Overview
Contoso is an online training provider

Current Environment

- The company currently has an Azure subscription named Contosoub1.This is associated with an Azure AD tenant named contoso.com
- The company has the following resource groups defined in the subscription
  - contosorg1
  - contosorg2
  - contosorg3
  - contosorg4
  - contosorg5
  - contosorg6
- The company has the following users defined in Azure AD

Name	City	Role
contosousr1	Montreal	Global Administrator
contosousr2	MONTREAL	Security Administrator
contosousr3	London	Privileged Role Administrator
contosousr4	Ontario	Application Administrator
contosousr5	Seattle	Cloud Application Administrator
contosousr6	Seattle	User Administrator
contosousr7	Sydney	Reports reader
contosousr8	Sydney	None

There are 2 security groups defined

Name	Membership type	Dynamic membership rule
contosogrp1	Dynamic user	user.city -contains “ON”

contosogrp2	Dynamic user	user.city -match “*on”

- contosousr2 has been given the permission to create virtual networks

The following networks are defined

Name	Resource Group
contosonetwork1	contosorg1
contosonetwork2	contosorg2
contosonetwork3	contosorg3
contosonetwork4	contosorg4

The following locks are defined

Name	Set On	Lock type
contosolock1	contosorg1	Delete
contosolock2	contosorg2	Read-only
contosolock3	contosorg3	Delete
contosolock4	contosorg3	Read-only

The following Azure policies are defined

Policy definition	Resource type	Scope
Allowed resource types	networkSecurity/Groups	contosorg4
Not allowed resource types	virtualNetworks/subnets	contosorg5
Not allowed	networkSecurity/Groups	contosorg5

resource types		
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	contosorg6

The following subnets are defined

Network	Subnet
contosonetwork1	subnetA, subnetB, subnetC
contosonetwork2	subnetD

The following virtual machines are defined

Name	Network Interface	Application Security Group	Connected to
contosovm1	NIC1	contosoasg1	subnetA
contosovm2	NIC2	contosoasg2	subnetA
contosovm3	NIC3	None	subnetB
contosovm4	NIC4	contosoasg1	subnetC
contosovm5	NIC5	None	subnetD

The following network security groups are defined

Name	Associated to
contosonsg1	NIC2
contosonsg2	subnetA
contosonsg3	subnetC

contososnsg4	subnetD

- Each virtual machine has a public IP address
- Each virtual machine ahs the Internet Information Services role installed
- The firewalls on each virtual machine allows ping and web requests

contosonsg1 has the following inbound security rules

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

contosonsg2 has the following inbound security rules

Priority	Port	Protocol	Source	Destination	Action
100	80	TCP	Internet	VirtualNetwork	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

contosonsg3 has the following inbound security rules

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	contosoasg1	contosoasg1	Allow
150	Any	Any	contosoasg2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow

65500	Any	Any	Any	Any	Deny

contosonsg4 has the following inbound security rules

Priority	Port	Protocol	Source	Destination	Action
100	Any	Any	Any	Any	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

All Network security groups have the same outbound security rules

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

The company is going to carry out the following changes

- Deploy Azure Firewall to contosonetwork1
- Register an application named “contosoapp” to Azure AD
- Whenever possible, use the principle of least privilege
- Enable Azure AD Privileged Identity Management (PIM) for the tenant