Unauthorized access, security threats, the inability to access inbound and outbound traffic or stealing crucial information, and the interruption of illicit software maximize network security risks in computers, thus making it vulnerable to Trojans and spyware. Firewalls function as an intrusion prevention system to one's PC and safeguards the local area network and keeps track of recognizable or undesirable stolen valuables out of your PC. Internet security is important but it completely depends upon the type and quality of the firewall and the way it has been set up.

Since cyber security comes with certain limitations, as they don't really hinder viruses, Trojans and spyware, which follow with normal Internet activities such as e-mailing and surfing. Certainly, all your system requires is important watchdog software in addition to firewalls. Typical firewalls generally keep watch on inbound traffic; the best example is Windows XP, so beware if you are still using it and going through innumerable threats. Obviously it's better than nothing, but a two-way firewall that checks both inbound and outbound traffic is astronomically better and the best option anyway.

Logically, the reasons behind network security are Trojans and key loggers. These threatening programs enter one's system through illicit sites visited by users without your consent, thus creating problems. Such threatening viruses allow its creator to manipulate your system while recording keystrokes, which may include Internet banking accounts and passwords and send those logs to the creator. An intrusion detection system is able to initiate an outbound connection and this is where the two-way firewall works.

If your firewall is set up with an appropriate method and doesn't override the outbound connection authorization, the key loggers certainly can't report back to their creator thereafter. An effective firewall blocks different ports through which loggers can seek important information from your system by blocking unauthorized traffic online. The best possible way to minimize threats on your system is by using firewall protection software. A firewall works dynamically as it protects the network from unauthorized access by outside parties, while letting appropriate traffic through. Since there are various firewalls depending upon one's choice, choosing the most appropriate one that suits your system requirements for Internet security is important.

Firewalls work as a simple concept as every communication transmitted between network devices is broken down into precise packets. These packets are equipped with both the origins, i.e. the originator of the message and the recipient. Packet filtering technology with built-in firewalls read it to determine the type of application message and properly assembling it if the originator of the message is authentic and easy to communicate with.

Now it may be clear that the basic functionality of a firewall is to protect your computer from illicit and unauthorized networks, thus network security is necessity. Those who access the Internet without a firewall are simply asking for trouble.

The Internet is replete with innumerable benefits that aid modern living. One can now communicate and stay in touch with a friend or family member, in real time, from across the globe. Internet banking and shopping has taken off and considerably improved their services and security offering significant conveniences for everyone. But on the flipside, the Internet can also bring security risks that can increase exponentially if you do not make sure that you protect yourself from the prevailing threats online; especially since it's as simple as installing the latest antivirus software.

There are various factors that impact internet security but if you have the latest antivirus protection program installed in your computer system, then it will keep you safe and secure from the security threats that come almost on a daily basis via internet.

Listed below are some factors that internet security:

Spyware

Spyware is a collective term that includes malware threats such as Trojans, adware, pop-up advertisement, modified cookies, key-logger and the like. Spyware does not include virus threats which are engineered to replicate themselves rather than spying or stealing information from computer systems. Basically spyware is configured in a certain manner to keep an eye on your online activities and uncover the security flaws. And that t is the first and foremost step in ensuring that your computer system is ready for stealing the vital information. With the help of spyware, computer hackers can steal sensitive information from your computer system-such as email and social networking user-ids and passwords, banking information, etc. And to keep your system safe and secure from spyware you must avoid free anti-spyware as many times it has been seen that most of the free anti-spyware programs turn out to be a spyware itself.

Spam Mail

Spam mails are not very dangerous; however, some of them may contain malicious links to websites and have some sort of embedded virus threats made using java-script or other similar programs. Once you click to browse or download (only if it contains downloadable files) your system can get severely affected with the embedded virus or even a spyware. And to avoid getting into these kinds of trap you must use the latest virus protection program along with the trusted email websites like Gmail, Yahoo Mail, Hotmail, etc., as they provide protection from spam mails by giving warning message as soon as you try to open an email from the spam or junk mail box.

Identity Theft

Hackers can steal sensitive information like credit/debit card details using numerous methods; and once they get access to it, they will use it for making online purchases using your credit/debit card details. In this situation only a well known antivirus software can protect you as most of the popular virus protection software comes with amazing features like offline scanning and protection, detects advanced threats, protects all emails from viruses, protects archived files and perform deep scans.

With the available software and advancements in technology today, something as simple as choosing the right Firewall for your computer might become a more complicated task than you had expected. A little confusion is justified-there are, after all, a lot of firewalls in the market today. A quick rundown of the best things to consider when shopping for a firewall should help clear things up.

1) What are the reasons for implementing a firewall?

"Because I need it for my computer security" is one of the top answers that would strike your mind after reading this question. But, there is also need to think about the technical objectives that you have in your mind about the implementation of the firewall. Such introspection is desired in driving the selection process. There is no need to pick the expensive or rich in features of the firewall, which is also too complicated for your technical requirements and can be met through simpler products.

2) How will the firewall fit into your network topology?

Consider also the following:

- Whether a firewall will accommodate the perimeter of the network or will be directly connected to the Internet, or will be serving to divide a sensitive LAN from the remainder of the organization?

- What will be the amount of traffic that will be processed?

- How many interfaces are desired to segment the traffic?

All the above aspects have a great part to play in the total cost in the implementation of the firewall, which saves you from under or over purchase of the computer security software.

3) An appliance or a software solution - Which will better suit your organization's network?

If you wish to ensure easy installation, then appliances are quite easier to install. One normally has to plug in the correct Ethernet cables and then has to carry on with the basic network configuration, which makes you ready to configure the rules. When it's about the software firewalls, then things can get a bit tricky at the time of installation and also require fine-tuning. Moreover, there's also miss in the security, which is many times constructed into the hardened OS of the firewall appliances.

4) Which operating system is best matched with your requirements?

You might know this, but yes even appliances run on an OS and, probably you might have to work with at some point in the firewall administration career. In case, if you're a Linux jockey, then you don't have to opt for a Windows-based firewall. Also, if you don't have an idea about the ⁄dev⁄null from ⁄var/log, then probably you want to stay away of the Unix-based solutions.