

## Firewall

---

Each computer that is connected to the [Internet](#) (and, more generally, to any [computer network](#)) is likely to become a victim of a computer attack by a hacker. The [methodology](#) generally used by [hackers](#) consists in scanning the network (by randomly sending out data packets) in search of a connected computer. Once a computer is found, the hacker searches for a security weakness in order to exploit it and access the data on the machine.

For several reasons, this threat is even greater when the machine is permanently connected to the Internet:

- The targeted machine is likely to be connected but not monitored
- The targeted machine is generally connected with a greater bandwidth
- The targeted machine does not change or rarely changes [IP addresses](#)

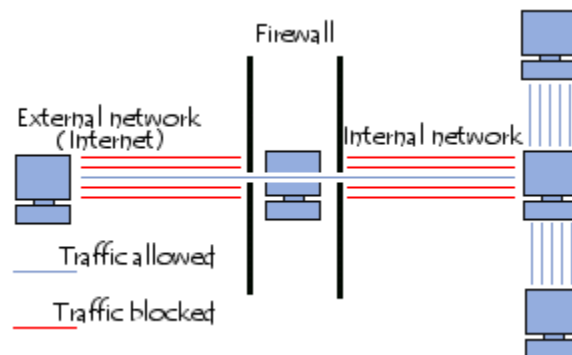
Therefore it is necessary for both company networks and Internet users with [cable](#) or [ADSL](#) connections to protect themselves from network intrusions by installing a protection device.

### What is a Firewall?

---

A **firewall** is a system that protects a computer or a computer network against intrusions coming from a third-party network (generally the Internet). A firewall is a system that filters data packets that are exchanged over the network. Therefore, it is a [filtering gateway](#) that comprises at least the following network interfaces:

- an interface for the network being protected (internal network)
- an interface for the external network



The firewall system is a software system, often supported by dedicated network hardware, forming an intermediary between the [local network](#) (or the local computer) and one or more external networks. A firewall system can be set up on any computer that uses any system as long as:

- The machine is powerful enough to process the traffic
- The system is secure
- No other service other than the packet filtering service is running on the server

In the case that a firewall system is provided in a black box, the term "appliance" applies.

### How a Firewall System Works

---

A firewall system contains a set of predefined rules that allow the system to:

- Authorise the connection (*allow*)

- Block the connection (*deny*)
- Reject the connection request without informing the issuer (*drop*)

All of these rules implement a filtering method that depends on the **security policy** that was adopted by the organisation. Security policies are usually broken down into two types that allow:

- the authorisation of only those communications that were explicitly authorised:
- "Everything that is not explicitly authorised is prohibited"
- the refusal of exchanges that were explicitly prohibited

The first method is without a doubt the safest. However, it imposes a precise and restrictive definition of communication needs.

### Stateless Packet Filtering

A firewall system operates on the principle of simple packet filtering, or *stateless packet filtering*. It analyses the header of each **data packet** (*datagram*) exchanged between an internal network computer and an external computer.

Thus, the data packets exchanged between an external network computer and an internal network computer pass through the firewall and contain the following headers, which are systematically analysed by the firewall:

- The IP address of the computer sending the packets
- The IP address of the computer receiving the packets
- The type of packet (**TCP**, **UDP**, etc.)
- The **port** number (reminder: a port is a number associated with a service or a network application).

The IP addresses contained in the packets allow you to identify the computer that is sending the packets and the target computer, while the type of packet and the port number indicate the type of service being used.

The table below gives examples of firewall rules:

Rule	Action	Source IP	Target IP	Protocol	Source Port	Target Port
1	Accept	192.168.10.20	194.154.192.3	tcp	any	25
2	Accept	any	192.168.10.3	tcp	any	80
3	Accept	192.168.10.0/24	any	tcp	any	80
4	Deny	any	any	any	any	any

**Recognised ports** (whose numbers are between 0 and 1023) are associated with ordinary services (e.g. ports 25 and 110 are associated with e-mail and port 80 with the Web). Most firewall devices are at least configured to filter communications according to the port being used. It is generally recommended to block all ports that are not essential (depending on the security policy in place).

For example, port 23 is often blocked by default by firewall devices because it corresponds to the **TELNET** protocol, which allows a person to emulate terminal access to a remote machine in order to remotely execute commands. The data exchanged over TELNET are not **encrypted**, which means that a hacker is

likely to [listen to the network](#) and steal any unencrypted passwords. Administrators generally prefer the [SSH protocol](#), which has a reputation for being safe and provides the same functionalities as TELNET.

## Dynamic Filtering

---

Stateless Packet Filtering only attempts to examine the IP packets independently, which corresponds to level 3 of the [OSI model](#). But most connections are supported by TCP protocol, which manages sessions, in order to ensure that exchanges take place smoothly. In addition, many services (e.g. FTP) initiate a connection on a static port but dynamically (i.e. randomly) open a port in order to establish a session between the machine acting as a server and the client machine.

Thus, with stateless packet filtering it is impossible to anticipate which ports should be authorised and which should be prohibited. To remedy this situation, the system of **dynamic packet filtering** is based on the inspection of layers 3 and 4 of the OSI model, allowing for full monitoring of the transactions between the client and the server. The term for this is "**stateful inspection**" or "*stateful packet filtering*".

A "stateful inspection" firewall device is able to ensure the monitoring of exchanges, meaning that it takes into account the status of previous packets when defining filtering rules. This way, starting when an authorised machine initiates a connection with a machine located on the other side of the firewall, all of the packets passing over this connection will be implicitly accepted by the firewall.

Even if dynamic filtering is more effective than basic packet filtering, that does not mean that it protects against hackers taking advantage of application vulnerabilities. And yet these vulnerabilities represent the majority of security risks.

## Application Filtering

---

Application filtering allows you to filter communications application by application. Application filtering operates at level 7 (the application layer) of the [OSI model](#), contrary to simple packet filtering (level 4). Application filtering implies knowledge of the [protocols](#) used by each application.

As the name indicates, application filtering allows you to filter communications application by application. Application filtering implies knowledge of the applications on the network and notably of the way in which it structures the exchanged data (ports, etc.).

A firewall performing application filtering is generally called an "[application gateway](#)" (or a "proxy") because it acts as a relay between two networks by intervening and performing a thorough evaluation of the content in the exchanged packets. Therefore, the proxy represents an intermediary between the internal network's computers and the external network, putting the attacks in their place. Moreover, application filtering allows for the headers that proceed application messages to be destroyed, which provides an additional level of security.

This type of firewall is highly effective and ensures good network protection if it is correctly run. On the other hand, detailed analysis of application data requires a lot of computing power, which often means slowed communications because each packet must be thoroughly analysed.

Moreover, the proxy must be able to interpret a wide range of protocols and know the related weaknesses in order to be effective.

Finally, a system like this may potentially have vulnerabilities inasmuch as it interprets requests that pass through its bias. Therefore, the firewall (dynamic or not) should be dissociated from the proxy in order to limit risks of compromising the system.

## The Concept of a Personal Firewall

---

The term **personal firewall** is used to describe the case where the protected area is limited to the computer on which the firewall is installed

A personal firewall allows you to control access to the network of applications installed on the computer and notably to prevent attacks like [Trojan horses](#), i.e. harmful programs that breach the system in order to allow a hacker to remotely take control of the computer. Personal firewalls allow you to repair and prevent breaches by applications that are not authorised to connect to your computer.

## Firewall Limitations

---

Firewall systems obviously do not provide absolute security--on the contrary. Firewalls only offer protection inasmuch as all outgoing communications systematically pass through them and they are correctly configured. Accesses to the external network that circumvent the firewall are also security weaknesses. This is notably the case of connections made from the internal network by way of a [modem](#) or any other means of connection that avoids the firewall.

Similarly, adding external storage media to internal network computers or laptops can greatly harm the overall security policy.

In order to guarantee a maximum level of protection, a firewall should be run on the computer and its activity log should be monitored in order to be able to detect intrusion attempts and anomalies. Moreover, security should be monitored (e.g. by signing up for CERT's security alerts) in order to modify the parameters of the firewall device according to published alerts.

Setting up a firewall must be done in conjunction with a true security policy.