

Configure and Verify URL Filtering

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[Configure Components for URL-Filtering Policy](#)

[Create URL Lists of Interest](#)

[Create Security Policy](#)

[Apply a Security Policy to a Device](#)

[Modify URL Filtering](#)

[Delete URL Filtering](#)

[Verify](#)

[Monitor URL Filtering From vManage GUI](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes how to configure and verify URL Filtering on Cisco IOS-XE® routers using Cisco Catalyst Manager GUI.

Prerequisites

Upload compatible UTD Software virtual image with the current Cisco IOS-XE code in vManage. Please check the Related information section for instructions on how to install the UTD Security Virtual Image on cEdge Routers.

Cisco Edge router must be on vManaged mode with template pre attached.

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco SD-WAN Overlay bring up with initial configuration.
- URL Filtering configuration Cisco Catalyst Manager GUI.

Components Used

This document is based on these software and hardware versions:

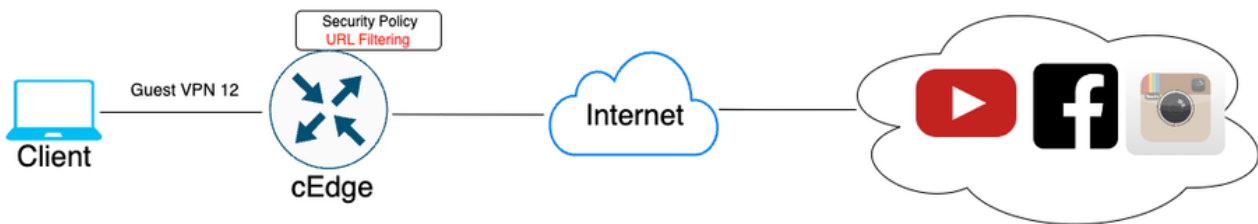
- Cisco Catalyst SD-WAN Manager version 20.14.1.
- Cisco Catalyst SD-WAN Controller version 20.14.1.

- Cisco Edge Router version 17.14.1.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



Configure Components for URL-Filtering Policy

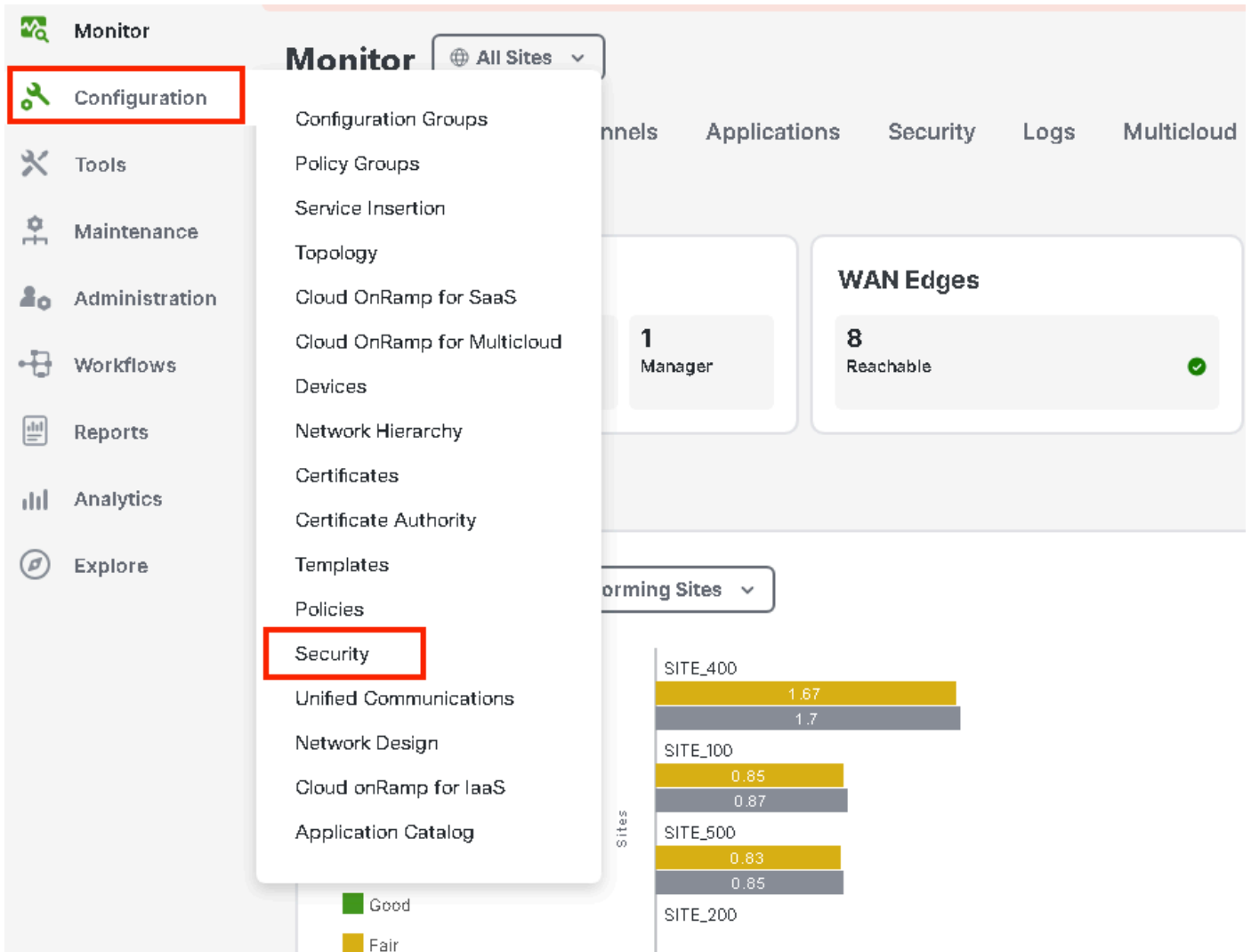
This article explains how to configure URL-Filtering to block/allow certain client HTTPS traffic based on category, reputation, or by domain block/allow lists given these example requirements:

- Block this HTTPS requests from clients on the guest VPN web categories:
 - Games
 - Gambling
 - Hacking
 - Illegal drugs
- Any HTTPS URL request to websites from client on guest VPN with a web reputation less than and equal to 60 must be blocked.
- HTTP(s) requests to websites from clients on the guest VPN block Facebook, Instagram, and YouTube, while allowing access to google.com and yahoo.com.

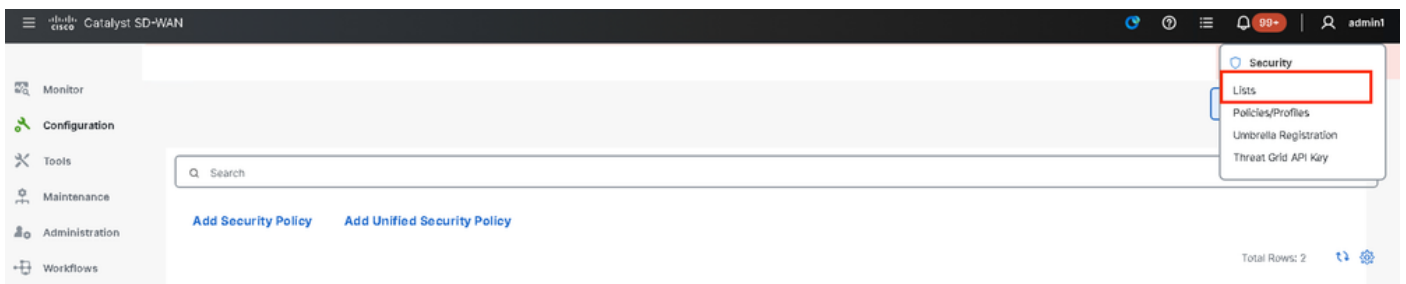
To configure URL Filtering:

Create URL Lists of Interest

1. On the Cisco SD-WAN Manager menu, navigate to **Configuration** > **Security** tab in the left side panel.



To create or manage **Allowlist URL List** or **Blocklist URL List**, select **Lists** from the **Custom Options** drop-down menu at the top right of the page.



Click on **Allow URLs Lists** from the left pane and create **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			

- In the URL List Name field, enter a list name consisting of up to 32 characters (letters, numbers, hyphens and underscores only).
- In the URL field, enter URLs to include in the list, separated with commas. You also can use the **Import** button to add lists from an accessible storage location.
- Click **Add** when you are finished.

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

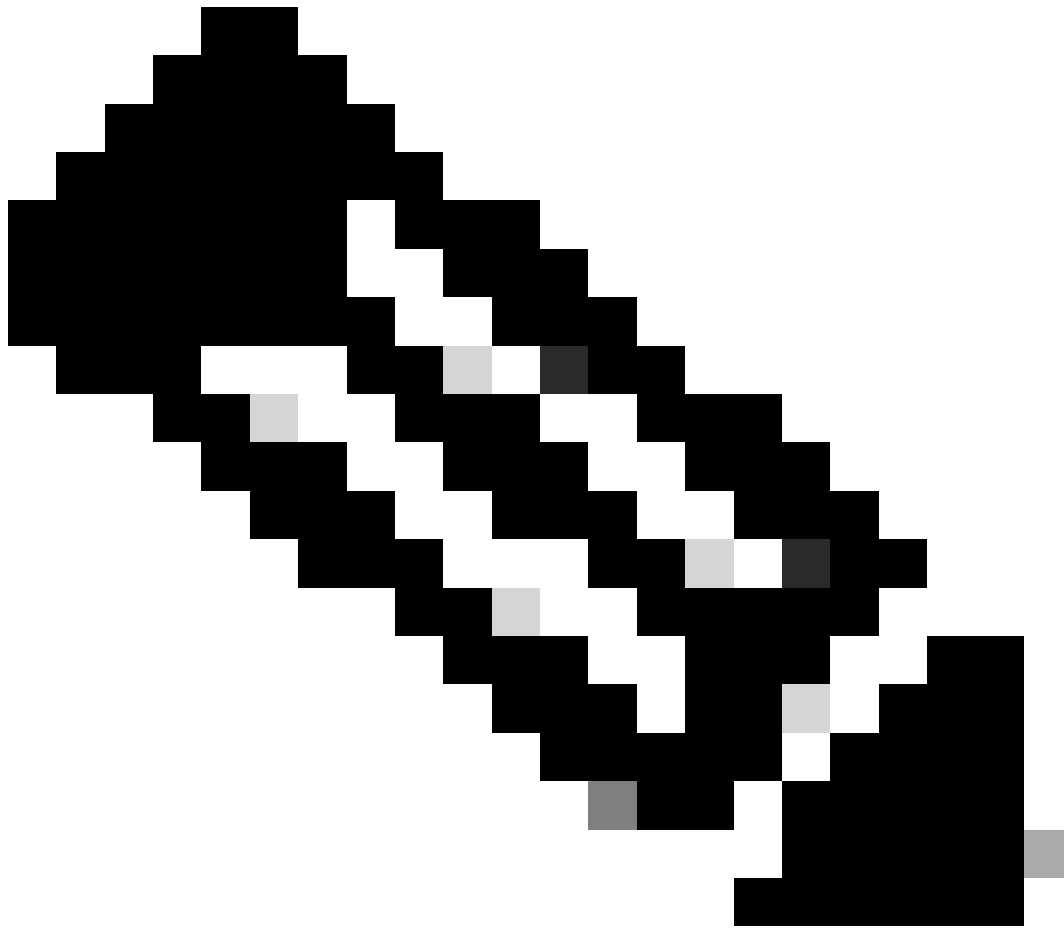
Add Allow URL *

www.google.com, www.yahoo.com

Import

Add

Cancel



Note: You can consider using a regex pattern for the domain name in allow and block lists

Click on **Block URLs Lists** from the left pane and create **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
------	---------	-----------------

- In the URL List Name field, enter a list name consisting of up to 32 characters (letters, numbers, hyphens and underscores only)
- In the URL field, enter URLs to include in the list, separated with commas. You also can use the **Import** button to add lists from an accessible storage location.
- Click **Add** when you are finished.

New Block URL List

Block URL List Name*

Guest_Block

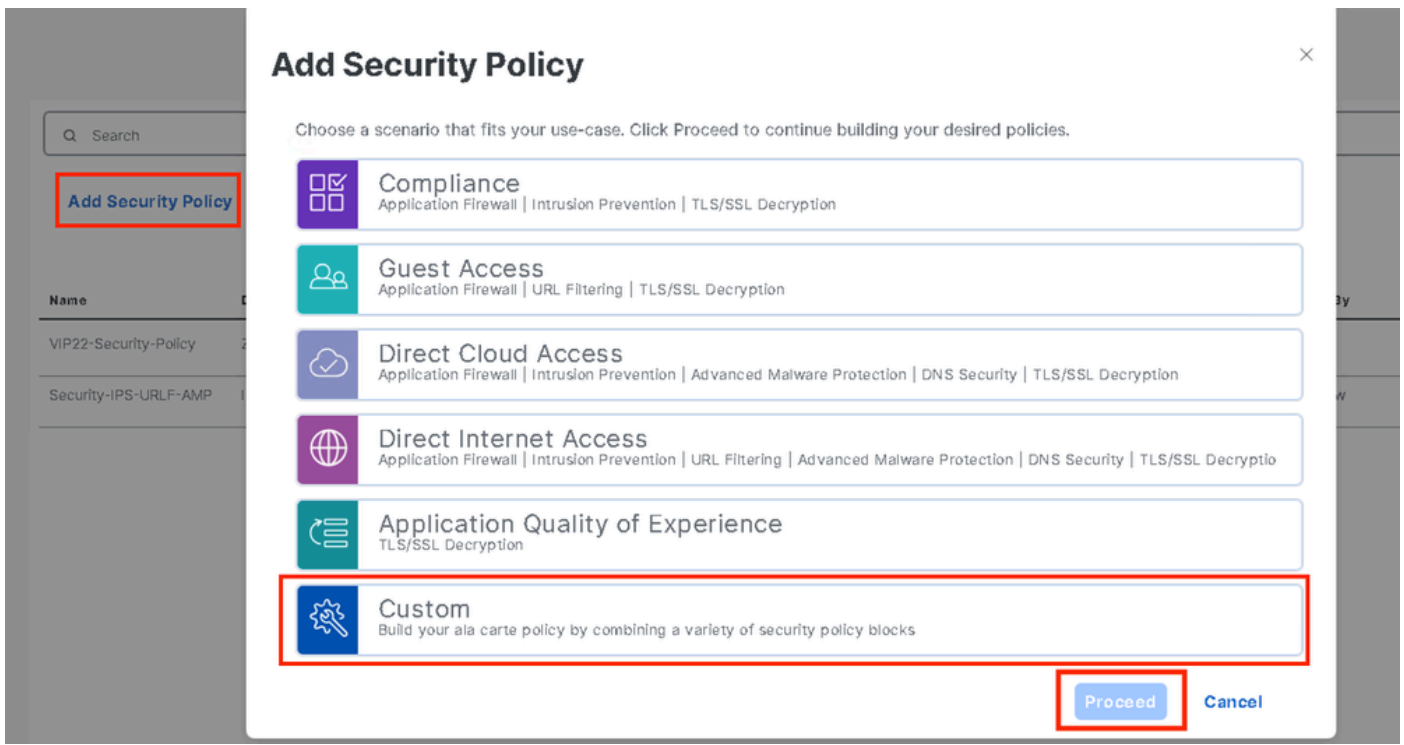
Add Block URL *

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

Add Cancel

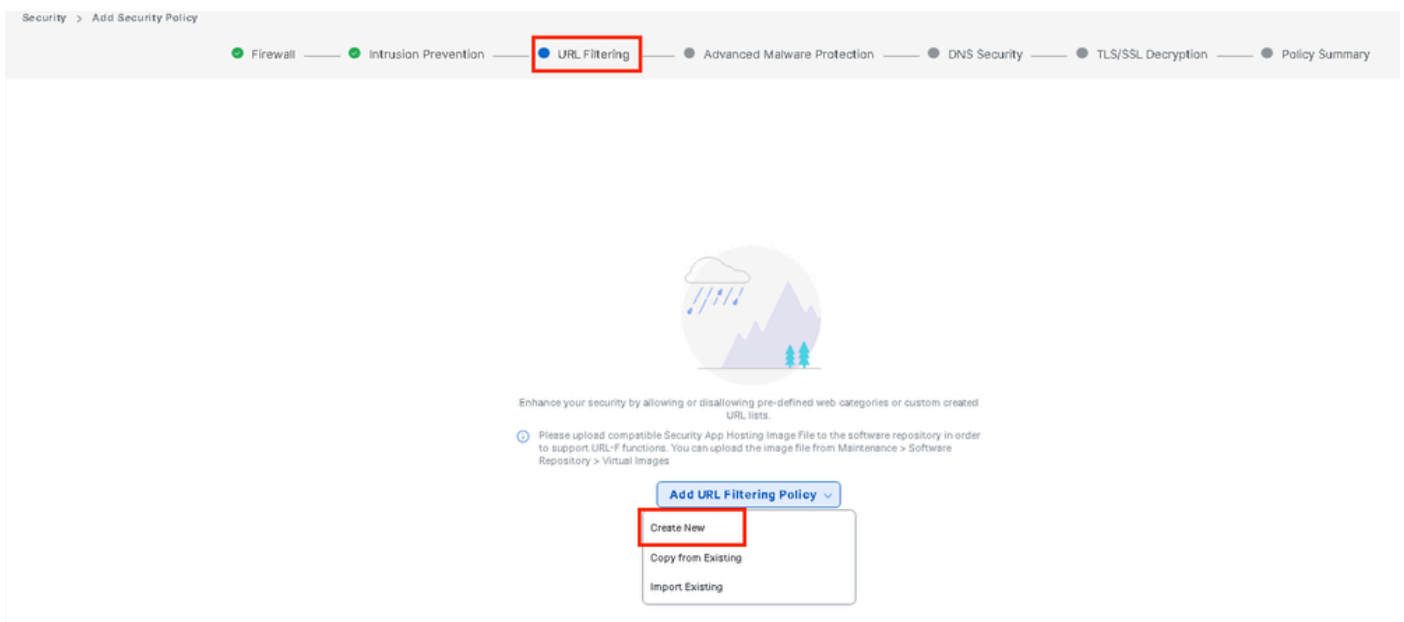
Create Security Policy

2. On the Cisco SD-WAN Manager menu, navigate to **Configuration > Security** Click on **Add new security policy**. The Add Security Policy wizard opens and various use-case scenarios are displayed or use existing policy from the list. Select **custom**, Click **Proceed** to add a URL filtering policy in the wizard.

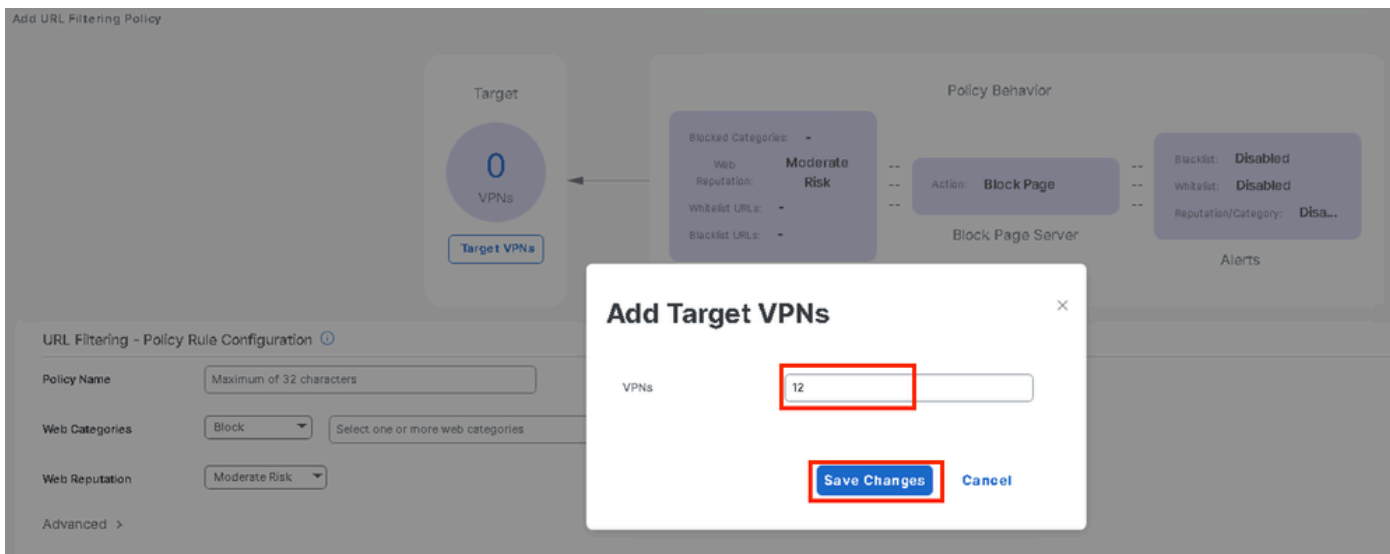


Note: In Add Security Policy, choose a scenario that supports URL filtering (Guest Access, Direct Internet Access, or Custom).

In the Add Security Policy wizard, click **Next** until the URL Filtering window is displayed. Now create a URL Filtering policy by going to **URL Filtering > Add URL Filtering Policy > Create New**. Click **Next**



Click **Target VPNs** to add the required number of VPNs in the Add Target VPNs wizard.



- Enter a policy name in the **Policy Name** field.
- Choose one of these options from the **Web Categories** drop-down, select **Block** and the websites that match the categories that you choose are blocked.

Block—Block websites that match the categories that you select.

Allow—Allow websites that match the categories that you select.

Choose a **Web Reputation** from the drop-down menu and set to **Moderate Risk**. Any URL that has a reputation score of 60 or lower is blocked.

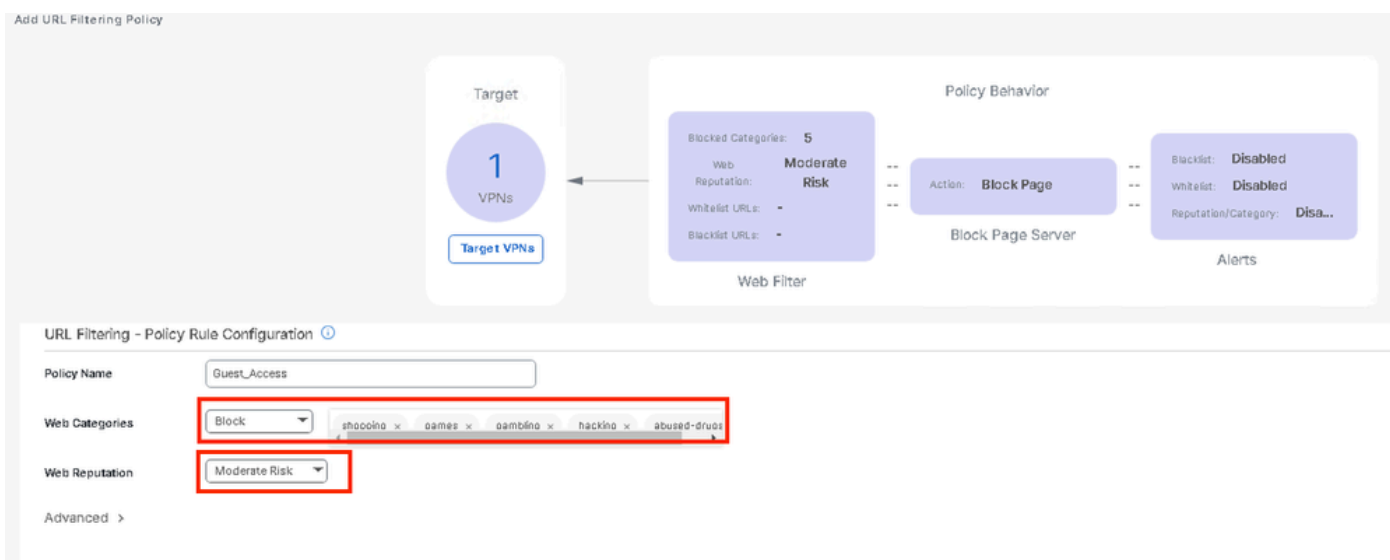
High Risk: Reputation score of 0 to 20.

Suspicious: Reputation score of 0 to 40.

Moderate Risk: Reputation score of 0 to 60.

Low Risk: Reputation score of 0 to 80.

Trustworthy: Reputation score of 0 to 100.



From **Advanced**, choose existing lists or create new list as needed from the **Allowlist URL List** or **blocklist URL List** drop-down menu.

Advanced ▾

Whitelist URL List

Select a whitelist url list

Blacklist URL List

Search

Guest_Allow

Guest_Allow

www\,google\.com

www\,yahoo\.com

Block Page Server

Block Page Content

Default Content Header

[New Allow URL List](#)

Blacklist URL List

Select a blacklist url list

Block Page Server

Block Page Content

Default Content Header

Content Body

Redirect URL ⓘ

Search

Guest_Block

Guest_Block

www\,youtube\.com

www\,facebook\.com

instagram.com

[New Block URL List](#)

If needed, change content body under Block Page Content and make sure all the Alerts are selected.

Click **Save URL filtering** Policy to add an URL filtering policy.

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

Click **Next** until the Policy Summary page is displayed.

Enter Security Policy Name and Security Policy Description in the respective fields.

● 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

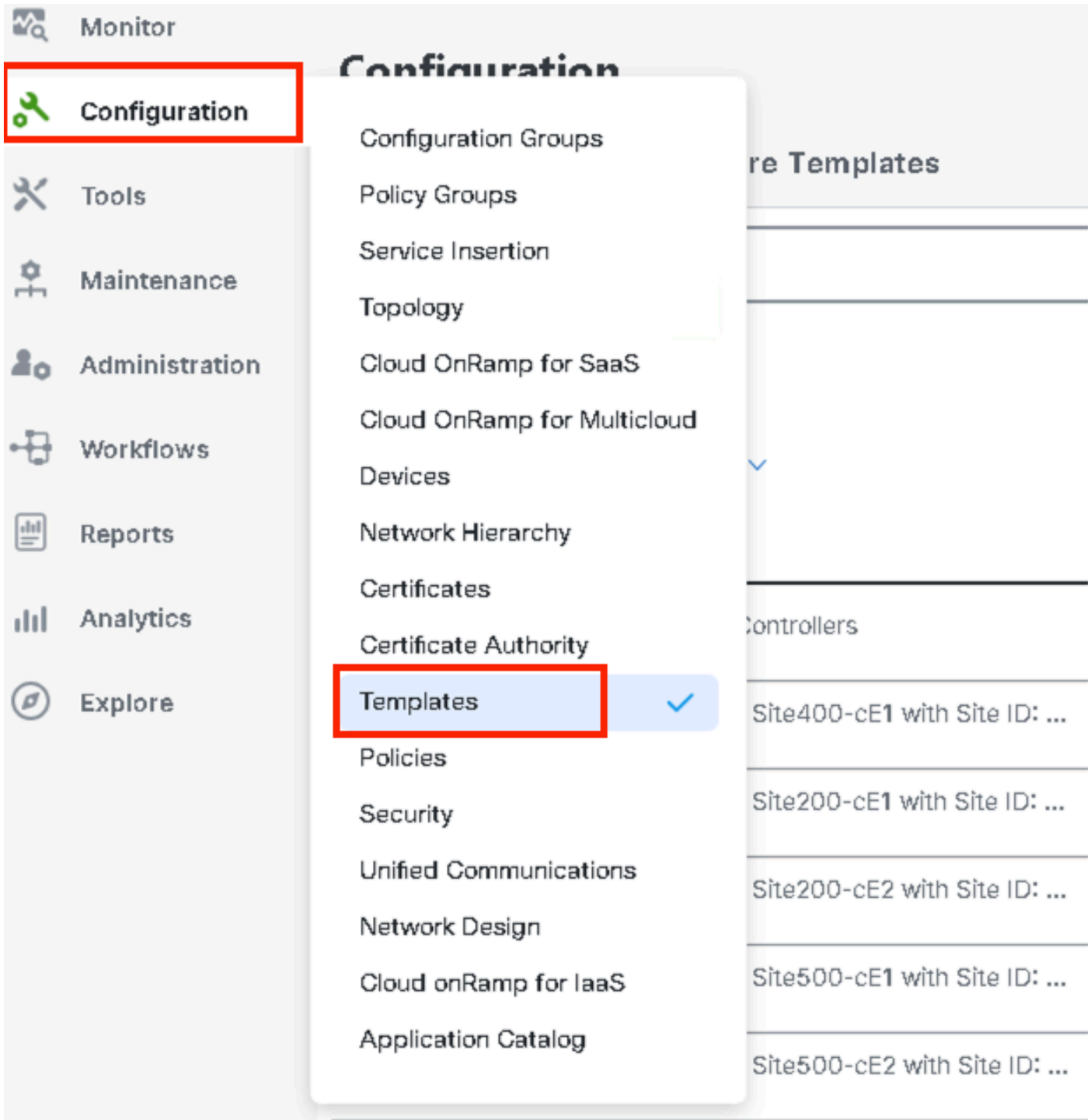
External Syslog Server VPN Server IP

Failure Mode

Apply a Security Policy to a Device

To apply a security policy to a device:

From the Cisco SD-WAN Manager menu, choose **Configuration > Templates**.



Click **Device Templates** and Click on **Edit** on Device Template.

Configuration

Device Templates Feature Templates

Q 300 x Search

Create Template v

Template Type Non-Default v

Total Rows: 1 of 9

Name	Description	Type	Device Model ...	Device Role	Feature Templates	Draft Mode	Devices Attached	Updated By	Last Updated	common.templateStatus
fc862ea4-e57e-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

Click **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

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

- From the **Security Policy** drop-down list, choose the name of the policy you configure under **Guest_URL_Policy** previously and Click **Update**.

Policy VIP07_DPI_Visibility v

Probes Choose... v

Tenant Choose... v

Security Policy **Guest_URL_Policy** v

Container Profile * **Factory_Default_UTD_Template** v ⓘ

Switch Port + Switch Port v

Update Cancel

Click on devices, and make sure the config is correct and Click **Config Diff** and **Side by Side Diff**.
Click **Configure Devices**.

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

Buttons: Config Preview, **Config Diff**, Side by Side Diff, Intent

Device list (Total: 1 devices)

Filter/Search

CBK-C19B1FE2-C89F-A311-DEA7-482A878B089A
Site900-cEj11301

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
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

```

Buttons: Back, **Configure Devices**, Cancel

vManage successfully configured the device template with the security policy and installed the UTD package on the Edge device.

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-C09F-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 apgid utd

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

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

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

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

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

Modify URL Flitering

To modify a URL Filtering policy, do these steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration > Security**.
2. In the Security screen, click the **Custom Options** drop-down menu , choose **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 8:32:39 PM

Click on **URL Filtering** on the left tab, for the desired policy you want to modify, click on **3 dots (...)** and choose **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

Modify the policy as required and click **Save URL Filtering Policy**.

URL Filtering - Policy Rule Configuration ⓘ

Policy Mode: Security ⓘ

Policy Name: Guest_Access

Web Categories: Block

abused-drugs x games x gambling x social-network x hact

Save URL Filtering Policy Cancel

Delete URL Filtering

To delete a URL filtering policy, you must first detach the policy from the security policy:

From the Cisco SD-WAN Manager menu, choose **Configuration > Security**.

To detach the URL filtering policy from the security policy:

- For the security policy that contains the URL filtering policy, click **3 dots (...)** then click **Edit**.

Add Security Policy Add Unified Security Policy

Total Rows: 3

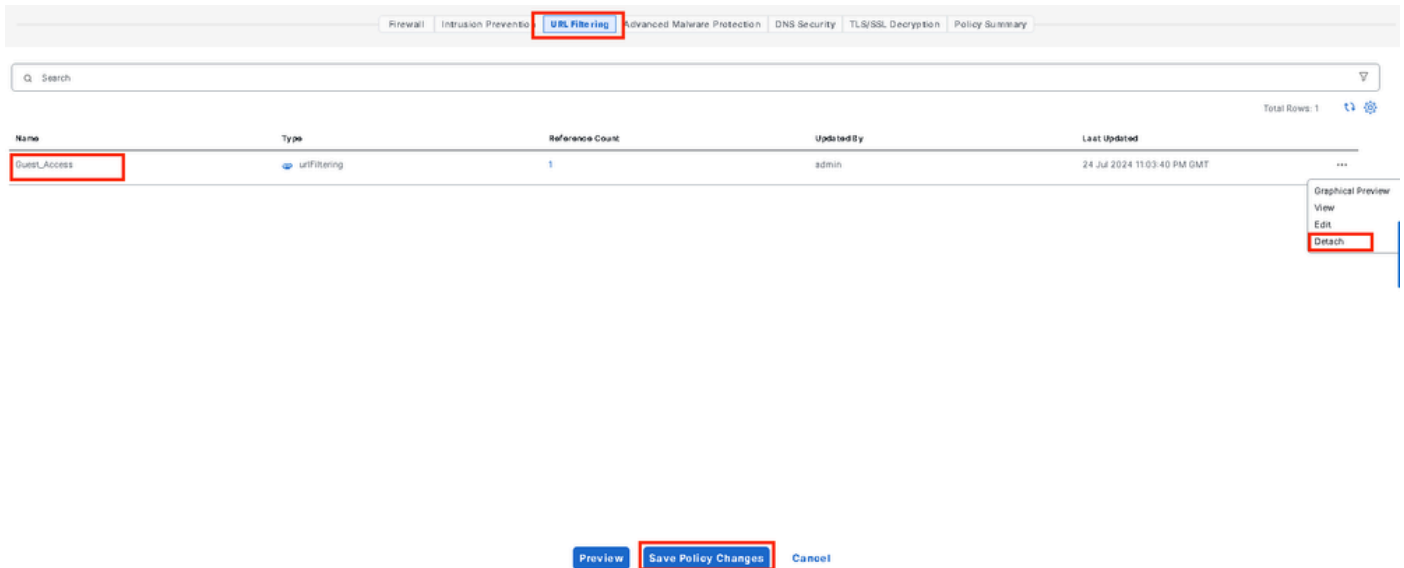
Name	Description	Use Case	Policy Mode	Devices Attached	DeviceTemplates/ConfigGroups	Updated By	Last Updated
VIP22-Security-Policy	ZBFW policy for DIA	Custom	security	0	0	admin	12 Apr 2024 9:32:39 PM ...
Security-IPS-URLF-AMP	IPS, URL-F, AMP	Custom	security	0	0	admin	24 Jul 2024 8:49:01 PM ...
Guest_URL_Policy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

View
Preview
Edit
Delete

The Policy Summary page is displayed. Click URL Filtering tab.

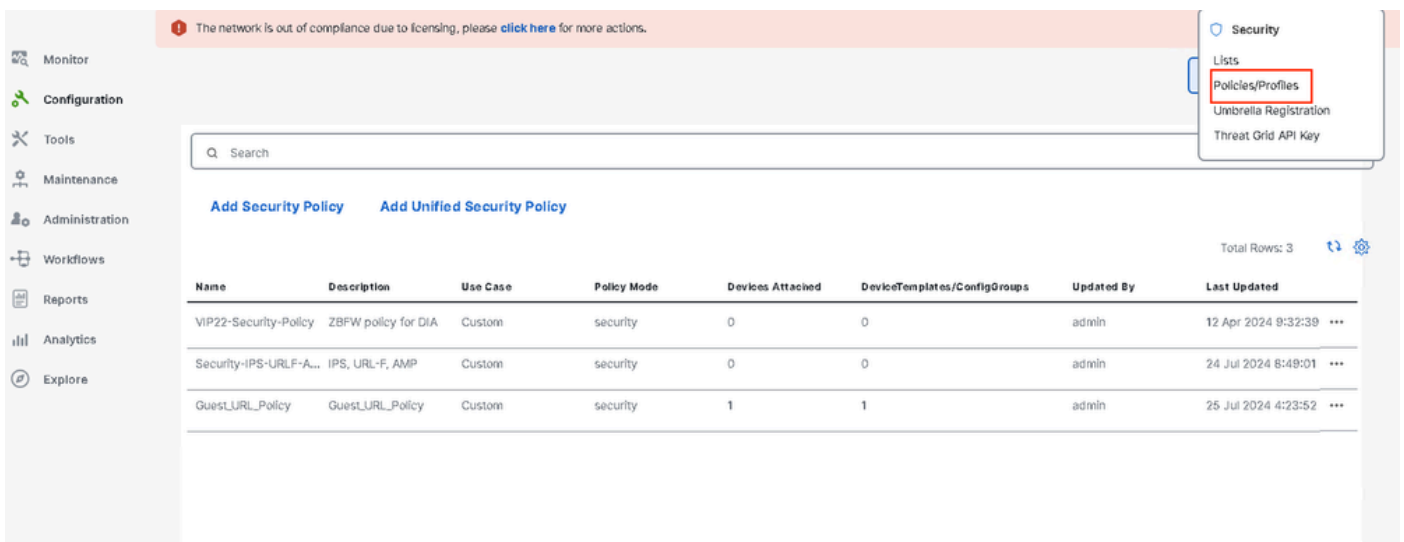
For the policy that you want to delete, click **3 dots (...)** then choose **Detach**.

Click **Save Policy Changes**.



To delete the URL filtering policy:

In the Security screen, click the **Custom Options** drop-down menu , choose **Policies/Profiles**, and then choose **URL Filtering**.



For the policy that you want to delete, click **3 dots (...)** then click **Delete**.

Click on **OK**.

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

Q Search

Add URL Filtering Policy (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	Graphical Preview View Edit Delete

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

Q Search

Add URL Filtering Policy

Are you sure you want to delete the policy?

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

Cancel **OK**

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

Verify

Verify whether the Cisco UTD version is installed.

```
<#root>
```

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

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

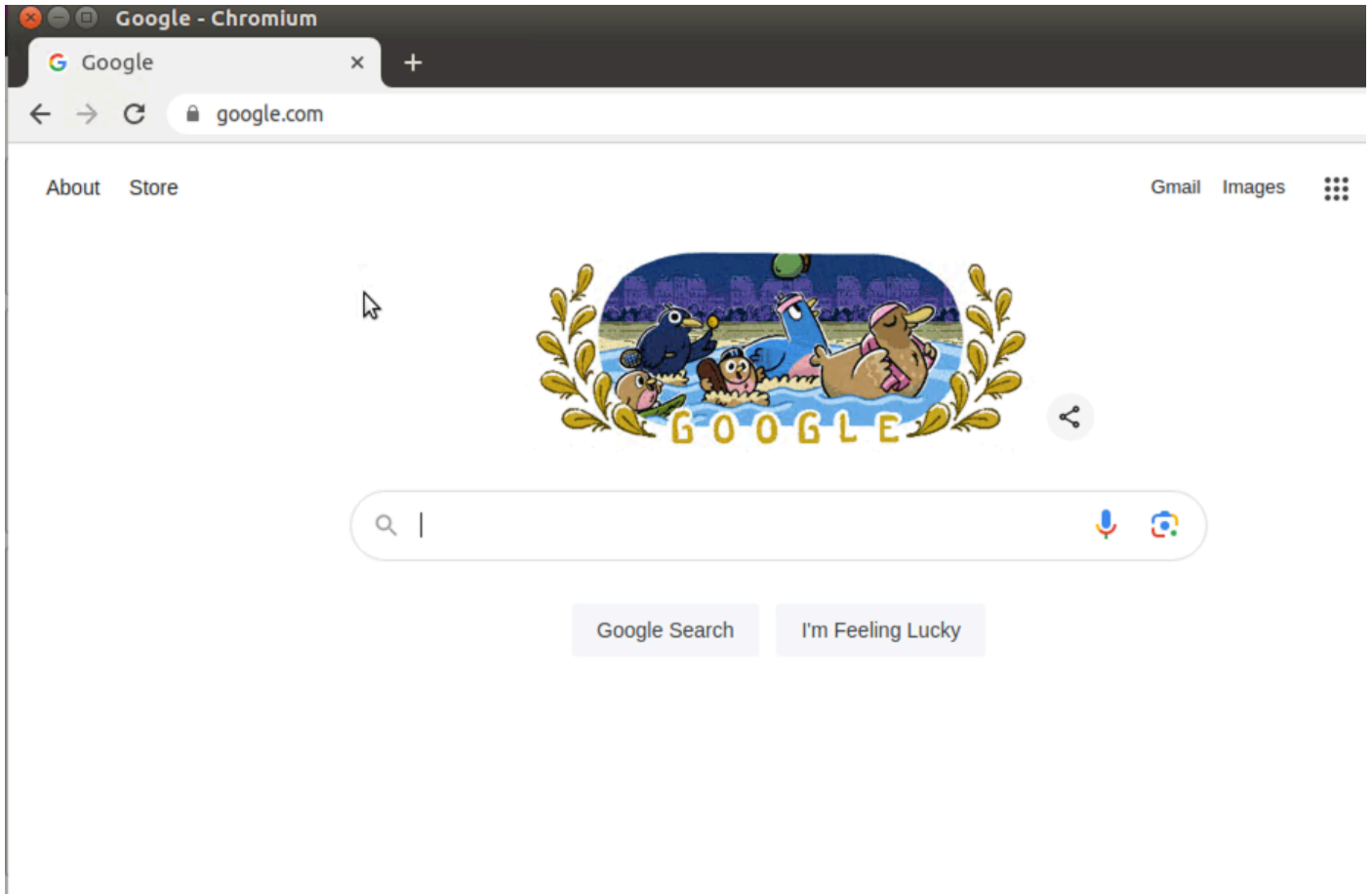
```
IOS-XE Recommended UTD Version: 1.0.2_SV3.1.67.0_XE17.14
```

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

```
UTD Installed Version:
```

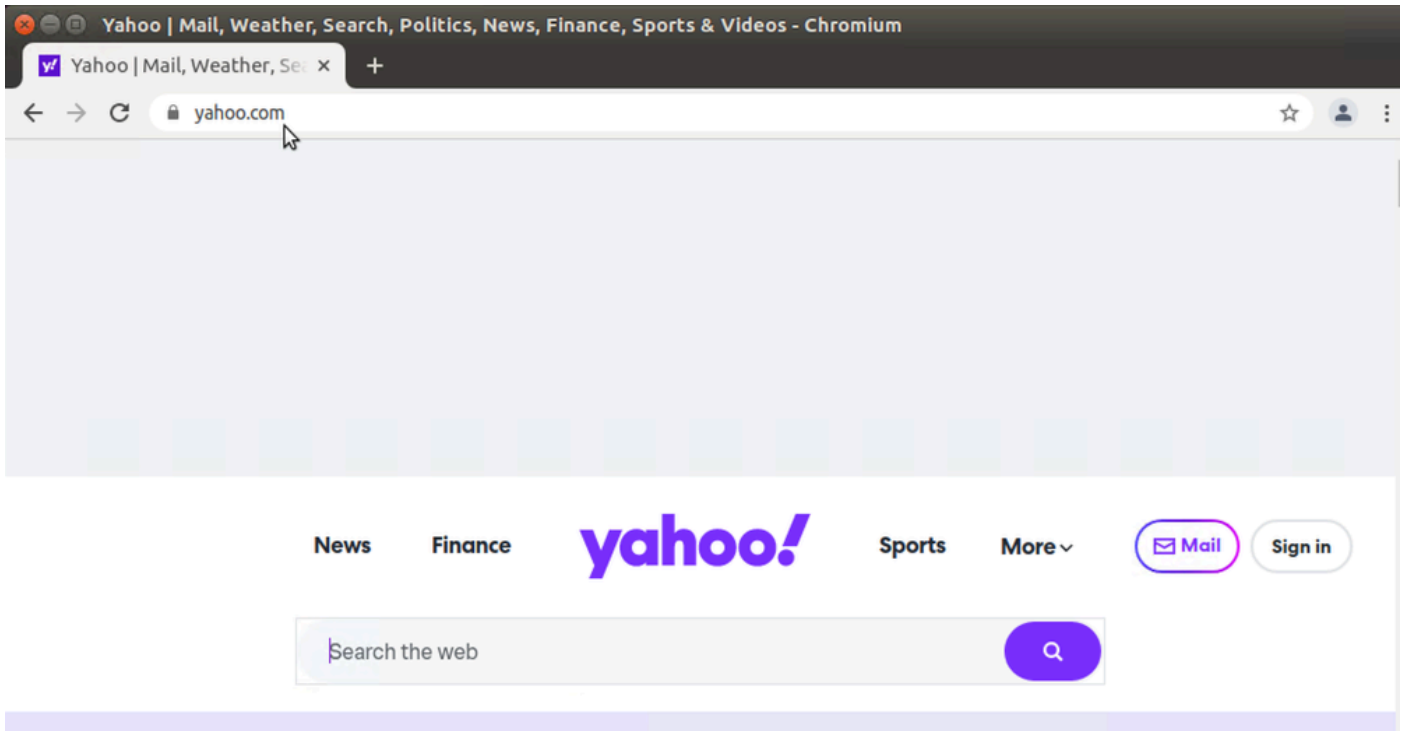
```
1.0.2_SV3.1.67.0_XE17.14
```

From the client PC located on the Guest VPN, if you try to open google.com and yahoo.com, they are allowed.



<#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

[**]

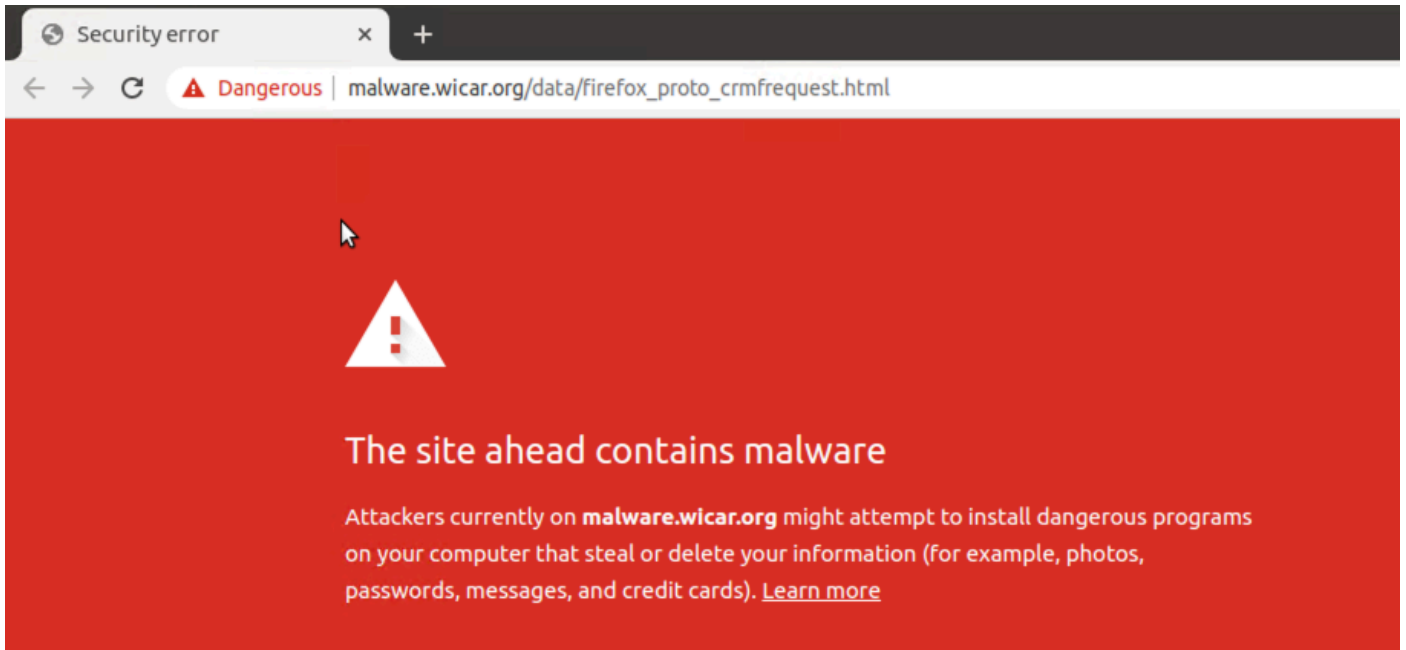
UTD WebFilter Allowlist

[**] [

URL: www.yahoo.com

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

From the client PC located on the Guest VPN, if you try to open web pages with low reputation scores or from one of the blocked web categories, the URL Filtering Engine denies the HTTPs request.



<#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

[**]

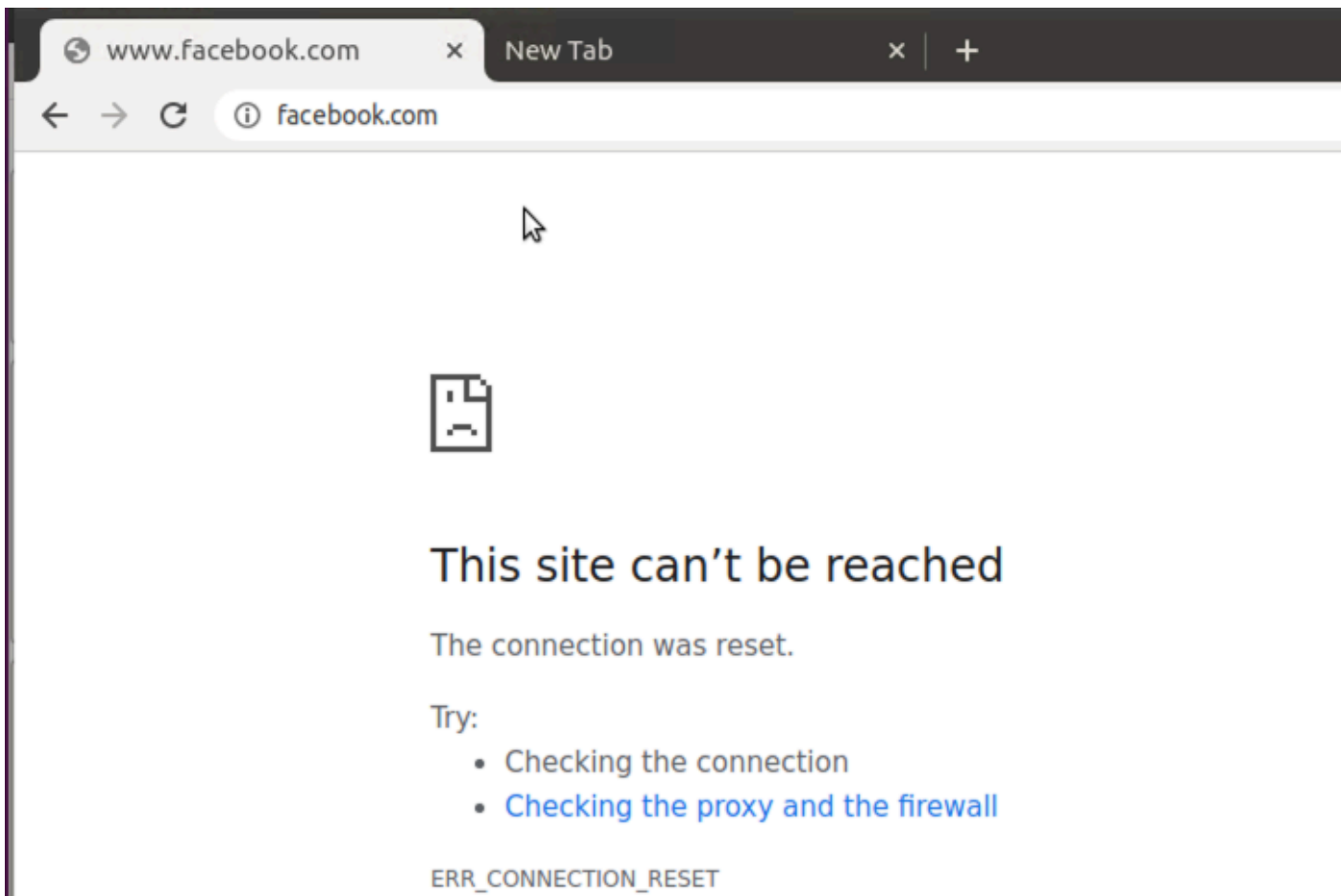
UTD WebFilter Category/Reputation

[**] [

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

From the client PC located on the Guest VPN, if you try to open facebook, instagram and youtube are blocked.



<#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

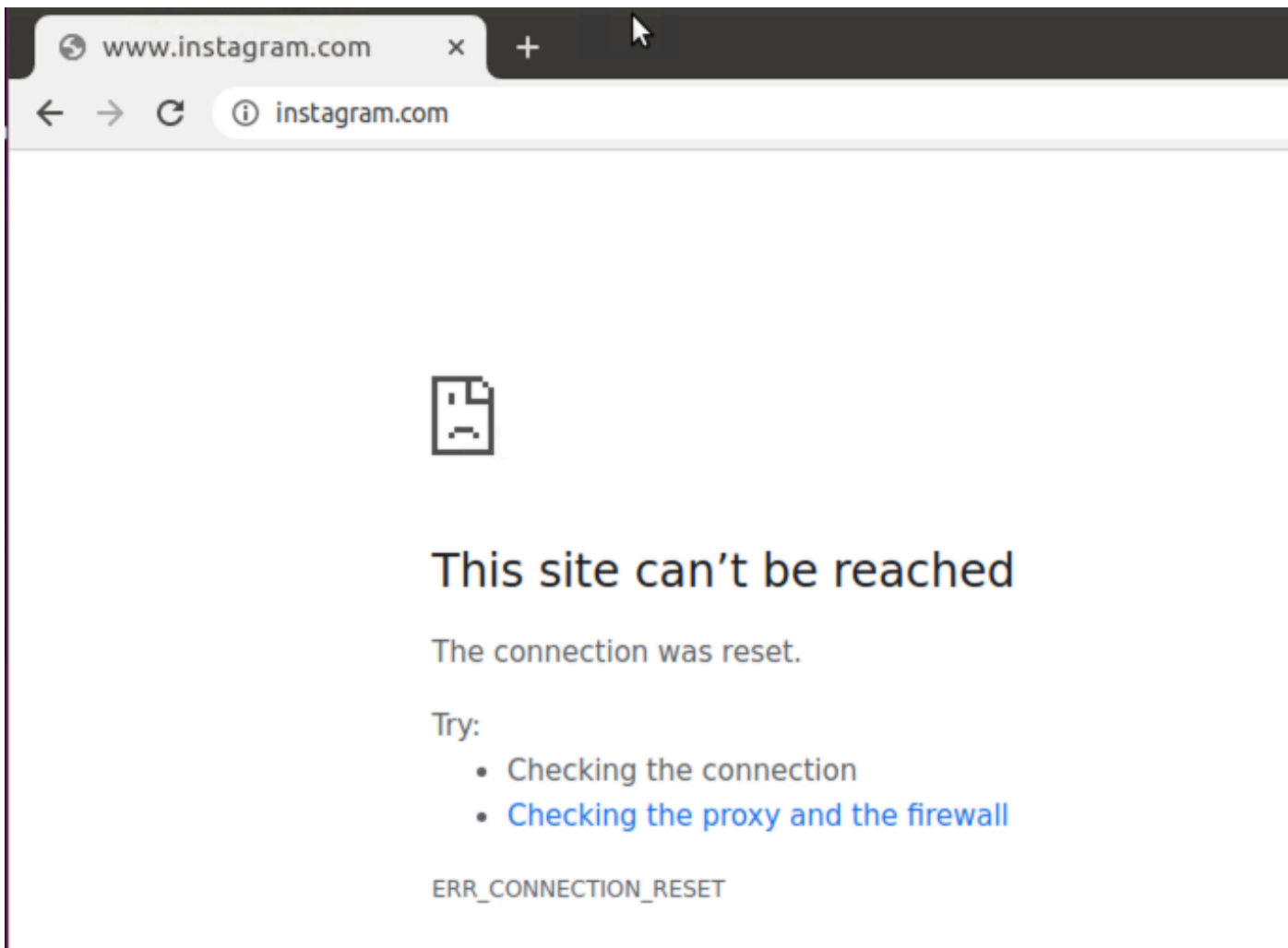
[**]

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

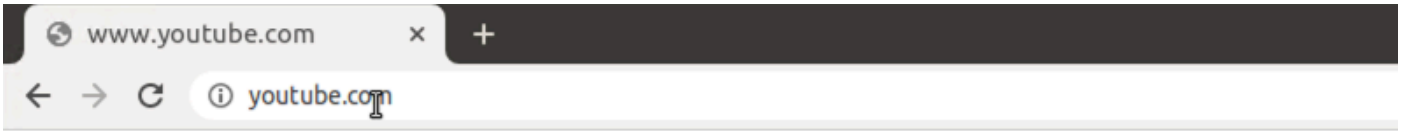
[**]

UTD WebFilter blocklist

[**] [

URL: www.instagram.com

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



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

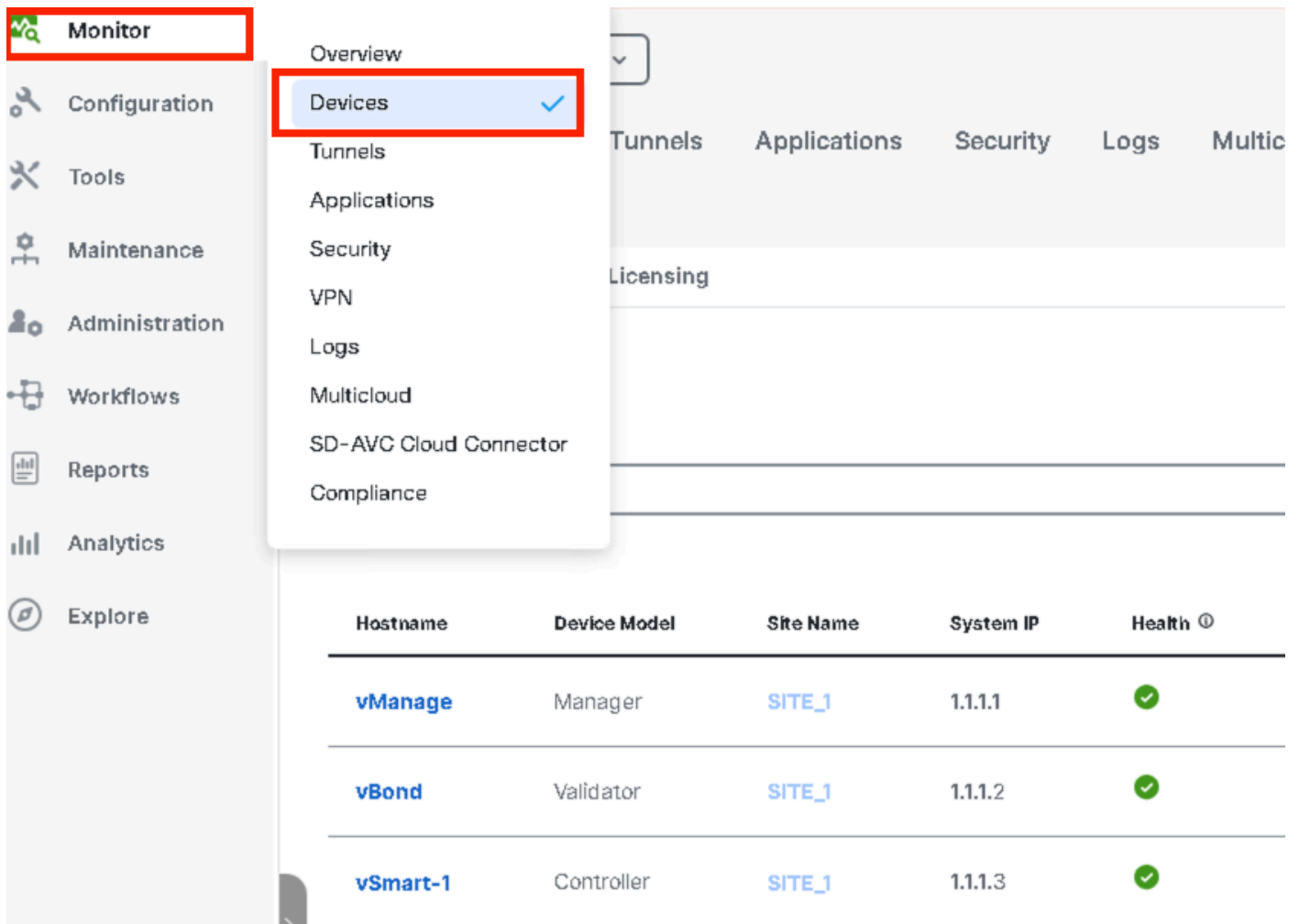
] [VRF: 12] {TCP} 10.32.1.10:54352 -> 142.250.72.206:443

Monitor URL Filtering From vManage GUI

You can monitor URL Filtering in real-time or historically for each device by web categories using these steps.

To monitor the URLs that are **blocked** or **allowed** on an Cisco IOS XE Catalyst SD-WAN device:

1. From the Cisco SD-WAN Manager menu, choose **Monitor > Devices > Select Device**



2. In the left pane, under **Security Monitoring**, click **URL Filtering**. The URL Filtering information displays in the right pane.

- Click **Blocked**. The session count on a blocked URL appears.
- Click **Allowed**. The session count on allowed URLs appears.

Note: UTD Installed version cannot be on UNSUPPORTED state.

Check if UTD is on **running** state.

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

Validate UTD health status is in **GREEN**.

<#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

Verify the URL Filtering feature is enabled.

<#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

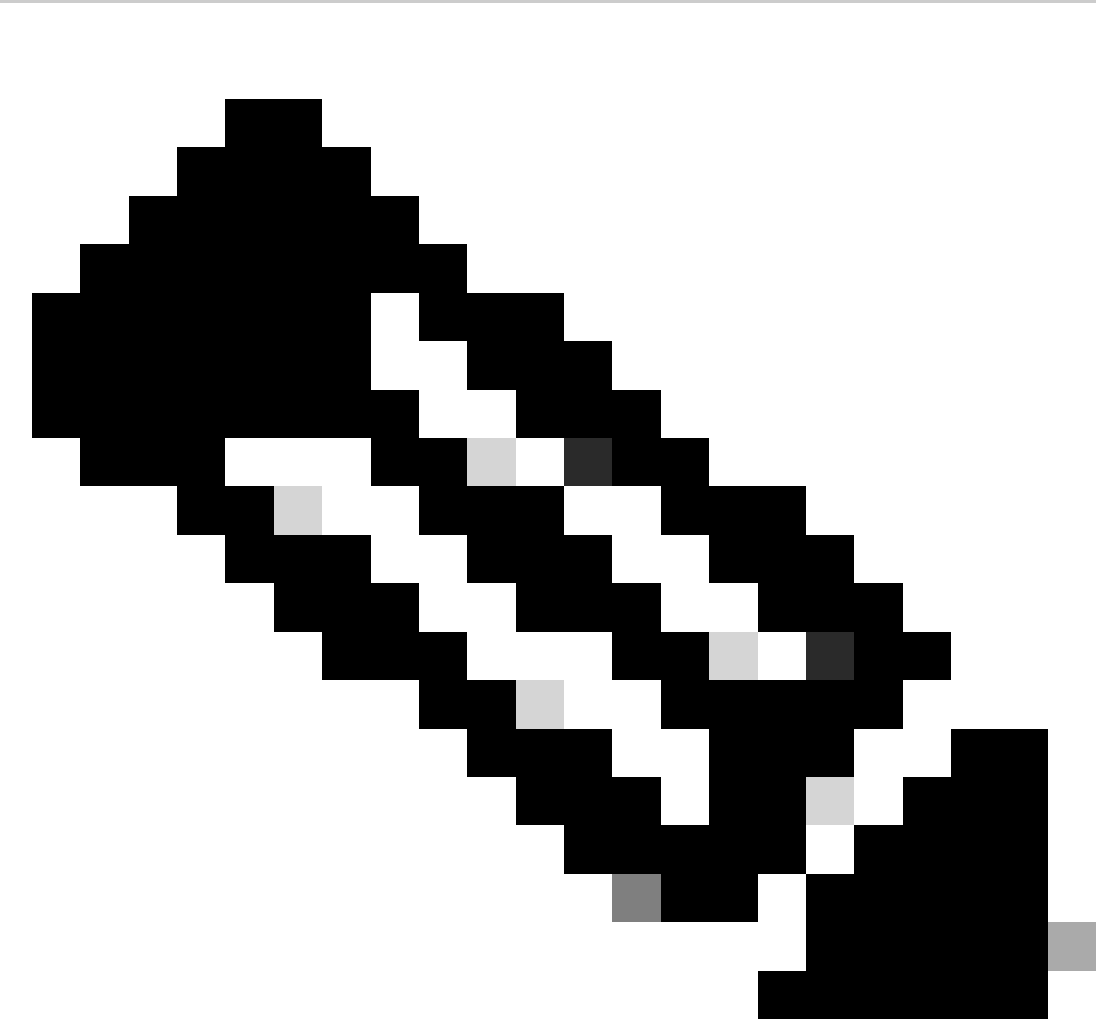
Ctx Flags: (0xc50001)
Engine: Standard
State : Enabled
SN Redirect Mode : Fail-open, Divert
Threat-inspection: Not Enabled
Domain Filtering : Not Enabled

URL Filtering : Enabled

File Inspection : Not Enabled
All Interfaces : Enabled

To display the URL Filtering logs run **show utd engine standard logging events url-filtering** command.

```
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
```



Note: Run the command **clear utd engine standard logging events** to clear old events.

Check ingress/egress packets into UTD container, delay on lookup.

```
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
```

Related Information

- [Cisco Catalyst SD-WAN Security Configuration Guide](#)
- [Install UTD Security Virtual Image on cEdge Routers](#)
- [Troubleshoot Datapath Handling by UTD and URL-Filtering](#)