What is a firewall?

A firewall sits between a network and the Internet, controlling the flow of data both in and out of the network in order to stop potential security threats.

Learning Center

- What is Web Application Security?
- Common Threats
- More Attacks
- Glossary

Learning Objectives

After reading this article you will be able to:

- Define a firewall
- Explain why a firewall needs to inspect both inbound and outbound data
- Understand the differences between a proxy firewall and a WAF

RELATED CONTENT

What is Web Application Security?

Zero Trust Security

Phishing Attack

On-Path Attack

Brute Force Attack

Copy article link

What is a firewall?

A firewall is a security system that monitors and controls network traffic based on a set of security rules. Firewalls usually sit between a trusted network and an untrusted network; oftentimes the untrusted network is the Internet. For example, office networks often use a firewall to protect their network from online threats.

Firewalls decide whether to allow incoming and outgoing traffic to pass through. They can be built into hardware, software, or a combination of both. The term ‘firewall’ is actually borrowed from a construction practice of building walls in between or through the middle of buildings designed to contain a fire. Similarly, network firewalls work to contain online threats.

Why use a firewall?

The primary use case for a firewall is security. Firewalls can intercept incoming malicious traffic before it reaches the network, as well as prevent sensitive information from leaving the network.

Firewalls can also be used for content filtering. For example, a school can configure a firewall to prevent users on their network from accessing adult material. Similarly, in some nations the government runs a firewall that can prevent people inside that nation-state from accessing certain parts of the Internet.

This article will focus on firewalls configured for security, of which there are several kinds.

What are the different types of firewall?

Proxy-based firewalls:

These are proxies* that sit in between clients and servers. Clients connect to the firewall, and the firewall inspects the outgoing packets, after which it will create a connection to the intended recipient (the web server). Similarly, when the web server attempts to send a response to the client, the firewall will intercept that request, inspect the packets, and then deliver that response in a separate connection between the firewall and the client. A proxy-based firewall effectively prevents a direct connection between the client and server.

A proxy-based firewall is kind of like a bouncer at a bar. This bouncer stops guests before they enter the bar to make sure they are not underage, armed, or in any other way a threat to the bar and its patrons. The bouncer also stops patrons on their way out to ensure that they have a safe way to get home and are not planning to drink and drive.

The downside of having a bouncer at the bar is that when a lot of people are trying to enter or leave the bar simultaneously, there will be a long line and several people will experience delays. Similarly, a major drawback of a proxy-based firewall is that it can cause latency, particularly during times of heavy traffic.

*A proxy is a computer that acts as a gateway between a local network and a larger network, such as the Internet.

Stateful firewalls:

In computer science, a 'stateful' application is one which saves data from previous events and interactions. A stateful firewall saves information regarding open connections and uses this information to analyze incoming and outgoing traffic, rather than inspecting each packet. Because they do not inspect every packet, stateful firewalls are faster than proxy-based firewalls.

Stateful firewalls rely on a lot of context when making decisions. For example, if the firewall records outgoing packets on one connection requesting a certain kind of response, it will only allow incoming packets on that connection if they provide the requested kind of response.

Stateful firewalls can also protect ports* by keeping them all closed unless incoming packets request access to a specific port. This can mitigate an attack known as port scanning.

A known vulnerability associated with stateful firewalls is that they can be manipulated by tricking a client into requesting a certain kind of information. Once the client requests that response, the attacker can then send malicious packets that match that criteria through the firewall. For example, unsecure websites can use JavaScript code to create these kinds of forged requests from a web browser.

*A network port is a location where information is sent; it's not a physical place but rather a communications endpoint.Learn more about ports >>

Next-Generation Firewalls (NGFW):

These are firewalls that have the capabilities of traditional firewalls but also employ a host of added features to address threats on other layers of the OSI Model. Some NGFW-specific features include:

- **Deep packet inspection (DPI)** - NGFWs perform much more in-depth inspection of packets than traditional firewalls. This deep inspection can look at things like packet payloads and which application is being accessed by the packets. This allows the firewall to enforce more granular filtering rules.

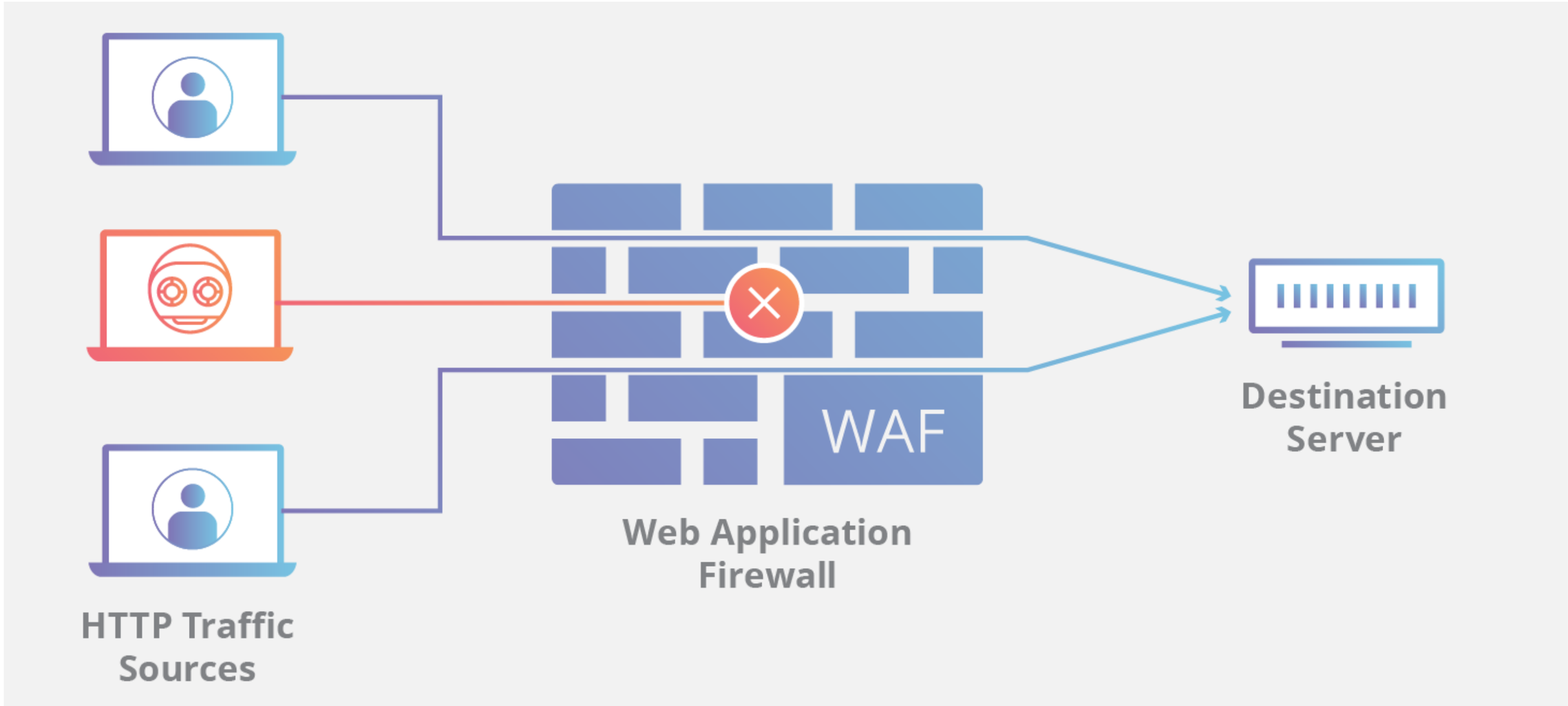
- **Application awareness** - Enabling this feature makes the firewall aware of which applications are running and which ports those applications are using. This can protect against certain types of malware that aim to terminate a running process and then take over its port.

- **Identity awareness** - This lets a firewall enforce rules based on identity, such as which computer is being used, which user is logged in, etc.

- **Sandboxing** - Firewalls can isolate pieces of code associated with incoming packets and execute them in a 'sandbox' environment to ensure they are not behaving maliciously. The results of this sandbox test can then be used as criteria when deciding whether or not to let the packets enter the network.

Web Application Firewalls (WAF):

While traditional firewalls help protect private networks from malicious web applications, WAFs help protect web applications from malicious users. A WAF helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It typically protects web applications from attacks like cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others.



By deploying a WAF in front of a web application, a shield is placed between the web application and the Internet. While a proxy-based firewall protects a client machine's identity by using an intermediary, a WAF is a type of reverse-proxy, protecting the server from exposure by having clients pass through the WAF before reaching the server.

A WAF operates through a set of rules often called policies. These policies aim to protect against vulnerabilities in the application by filtering out malicious traffic. The value of a WAF comes in part from the speed and ease with which policy modification can be implemented, allowing for faster response to varying attack vectors; during a DDoS attack, rate limiting can be quickly implemented by modifying WAF policies. Commercial WAF products like Cloudflare's Web Application Firewall protect millions of web applications from attacks every day.