Azure Security Infrastructure Suite

Redback Operations

Contents

[Azure Security Considerations for Web Application Infrastructure Deployment 3](#_Toc165206844)

[Identity and Access Management (IAM) using Identity as a Service (IDaaS) with Azure Entra ID 3](#_Toc165206845)

[Firewalls with Azure Firewall 4](#_Toc165206846)

[Secret Management with Azure Key Vault 5](#_Toc165206847)

[Benefits of using Microsoft Azure Products: 5](#_Toc165206848)

# Azure Security Considerations for Web Application Infrastructure Deployment

This document is a comprehensive overview of security considerations when deploying web application infrastructure on Microsoft Azure. Beginning with the assumption a secure password policy is already in place to ensure the implementation of the authentication factor "something you know," this document further reinforces this security measure by leveraging Azure suite products. Specifically, it concentrates on enhancing security through Identity and Access Management (IAM), Firewalls, and Secret Management.

# Identity and Access Management (IAM) using Identity as a Service (IDaaS) with Azure Entra ID

**Role-Based Access Control (RBAC):** Azure Entra ID, formerly Azure Active Directory (Azure AD), utilizes RBAC to grant users access to Azure resources based on their roles and responsibilities[1]. This enforces the principle of least privilege, minimizing access risks [1]. This can be viewed as “something you are” factor in authentication.

**Multi-Factor Authentication (MFA):** Acts as an additional layer of security by requiring verification of a user’s identity through a device they own [1]. This factor could be referred to as “something you have”.

**Conditional Access:** Conditional access policies can be implemented to restrict access based on location, device, or time of day [1]. This could be considered “somewhere you are”.

**Azure Entra ID Privileged Identity Management (PIM):** For highly privileged tasks, leverage Entra’s PIM to provide temporary access and multi-factor authentication [1] (MFA) for enhanced security.

**Recommendations:**

* Implement RBAC with custom roles tailored to specific resource access needs [1].
* Enable Azure AD Privileged Identity Management (PIM) for just-in-time (JIT) access to highly privileged roles [1].
* Utilize Azure Monitor to identify unused or excessive permissions and remove them [1].

# Firewalls with Azure Firewall

Azure Firewall offers hierarchical policy enforcement across subscriptions, resource groups, and individual virtual networks [2].Azure Firewall inspects incoming and outgoing traffic for potential threats, providing granular control over network access [2]. Azure Firewall also protects against DoS attacks, safeguarding web application infrastructure [2].

* **Azure Firewall Standard**:
  + Provides Layer 3-7 filtering and threat intelligence feeds directly from Microsoft Cyber Security [2].
  + Threat intelligence-based filtering alerts and denies traffic to/from known malicious IP addresses and domains in real time [2].
  + Ideal for robust threat protection [2].
* **Azure Firewall Premium**:
  + Offers advanced capabilities, including signature-based Intrusion Detection and Prevention System (IDPS) [2].
  + Detects attacks by analysing specific patterns (e.g., byte sequences or known malicious instructions) [2].
  + Over 67,000 signatures across various exploit categories (malware, phishing, coin mining, Trojans) are updated in real time [2].
  + Perfect for rapid attack detection.
* **Azure Firewall Basic**:
  + Designed for small and medium-sized (SMB) customers [2].
  + Provides essential protection at an affordable price point [2].
  + Main limitations:
    - Supports Threat Intel alert mode only.
    - Fixed scale unit with two virtual machine backend instances.
    - Recommended for environments with an estimated throughput of 250 Mbps.

**Recommendations:**

* Implement a layered firewall approach with Azure Firewall at the perimeter and Network Security Groups (NSGs) for individual resources [2].
* Utilize the built-in DoS protection capabilities of Azure Firewall [2].
* Leverage Azure Monitor for firewall log analysis and security insights [2].

# SecretManagement with Azure Key Vault

**Secure Storage:** Azure Key Vault provides a secure repository for storing sensitive information like passwords, API keys, and certificates [3].

**Access Control:** Granular access control ensures only authorized users can access secrets [3].

**Key Rotation:** Secrets can be rotated periodically to minimize damage if compromised [3].

**Recommendations:**

* Store all application secrets in Azure Key Vault as opposed to code or configuration files [3].
* Implement RBAC to control access to secrets based on user roles [3].
* Automate secret rotation to enhance security posture [3].

# Benefits of using Microsoft Azure Products:

By leveraging Azure security features, you can build a secure and reliable foundation for your web applications. Azure offers a unified platform that streamlines security management across identity, access control, resources, and security tools [1]. Built-in encryption and adherence to industry best practices reduce your security burden [1]. Furthermore, Azure offers a suite of comprehensive security tools for continuous monitoring, threat detection, and proactive threat management [1]. Maximize your security posture by integrating Azure Security Centre for advanced threat protection and best practice recommendations [1]. Additionally, leverage Azure Monitor for centralized logging and resource health insights [1]. By regularly reviewing and updating your security policies, you can ensure a strong security posture for your web applications on Azure.

# References

|  |  |
| --- | --- |
| [1] | Microsoft, “What is Microsoft Entra ID?,” [Online]. Available: https://learn.microsoft.com/en-us/entra/fundamentals/whatis. |
| [2] | Microsoft, “Azure Firewall documentation,” [Online]. Available: https://learn.microsoft.com/en-us/azure/firewall/. |
| [3] | Microsoft, “Azure Key Vault documentation,” [Online]. Available: https://learn.microsoft.com/en-us/azure/key-vault/. |