# What is a Firewall?

A firewall is a tool that monitors communication to and from your computer and sits between your computer and the rest of the network, and according to some criteria, it decides which communication to allow, and which communication to block.

## What Is It Good For?

Identifying and blocking remote access Trojans. The most common way to break into a home computer and gain control, is by using a remote access Trojan (RAT). A Trojan horse, is a program that claims to do something really innocent, but in fact does something much less innocent. You may sometimes get some program, and believe this program to be something good, while in fact running it will do something less nice to your computer. Such programs are called Trojan horses. Personal firewalls can identify and block remote communication efforts to the more common RATs and by thus blocking the attacker, and identifying the RAT.

## How Does It Secure our PC?

- **Blocking/Identifying Other Types of Trojans and Worms?**

  There are many other types of Trojan horses which may try to communicate with the outside from your computer. Whether they are e-mail worms trying to distribute themselves using their own SMTP engine, or they might be password stealers, or anything else. Many of them can be identified and blocked by a personal firewall.

- **Blocking Advertisements?**

  Some of the better personal firewalls can be set to block communication with specific sites. This can be used in order to prevent downloading of advertisements in web pages, and thus to accelerate the download process of the web sites. This is not a very common use of a personal firewall, though.

- **Identifying/Blocking Spyware's/Adbots?**

  The term "spyware" is commonly used for various adware (and adware is a program that is supported by presenting advertisements to the user), and that during their installation process, they install an independent program which we shall call "adbot". The adbot runs independently even if the hosting adware is not running, and it maintains the advertisements, downloads them from the remote server, and provides information to the remote server. The adbot is usually hidden. There are many companies that offer adbots, and advertisements services to adware. The information that the adbots deliver

to their servers from the computer where the adbot is installed, is "how much time each advertisement is shown, which was the hosting adware, and whether the user clicked on the advertisement.

- **Hiding Your Computer on the Internet?**

  Without a firewall, on a typical computer, even if well maintained, a remote person will still be able to know that the communication effort has reached some computer, and perhaps some information about the operating system on that computer. If that computer is handled well, the remote user will not be able to get much more information from your computer, but might still be able to identify also who your ISP is, and might decide to invest further time in cracking into your computer.
  With a firewall, you can set the firewall so that any communication effort from remote users (in the better firewalls you may define an exception list) will not be responded at all. This way the remote user will not be able to even know that it reached a live computer. This might discourage the remote attacker from investing further time in effort to crack into your computer.

- **Preventing Communication to Tracking Sites?**

  Some web pages contain references to tracking sites. e.g. instruct the web browser to download a small picture (sometimes invisible) from tracking sites. Sometimes, the pictures are visible and provide some statistics about the site. Those tracking sites will try to save a small text either as a small file in a special directory, or as a line in a special file (depending on what is your browser), and your browser will usually allow the saving site to read the text that it saved on your computer. This is called "web cookies" or sometimes simply "cookies". Cookies allow a web site to keep information that it saved some time when you entered it, to be read whenever you enter the site again. This allow the web site to customize itself for you, and to keep track on everything that you did on that site. It does not have to keep that information on your computer. All it has to save on your computer is a unique identifying number, and then it can keep in the server's side information regarding what has been done by the browser that used that cookie. Yet, by this method, a web site can get only information regarding your visits in it. Some sites such as "DoubleClick" or "hitbox" can collect information from various affiliated sites, by putting a small reference in the affiliated pages to some picture on their servers. When you enter one of the affiliated web pages, your browser will communicate with the tracking site, and this will allow the tracking site to put or to read a cookie that identifies your computer uniquely, and it can also know what was the web page that referred to it, and any other information that the affiliated web site wanted to deliver to the tracking site. This way tracking sites can correlate information from many affiliated sites, to build information that for example will allow them to better customize the advertisements that are put on those sites when you browse them.
  Some personal firewalls can be set to block communication to tracking sites. It is not a

common use of a personal firewall, though, and a personal firewall is not the best tool for that, but if you already have one, this is yet another possible use of it.