Most of the computer users are familiar with the term Firewall. Firewalls are Hardware or Software programs that monitor incoming and outgoing connections analyzing the packet data for malicious behavior. Like the definition says, there are both Software and Hardware Firewall. In this modern age, we are literally at war with hackers and malware and virus developers, all the time and data security has become the number one concern. To protect our computers, we use security software like Antivirus and Firewalls – and as we just mentioned, there are two kinds of firewalls – Hardware firewalls and Software firewalls.

Hardware firewall vs Software firewall

In this article we'll talk about difference between Software Firewall & Hardware Firewall.

Hardware Firewall

Hardware Firewalls are mostly seen in broadband modems, and is the first line of defense, using Packet Filtering. Before an Internet packet reaches your PC, the Hardware Firewall will monitor the packets and check where it comes from. It also checks if the IP address or header can be trusted. After these checks, the packet then reaches your PC. It blocks any links that contains malicious behavior based on the current Firewall setup in the device. Hardware Firewall usually do not need a lot of configuration. Most of the rules are built-in and predefined and based on these in-built rules, the Packet Filtering is done.

Today's technology has improved so much that it not just the traditional Packet Filtering which is carried out. The Hardware Firewall has built-in IPS / IPDS (**Intrusion Prevention Systems**), that earlier used to be a separate device. But now these are included, offering us greater protection.

When an IPDS detects a malicious activity it sends and signal and reset the connection and block the IP address. It uses signature-based, statistical anomaly-based and stateful protocol analysis. The main drawback I find, is that it allows all the outgoing packets i.e. if by chance, a malware got into your system and started transmitting data, it would be allowed unless the user became aware of it, and decided to stop it. But in most cases, this does not happen.

Hardware Firewall are typically good for small or medium business owners, with 5 or more PC or a co-operate environment. The main reason is that it then becomes cost-effective, because if you're to purchase Internet Security/Firewall software licenses for 10 to 50 copies, and that too on an annual subscription basis, it will cost a lot of money and deployment could also be an issue. The users will have better control over the environment. If the user is not tech savvy and if they choose to inadvertently allow a connection that has Malware behavior, it could ruin the entire network and put the company in risk with data security. A hardware firewall could thus be very useful in such cases.

There are always few **things you have to consider** before buying a Hardware based firewall. The number of users in your network, number of VPN users in your network, because under-estimating the number could exhaust the performance of your device and affect the performance of the Internet connection as well. Also make sure you have enough licenses for VPN client connection, and it has SSL, PPTP, etc. connection support too. Even if you have to pay a subscription, go for it – because subscription means, you get the latest definitions.

Manufactures are now including Gateway Antivirus, Malware scanners and Content Filters, so you'll get maximum protection with them. For example CISCO Hardware includes "*Cisco ProtectLink Security Solutions*" on selected devices. It addresses a specific security threat, and as part of an overall security approach, provides layers of protection against different threats.

There are a lot of companies you can choose from like CISCO, SonicWall, Netgear, ProSafe, D-Link etc. Make sure you either have a certified network professional with you while setting up or a good tech support, because trust me you'll need them when you configure the system.

Software Firewall

Now that we know how Hardware Firewalls work, I'll talk a bit Software Firewalls. To be honest, Software Firewalls do not need a whole lot of explanation because most of us are aware of it and are already using it. Like I said in the Hardware Firewall section, if the user is not tech savvy and if they choose to allow a connection that has Malware behavior, it could ruin the entire network and put the company in risk with data security. **That's where software firewall comes into picture, as here can we block both incoming and outgoing connections and setup trusted rules so these accidents can be avoided.** Firewall vendors constantly research in this matter and see out updates as and when required, so the chances of your computer getting compromised are slim.

It's a confusing job to pick a complete Internet Security solution that is just right for you. When you search in forums you can see flaming debate, where each member is defending their favorite ones. You'll be lost in these debates ending up more confused than when you started. The rule is to set your priorities straight. Create a list of things you want. For example do you want a free Firewall solution or paid one? What features you need in your Firewall, What additional features are required, like say Antispam, Web Protection, Malware scanner, Antivirus, etc. Do you want to go in for an Internet Security Suite? Once you decide compare the features.

5 free software firewalls for Windows

The ***importance of a firewall*** cannot be over-emphasized. A Firewall can ***block threats*** that your antivirus may miss. Not only that, it can ***prevent hackers*** from breaking into your computer! The in-built Windows firewall is great – and just good enough for the regular home-user who wants protection and who does not want to be bothered with setting it up. Leaving the default values for your Windows firewall should suffice, and along with a good antivirus software, give you ample protection for your Windows computer. But if you want a package that offers more options and better protection then take a look at the following.

Free Firewall software for Windows

Let us check out some ***free stand-alone firewall software*** for your Windows PC.

Comodo Free Firewall

These days, the feature-rich and easy-to-use ***Comodo Free Firewall*** has become very popular. It promises to stealth your computer's ports against hackers and will also block malicious software from transmitting your confidential data over the Internet. The Comodo Free Firewall will monitor all aspects of communications between your computer and the Internet. This prevents common hacking methods such as port scanning. The firewall references a list of over two million known PC-friendly applications. If a file is not on this 'safe-list', the Firewall immediately alerts you to the possibility of attacking malware.

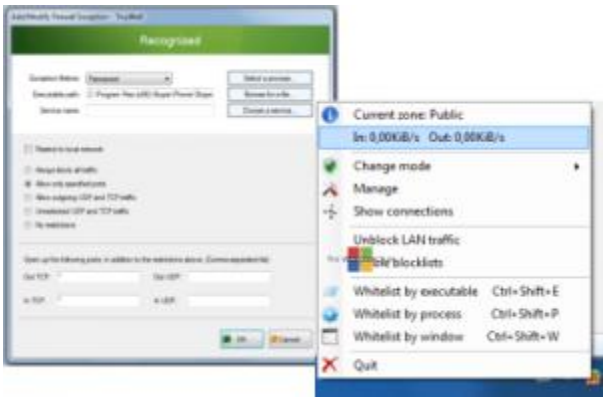
ZoneAlarm Free Firewall

ZoneAlarm Free Firewall at one point of time was the most popular third-part firewall for Windows – but over a time some started getting the feeling that it had become too bloated. It is nevertheless still the worlds most downloaded firewall software. The firewall is very easy to configure and fr an average user, its settings are best left at default. It is very effective in stopping Internet attacks at the front door and even catches thieves on their way out. Its 2-way firewall proactively protects against inbound and outbound attacks while making you invisible to hackers. *There are still many today who swear by it.*

Emsisoft Online Armor Free Firewall

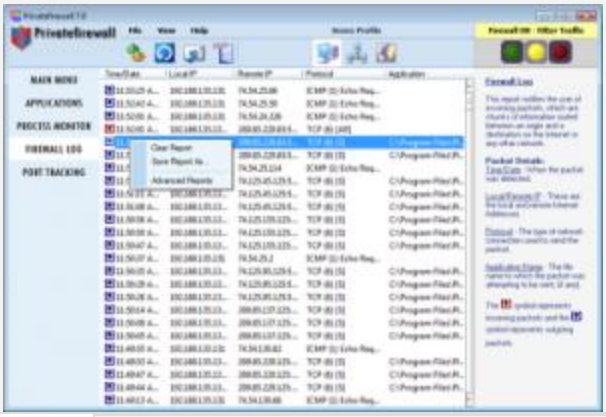
Online Armor Free Firewall helps stop Hackers, stops Malicious Programs and protects your Identity. It offers the following protection: Kernel Mode Security, Web Shield File/Registry Shield, Phishing Filter, Execution Protection, Termination Protection Limited Autostart Protection, Keylogger Detection, Tamper Protection, DNS Spoofing Protection and Script/Worm protection. *The free version offers lesser features as compared to its paid premium* offering - but if its basic inbound-outbound protection you are looking for, this firewall servers the purpose.

TinyWall



There are ways you can configure the Windows firewall using some thirdy-party tool. ***TinyWall*** is freeware that further hardens the advanced firewall of Windows 7. It is a light-weight solution with negligibale performance impact and lets you work without giving out any pop-ups whatsoever. No additional drivers or kernal components are installed with it. TinyWall will give your Windows Firewall a secure configuration and present you with a simple interface where you can easily define what has network access and what not. It will also allow you to easily prevent other programs from modifing or overwriting your firewall settings. If you are looking for a very basic and simple solution, you might want to consider using this firewall.

PrivateFirewall



PrivateFirewall

PrivateFirewall is a proactive, multi-layered defense solution for Windows desktops and servers. It detects, blocks and quarantines activity characteristic of known malware, hacking, phishing and other threat types. Its packet inspection, URL filtering, anti-logger, process monitor, and application/system behavior modeling and anomaly detection components stop hackers, spyware, viruses and other forms of malware before they can cause damage.