Access Control Using Content Restriction

Major search engines and content delivery services provide features that allow you to restrict search results and website content. For example, schools use content restriction features to comply with the Children's Internet Protection Act (CIPA).

When implemented by search engines and content delivery services, you can enforce content restriction features only for individual browsers or users. The Firepower System allows you to extend these features to your entire network.

The system allows you to enforce:

- *Safe Search*—Supported in many major search engines, this service filters out explicit and adult-oriented content that particular environments (business, government, education, etc.) classify as objectionable. The system does not restrict a user's ability to access the home pages for supported search engines. Note that YouTube Restricted Mode is a subfeature of Safe Search.
- *YouTube EDU*—This service filters YouTube content for an educational environment. It allows schools to set access for educational content while limiting access to noneducational content. YouTube EDU is a different feature than YouTube Restricted Mode, which enforces restrictions on YouTube searches as part of Google's Safe Search feature. With YouTube EDU, users access the YouTube EDU home page, rather than the standard YouTube home page.

Content restriction features communicate the restricted status of a search or content query via an element in the request URI, an associated cookie, or a custom HTTP header element. You can configure access control rules to modify these elements as the system processes traffic.

Note that, to enforce content restriction, you must also enable an SSL policy, which impacts performance.

If you enable logging of connection events for these access control rules, the system logs related events with a **Reason** of `Content Restriction`.

The following topics describe how to enforce content restriction using access control rules:

- Using Access Control Rules to Enforce Content Restriction, page 13-1
- Safe Search Options for Access Control Rules, page 13-3
- YouTube EDU Options for Access Control Rules, page 13-3
- Content Restriction Rule Order, page 13-4

Using Access Control Rules to Enforce Content Restriction

License: Any

Caution To avoid rule preemption, position rules governing YouTube EDU above rules governing Safe Search in both SSL and access control policies. For more information, see Content Restriction Rule Order, page 13-4.

To enforce content restriction using access control rules:

Step 1 Create an SSL policy; see Creating a Basic SSL Policy, page 15-2.

Step 2 Add SSL rules for handling Safe Search and YouTube EDU traffic:

- Choose **Decrypt - Resign** as the **Action** for the rules. The system does not allow any other action for content restriction handling.
- In the **Applications** tab, add selections to the **Selected Applications and Filters** list:
  - Safe Search—Add the `safesearch supported` filter.
  - YouTube EDU—Search for "YouTube" in the **Available Applications** list, and add the resulting applications.

  For more information, see Controlling Encrypted Traffic Based on Application, page 17-8.

Step 3 Set rule positions for the SSL rules you added. Click and drag, or use the right-click menu to cut and paste.

Step 4 Create or edit an access control policy, and associate the SSL policy with the access control policy; see Associating Other Policies with Access Control, page 4-10.

Step 5 In the access control policy, add rules for handling Safe Search and YouTube EDU traffic, placing the Safe Search rule after the YouTube EDU rule:

- Choose **Allow** as the **Action** for the rules. The system does not allow any other action for content restriction handling.
- In the **Applications** tab, click the dimmed icon for either Safe Search (🔒) or YouTube EDU (☑) , and set related options. These icons are disabled, rather than dimmed, if you choose any **Action** other than **Allow** for the rule.

Note You cannot enable Safe Search and YouTube EDU restrictions for the same access control rule.

- In the **Applications** tab, refine application selections in the **Selected Applications and Filters** list.

  In most cases, enabling Safe Search or YouTube EDU populates the **Selected Applications and Filters** list with the appropriate values. The system does not automatically populate the list if a Safe Search or YouTube application is already present in the list when you enable the feature. If applications do not populate as expected, manually add them as follows:
  - Safe Search—Add the `search engines` filter.
  - YouTube EDU—Search for "YouTube" in the **Available Applications** list, and add the resulting applications.

  For more information, see Adding an Application Condition to an Access Control Rule, page 8-5.

Step 6 Set rule positions for the access control rules you added. Click and drag, or use the right-click menu to cut and paste.

Step 7 Configure the **Block Response Page** that the system displays when it blocks restricted content; see Displaying a Custom Web Page for Blocked URLs, page 8-14.

What to Do Next

- Deploy configuration changes; see Deploying Configuration Changes, page 4-12.

Safe Search Options for Access Control Rules

The Firepower System supports Safe Search filtering for specific search engines only. For a list of supported search engines, see applications tagged `safesearch supported` in the **Applications** tab of the access control rule editor. For a list of unsupported search engines, see applications tagged `safesearch unsupported`.

When enabling Safe Search for an access control rule, set the following parameters:

Enable Safe Search

Enables Safe Search filtering for traffic that matches this rule.

Unsupported Search Traffic

Specifies the action you want the system to take when it processes traffic from unsupported search engines. If you choose **Block** or **Block with Reset**, you must also configure the HTTP response page that the system displays when it blocks restricted content; see Displaying a Custom Web Page for Blocked URLs, page 8-14.

YouTube EDU Options for Access Control Rules

When enabling YouTube EDU for an access control rule, set the following parameters:

Enable YouTube EDU

Enables YouTube EDU filtering for traffic that matches this rule.

Custom ID

Specifies the value that uniquely identifies a school or district network in the YouTube EDU initiative. YouTube provides this ID when a school or district registers for a YouTube EDU account.

Note If you check **Enable YouTube EDU**, you must enter a **Custom ID**. This ID is defined externally by YouTube. The system does not validate what you enter against the YouTube system. If you enter an invalid ID, YouTube EDU restrictions may not perform as expected.

Content Restriction Rule Order

To avoid rule preemption in both SSL and access control policies, position rules governing YouTube restriction above rules governing Safe Search restriction.

When you enable Safe Search for an access control rule, the system adds the search engine category to the **Selected Applications and Filters** list. This application category includes YouTube. As a result, YouTube traffic matches to the Safe Search rule unless YouTube EDU is enabled in a rule with a higher evaluation priority.

A similar rule preemption occurs if you position an SSL rule with the `safesearch supported` filter higher in the evaluation order than an SSL rule with specific YouTube application conditions.

For more information, see Ordering Rules to Improve Performance and Avoid Preemption, page 4-15.