Global Brands Group

Scope of Work

E-Commerce Application

Contents

Overview:

This Scope of Work (SOW) outlines the activities, deliverables, timelines, and responsibilities involved in the design, implementation, and deployment of highly available and secure Azure infrastructure for an e-commerce company expanding operations into Europe. The architecture will be based on Hub & Spoke design with Azure App Services**,** SQL Database**,** Private Endpoints**,** Application Gateway with WAF**,** DDoS protection, and VPN S2S for hybrid connectivity.

Objectives:

1) Design a secure and scalable Hub & Spoke architecture in Azure to support the e-commerce application and database infrastructure.
2) Deploy Azure App Services (API + Web) integrated with Private Endpoints for secure access to the database.
3) Implement Azure Application Gateway with WAF to protect the web application against attacks and to handle load balancing.
4) Establish VPN S2S connectivity between the Azure VNets and the on-premises infrastructure for hybrid scenarios.

Scope of Services:

This scope is based on multi-region perspective; therefore, the number is distributed across **two** regions:

Resources	Notes
Virtual Networks (4)	Hub & Spoke.
Subnets (6)	General-Subnet ApplicationGWSubnet Virtual Network Gateway Subnet Bastion Subnet App-DB-Subnet AppService-Subnet
Application Service (2)	Hosts the e-commerce application.
Endpoints (4)	Private endpoints for secure connection between the app and the internal resources.
Application Gateway (2)	Routes internet traffic to AppService
Web Application Firewall - WAF (2)	Safeguards the application from common web attacks and vulnerabilities.
SQL Database (2)	Stores the application data.
VPN Gateway Device (2)	Sends encrypted traffic between Azure virtual networks in different regions.
Bastion (2)	Used as a jump box to connect to your resources using native SSH or RDP client over HTTPS.
Distributed Denial of Service - DDoS Plan	Secures your services from network disrupting DDoS attacks.
Defender	Provides comprehensive security for your cloud workloads.
Site-to-Site - S2S VPN (1)	Provide a secure encrypted tunnel from your on-premises to your cloud environment.
Traffic Manager	Distributes traffic to both Application Gateways based on a certain policy.
Peering (2)	From Hub to Spoke in each region

Technical Details:

1. Virtual Network (VNet) Setup:

- **Step 1**: Create Hub VNet for shared services (DNS, VPN).
- **Step 2**: Create Spoke VNets for App Service and SQL Database workloads.
- **Step 3**: Define subnets within VNets for each service (e.g., App Service, Application Gateway).

---

2. Azure Resources Setup:

- **Step 1**: Deploy Azure App Services for API and Web applications.
  - Choose the appropriate SKU (Basic for cost control).
- **Step 2**: Set up SQL Database with Private Endpoint for secure access from App Services.
- **Step 3**: Configure Application Gateway with WAF to secure traffic:
  - Set up backend pools**,** health probes, and routing rules.

---

3. VNet to VNet VPN:

- For multi-region connectivity Create VPN Gateway in the Hub VNets.

---

4. Security Configuration:

- **Step 1**: Enable DDoS Protection (Basic) for all VNets to prevent external threats.
- **Step 2**: Enable Azure Defender for App Services and SQL Database.
- **Step 3**: Configure WAF on Application Gateway to protect web applications from threats.

---

5. DNS Configuration:

- **Step 1**: Create Private DNS Zones for private endpoint resolution
- **Step 2**: Link DNS Zones to the Spoke VNets**.**

---

6. Monitoring & Logging:

- **Step 1**: Set up AppInsight and Log Analytics for application tracking and log collection.

Scope of Work Man-days:

The following table outlines the estimated level of effort required to complete each phase of the project:

Phase	Man-days
Architecture Design & Planning	2 Days
VNet & Subnet Configuration	1 Days
AppService Deployment	1 Days
SQL Database Setup & Integration	1 Days
Application Gateway & WAF Setup	1 Days
VPN S2S Setup	2 Days
Security Configurations	2 Days
Testing & Validation	2 Days
Documentation & Handover	2 Days
Total	**14 Days (2 Weeks)**

Conclusion

This Scope of Work provides a comprehensive framework for designing, deploying, and testing a highly available and secure Azure infrastructure for the e-commerce application. By leveraging Azure App Services**,** Private Endpoints**,** Application Gateway with WAF, and VPN S2S, the solution ensures both security and scalability, meeting the project's objectives. The estimated 33 man-days for implementation, testing, and documentation are structured to align with the defined scope and deliverables, providing a clear path to successful project completion.

Thank You!