Filters and tools for internet

The purpose of this document is to present some possible tools to filter the Internet. They are not perfect and some of them can be disabled easily, but they are useful for prudent use of the Internet. This document is divided into two main sections: network filters and personal filters. The first part includes various possibilities for configuring a filter in a server or router on a particular network and for blocking access to undesired web pages to all the computers and devices within that network. The second part presents various programs that can be installed directly onto the computer, smartphone, or tablet so as to block undesired pages, regardless of the network to which the device is connected.. At the end of the document there is a brief annex with instructions for some of the filters presented.

The difficulty of installation for the solutions contained in this document varies. If looking for a network filter that offers some protection to all users, OpenDNS (cf. 1.1.a) is a good option and is easy to install. For a personal computer, smartphone, or tablet, mobicip or k9webprotector can be of use (cf. 2.1).

1. Network filters

1. DNS filtering

Basic concepts: To access a web page, it is necessary to know the IP address of the server that hosts the page. When one wants to access a web page, usually only the URL address is known (e.g. www.google.com); nevertheless, on the technical level, it is the IP address that is essential. The computer retrieves the IP address from a Domain Name Server (DNS) (in this case 173.194.36.46). With the IP known, it is possible to access the web page. Without a DNS server the only way to do so is by directly keying in the IP address into the browser.

All internet connections are assigned a DNS server; normally, it is the one provided by the Internet Service Provider (ISP). It is possible, however, to change the DNS server by altering the Internet Service Provider settings. Some DNS servers include a filter, such that they will only retrieve IP addresses for acceptable web pages, and will block access to undesired sites. This means that none of the devices connected to that specific network can retrieve the IP addresses of blocked pages, and therefore the user is unable to visit those sites.

Advantages of implementing DNS filtering:

- It is possible to filter all the devices inside a network (regardless of the device's Operating System, i.e. Windows, Mac, Mac, Android, iOS, etc.) without any special installation or configuration on the clients (i.e mobiles, PCs, tablets, etc.)

Limitations:

- If a user already knows the IP address of a web page (for example, he procured it from another network, e.g in his college or internet cafe), he can access the blocked page (e.g google) by simply keying in the numeric address (173.194.36.46, for google) in a browser and he will successfully reach the site without passing through the DNS filter.

- The network needs a firewall (e.g. a router) to force all clients to use the desired DNS server.

a. OpenDNS (www.opendns.com)

OpenDNS is a free public web filter DNS server (there are additional security services, which are available at a premium charge). The configuration is easy and information about it is readily available on the web.

Advantages

- Very easy to use: anyone can install it in a network (cf. Annex 1).

- A local DNS server is not needed.

- Maintenance is not necessary.

Limitations

- The OpenDNS server might be slower than a local DNS filter would be (cf. 1.1). This limitation can be remedied in part by configuring the router for *DNS caching* (cf. Annex 1).

b. Nxfilter (www.nxfilter.org)

Nxfilter is a program for Windows, Mac and Linux, for installation of a local DNS server with its own filter in a network. All the clients on the network that wish to access a webpage will request the IP from the internal *local* DNS server which will in turn request the external Internet DNS server for that IP address. It is easy to install and the configuration is not difficult; a tutorial can be found on the company's web page.

It is similar to OpenDNS but has more options, such as advertisement filters, and it is easier to enable custom filters and timetables for different users. It is very useful if one needs more options beyond the basic filtering and controls that are available in OpenDNS. It is also possible to use Nxfilter together with OpenDNS.

For added control over specific clients, *Nxfilter* allows for installation of "agents" (small programs) on those client machines (for Windows and Mac). This could be useful, for example, for a computer room used by children, in which access to some programs needs to be restricted. Installation of such agents, however, is not necessary for personal computers.

Advantages

- Easy to install, little configuration.
- For basic filter features, there is no need for installation of agent-programs on the client side.
- Capacity of specifying user profiles and timetables.
- An old or small computer is sufficient to run a small-medium network filter, given that it is a lightweight program (e.g. *raspberry pi 2*).

Disadvantages

- Requires a server, on which Nxfilter is installed, to be always running.

2. Proxy server

A proxy-server is a server that acts as an intermediary for requests from clients seeking access to a webpage or other resources. The client makes the request to the proxy-server, which in turn retrieves the requested page through the DNS server. This implies that clients do not have direct access to the Internet, and make all their webpage requests through the proxy server

There are two possible configurations:

- Transparent proxy: Client machines on the network are unaware of the proxy's existence. The proxy server simply transmits information without modifying requests or responses.
- Non transparent: Clients have to explicitly request the proxy server to retrieve desired web pages. Either the browser or the internet connection must be configured to use the proxy-server. If any client tries to access the Internet directly, bypassing the proxy-server, the request will fail.

Advantages

- Blocks access to web pages even when the user attempts to retrieve them with the IP address.
- Includes additional filtering possibilities through configuration of the proxy server.

Limitations

- Difficult to install and requires maintenance.
- The computer with the proxy must be always running.
- Transparent proxies are easier but cannot filter "https" web pages (Gmail, Google, Facebook,

Youtube).

- Non transparent proxies generally can filter requests for https pages. They do not always work, however, with Android devices. One solution could be to implement a non-transparent proxy, and open port 443 (the one for https) only for Android devices, which would not have any filter for https pages. Https requests from non-Android devices using the proxy would be filtered, given that they would not be using the unfiltered port.

To install the proxy server in a computer, there are two possibilities: installation of a ready-to-use server or installation of proxy software in an already running operating system.

a. Out of the box server OS (Operating System)

Here are three possibilities:

- *Untangle:* a paid version with more features than the free versions listed below. *Untangle Web Filter Lite* (www.untangle.com/shop/Web-Filter-Lite) is the free version of *Untangle* in which one can choose between 15 filter categories. It is the easiest to install and has a web GUI that facilitates configuration.
- *IPFire* (www.ipfire.org): free Linux distribution ready-to-use server. It is open source and has no limitations. Information is readily available in the web and it has a web GUI for configuration.
- *pfSense* (www.pfsense.org): free BSD distribution, with the most complete GUI for configuration, which, however, makes it the most complicated of these to use.

Advantages

- Installation and configuration is not difficult, given that the system is 'ready to be used' as a server.

Disadvantages

- It would probably be difficult to use the computer with the proxy server for other purposes, but this is normal.

b. Proxy server software

For those who prefer to install one's own server, here are some programs that have a proxy filter:

Linux:

The configuration is not very difficult, but it is not very intuitive and user-friendly. The OS presented in 2.a also use these programs, but they also provide their own more user-friendly configuration

programs.

- Squid: is the proxy server.
- Squidguard: a proxy filter that works with squid.
- Dansguardian: similar to squidguard.
- Iptables: firewall.

Windows:

There are few good free possibilities. The ones mentioned below have many limitations, but they can be of use in small networks, especially if the objective is to provide access to a small number of web pages. Nevertheless, Nxfilter would probably be a better option.

- Privoxy
- ccproxy

Disadvantages

- Installation is not easy and the configuration is not user-friendly at all.

2. Personal filters and other tools

These items can be useful when the network does not have its own filter or if the computer (i.e. laptop) is used in various locations.

1. General filters

There are various programs that can be installed locally to control internet access.

a. Smartphones and tablets

There are many programs that filter internet for smartphones and tablets. The two below are modifications of Firefox, an open source browser that has the capability of applying filters, which are only implemented on the app itself (i.e. the user accesses the Internet using the app's browser) and not on other programs and browsers on the device. Both can be used with Android and iOS. *Mobicip* is probably the best option, because it works better and is more regularly updated, although k9webprotection also works well.

- *mobicip* (www.mobicip.com): commercial software, but with a free version as well. It is better than k9webprotection in performance, but the configuration of the filter is more limited (in the free version). It is not possible to filter by categories, although the settings allow for selection of various modes (strict, moderate and mature) with pre-established categories. The moderate mode seems to be sufficient and can also block apps on the device. To prevent any possibility of being uninstalled, one should block the "*install and uninstall apps*" option.

- *k9webprotection* (www.k9webprotection.com): free program with category filter. The primary disadvantage is that it is easy to disable (by going to: apps > running apps > stop process.). If one wants to block any possible access to the Internet, an app to block other apps (like *AppLock* for Android and iOS) should be installed and set to block all browsers and disable the possibility of installing and uninstalling apps. With this configuration, if the user disables k9webprotection, he will not have access to the Internet at all, given that all the other browsers are blocked too.

Both of the programs above are good options, although in smartphones or tablets with less operating capacity, they can be a little slow. However, they do not work well for all web pages and sometimes the program/browser crashes.

Apart from mobicip and K9, for Android some filtering can be applied through the settings available on Android*'s old* browser and this option requires fewer system resources. The problem is that Google has not released recent updates, given that they decided to stop maintaining the old browser. The browser and filter tend to work better if picture loading is disabled (an option for browsers on almost all smartphones, to minimize incoming data). Two examples of such filters are *Safe Browser - The Web Filter*, and *Ranger Pro Safe*. If running on an old device, many web pages will make the filter program crash. If such is the case, then, it would probably be best to buy a new smartphone and use mobicip.

In Annex 2 other possibilities to filter a device are included, although they are more complicated and they are relatively new. They can be kept in mind as potential options for the future.

b. Computers:

For personal computers and laptops, the same programs detailed above for mobile devices are also available and work quite well.

- *k9webprotection* (www1.k9webprotection.com): for Windows and Mac, easy to install.

- *mobicip* (www.mobicip.com): only for Windows.

2. Plugins chrome, firefox, opera

Many browsers offer the possibility of installing plugins and some of them are very useful for filtering the internet. There are three possibilities: filters, ad blocking, and image blocking.

The following plugins are only for computers, because the iOS and Android versions of these browsers do not support them. Currently, on these mobile operating systems, only Firefox supports

plugins and there are very few available. This will most likely change in the future.

Plugins are very easy to use and easily accessible. They are not intended to block the Internet, because they can be disabled easily. For some, passwords can be applied, but for anyone with some experience, they are easy to get around. Simply put, they are tools that make Internet use more comfortable.

a. Filters

The following are web content filters. The user can apply white (viewable sites) and black (blocked sites) lists.

- *Foxfilter*, *WebFilter Pro* or *Blocksi*.

b. Ad blocks

Block all advertisements on web pages.

- *AdBlock Plus*: for Opera, Firefox, and Chrome (in Chrome, personal filters can be applied).

c. Image blocking

These are very useful tools, because they block all images on a web page, enabling the user to browse sites with fewer worries about content. Keeping in mind that there are no perfect filters, these plugins can help make internet use more peaceful.

- Some plugins enable and disable image viewing with a simple ON/OFF switch (e.g *Hide all images 1.4.1*, *Image block*).

- Others provide more options. For example *Wizmage Image Blocker* for Chrome blocks all images at first, but allows the user to display them by clicking them one by one in the top right corner of the image. Also, the user can create a white-list of web pages, in which images are loaded immediately.

- *Opera* and *Chrome* allow for image blocking without having to install a plugin:

    - For Opera: *Settings* > *Web content*. Also in Opera, one can permanently block or make certain pages viewable.

    - For Chrome: *Settings* > *Privacy - Content settings* > *Images*.

Annex 1 - Install OpenDNS

1. Get an OpenDNS account (*OpenDNS >Personal >Parental controls>OpenDNS Home*).

2. Configure the account

    a. Select the categories to filter.

    b. Add your network. Why it is necessary to add a network? Because when you add your network (your IP address) OpenDNS will apply your configuration to all the connections on that network. It is the way OpenDNS recognizes clients. With the IP address, OpenDNS is able to identify the network. Because most people do not have a static IP address, OpenDNS has a system to update the IP address of the users, as explained below. (https://support.opendns.com/entries/25213189-Dynamic-IP-General-Information-for-OpenDNS-usage)

3. Configure a network to update the IP address in OpenDNS. There are two possibilities:

    a. Configure the router to do it. This is the best option and many routers support it. Every router is different. In Google, search for "how to update OpenDNS for each particular router". In most cases, the router has the setting "*configure a dynamic DNS service",* or something similar, and the administrator simply inputs the OpenDNS user and password.

    b. A second option is to install a program, which is made available by OpenDNS, in one computer on the network. The computer does not need to be running for the filter to be active, but has to be turned on from time to time, so as to update the IP address. If the Internet Service Provider changes your IP every time the router is turned off, then the computer with the program must be switched on every time the router restarts (https://support.opendns.com/entries/23282614).

4. Configure the clients to use OpenDNS. There are two ways: configure the router or configure each client.

    a. Configure the router (recommended): configure the router to use the OpenDNS server by default (https://support.opendns.com/entries/27350174-Generalized-Router-Configuration-Instructions). It is advisable to enable *dns caching* whenever possible (available on many routers and they tend have it enabled by default). Also, it is necessary to configure the router to block other connections to DNS servers and set the internet connection setting to DHCP on the client machines (this tends to be the default setting).
    b. Configure each computer: in the internet connection settings, set OpenDNS as the DNS server.

Annex 2. Alternatives for mobile devices

As mentioned before (cf. 2.1.a), the recommended apps are simply modifications of open source browsers. They do not filter the Internet throughout the device, but only in the app itself. The filter does not apply to other apps (Youtube, other browsers, etc.). At the moment, they are the best option available to filter a mobile device.

VPN connections: Nevertheless, there is one way to filter a phone, without having to resort to a modified browser. A VPN is a connection to a private network. It is often used for security purposes, or to make available certain services, for instance in our case, a filter.

Although mobicip seems more practical for now, this system might be useful in the future. Here are some ways of using a VPN for filtering:

- *Safe Browsing Parental Control*: these apps connect devices with a filter via *vpn*. It is not entirely clear if the network through which the filter is provided is trustworthy. At the moment, it is not recommendable, but it can be kept in mind for the future. There is an Android version currently available, and there will be one for iOS soon.

- The second option is to use the filter implemented on one's own network. This is possible when the filter is applied with the DNS system explained above. It is necessary to have a VPN server. In some cases, this could be a router. Another possibility is to use the same server used for filtering, but applying a strong password (given that it is an open door to the Internet). Then a new VPN connection must be added to the mobile device to this VPN with the local DNS server as the connection's first DNS server. It is not necessary to have a static IP address because VPN supports dynamic IP addresses (with *DynDNS* or *no-ip*, for example). With a static IP address it is not necessary to have a VPN, because it is possible to use a local DNS server in the device with the static IP address. This system is complicated and only worthwhile if many people are going to use the same VPN.

The problem with using OpenDNS for portable devices is that it is a solution for networks, not individual devices. Thus, a mobile phone with 3G, an internet network for phones, does not have its own network, and therefore can have a different IP each time it connects, making it unrecognizable to the OpenDNS server. Also, even when it is possible to update the IP address in OpenDNS, the system can detect that the device is in a public network and disable the filter. OpenDNS does that to avoid applying one user's configuration to another user who is using OpenDNS in the same public network. One possible workaround would be to install a program to change the DNS settings in the device (*DNSet*) and another to update the IP in OpenDNS (*Dynamic DNS update*).