Content Restriction

The following topics describe how to configure access control policies to use content restriction features:

- About Content Restriction, on page 1
- Requirements and Prerequisites for Content Restriction, on page 2
- Guidelines and Limitations for Content Restriction, on page 3
- Using Access Control Rules to Enforce Content Restriction, on page 3
- Using a DNS Sinkhole to Enforce Content Restriction, on page 4

About 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 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 business, government, and education environments classify as objectionable. The system does not restrict a user's ability to access the home pages for supported search engines.

You can use two methods to configure the system to enforce these features:

Method: Access Control Rules
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.

Method: DNS Sinkhole
For Google searches, you can configure the system to redirect traffic to the Google SafeSearch Virtual IP Address (VIP), which imposes filters for Safe Search.

The table below describes the differences between these enforcement methods.

Table 1: Comparison of Content Restriction Methods

Attribute	Method: Access Control Rules	Method: DNS Sinkhole
Supported devices	Any	Secure Firewall Threat Defense only
Search engines supported	Any tagged `safesearch supported` in the **Applications** tab of the rule editor	Google only
YouTube Restricted Mode supported	Yes	Yes
SSL policy required	Yes	No
Hosts must be using IPv4	No	Yes
Connection event logging	Yes	Yes

When determining which method to use, consider the following limitations:

- The access control rules method requires an SSL policy, which impacts performance.
- The Google SafeSearch VIP supports IPv4 traffic only. If you configure a DNS sinkhole to manage Google searches, any hosts on the affected network must be using IPv4.

The system logs different values for the **Reason** field in connection events, depending on the method:

- Access Control Rules—`Content Restriction`
- DNS Sinkhole—`DNS Block`

Requirements and Prerequisites for Content Restriction

Model Support

Any, or as indicated in the procedure.

Supported Domains

Any

User Roles

- Admin
- Access Admin
- Network Admin

Guidelines and Limitations for Content Restriction

- Safe search is supported by Snort 2 only.
- YouTube and Google do not support the YouTubeEDU feature that was implemented in access control rules. Please remove any access control rules that configure YouTubeEDU as they are not truly functional. You can also remove associated decryption rules.

Using Access Control Rules to Enforce Content Restriction

The following procedure explains how to configure access control rules to restrict content.”

Note When safe search is enabled in an access control rule, inline normalization is enabled automatically.

Procedure

Step 1 Create a decryption policy.

Step 2 Add rules for handling Safe Search traffic:

- Choose **Decrypt - Resign** as the **Action** for the rules.
- In **Applications**, add selections to the **Selected Applications and Filters** list:
  - Safe Search—Add the `Category: search engine` filter.

Step 3 Set rule positions for the 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 decryption policy with the access control policy.

For more information, see Associating Other Policies with Access Control.

Step 5 In the access control policy, add rules for handling Safe Search traffic:

- Choose **Allow** as the **Action** for the rules.
- In **Applications**, click the icon for **Safe search** (🔒) and set related options.
  - Safe Search Options for Access Control Rules, on page 4
- In **Applications**, refine application selections in the **Selected Applications and Filters** list.

  In most cases, enabling Safe Search populates the **Selected Applications and Filters** list with the appropriate values. The system does not automatically populate the list if a Safe Search 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 `Category: search engine` filter.

For more information, see Configuring Application Conditions and Filters.

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 HTTP response page that the system displays when it blocks restricted content; see Choosing HTTP Response Pages.

Step 8 Deploy configuration changes; see Deploy Configuration Changes.

Safe Search Options for Access Control Rules

The 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 Choosing HTTP Response Pages.

Using a DNS Sinkhole to Enforce Content Restriction

Typically, a DNS sinkhole directs traffic away from a particular target. This procedure describes how to configure a DNS sinkhole to redirect traffic to the Google SafeSearch Virtual IP Address (VIP), which imposes content filters on Google and YouTube search results.

Because Google SafeSearch uses a single IPv4 address for the VIP, hosts must use IPv4 addressing.

Caution If your network includes proxy servers, this content restriction method is not effective unless you position your threat defense devices between the proxy servers and the Internet.

This procedure describes enforcing content restriction for Google searches only. To enforce content restriction for other search engines, see Using Access Control Rules to Enforce Content Restriction, on page 3.

Before you begin

This procedure applies to threat defense only, and requires the IPS license.

Procedure

Step 1 Obtain a list of supported Google domains via the following URL: https://www.google.com/supported_domains.

Step 2 Create a custom DNS list on your local computer, and add the following entries:

- To enforce Google SafeSearch, add an entry for each supported Google domain.
- To enforce YouTube Restricted Mode, add a "youtube.com" entry.

The custom DNS list must be in text file (.txt) format. Each line of the text file must specify an individual domain name, stripped of any leading periods. For example, the supported domain ".google.com" must appear as "google.com".

Step 3 Upload the custom DNS list to the management center; see Uploading New Security Intelligence Lists to the Secure Firewall Management Center.

Step 4 Determine the IPv4 address for the Google SafeSearch VIP. For example, run `nslookup` on forcesafesearch.google.com.

Step 5 Create a sinkhole object for the SafeSearch VIP; see Creating Sinkhole Objects.

Use the following values for this object:

- IPv4 Address—Enter the SafeSearch VIP address.
- IPv6 Address—Enter the IPv6 loopback address (`::1`).
- Log Connections to Sinkhole—Click Log Connections.
- Type—Choose **None**.

Step 6 Create a basic DNS policy; see Creating Basic DNS Policies.

Step 7 Add a DNS rule for the sinkhole; see Creating and Editing DNS Rules.

For this rule:

- Check the **Enabled** check box.
- Choose `Sinkhole` from the **Action** drop-down list.
- Choose the sinkhole object you created from the **Sinkhole** drop-down list.
- Add the custom DNS list you created to the **Selected Items** list on **DNS**.
- (Optional) Choose a network in **Networks** to limit content restriction to specific users. For example, if you want to limit content restriction to student users, assign students to a different subnet than faculty, and specify that subnet in this rule.

Step 8 Associate the DNS policy with an access control policy; see Associating Other Policies with Access Control.

Step 9 Deploy configuration changes; see Deploy Configuration Changes.