A firewall is a firmware or software that prevents any unauthorized access to a network. It uses a set of rules to inspect incoming and outgoing traffic and blocks threats accordingly.

Firewalls are used in individual as well as enterprise settings. Many devices come with built-in firewalls, since they are considered a very essential component of network security.

**Why is a Firewall Important?**

Firewalls first emerged during early days of the internet, but are still widely used due to their influence on security. In fact, firewalls are the foundation of network security in a client-server model. In order to mitigate threats and inspect traffic, most of the devices use firewalls or tools that are closely related.

**Uses of Firewall**

Modern businesses use firewalls in integration with Security Information and Event Management (SIEM) strategy along with other cybersecurity devices. They are installed within either the network itself to create segmentation and protect against insider threats, or at the network perimeter for guarding against external threats.

Apart from swift threat defense, they also carry out important audit and logging functions. Administrators can use the record of events for identifying patterns and improving rule sets. Rules need to be updated from time to time in order to keep up with evolving threats. Hence, vendors can discover new threats and create patches to fix them quickly.

Firewalls are useful especially for connections that are always on, such as cable modem or Digital Subscriber Line (DSL), since those connections use static IP addresses. Firewalls are often used along with antivirus applications. Firmware/hardware firewalls are usually used to set up restrictions among in-home devices.

**Why Do You Need a Firewall?**

A firewall is crucial for secure web surfing. It generally does not allow any connection inside the network that is initiated from outside the network unless granted permission. Without a firewall, any application that runs on your system and accepts network connection can be connected with anyone over the internet. If a hacker makes connection with your application, they can easily compromise your computer in case they exploit a vulnerability in that application. Hence, a firewall is your first and most important line of defence on the internet.

In summary, firewalls are essential for preventing any intrusion into your private network and the computer systems connected to it. Whenever you are connected to the internet, it is recommended to position your system behind a firewall and avoid a cyber attack.