AWS WAF

Short for **Web Application Firewall**, AWS WAF helps protect web applications against malicious actors by providing us with a firewall that filters and monitors HTTP requests, allowing us to block **SQL injection**, **cross-site scripting (XSS)**, and other common web exploits. It can also be used to restrict access to our website by IP addresses, geographic locations, or other criteria, making it an essential layer of defense for our web resources.

Note that AWS WAF operates on the application layer of the OSI model, and is a different service from AWS Network Firewall (discussed in a later section) which operates primarily on the network layer (consult the Background on Networking if a refresher on the OSI layer model is needed).

Additionally, AWS WAF also has an easy-to-configure feature called **rate-based limiting**, which detects source IP addresses that make large numbers of HTTP requests within a 5-minute time span and automatically blocks requests from the offending source IP until the rate of requests falls below a set threshold. This can help us mitigate against DDoS style attacks on the application layer, an area not covered by services like AWS Shield, which focus primarily on network and transportation layer protection.

Now, AWS WAF is an account-specific service and is limited to being managed by a single account though some of the service's shortcomings can be circumvented using **AWS Firewall Manager**, a service which allows us to manage firewalls across multiple AWS accounts, allowing us to create and enforce WAF policies across a multi-account AWS environment.