

# 配置和驗證URL過濾

## 目錄

---

### [簡介](#)

### [必要條件](#)

#### [需求](#)

#### [採用元件](#)

### [設定](#)

#### [網路圖表](#)

#### [配置URL過濾策略的元件](#)

##### [建立感興趣的URL清單](#)

##### [建立安全策略](#)

#### [將安全策略應用於裝置](#)

#### [修改URL篩選](#)

#### [刪除URL篩選](#)

### [驗證](#)

### [從vManage GUI監控URL過濾](#)

### [疑難排解](#)

### [相關資訊](#)

---

## 簡介

本文檔介紹如何使用Cisco Catalyst Manager GUI在Cisco IOS-XE®路由器上配置和驗證URL過濾。

## 必要條件

在vManage中上傳具有當前Cisco IOS-XE代碼的相容UTD軟體虛擬映像。有關在cEdge路由器上安裝UTD安全虛擬映像的說明，請檢視相關資訊部分。

Cisco Edge路由器必須處於vManaged模式，並且必須預先連線模板。

## 需求

思科建議您瞭解以下主題：

- Cisco SD-WAN Overlay會啟動初始配置。
- URL過濾配置Cisco Catalyst Manager GUI。

## 採用元件

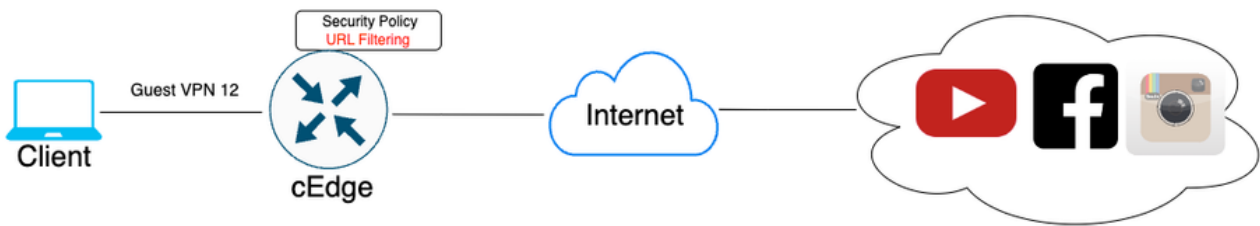
本檔案根據這些軟體和硬體版本：

- Cisco Catalyst SD-WAN Manager 20.14.1版。
- Cisco Catalyst SD-WAN控制器版本20.14.1。
- 思科邊緣路由器版本17.14.1。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 設定

### 網路圖表



### 配置URL過濾策略的元件

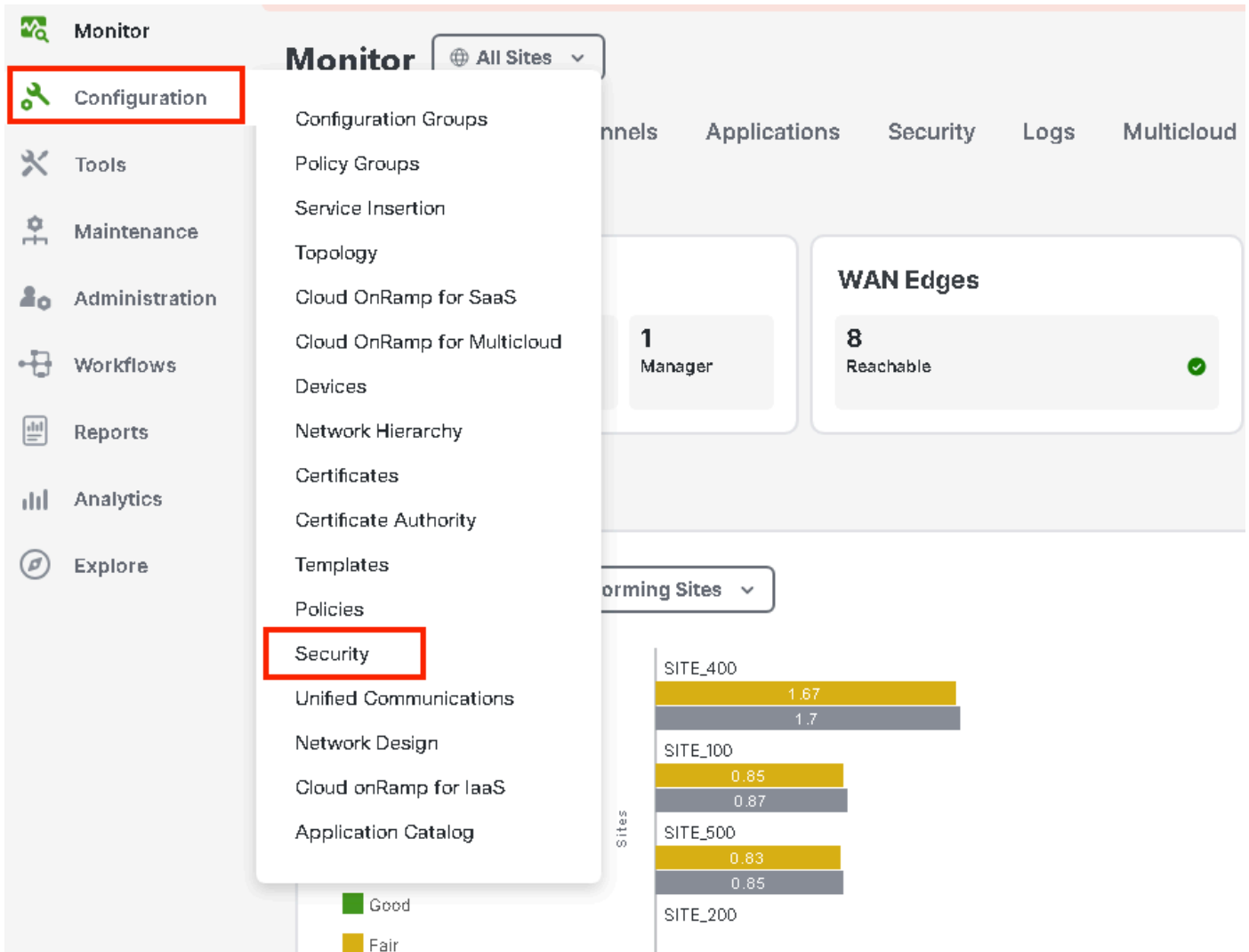
本文根據以下示例要求，說明了如何根據類別、信譽或按域阻止/允許清單配置URL過濾以阻止/允許特定客戶端HTTPS流量：

- 阻止來自訪客VPN Web類別上的客戶端的此HTTPS請求：
  - 遊戲
  - 賭博
  - 駭客
  - 非法毒品
- 必須阻止來自訪客VPN上具有Web信譽小於或等於60的客戶端到網站的任何HTTPS URL請求。
- 訪客VPN上的客戶端對網站的HTTP(s)請求阻止了Facebook、Instagram和YouTube，同時允許訪問google.com和yahoo.com。

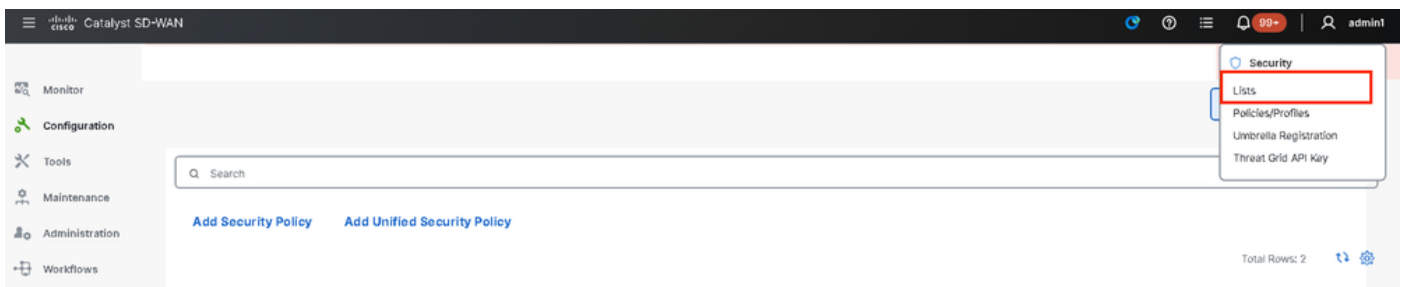
要配置URL過濾：

#### 建立感興趣的URL清單

1. 在Cisco SD-WAN Manager選單上，導航到左側面板中的Configuration > Security頁籤。



要建立或管理Allowlist URL List或Blocklist URL List，請從頁面右上角的Custom Options下拉選單中選擇Lists。



按一下左側窗格中的Allow URLs Lists，並建立New Allow 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 Allow URL List

Name	Entries	Reference Count	Update
No data available			

- 在URL List Name欄位中，輸入最多包含32個字元（僅限字母、數字、連字型大小和底線）的清單名稱。
- 在URL欄位中，輸入要包含在清單中的URL，並以逗號分隔。還可以使用導入按鈕從可訪問的儲存位置增加清單。
- 完成後，按一下Add。

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

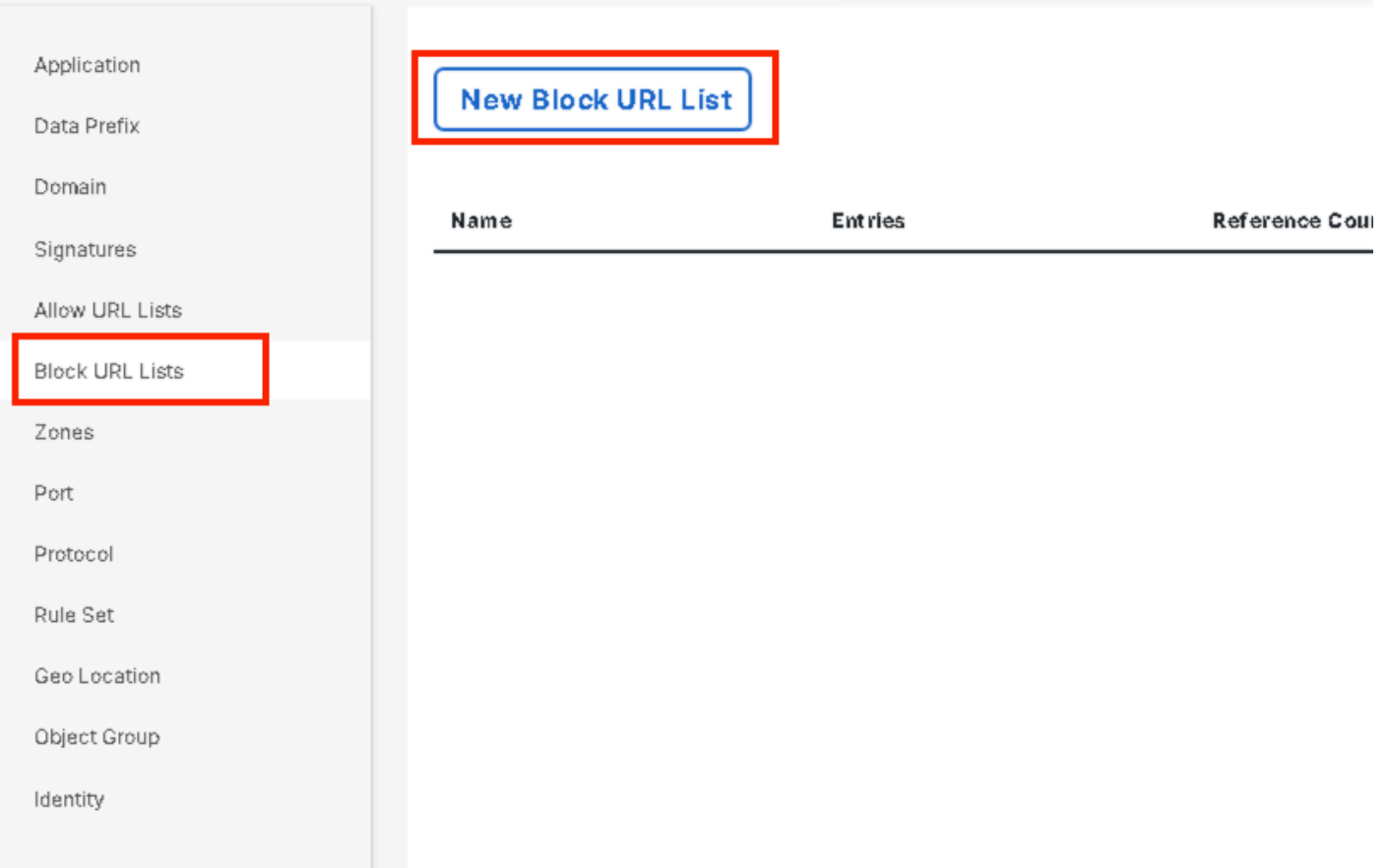


注意：可以考慮在允許清單和阻止清單中為域名使用regex模式

---

按一下左側窗格中的Block URLs Lists，然後建立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
------	---------	-----------------

- 在「URL清單名稱」欄位中，輸入最多包含32個字元（僅限字母、數字、連字型大小和底線）的清單名稱
- 在URL欄位中，輸入要包含在清單中的URL，並以逗號分隔。還可以使用導入按鈕從可訪問的儲存位置增加清單。
- 完成後，按一下Add。



**New Block URL List**

Block URL List Name\*

Guest\_Block

Add Block URL \*

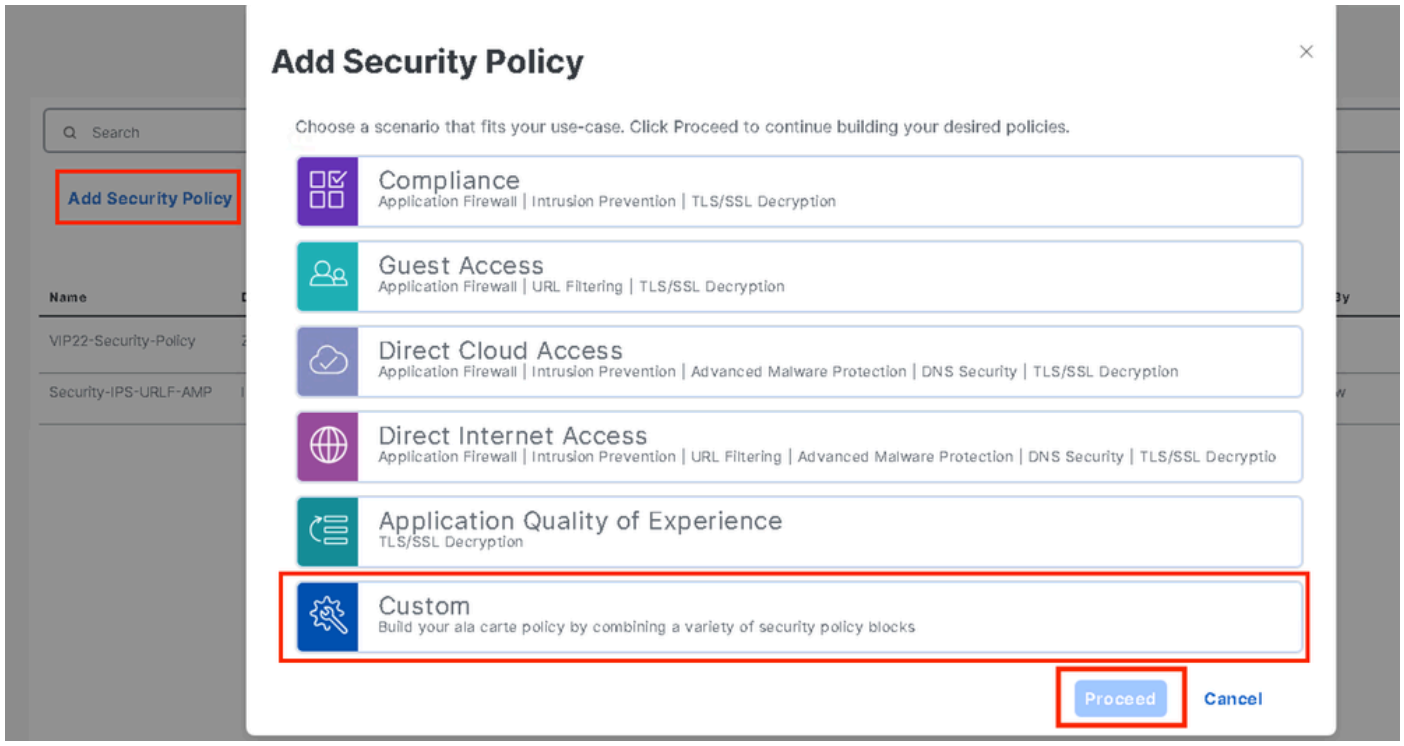
www.youtube.com,www.facebook.com,instagram.com

Import

Add Cancel

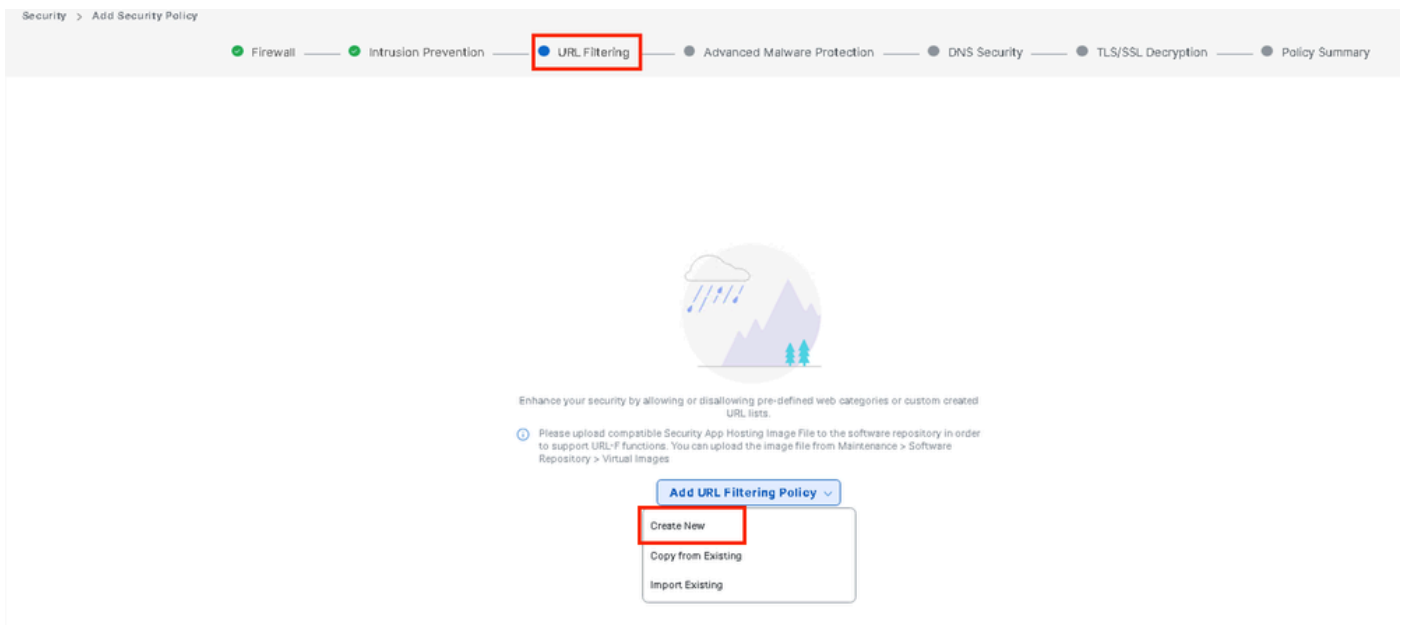
## 建立安全策略

2. 在Cisco SD-WAN Manager選單上，導航到Configuration > Security，然後按一下Add new security policy。將打開「增加安全策略」嚮導，並顯示各種使用案例場景或使用清單中的現有策略。選擇custom，然後按一下Proceed在嚮導中增加URL過濾策略。

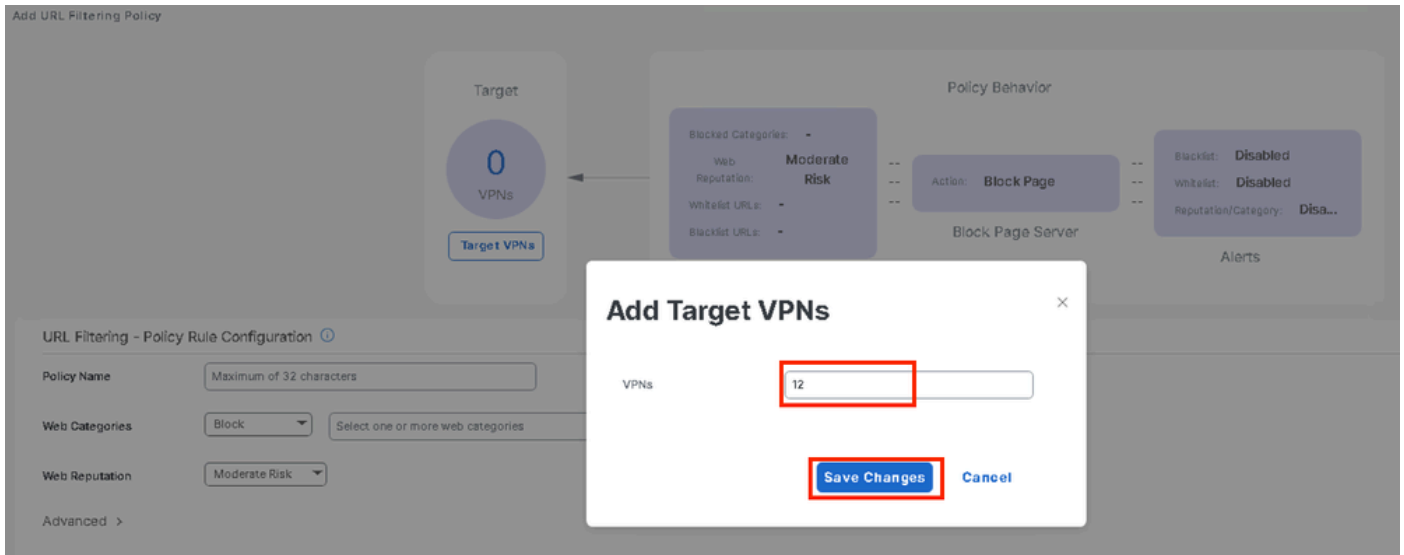


注意：在增加安全策略中，選擇支援URL過濾的方案（訪客訪問、直接網際網路訪問或自定義）。

在增加安全策略嚮導，按一下下一步，直到顯示URL過濾窗口。現在轉到URL Filtering > Add URL Filtering Policy > Create New以建立URL過濾策略。按一下下一步



按一下Target VPNs以便在Add Target VPNs嚮導中增加所需的VPN數量。

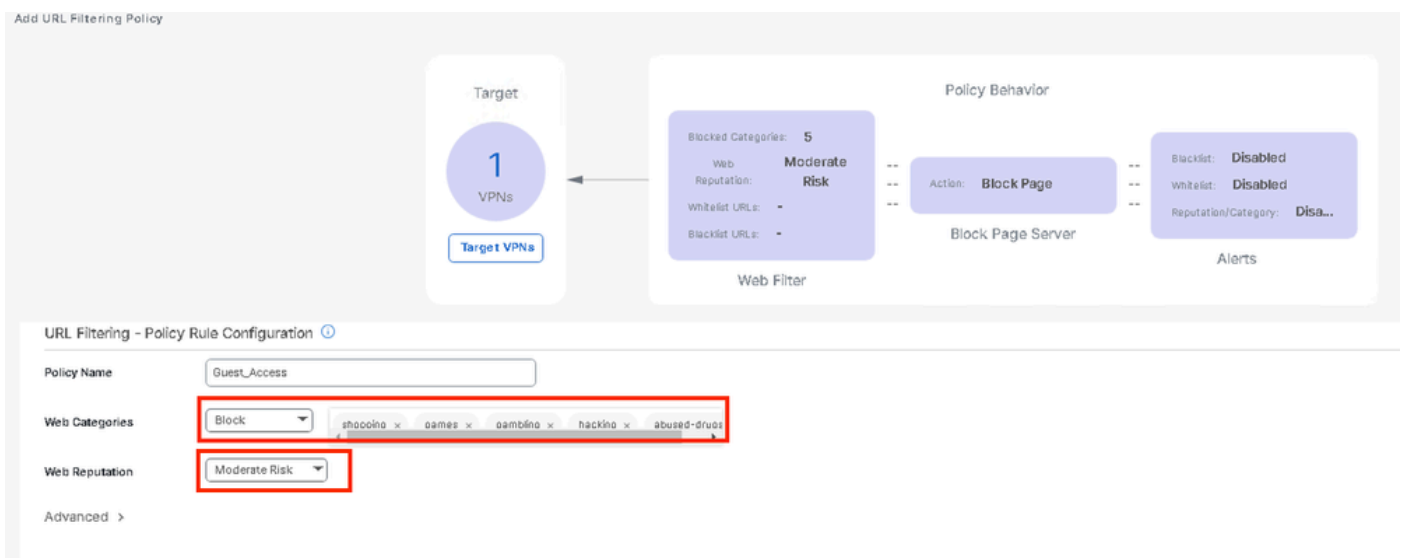


- 在Policy Name欄位中輸入策略名稱。
- 從Web Categories ( Web類別 ) 下拉選單中選擇其中一個選項，選擇Block ( 阻止 ) ，則會阻止與您選擇的類別匹配的網站。

Block -阻止與您選擇的類別匹配的網站。  
 Allow -允許與您選擇的類別匹配的網站。

從下拉選單中選擇一個Web信譽(Web Reputation)，並將其設定為中度風險(Moderate Risk)。信譽得分等於或低於60分的所有URL都會被阻止。

- 高風險：信譽得分0到20。
- 可疑：信譽分數為0到40。
- 中等風險：信譽得分為0到60。
- 低風險：信譽得分為0到80。
- 值得信任：信譽得分為0到100。



在高級中，根據需要從Allowlist URL List或blocklist URL List下拉選單中選擇現有清單或建立新清單



Advanced ▾

**Whitelist URL List**

**Blacklist URL List**

Block Page Server

Block Page Content

**Default Content Header**

**Content Body**

**Guest\_Allow**

www\,google\.com

www\,yahoo\.com

[New Allow URL List](#)

**Blacklist URL List**

Block Page Server

Block Page Content

**Default Content Header**

**Content Body**

Redirect URL ⓘ

**Guest\_Block**

www\,youtube\.com

www\,facebook\.com

instagram.com

[New Block URL List](#)

如果需要，請更改「阻止頁面內容」下的內容正文，並確保已選擇所有警報。

按一下Save URL filtering策略以增加URL過濾策略。

## URL Filtering - Policy Rule Configuration ⓘ

Advanced ▾

Whitelist URL List

Blacklist URL List

Block Page Server

Block Page Content

Default Content Header

Content Body

Redirect URL ⓘ

Alerts and Logs ⓘ

Alerts  Blacklist  Whitelist  Reputation/Category

按一下Next，直到顯示「Policy Summary」頁。

在各自的欄位中輸入安全策略名稱和安全策略說明。

● 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

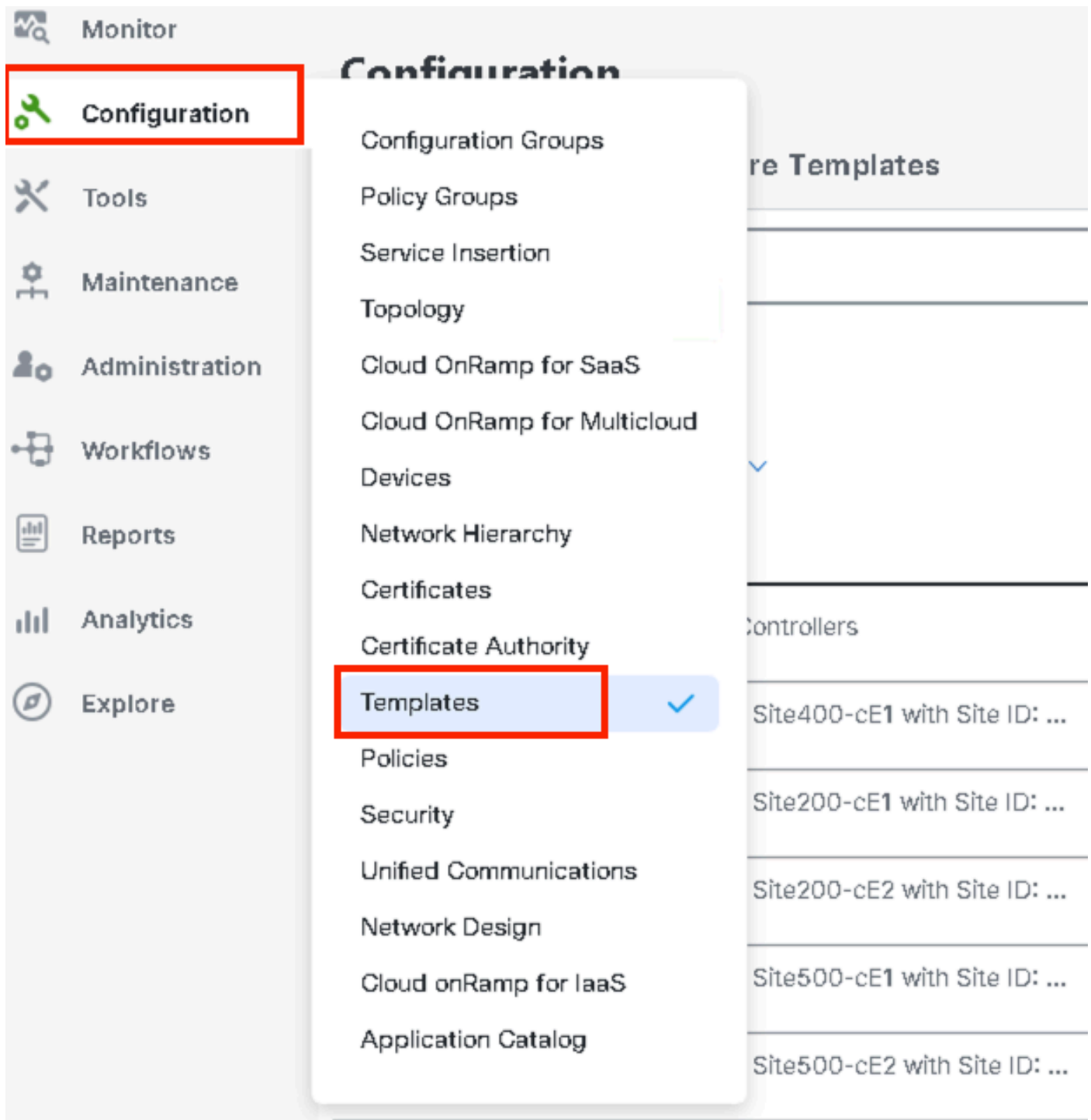
External Syslog Server  VPN  ⓘ Server IP

Failure Mode

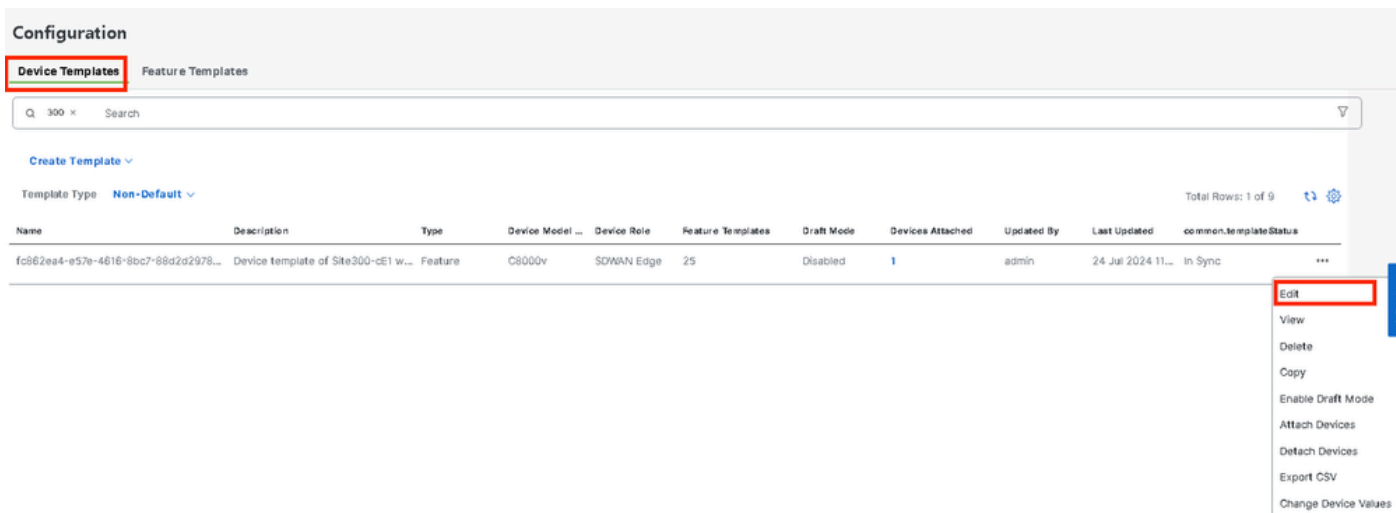
## 將安全策略應用於裝置

要將安全策略應用到裝置，請執行以下操作：

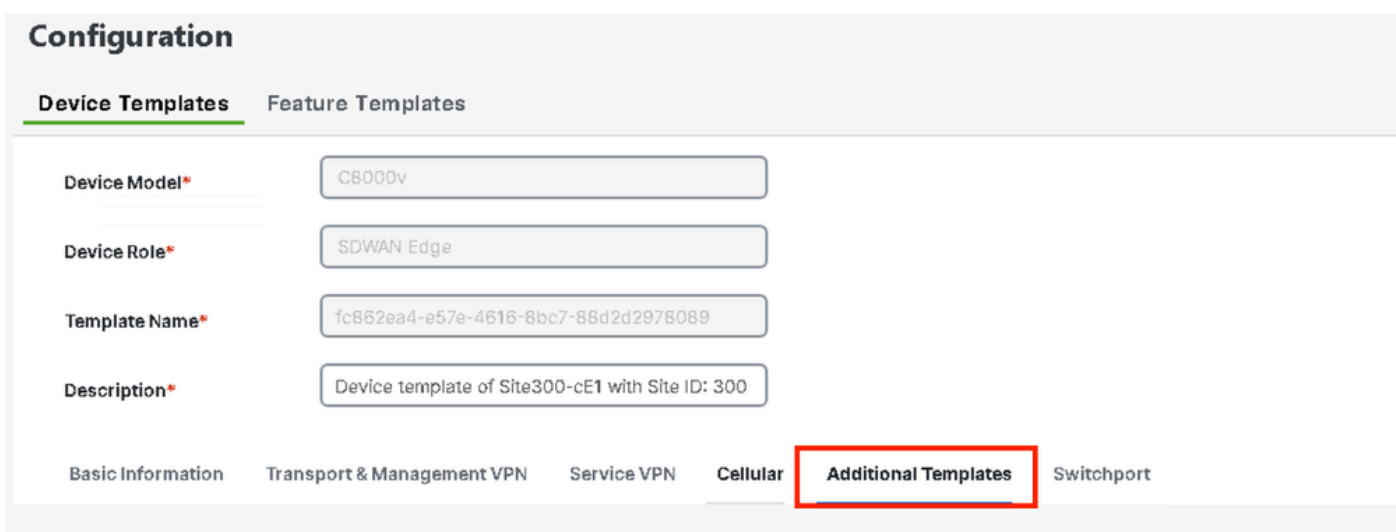
從Cisco SD-WAN Manager選單中，選擇Configuration > Templates。



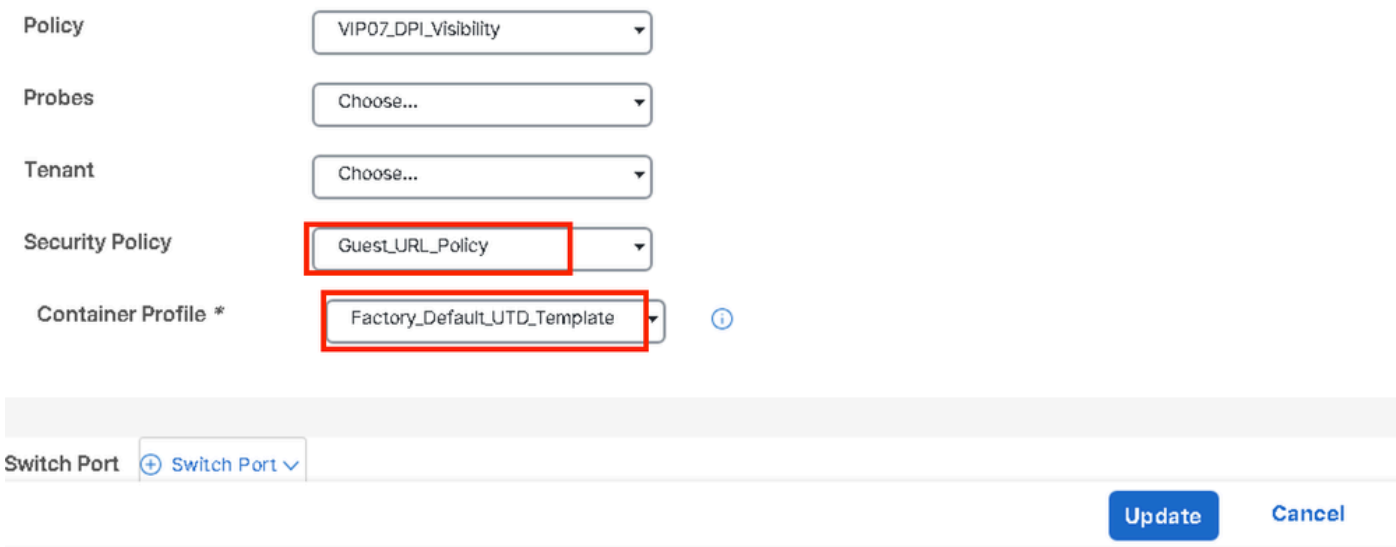
按一下Device Templates，然後按一下Edit on Device Template。



按一下Additional Templates。



- 從Security Policy下拉選單中，選擇之前在Guest\_URL\_Policy下配置的策略名稱，然後按一下Update。



按一下裝置，確保配置正確，然後按一下Config Diff和Side Diff。按一下Configure Devices。

Device Template: fc862ea4-e57e-4616-8... Total: 1

Config Preview | **Config Diff** | Side by Side Diff | Intent

Device list (Total: 1 devices)

Filter/Search

CBK-C19B1FE2-C89F-A311-DEA7-482A878B089A  
Site900-cE|11301

Configure Devi...

Local Configuration vs. New Configuration

1	1	system
2	2	ztp-status in-progress
3	3	device-model vedge-C8000V
4	4	gps-location latitude -23.60911
5	5	gps-location longitude -46.69768
6	6	system-ip 1.1.30.1
7	7	overlay-id 1
8	8	site-id 300
9	9	no transport-gateway enable
10	10	port-offset 0
11	11	control-session-pps 300
12	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
446   Administrator
447   exit
448 web-filter url profile Guest_Access
449   alert blacklist categories-reputation whitelist
450   blacklist
451   parameter-map regex Guest_Block-bl_
452   exit
453   categories block
454     abused-drugs
455     gambling
456     games
457     hacking
458     shopping
459   exit
460   block page-profile block-Guest_Access
461   log level error
462   reputation
463   block-threshold moderate-risk
464   exit
465   whitelist
466   parameter-map regex Guest_Allow-wl_
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

```

Back | **Configure Devices** | Cancel

vManage已成功使用安全策略配置裝置模板，並在邊緣裝置上安裝UTD軟體套件。

**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

## 修改URL篩選

要修改URL過濾策略，請執行以下步驟：

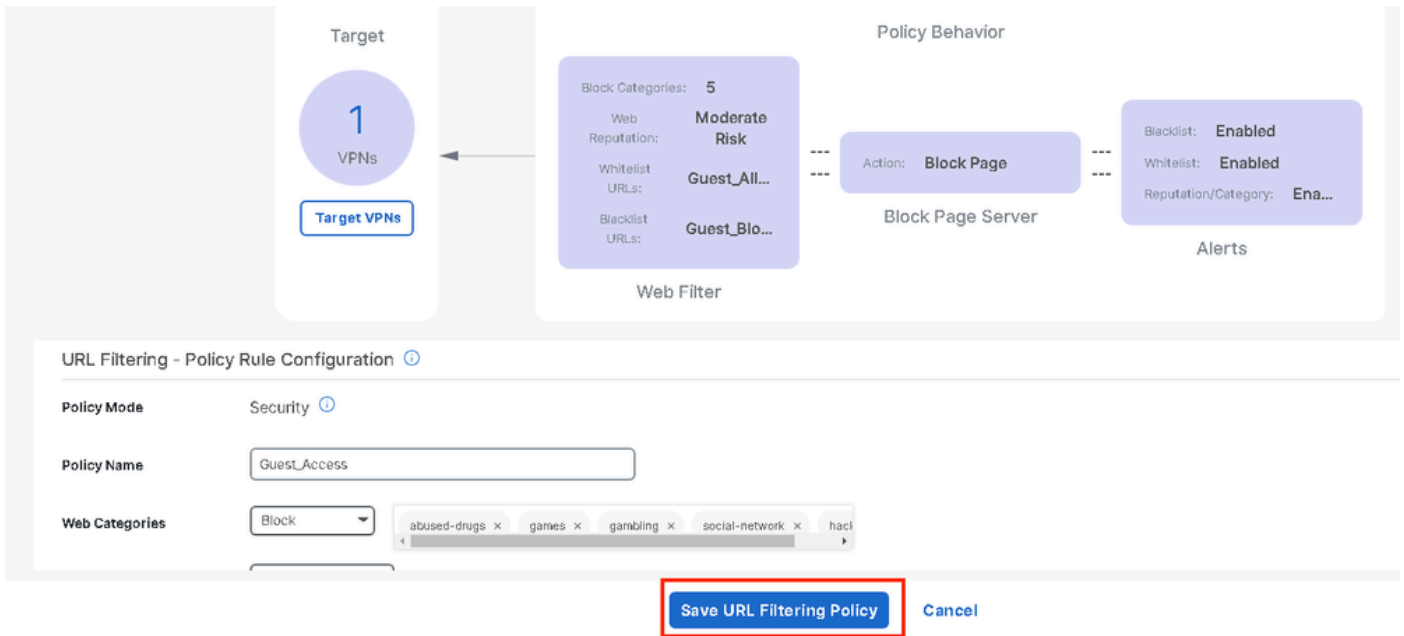
1. 從Cisco SD-WAN Manager選單中選擇Configuration > Security。
2. 在「Security」螢幕中，按一下Custom Options下拉選單，然後選擇Policies/Profiles。

Name	Description	Use Case	Policy Mode	Devices Attached	Device Templates/Config Groups	Updated By	Last Updated
VIP22-Security-Policy	ZBFW policy for DIA	Custom	security	0	0	admin	12 Apr 2024 8:32:39 PM

按一下左側頁籤上的URL Filtering，針對要修改的所需策略，按一下3點(...)，然後選擇Edit。

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

根據需要修改策略，然後按一下Save URL Filtering Policy。



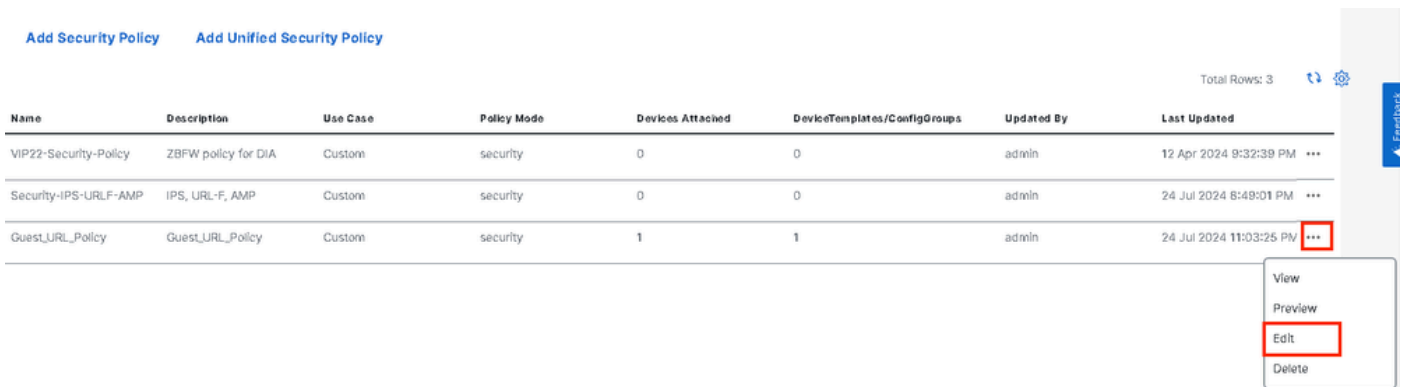
## 刪除URL篩選

要刪除URL過濾策略，必須首先從安全策略分離策略：

從Cisco SD-WAN Manager選單中，選擇Configuration > Security。

將URL過濾策略與安全策略分離：

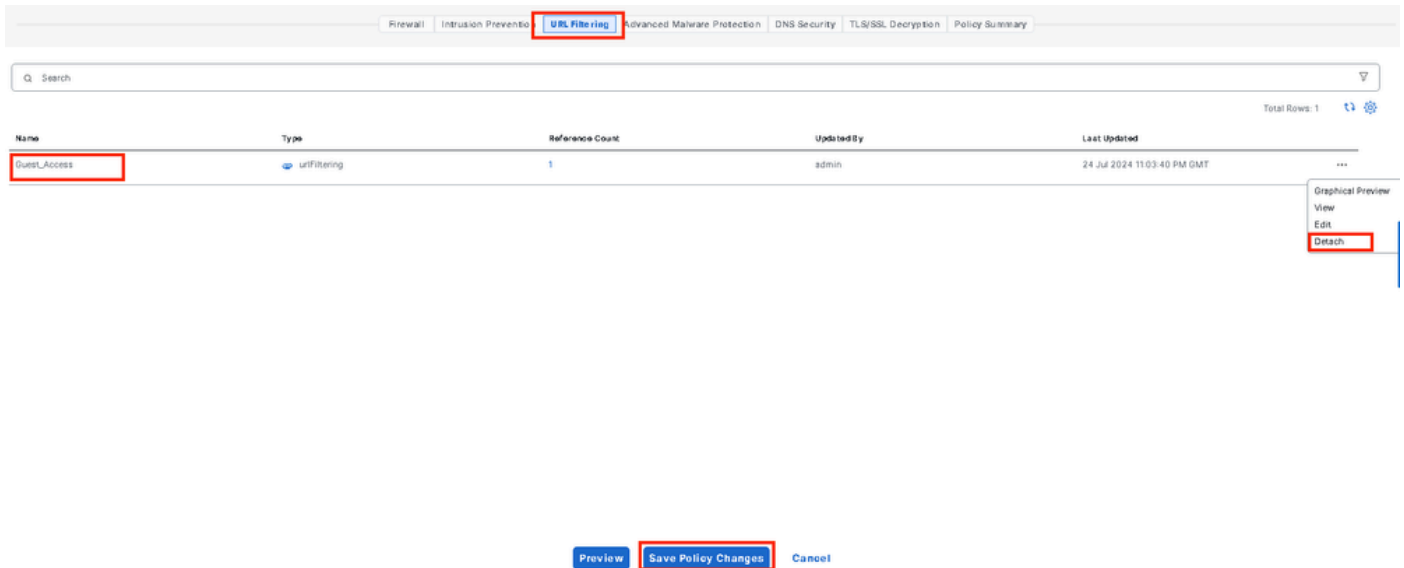
- 對於包含URL過濾策略的安全策略，請點選3點(...)，然後點選編輯。



接著顯示[原則摘要]頁面。按一下URL Filtering ( URL過濾 ) 頁籤。

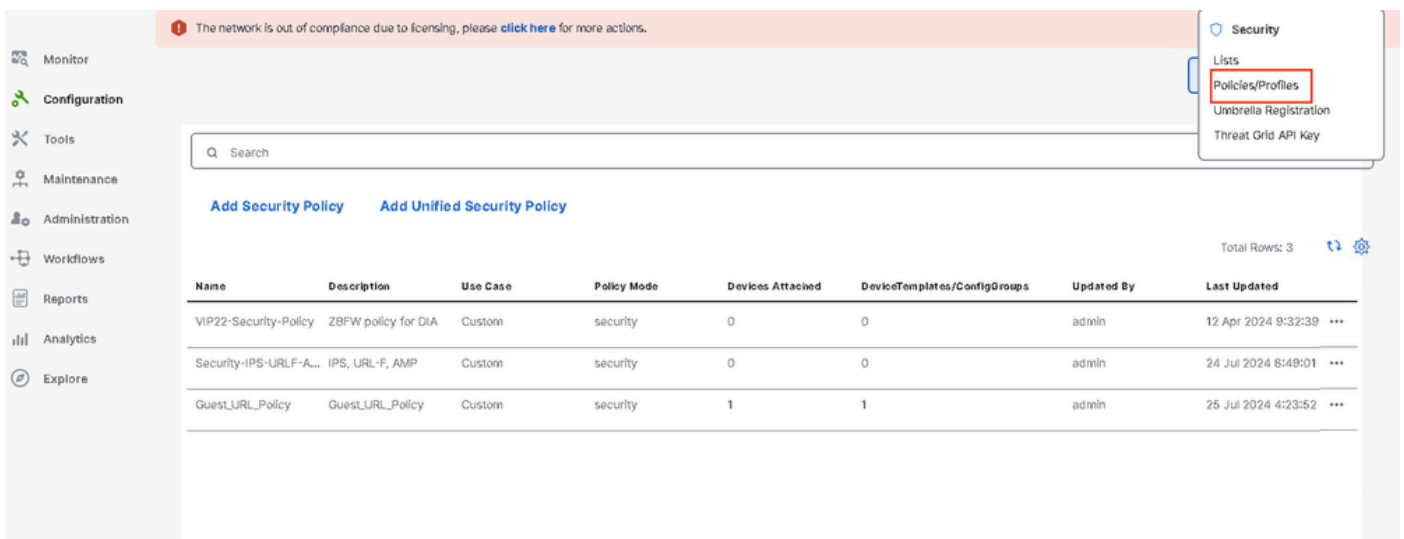
對於要刪除的策略，請點選3點(...)，然後選擇分離。

按一下Save Policy Changes。



要刪除URL過濾策略：

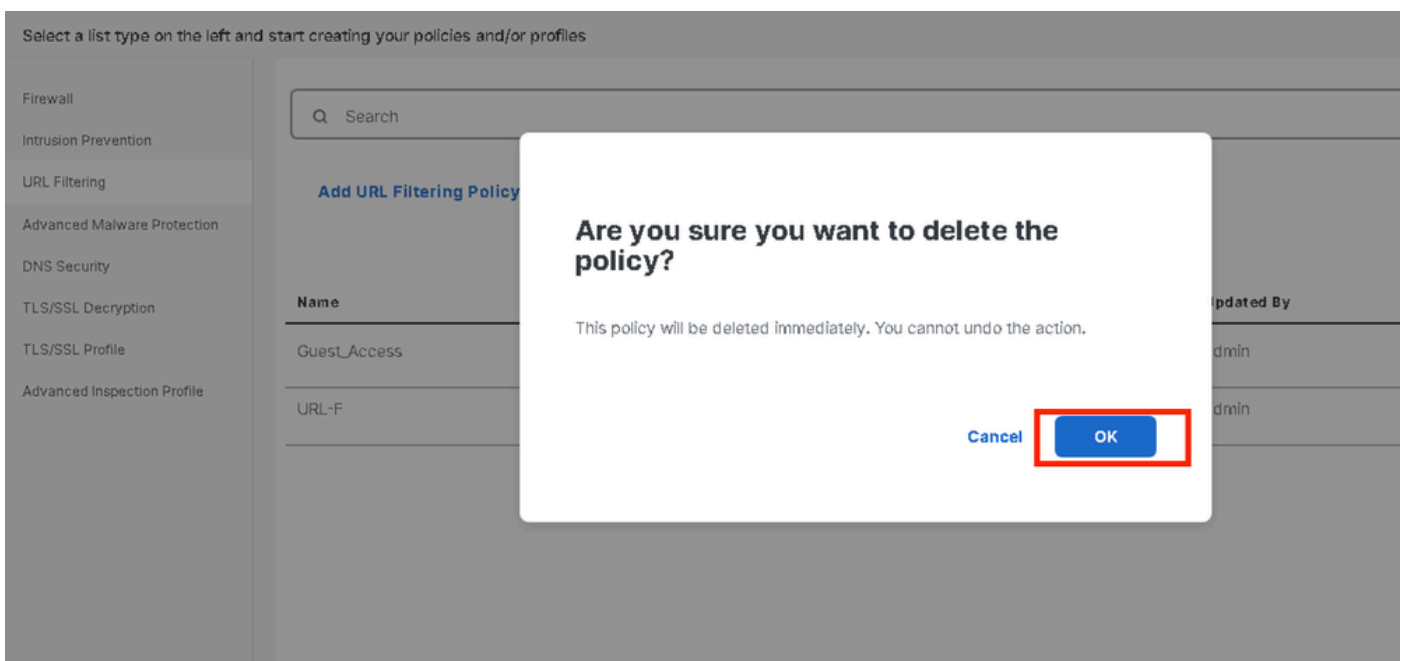
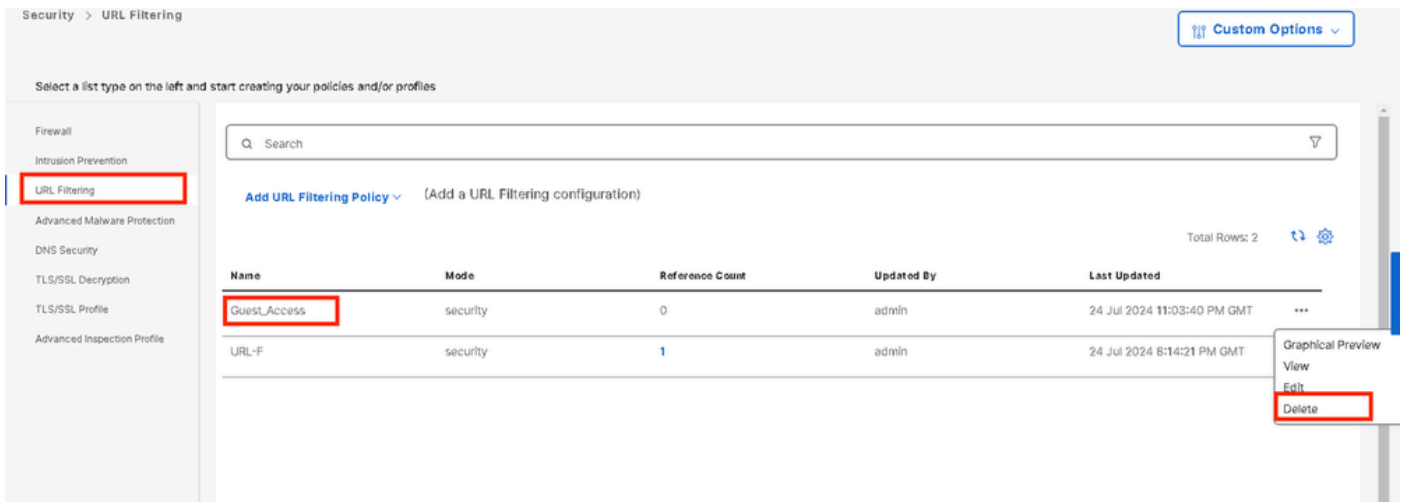
在Security螢幕中，點選Custom Options下拉選單（在Windows 2000中為Linux系統），選擇Policies/Profiles，然後選擇URL Filtering。



對於要刪除的策略，請點選3點(...)，然後點選刪除。

按一下OK。





## 驗證

驗證是否已安裝Cisco UTD版本。

<#root>

```
Site300-cE1#show utd engine standard version
```

```
UTD Virtual-service Name: utd
```

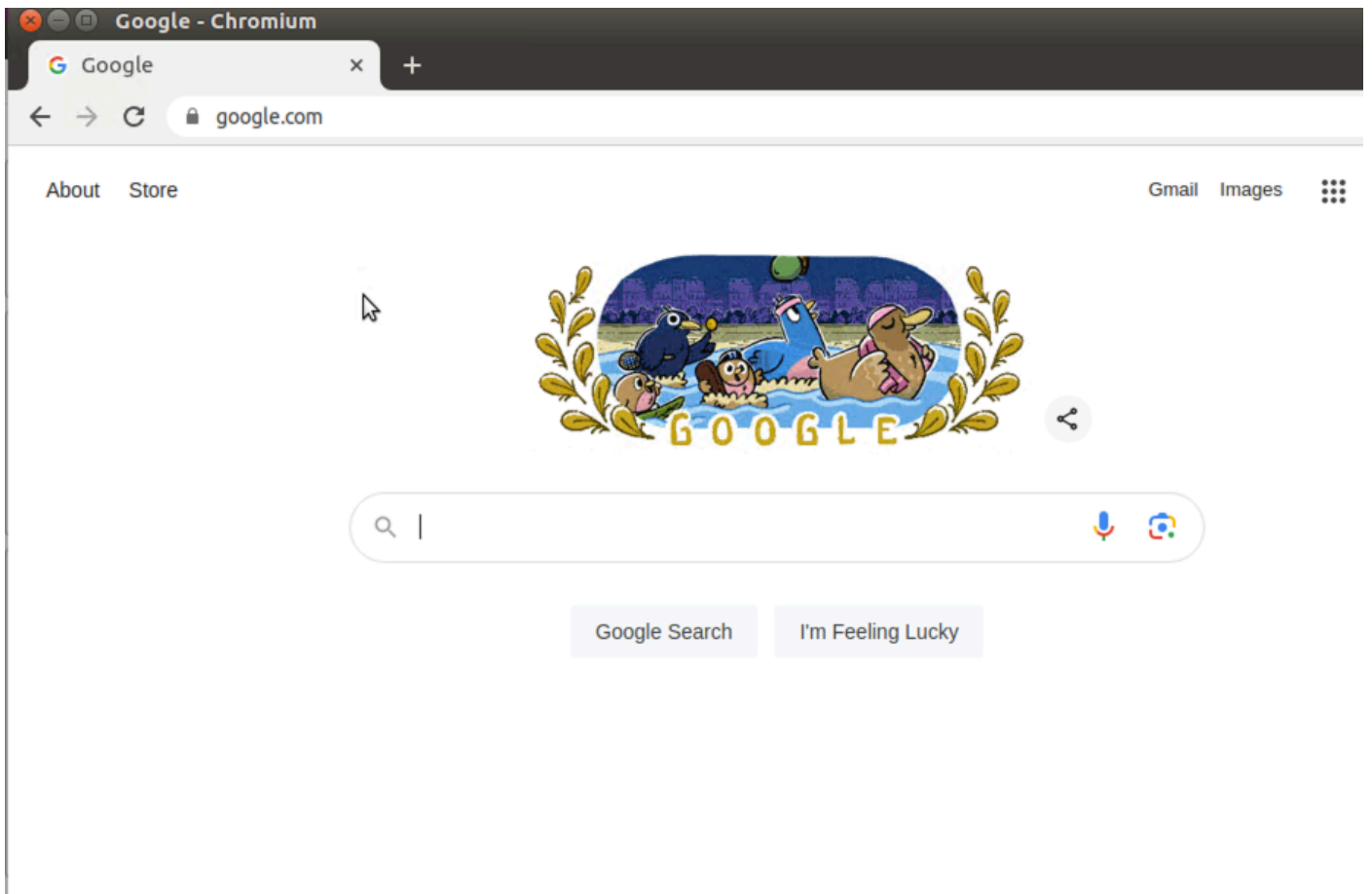
```
IOS-XE Recommended UTD Version: 1.0.2_SV3.1.67.0_XE17.14
```

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

```
UTD Installed Version:
```

```
1.0.2_SV3.1.67.0_XE17.14
```

在位於訪客VPN上的客戶端PC上，如果您嘗試打開google.com和yahoo.com，則允許這些訪問。



<#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

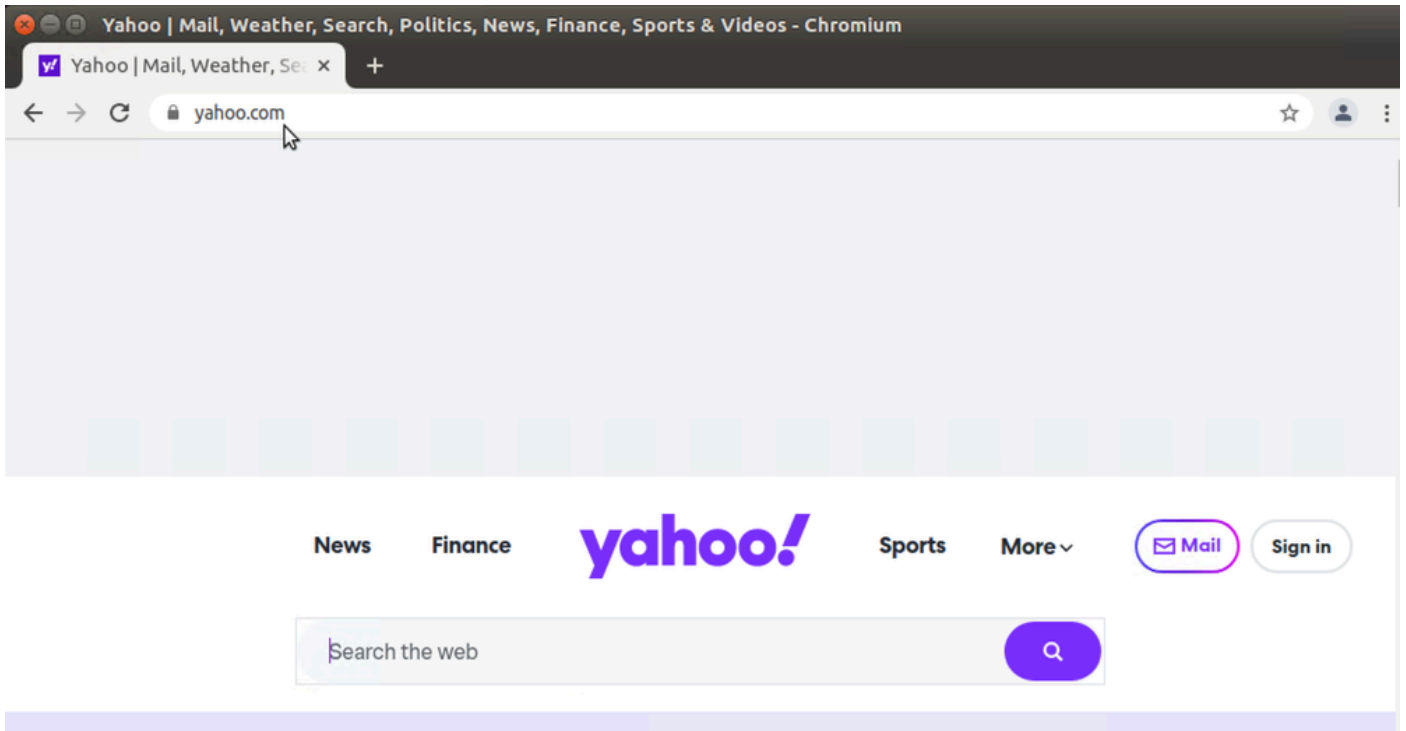
[\*\*]

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

[\*\*]

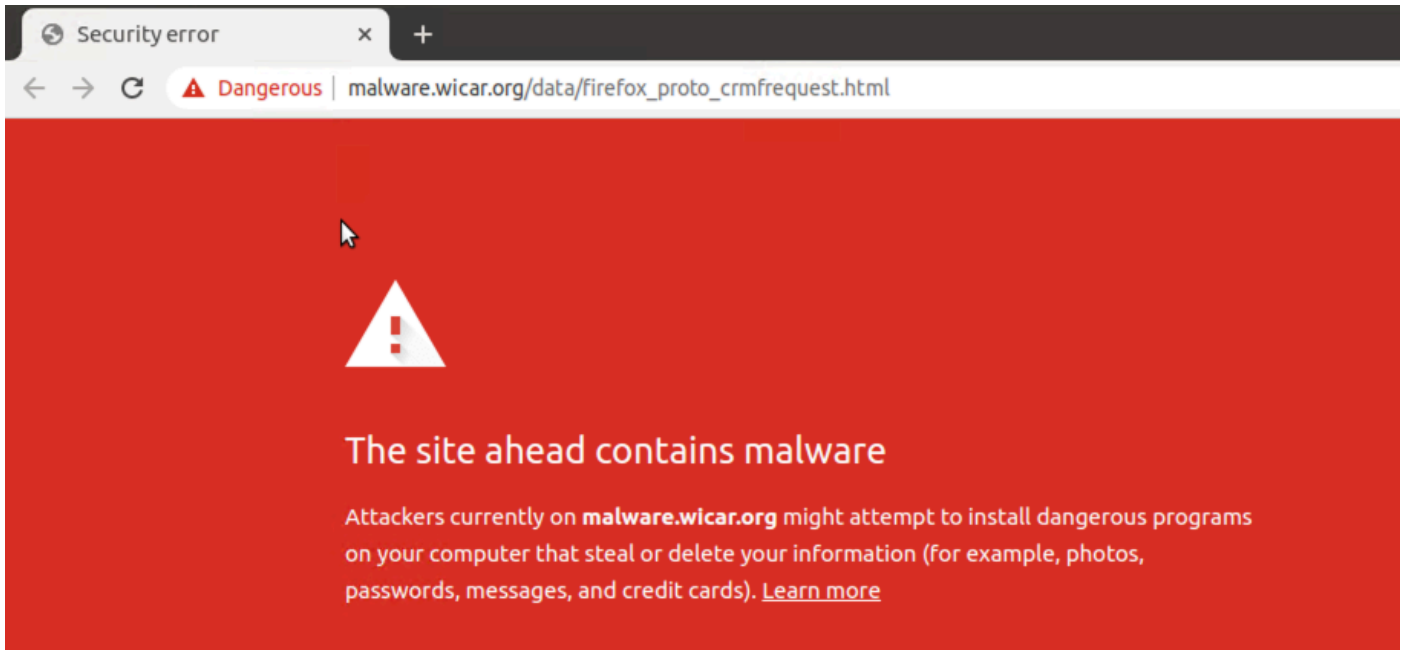
UTD WebFilter Allowlist

[\*\*] [

URL: www.yahoo.com

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

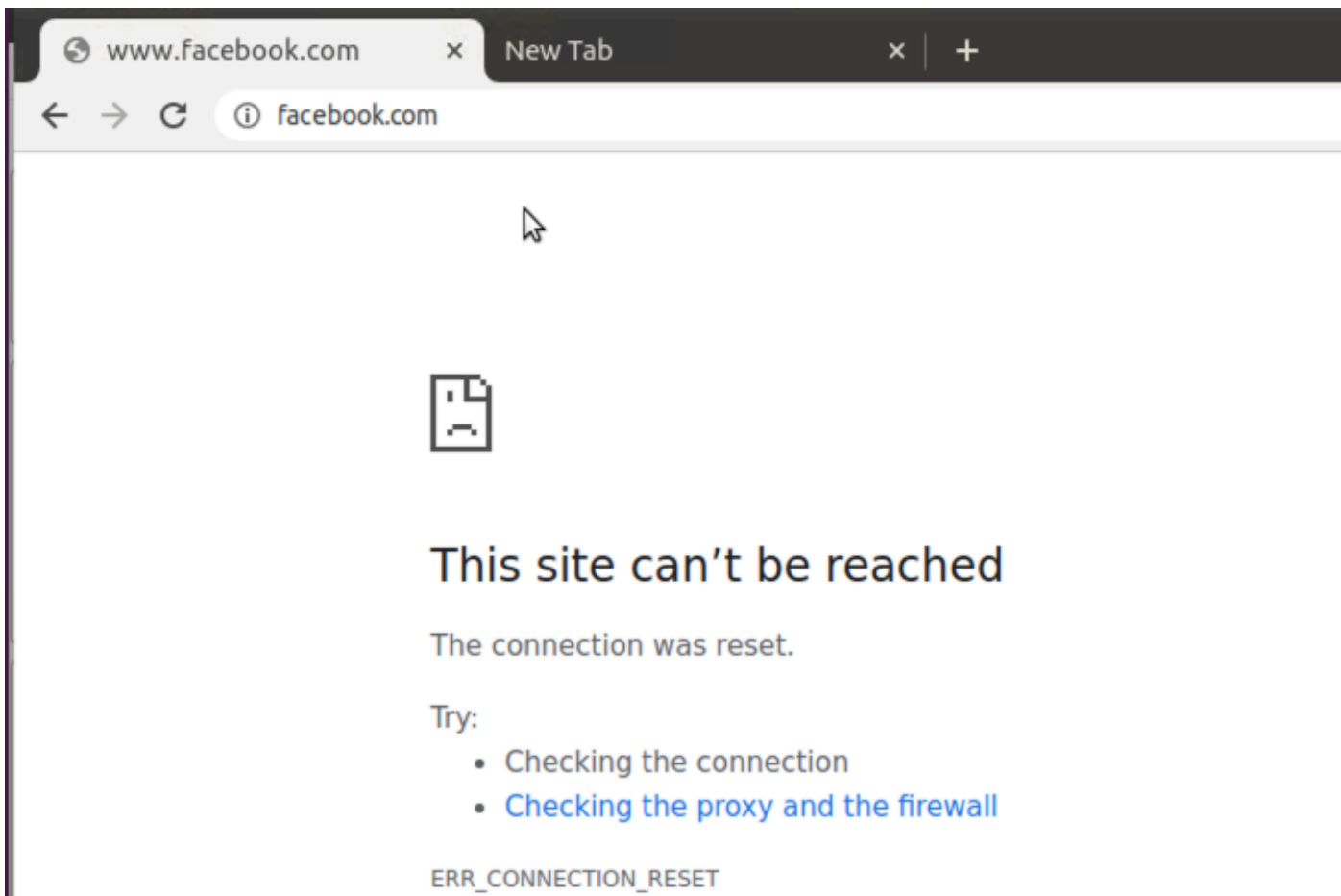
從位於訪客VPN上的客戶端PC上，如果您嘗試打開信譽得分較低的網頁，或者從其中一個被阻止的Web類別打開，URL過濾引擎將拒絕HTTPS請求。



<#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
```

在位於訪客VPN上的客戶端PC上，如果您嘗試打開facebook，instagram和youtube將被阻止。



<#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

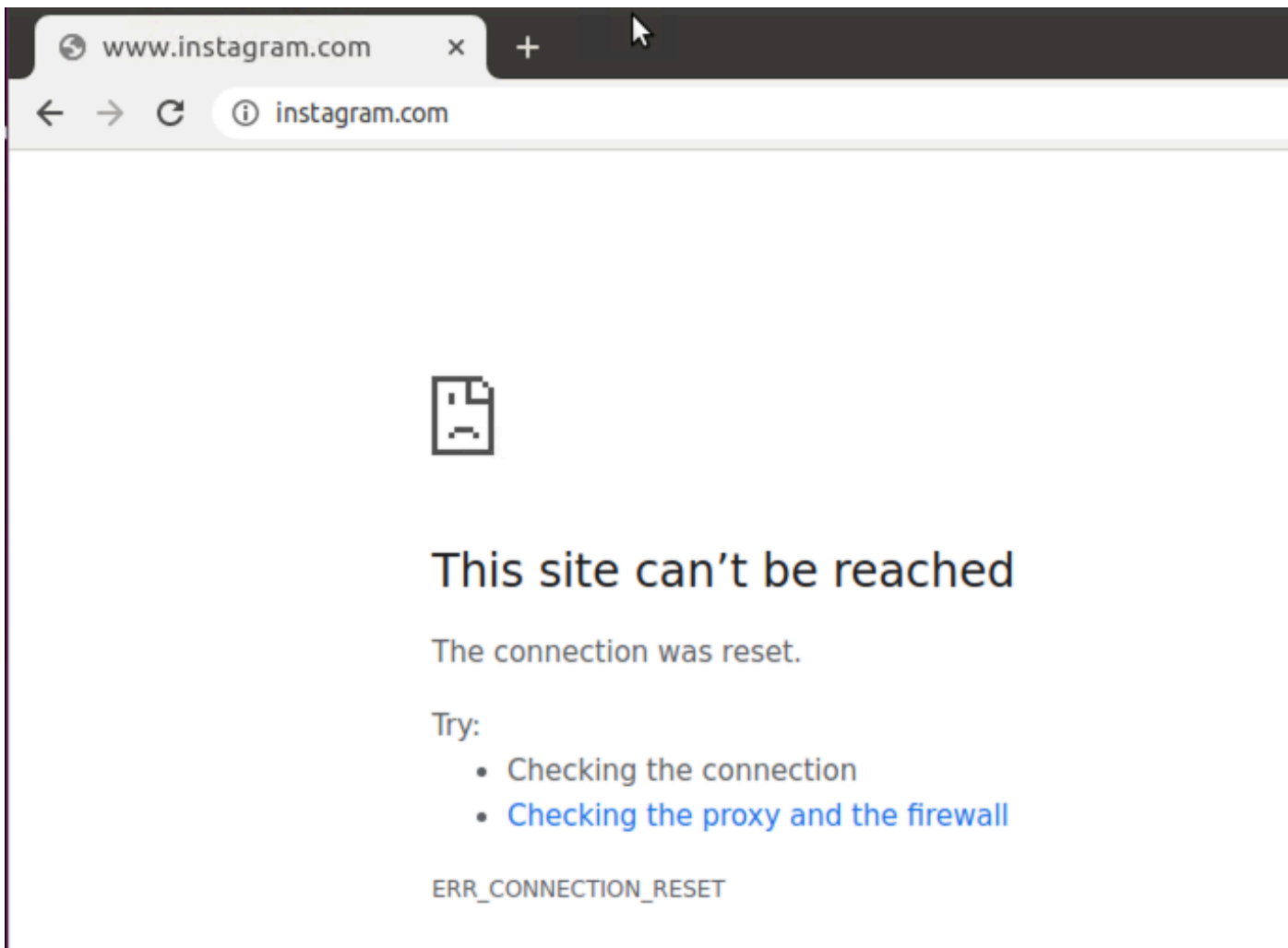
[\*\*]

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

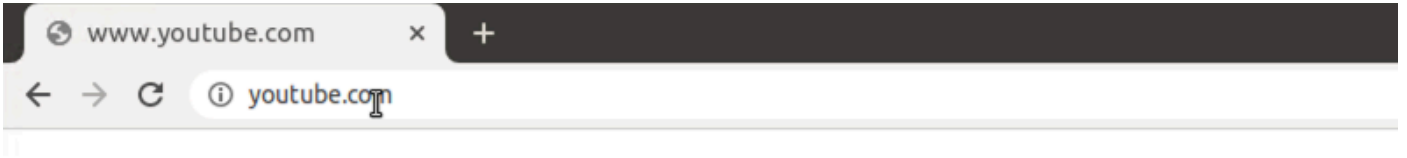
[\*\*]

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

## 從vManage GUI監控URL過濾

您可以使用這些步驟，按網路類別即時或歷史地監控每台裝置的URL過濾。

監控Cisco IOS XE Catalyst SD-WAN裝置上被阻止或允許的URL：

1. 在Cisco SD-WAN Manager選單中，選擇Monitor > Devices > Select Device



The screenshot shows a network management interface. On the left, a sidebar menu has 'Monitor' highlighted with a red box. A dropdown menu is open under 'Monitor', with 'Devices' selected and also highlighted with a red box. The main content area shows a table of devices 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. 在左窗格的「安全監控」下，按一下「URL過濾」。URL過濾資訊顯示在右窗格中。

- 按一下Blocked。系統將顯示阻止URL上的會話計數。
- 按一下允許。系統將顯示允許URL上的會話計數。



---

注意：UTD安裝的版本不能處於「不受支援」狀態。

---

檢查UTD是否處於onrunning狀態。

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

驗證UTD健康狀況為綠色。

<#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

驗證是否已啟用URL過濾功能。

<#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

要顯示URL過濾日誌，請運行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：運行clear utd engine standard logging events命令清除舊事件。

---

將輸入/輸出資料包檢查到UTD容器，查詢延遲。

```
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

## 相關資訊

- [Cisco Catalyst SD-WAN安全配置指南](#)
- [在cEdge路由器上安裝UTD安全虛擬映像](#)
- [透過UTD和URL過濾排除資料路徑處理故障](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。