URLフィルタリングの設定と確認

内容

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

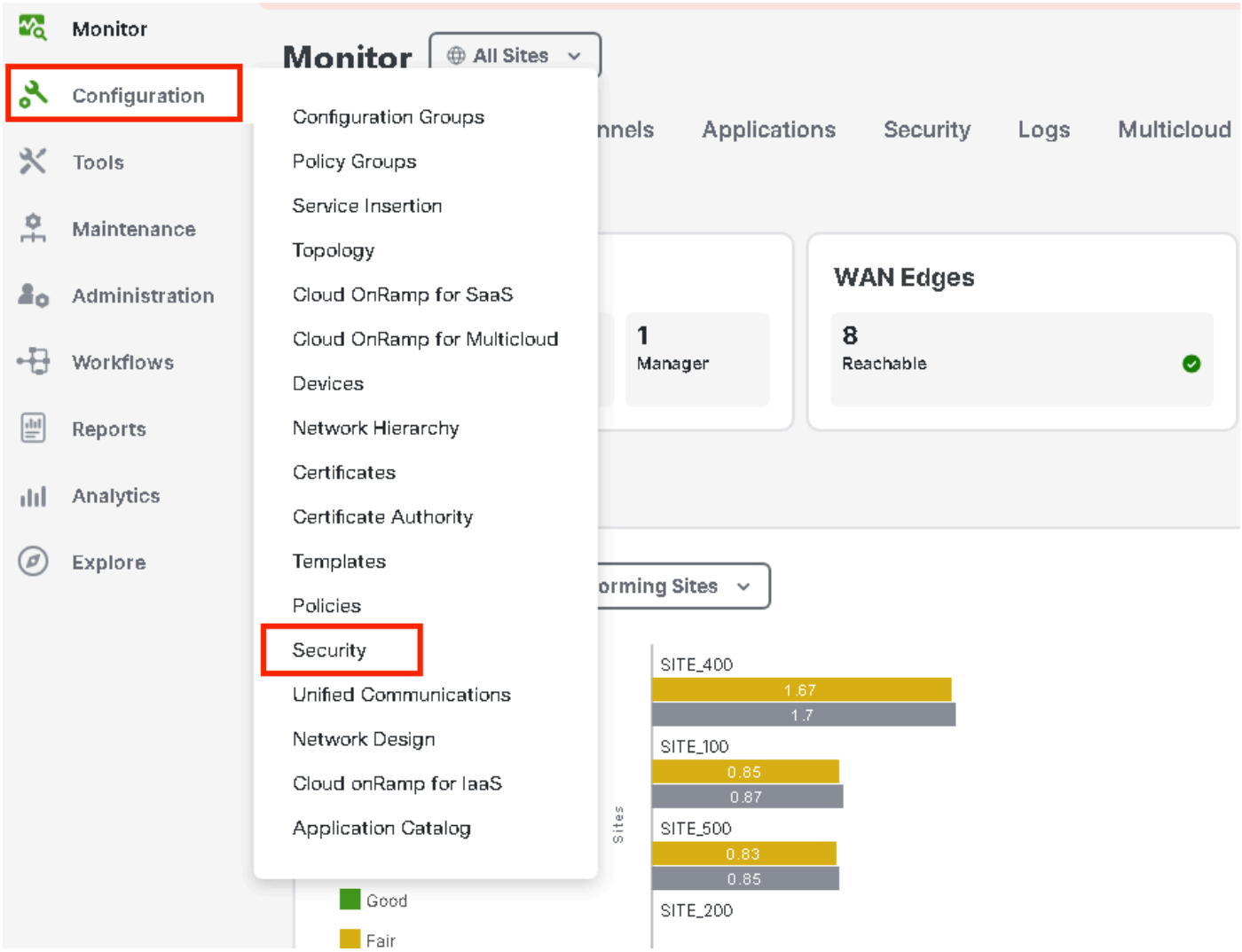
- Webレピュテーションが60以下のゲストVPN上のクライアントからWebサイトへのHTTPS URL要求はすべてブロックする必要があります。

- 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。

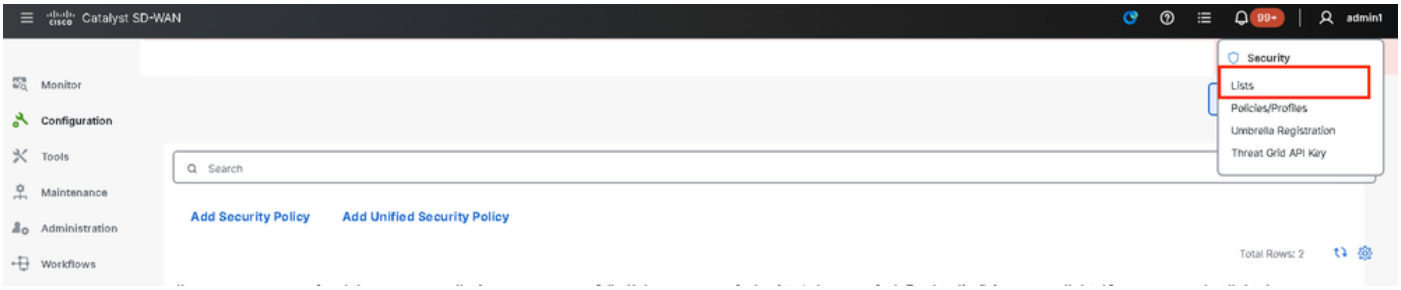
URLフィルタリングを設定するには：

対象のURLリストの作成

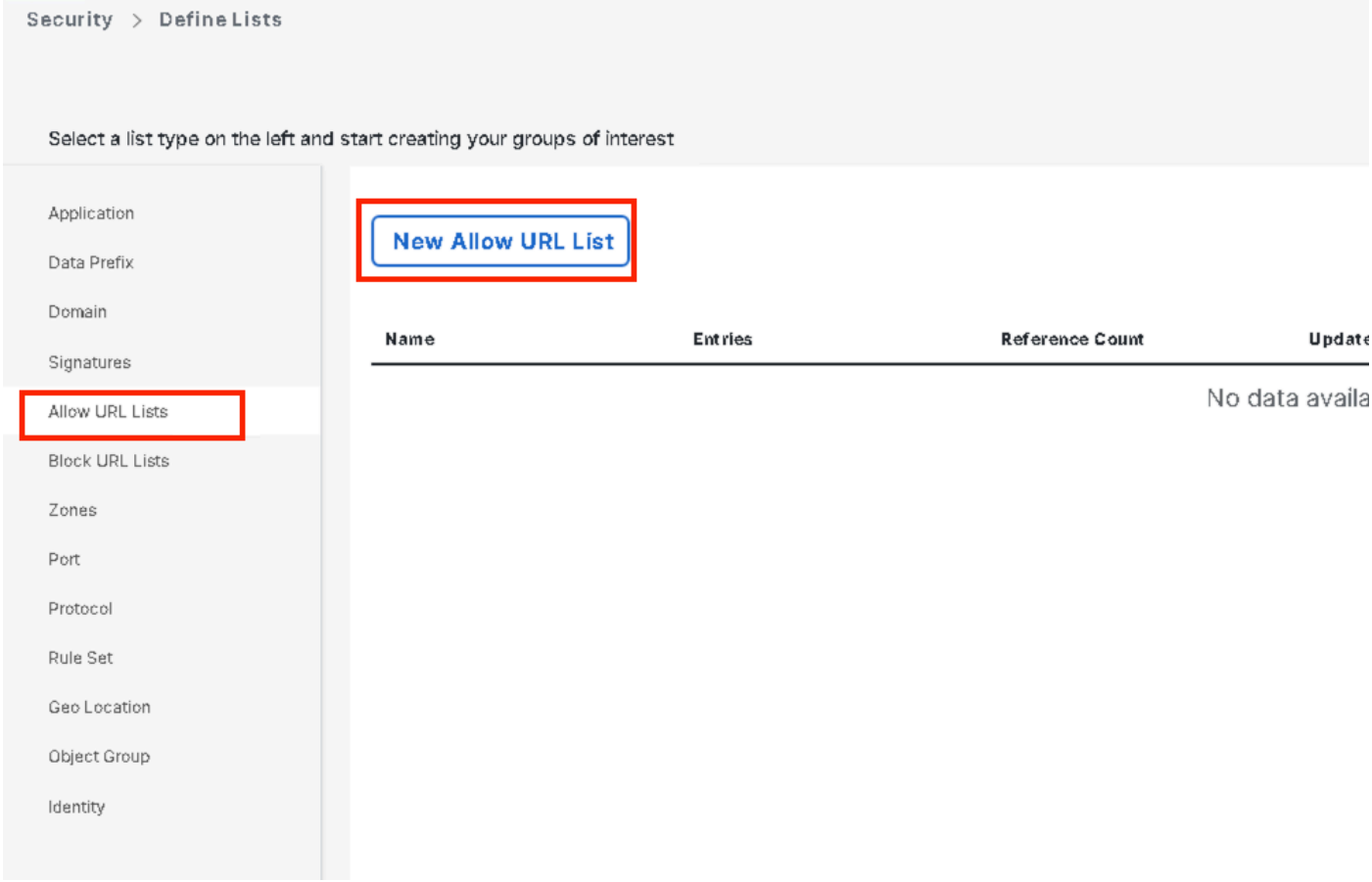
1. Cisco SD-WAN Managerメニューで、左側のパネルにあるConfiguration > Securityタブに移動します。



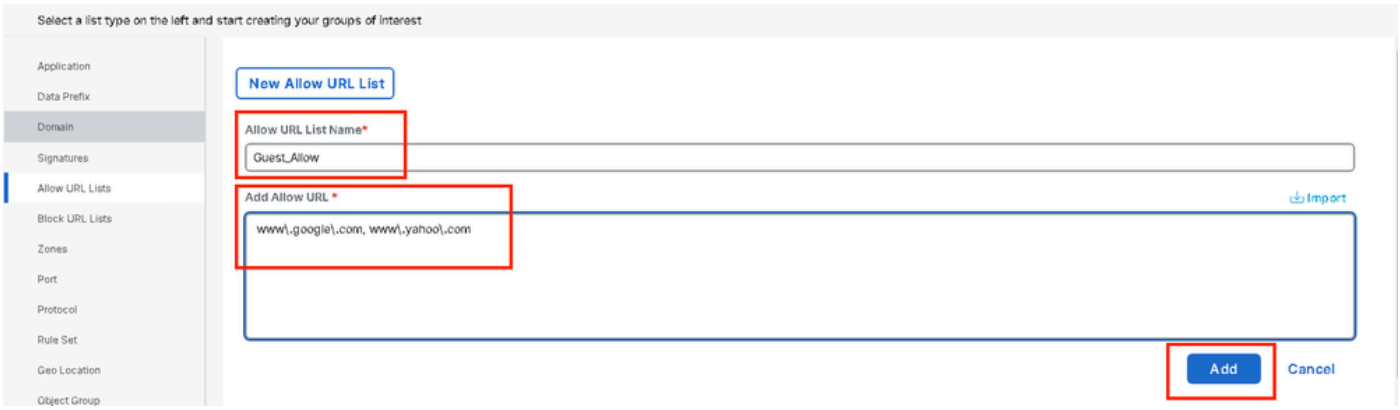
Allowlist URL ListまたはBlocklist URL Listを作成または管理するには、ページ右上のCustom Optionsドロップダウンメニューから**Lists**を選択します。

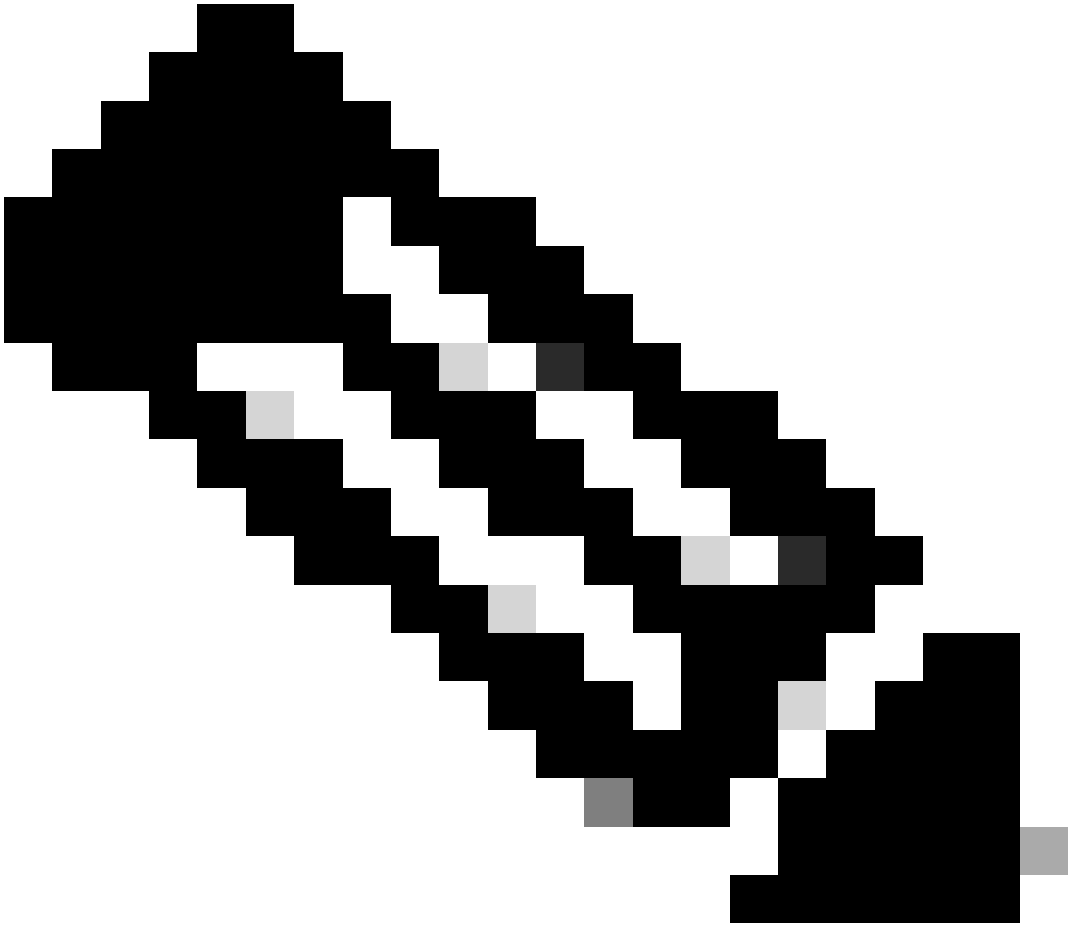


左側のペインでAllow URLs Listsをクリックし、New Allow URLs Listを作成します。



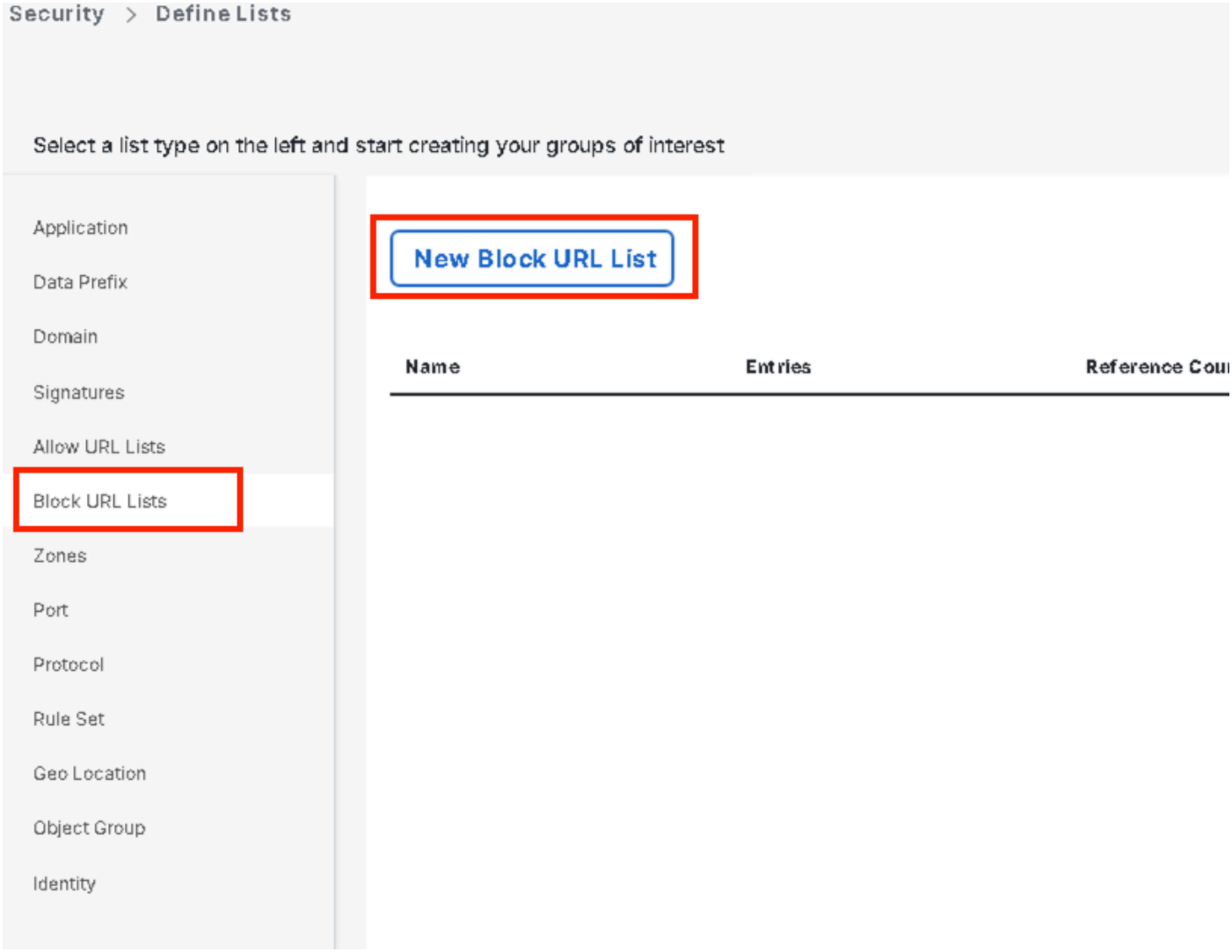
- 「URLリスト名」フィールドに、最大32文字（文字、数字、ハイフン、アンダースコアのみ）で構成されるリスト名を入力します。
- URLフィールドに、リストに含めるURLをカンマで区切って入力します。Importボタンを使用して、アクセス可能な保存場所からリストを追加することもできます。
- 終了したら Add をクリックします。



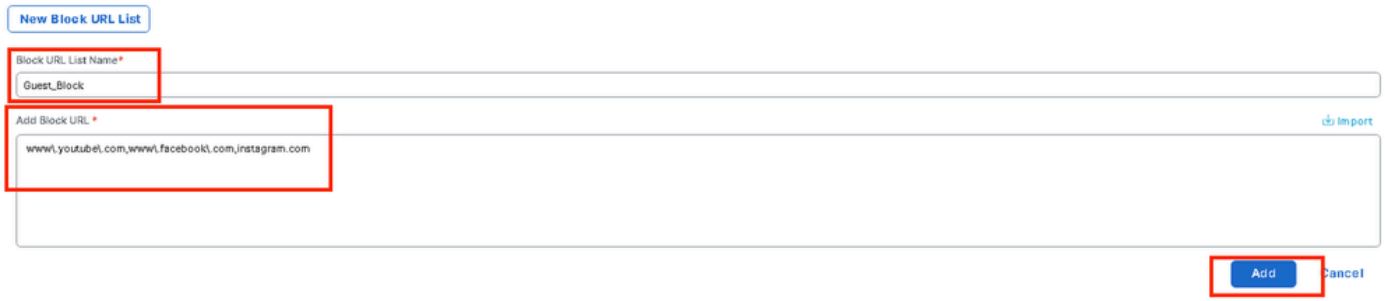


注：許可リストとブロックリストのドメイン名に正規表現パターンを使用することを検討できます

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。



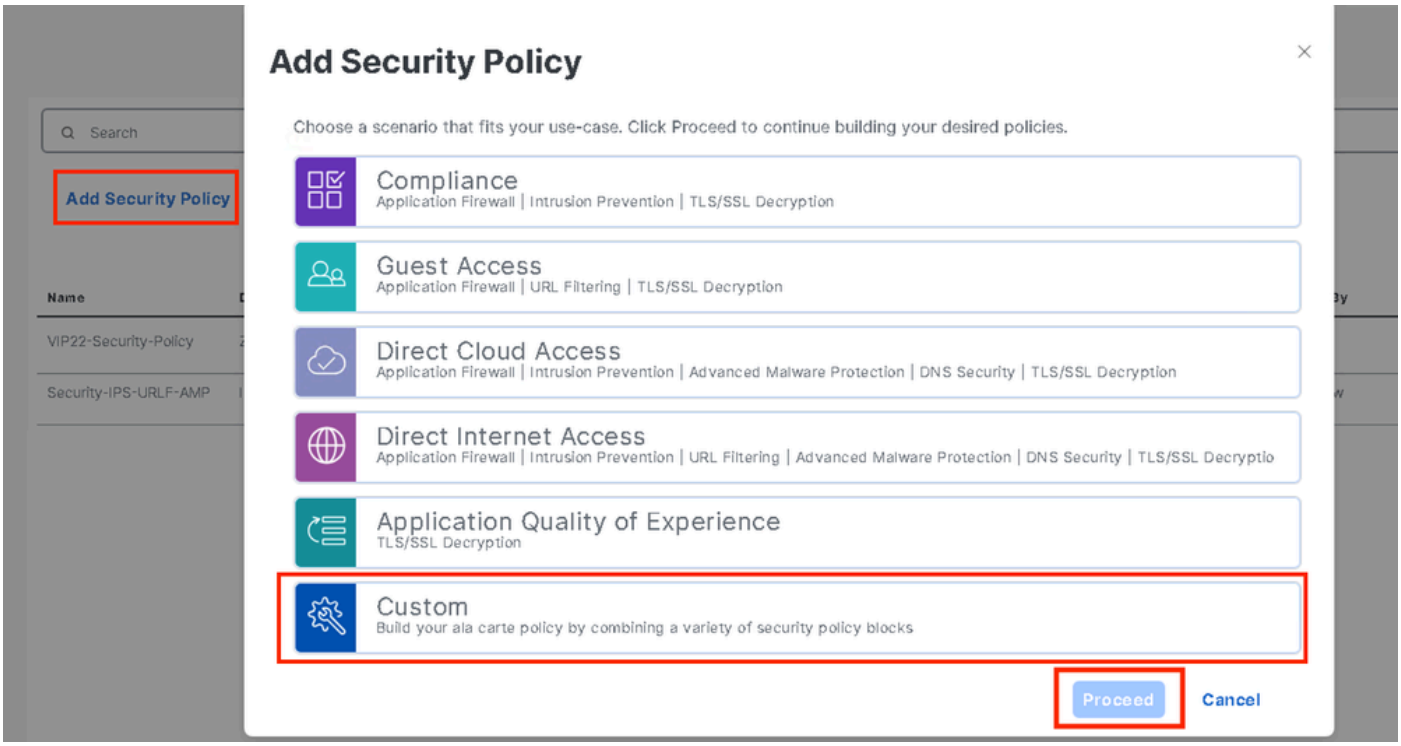
- 「URLリスト名」フィールドに、最大32文字（文字、数字、ハイフン、アンダースコアのみ）で構成されるリスト名を入力します
- URLフィールドに、リストに含めるURLをカンマで区切って入力します。Importボタンを使用して、アクセス可能な保存場所からリストを追加することもできます。
- 終了したら Add をクリックします。



セキュリティポリシーの作成

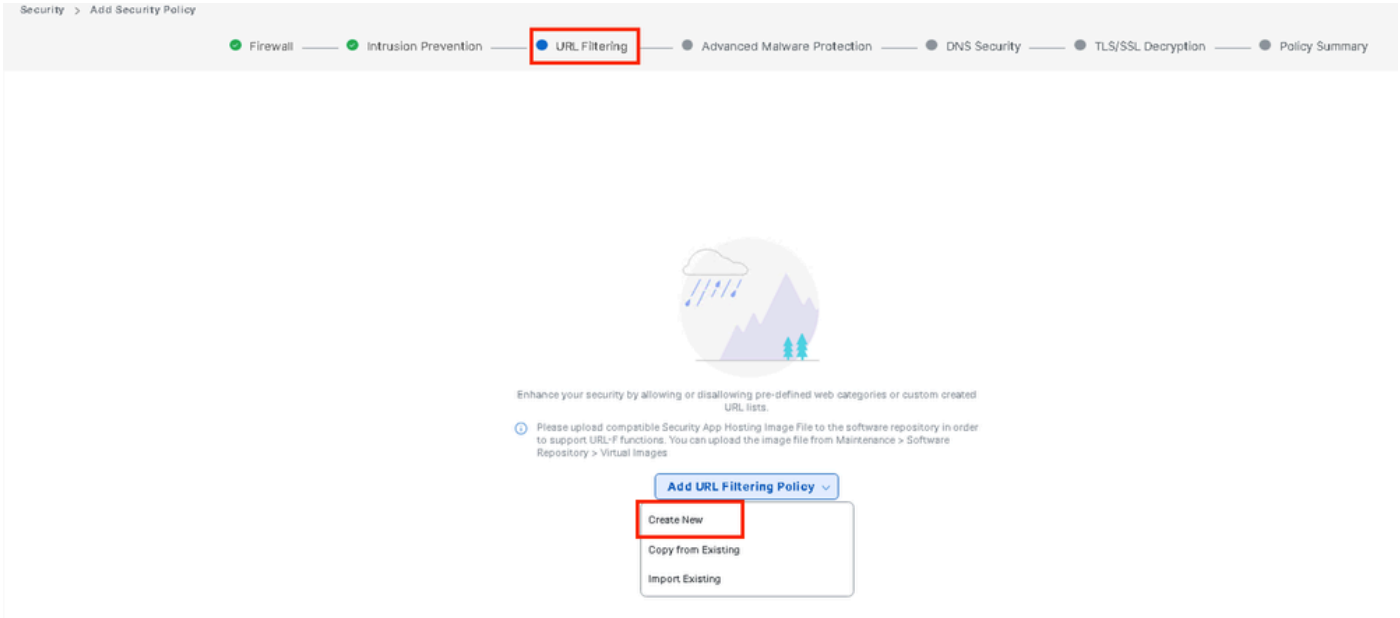
2. Cisco SD-WAN Managerメニューで、Configuration > Securityの順に移動し、Add new security policyをクリックします。セキュリティポリシーの追加ウィザードが開き、さまざまなユースケースのシナリオが表示されるか、リストの既存のポリシーが使用されます。ウィザードでcustomを

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。

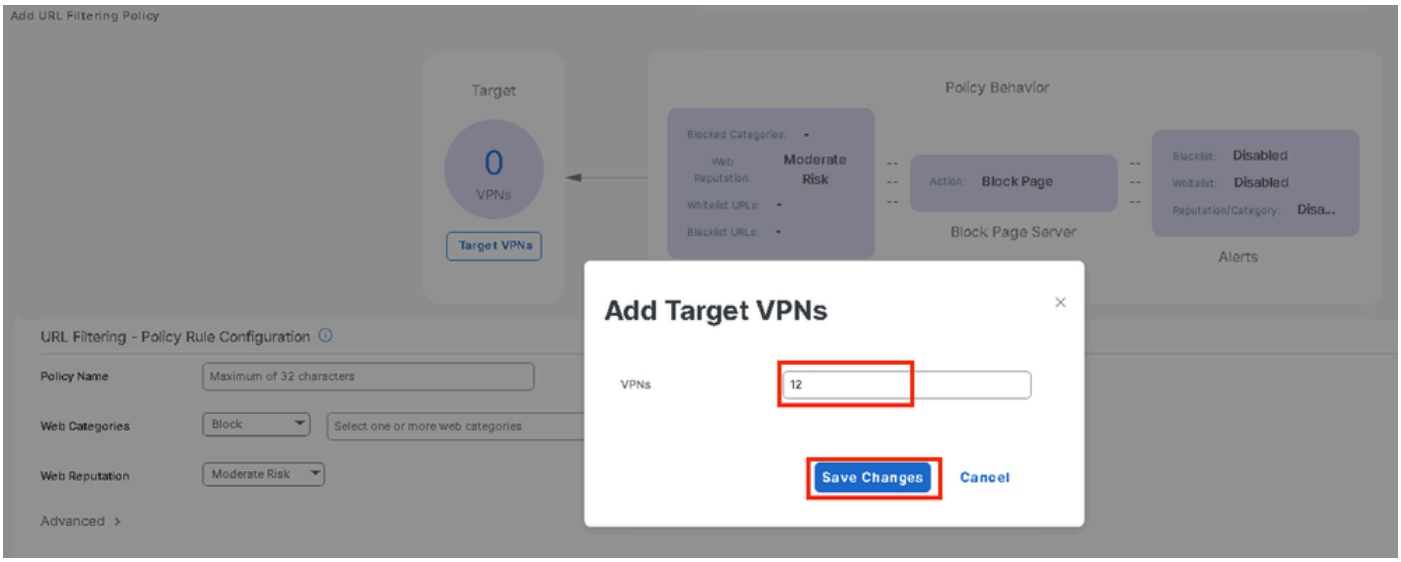


注: [セキュリティポリシーの追加]で、URLフィルタリングをサポートするシナリオ（ゲストアクセス、ダイレクトインターネットアクセス、またはカスタム）を選択します。

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。

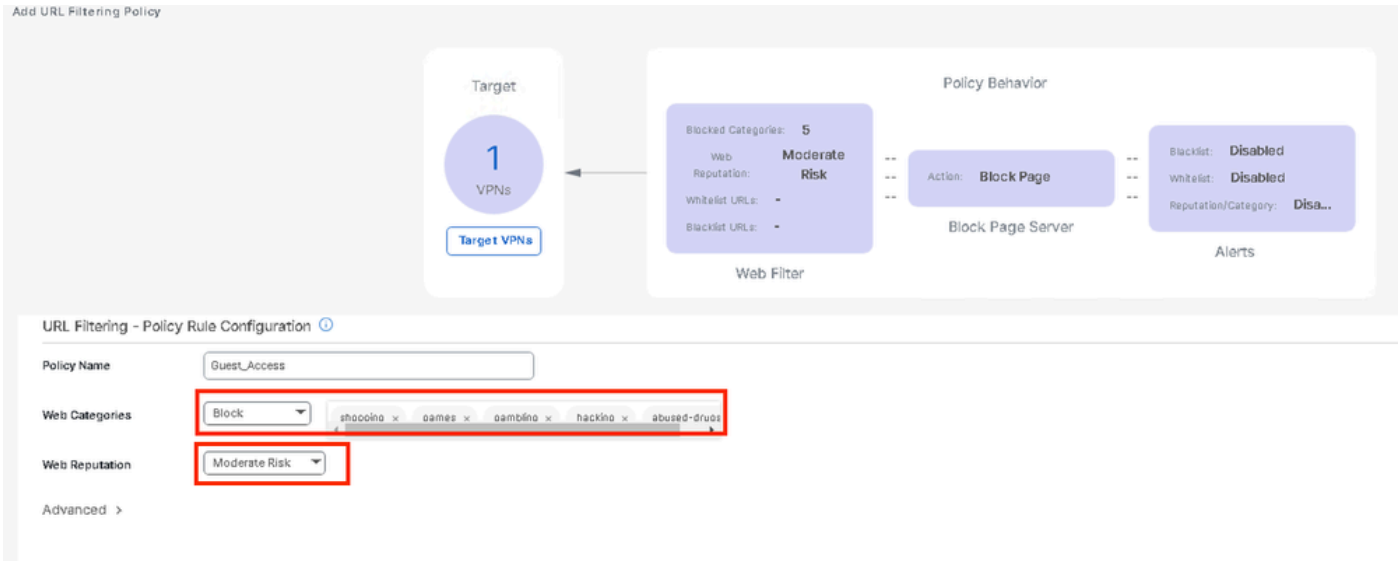


- Policy Nameフィールドにポリシー名を入力します。
- [Webカテゴリ]ドロップダウンからいずれかのオプションを選択し、[ブロック]を選択すると、選択したカテゴリに一致するWebサイトがブロックされます。

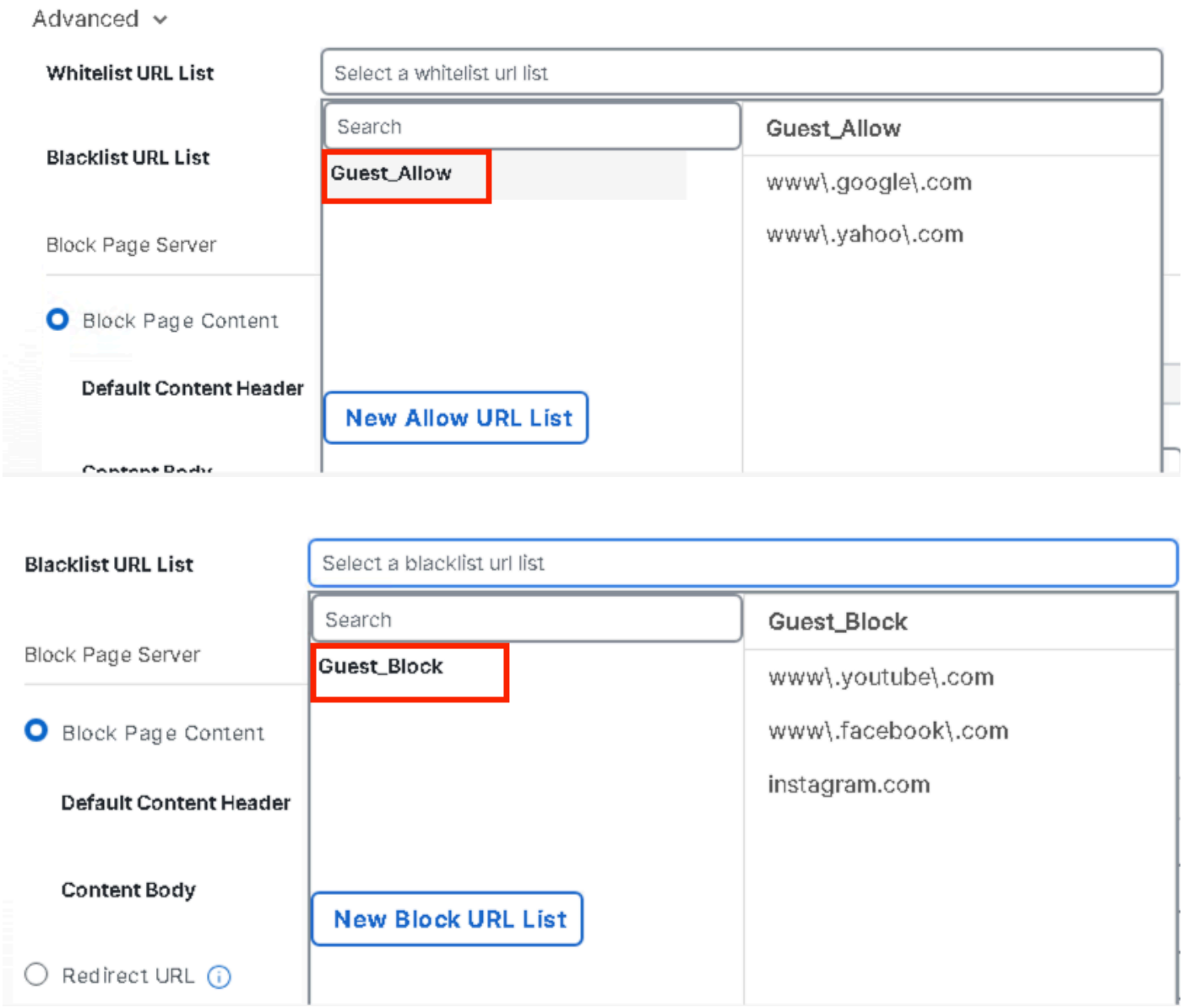
    ブロック：選択したカテゴリに一致するWebサイトをブロックします。
    許可：選択したカテゴリに一致するWebサイトを許可します。

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。

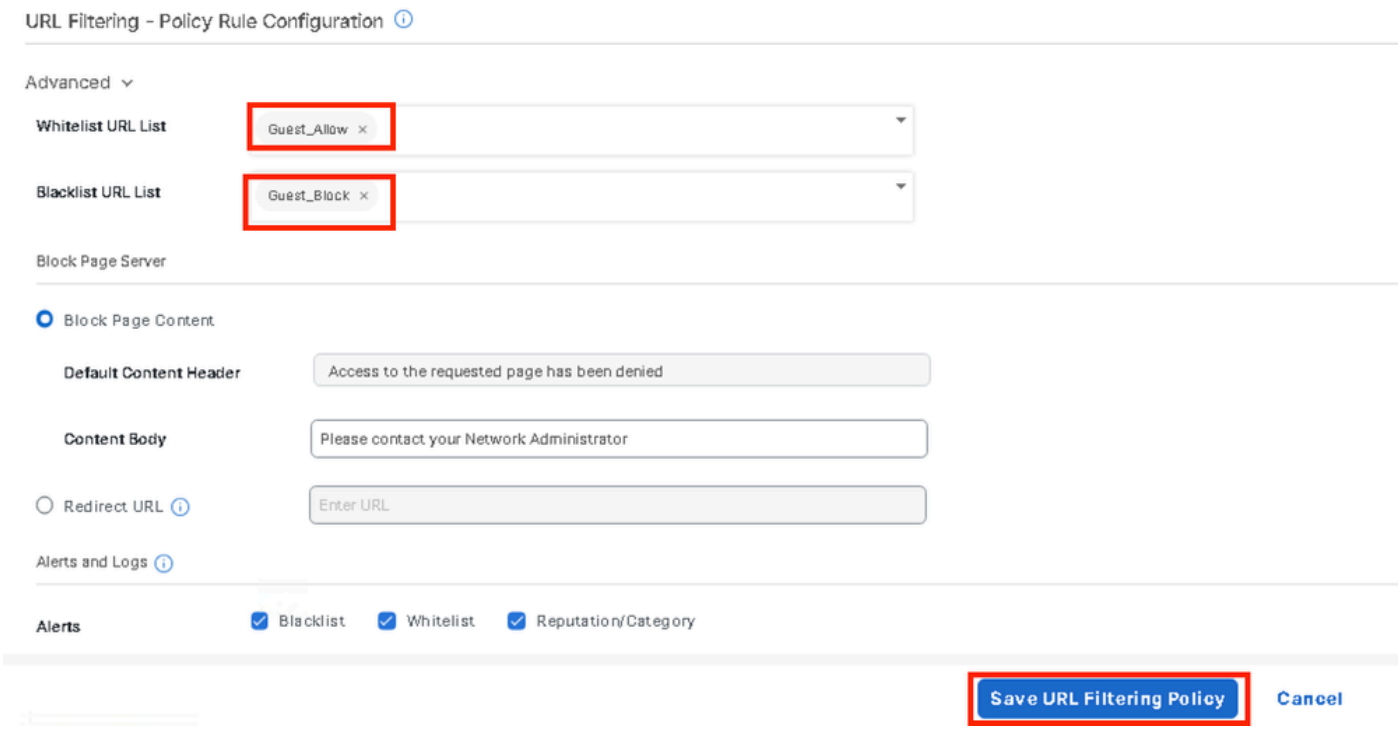


Advancedで、必要に応じて、Allowlist URL ListまたはblocklistURL Listドロップダウンメニューから既存のリストを選択するか、新しいリストを作成します。



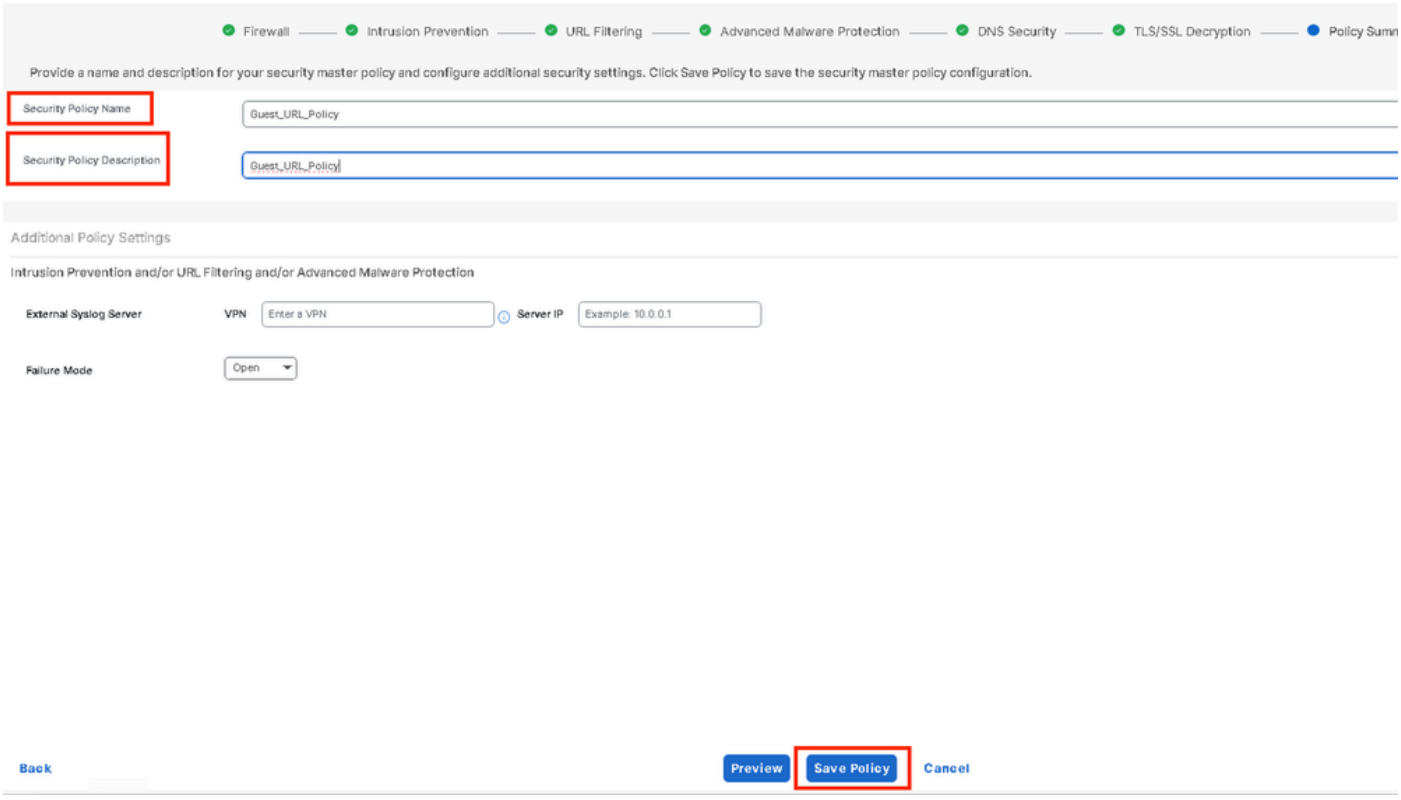
必要に応じて、[ブロックページコンテンツ]の下のコンテンツ本体を変更し、すべての通知が選択されていることを確認します。

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。



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

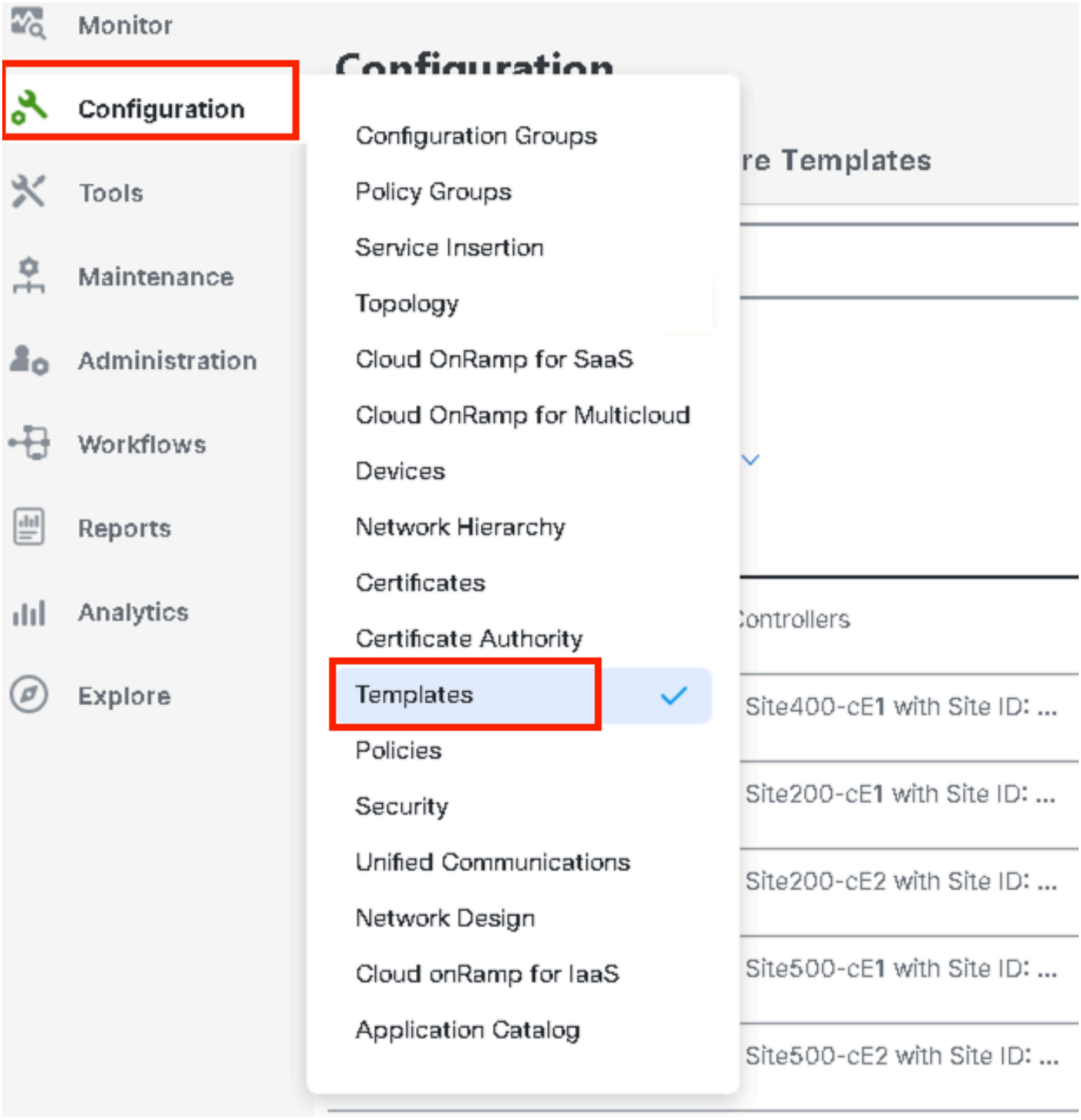
各フィールドにSecurity Policy NameとSecurity Policy Descriptionを入力します。



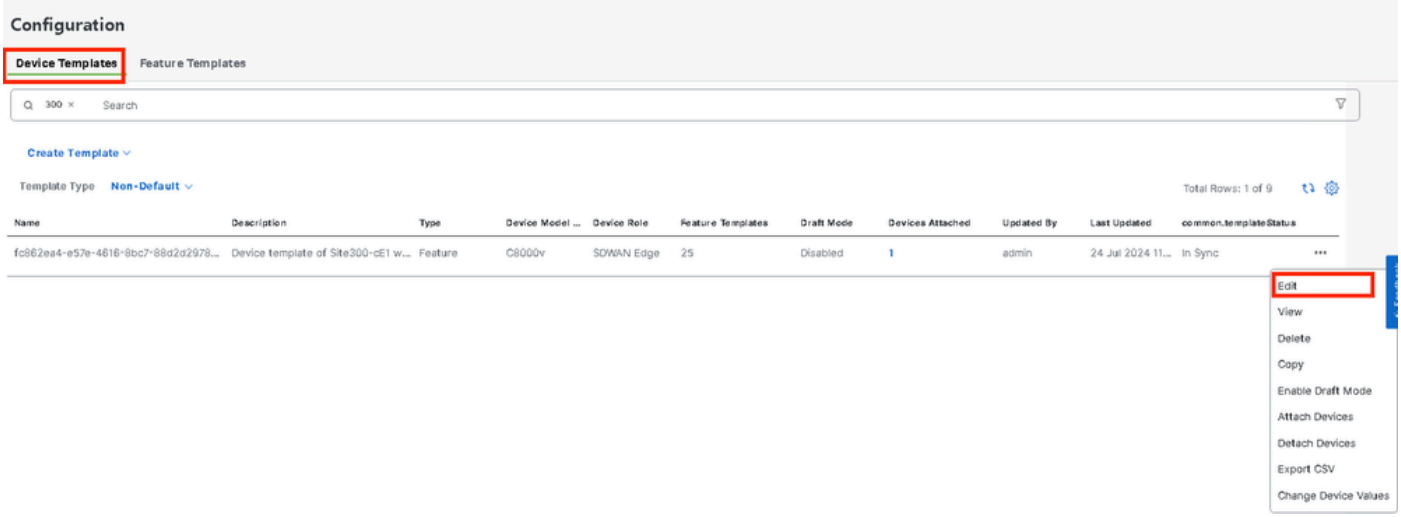
デバイスへのセキュリティポリシーの適用

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。

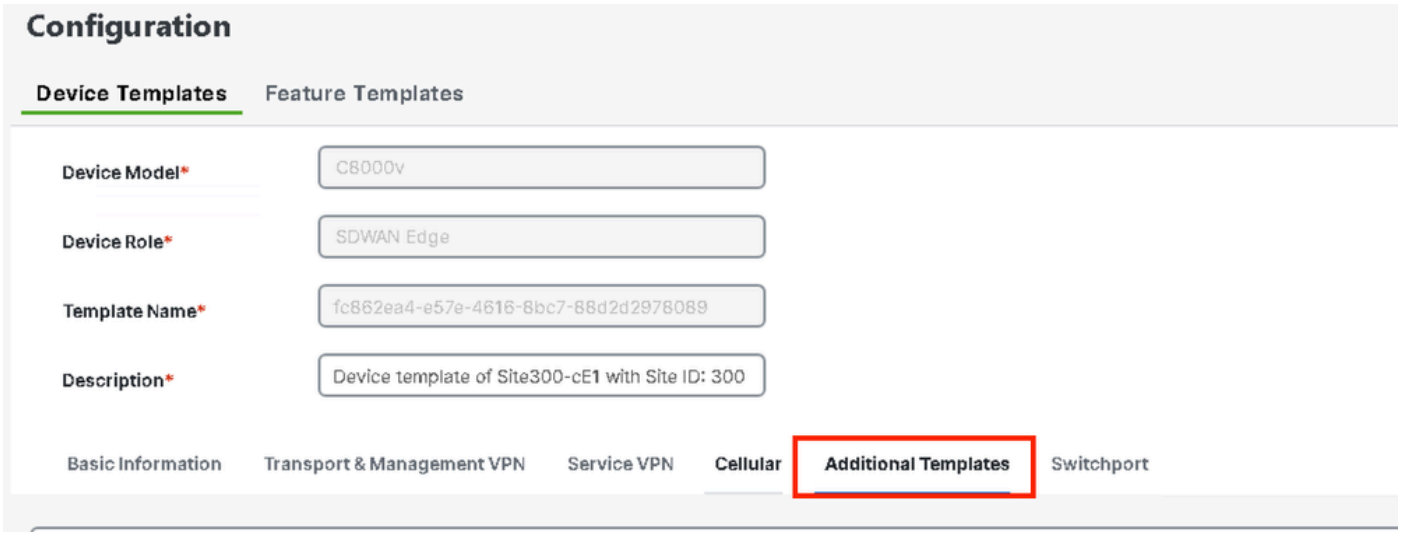
Cisco SD-WAN Managerメニューから、Configuration > Templatesの順に選択します。



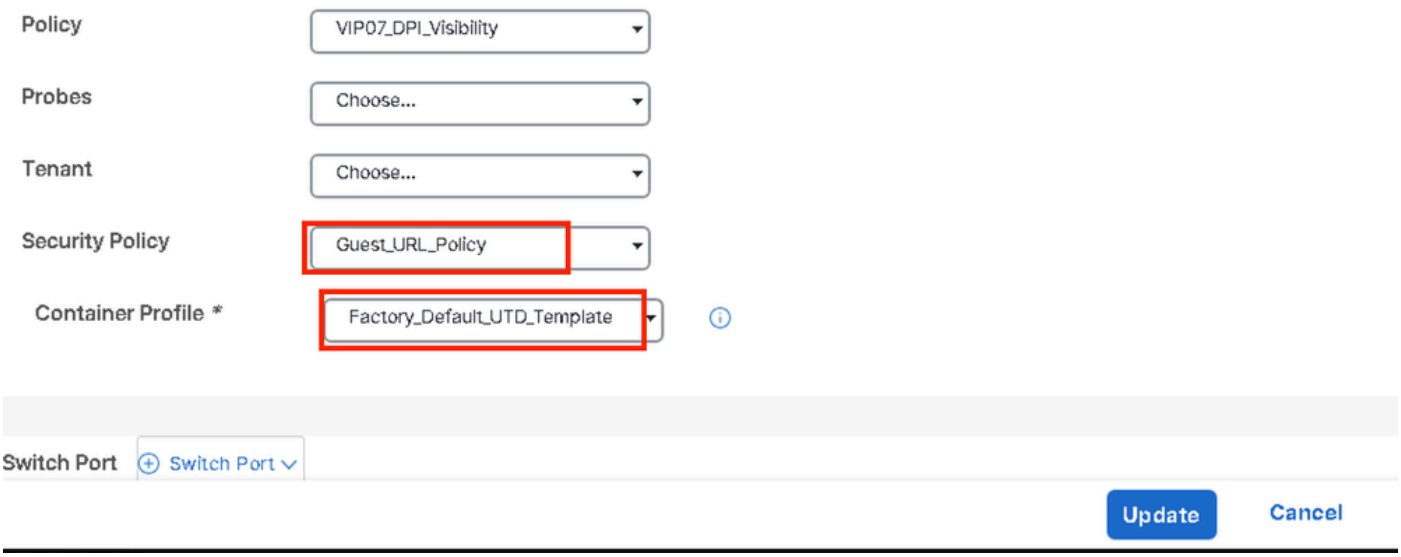
Device Templatesをクリックし、Editをクリックします。



Additional Templatesをクリックします。

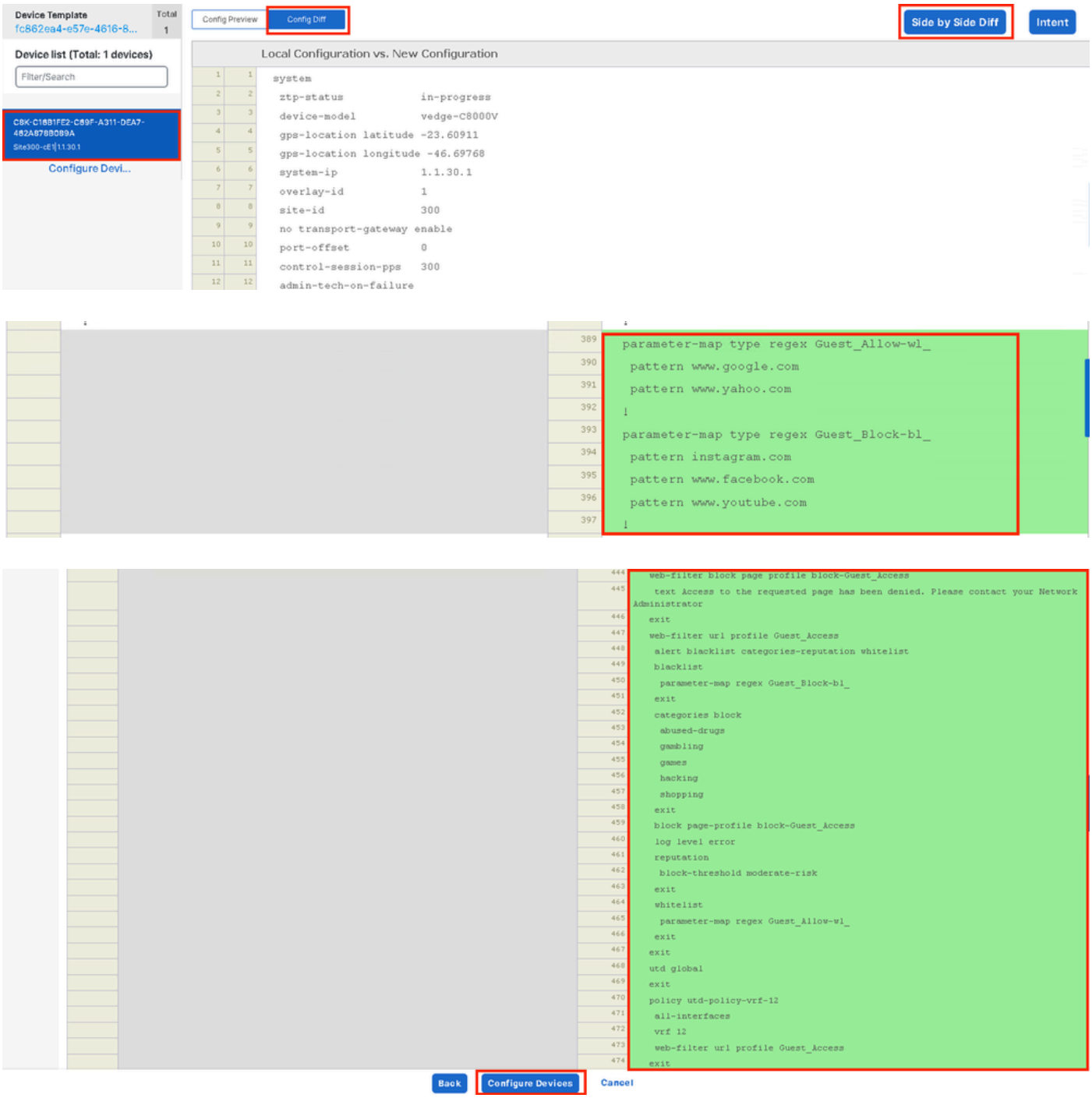


- Security Policyドロップダウンリストから、以前にGuest_URL_Policyの下で設定したポリシーの名前を選択し、Updateをクリックします。

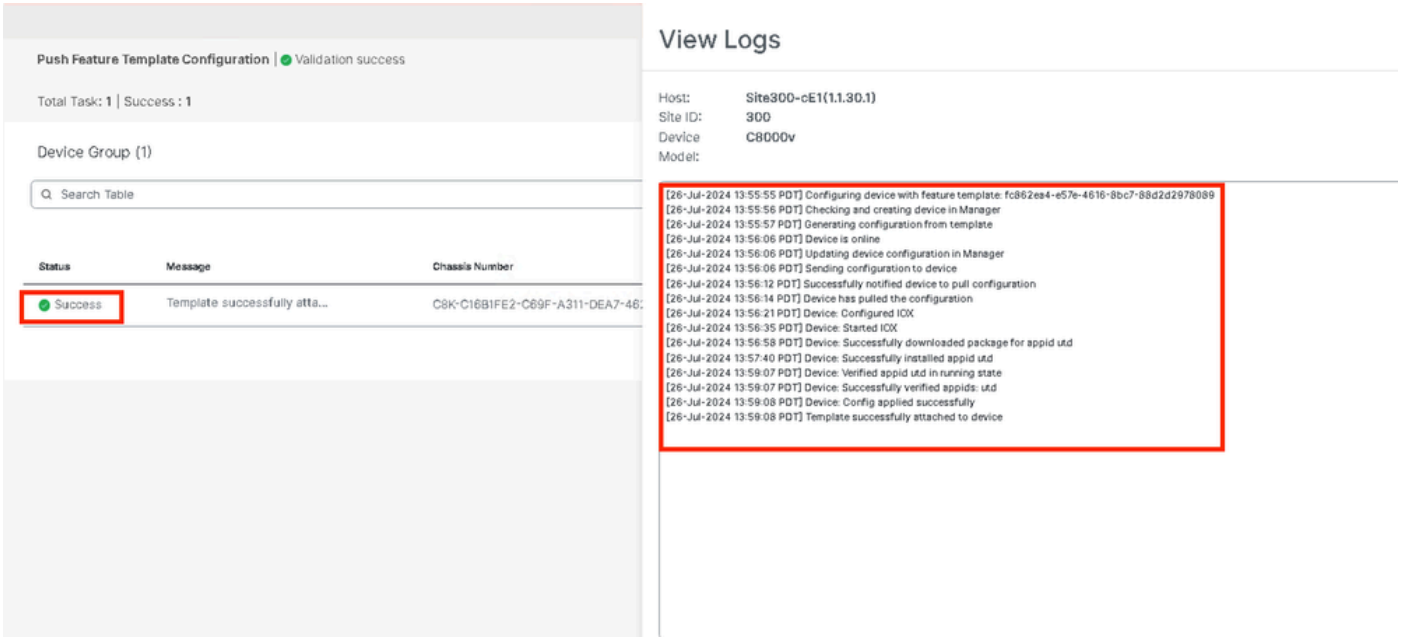


デバイスをクリックし、設定が正しいことを確認して、Config DiffとSide by Side Diffをクリック

します。Configure Devicesをクリックします。



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。

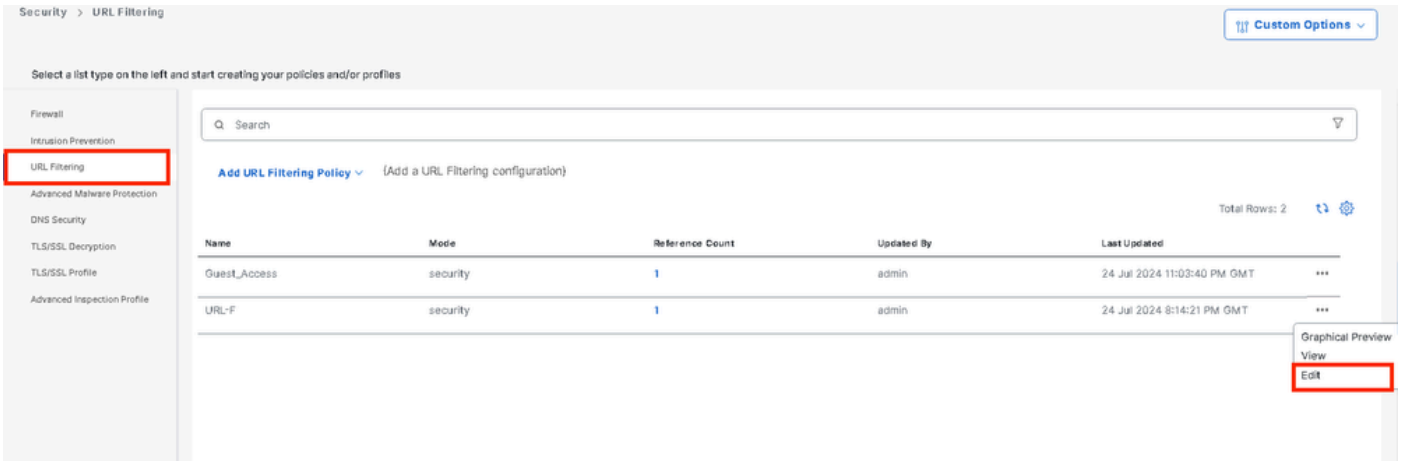


URLフィルタの変更

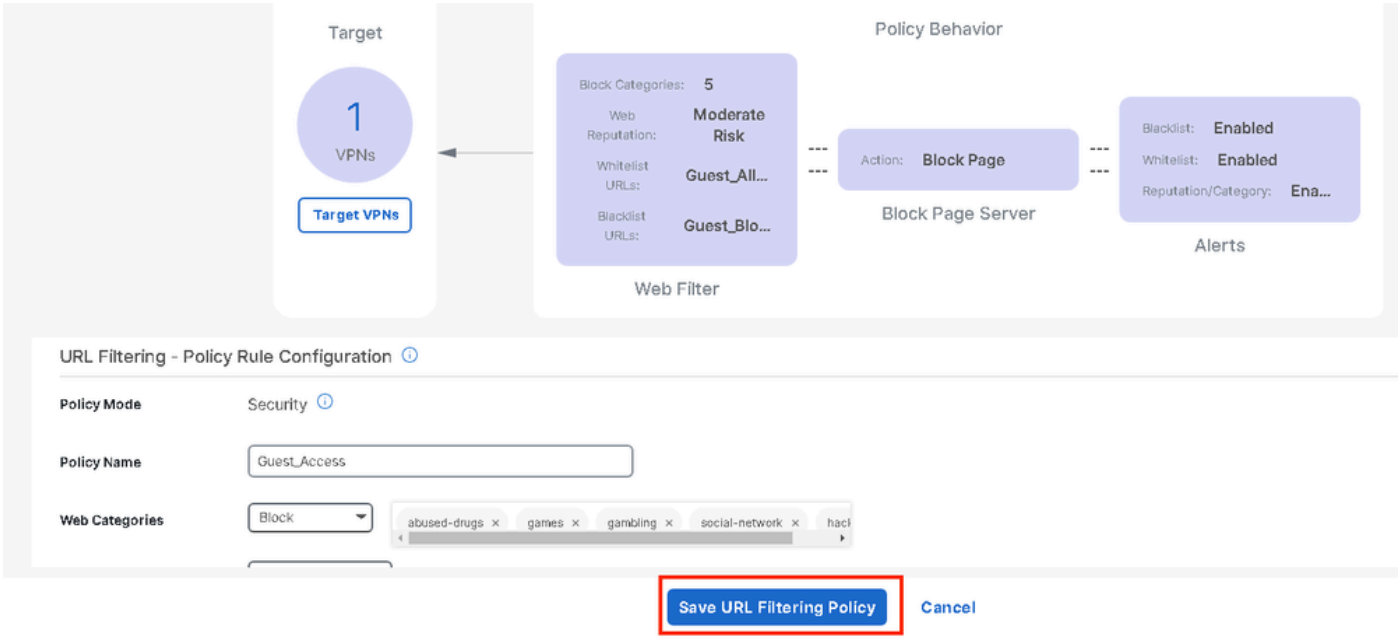
URLフィルタリングポリシーを変更するには、次の手順を実行します。

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。

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。



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。



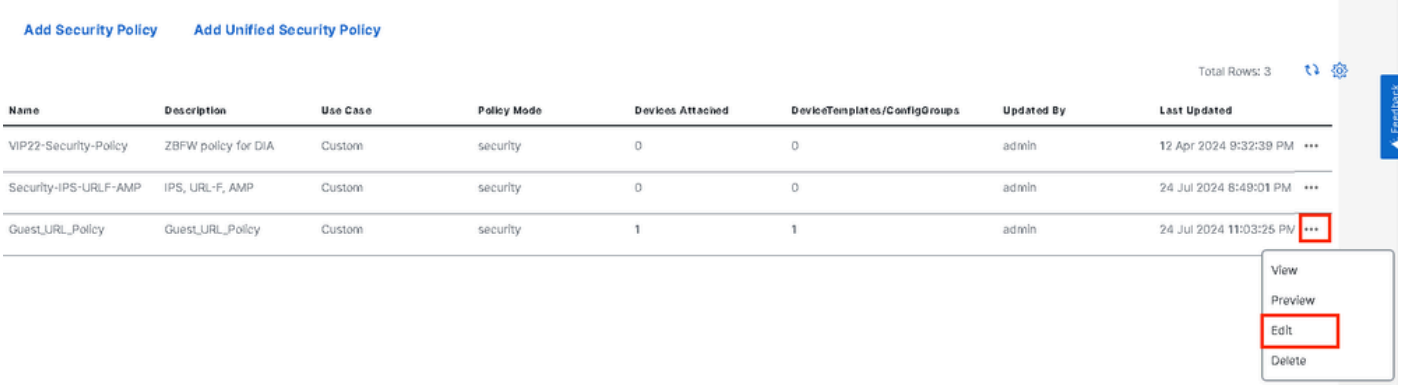
URLフィルタリングの削除

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。

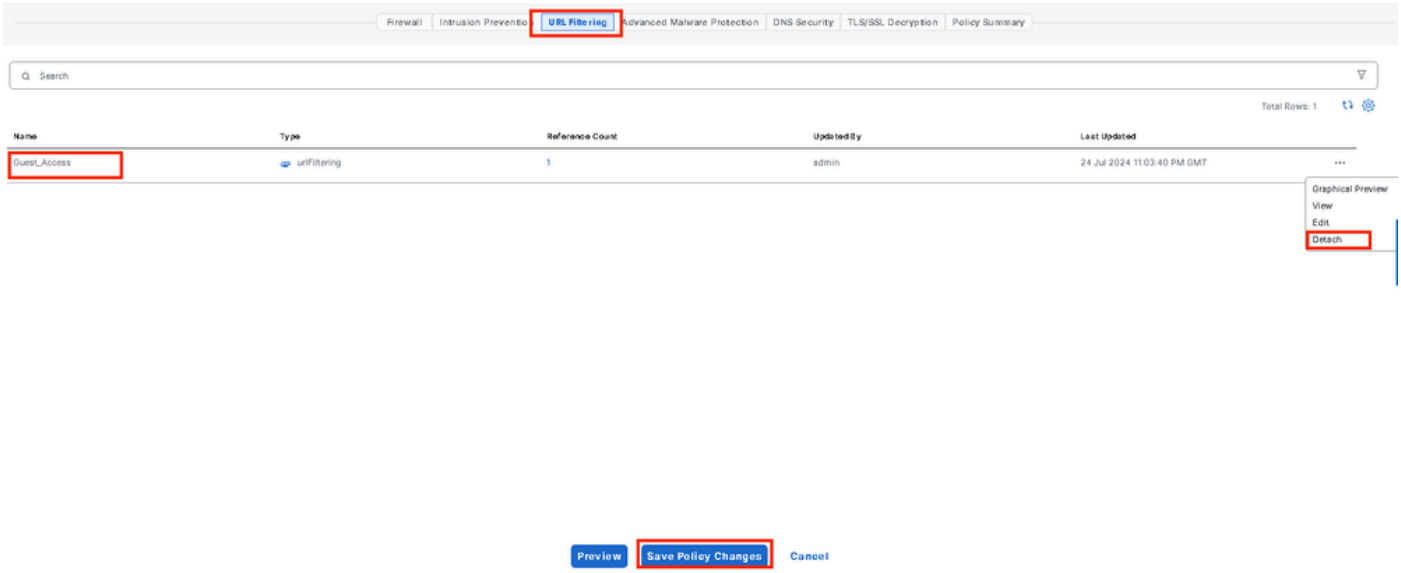
- URLフィルタリングポリシーを含むセキュリティポリシーの場合は、3個のドット(...)をクリックし、次にEditをクリックします。



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

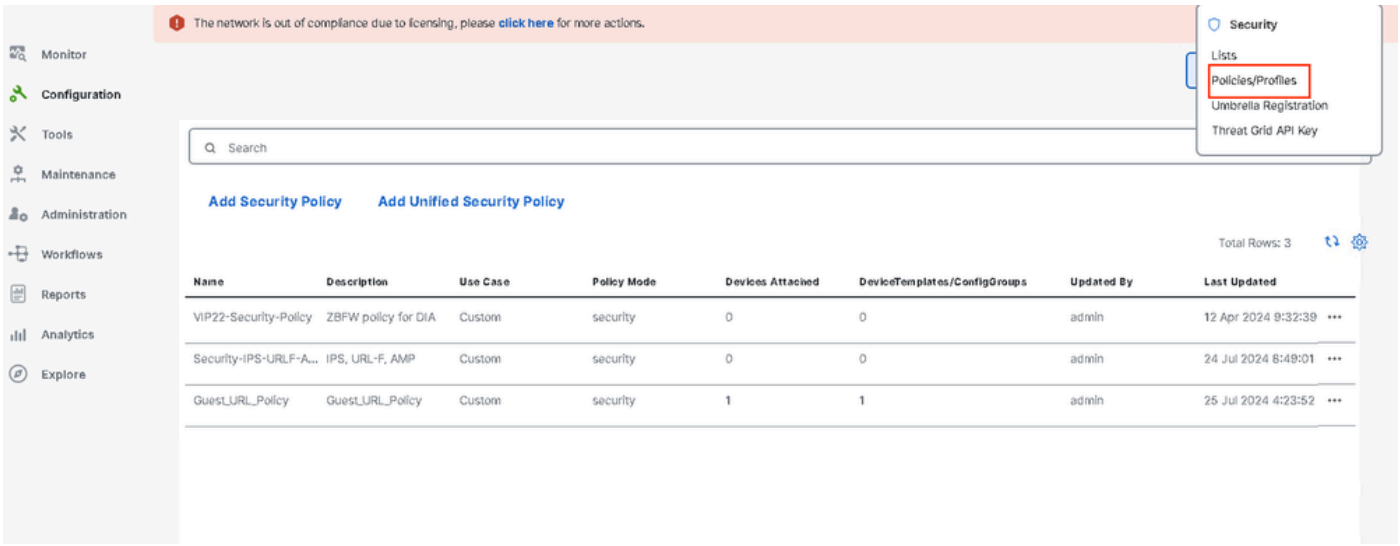
削除するポリシーに対して、3ドット(...)をクリックし、Detachを選択します。

Save Policy Changesをクリックします。



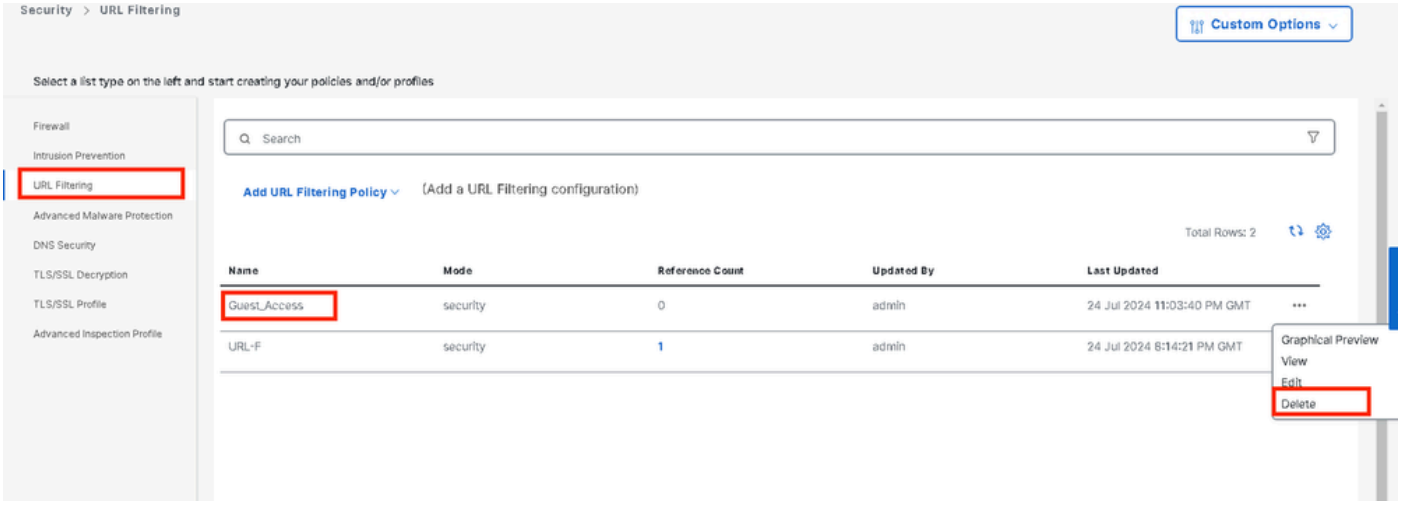
URLフィルタリングポリシーを削除するには、次の手順を実行します。

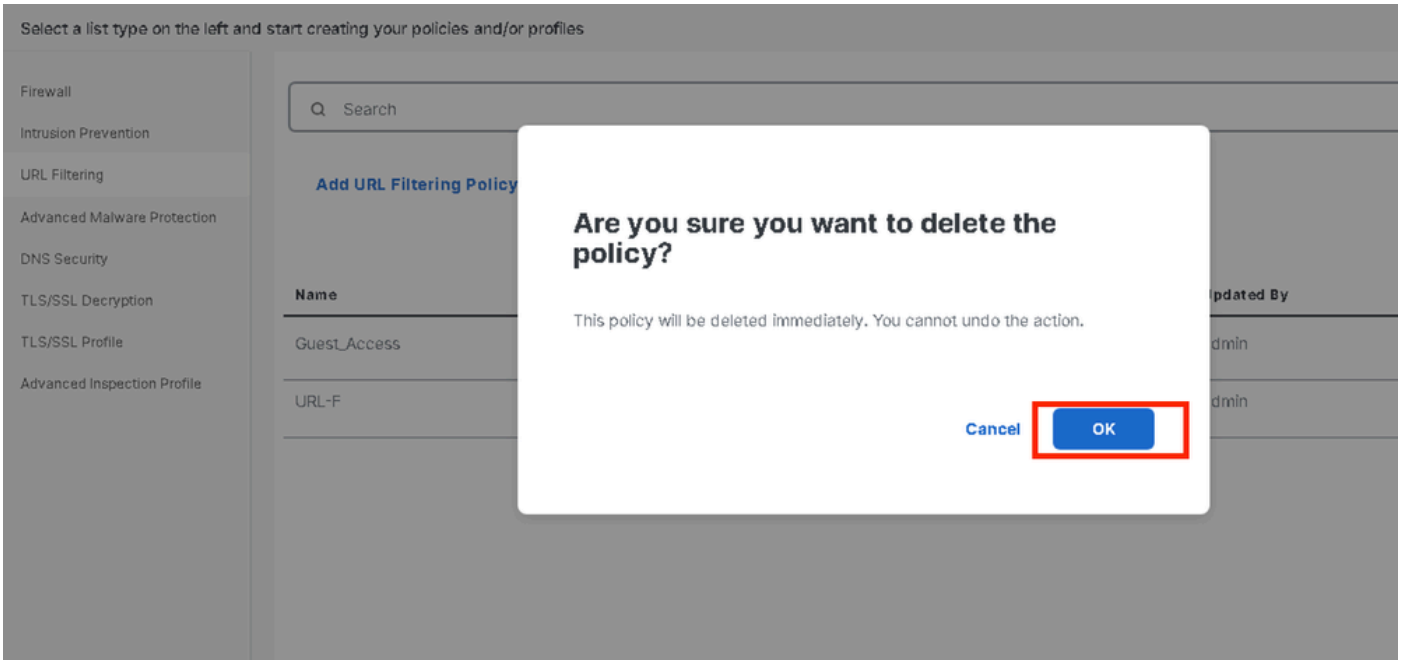
Security画面で、Custom Optionsドロップダウンメニューをクリックし、Policies/Profilesを選択して、URL Filteringを選択します。



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。

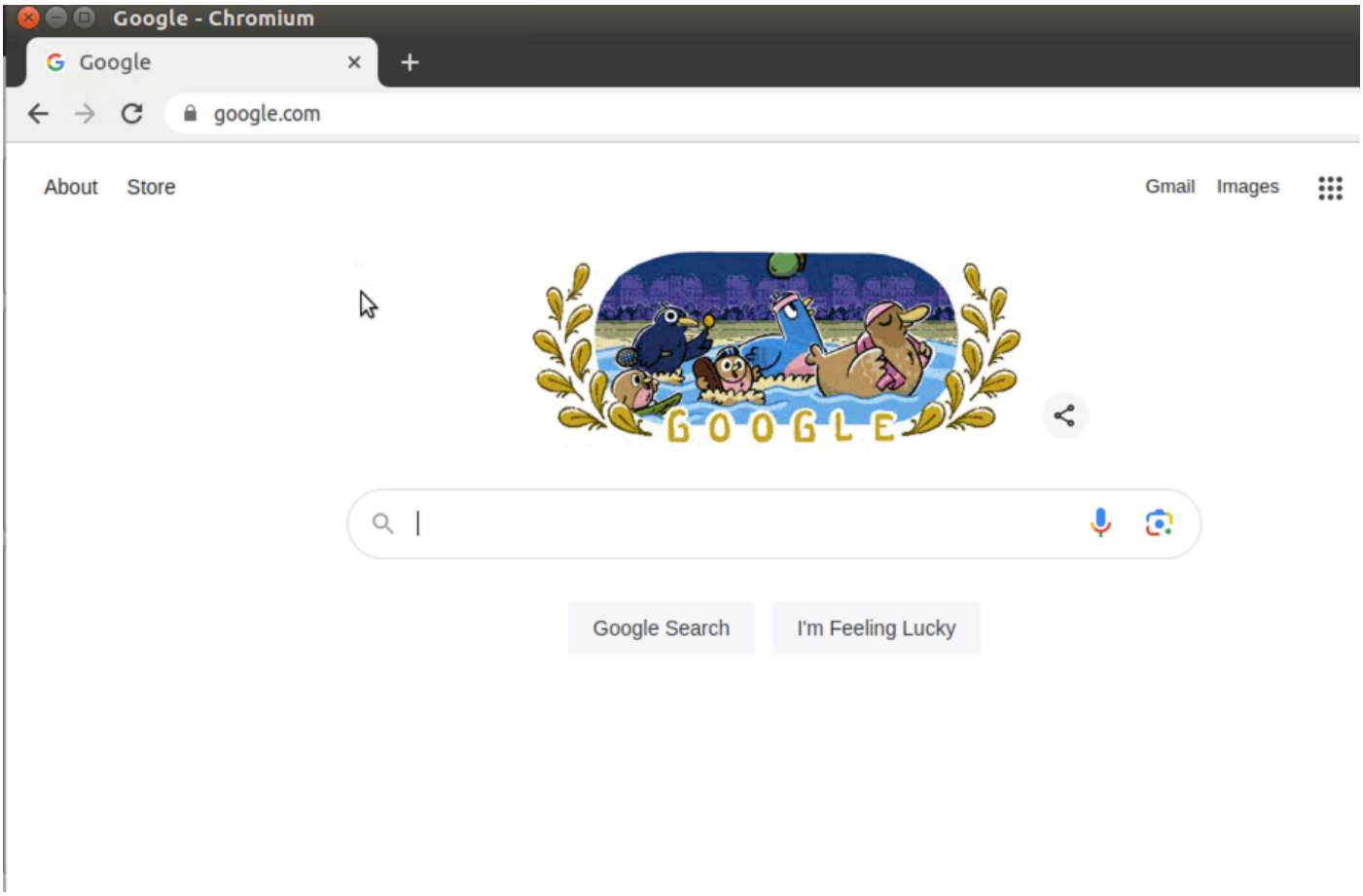
<#root>

```
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

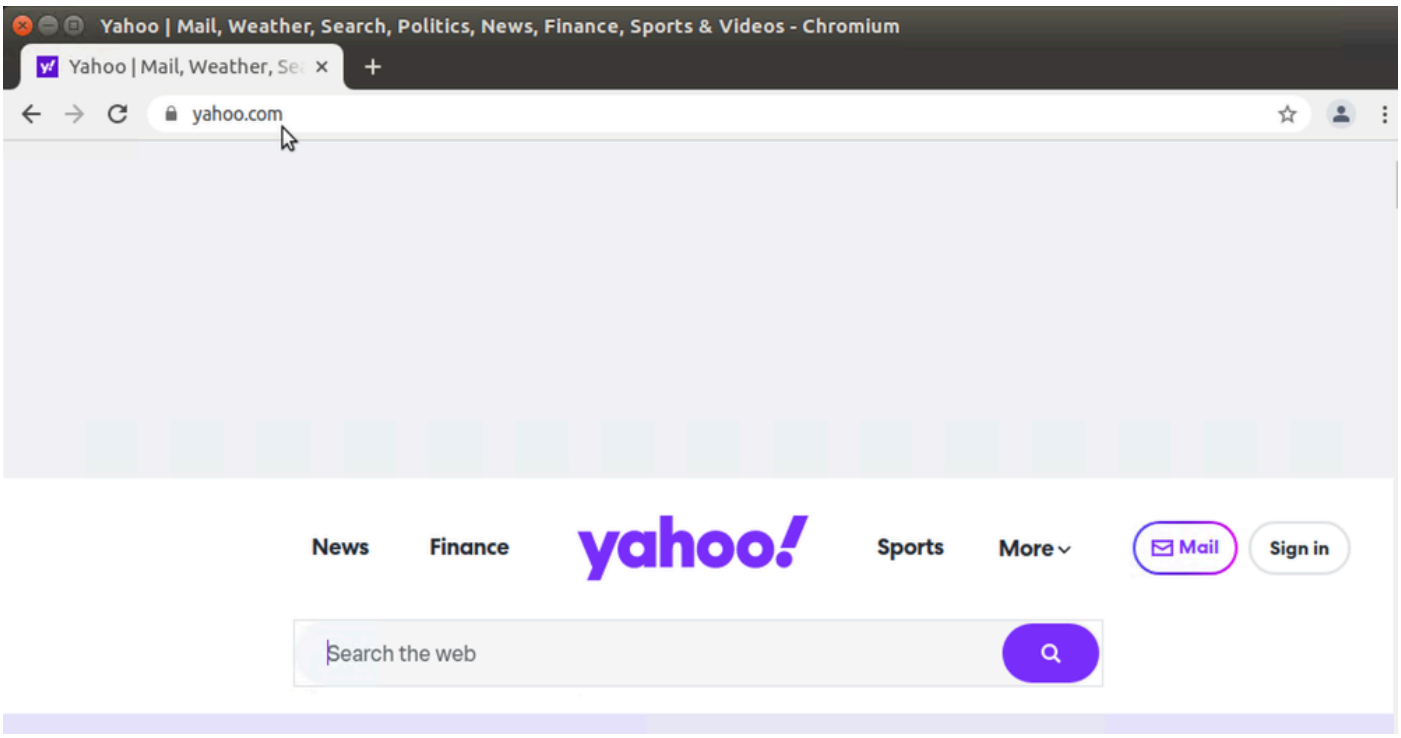
[**]

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

 [**]

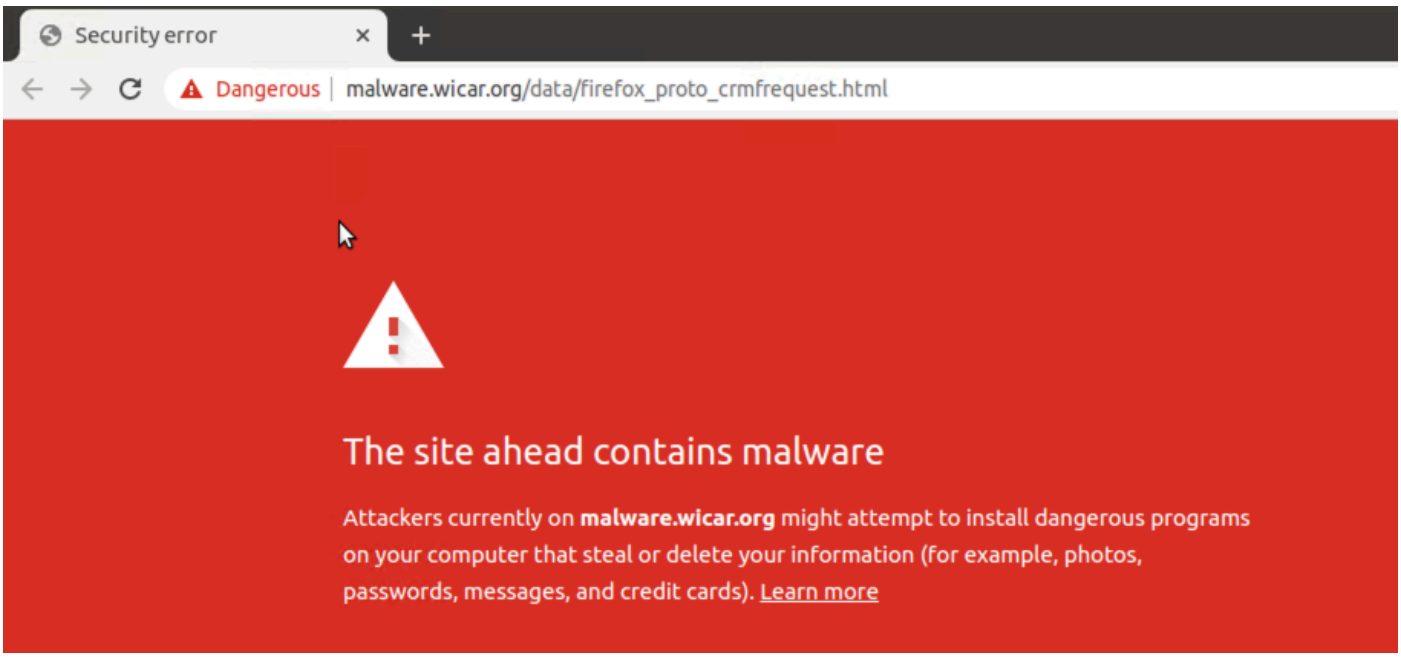
UTD WebFilter Allowlist

 [**] [

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

[**]

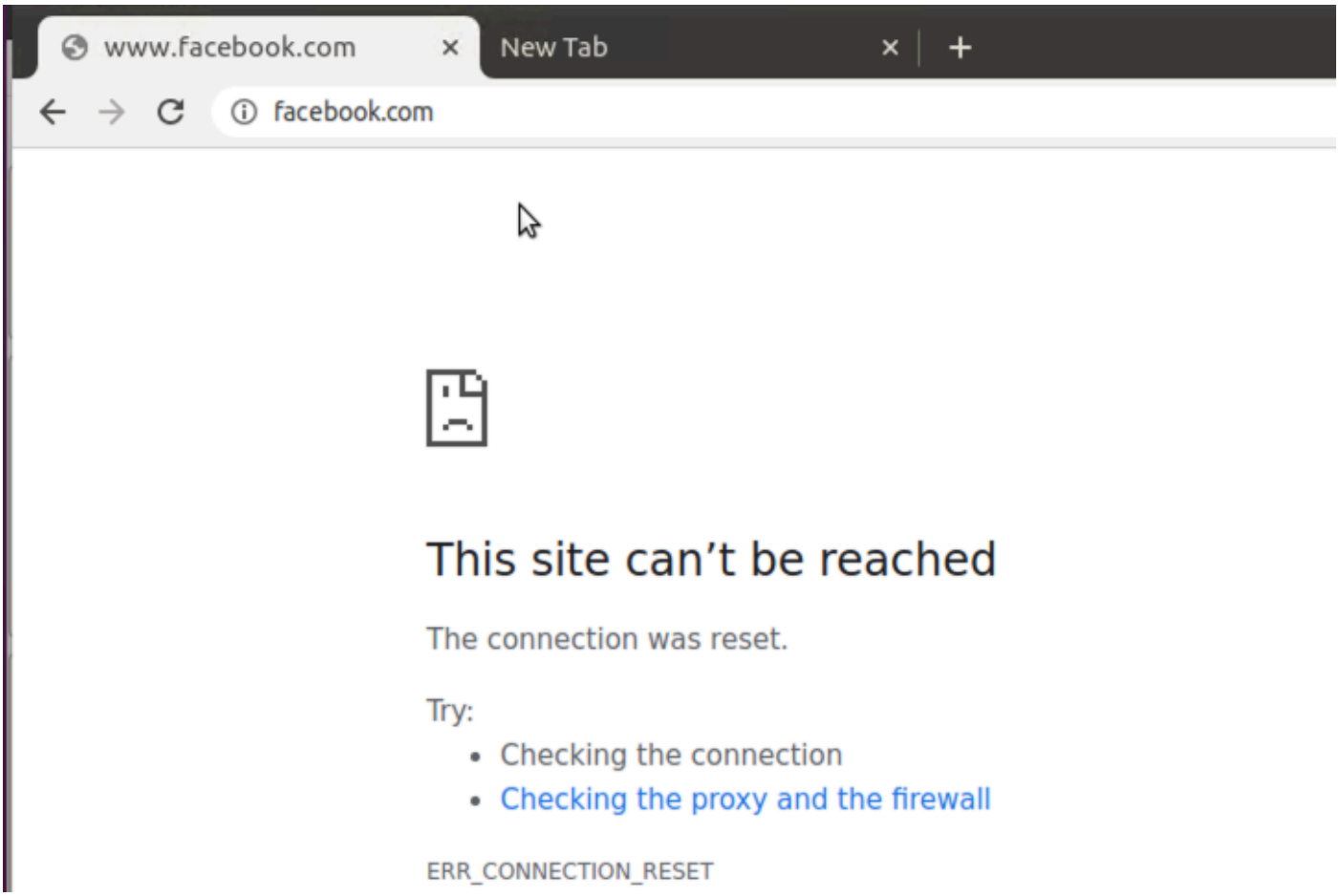
UTD WebFilter Category/Reputation

[**] [

URL: malware.wicar.org/data/firefox_proto_crmfrequest.html

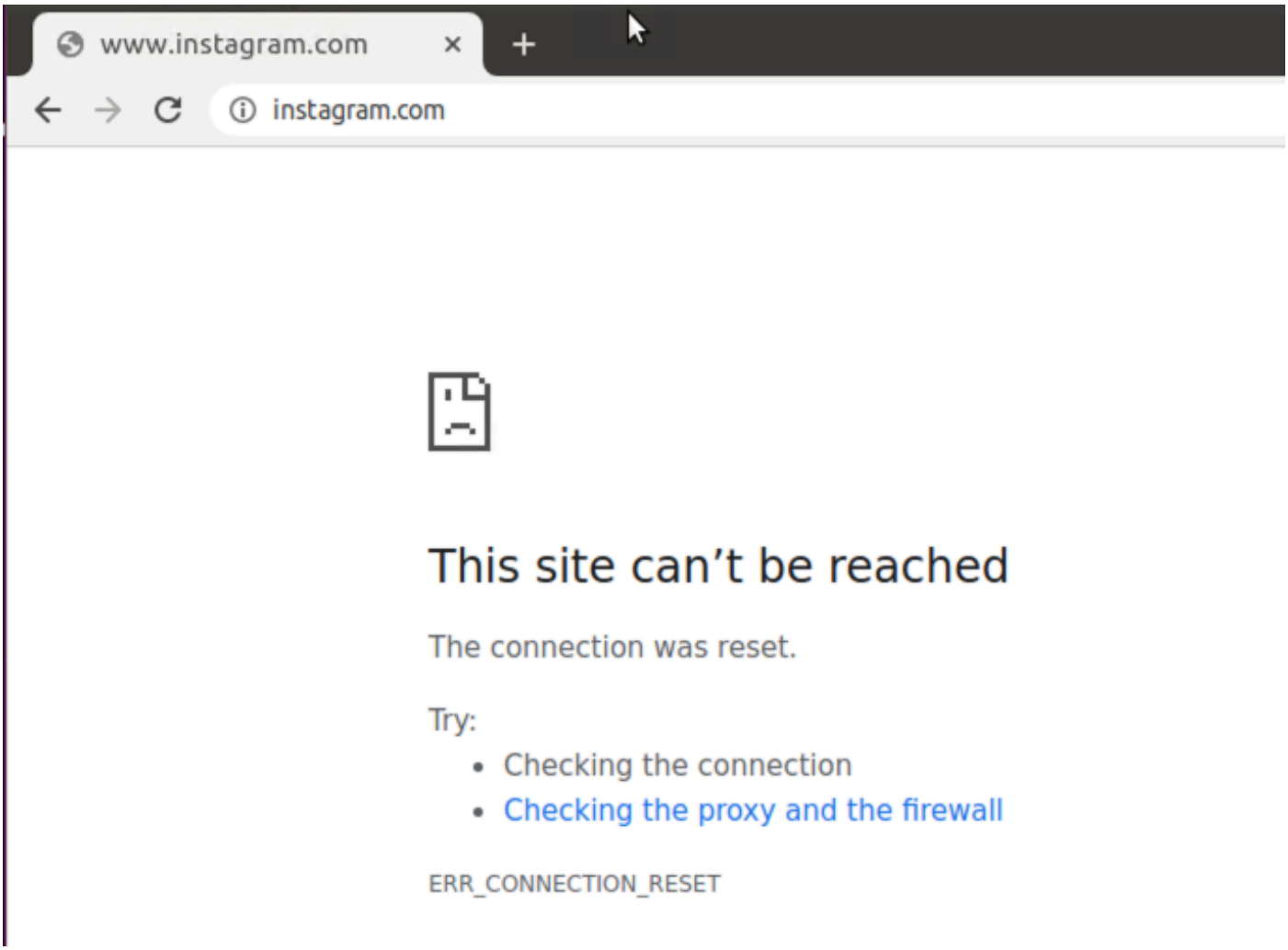
```
] ** [Category: Malware Sites] ** [Reputation: 10] [VRF: 12] {TCP} 10.32.1.10:40154 -> 208.94.116.246:8
```

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 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
```



<#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

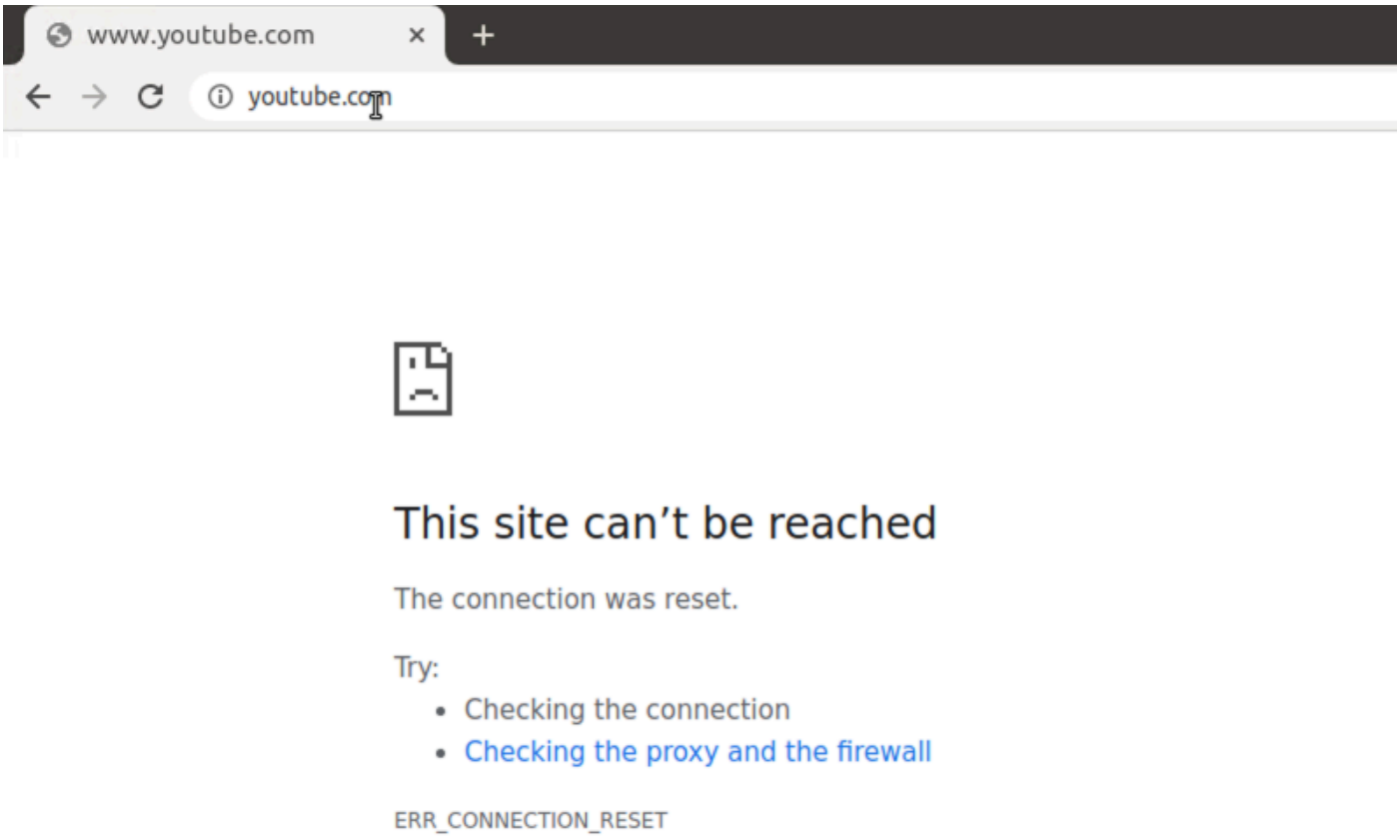
[**]

UTD WebFilter blocklist

[**] [

URL: www.instagram.com

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



<#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

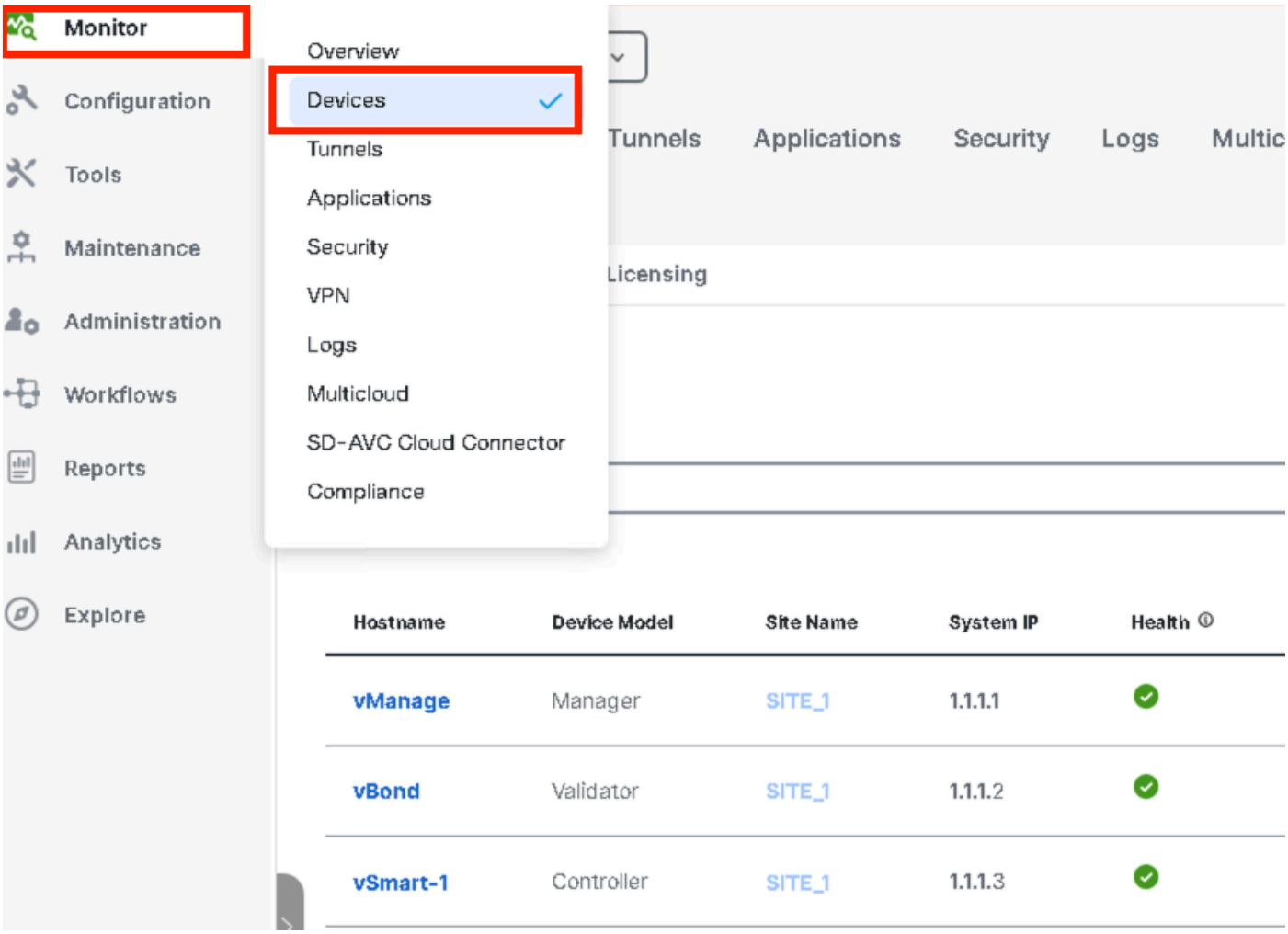
] [VRF: 12] {TCP} 10.32.1.10:54352 -> 142.250.72.206:443

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。

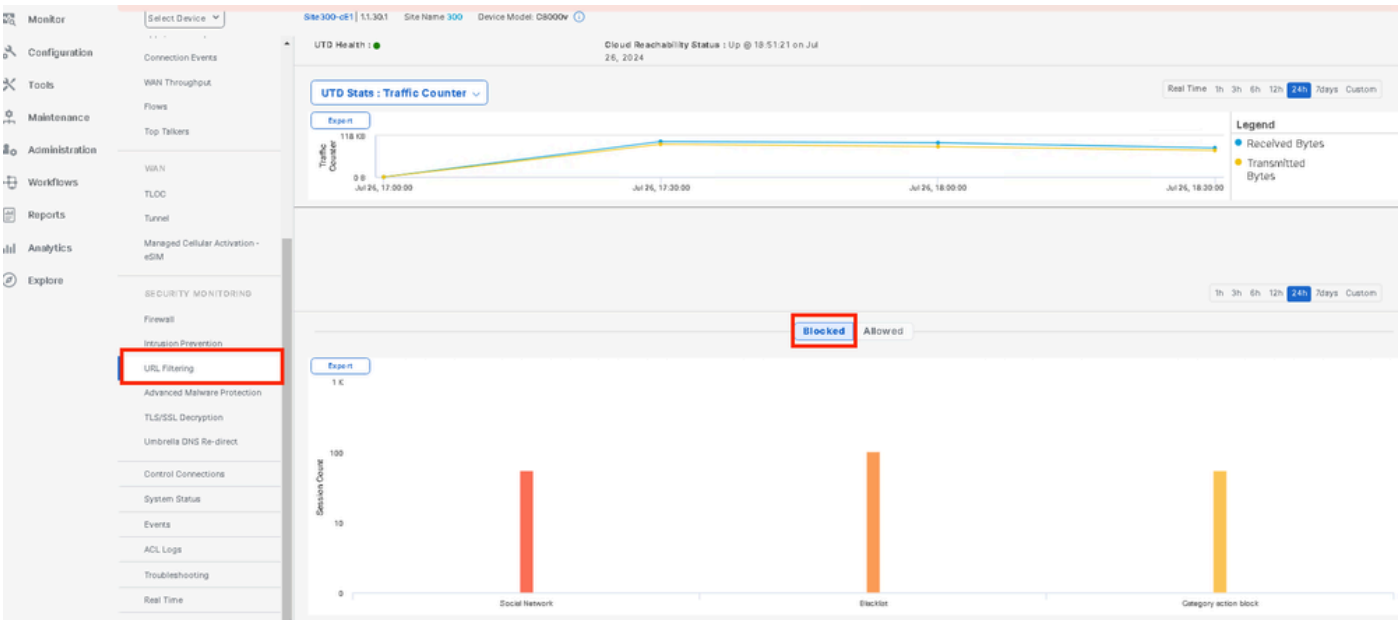
Cisco IOS XE Catalyst SD-WANデバイスでブロックまたは許可されているURLをモニタするには、次の手順を実行します。

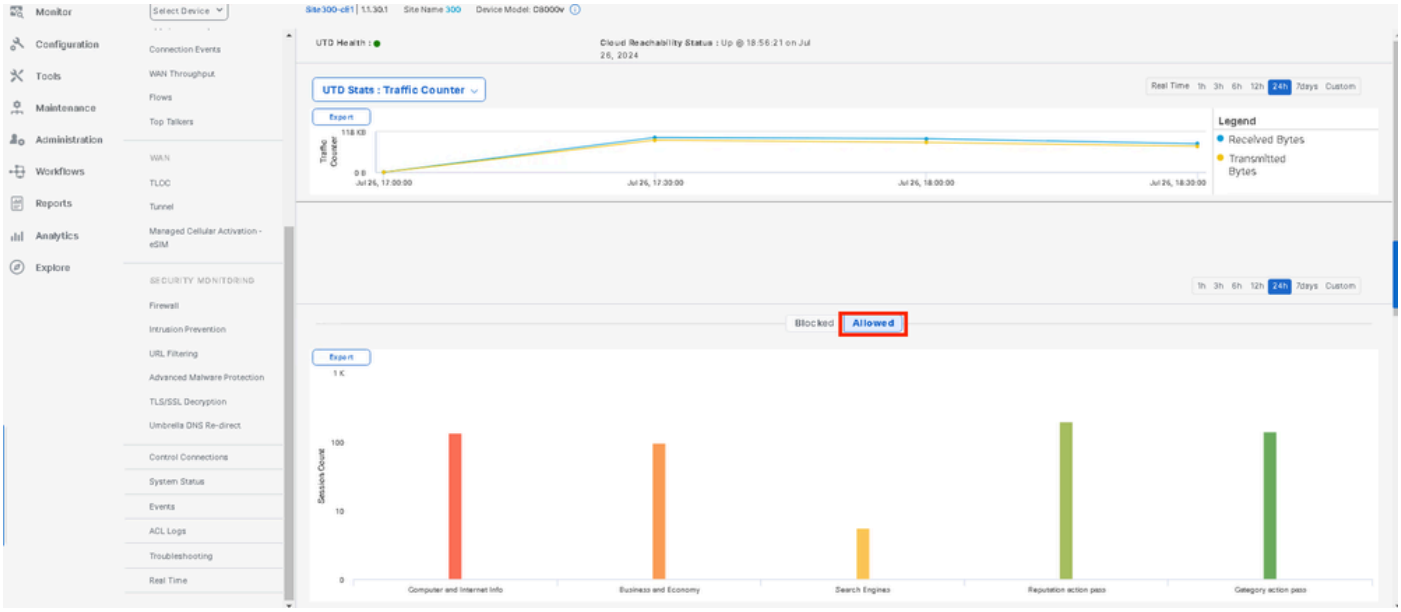
1. Cisco SD-WAN Managerメニューから、Monitor > Devices > Select Deviceの順に選択します。



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。





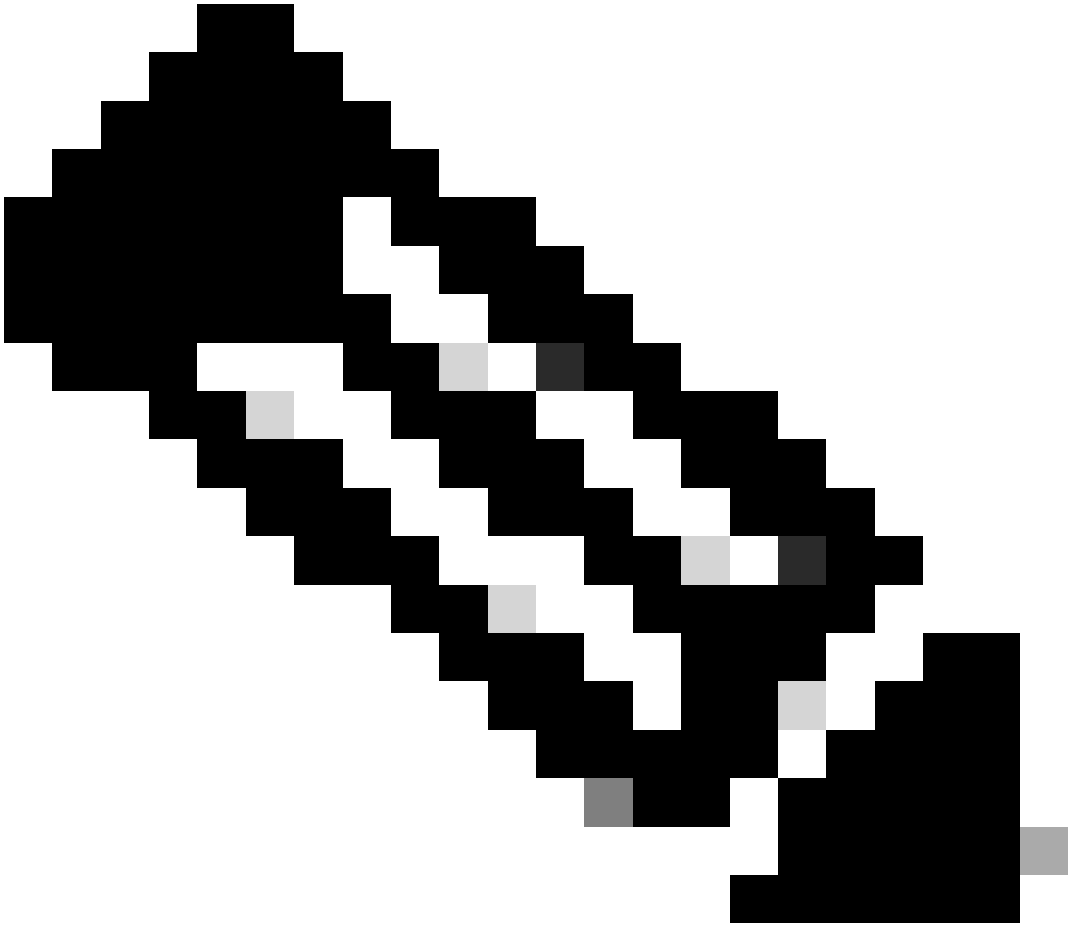
トラブルシュート

サポートされている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 <<<<<<<<<<<<<<<<



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。

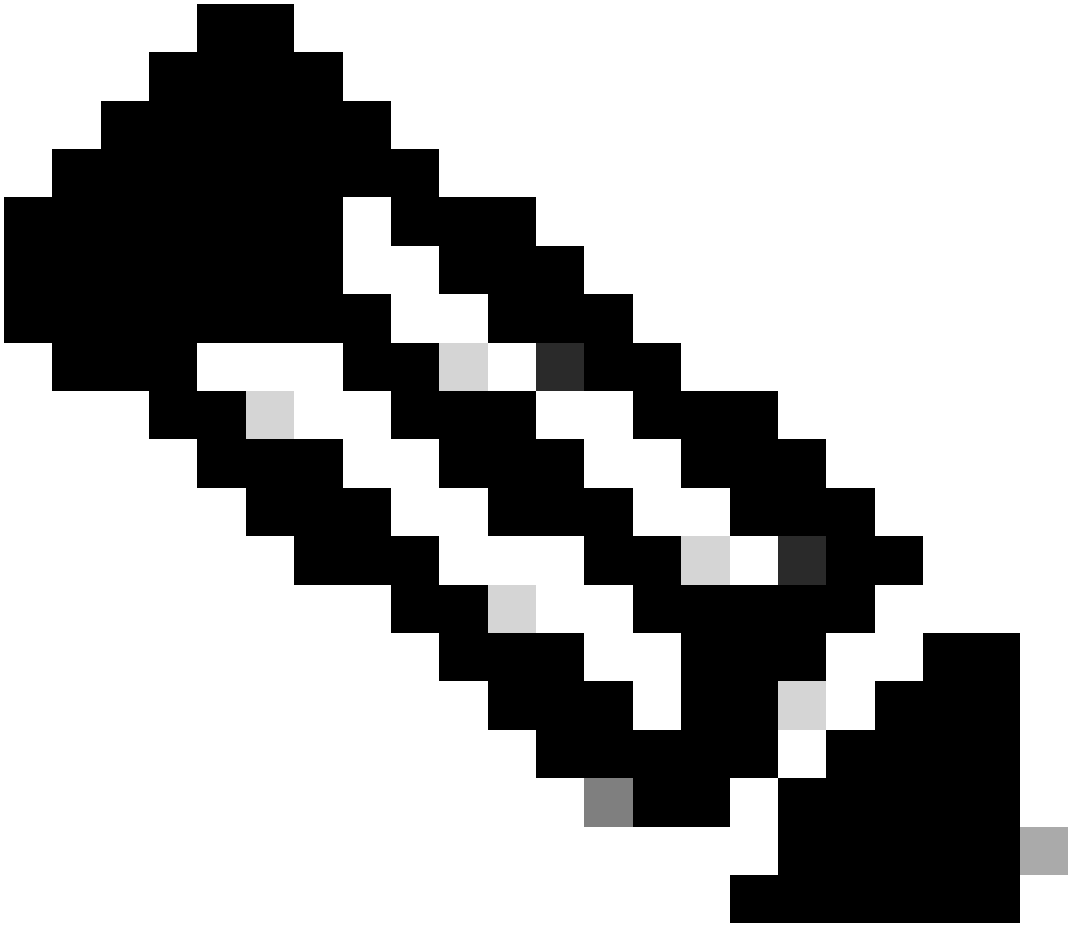
<#root>

```
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。