

How to Block Facebook access on Microsoft Windows XP / Vista / 7 and 8

Author : admin



In Office home network, there is a Windows XP computer which is spending all his official work time in facebook.

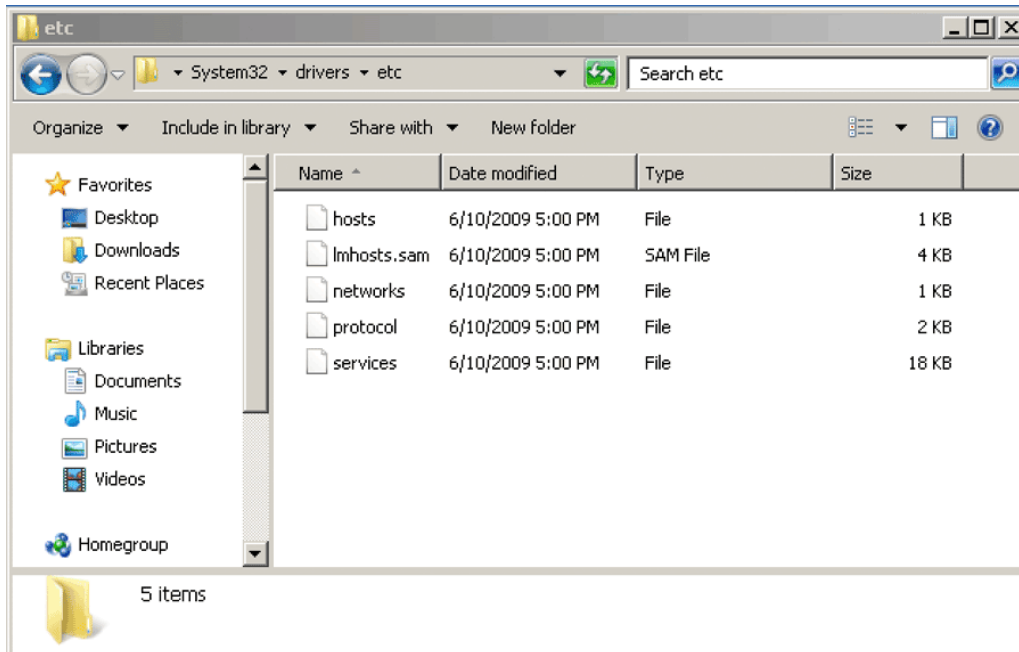
Hanging in facebook makes this social network freak work quite inefficient so something had to be done immediately ... and guess who had to do it ...

Usually I do [facebook filtering via iptables rules directly from Linux NAT router](#), but filtering facebook **https** (port 443 traffic) is real pain in the ass and moreover facebook has a bunch of hosts so filtering from Linux i-net router is not always best solution. In this specific case the Linux router deliving internet to the Win host was also having complete routing so filtering with iptables wasn't so easy.

To save myself from loosing few hours trying to discover *why I can't manage to filter facebook from Linux router*, checked online *if it possible to filter facebook using standard Windows method*.

It turns out on *Windows computer it is possible filter facebook by simply mapping all Facebook main hosts to localhost (127.0.0.1)* using **hosts** map file. In my case Win computer was running Windows XP, however on All Windows XP / Vista / 7 and 8, default location of hosts file is in:

C:\WINDOWS\system32\drivers\etc\hosts



Therefore I used Windows Explorer, navigated to *C:\WINDOWS\system32\drivers\etc* copied hosts file to Desktop, edited with **Notepad** and placed at the end of it following lines:

Block Facebook

```
127.0.0.1 api.facebook.com
127.0.0.1 connect.facebook.net
127.0.0.1 facebook.com
127.0.0.1 www.facebook.com
127.0.0.1 graph.facebook.com
127.0.0.1 profile-b.xx.fbcdn.net
127.0.0.1 s-static.ak.facebook.com
127.0.0.1 static.ak.connect.facebook.com
127.0.0.1 static.ak.facebook.com
127.0.0.1 static.ak.fbcdn.net
127.0.0.1 www.fbcdn.com
127.0.0.1 static.facebook.com
127.0.0.1 www.static.ak.connect.facebook.com
127.0.0.1 www.login.facebook.com
127.0.0.1 login.facebook.com
```

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10      x.acme.com             # x client host
127.0.0.1        localhost
# Block Facebook
127.0.0.1        www.facebook.com
127.0.0.1        facebook.com
127.0.0.1        static.ak.fbcdn.net
127.0.0.1        www.static.ak.fbcdn.net
127.0.0.1        login.facebook.com
127.0.0.1        www.login.facebook.com
127.0.0.1        fbcdn.net
127.0.0.1        www.fbcdn.net
127.0.0.1        fbcdn.com
127.0.0.1        www.fbcdn.com
127.0.0.1        static.ak.connect.facebook.com
127.0.0.1        www.static.ak.connect.facebook.com
```

Then copied the new modified hosts files from Desktop back to **C:\WINDOWS\system32\drivers\etc**
Following same logic, its possible to disable access to any host on the Internet. There are even some software like SpyBot which does by default change Windows default **hosts** file with pre-mapped well known *spammer / spyware / malware hosts* to prevent viruses and spyware to download more of themselves.

Finally to make Windows re-read new hosts file I had to restart the PC, and **Voila!** *Facebook access was cut :)*