Microsoft

Azure Rendering

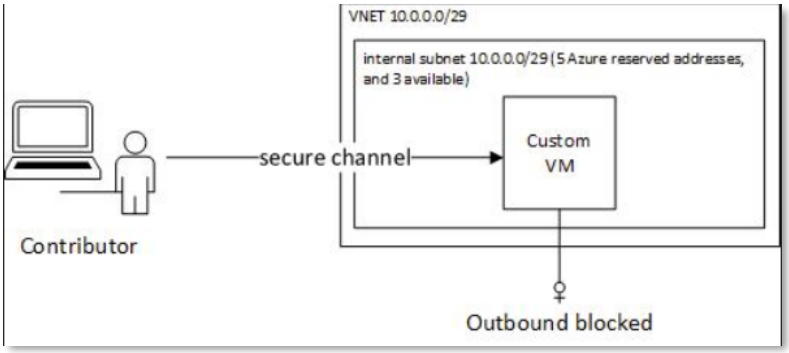
Secure Render Pilot

Phase 1

Summary

Objective: Achieve single frame render with maximize lock down of user access and data

Scope: 1 Custom VM via Point-to-Site VPN



Steps

1. Role based access control (RBAC)
2. Secured Network
3. Governance Enablement via Azure Policy
4. Security Audit Exercise

Governance

To enforce governance during Build, Upload, Deployment, and Operation we will focus on the following security capabilities:

- **Role-based Access Control** (RBAC) – Manages who has access to Azure resources, what they can do with those resources, and what areas they have access to. RBAC is an authorization system that provides fine-grained access management of Azure resources (https://docs.microsoft.com/en-us/azure/role-based-access-control/overview)

- **Azure Policy** – Used to create, assign, and manage policies to enforce rules on Azure resources. Ensures Azure resources stay compliant with corporate governance standards. (https://docs.microsoft.com/en-us/azure/governance/policy/overview)

- **Network Security Groups** - Filter network traffic to and from Azure resources in an Azure virtual network. Contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. (https://docs.microsoft.com/en-us/azure/virtual-network/security-overview)

1. Role-based Access Control

Examples

- Owner - Lets you manage everything, including access to resources.
- Virtual Machine Contributor – Restricts access to manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.

Custom Image Process

Reference: (https://github.com/Azure/Avere/tree/master/src/terraform/examples/securedimage)

Process Summary

1. Build custom image by *Administrator*
2. Upload Custom Image via a managed disk by *Administrator*
3. Create the access for the *Contributor* by *Administrator*
4. Deploy custom image by *Contributor*

2. Secured Network

Network Security Groups

Assigning 3 security roles

1. Allows only port 22 access from a specific IP (begins at row 46 in Main.tf)
2. Deny remaining inbound on VNet (begins at row 60 in Main.tf); Denies all other inbound traffic
3. Deny all outbound traffic

3. Governance

Policy Enforcement

Assign Azure Policy to VNet

1. Denies SSH from a fully open Internet
2. Denies Azure Storage account creation without private endpoint

4. Security Audit Exercise

1. Contributor to try to list all resource groups: az group list
2. Contributor to try to create a resource group: az group create -l eastus -n test
3. Contributor to try to create a storage account in same rg: az storage account create -l eastus -g azuresandbox -n anhowesandbox --sku standard_lrs
4. On VM: ping 8.8.8.8
5. On VM: wget bing.com
6. Review Policies
7. Review Activity Log

For Reference

Sample URL

/subscriptions/c52fce95-dz4f-4b37-afca-db203a5d0b6a/resourceGroups/rendersandbox-rg/providers/Microsoft.Network/virtualNetworks/render-vnet/subnets/internal

Sample Hierarchy

- Azure Account
    - Subscription – Subscription ID (c52fce95-dz4f-4b37-afca-db203a5d0b6a)
        - Resource Group – Resource Group Name (rendersandbox-rg)
            - Resource Providers (Microsoft.Network)
                - Resource Type (virtualNetworks)
                    - Subnets (internal)