Firewall Information - Computer Firewalls

www.firewallinformation.com/

Introduction

Firewalls are computer security systems that protect your office/home PCs or your network from intruders, hackers & malicious code. Firewalls protect you from offensive software that may come to reside on your systems or from prying hackers. In a day and age when online security concerns are the top priority of the computer users, Firewalls provide you with the necessary safety and protection.

What exactly are firewalls?

Firewalls are software programs or hardware devices that filter the traffic that flows into you PC or your network through a internet connection. They sift through the data flow & block that which they deem (based on how & for what you have tuned the firewall) harmful to your network or computer system.

When connected to the internet, even a standalone PC or a network of interconnected computers make easy targets for malicious software & unscrupulous hackers. A firewall can offer the security that makes you less vulnerable and also protect your data from being compromised or your computers being taken hostage.

How do they work?

Firewalls are setup at every connection to the Internet, therefore subjecting all data flow to careful monitoring. Firewalls can also be tuned to follow "rules". These Rules are simply security rules that can be set up by yourself or by the network administrators to allow traffic to their web servers, FTP servers, Telnet servers, thereby giving the computer owners/administrators immense control over the traffic that flows in & out of their systems or networks.

Rules will decide who can connect to the internet, what kind of connections can be made, which or what kind of files can be transmitted in out. Basically all traffic in & out can be watched and controlled thus giving the firewall installer a high level of security & protection.

Firewall logic

Firewalls use 3 types of filtering mechanisms:

- Packet filtering or packet purity

  Data flow consists of packets of information and firewalls analyze these packets to sniff out offensive or unwanted packets depending on what you have defined as unwanted packets.

- Proxy

  Firewalls in this case assume the role of a recipient & in turn sends it to the node that has requested the information & vice versa.

- Inspection

  In this case Firewalls instead of sifting through all of the information in the packets, mark key features in all outgoing requests & check for the same matching characteristics in the inflow to decide if it relevant information that is coming through.

Firewall Rules

Firewalls rules can be customized as per your needs, requirements & security threat levels. You can create or disable firewall filter rules based on such conditions as:

- IP Addresses

  Blocking off a certain IP address or a range of IP addresses, which you think are predatory. What is my IP address? Where is an IP address located?

- Domain names

  You can only allow certain specific domain names to access your systems/servers or allow access to only some specified types of domain names or domain name extension like .edu or .mil.

- Protocols

  A firewall can decide which of the systems can allow or have access to common protocols like IP, SMTP, FTP, UDP,ICMP,Telnet or SNMP.

- Ports

  Blocking or disabling ports of servers that are connected to the internet will help maintain the kind of data flow you want to see it used for & also close down possible entry points for hackers or malignant software.

- Keywords

  Firewalls also can sift through the data flow for a match of the keywords or phrases to block out offensive or unwanted data from flowing in.

Types of Firewall

- Software firewalls

  New generation Operating systems come with built in firewalls or you can buy a firewall software for the computer that accesses the internet or acts as the gateway to your home network.

- Hardware firewalls

  Hardware firewalls are usually routers with a built in Ethernet card and hub. Your computer or computers on your network connect to this router & access the web.

Summary

Firewalls are a must have for any kind of computer usage that go online. They protect you from all kinds of abuse & unauthorised access like trojans that allow taking control of your computers by remote logins or backdoors, virus or use your resources to launch DOS attacks.

Firewalls are worth installing. Be it a basic standalone system, a home network or a office network, all face varying levels of risks & Firewalls do a good job in mitigating these risks. Tune the firewall for your requirements & security levels and you have one reason less to worry.

Some of the firewall products that you may want to check out are:

- McAfee Internet Security
- Microsoft Windows Firewall
- Norton Personal Firewall
- Trend Micro PC-cillin
- ZoneAlarm Security Suit

List firewall products at Amazon