**FIREWALL**

A firewall is a type of network security device that monitors incoming and outgoing network traffic and allows or denies data packets depending on a set of security rules. Its objective is to create a barrier between your internal network and incoming traffic from outside sources (such as the internet) in order to prevent unwanted traffic such as viruses and hackers.

**Based on their method of operation, there are four different types of firewalls.**

* Packet Filtering Firewalls. Packet filtering firewalls are the oldest, most basic type of firewalls. ...
* Circuit-Level Gateways. ...
* Stateful Inspection Firewalls. ...
* Application-Level Gateways (Proxy Firewalls)

**How does a firewall work?**

To prevent attacks, firewalls thoroughly examine incoming traffic based on pre-defined criteria and filter traffic coming from unsecured or suspect sources. Firewalls protect traffic at a computer’s entrance point, known as ports, where data is exchanged with external devices.

**Why Firewall is needed?**

Firewalls are designed to prevent malware and application-layer attacks. Together with an integrated intrusion prevention system (IPS), these Next Generation Firewalls can identify and battle assaults across the entire network in real-time. Firewalls can operate on previously defined policies to better safeguard your network and can do fast assessments to detect and shut down unwanted or suspicious activities, such as malware. When you use a firewall as part of your security infrastructure, you configure your network with precise policies that allow or prohibit incoming and outgoing traffic.

**Types of Firewalls**

Types of firewalls are mainly classified into four types. They are

* Next-Generation Firewalls
* Proxy Firewalls
* Stateful Multilayer Inspection (SMLI) Firewalls
* Network Address Translation (NAT) Firewalls

**Next-generation firewalls (NGFW)** integrate classic firewall technology with new features such as encrypted traffic inspection, intrusion prevention systems, anti-virus, and more. Deep packet inspection is its most remarkable feature (DPI). Deep packet inspection, as opposed to typical firewalls, analyses the data within the packet itself, allowing users to more efficiently identify, categorize, and stop harmful data packets.

**Proxy Firewalls:** At the application level, proxy firewalls filter network traffic. Unlike traditional firewalls, the proxy operates as a middleman between two end systems. The client must send a request to the firewall, which must then analyse it against a set of security rules before allowing or blocking it. Proxy firewalls, in particular, monitor traffic for layer 7 protocols such as HTTP and FTP and detect malicious traffic using both stateful and deep packet inspection.

**Stateful Multilayer Inspection (SMLI) Firewalls:** Firewalls using stateful multilayer inspection (SMLI) filter packets at the network, transport, and application levels by comparing them to known trusted packets. SMLI, like NGFW firewalls, examines the entire packet and only allows it to pass if it passes each tier individually. These firewalls scan packets to determine the status of the communication (thus the name) in order to ensure that all initiated communication occurs only with trustworthy sources.

**Network Address Translation (NAT) Firewalls** enable numerous devices with distinct network addresses to connect to the internet using a single IP address while concealing individual IP addresses. As a result, attackers scanning a network for IP addresses are unable to obtain precise details, increasing protection against attacks. NAT firewalls, like proxy firewalls, serve as an intermediate between a group of computers and outside traffic.

**Proxy and Application Layer Firewalls**: By filtering and inspecting the payload of a packet, proxy firewalls can protect the application layer by distinguishing valid requests from dangerous code masquerading as valid data requests. Proxy firewalls keep application layer attacks on web servers from becoming more frequent. Furthermore, proxy firewalls provide security engineers with greater granular control over network traffic.

Application layer filtering using proxy firewalls, on the other hand, allows us to prevent malware and distinguish misused protocols such as Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), specific programs, and domain name systems (DNS).

**Advantages and Disadvantages of Firewalls**

**Advantages of Firewalls**

Firewalls play a significant role in security management in businesses. The following are some of the most significant benefits of firewalls.

* It improves security and privacy when using susceptible services. It keeps unauthorised users from connecting to a private network that is linked to the internet.
* Firewalls respond faster and can manage higher traffic loads.
* A firewall makes it possible to manage and update security protocols from a single authorised device.
* It protects your network from phishing assaults.

**Disadvantages of Firewalls**

* Firewalls are unable to prevent users from obtaining data or information from rogue websites, exposing them to internal dangers or attacks.
* It cannot guard against the transfer of virus-infected data or software if security rules are incorrectly implemented, nor can it protect against non-technical security concerns (social engineering)
* It does not prevent password misuse or attackers using modems from dialing in or out of the internal network.
* Firewalls do not protect systems that are already compromised.

Link : <https://forumautomation.com/t/what-is-a-firewall/10695>

**Hardware vs software firewall**

**Software vs Hardware Firewalls**

The main difference between a hardware firewall and a software firewall is that **the hardware firewall runs on its own physical device, while a software firewall is installed on another machine**.

## How Does a Hardware Firewall Work?

A [network security solution](https://www.checkpoint.com/solutions/network-security/), a hardware firewall is designed to protect an organization’s network boundary by being deployed in inline mode. This means that the physical network cables over which traffic can cross this boundary are connected to ports on the “inside” and “outside” of the firewall.

When traffic enters a [network firewall](https://www.checkpoint.com/cyber-hub/network-security/what-is-network-firewall/), it is subjected to security inspection and may have multiple different controls applied to it. At a high level, [firewalls](https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/) commonly are configured to block certain types of traffic from crossing the network boundary. This can help to block traffic over any unused or undesirable ports from entering the network and to stop certain types of traffic from leaving the network (such as traffic that could leak sensitive data).

Beyond this, many firewalls also have additional access controls and security inspection capabilities. They may be able to apply signature detection or machine learning to traffic to identify malicious content and to apply access controls for certain resources. All of these filters and protections help to secure the network and the systems connected to it against exploitation.

## Software vs Hardware Firewalls

Hardware firewalls are not the only available firewall option. An organization may choose to deploy a software-based firewall as well.

The main difference between a hardware firewall and a software firewall is that the hardware firewall runs on its own physical device, while a software firewall is installed on another machine. A common example of a software firewall is the firewall built into most operating systems like Windows and macOS. These OS firewalls are bundled with the operating system and can run on any compatible hardware.

However, these OS firewalls are not the only options for software firewalls. Like hardware firewalls, software firewalls are also offered as standalone solutions. An organization can purchase and deploy these firewalls in locations where a hardware firewall may not be a viable option, such as in cloud environments.

**Key Benefits of Hardware Firewalls**

Hardware firewalls, deployed as physical appliances, provide a number of benefits compared to software firewalls, including:

* **Consistent Security:** Software firewalls installed on different computers can all be configured differently. Unless an organization can implement and enforce a consistent security configuration, software firewalls may be disabled or have varying levels of security. A hardware firewall, on the other hand, provides consistent protection to all devices protected by it.
* **Standalone Protection:** A software firewall likely runs on the protected computer. This means that it takes up resources that could otherwise be used for other purposes. A hardware firewall runs on its own hardware, meaning that increases in traffic volume or security requirements do not impact the performance of the protected machines.
* **Simplified Management:** With a software firewall, each computer needs to be individually configured, managed, and updated to provide strong protection against cyber threats. A hardware firewall, on the other hand, is a single appliance that protects the entire network. Any updates or configuration changes that are required can be applied once and will instantly apply to all devices protected by the firewall.
* **Improved Security:** A hardware firewall runs on its own dedicated hardware instead of relying on the resources of the computer where it is installed. This can help to protect it against attacks designed to exploit the underlying operating system or the programs running alongside it.
* **Centralized Visibility:** Running independent software firewalls on each device within an organization’s network means that the security team either lacks complete network visibility or must put in extra effort to aggregate and assimilate information from all of the various devices. A hardware firewall centralizes all network monitoring and logging in a single appliance.

Link: <https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/what-is-a-hardware-firewall/>

Afbeelding met tekst, oranje

Automatisch gegenereerde beschrijving

There are a variety of successful open-source firewalls, like [pfSense software](https://www.sunnyvalley.io/docs/network-security-tutorials/pfsense), OPNSense, [IPFire](https://www.sunnyvalley.io/docs/network-security-tutorials/ipfire-installation), etc. They are quite stable firewall solutions and have a handful of features, commercial-grade performance, timely updates, and great community support.

You may find more information about open-source firewalls in the [Best Open-Source Firewall](https://www.sunnyvalley.io/docs/network-security-tutorials/best-open-source-firewalls) article written by Sunny Valley Networks.

It is achievable to build the best next-generation firewall (NGFW) for home use combining an open-source firewall, a fanless mini PC, and a packet inspection module.

Link : <https://www.sunnyvalley.io/docs/network-security-tutorials/how-to-build-ngfw-for-home>

  
  
Afbeelding met tekst

Automatisch gegenereerde beschrijving

Link : <https://stackoverflow.com/questions/3189138/is-it-possible-to-write-a-firewall-in-python>

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Link: <https://ldx.github.io/python-iptables/index.html>