Info Firewall

# What is a Firewall?

A Firewall is a network security device that **monitors and filters incoming and outgoing network traffic** and decides whether to allow or block specific traffic based on a defined set of security rules. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall’s main purpose is to **allow non-threatening traffic in and to keep dangerous traffic out**.

A firewall can be hardware, software, software-as-a service (SaaS), public cloud, or private cloud (virtual).

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

https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

# How Do Firewalls Operate and Why Are They Important?

A firewall is important because it acts as the network’s first line of defence. An effective firewall can identify and block a wide variety of threats, preventing them from reaching the internal network. This decreases the amount of malicious traffic that other security solutions must inspect, and the potential threats faced by the internal network.

A simple way to explain how a firewall works is to think of it as a security guard with intimate knowledge of millions of potential criminals. If the guard sees one, he or she keeps the criminal out of the building. Similarly, a firewall’s protection comes from monitoring and regulating traffic that goes in and out of your network. This is accomplished using a few different methods, including packet filtering, a proxy service, and stateful inspection.

## Different types

**Packet Filtering**

Data is organized in packets. When a firewall executes packet filtering, it examines the packets of data, comparing it against filters, which consist of information used to identify malicious data. If a data packet meets the parameters of a threat as defined by a filter, then it is discarded and your network is protected. Data packets that are deemed safe are allowed to pass through

**Stateful vs. Stateless**

A stateless firewall inspects traffic on a packet-by-packet basis. The earliest firewalls were limited to checking source and destination IP addresses and ports and other header information to determine if a particular packet met simple access control list requirements. This enabled firewalls to block certain types of traffic from crossing the network boundary, limiting their exploitability and ability to leak sensitive data.

Stateful firewalls are designed to track details of a session from its beginning to its end. This enabled these firewalls to identify and block packets that don’t make sense in context (such as a SYN/ACK packet sent without a corresponding SYN). The greater functionality provided by stateful firewalls means that they have completely replaced stateless ones in common usage.

**Proxy firewall**

An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.

**Unified threat management (UTM) firewall**

A UTM device typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention and antivirus. It may also include additional services and often cloud management. UTMs focus on simplicity and ease of use.

**Next Generation Firewall**

Firewalls have evolved beyond simple packet filtering and stateful inspection. Most companies are deploying next-generation firewalls to block modern threats such as advanced malware and application-layer attacks.

According to Gartner, Inc.’s definition, a next-generation firewall must include:

* Intelligence-based access control with stateful inspection
* Integrated intrusion prevention system (IPS)
* Application awareness and control to see and block risky apps
* Upgrade paths to include future information feeds
* Techniques to address evolving security threats
* URL filtering based on geolocation and reputation

While these capabilities are increasingly becoming the standard for most companies, NGFWs can do more.

Threat-focused NGFW

These firewalls include all the capabilities of a traditional NGFW and also provide advanced threat detection and remediation. With a threat-focused NGFW you can:

* Know which assets are most at risk with complete context awareness
* Quickly react to attacks with intelligent security automation that sets policies and hardens your defenses dynamically
* Better detect evasive or suspicious activity with network and endpoint event correlation
* Greatly decrease the time from detection to cleanup with retrospective security that continuously monitors for suspicious activity and behavior even after initial inspection
* Ease administration and reduce complexity with unified policies that protect across the entire attack continuum

Another way to distinguish between different types of firewalls is based on how they are implemented. Firewalls generally fall into three categories:

**#1. Hardware Firewalls**: These firewalls are implemented as a physical appliance deployed in an organization’s server room or data center. While these firewalls have the advantage of running as “bare metal” and on hardware designed specifically for them, they are also constrained by the limitations of their hardware (number of network interface cards (NICs), bandwidth limitations, etc.).

3 Key Benefits of Hardware Firewall

1. Can be used to intelligently control the traffic that reaches your server
2. Can be configured with specific rules for all traffic
3. Can ease the burden on other server resources. For example, you can disable software firewalls, which can free up much-needed memory and processor power

**#2. Software Firewalls**: Software firewalls are implemented as code on a computer. These firewalls include both the firewalls built into common operating systems and virtual appliances that contain the full functionality of a hardware firewall but are implemented as a virtual machine.

**#3. Cloud Firewalls:** Organizations are increasingly moving critical data and resources to the cloud, and cloud-native firewalls are designed to follow suit. These virtual appliances are specifically designed to be deployed in the cloud and may be available as either standalone virtual machines or as a Software as a Service (SaaS) offering.

## What Is a Hybrid Firewall?

Hybrid firewalls consist of multiple firewalls, each providing a specified set of functions. For instance, you can use one firewall to execute packet filtering while another firewall acts as a proxy. In this way, you can tweak the performance of your security system, taking advantage of the diverse range of capabilities the different firewalls offer.

**How does a hybrid firewall work?**

As a hybrid firewall example, you can set up two firewalls that work in tandem, one of which is your proxy firewall and the other filters data packets. The firewall acting as your proxy server processes web requests while the packet filtering firewall ensures that all data coming into and exiting your network security system is safe. In this way, the two firewalls act as a single hybrid system, protecting your organization in two different ways.

Another benefit of a hybrid firewall architecture is you can add a new firewall to an existing security system without having to remove or replace your current firewall. This hybrid firewall application enables you to add another layer of security without compromising the benefits of your existing architecture. The ability to add firewall infrastructure to an existing system can allow you to set up a distributed firewall, which enables you to establish security rules that control access between two separate networks.

<https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/the-different-types-of-firewalls/>

<https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html#~types-of-firewalls>

<https://www.fortinet.com/resources/cyberglossary/how-does-a-firewall-work>

<https://www.fortinet.com/resources/cyberglossary/hybrid-firewall-advantages-disadvantages>

# How Does a Firewall Protect Data?

Firewall filters keep harmful data outside your computer. Some of the top risks from which firewalls protect your computer include backdoors, denial-of-service (DoS) attacks, macros, remote logins, spam, and viruses.

Backdoors are “doorways” to applications with vulnerabilities that attackers exploit to get inside. This includes operating systems that may have bugs that hackers can use to gain access to your computer.

DoS attacks are executed when a hacker requests permission to connect to a server, and when the server responds, it cannot find the system that made the request. When this is done again and again, the server gets flooded and has to expend so much power to deal with the mass of requests, rendering it unable to meet the needs of legitimate visitors. In some cases, the server has to come offline completely. There are some firewalls that can check whether the connection requests are legitimate, and thus, protect your network from DoS attacks.

Macros refer to scripts run by applications to automate processes. A macro can contain a series of dependent steps that are all launched by one command. Hackers design or purchase macros intended to work within certain applications. A macro can be hidden inside seemingly innocent data, and once it enters your computer, it wreaks havoc on your system. A firewall can detect malicious macros as it examines the packets of data that attempt to pass through.

Remote logins are often used to help someone with a computer issue. However, in the hands of the wrong person, they can be abused, particularly because remote logins provide nearly complete access to your system.

Spam can sometimes include links to malicious websites. These types of sites activate malicious code that forces cookies onto a computer. The cookies create backdoors for hackers to gain access to the computer. Preventing a spam attack is often as simple as not clicking on anything suspicious in an email, regardless of who the sender appears to be. A firewall can inspect your emails and prevent your computer from getting infected.

Viruses, once on a computer, copy themselves and spread to another device on the network. Viruses can be used to do a variety of things, ranging from relatively harmless activity to erasing data on your computer. Firewalls can inspect data packets for viruses, but it is better to use antivirus software in conjunction with a firewall to maximize your security.