Backgrounder
Access impediment methods / Blocking Internet pages
Updated: Mai 2010

The word „blocking“has been widely replaced by „access impediment“when it comes to manipulating the Internet infrastructure to prevent the access to Internet pages. That is due to the fact that there is a way around all the currently existing methods and therefore neither of them can claim to really block an Internet page. Each one of the different methods has its disadvantages and puts the functioning of the Internet at risk.

The technically easiest method to implement blocks[1] is to manipulate the Domain Name System (DNS). Similar to a phone directory, the DNS translates a domain name into the IP-address. Of course, this IP-address can be entered as a number directly into the browser window as a way to go around the block at the DNS server. As an alternative, the user can make simple settings changes, easy even for lay people, to search other DNS servers, in other words to prompt their computers to call a different telephone directory. What has been learned from experiences with previous blocking attempts is that providers of illegal contents react to such blockings within hours and change their domain names as a way around the blocking.

Moreover, DNS blocks lead to completely different and -objectively seen- wrong DNS data in the individual servers. When the hierarchical DNS was developed, however, there was particular emphasis put on the availability and consistency of all data. This is achieved by using primary and secondary servers that update each other fully automatically. Once the DNS is manipulated, these servers no longer reflect the real world. The DNS management will become an absurd Endeavour and ultimately turn into a purely German DNS.

The numbers of infringements that come into consideration and the number of unwanted pages on the Internet that require blocking can quickly amount to thousands. When individual domains have to be blocked from the DNS more than once and when huge lists of to-be-blocked websites have to be updated daily, the performance of the DNS will suffer very quickly. Regular Internet surfers have to suffer a loss of quality, the net becomes extremely slow. The access providers are burdened with significant costs.

The alternatives for the DNS blocking, the IP blocking or proxy blocking can be bypassed with easy technical measures, both by the providers as well as the users. Depending on which type of blocking is used and depending on the configuration of the blocked server, besides illegal content, other services and content can be blocked too, for instance email or domains that were not supposed to be blocked at all.

[1] A detailed description of the different technical methods and their problems can be found in the appendix

The act of blocking is an intrusion into the right for informational freedom guaranteed by the basic law, according to which any person has the right „to inform himself without hindrance from generally accessible sources. “ Even if violations of general laws or the youth protection law can justify such an intrusion, in each case, it is necessary to weigh the interests protected by the right for informational freedom against the legally protected interests which justify the inadmissibility of the objected www contents according to the respective laws. Blocking legal contents at the same time, however, cannot be justified like this.

Content providers affected by blocks so far have not had a point of contact where they can object to the blocking or ask for the page to be released if the illegal content was removed. They probably initially contact their access provider who, however, is not in the position to make a decision.

The blocking discussion should not lead to a situation where access providers are made responsible for contents that are put through. The German Telemedia Act (TMG), respectively the previous Telemedia Law (TDG), based on the implementation of a EU-Guideline (200/31/EG) categorically rules out that access providers are held responsible for contents that are put through.

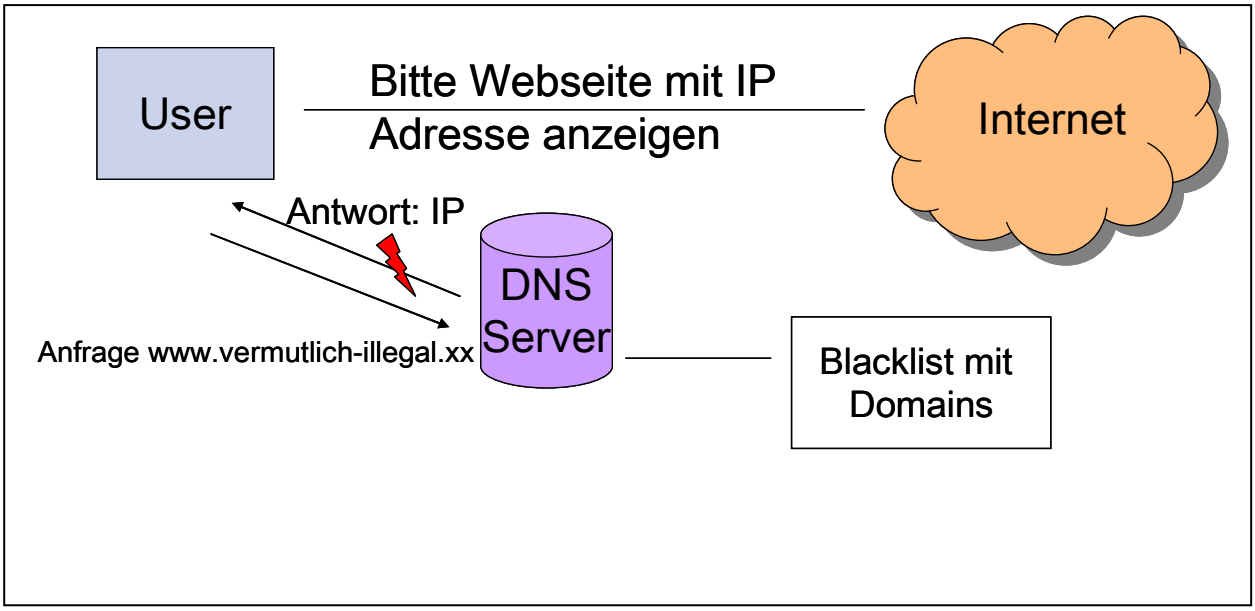
What's more, data privacy laws disallow the surveillance of Internet traffic by access providers. Access providers are also not obligated to proactively monitor contents that are put through. The law makers wanted to avoid access providers from being burdened with a surveillance obligation for contents which would not be feasible due to the amount of data alone.

Further information on current political and legal topics regarding the Internet can be found at www.eco.de/politik

Appendix

Explanation regarding the different blocking methods[2]

[2] The explanations are based on an article in the publication Spiegel Online (author Konrad Lischka) from February 5th, 2008 and were checked and amended by eco, the graphics are done by eco



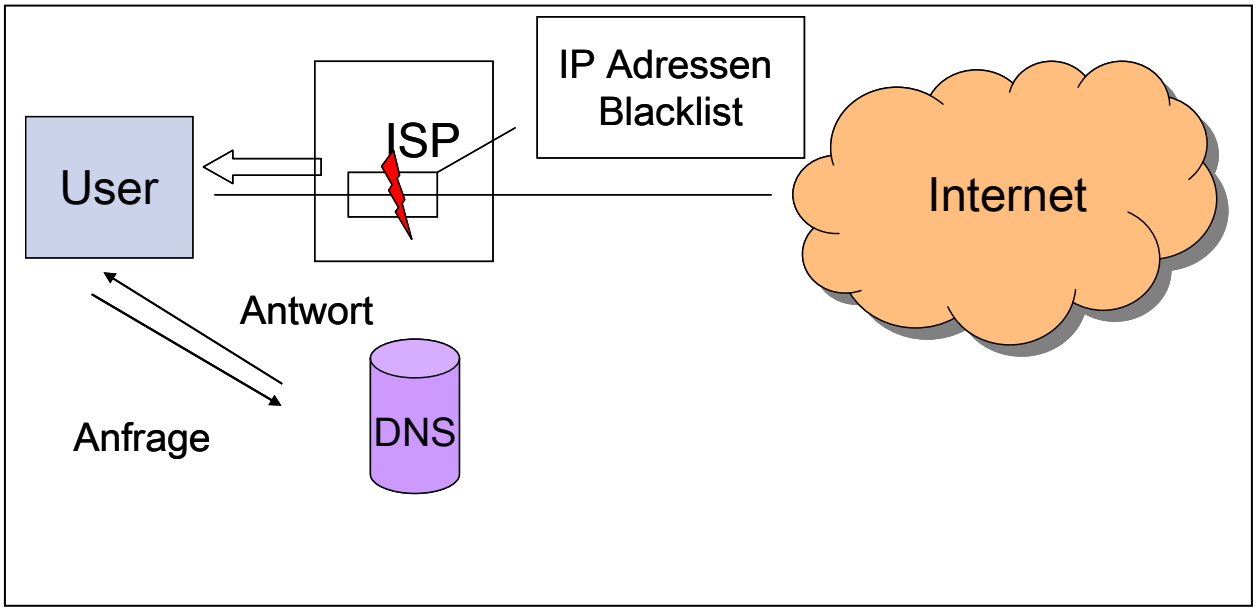
Principle:

The web addresses (URLs) entered into the browser as a string of letters have to be translated into a certain string of numbers, the so-called IP-address, in order to access Internet contents from the respective sources. The Name Server IP-address directories, comparable to a phone book, store the information regarding which IP-addresses currently belong to which URLs. Generally, every Internet provider has their own name server for their customers. The provider could as an example take the address smut.xx and assign it a false IP-address that for instance links to a website containing information about the blocking.

Problem:

It is relatively easy to go around this blocking, because the users can determine themselves which name server their computers use. Besides, there are free web offers that translate a URL into an IP-address. There is also the dangerous possibility that a multitude of completely harmless pages are also affected by the blocking since a whole domain is blocked which makes legal contents also inaccessible.

2. IP-level blocking



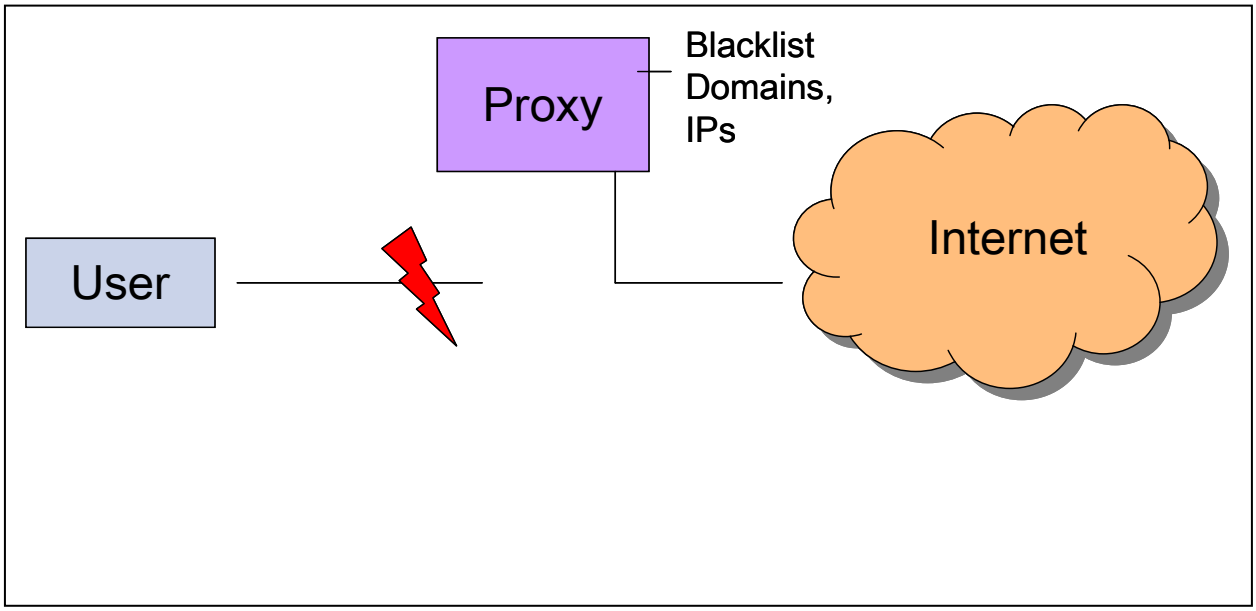
Principle:

The provider can block the respective IP-address behind the URL that is supposed to be blocked.

Problem:

Several thousand URLs can be behind an IP-address. In such cases the IP-address leads to the server of a larger provider of web storage. The provider himself distributes the entire traffic to the offers he provides. When the provider blocks such a mass IP-address, the collateral damage is quite possibly enormous. Besides the actual goal for a specific block, it is possible that many completely harmless contents are blocked as well. What's more, this block can also be bypassed at the transport level: That is made possible by open proxies used to route data traffic or by using anonymizer services such as TOR or JAP.

3. URL-level blocking



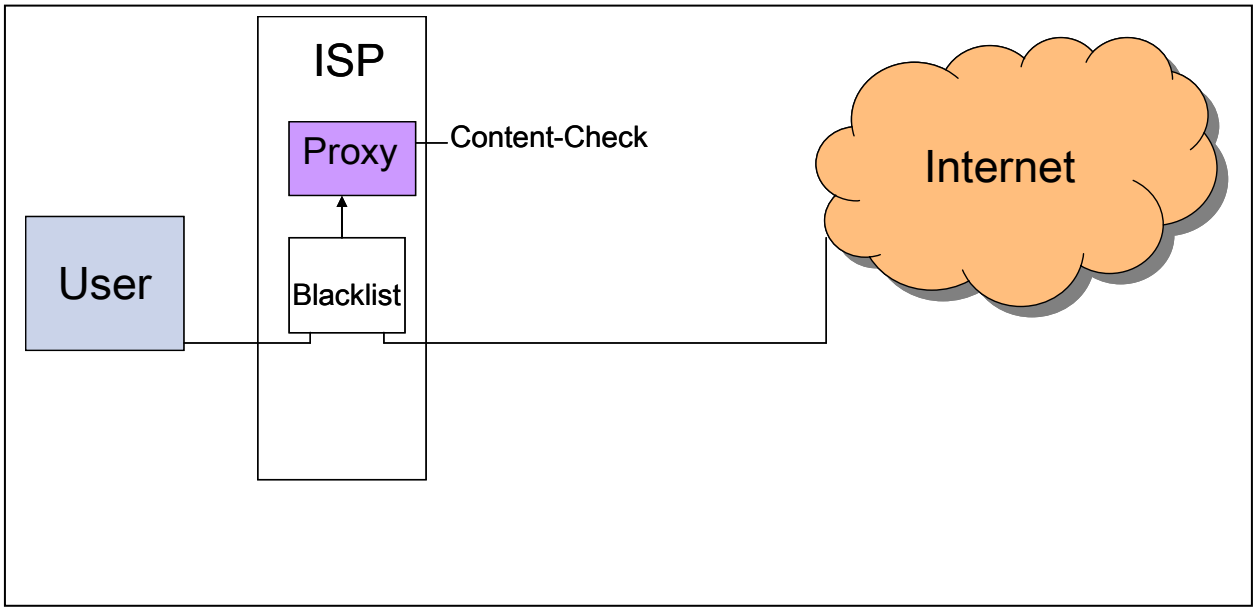
Principle:

In order to filter at this level, the provider has to do an in-depth analysis of his users'data traffic. It takes a lot of effort to find out which web-address is requested. This is how collateral damage can be avoided: Even with identical IP-addresses the provider differentiates with this principle which content is accessed.

Problem:

This filtering method requires a very high computing power to analyze the data traffic. Moreover, the necessary systems have to be acquired since these are generally not in place. The consequence is: very high cost, occasional slower connection time, and compromised reliability. Apart from this, such analyses may bring up legal issues in Germany: The secrecy of telecommunications principle may disallow such an intensive analysis of Internet use.

4. IP and URL-level blocking



Principle:

This system combines filtering at the IP and URL level. This is somewhat similar to the cleanfeed system practiced by the British Telekom (BT) in the UK. The cleanfeed is a two level hybrid blocking system used by the BT in order to block access to websites with child pornography content. The cleanfeed is a combination of IP blocking and proxy blocking. Basically, the IP blocking method is used, whereas (only) selected traffic is routed to a proxy; a suspicious IP domain is predefined. Only when the users request data from this address domain does the complex data traffic analysis begin. This proxy „decides“then according to a URL blacklist (in the case of BT generated by the Internet Watch Foundation –IWF) whether to block or not to block. So at the first level a check is done to see if the IP address to be used points to suspicious contents. If this is the case, another check is done at the proxy to see if the „accessed“URL is on the proxy blacklist. If that is also the case, a block is placed. The user receives a 404 error message. In all other cases the desired website can be accessed by the user.
When the IP addresses are checked in the first steps, the IPs matching the blacklisted URLs are sorted out. The IP list used for the check is generated by translating the URLs into IP-addresses (DNS).

Problem:

The procedure is very costly, extremely high implementation costs are expected. German providers do not have the necessary technology in place. Moreover, the measure represents a massive intrusion into the Internet infrastructure which brings up considerable legal issues. Our research has shown that the number of addresses to be blocked in existing systems is limited. It must be assumed that this method is not suitable to be broadly used in the fight against a multitude of illegal contents (child pornography, right-wing extremism, copy rights infringements, illegal gambling, unfair competition, etc.)