**Web Application Firewall and Shield**

* WAF and Shield help protect your AWS resources from web exploits and DDoS attacks
* WAF is a web application firewall service that helps protect your web apps from common exploits that could affect app availability, compromise security or consume excessive resources
* Shield provides expanded DDoS attach protection for your AWS resources. Get 24/7 support from our DDoS response team and detailed visibility into DDoS events
* We’ll now go into more detail on each service
* **WAF**
  + WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources
  + WAF helps protect web applications from attacks by allowing you to configure rules that allow, block or monitor web requests based on conditions that you define
  + These conditions include IP addresses, HTTP headers, HTTP body, URI strings, SQL injection and cross-site scripting
  + AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules
  + New rules can be deployed within minutes, letting you respond quickly to changing traffic patterns
  + When AWS services receive requests for web sites, the requests are forwraded to AWS SAF for inspection against defined rules
  + Once a request meets a condition defined in the rules, WAF instructs the underlying service to either block or allow the request based on the action you define
  + With WAF you pay only for what you use
  + WAF pricing is based on how many rules you deploy and how many web requests your web application receives
  + There are no upfront commitments
  + WAF is tightly integrated with CF and ALB
  + When you use WAF on CF, rules run in all Edge locations, located around the world close to end users
  + This means security doesn’t come at the expense of performance
  + Blocked requests are stopped before they reach your web servers
  + When you use a WAF on an ALB, your rules run in region and can be used to protect internet facing as well as international load balancers
* **Web Traffic Filtering**
  + AWS WAF lets you create rules to filter web traffic based on conditions that include IP addresses, HTTP headers and body or custom URLs
  + This gives you an additional layer of protection from web attacks that attempt to exploit vulnerabilities in custom or thrid party web applications
  + In addition, WAF makes it easy to create rules that block common web exploits like SQL injection and cross site scripting
  + WAF allows you to create a centralized set of rules that you can deploy across multiple websites
  + This means that in an environment with many websites and web applications you can create a single set of rules that you can reuse across applications rather than recreating that rule on every application you want to protect
* **Full feature API**
  + AWS WAF can be completely administered via APIs
  + This provides organizations with the ability to create and maintain rules automaticalyl and incorporate them into the development and design process
  + For example, a developer who has detailed knowledge of the web application could create a security rule as part of the deployment process
  + This capability to incorporate security into your development process avoids the need for complex handoffs between application and security teams to make sure rules are kept up to date
  + AWS WAF can also be deployed and provisioined automatically with CF sample templates that allow you to describe all seciruty rules you would like to deploy for your web applications delivered by CF
  + WAF is integrated with CF, which supports custom origins outside of AWS – this means you can protect web sites not hosted in AWS
  + Support for IPv6 allows the WAF to inspect HTTP/S requests coming from both IPv6 and IPv4 addresses
* **Real-time visibility**
  + WAF provides real-time metrics and captures raw requests that include details about IP addresses, geo locations, URIs, User-Agent and referers
  + WAF is fully integrated with CW making it easy to setup custom alarms when thresholds are exceeded or particular attacks occur
  + This information provides valuable intelligence that can be used to create new rules to better protect applications
* **Shield**
  + Shield is a managed Distributed Denial of Service(DDoS) protection service that safeguards applications running on AWS
  + AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency
  + There are two ties, Standard and Advanced
    - **Shield Standard**
      * All AWS customers benefit from the automatic protections of Shield Standard at no additional charge
      * Shield Standard defends against most common, frequently occuring network and transport layer DDoS attacks that target web sites or applications
      * Whn using Shield Standard with CF and R53 you receive comprehensive availability protection agains all known infrastructure(Layer 3 and 4) attacks
    - **Shield Advanced**
      * Provides higher levels of protection against attacks targeting applications running on EC2, ELB, CF, Global Accelerator and R 53
      * In addition to the network and transport layer protections that come with Standard, Shield Advanced provides additional detection and mitigation against large and sophisticated DDoS attacks, near real-time visibility into attacks, and integration with WAF, a web application firewall
      * **Shield Advanced also gives you access to 24x7 DDoS Response Team** and protection against DDoS related spikes
      * Origin servers can be S3, EC2, ELB