URL Filtering

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

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.

Note A NAT direct internet access route is necessary to implement URL Filtering.

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.

When there is no allowed 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.

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 displayed. URL Filtering will not decode any encoded URL before performing a lookup. Because the SSL/TLS session is still being established at the time it is determined the request should be blocked, the client is not expected to receive a HTTP response, whether it is the injected HTTP blocked page or redirect URL, which causes a protocol error to occur.

In Cisco Catalyst SD-WAN, a HTTP response can be inserted into the HTTPS session if this traffic is routed through SSL/TLS proxy. The SSL/TLS session is allowed to establish in this case, and when the HTTP GET is received on the decrypted HTTPS session, the HTTP blocked page or redirect URL is injected and it is accepted by the client.

Database Overview

By default, WAN Edge routers do not download the URL database from the cloud.

To enable the URL database download:

- prior to Cisco vManage Release 20.5, you must set the **Resource Profile** to **High** in the App-hosting Security Feature Template.
- from Cisco vManage Release 20.5 onwards, you must enable **Download URL Database on Device** in the App-hosting Security Feature Template.

Additional memory is required to download the URL database.

If configured, WAN Edge routers download 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, Cisco SD-WAN Manager 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.

Filtering Options

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

Category-Based Filtering

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.

A URL may be associated with up to five different categories. If any of these categories match a configured blocked category, then the request will be blocked.

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 Cisco SD-WAN Manager, 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 Cisco SD-WAN Manager, 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).
- You can 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.

Note If you are using the *www* prefix in the allowed or blocked regex pattern, it can create a problem if the Server Name Indicator (SNI) returned in the client message doesn't match. For example, if you want to allow *www./foo./com* and SNI returns as *foo.com* only. We recommend not to include the *www* in the regex match.

For more information, see Regular Expression for URL Filtering and DNS Security.

Cloud-Lookup

The Cloud-Lookup feature is enabled by default and is used to retrieve the category and reputation score of URLs that are not available in the local database.

The category and reputation score of unknown URLs are returned as follows:

Name based URLs:

- Valid URL — corresponding category and reputation score is received.
- Unknown URL (new URL or unknown to the cloud) — category is 'uncategorized' and reputation score is 40
- Internal URLs with proper domain name (for example, internal.abc.com) — category and reputation score is based on the base domain name (abc.com from the example above).
- Completely internal URLs (for example, abc.xyz) — category is 'uncategorized' and reputation score is 40

IP based URLs:

- Public hosted IP — corresponding category and reputation score is received.
- Private IP like 10.<>, 192.168.<> — category is 'uncategorized' and reputation score is 100
- Non-hosted/Non-routable IP — category is 'uncategorized' and reputation score is 40

The Cloud-Lookup score is different from the on-box database for these URLs (Unknown/Non-hosted/Non-routable/Internal URLs).

Configure and Apply URL Filtering

To configure and apply URL Filtering to a Cisco IOS XE Catalyst 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 Cisco SD-WAN Manager security configuration wizard:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Click **Add Security Policy**. The Add Security Policy wizard opens, and various use-case scenarios are displayed.
3. In Add Security Policy, choose 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** window is displayed.
6. Click the **Add URL Filtering Policy** drop-down menu and choose **Create New** to create a new URL filtering policy. The URL filtering - Policy Rule Configuration wizard appears.
7. Click **Target VPNs** to add the required number of target service 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 choose.
   - **Allow**: Allow websites that match the categories that you choose.
10. Choose one or more categories to block or allow from the **Web Categories** list.
11. Choose a Web Reputation from the drop-down menu. The options are:
    - **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.
12. (Optional) From **Advanced**, choose one or more existing lists or create new ones as needed from the **Whitelist URL List** or **Blacklist URL List** drop-down menu.

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** in the drop-down menu.
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 **Import** to add lists from an accessible storage location.
d. Click **Save** when you are finished.

You also can create or manage URL lists. To do this:

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

b. Choose **Lists** from the **Custom Options** drop-down menu.

c. Choose **Whitelist URLs** or **Blacklist URLs** in the left pane.

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, choose 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.

      You can use Look up URL or IP tool to validate how a website is classified using URL-Filtering feature. It only shows the output for the configured URL filtering alerts or events.

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. To edit the existing URL filtering policy, click **Custom Options** in the right-side panel of the Security wizard.

Apply a Security Policy to a Device

To apply a security policy to a device:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is called **Device**.

3. From the **Create Template** drop-down list, choose **From Feature Template**.
4. From the **Device Model** drop-down list, choose one of the devices.
5. Click **Additional Templates**.

   The **Additional Templates** section is displayed.
6. From the **Security Policy** drop-down list, choose the name of the policy you configured previously.
7. Click **Create** to apply the security policy to a device.
8. Click **…** next to the device template that you created.
9. Click **Attach Devices**.
10. Choose the devices to which you want to attach the device template.
11. Click **Attach**.

Note If you are migrating from older releases to Cisco IOS XE Release 17.2 or later with Application lists and the zone-based firewall that is configured in Cisco SD-WAN Manager, you must first remove the security template from the base template and push the base template. Thereafter, reattach the security template and then push the template to the device.

Note When a Zone based firewall template in attached to a Cisco IOS XE Catalyst SD-WAN device running on Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or later, there may be an increase in time for completion of tasks. This is due to the updates in the software version of Cisco vManage Release 20.6.1.

Modify URL Flitering

To modify a URL Filtering policy, do the following:

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**, and then choose **URL Filtering**.

3. For the desired policy you want to modify, click **...** and choose **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. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. To detach the URL filtering policy from the security policy:
   a. For the security policy that contains the URL filtering policy, click **...** and click **Edit**.

      The Policy Summary page is displayed.

   b. Click **URL Filtering**.
   c. For the policy that you want to delete, click **...** and choose **Detach**.
   d. Click **Save Policy Changes**.
3. To delete the URL filtering policy:
   a. In the Security screen, click the **Custom Options** drop-down menu , choose **Policies/Profiles**, and then choose **URL Filtering**.
   b. For the policy that you want to delete, click **...** and click **Delete**.
   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 Cisco IOS XE Catalyst SD-WAN device:

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

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. In the left pane, under Security Monitoring, click **URL Filtering**. The URL Filtering information displays in the right pane.
3. Click **Blocked**. The session count on a blocked URL appears.
4. Click **Allowed**. The session count on allowed URLs appears.

Configure URL Filtering for Unified Security Policy

You can create a URL filtering policy specifically for use in a unified security policy. After being created, the URL filtering policy is included in the advanced inspection profile and applied to the unified security policy for implementation on Cisco IOS XE Catalyst SD-WAN devices.

To configure a URL filtering policy for a unified security policy, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Security**.
2. Click **Custom Options**.
3. Click **Policies/Profiles**.
4. Click **URL Filtering** in the left pane.
5. Click **Add URL Filtering Policy**, and choose **Create New**.
6. Click **Policy Mode** to enable the unified mode.

   This implies that you are creating a URL filtering policy for use in the unified security policy.

Note

- Target VPNs are not applicable for the advanced malware protection used in a unified security policy.
- You can enable Policy Mode only when creating advanced malware protection policies. You cannot configure the unified mode once the policy is saved.

7. Enter a policy name in the **Policy Name** field.
8. Choose one of the following options from **Web Categories**.
   - **Block**:Block websites that match the categories that you choose.
   - **Allow**:Allow websites that match the categories that you choose.
9. Choose one or more categories to block or allow from the **Web Categories** drop-down list.
10. Choose the **Web Reputation** from the drop-down list. The options are:
    - **High Risk**: The Reputation score is between 0 to 20.
    - **Suspicious**: The Reputation score is between 21 to 40.
    - **Moderate Risk**: The Reputation score is between 41 to 60.
    - **Low Risk**: The Reputation score is between 61 to 80.
    - **Trustworthy**: The Reputation score is between 81 to 100.
11. (Optional) From **Advanced**, choose one or more existing lists or create new ones, as needed, from the **Whitelist URL List** or **Blacklist URL List** drop-down lists.

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

To create a new list, do the following:

a. Click **New Whitelist URL List** or **New Blacklist URL List** in the drop-down list.

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 **URL** field, enter URLs to include in the list, separated by commas. You also can use **Import** to add lists from an accessible storage location.

d. Click **Save**.

You also can create or manage URL lists by choosing **Configuration** > **Security**, and then choosing **Lists** from **Custom Options** top-right corner of the window, and then clicking **Whitelist URLs** or **Blacklist URLs** in the left pane.

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

12. (Optional) In the **Block Page Server** pane, choose an option to designate what happens when a user visits a URL that is blocked.

If you click **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 click **Redirect URL**, enter a URL to which users are redirected.

13. (Optional) In the **Alerts and Logs** pane, choose alert type option:

- **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 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.

14. Configure the address of the external log server in the **Policy Summary** page.

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