**Azure DMZ Landing Zone - Detailed Design Document**

**1. Purpose**

This document defines the **detailed design** for implementing a new **DMZ Landing Zone** on Microsoft Azure. It replaces the existing public-facing tenancy design and aims to align with the Cloud Adoption Framework (CAF) and ISM PROTECTED controls.

**2. Background**

The current UAT environment comprises multiple VNets (infrastructure-official-uat-1-\*) across AUEast, AUCentral, and AUCentral2. These are peered and contain ASE, APIM, databases, AI workloads, and bastion hosts. The subscription hierarchy spans Official, Protected, and DevOps branches under a structured management group model.

**3. Scope**

**In scope:**

* Creation of a new DMZ Landing Zone aligned with CAF
* Hub-and-Spoke network architecture
* Secure boundary with Azure Firewall, Application Gateway, Private Endpoints
* Compliance with ISM PROTECTED, Essential Eight

**Out of scope:**

* Redesign of operational processes or existing DevOps toolchains
* Integration with third-party tools
* Application code changes

**4. Design Principles**

* Zero Trust architecture
* Network and identity segmentation
* Infrastructure-as-Code deployment
* Principle of least privilege
* Automation, monitoring, and compliance-first

**5. Landing Zone Architecture**

**5.1 Hub**

* **VNet Name:** dmz-hub-vnet
* **Components:**
  + Azure Firewall Premium
  + Azure Bastion
  + DNS forwarders (Private DNS Resolver)
  + Log Analytics Workspace
  + Azure Key Vault with HSM (optional)
  + DDoS Protection Plan

**5.2 Spokes**

Spoke VNets will be aligned per workload/application:

* dmz-web-spoke – Internet-facing apps
* dmz-api-spoke – API and backend services
* dmz-data-spoke – Azure SQL, Cosmos DB, etc.
* dmz-mgmt-spoke – Jumpboxes, monitoring, automation
* dmz-hybrid-spoke – ExpressRoute/VPN connectivity

**6. Network Configuration**

* NSGs per subnet with deny-by-default
* ASGs for workload grouping
* UDRs to force egress through Firewall
* Private Endpoints for PaaS resources (Key Vault, SQL, Storage)
* ExpressRoute with IPSec or MACsec for sensitive traffic
* Application Gateway WAF (for Layer 7 control)

**7. Identity & Access Management**

* Hybrid AAD with Entra ID and ADFS
* MFA enforced via Conditional Access
* Privileged Identity Management (PIM) for JIT access
* RBAC using built-in and custom roles

**8. Management & Governance**

* Management Groups:
  + Official
    - Official-UAT
    - Official-PRD
  + Protected
    - Protected-Mgmt, Protected-UAT, Protected-Spokes
* Policies:
  + Allowed regions (AUCentral, AUEast)
  + Allowed SKUs
  + Mandatory tagging
* Monitoring:
  + Azure Monitor, Log Analytics, Azure Sentinel

**9. Security Controls**

* Encryption at rest (Storage/SQL/VMs) and in transit (TLS 1.3)
* Defender for Cloud: Secure Score, recommendations
* Microsoft Sentinel: SIEM and SOAR integration
* Just-in-Time VM access
* Immutable backup via Recovery Services Vaults

**10. Landing Zone Transformation Plan**

To replace the current public-facing design with the DMZ Landing Zone, the following detailed transformation steps will be applied:

1. **Analysis & Discovery:**
   * Identify existing workloads with public endpoints.
   * Inventory dependencies, NSG rules, and ingress/egress patterns.
   * Classify workloads by sensitivity and internet exposure requirements.
2. **New Landing Zone Build:**
   * Deploy new DMZ Landing Zone using Infrastructure-as-Code aligned with CAF.
   * Ensure Hub is provisioned with firewall, diagnostics, and DNS forwarding.
   * Define and deploy spokes as per classification (web/API/data/mgmt).
3. **Segregation Enforcement:**
   * Remove public IPs on existing resources where not justified.
   * Migrate public-facing workloads behind Azure Application Gateway in the DMZ web spoke.
   * Move internal-only services to respective spokes using private IPs and endpoints.
4. **Policy and Security Configuration:**
   * Apply network policies (UDRs, NSGs, ASGs) for traffic control.
   * Attach Azure Policies to prevent public IP creation unless exception is approved.
   * Enable Defender for Cloud and configure security baselines.
5. **Peering and Connectivity:**
   * Peer new DMZ spokes with hub, enforce traffic routing through central firewall.
   * Connect legacy VNets (e.g., infrastructure-official-uat-\*) with new hub as needed.
6. **Testing and Cutover:**
   * Test connectivity, NSG logs, firewall logging.
   * Conduct phased cutover per workload type (web, API, data).
   * Validate workloads using monitoring and connection testing.
7. **Decommission Legacy Design:**
   * After validation and documentation, decommission public-tenancy approach.
   * Ensure all PaaS services are accessed via private link.

**11. Implementation Plan**

|  |  |  |
| --- | --- | --- |
| **Phase** | **Activity** | **Duration** |
| Phase 1 | Deploy Hub + Policies | 2 weeks |
| Phase 2 | Deploy Spokes + UDRs, NSGs | 2 weeks |
| Phase 3 | Integrate Identity & Firewall Rules | 2 weeks |
| Phase 4 | Validate & Pilot Migration | 2 weeks |
| Phase 5 | Full Migration & Cutover | 4-6 weeks |
| Phase 6 | Optimisation, Documentation, KT | 2 weeks |

**12. Appendices**

* Appendix A: Subscription/Management Group Topology
* Appendix B: NSG and Firewall Rule Matrix
* Appendix C: IP Address Plan
* Appendix D: High-Level Logical Diagram (from original design doc)