Youth protection filter

Opportunities and measures regarding WiFi hotspots

HOTSPLOTS whitepaper, last updated: March 2022

hotsplots GmbH
Dr Ulrich Meier, Dr Jörg Ontrup
Rotherstr. 22
10245 Berlin, Germany
E-mail info@hotsplots.de
Phone: +49 (0)30 29 77 348 0

General information on filter solutions for WiFi hotspots

At certain locations (e.g. in schools or children's libraries, but also in public transport), the use of a youth protection filter is often mandatory or desired by the operators. In addition to children and adolescents who are to be protected by the filter, adults naturally also use these Internet access points.

The operation of filter solutions at public Internet access points is therefore not without its problems. The basic rights of adult users can be violated by this filter. For example, a so-called content filter, in which the content of accessed websites is searched for keywords, violates the confidentiality of telecommunications. Other filters such as content analyses, deep packet inspection and similar technologies are also incompatible with telecommunications privacy policy in Germany.

Due to the importance of maintaining telecommunications privacy, filters based on DNS[1] are preferred over content filters. URLs that are comprehensible for humans like *www.hotsplots.de* are translated via DNS into IP addresses readable by computers, like *92.51.175.170*.

Notes on the use of filter solutions

Since filter solutions can restrict adults' basic rights and the inaccessibility of websites can also cause financial damage, this must be pointed out before using a hotspot with an active youth protection filter.

With HOTSPLOTS, the reference to an active parental control filter is automatically displayed on the respective login page.

Every site owner should be aware that a perfect filter solution on the Internet is not technically feasible. Any filtering solution allows pages that should be blocked and blocks pages that should be reachable. Technically savvy users can also find ways to bypass the filter.

If, for example, a hotspot user knows the IP address of an inappropriate page and calls up the page directly via the IP address (e.g. *92.51.175.170*) instead of the understandable URL[2] (e.g. www.hotsplots.de), no DNS service is required and the filter will not work. In addition, certain settings on the end device can be used to select a different DNS server without DNS filter – this bypasses the protection mechanism.

An image search via search engines such as Google will always lead to corresponding results, as search engines are not found on the filter list and their search results are not blocked accordingly. To ensure better protection for children and adolescents, HOTSPLOTS refers to search results generated by the search engine with the "SafeSearch" configuration enabled (see section "SafeSearch at Google or Bing, YouTube Restricted Mode" on page 4 of this document).

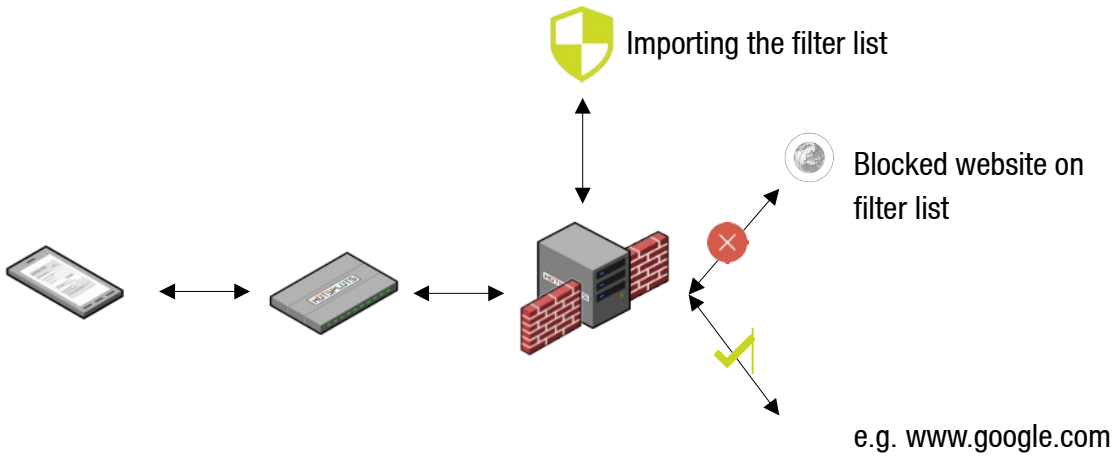
[1] DNS is the abbreviation for Domain Name Service.
[2] Uniform Resource Locator – in common usage, URLs are also referred to as Internet or Web addresses.

Furthermore, it can always happen that some websites that would be important and helpful for some users are included on the filter list.

So the bottom line must be this: A DNS-based filter is a reasonably effective way to protect children and teenagers on the Internet from content that is harmful to minors or not suitable for minors, but complete protection is technically never possible.

The filter solution at HOTSPLOTS

Youth protection filters at HOTSPLOTS are always provided on the basis of a DNS filter. In concrete terms, this means that all user website requests are first checked by the filter. If the requested page is on the filter list, it will be blocked with a notification.



The filter lists used by HOTSPLOTS currently contain more than two million entries and are continuously updated and further developed.

All users are informed on the login page of the hotspot that a youth protection filter is activated at this hotspot. This also documents to the user that the site owner takes the topic seriously and deals competently with sensitive topics.

SafeSearch at Google or Bing, YouTube Restricted Mode

DNS filters especially do not work on search engines like Google or Bing because – as mentioned above – search engines are not listed in the filter lists.

In addition to the DNS-based filter, the search engines offer configurations with which the respective search results are filtered both in the traditional (text) search and in the image search before being displayed in the browser. When using a HOTSPLOTS Parental Controls Filter, the call of these configurations is activated on the server side at the respective location.

Specifically, that means: Once the Parental Controls filter is enabled, the end user data accessed via the HOTSPLOTS servers is automatically redirected to the Google or Bing “SafeSearch” configurations or to YouTube Restricted Mode.

As a site owner, it is important for you to know that in these cases, content will be filtered that is considered to be adult or harmful to minors under U.S. law. In YouTube Restricted Mode, the comment function for the displayed videos is also partially hidden.

Technical implications and limitations when using DNS-based youth protection filters

By using the SafeSearch configurations of the major search engine and service providers such as Google or Microsoft, there is a considerable risk that services of these providers cannot be used transparently and completely without errors. At various locations, for example, it was observed that services such as Google Meet or Microsoft Teams can only be used to a limited extent if the youth protection filter is activated. Further restrictions were also observed in connection with WiFi Calling functions.These restrictions are beyond the control of HOTSPLOTS, as many services rely on DNS to realise certain functions. Therefore, before switching on a DNS filter, it should be taken into account, that certain web applications or services may no longer be fully functional.

Friendly WiFi

"Friendly WiFi" is a secure certification standard for public WiFi initiated by the British government. It was launched in 2014 to ensure that public WiFi meets minimum filtering standards, especially in areas where children are present.

Friendly WiFi cooperates with "Project Arachnid". Project Arachnid is a global solution that Internet Service Providers (ISPs) and filtering companies can access to improve their filtering solutions in the global fight against online threats to children and young people. This filter list is updated daily. A special feature of Project Arachnid is that not only are the URLs to be filtered collected and made available, but the project also actively supports the removal of content from the Internet.

As an Internet service provider, HOTSPLOTS meets the requirements for the certificate of Friendly WiFi.