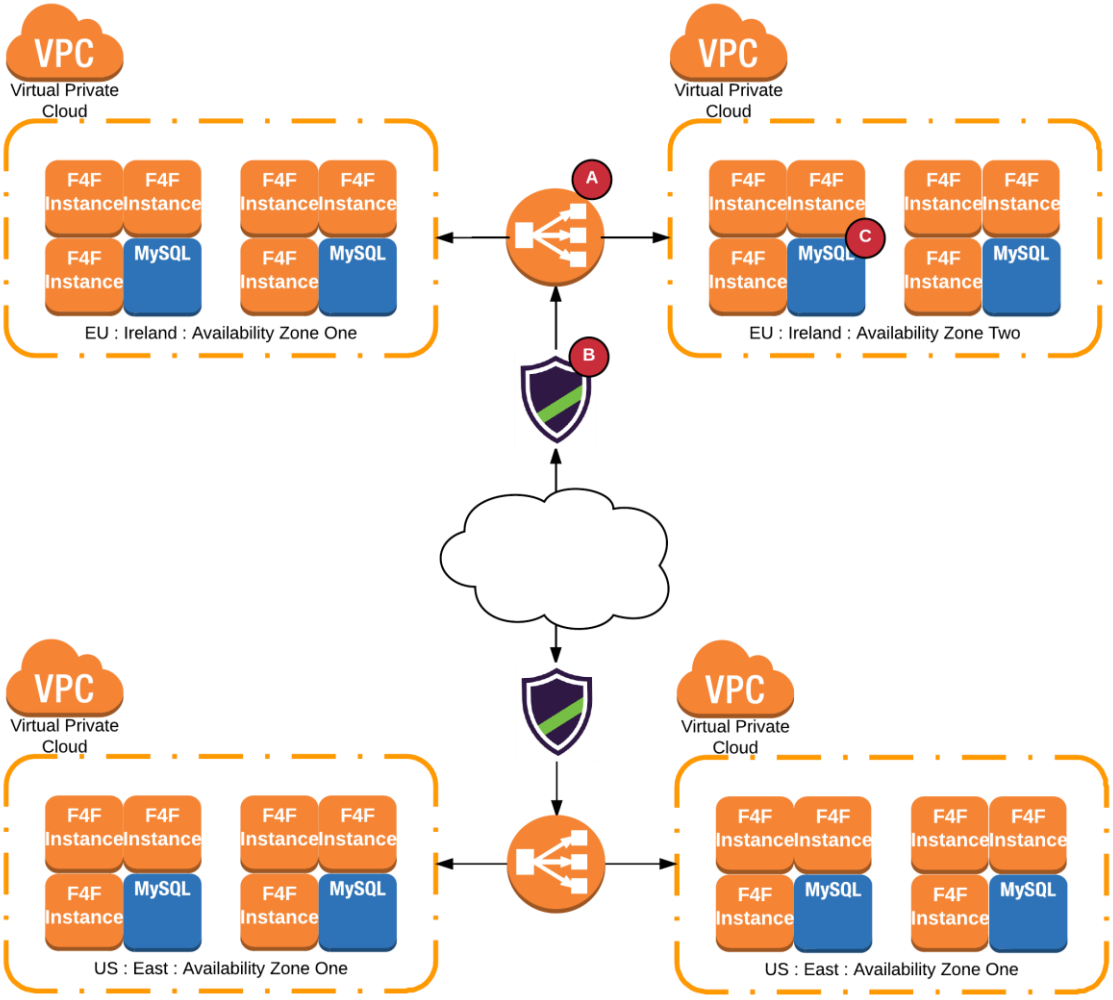
High Level Overview : Production Environment



A **Elastic Load Balancers (ELBs)**

Available Achieve higher levels of fault tolerance for your applications by using Elastic Load Balancing to automatically route traffic across multiple targets and multiple Availability Zones. Elastic Load Balancing ensures that only healthy targets receive traffic by detecting unhealthy targets and rerouting traffic across the remaining healthy targets. If all of your targets in one Availability Zone are unhealthy, and you have set up targets in multiple Availability Zones, Elastic Load Balancing will route traffic to your healthy targets in those other zones.
Elastic Elastic Load Balancing automatically scales its request handling capacity to meet the demands of application traffic. Additionally, Elastic Load Balancing offers integration with Auto Scaling to ensure that you have back-end capacity to meet varying levels of traffic levels without requiring manual intervention.
Secure Elastic Load Balancing works with Amazon Virtual Private Cloud (VPC) to provide robust networking and security features. You can create an internal (non-internet facing) load balancer to route traffic using private IP addresses within your virtual network. You can implement a multi-tiered architecture using internal and internet-facing load balancers to route traffic between application tiers. With this multi-tier architecture, your application infrastructure can use private IP addresses and security groups, allowing you to expose only the internet-facing tier with public IP addresses.

B **Incapsula WAFs**

Protection Against OWASP Top 10 Threats
- Protects against the most critical web application security risks, such as SQL injection, cross-site scripting, illegal resource access, remote file inclusion and other OWASP Top 10 threats
- Guards against newly discovered vulnerabilities to prevent disruption to your application and improve website performance

Most Comprehensive DDoS Protection Service
- Works for single sites as well as multi-gigabit deployments with thousands of sites
- Automatic mitigation of all network, application and protocol layer DDoS attacks launched at websites and web applications
- DNS Protection automatically identifies and blocks attacks seeking to target DNS servers
- Blanket Infrastructure protection for all types of services (UDP/TCP, SMTP, FTP, SSH, VoIP, etc.)

PCI Certification and Reporting
- Incapsula's Web Application Firewall is certified by the PCI Security Standards Council
- Cost-effective compliance with PCI DSS requirement 6.6 without any hardware or software installation and without changes to your web application
- Protects you from liabilities and non-compliance penalties, while protecting your customers' sensitive data from exposure on your site
- PCI compliance report audits security rules configuration changes and periodically reports on your compliance with PCI 6.6 requirements

C **Amazon RDS**

Amazon RDS automatically creates a primary DB instance and synchronously replicates the data to a standby instance in a different Availability Zone (AZ). In case of an infrastructure failure, Amazon RDS performs an automatic failover to the standby DB instance. Since the endpoint for your DB Instance remains the same after a failover, your application can resume database operation without the need for manual administrative intervention