Security in Azure

Memi Lavi
www.memilavi.com

Security

- Security is one of the most important parts of every system
- Azure offers a lot of security measures for its resources
- It's extremely important to use those measures and follow security patterns to avoid security incidents
- We've covered most of them, here we'll summarize and emphasize some new techniques

VM Security Best Practices

- Restrict access to the VM as much as possible
- Make sure only the required ports are open to the internet

  (22/1389/443/80)
- Limit access to specific IP addresses when possible

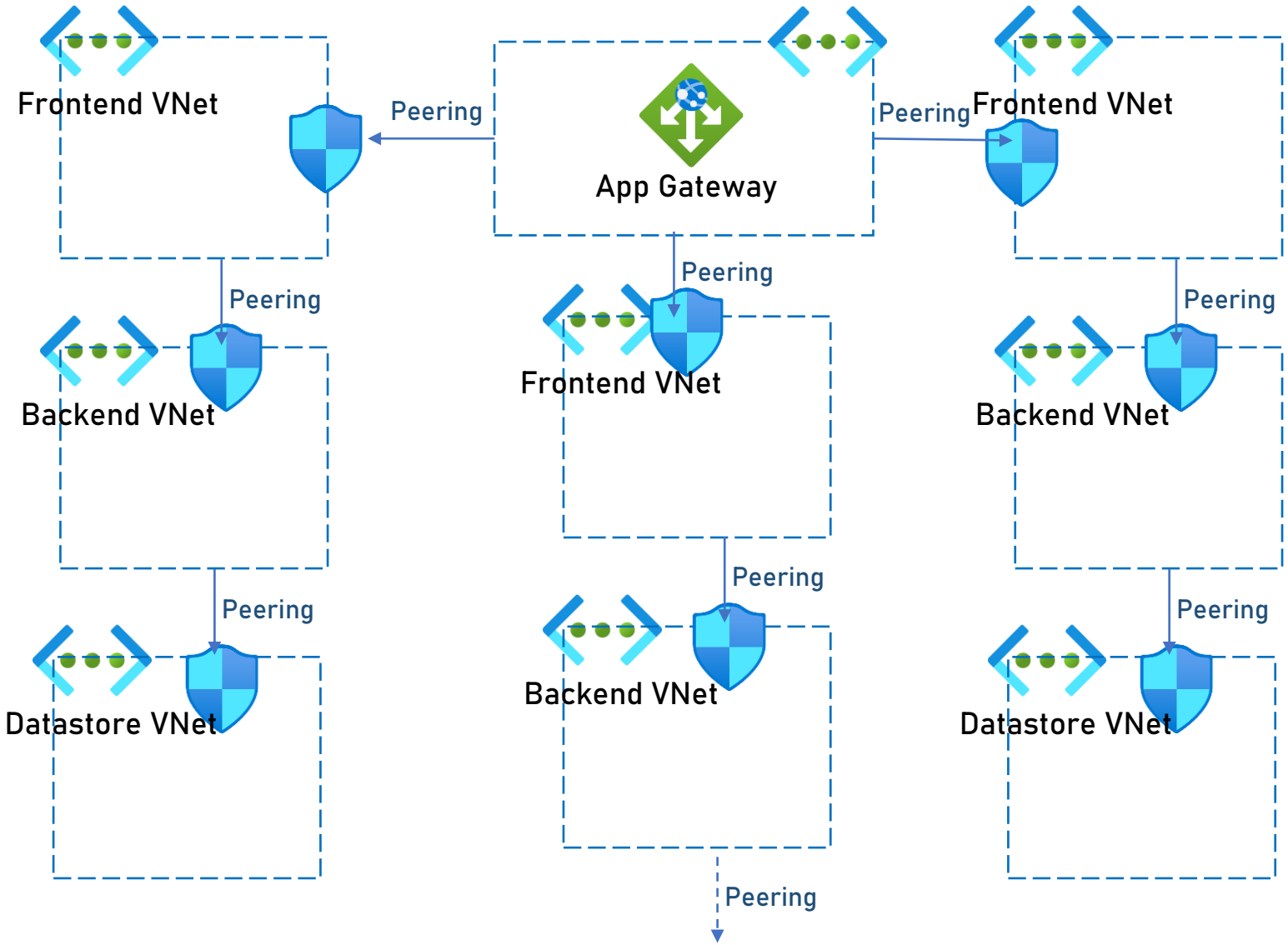
VM Security Best Practices

- Prefer using Bastion for accessing the VM, so no need for open ports
- If the VM is not public facing – place it in a VNet that's not connected directly to the internet

Networking Security Best Practices

- VNet that contains private resources only – should not be exposed to the internet
- ALWAYS use NSG to restrict access to subnets
- Use Service Endpoints / Private Endpoint to restrict access to resources
- Use the Hub-and-Spoke security model

Hub and Spoke



Database Security Best Practices

- Use encryption at rest and encryption at transit (usually On by default)
- Connect DB to relevant VNet using Services Endpoint / Private Endpoint
- Access DB from app using Managed Identities
- Use DB's Firewall rule to restrict external access

App Service Security Best Practices

- Don't expose directly to the internet, use Application Gateway
- Connect to App Gateway's VNet using Service Endpoint / Private Endpoint
- Use Azure AD for Authentication, enforce with MFA
- Use Managed Identity to access other resources when possible

KeyVault

- Many apps have secrets that need to be kept safely
  - Connection Strings
  - Keys
  - Certificates
  - API Keys
  - And more…

KeyVault

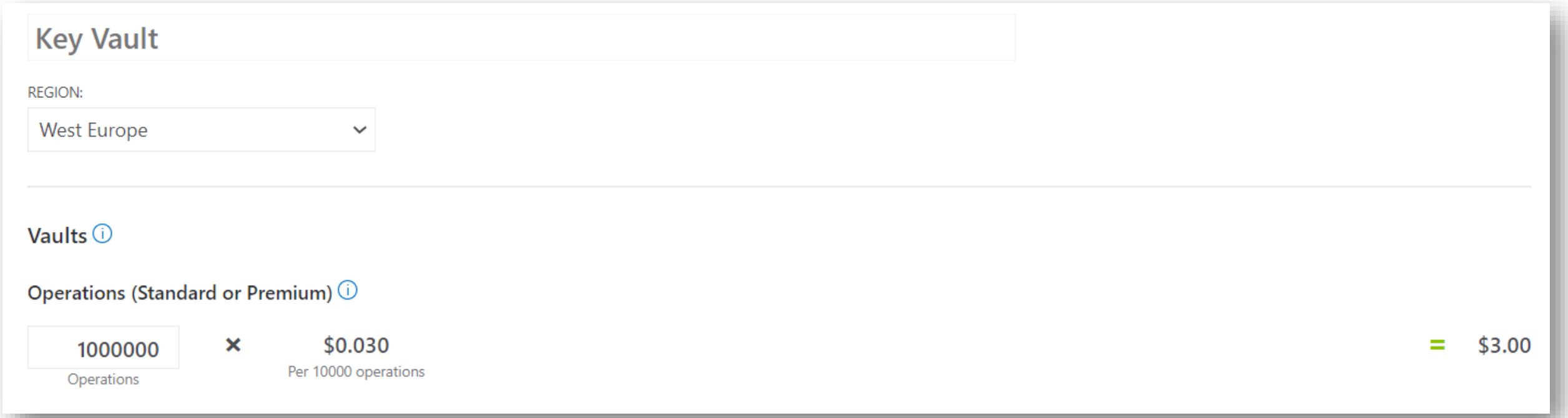
- Usually kept in configuration files, configuration DB etc.
- Not really secure…
- KeyVault solves this problem

KeyVault

- Safely stores secrets of various types
- Very restricted access – needs Azure AD authentication
- Supports Hardware Security Modules (for enhanced security)
- Easily manageable
- Accessed via REST API

KeyVault

- Very cost effective



Security Center

- A central location for monitoring and alerting security-related issues
- Displays a summarized list of problems found in the subscription's resources
- In some cases, allow a single-click fix
- Good practice to take a look once in a while

ReadIt!

Cloud Architecture