Security SME Word Press GCP Deployment

Usage pattern requirements:

* Cache to San Francisco and Tokyo to increase access to site
* Map load to scale down during average ours for more efficiency for 1k users
* Make sure platform can handle up to 10k active users in future
* Make sure architecture can scale on the 1st and 15th to handle 1,000,000 for 24 hours
* The site can be updated with no down time
* No logins to secure for customers
* No queries
* Less complex for security
* GCP security best practices and cloud native

Security Architecture

WordPress Admin page defensive lockdown:

* changing your default wp-admin login URL
* limiting login attempts
* add HTTP authentication

Common web vulnerabilities defense:

* Two blocks back doors use two-factor authentication, blocking IPs, restricting admin access and preventing unauthorized execution of PHP files
* Prevent Pharma hacks by using recommend WordPress hosting providers with up to date servers and regularly update WordPress installations, themes, and plugins
* Prevent Brute-force Login Attempts by Two-step authentication, [limiting login attempts,](https://kinsta.com/blog/limit-wp-admin-login-attempts/) monitoring unauthorized logins, blocking IPs and using strong password
* Stop Malicious Redirects and Cross-Site Scripting (XSS) by preventing hotlinking

DDoS defense:

* Prevent DDoS using Google Cloud Platform's new Cloud Armor tool which uses global HTTP(S) load balancing
* Cloud Armor can provide both level 3 and 7 OSI protection

Offensive security:

* choose a host that you can trust with your business
* Use Latest PHP Version
* Require complex passwords and usernames for admins
* Use latest versions of WordPress, Plugins and Themes
* Lockdown a URL path
* Take Advantage of Two-Factor Authentication
* Use HTTPS for Encrypted Connections – SSL Certificate
* Harden Your wp-config.php file (Move wp-config.php)
* Update WordPress Security Keys
* Disable XML-RPC
* Hide Your WordPress Version
* Add Latest HTTP Security Headers
* Use WordPress Security Plugins
* Harden Database Security
* Always Use Secure Connections
* Check File and Server Permissions
* Disable File Editing in WordPress Dashboard
* Prevent Hotlinking
* Always Take Backups
* DDoS Protection
* Use Google Cloud WordPress hosting

Ongoing security plan to address future security issues:

* Use GCP best practices
* Segregate resources by projects
* Limit the use of Cloud IAM primitive roles
* Rotate Cloud IAM service account access keys periodically
* Ensure firewall rules are not overly permissive
* Enable VPC Flow Logs
* Ensure Cloud Storage buckets enforce appropriate access controls
* Ensure Cloud Storage buckets have logging and versioning enabled
* Create periodic snapshots of Compute Engine instances
* Create periodic backups of Cloud SQL instances
* Enable and configure Stack driver logging and monitoring
* Have a plan to mature cloud infrastructure
* Implement security features in micro steps to prevent major mistakes
* Use Vulnerability management software and service
* Implement event driven security

References

<https://kinsta.com/blog/wordpress-security/#lock-down-admin>

<https://www.techrepublic.com/article/google-cloud-platform-adds-new-security-service-to-protect-against-ddos-attacks/>

<https://www.slidedeck.com/google-cloud-wordpress-hosting/>