URL Filtering

The URL Filtering feature enables the user to provide controlled access to Internet websites or Intranet sites by configuring the URL-based policies and filters on the device. The user can configure the URL Filtering profiles to manage the web access. The URL Filtering feature is implemented using the security virtual image similar to the IPS feature.

URL Filtering can either allow or deny access to a specific URL based on:

- Allowed list and blocked list: These are static rules, which helps the user to either allow or deny URLs. If the same pattern is configured under both the allowed and blocked lists, the traffic is allowed.
- Category: URLs can be classified into multiple categories such as News, Social Media, Education, Adult and so on. Based on the requirements, user has the option to block or allow one or more categories.
- Reputation: Each URL has a reputation score associated with it. The reputation score range is from 0-100, and it is categorized as: high-risk (reputation score (0-20), suspicious (21-40), moderate-risk (41-60), low-risk (61-80), and trustworthy (81-100). Based on the reputation score of a URL and the configuration, a URL is either blocked or allowed.

This section contains the following topics:

Overview of URL Filtering

The URL Filtering feature enables the user to provide controlled access to Internet websites by configuring the URL-based policies and filters on the device.

The URL Filtering feature allows a user to control access to Internet websites by permitting or denying access to specific websites based on the category, reputation, or URL. For example, when a client sends a HTTP/HTTP(s) request through the router, the HTTP/HTTP(s) traffic is inspected based on the URL Filtering policies (allowed list/ blocked list, Category, and Reputation). If the HTTP/HTTP(s) request matches the blocked list, the HTTP(s) request is blocked by an inline block page response. If the HTTP/HTTP(s) request matches the allowed list, the traffic is allowed without further URL Filtering inspection.

For HTTPS traffic, the inline block page is not be displayed. URL Filtering will not decode any encoded URL before performing a lookup.

When there is no alloweed list or blocked list configured on the device, based on the category and reputation of the URL, traffic is allowed or blocked using a block page. For HTTP(s), a block page is not displayed and the traffic is dropped.

Filtering Options

The URL Filtering allows you to filter traffic using the following options:

Category-Based Filtering

Note By default, vManage does not download the URL database from the cloud. To enable the URL database download, you must set the **Resource Profile** to **High** in the Feature Template.

If configured, vManage downloads the URL database from the cloud. After the full database is downloaded from the cloud, if there are any updates to the existing database, the incremental updates will be automatically downloaded every 15 minutes. The complete database size is approximately 440 MB and the downloaded database should always synchronize with the cloud. The database will be invalid if the connection to the cloud is lost for more than 24 hours. The default URL category/reputation database only has a few IP address based records. The category/reputation look up occurs only when the host portion of the URL has the domain name.

If the device does not get the database updates from the cloud, vManage ensures that the traffic designated for URL Filtering is not dropped.

Note The URL Filtering database is periodically updated from the cloud in every 15 minutes.

Reputation-Based Filtering

In addition to category-based filtering, you can also filter based on the reputation of the URL. Each URL has a reputation score associated with it. The reputation score range is from 0-100 and it is categorized as:

- High risk: Reputation score of 0 to 20
- Suspicious: Reputation score of 21 to 40
- Moderate risk: Reputation score of 41 to 60
- Low risk: Reputation score of 61 to 80
- Trustworthy: Reputation score of 81 to 100

When you configure a web reputation in vManage, you are setting a reputation threshold. Any URL that is below the threshold is blocked by URL filtering. For example, if you set the web reputation to **Moderate Risk** in vManage, any URL that has a reputation score below than and equal to 60 is blocked.

Based on the reputation score of a URL and the configuration, a URL is either blocked or allowed.

List-based Filtering

List-based filtering allows the user to control access by permitting or denying access based on allowed or blocked lists. Here are some important points to note regarding these lists:

- URLs that are allowed are not subjected to any category-based filtering (even if they are configured).
- If the same item is configured under both the allowed and blocked list, the traffic is allowed.
- If the traffic does not match either the allowed or blocked lists, then it is subjected to category-based and reputation-based filtering (if configured).
- A user may consider using a combination of allowed and blocked pattern lists to design the filters. For example, if you want to allow *www\.foo\.com* but also want to block other URLs such as *www\.foo\.abc* and *www\.foo\.xyz*, you can configure *www\.foo\.com* in the allowed list and *www\.foo\.* in the blocked list.

Configure and Apply URL Filtering

To configure and apply URL Filtering to a Cisco IOS XE SD-WAN device, do the following:

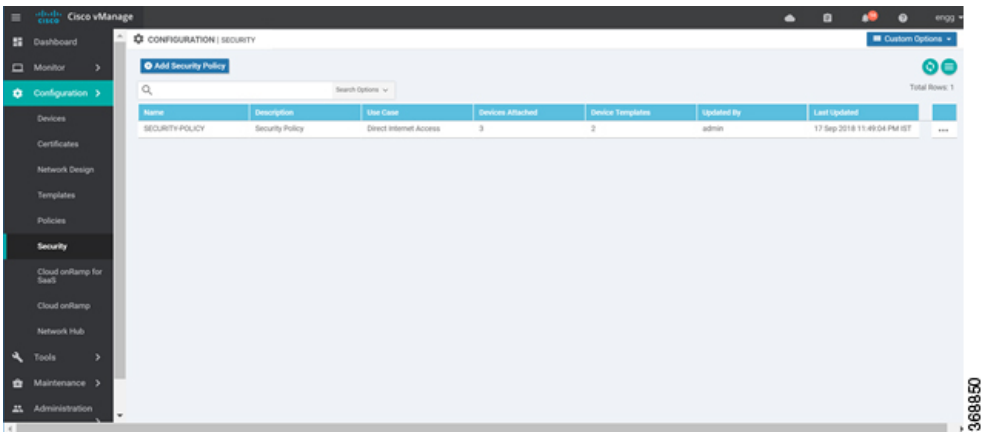
Before you Begin

Before you apply an IPS/IDS, URL Filtering, or Advanced Malware Protection policy for the first time, you must Upload the Cisco Security Virtual Image to vManage.

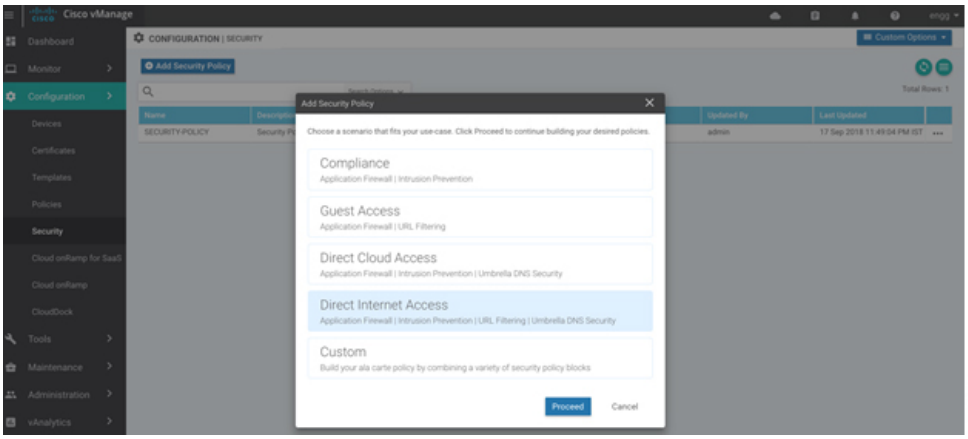
Configure URL Filtering

To configure URL Filtering through a security policy, use the vManage security configuration wizard:

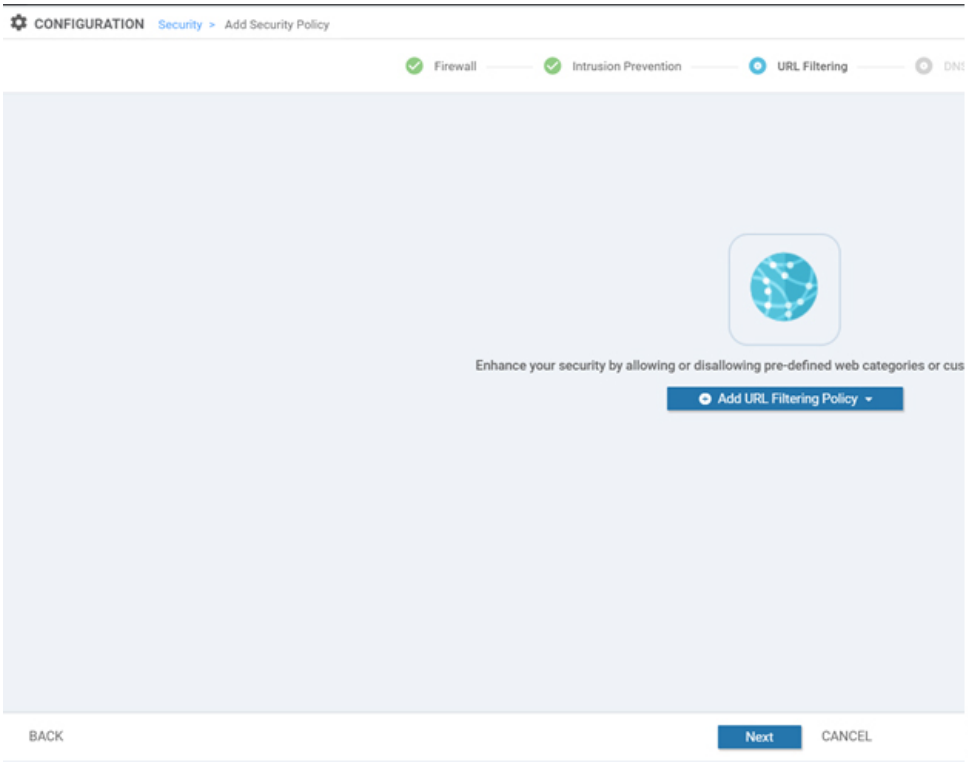
1. In Cisco vManage, select the **Configuration** > **Security** tab in the left side panel.



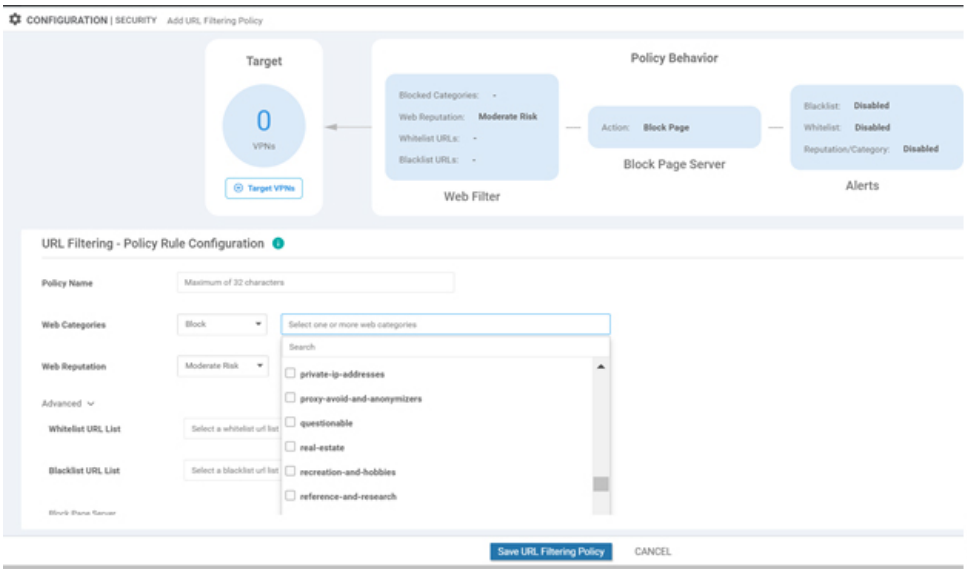
2. Click **Add Security Policy**. The Add Security Policy wizard opens, and various use-case scenarios are displayed.



3. In Add Security Policy, select a scenario that supports URL filtering (**Guest Access**, **Direct Internet Access**, or **Custom**).
4. Click **Proceed** to add a URL filtering policy in the wizard.
5. In the **Add Security Policy** wizard, click **Next** until the **URL Filtering** screen is displayed.



6. Click the **Add URL Filtering Policy** drop-down and choose **Create New** to create a new URL filtering policy. The URL filtering - Policy Rule Configuration wizard appears.



7. Click on **Target VPNs** to add the required number of VPNs in the Add Target VPNs wizard.
8. Enter a policy name in the **Policy Name** field.
9. Choose one of the following options from the Web Categories drop-down:
   - **Block**—Block websites that match the categories that you select.
   - **Allow**—Allow websites that match the categories that you select.
10. Select one or more categories to block or allow from the Web Categories list.
11. Select the Web Reputation from the drop-down. The options are:
    - **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.
12. (Optional) From the **Advanced** tab, choose one or more existing lists or create new ones as needed from the **Whitelist URL List** or **Blacklist URL List** drop-down.

Note Items on the allowed lists are not subject to category-based filtering. However, items on the blocked lists are subject to category-based filtering. If the same item is configured under both the allowed and blocked lists, the traffic is allowed.

To create a new list, do the following:

a. Click **New Whitelist URL List** or **New Blacklist URL List** at the bottom of the drop-down.

b. In the URL List Name field, enter a list name consisting of up to 32 characters (letters, numbers, hyphens and underscores only)

c. 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.

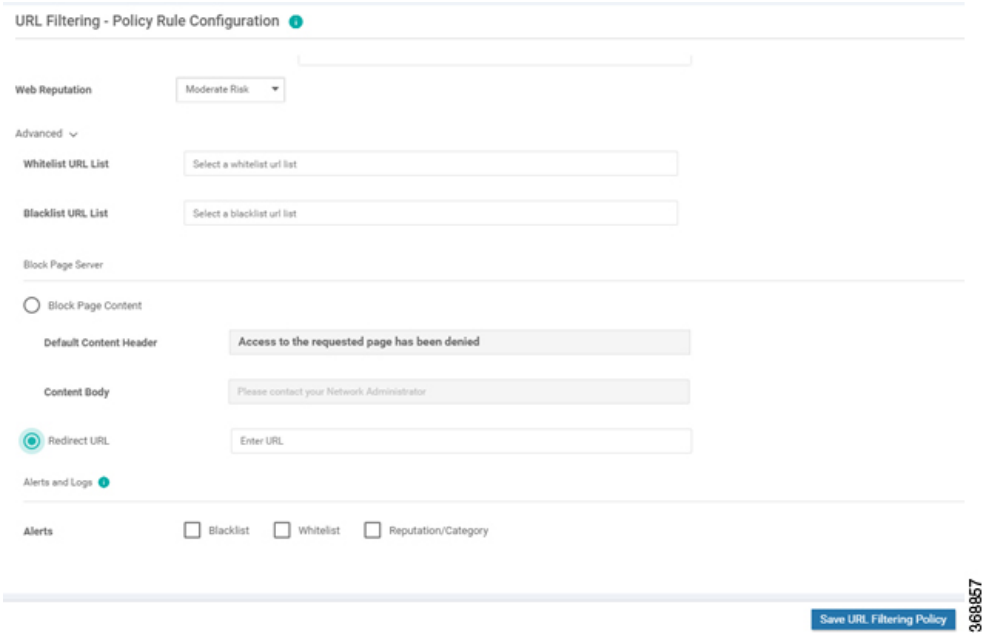
d. Click **Save** when you are finished.

You also can create or manage URL lists by selecting the **Configuration** > **Security** tab in the left side panel, choosing **Lists** from the **Custom Options** drop-down at the top right of the page, and then selecting **Whitelist URLs** or **Blacklist URLs** in the left panel.

To remove a URL list from the URL List field, click the **X** next to the list name in the field.

13. (Optional) In the Block Page Server pane, choose an option to designate what happens when a user visits a URL that is blocked. Choose Block Page Content to display a message that access to the page has been denied, or choose Redirect URL to display another page.

If you choose Block Page Content, users see the content header "Access to the requested page has been denied." in the Content Body field, enter text to display under this content header. The default content body text is "Please contact your Network Administrator." If you choose Redirect URL, enter a URL to which users are redirected.



14. (Optional) In the Alerts and Logs pane, select the alert types from the following options:

- **Blacklist**—Exports an alert as a Syslog message if a user tries to access a URL that is configured in the blocked URL List.
- **Whitelist**—Exports an alert as a Syslog message if a user tries to access a URL that is configured in the allowed URL List.
- **Reputation/Category**—Exports an alert as a Syslog message if a user tries to access a URL that has a reputation that is configured as blocked in the Web Reputation field or that matches a blocked web category.

Alerts for allowed reputations or allowed categories are not exported as Syslog messages.

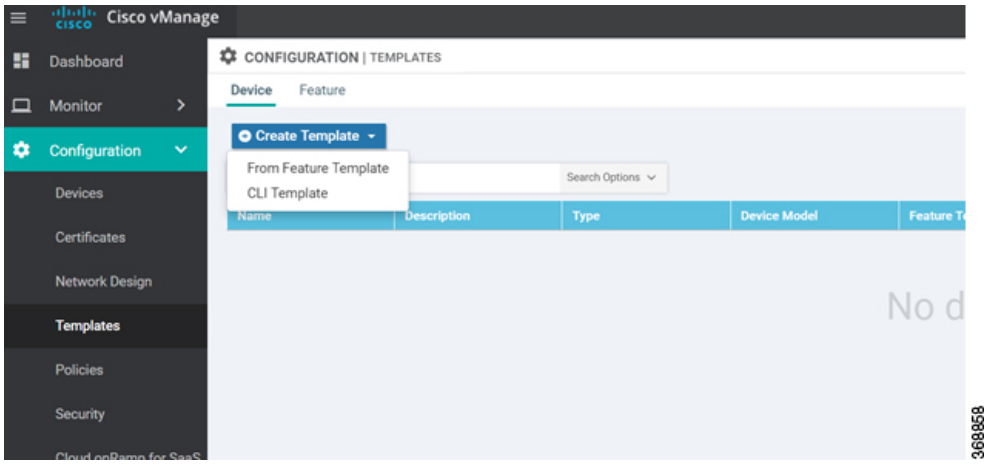
15. You must configure the address of the external log server in the Policy Summary page.
16. Click **Save URL filtering Policy**to add an URL filtering policy.

17. Click **Next** until the Policy Summary page is displayed.
18. Enter Security Policy Name and Security Policy Description in the respective fields.
19. If you enabled Alerts and Logs, in the Additional Policy Settings section you must specify the following:
    - External Syslog Server VPN: The syslog server should be reachable from this VPN.
    - Server IP: IP address of the server.
    - Failure Mode: **Open** or **Close**
20. Click **Save Policy** to save the Security policy.
21. You can edit the existing URL filtering policy by clicking on **Custom Options** in the right-side panel of the **vManage** > **Configuration** > **Security** wizard.

Apply a Security Policy to a Device

To apply a security policy to a device:

1. In vManage, select the **Configuration** > **Templates** screen.



2. In the Device tab, from the **Create Template** drop-down, select **From Feature Template**.
3. From the **Device Model** drop-down, select one of the IOS XE SD-WAN devices.

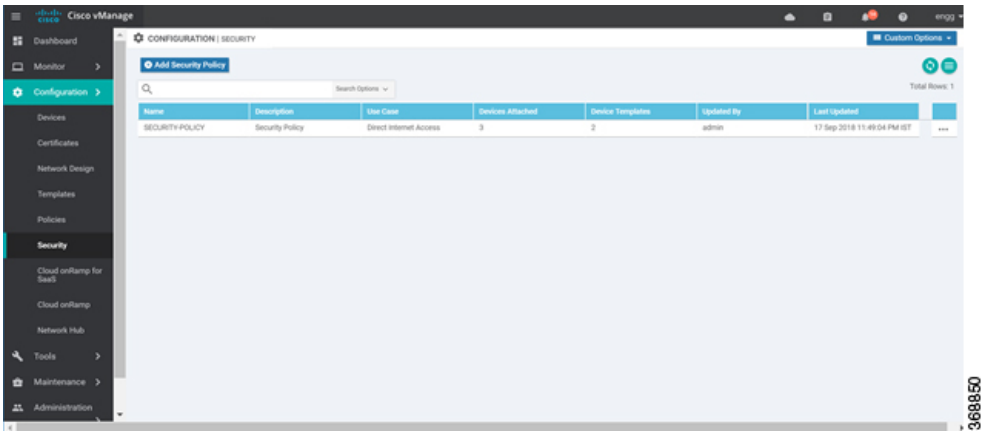
4. Click the **Additional Templates** tab located directly beneath the **Description** field. The screen scrolls to the **Additional Templates** section.

5. From the **Security Policy** drop-down, select the name of the policy you configured in the previous procedure.
6. Click **Create** to apply the security policy to a device.

Modify URL Flitering

To modify a URL Filtering policy, do the following:

1. In Cisco vManage, select the **Configuration** > **Security** tab in the left side panel.

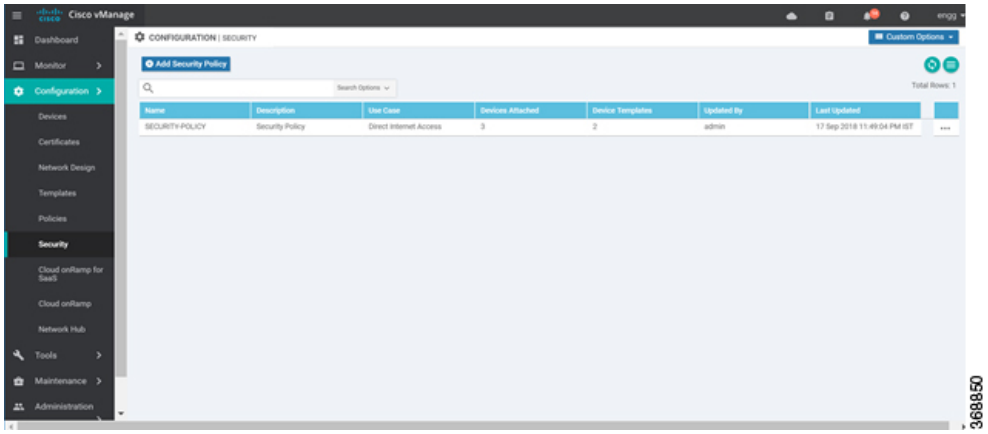


2. In the Security screen, click the **Custom Options** drop-down and select **URL Filtering**.
3. For the policy that you want to modify, click the **More Actions** icon to the far right of the policy and select **Edit**.
4. Modify the policy as required and click **Save URL Filtering Policy**.

Delete URL Filtering

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

1. In Cisco vManage, select the **Configuration** > **Security** tab in the left side panel.



2. Detach the URL filtering policy from the security policy as follows:
   a. For the security policy that contains the URL filtering policy, click the **More Actions** icon to the far right of the policy and select **Edit**.

      The Policy Summary page is displayed.

   b. Click the **URL Filtering** tab.

   c. For the policy that you want to delete, click the **More Actions** icon to the far right of the policy and select **Detach**.

   d. Click **Save Policy Changes**.

3. Delete the URL filtering policy as follows:
   a. In the Security screen, click the **Custom Options** drop-down and select **URL Filtering**.

   b. For the policy that you want to delete, click the **More Actions** icon to the far right of the policy and select **Delete**.

      A dialog box is displayed.

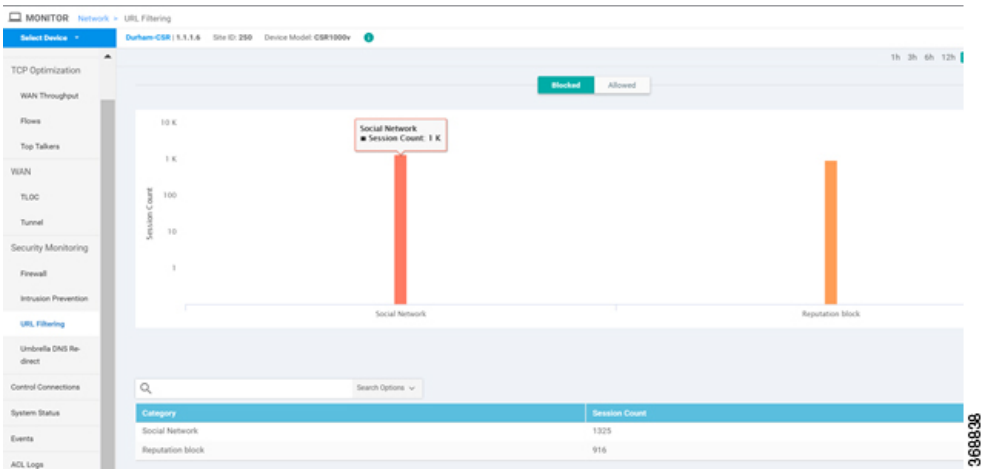
   c. Click **OK**.

Monitor URL Filtering

You can monitor the URL Filtering for a device by web categories using the following steps.

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

1. From the **Monitor** > **Network** screen, select a device.
2. In the left panel, under Security Monitoring, select the **URL Filtering** tab. The URL Filtering wizard displays.
3. Click on the **Blocked** tab, the session count on a blocked URL appears as shown in the following screenshot.



4. Click on the **Allowed** tab, the session count on allowed URLs appear as shown in the following screenshot.