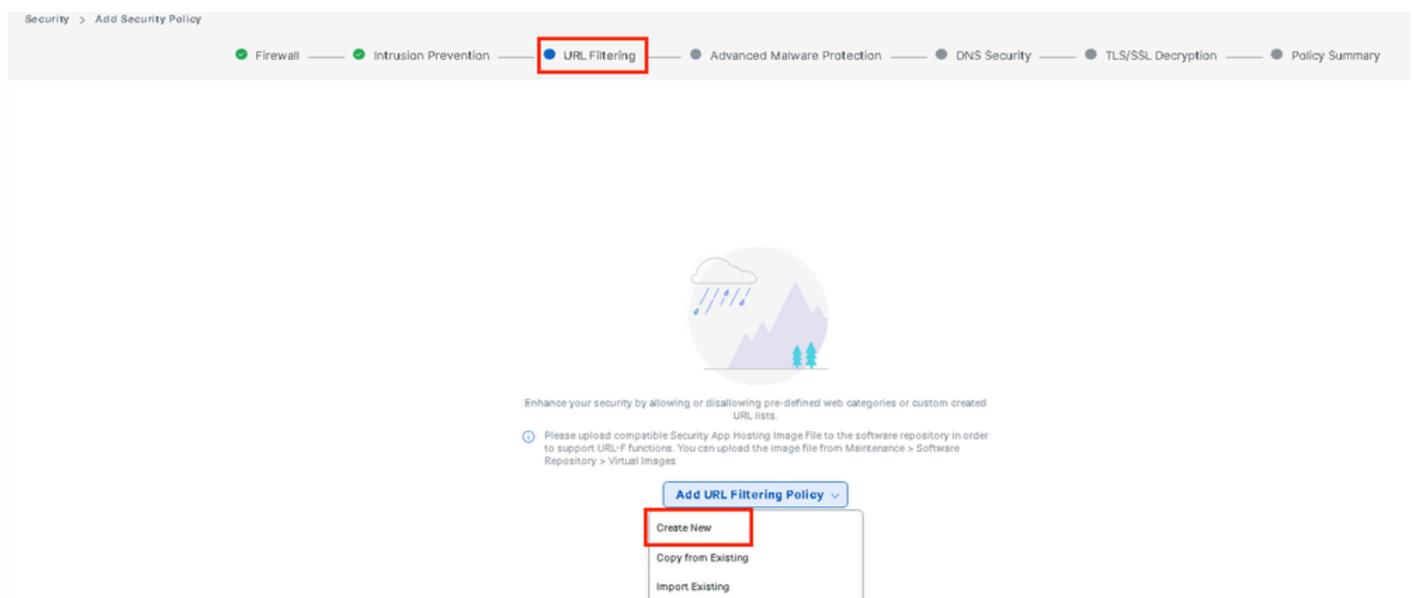
2. Cisco SD-WAN Managerメニューで、Configuration > Securityの順に移動し、Add new security policyをクリックします。セキュリティポリシーの追加ウィザードが開き、さまざまなユースケースのシナリオが表示されるか、リストの既存のポリシーが使用されます。ウィザードでcustomを

選択し、ProceedをクリックしてURLフィルタリングポリシーを追加します。

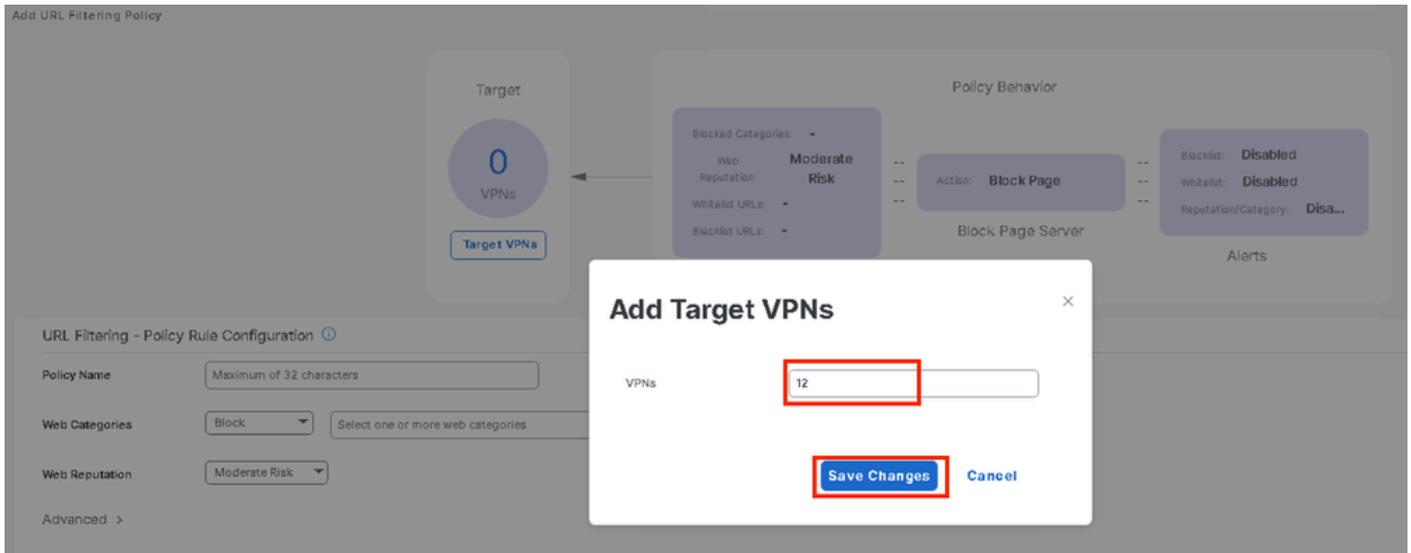


注: [セキュリティポリシーの追加]で、URLフィルタリングをサポートするシナリオ (ゲストアクセス、ダイレクトインターネットアクセス、またはカスタム) を選択します。

Add Security Policyウィザードで、URL Filteringウィンドウが表示されるまでNextをクリックします。ここで、URL Filtering > Add URL Filtering Policy > Create Newの順に選択して、URL Filteringポリシーを作成します。[Next] をクリックします。



Add Target VPNsウィザードでTarget VPNsをクリックして、必要な数のVPNを追加します。



- Policy Nameフィールドにポリシー名を入力します。
- [Webカテゴリ]ドロップダウンからいずれかのオプションを選択し、[ブロック]を選択すると、選択したカテゴリに一致するWebサイトがブロックされます。

ブロック：選択したカテゴリに一致するWebサイトをブロックします。

許可：選択したカテゴリに一致するWebサイトを許可します。

ドロップダウンメニューからWebレピュテーションを選択し、Moderate Riskに設定します。レピュテーションスコアが60以下のURLはすべてブロックされます。

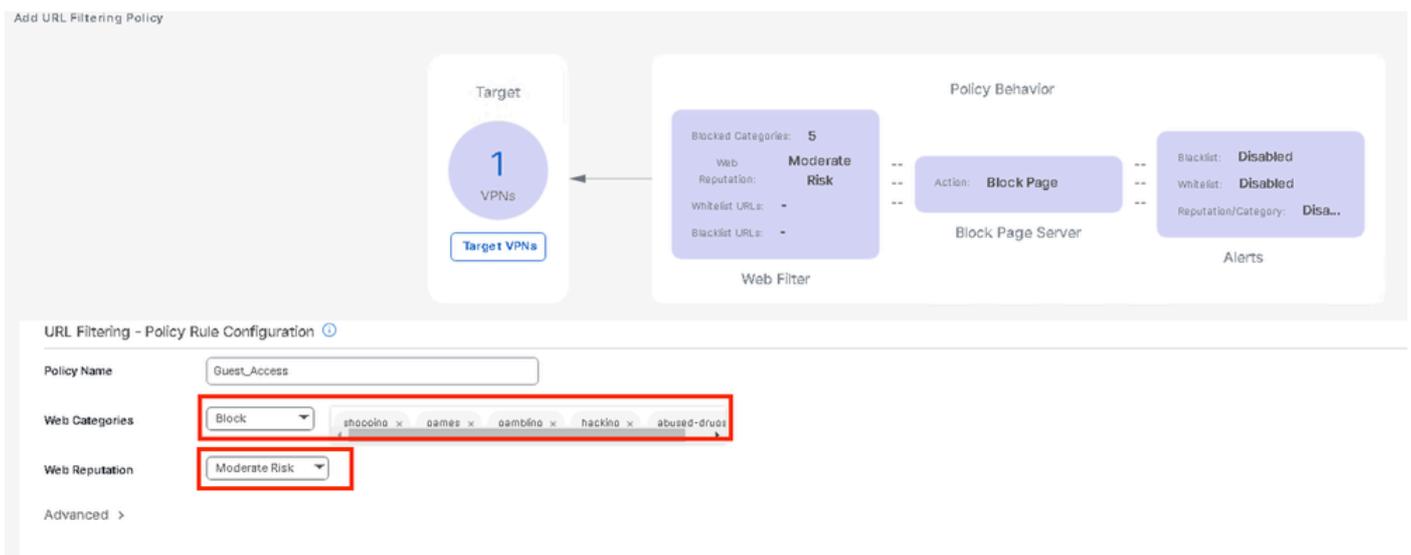
高リスク：レピュテーションスコアは0 ~ 20。

不審：レピュテーションスコアは0 ~ 40。

中程度のリスク：レピュテーションスコア0 ~ 60

低リスク：レピュテーションスコアは0 ~ 80

Trustworthy:レピュテーションスコア0 ~ 100。



Advancedで、必要に応じて、Allowlist URL Listまたはblocklist URL Listドロップダウンメニューから既存のリストを選択するか、新しいリストを作成します。

Advanced ▾

**Whitelist URL List**

**Blacklist URL List**  **Guest\_Allow**

<b>Guest_Allow</b>	www\.google\.com www\.yahoo\.com
--------------------	-------------------------------------

Block Page Server

Block Page Content

**Default Content Header**

Content Body

**Blacklist URL List**

Block Page Server

Block Page Content

**Default Content Header**

Content Body

Redirect URL ⓘ

**Guest\_Block**

<b>Guest_Block</b>	www\.youtube\.com www\.facebook\.com instagram.com
--------------------	--

必要に応じて、[ブロックページコンテンツ]の下のコンテンツ本体を変更し、すべての通知が選択されていることを確認します。

Save URL filtering Policyをクリックして、URLフィルタリングポリシーを追加します。

## 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

Policy Summaryページが表示されるまでNextをクリックします。

各フィールドにSecurity Policy NameとSecurity Policy Descriptionを入力します。

● 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

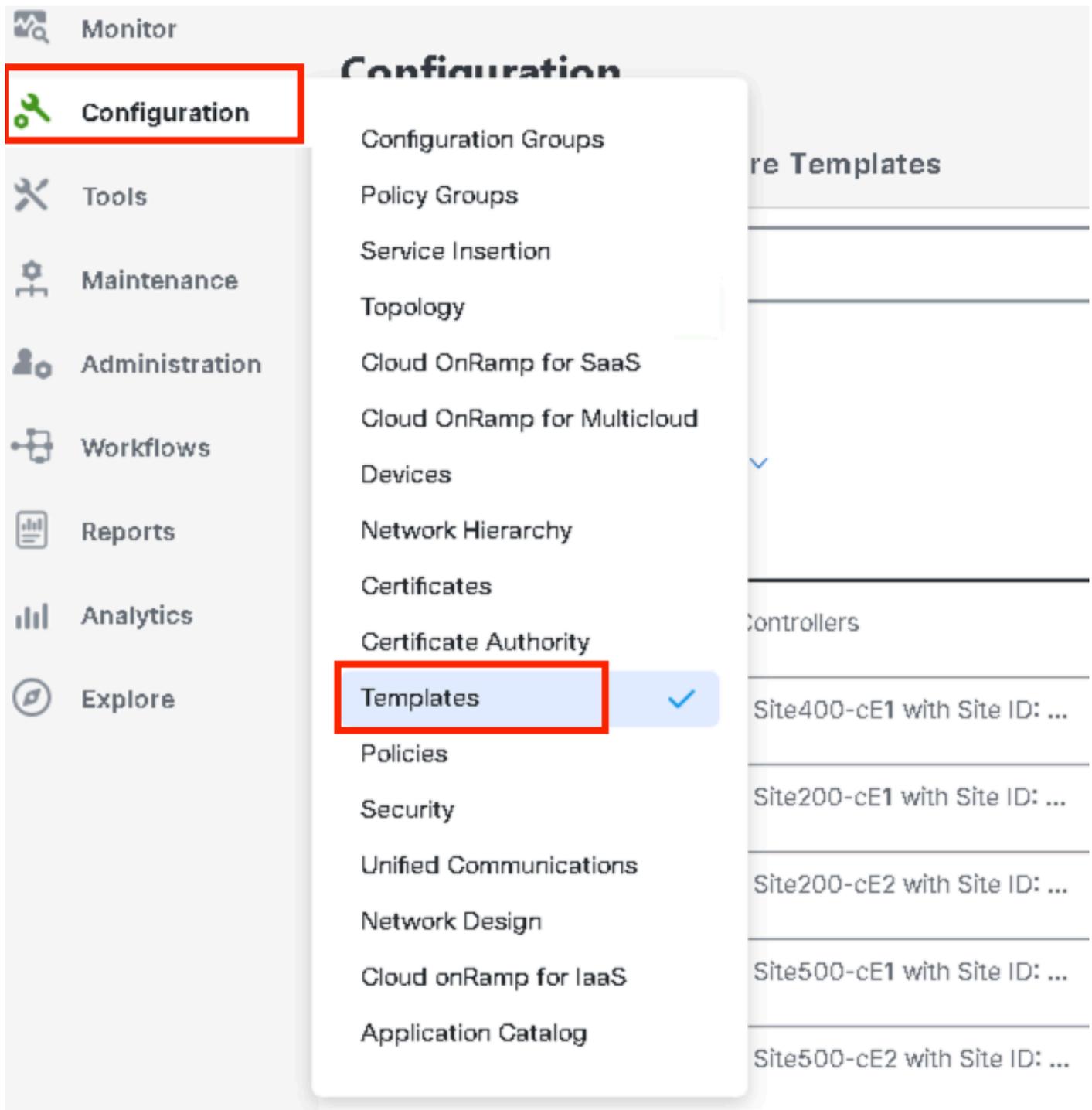
Failure Mode

Back   Cancel

## デバイスへのセキュリティポリシーの適用

デバイスにセキュリティポリシーを適用するには、次の手順を実行します。

Cisco SD-WAN Managerメニューから、Configuration > Templatesの順に選択します。



Device Templatesをクリックし、Editをクリックします。

**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-4616-8bc7-88d2d2978...	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

Additional Templatesをクリックします。

**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

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

- Security Policy ドロップダウンリストから、以前に Guest\_URL\_Policy の下で設定したポリシーの名前を選択し、Update をクリックします。

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

デバイスをクリックし、設定が正しいことを確認して、Config Diff と Side by Side Diff をクリック

します。Configure Devicesをクリックします。

The screenshot displays the vManage configuration interface. At the top left, the 'Device Template' section shows the ID 'fc862ea4-e57e-4616-8...' and a 'Total' of 1 device. A 'Device list' section contains a search filter and a list of devices, with one device highlighted in blue: 'CBK-C1881F22-C89F-A311-DEA7-482A978D089A' with IP '192.168.1.11301'. A 'Configure Devi...' button is visible below the list.

The main area is titled 'Local Configuration vs. New Configuration' and shows a comparison of configurations. The left column lists system parameters, and the right column shows the corresponding configuration values. A red box highlights the 'Configure Devices' button at the bottom of the interface.

Line	Local Configuration	New Configuration
1	system	
2	ztp-status	in-progress
3	device-model	vedge-C8000V
4	gps-location latitude	-23.60911
5	gps-location longitude	-46.69768
6	system-ip	1.1.30.1
7	overlay-id	1
8	site-id	300
9	no transport-gateway	enable
10	port-offset	0
11	control-session-pps	300
12	admin-tech-on-failure	

```
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
```

vManageは、セキュリティポリシーを使用してデバイステンプレートを正常に構成し、エッジデバイスにUTDパッケージをインストールしました。

**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(1.1.30.1)  
 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 apid utd

[26-Jul-2024 13:57:40 PDT] Device: Successfully installed apid utd

[26-Jul-2024 13:59:07 PDT] Device: Verified apid utd in running state

[26-Jul-2024 13:59:07 PDT] Device: Successfully verified apid: utd

[26-Jul-2024 13:59:08 PDT] Device: Config applied successfully

[26-Jul-2024 13:59:08 PDT] Template successfully attached to device

## URLフィルタの変更

URLフィルタリングポリシーを変更するには、次の手順を実行します。

1. Cisco SD-WAN Managerメニューから、Configuration > Securityの順に選択します。
2. Security画面で、Custom Optionsドロップダウンメニューをクリックし、Policies/Profilesを選択します。

The screenshot shows the Cisco SD-WAN Manager interface. On the left is a navigation menu with 'Configuration' selected. The main content area shows the 'Security' section with a search bar and two buttons: 'Add Security Policy' and 'Add Unified Security Policy'. Below is a table with columns: Name, Description, Use Case, Policy Mode, Devices Attached, DeviceTemplates/ConfigGroups, Updated By, and Last Updated. A dropdown menu is open in the top right corner, showing 'Security' as the selected category and 'Policies/Profiles' as the selected option, which is highlighted with a red box. Other options in the dropdown include 'Lists', 'Umbrella Registration', and 'Threat Grid API Key'.

左側のタブで、変更するポリシーのURL Filteringをクリックし、3個のドット(...)をクリックしてEditを選択します。

Security > URL Filtering Custom Options

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

- Firewall
- Intrusion Prevention
- URL Filtering
- Advanced Malware Protection
- DNS Security
- TLS/SSL Decryption
- TLS/SSL Profile
- Advanced Inspection Profile

Add URL Filtering Policy (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	...

Graphical Preview View  
Edit

必要に応じてポリシーを変更し、Save URL Filtering Policyをクリックします。

Target

1

VPNs

Target VPNs

Block Categories: 5

Web Reputation: **Moderate Risk**

Whitelist URLs: Guest\_All...

Blacklist URLs: Guest\_Blo...

Web Filter

Policy Behavior

Action: **Block Page**

Block Page Server

Blacklist: **Enabled**

Whitelist: **Enabled**

Reputation/Category: **Ena...**

Alerts

URL Filtering - Policy Rule Configuration

Policy Mode: Security

Policy Name:

Web Categories: Block abused-drugs x games x gambling x social-network x hack

Save URL Filtering Policy
Cancel

## URLフィルタリングの削除

URLフィルタリングポリシーを削除するには、最初にセキュリティポリシーからポリシーを切り離す必要があります。

Cisco SD-WAN Managerメニューから、Configuration > Securityの順に選択します。

URLフィルタリングポリシーをセキュリティポリシーから切り離すには、次の手順を実行します

。

- URLフィルタリングポリシーを含むセキュリティポリシーの場合は、3個のドット(...)をクリックし、次にEditをクリックします。

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

[Policy Summary]ページが表示されます。URL Filteringタブをクリックします。

削除するポリシーに対して、3ドット(...)をクリックし、Detachを選択します。

Save Policy Changesをクリックします。

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
<b>Guest_Access</b>	urlFiltering	1	admin	24 Jul 2024 11:03:40 PM GMT

- Graphical Preview
- View
- Edit
- Detach**

Preview **Save Policy Changes** Cancel

URLフィルタリングポリシーを削除するには、次の手順を実行します。

Security画面で、Custom Optionsドロップダウンメニューをクリックし、Policies/Profilesを選択して、URL Filteringを選択します。

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

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

Q Search

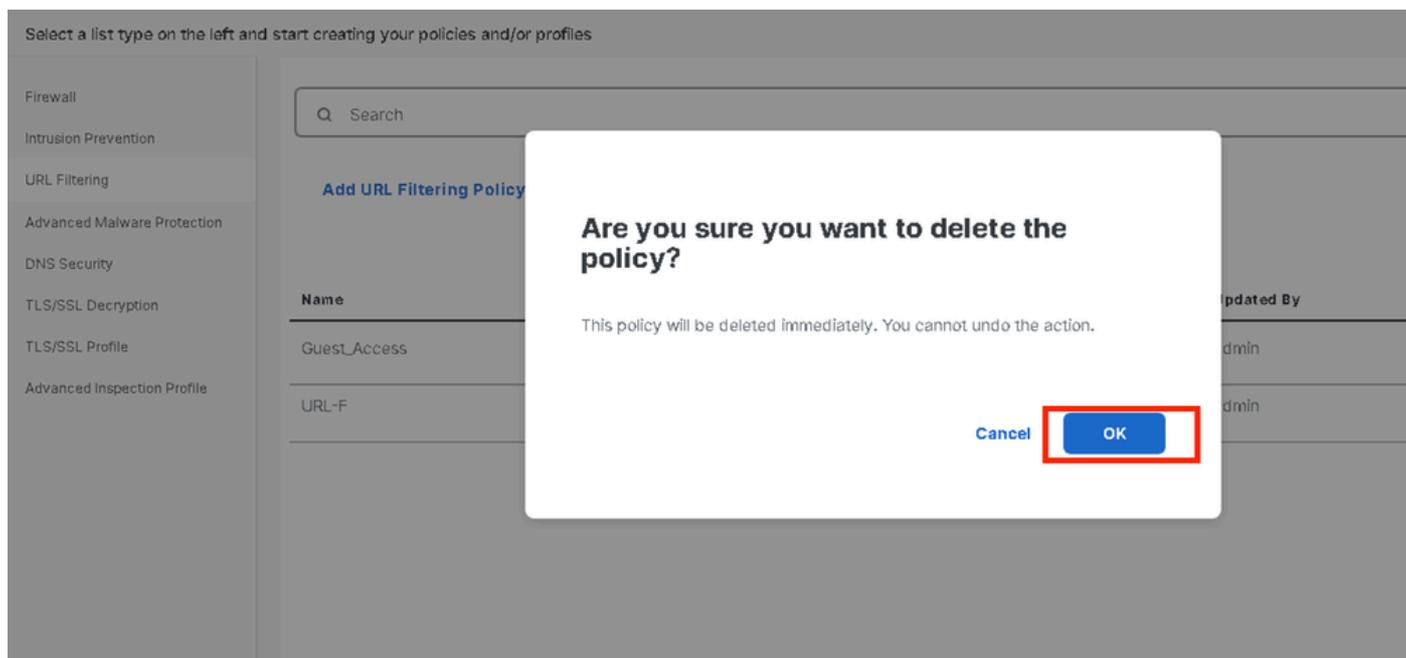
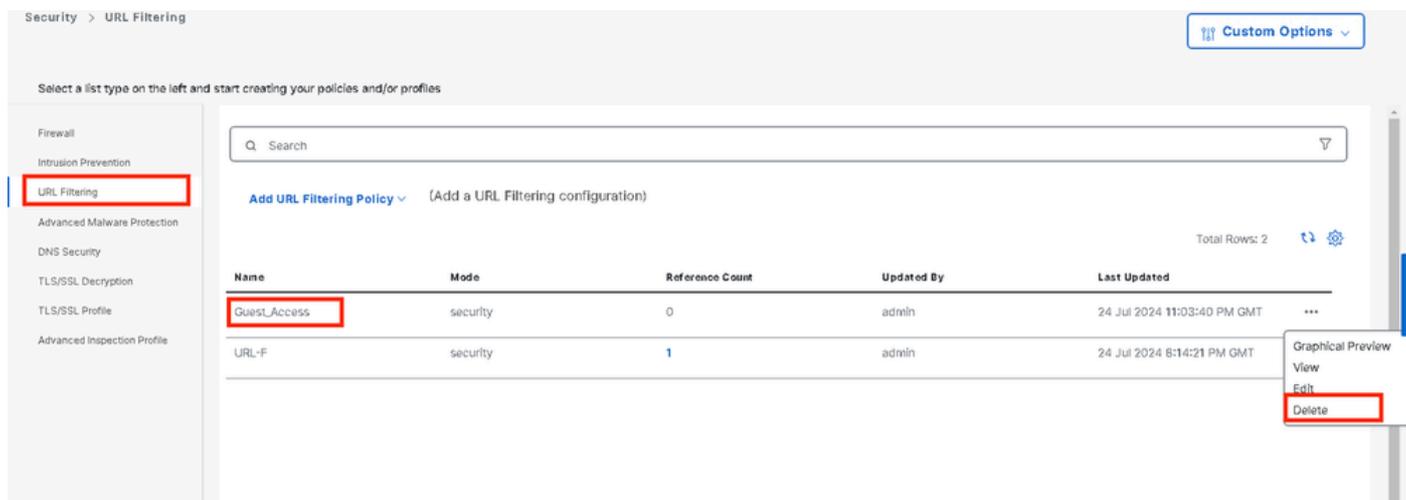
Add Security Policy Add Unified Security Policy

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 ...

削除するポリシーに対して、3つのドット(...)をクリックし、Deleteをクリックします。

OKをクリックします。



## 確認

Cisco UTDバージョンがインストールされているかどうかを確認します。

<#root>

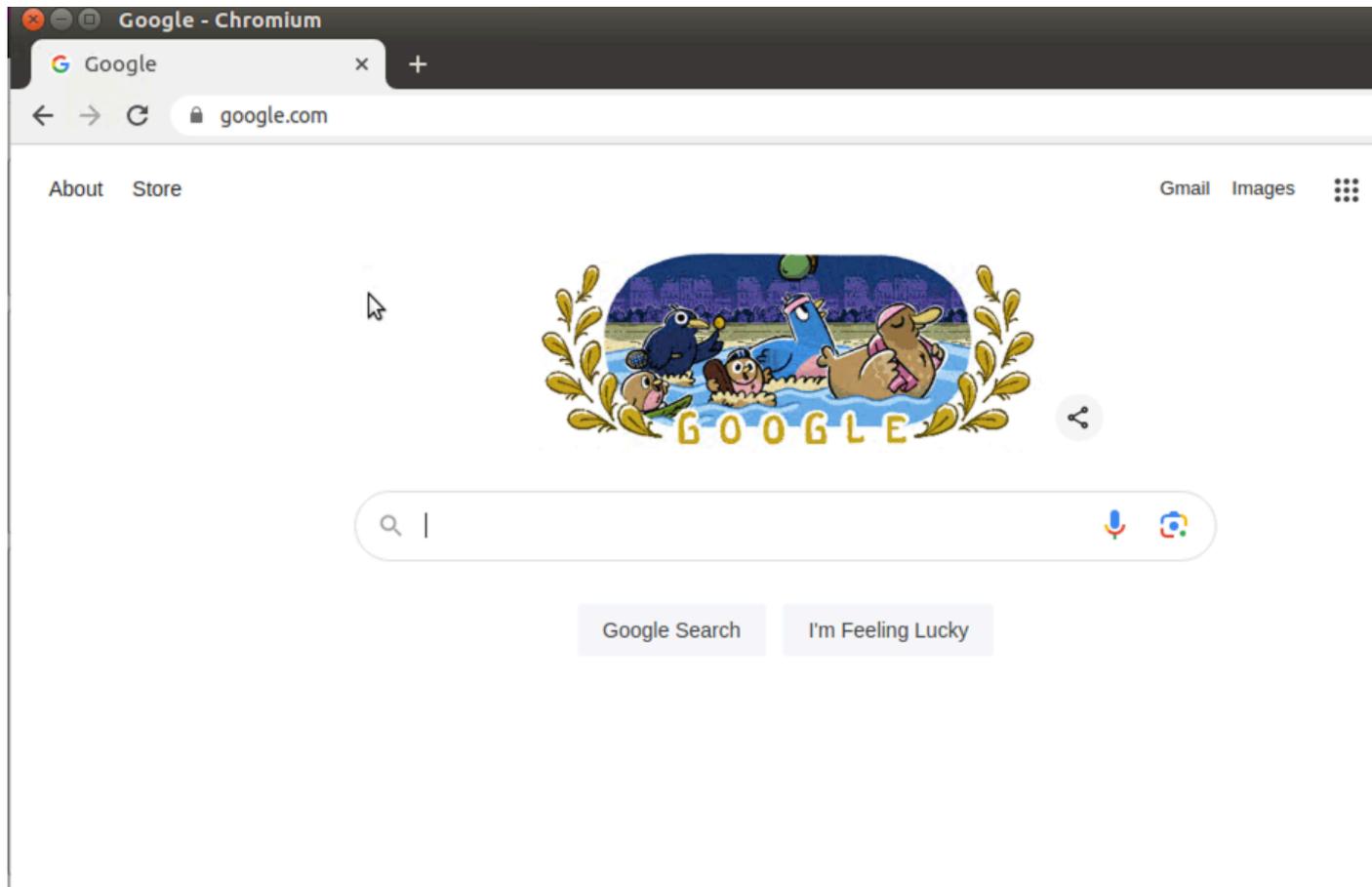
```
Site300-cE1#show utd engine standard version
UTD Virtual-service Name: utd
IOS-XE Recommended UTD Version: 1.0.2_SV3.1.67.0_XE17.14
```

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

UTD Installed Version:

1.0.2\_SV3.1.67.0\_XE17.14

ゲストVPN上のクライアントPCからgoogle.comとyahoo.comを開こうとすると、許可されます。



<#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

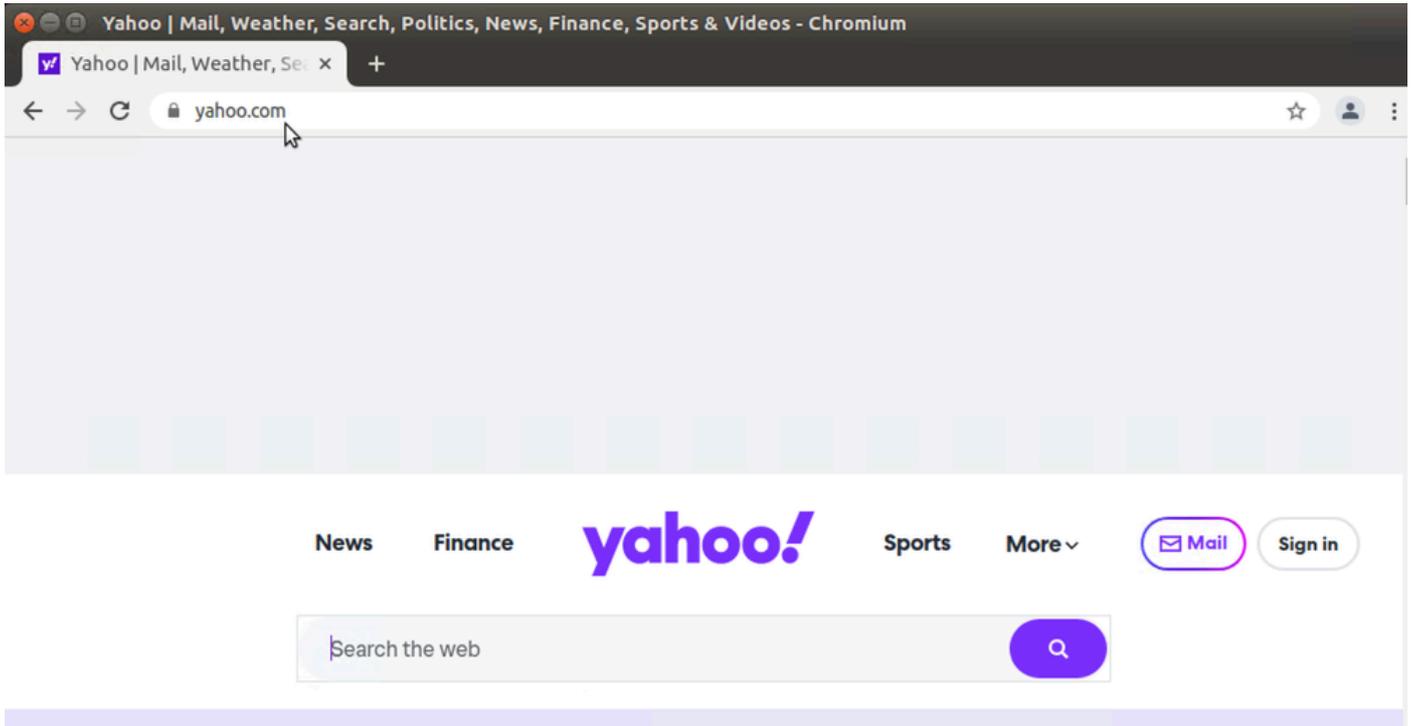
[\*\*]

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

[\*\*]

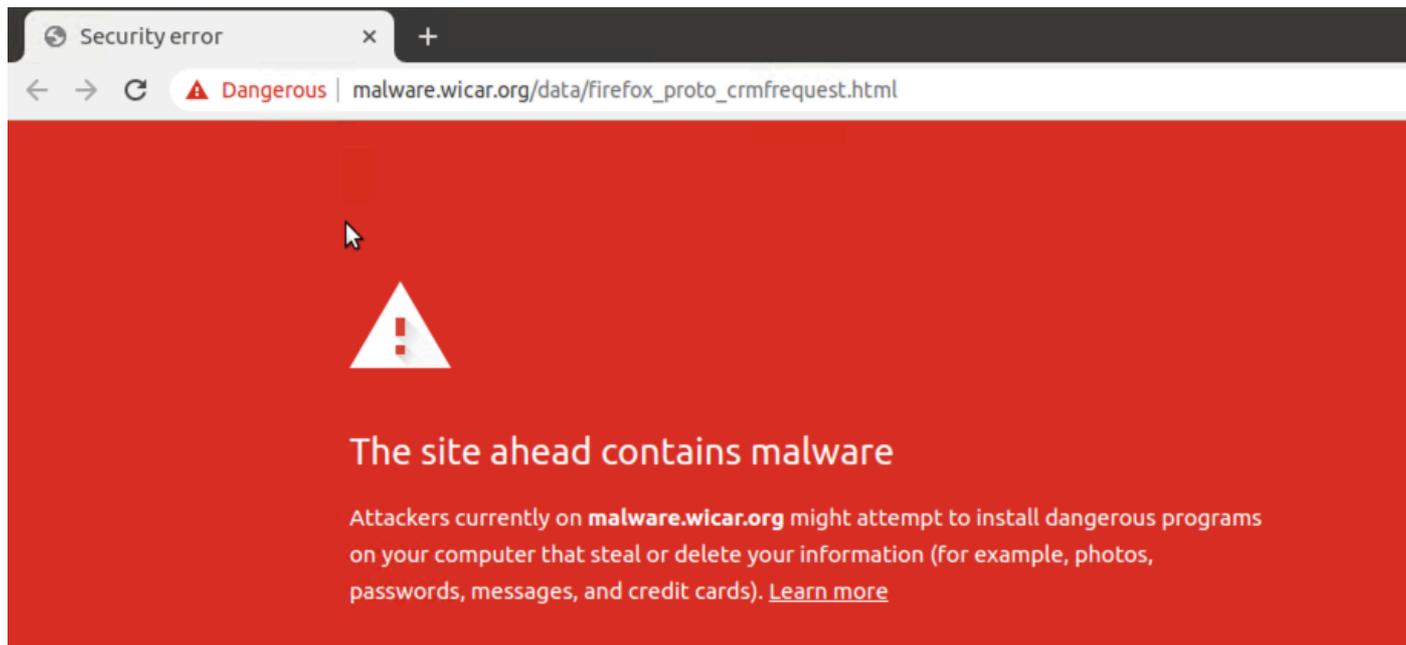
UTD WebFilter Allowlist

[\*\*] [

URL: www.yahoo.com

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

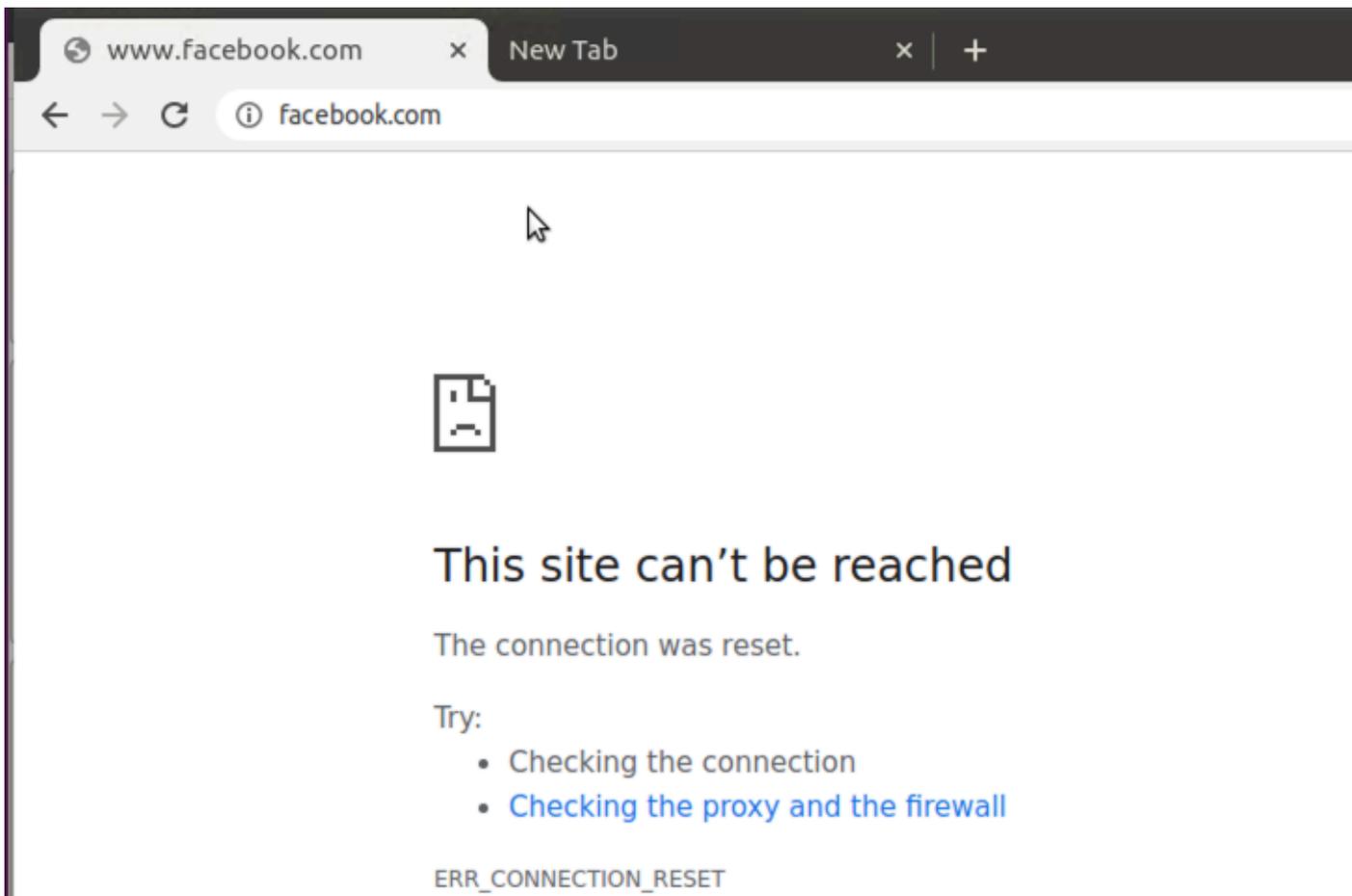
ゲストVPN上のクライアントPCから、レピュテーションスコアが低いWebページや、ブロックされたWebカテゴリの1つからWebページを開こうとすると、URLフィルタリングエンジンはHTTP要求を拒否します。



<#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
```

ゲストVPN上にあるクライアントPCから、Facebook、Instagram、YouTubeを開こうとするとブ  
ロックされます。



<#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

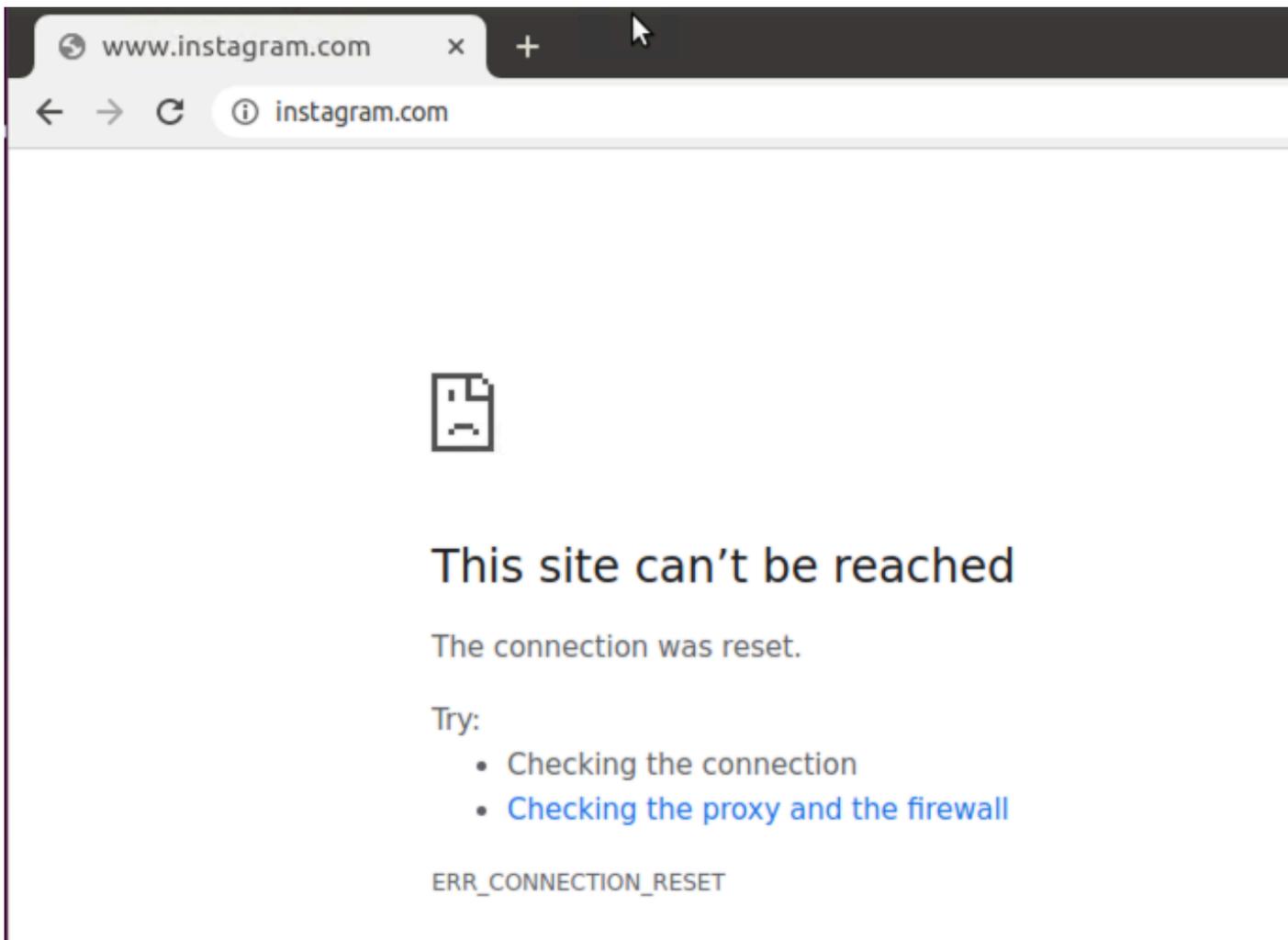
[\*\*]

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

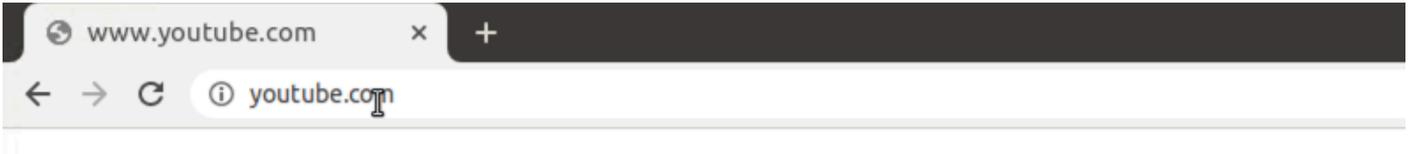
[\*\*]

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 blacklist

[\*\*] [

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 blacklist

[\*\*] [

URL: www.youtube.com

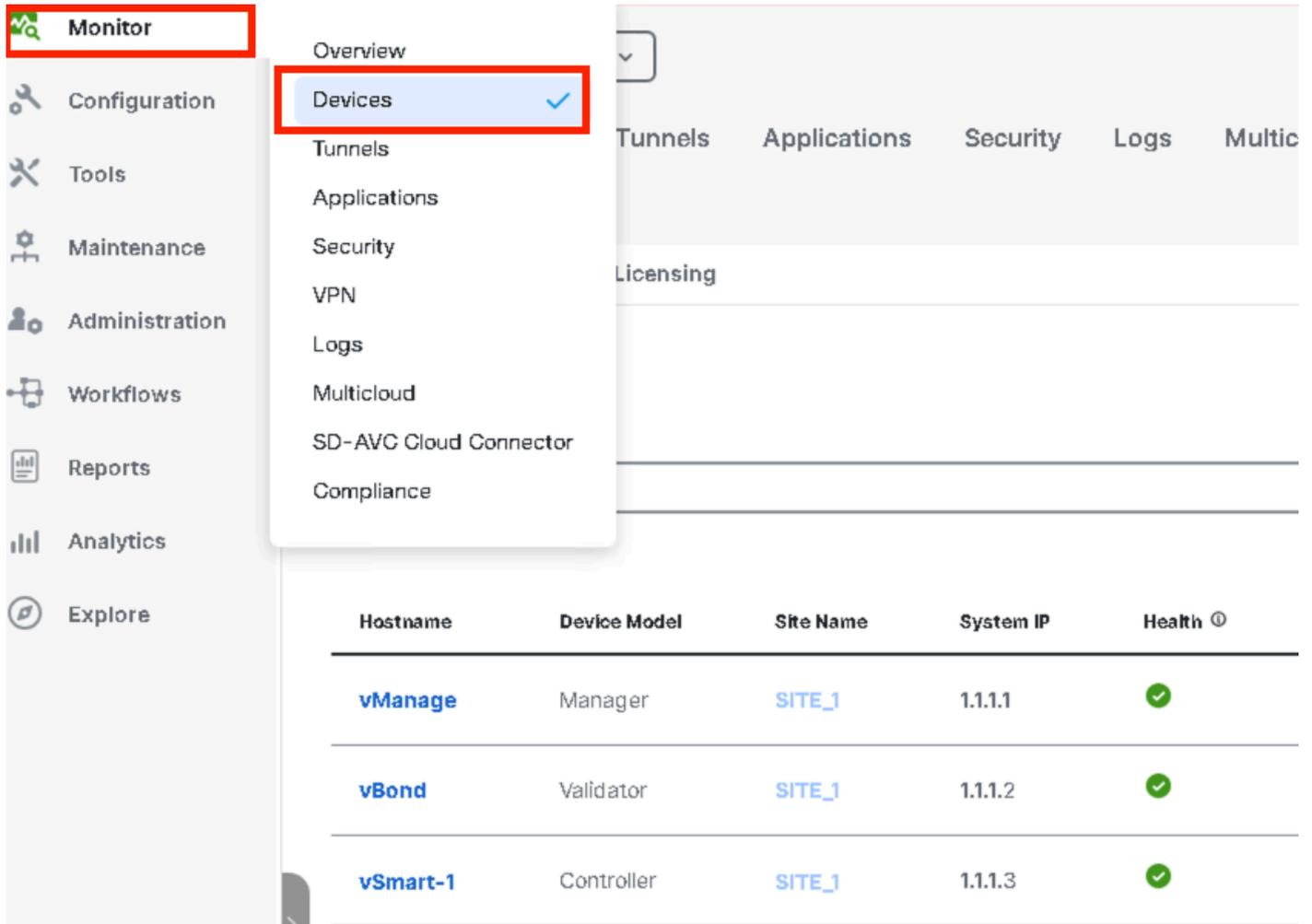
] [VRF: 12] {TCP} 10.32.1.10:54352 -> 142.250.72.206:443

## vManage GUIからのURLフィルタリングのモニタ

次の手順を使用して、Webカテゴリ別に各デバイスのリアルタイムまたは履歴でURLフィルタリングをモニタできます。

Cisco IOS XE Catalyst SD-WANデバイスでブロックまたは許可されているURLをモニタするには、次の手順を実行します。

1. Cisco SD-WAN Managerメニューから、Monitor > Devices > Select Deviceの順に選択します。



2. 左側のペインのSecurity Monitoringで、URL Filteringをクリックします。右側のペインにURLフィルタリング情報が表示されます。

- Blockedをクリックします。ブロックされたURLのセッションカウントが表示されます。
- Allowedをクリックします。許可されたURLのセッションカウントが表示されます。



---

注:UTDがインストールされたバージョンは、UNSUPPORTED状態になることはできません。

---

UTDがonrunning状態かどうかを確認します。

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

UTDヘルスステータスが緑色であることを確認します。

<#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

URLフィルタリング機能が有効になっていることを確認します。

<#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

URLフィルタリングログを表示するには、show utd engine standard logging events url-filteringコマンドを実行します。

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：古いイベントをクリアするには、clear utd engine standard logging eventsコマンドを実行します。

---

UTDコンテナへの入出力パケットをチェックし、ルックアップで遅延が発生します。

```
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
```

## 関連情報

- [Cisco Catalyst SD-WANセキュリティ設定ガイド](#)
- [cEdgeルータへのUTDセキュリティ仮想イメージのインストール](#)
- [UTDおよびURLフィルタリングによるデータパス処理のトラブルシューティング](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。