Protex Emailed Reports:

What they are

Some tips on interpretation

1. Search Engine Alerts

Protex scans the internet logs for blocked searches made on Google, Bing etc across all standard filter profiles. It will send an alert to defined school email addresses within 5 minutes of a blocked search. This will show the time and date, the blocked search term, the IP address of the device, and if available, the username and device name.

2. Blocked Site Summary Report

Protex will send a report via email once a day, summarising the total number of blocked site web sites in selected categories for each filtering profile. This includes reporting on the Internet Watch Foundation Child Abuse list and also the UK Home Office Prevent list.

Please log a ticket via support@internet4schools.uk if you would like these features enabled on your Protex filtering system.

Interpreting the Daily Blocked Sites Alert Summary Report

The report provides the school with daily evidence that safeguarding via web filtering is taking place and therefore fulfilling DfE requirement for filtering. These e-mailed reports only contain blocked access, in other words if a site is listed it means that access has been prevented..

The reports will list many web sites in categories that may seem concerning such as Pornography and Illegal Hacking. However, unless the web site name is well-known or obviously reflects the reported category, it is likely the listed sites are actually “secondary” items such as revenue generating advertising or tracking sites that are called in the background when users or apps make requests to bona-fide web sites. These might include obscurely named "content-delivery" web sites that have been known to harbour harmful or dubious content.

In other-words it is unlikely that users will have deliberately attempted to access any of the listed sites.

When a user browses and loads up an internet page there may be many linked "background" calls to advertising and tracking sites, and pop-ups trying to take you to other things like chat bots and embedded "news" banners etc. The user may type a bona-fide web site name into a browser address bar and be totally unaware of all the background activity going on. Or it could be a block was made because a download from part of a web site has been prevented, for example .zip and other file types are not allowed from untrusted sites.

Although not infallible , the search term alerting that is also in place for Protex Filtering users should have created a separate real-time blocked-search report if a user were actively searching for harmful content.

To investigate any of the blocked sites in more detail , the process would be:

1. Login to the Protex system
2. Go to Logging > Log Analysis
3. Select a date (range) NB reports are generated at 3:00am for the previous day's activity.
4. Enter the URL that you want to report on into the "Enter a URL" box. e.g. cm.mgid.com
5. Tick the 'Check to download results into a .csv file'
6. Run Report - if you get a warning that a report could take a long time, just click the Run Report again.
7. You should get a web-page of results and also a csv file. The results file will contain the IP address and/or username of the client(s).

Interpreting Blocked Search Reports

Blocked Search Reports are emailed out within 5 minutes of the search being made and blocked by Protex. There are six classes of blocking.

Banned Search Words
Banned search term
combination search term
Exception search term
Weighted search term limit

Content Check limit

The first five types all relate directly to the words that are typed into the search engine. See below example where a user has searched for a specific games site.

Time: 08/09/23 10:50:01
UserName: none
DeviceName: GBLS-ACER.school.domain
User IP address: 10.12.13.14
Filter Profile: E2BN:Primary
Search Term: fortnite
Blocking Type: "Banned Search Words: " Protex Status: BLOCKED by Protex

The "Content Check limit" blocking type can be triggered for a variety of reasons. It could be triggered directly by search words that have been typed into the search engine but it more often it will be related to Protex inspection of the search results; or the "feed" of suggested images or videos. The individual suggestions may not be overly inappropriate but when totalled can trip Protex's content-check mechanism. In the case of content-check limit you may often see the **Search Term** entered by the user is not inappropriate at all and is not cause for concern.

Example of content check where search term IS inappropriate

Time: 08/09/23 10:40:17
UserName: none
DeviceName: none
User IP address: 10.12.13.14
Filter Profile: E2BN:Primary
Search Term: friday the 13th game
Blocking Type: "Content Check limit " Protex Status: BLOCKED by Protex

Example of content check where search term is NOT overtly inappropriate

Time: 13/09/23 10:24:04
UserName: none
DeviceName: none
User IP address: 10.12.13.14
Filter Profile: E2BN:Primary
Search Term: ring
Blocking Type: "Content Check limit " Protex Status: BLOCKED by Protex

To run an daily activity report for a user or IP reported in a blocked searches alert the process would be:

1. Login to the Protex system
2. Go to Logging > Log Analysis
3. Select the date of the report
4. Enter the Username if shown in the report and/or IP address
5. View Activity by ACTION – SHOW ALL DENIED (SHOW ALL if you want everything)
6. If you just want a summary you can tick the “Show summary information Top NN DENIED/ALLOWED”
7. Tick the 'Check to download results into a .csv file'
8. Run Report - if you get a warning that a report could take a long time, just click the Run Report again.
9. You should get a web-page of results and also a csv file. The results file will contain the IP address and/or username of the client(s).

If you are concerned about a particular online activity or incident, please contact us for help and support with analysing the weblogs.