Workplace Firewalls

Emily Parra

University of Advancing Technology

## What is a firewall?

As defined by Cisco, “a firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules” (Cisco, n.d.). Additionally, there are several types of firewalls to choose from, so companies can find the best firewall for their workplace needs. The different types of firewalls are as follows (they can be hardware, software, cloud-based, or virtual): proxy, stateful inspection, unified threat management (UTM), next generation (NGFW), threat focused NGFW, virtual, and cloud native (Cisco, n.d.). Virtual and cloud native firewalls operate in cloud-based environments, so those firewalls are best suited for cloud-based companies, while the other options are best suited for physical environments. Firewalls have their own level of security measures as well, like threat focused NGFW and next-gen NGFW, which deploy strong threat measures (IPS systems and advanced threat detection, etc.) (Cisco, n.d.). Those types of firewalls are suitable for security-conscious companies as well as companies that handle sensitive data like banks and hospitals. Regardless, it all boils down to the needs of the company and what they feel is the best option for their network.

### **Purpose of a firewall**

As mentioned above, firewalls all serve different purposes, whether they are intended for cloud environments or high-security networks. Regardless of the type of firewall used, its core functions remain the same, monitor network traffic and allow or block it depending on the rules (see important workplace firewall settings). Without a firewall, network traffic would go unmonitored and put the company at risk for attacks and unwanted network activity, like malware or an unauthorized user fishing around the network. Think of a firewall as a castle wall with several guarded checkpoints (ports) in it. The guards at these checkpoints (firewall rules) monitor incoming and outgoing citizens for suspicious activity. When spotted, the suspicious person (activity that is blocked by security rules) gets stopped from entering the castle (blocked by firewall rules).

#### Why are firewalls important?

Firewalls are important because they add an extra layer of security to a company’s network and prevent attacks from taking place. Using the same castle wall analogy, if a castle didn’t have a wall or guards to protect its checkpoints, almost anyone could get in without being detected. They could steal, attack, or even spy on the castle. The same goes for companies and their networks. It is especially important for a highly sensitive company, like a bank or hospital, to have a heavily guarded firewall because of the nature of the data they handle. However, it is important overall, regardless of the data a company handles, for a company to employ some sort of firewall and customize it to suit their security needs.

##### **Important workplace firewall settings**

Firewall settings are specific rules put in place by a company’s network security team to ensure the protection of incoming and outgoing data via the firewall. As stated above, in addition to monitoring incoming and outgoing traffic, some firewalls can be set to employ the use of an IPS and advanced threat detection system along with other features. Here are some of the additional features that every company should include in their firewall (Stanfield, 2019):

* Bandwidth control and monitoring
	+ Disperses bandwidth on a network to ensure efficiency, productivity, and security. For example, giving backups or security updates more bandwidth during off hours so they can finish faster and ensure complete protection of the network.
* Web filtering
	+ Filters certain web traffic from being used by employees, like unsecured websites, pornography, and illegal content. This protects the network from being compromised by web activity that may be malicious.
* Logging
	+ This feature is like the firewall writing down everything that happens on the network with extreme accuracy. It helps the security team determine factors like malicious activity on the network, repeated unsuccessful login attempts, and more.
* Internet aggregation and SD WAN
	+ Both features allow the company to branch off and connect with external links via the use of broadband and other transport services. These are important feature for companies with other offices and/or external cloud servers because it allows them to connect securely.
* Sandboxing
	+ Takes downloaded files and opening them in a quarantined environment before letting them be downloaded. Sandboxing is extremely important because it quickly protects the network from malicious files, malware, and other downloadable attacks by scanning files for suspicious activity.
* Deep Packet Inspection (DPI)
	+ Examines the contents of packets for suspicious activity (like hidden viruses) by operating on a set of rules assigned by the organization, afterwards passing it off to the firewall to decide whether to allow or block the traffic. This process protects the network by inspecting the contents of packets and blocking the suspicious ones.
* Virtual Private Networks
	+ Allows remote users to securely access a site or office by encrypting their traffic. VPNs are especially important when accessing sensitive data off-site, like a database containing PII. The only way VPNs can truly keep a network safe is if both the user and area the user is connecting to are secured.
* Malware and virus filtering
	+ Scans the network (even SSL/TLS connections) for all types of malware and viruses, excluding zero-day attacks. Malware and virus filtering keep the network secured by autonomously looking out for attacks and flagging suspicious activity.
* Intrusion Prevention System (IPS)
	+ Monitors the network, notes information about possible attacks, and alerts the security team upon finding suspicious information. Although not completely autonomous, IPS still protects the network by consistently scanning it.
* Identity management integration and Single Sign On (SSO)
	+ SSO authenticates the user securely through a single log-on by validating them through a 3rd party and ensuring the absence of security breaches. This is an important security feature because of its authentication technique that validates the user and ensures that an attacker is not posing as them.

A firewall is a customizable device that protects a company’s network by scanning incoming and outgoing traffic for suspicious activity. Their purpose is to secure a company’s network from outside attacks, basically acting as a castle wall in front of a castle. Based on the firewall rules set by a company, a firewall can do a variety of things like autonomously scan for threats, log traffic, and even deep scan packet data. They also come in many forms, like cloud-based, physical, or virtual to adapt to the needs of any company. Without a firewall, a company has little to no protection from threats like malware, viruses, or malicious spying on their network. Overall, firewalls are extremely important and should be utilized by every company, regardless of their size or purpose.

References

Cisco. (n.d.). *What is a firewall?* <https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html>

Fortinet. (n.d.). *Firewall benefits: The importance of firewall security*. <https://www.fortinet.com/resources/cyberglossary/benefits-of-firewall>

Johansen, A. (2021, June 17). *What is a firewall? Firewalls explained and why you need one*. Norton. <https://us.norton.com/blog/emerging-threats/what-is-firewall>

Stanfield, N. (2019, December 4). *11 firewall features you can't live without*. Stanfield IT. <https://www.stanfieldit.com/11-firewall-features/>