Firewall

What is a Firewall? A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization’s previously established security policies. 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.

There are two types of firewall, these two include:

**Hardware Firewalls**

A hardware firewall (or an **appliance firewall**) is a separate piece of [hardware](https://phoenixnap.com/glossary/what-is-hardware) that filters traffic entering and coming out of a network. Unlike a software firewall, these self-contained devices have their own resources and do not consume any CPU or RAM from host devices.

For some SMBs, a hardware firewall is a bit of an overkill, and they might find more value in per-host software firewalls. Hardware firewalls are an excellent choice for larger organizations with several subnetworks containing multiple computers.

**Pros of hardware firewalls:**

* Protect multiple devices with one solution.
* Top-tier perimeter security as malicious traffic never reaches host devices.
* Do not consume resources of host devices.
* An admin manage only one firewall for the entire network.

**Cons of hardware firewalls:**

* More expensive than software firewalls.
* Insider threats are a considerable weakness.
* Configuration and management require more skill than software-based firewalls.

**Software Firewalls**

A software firewall (or a **host firewall**) installs directly on the host device. This type of firewall protects only one machine (network endpoint, PC, laptop, server, etc.), so admins must install a version of the software on each device they want to protect.

Since admins attach a software firewall to a specific device, there's no avoiding some resource usage. These firewalls inevitably eat up some system RAM and CPU, which is a deal-breaker for some use cases.

**Pros of software firewalls:**

* Excellent protection for their assigned device.
* Isolate individual network endpoints from one another.
* Highly granular security in which an admin has complete control over allowed programs.
* Readily available.

**Cons of software firewalls:**

* Consume the device's CPU, RAM, and [storage](https://phoenixnap.com/blog/object-storage-vs-block-storage).
* Require configuration for each host device.
* Day-to-day maintenance is difficult and time-consuming.
* Not all devices are compatible with every firewall, so you may have to use different solutions within the same network.

Firewalls are used in different cases such as:

* **Threat defense.** Firewalls can be installed at an organization's network perimeter to guard against external threats, such as malware attacks or hacking attempts, or within the network to create segmentation and [guard against insider threats](https://www.techtarget.com/searchsecurity/tip/Five-common-insider-threats-and-how-to-mitigate-them).
* **Logging and audit functions.** Firewalls keep a record of events that administrators can use to identify patterns and improve rule sets. Rules should be updated regularly to keep up with ever-evolving cybersecurity threats. Vendors discover new threats and develop patches to cover them as soon as possible.
* **Traffic filtering.** In a single home network, a firewall can filter traffic and alert the user to intrusions. They're especially useful for always-on connections, such as Digital Subscriber Line or cable modems, because those connection types use static IP addresses. A firewall ensures that only intended and nondestructive content from the internet passes through.
* **Controlling and blocking access.** Firewalls can be used for controlling and blocking access to certain websites and online services to prevent unauthorized use. For example, an organization can use a firewall to block access to objectionable websites to ensure employees comply with company policies when browsing the internet.
* **Secure remote access.** Firewalls can be used to grant secure remote access to a network through a virtual private network ([VPN](https://www.techtarget.com/searchnetworking/definition/virtual-private-network)) or other secure remote access technology.

**List of Best Practices Firewalls can be used for:**

**1. Block traffic by default and monitor user access**

It is advisable to block all traffic to the network by default. Allow only some specific traffic to certain known services. This helps you to have control over who can access your network and prevents any security breaches from occurring.

The firewall being your first layer of protection against threats, must not allow access to anyone and everyone to alter the configuration. User permission control is necessary to ensure that only authorized administrators have access to change firewall configurations. Apart from this, every time an authorized administrator does change any configuration, it must be recorded in the log for audits and compliance. Any unwarranted configuration changes can thus be detected, and configuration restore may be implemented in such a case.

You can also create separate user profiles to provide various levels of access to the IT staff, only as much as needed for a job. Firewall logs must be monitored regularly to detect any unauthorized break-ins to the firewall, from inside or outside the network.

**2. Establish a firewall configuration change plan**

Your network’s firewall will need to be updated from time to time for various reasons. This is necessary to ensure that the firewall remains strong and capable of protecting against new threats. But it is important to have a change management plan so that the process is smooth and secure. Any unplanned configuration change leaves a loophole in your network’s security.

A well-defined and robust firewall change management plan must include certain basic features:

* It must define the changes that are required and their objectives.
* It should also enlist the risks involved due to the policy changes, their impacts on the network, and a mitigation plan to minimize the risks.
* A well-defined structure of change management workflow between various network teams.
* Proper audit trails that record who made the change, why, and when.

**3. Optimize the firewall rules of your network**

The firewall rules must be well-defined and optimized to provide the expected protection. Cleaning up your firewall rule base of any kind of unnecessary clutter can have a positive impact on your network security.

Your firewall rule base may have certain redundant elements, duplicates, or bloated unnecessary rules that make the guidelines complicated and less effective. It is important to get rid of such rules to have a clear set of guidelines that can be followed better.

To clean your firewall rule base, you must:

* Eliminate redundant or duplicate rules that slow down the firewall performance as they require the firewall to process more rules in its sequence than necessary.
* Remove the rules that are obsolete or no longer in use. These only make the firewall [management](https://backbox.com/harnessing-the-power-of-machine-learning-in-inventory-management/) more complex, and can even be a threat to network security if not updated.
* Remove shadowed rules that are not essential. These may lead to more critical rules being neglected.
* Conflicting rules must be eliminated.
* Any errors or inaccuracies in the rules must be eliminated as these may result in malfunctions.

**4. Update your firewall software regularly**

Firewall vendors usually release software updates regularly. These updates address any new potential security threats by making minor changes to the software. It is important to keep updating your firewall software to ensure that your network is secure, and there are no loopholes in the system that could pose a threat to security. You must check from time to time if your firewall software is updated to the latest version.

**5. Conduct regular firewall security audits**

Security audits are necessary to ensure that the firewall rules comply with the organizational, as well as external security regulations that apply to the [network](https://backbox.com/automated-network-documentation/). Unauthorized firewall configuration changes that are a policy violation can cause non-compliance. It is important for administrators and IT security staff to carry out regular security audits to ensure no unauthorized changes have taken place.

This will also keep you updated on the necessary changes made to the firewall and warn you against any potential risks created by these changes. Security audits are most essential when there is a new firewall installed, firewall migration activity happening, or when there are bulk configuration changes made on firewalls.

**6. Have a centralized management tool for multi-vendor firewalls**

Multi-vendor firewalls are quite common in most organizations. Companies prefer firewalls manufactured by different companies installed in the systems to offer additional layers of security. But the challenge here is that the architecture of firewalls from different manufacturers is usually different.

It is important to manage all your firewalls centrally at one place to ensure they are all functioning properly. Using a multi-vendor firewall management tool allows you to have a unified view of firewall policies and rules, enabling you to compare and manage firewall rules easily. You can also perform security auditing and reporting, troubleshoot configuration issues, and provide support with a gap analysis for firewall migration through this centralized management tool.

**7. Automate the process of firewall updating**

With improvements in technology, many processes have become faster and easier. It may not always be possible for firewall administrators to constantly check for updates and perform software updates regularly. This leaves the network at risk of security breaches.

To avoid any lapse in updating your firewall, you can automate the process instead. An automated system can be scheduled to check for available updates and implement the updates when they find one. This reduces the need for human intervention and keeps the firewall secure and robust at all times.

How to also secure a firewall

1. Limit VPN Access[​](https://www.sunnyvalley.io/docs/network-security-tutorials/how-to-improve-your-firewall-security#1-limit-vpn-access)

If you have a sophisticated VPN system, you can make a [firewall](https://www.sunnyvalley.io/docs/network-security-tutorials/what-is-firewall) far more secure. A secure [VPN](https://www.sunnyvalley.io/docs/network-security-tutorials/what-is-vpn), which stands for Virtual Private Network, allows you to choose which parts of your server various users see. You may reduce the danger of a [data breach](https://www.sunnyvalley.io/docs/network-security-tutorials/what-is-data-breach) by restricting VPN access to only the areas of your site that they need to work on, especially if they are accessing your server remotely.

2. Monitor User Access[​](https://www.sunnyvalley.io/docs/network-security-tutorials/how-to-improve-your-firewall-security#2-monitor-user-access)

By default, it's a good idea to block all network traffic. Allow just specified types of traffic to recognized services. This gives you more control over who may access your network and helps you avoid security breaches.

Because the firewall is your first line of defense against attacks, anybody and everyone should not be able to change the settings. To guarantee that only authorized administrators have access to update firewall configurations, user permission control is required. Aside from that, all configuration changes made by an authorized administrator must be documented in the log for [auditing](https://www.sunnyvalley.io/docs/network-security-tutorials/what-is-firewall-auditing) and compliance purposes. Any unintentional configuration changes may therefore be recognized, and configuration restoration can be carried out if necessary.

You may also establish additional user accounts to provide IT workers different levels of access, only as much as they need for their jobs. Firewall logs must be checked on a regular basis to detect any illegal firewall intrusions from within or outside the network.

3. Shut Off Unused Network Services[​](https://www.sunnyvalley.io/docs/network-security-tutorials/how-to-improve-your-firewall-security#3-shut-off-unused-network-services)

A big business network may have four or five servers actively engaged in e-mail delivery, but a typical corporate network may also have 95 servers listening on the SMTP port. Determine which of the 95 hosts is most likely to have hidden mail server vulnerabilities. Examine the network for services that aren't supposed to be functioning. Turn off file-sharing protocols if a machine is serving as a Windows file server but has never been utilized as a file server.

4. Update Firewall Software[​](https://www.sunnyvalley.io/docs/network-security-tutorials/how-to-improve-your-firewall-security#4-update-firewall-software)

Software updates from firewall suppliers are frequently released on a regular basis. By making tiny modifications to the program, these upgrades address any new possible security issues. It is critical to maintaining your firewall software up to date in order to guarantee that your network is safe and that there are no security flaws in the system. You should check to see if your firewall software is up to date on a regular basis.

5. Automate the process of firewall updating[​](https://www.sunnyvalley.io/docs/network-security-tutorials/how-to-improve-your-firewall-security#5-automate-the-process-of-firewall-updating)

Many procedures have grown faster and easier as technology has advanced. Firewall administrators may not always be able to check for updates and conduct software updates on a regular basis. As a result, the network is vulnerable to security breaches. Instead of manually upgrading your firewall, you may automate the procedure. An automatic system may be set up to look for available updates and install them if one is found. This eliminates the need for human intervention and ensures that the firewall is always safe and reliable.

6. Buy New Security Hardware[​](https://www.sunnyvalley.io/docs/network-security-tutorials/how-to-improve-your-firewall-security#6-buy-new-security-hardware)

If your firewall isn't up to snuff, there's no harm in upgrading to a newer and better type. If you start to notice insufficient hardware resource difficulties on your firewall, such as high CPU or memory utilization or poor throughput values, it could be an indication that your firewall is nearing the end of its life and you need to replace it right away before a calamity occurs.

7. Secure Wireless Access[​](https://www.sunnyvalley.io/docs/network-security-tutorials/how-to-improve-your-firewall-security#7-secure-wireless-access)

Examine your network for wireless issues. Rogue wireless access points must be eliminated. Recognize that secure wireless network access is a truly interesting and valuable feature, and provide it. Allow users to VPN through an access point placed beyond your perimeter firewalls. If your network already has wireless connectivity, users are significantly less likely to go out of their way to create rogue [wireless access points](https://www.sunnyvalley.io/docs/network-basics/what-is-wireless-access-point).