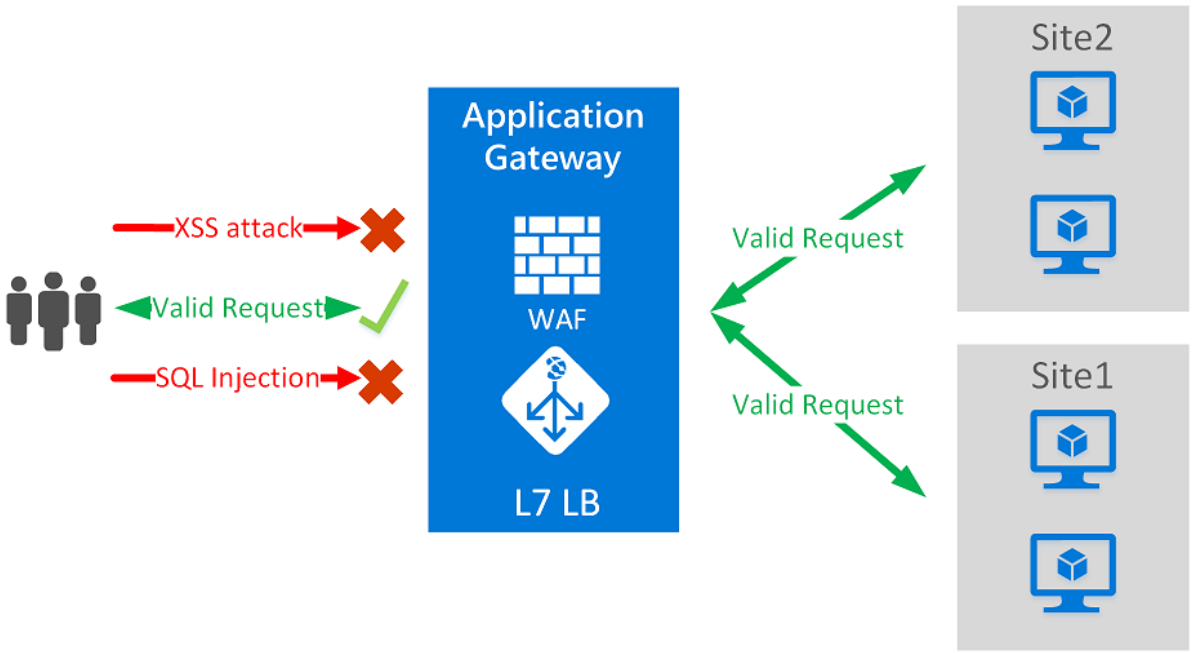
Web Application Firewall:

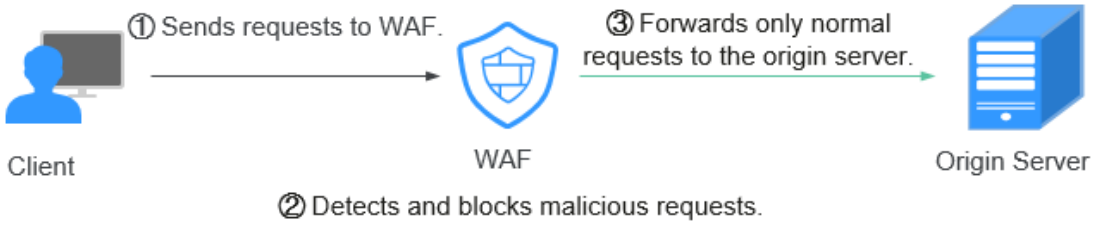
WAF is an abbreviation for Web Application Firewall. A Web Application Firewall (WAF) is a network security firewall solution that protects web applications from HTTP and web application-based security vulnerabilities.
A traditional firewall is limited to functions such as packet filtering, network- and port-address translations (NAT) and VPN's. It makes its decisions based on ports, protocols and IP addresses. Nowadays it's no longer practical nor reliable to implement security policies in such an inflexible and non-transparent way.

NGFWs provide this approach by adding more context to security policies. Context-based systems are designed to use information like location, identity, time, etc… in an intelligent way with the purpose of making more effective security decisions. Next Generation Firewalls also distinguish themselves from traditional firewalls by adding features such as URL filtering, anti-virus/anti-malware, Intrusion Prevention Systems (IPS) and more. Instead of using several different point solutions, a NGFW greatly simplifies and improves the effectiveness of implementing security policies in an increasingly complex computing world.

A WAF specifically targets application traffic. It protects HTTP and Hypertext Transfer Protocol Secure (HTTPS) traffic and applications in internet-facing zones of the network. This secures businesses against threats like cross-site scripting (XSS) attacks, distributed denial-of-service (DDoS) attacks, and SQL injection attacks. WAFs protect attacks at OSI model Layer 7, which is the application level. This includes attacks against applications like Ajax, ActiveX, and JavaScript, as well as cookie manipulation, SQL injection, and URL attacks. They also target web application protocols HTTP and HTTPS, which are used to connect web browsers and web servers.
WAFs can follow either a positive security model, a negative security model, or a combination of both. A positive security model WAF (also known as "whitelist") rejects everything not named as allowed. A negative security model (also known as "denylist") has a list of banned items and allows everything not on that list.

Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.
WAF devices are widely used to protect websites, E-commerce, mobile apps and other online applications. A WAF is deployed between application servers and network edge routers and firewalls. A WAF filters, monitors, and blocks HTTP/HTTPS traffic to and from a web application to protect against attack to compromise the system data.





The main difference between a firewall and a web application firewall (WAF) definition is that a firewall usually protects network and transport layers (layers 3 and 4). A WAF offers protection on the application layer (layer 7).

https://owasp.org/www-project-top-ten/

https://owasp.org/www-project-top-ten/2017/Top_10.html