Secure Azure Network and IAM Architecture for Startup Enterprise

Name: Seth Vaughn

Date: 28/04/2025

Table of Contents

Scenario

This project simulates the design and implementation of a secure cloud infrastructure in Microsoft Azure for a small organisation (CaribSecure) with under 100 users. The solution is divided into two key phases. Phase 1 focuses on Identity and Access Management (IAM), where users are assigned to department-based Azure AD groups with role-based access controls applied using RBAC. Next, phase 2 focuses on network segmentation and security, where each department is logically isolated using subnets and Network Security Groups (NSGs).

Purpose

The purpose of this project is to demonstrate a practical, beginner-friendly approach to securing cloud resources using Microsoft Azure. It showcases core skills in IAM, RBAC, network segmentation and access control testing. This project reflects real-world infrastructure challenges and is structured to highlight the fundamentals of cloud security design and implementation.

1. Phase 1 Objectives — Identity & Access Management (IAM)

1. Simulate Organisational Structure

- Define 5 departments: Management, Finance, Marketing, IT, and R&D

2. Create Azure AD Groups

- One security group per department
- Create 4 users per department
- Assign users to their respective groups for centralised management (recommended)

3. Implement Role-Based Access Control (RBAC)

- Define and create resource groups
- Assign Azure roles at the resource group level based on each group’s needs
- Ensure least-privilege access for all users

4. Enforce Multi-Factor Authentication (MFA)

- Apply conditional access policies to enforce MFA for sensitive departments (e.g IT, Finance, Management)

5. IAM Test Cases

- To validate that users can only access permitted resources
- Confirm MFA prompts trigger for protected users

1.1. Simulate Organisational Structure

Objective: Define the business layout

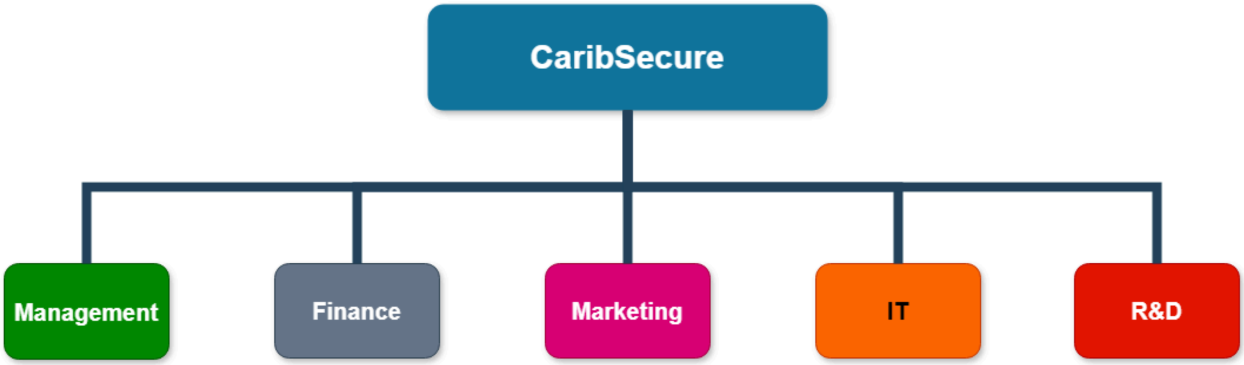


Figure 1.1: Organisational Structure Diagram

- List of departments:
  - Management
  - Finance
  - Marketing
  - IT
  - Research & Development (R&D)

- Number of users per department: 4

Department	Description
Management	Leadership and reporting, high privilege, minimal access
Finance	Handles budgeting and reports
Marketing	Handles campaigns and media
IT	Manages infrastructure; administrative control
R&D	Develops internal tools, Sensitive data zone (restricted outbound)

Table 1.1: Departments & Responsibilities

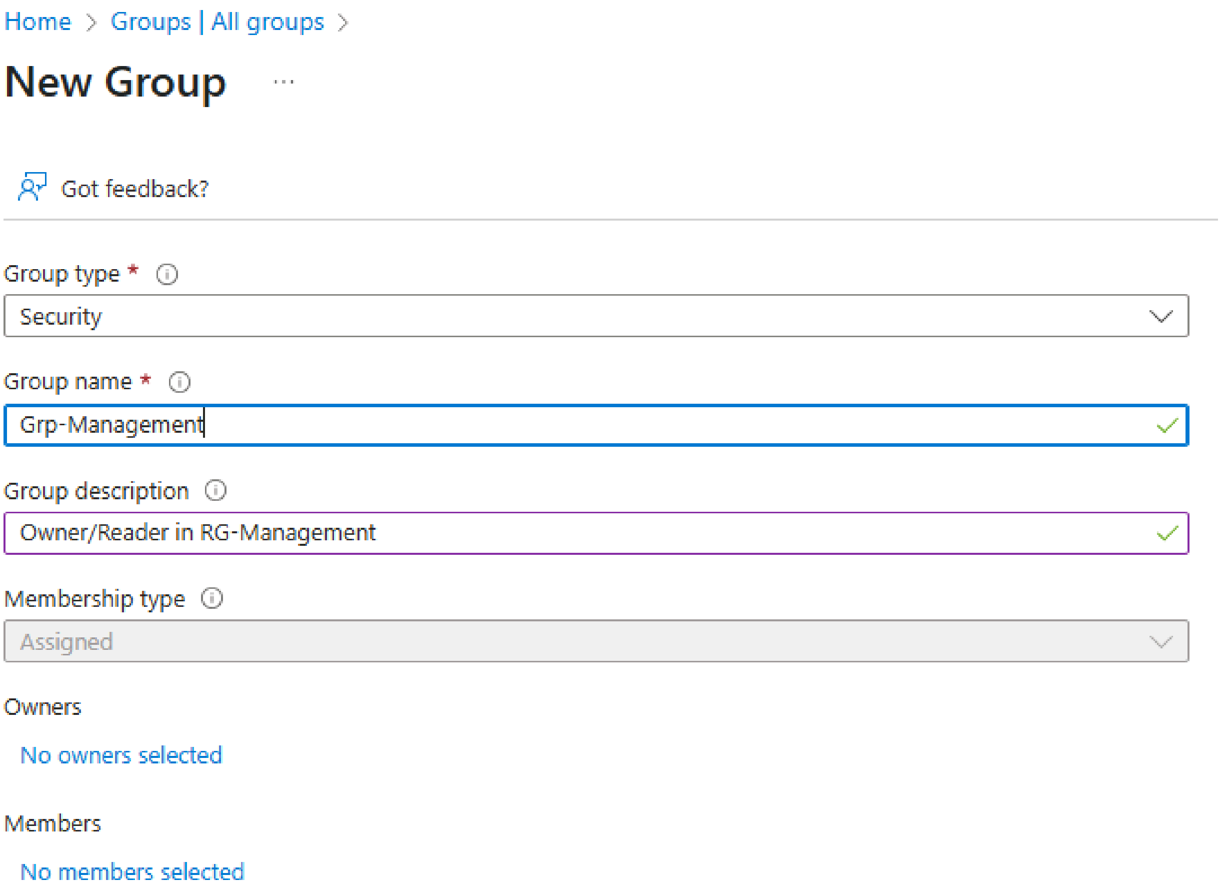
1.2. Create Azure AD Groups

Objective: Create Azure AD groups for each department.

- Steps to create AD Groups:

Go to **Microsoft Entra ID → Groups → + New Group**

- Group Creation



Group type * : Security

Group name * : Grp-Management

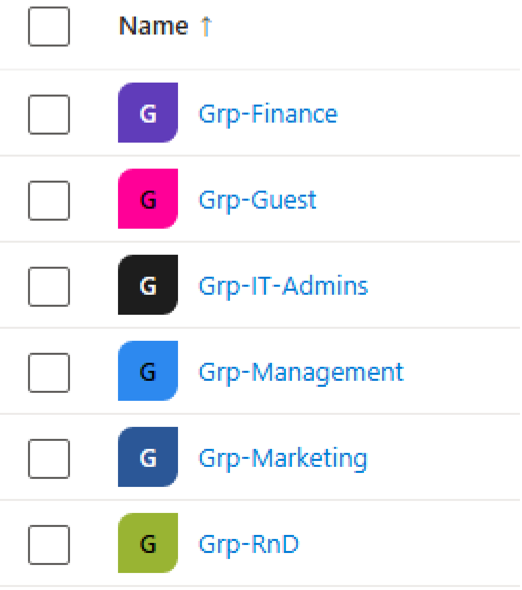
Group description: Owner/Reader in RG-Management

Membership type: Assigned

Owners: No owners selected

Members: No members selected

Figure 1.2: Creation of the Management group in Microsoft Entra ID



□ Name ↑

□ G Grp-Finance

□ G Grp-Guest

□ G Grp-IT-Admins

□ G Grp-Management

□ G Grp-Marketing

□ G Grp-RnD

Figure 1.3: List of all AD group names

Azure AD Group	Assigned To Department	Role
Grp-Management	Mangement	Reader
Grp-Finance	Finance	Contributor
Grp-Marketing	Marketing	Contributor
Grp-IT-Admins	IT	Owner
Grp-RnD	R&D	Contributor

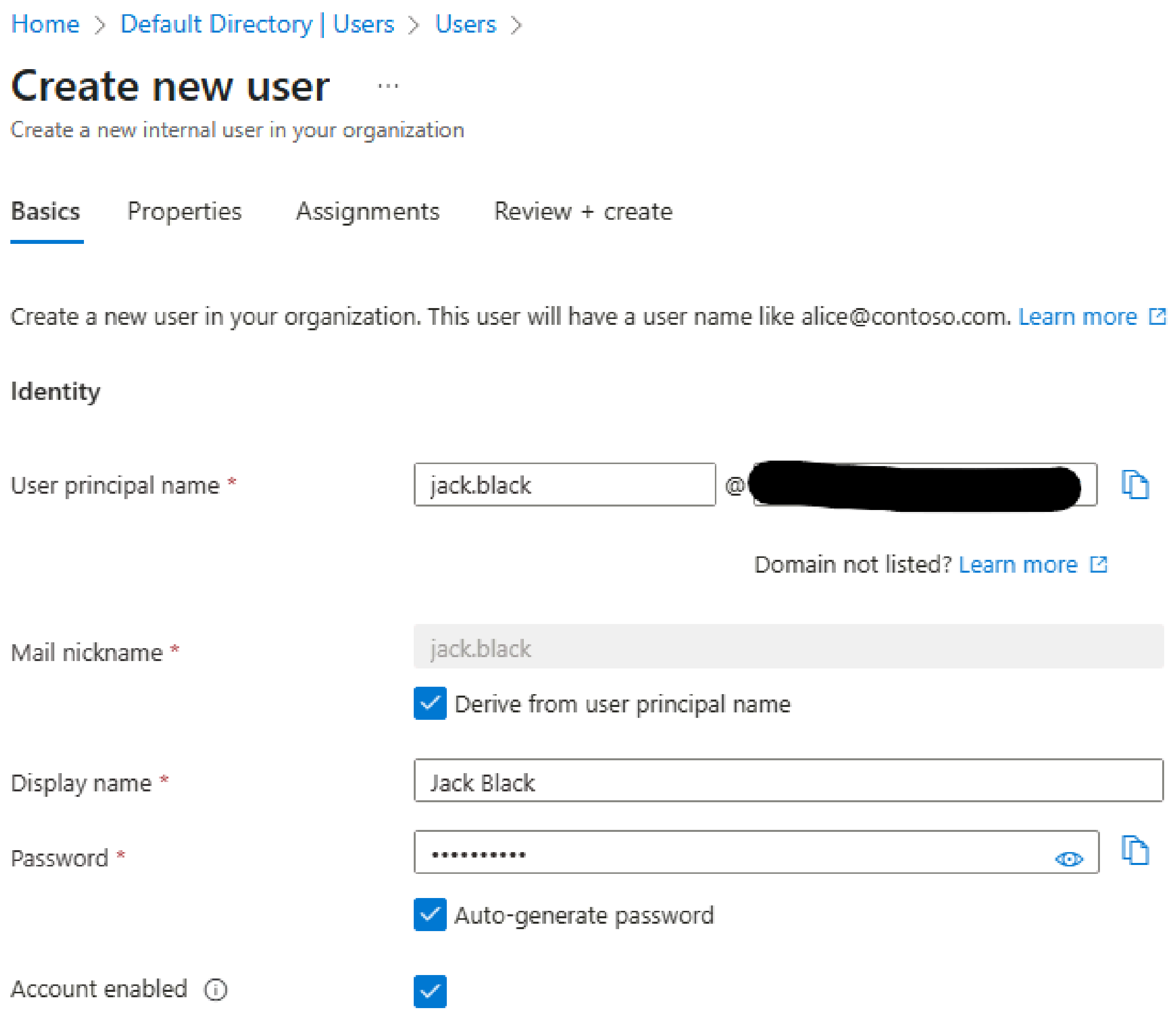
Table 1.2: Azure AD Groups

1.2.1. User Creation & Assignment

Objective: Add 4 realistic users per department and assign them to the corresponding group.

- Step 1: Create Users

Go to **Microsoft Entra ID → Users → + New User**



Home > Default Directory | Users > Users >
Create new user ···
Create a new internal user in your organization
Basics
Properties
Assignments
Review + create

Create a new user in your organization. This user will have a user name like alice@contoso.com. Learn more

Identity

User principal name * jack.black @[redacted]

Domain not listed? Learn more

Mail nickname * jack.black

☑ Derive from user principal name

Display name * Jack Black

Password * •••••••••••

☑ Auto-generate password

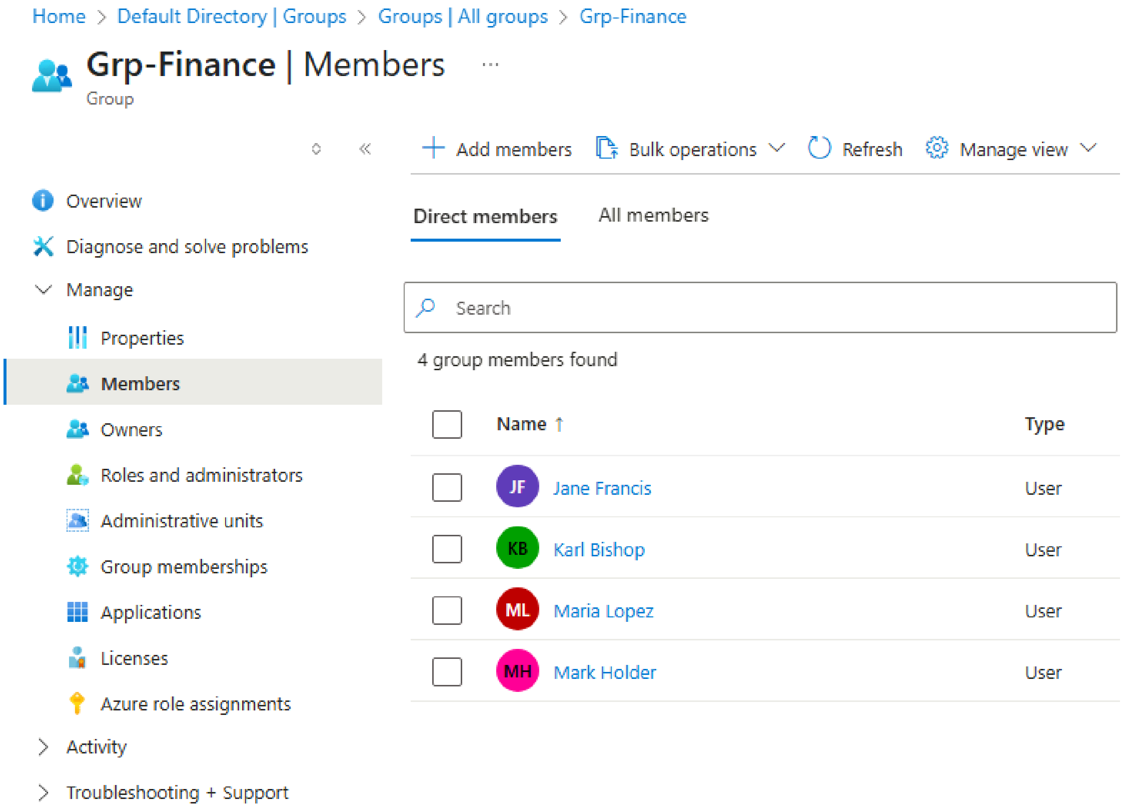
Account enabled ☑

Figure 1.4: Creation of new user, Jack Black, in Microsoft Entra ID

- Step 2: Assign New Users to AD Groups

Go to **Microsoft Entra ID → Groups → [Your Group] → Members → + Add Members**

- Select the appropriate users for:
  - Grp-Management
  - Grp-Finance
  - Grp-Marketing
  - Grp-IT-Admins
  - Grp-RnD



4 group members found

□	Name ↑	Type
□	JF Jane Francis	User
□	KB Karl Bishop	User
□	ML Maria Lopez	User
□	MH Mark Holder	User

Figure 1.5: Screenshot of the member list of Grp-Finance

User Email	Department	Azure AD Group
julian.bennett@mydomain.com	R&D	Grp-RnD
tina.grant@mydomain.com	Marketing	Grp-Marketing

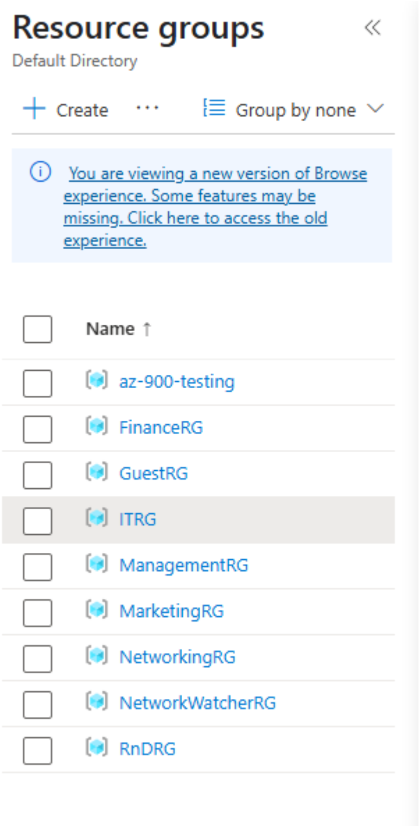
Table 1.3: Example of User Creation and Assignment

1.3. Implement Role-Based Access Control (RBAC)

Objective: Define and create resource groups that departments can only access and control.

RG Name	Purpose	Department Access
ManagementRG	Shared docs, dashboards, and mail access	Management
FinanceRG	Financial apps, reports	Finance
MarketingRG	Content creation, campaigns storage	Marketing
ITRG	Identity, monitoring, shared services	IT
RnDRG	Research, products and services, and app hosting	R&D
NetworkingRG	Firewalls, VNets, NSGs	IT

Table 1.4: Brief description of each resource group



You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.

□	Name ↑
□	az-900-testing
□	FinanceRG
□	GuestRG
□	ITRG
□	ManagementRG
□	MarketingRG
□	NetworkingRG
□	NetworkWatcherRG
□	RnDRG

Figure 1.6: List of Azure Resource Groups

1.3.1. RBAC Role Assignments

Objective: Assign access control roles to each AD group, using least-privilege principles.

- RBAC Roles

   1. **Reader**
      - Can view resources, but cannot apply any changes. This is suitable for management and auditing.

   2. **Contributor**
      - Can create and manage resources, but cannot assign roles to others. This is ideal for teams managing their environments.

   3. **Owner**
      - Has full control and access to every resource, including the ability to assign roles. However, “with great power comes great responsibility.” This is most suitable for IT admins.

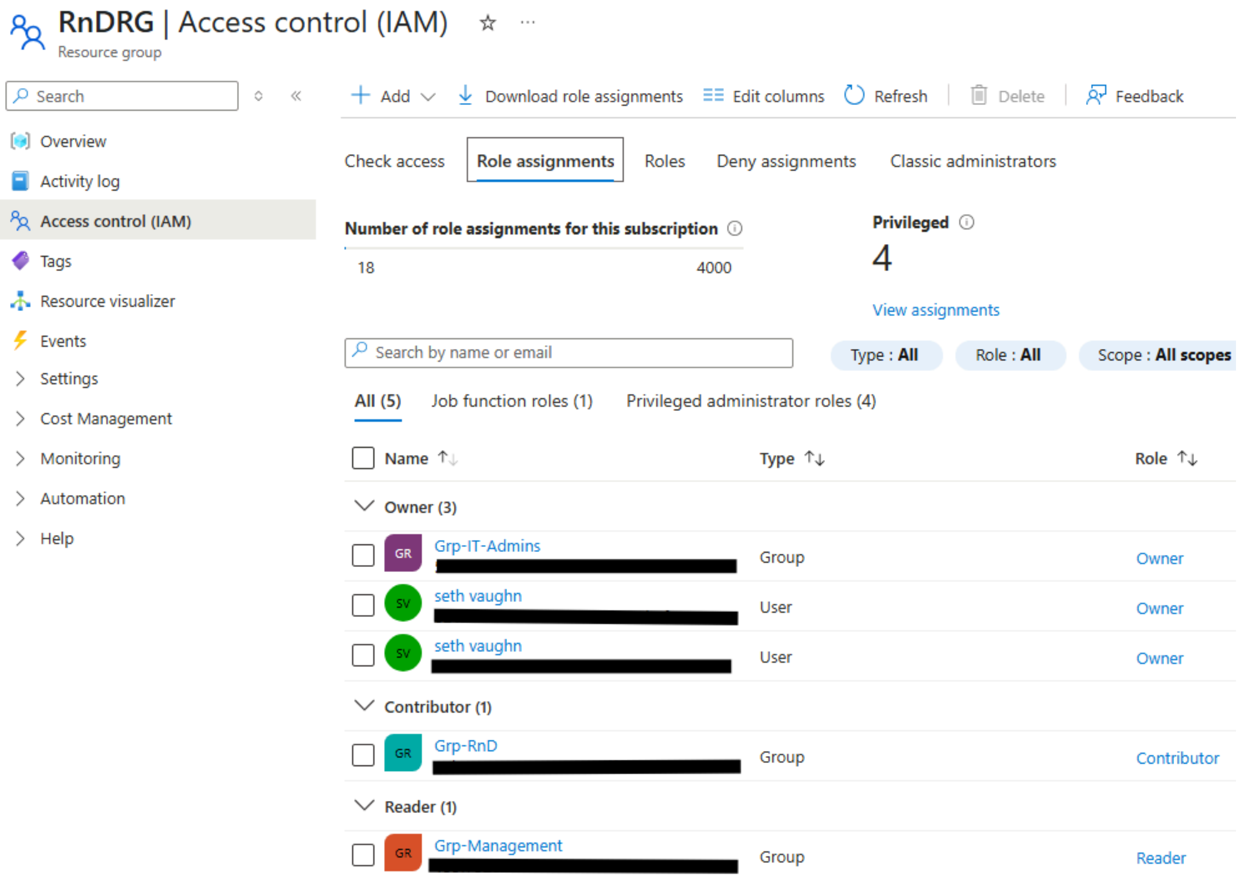
- Rationale for Group-based assignment

This project follows an Azure RBAC-recommended practice of using group-based role assignments rather than giving responsibilities to specific individuals. By assigning roles to Azure AD groups, it makes access management simpler, more scalable, and easier to maintain. For example, when a new employee enters or departs from a department, access can be provided or revoked simply by adding or removing them from the group. This approach improves security by reducing human error, ensuring consistent permission across team members and aligns with real-world enterprise practices where access is linked to department or job roles rather than individual identities.

Department	Azure AD Group	Resource Group	IAM Roles
Management	Grp-Management	MarketingRG	Reader
Finance	Grp-Finance	FinanceRG	Contributor
Marketing	Grp-Marketing	MarketingRG	Contributor
IT	Grp-IT-Admins	ITRG	Owner
R&D	Grp-RnD	RnDRG	Contributor

Table 1.5: RBAC Role Assignments

Screenshot of Access control (IAM) panel:



RnDRG | Access control (IAM)

Resource group

Number of role assignments for this subscription: 18 / 4000

Privileged: 4

View assignments

Name	Type	Role
Owner (3)		
Grp-IT-Admins [redacted]	Group	Owner
seth vaughn [redacted]	User	Owner
seth vaughn [redacted]	User	Owner
Contributor (1)		
Grp-RnD [redacted]	Group	Contributor
Reader (1)		
Grp-Management [redacted]	Group	Reader

Figure 1.7: Shows the Access Control panel for the Research & Development resource group. It comprises three role assignments, which include the IT admins and me who own the resource group, the contributing members within the R&D AD Group, who shall act as contributors in this environment, as well as a reader for Management.

1.4. Enforce Multi-Factor Authentication (MFA)

Objective: Enforce MFA for specific departments using Azure Conditional Access

- Group users who require MFA

Department	MFA Required?	Rationale
Management	Yes	High privilege, confidential
Finance	Yes	Financial data & compliance risk
Marketing	No	Public-facing assets (low impact)
IT	Yes	Admins, full access to all RGs
R&D	Yes	Codebase, CI/CD pipelines

Table 1.6: MFA Requirement for each department

- Limitation

Due to the use of an Azure Free Tier, I was unable to perform conditional access rules, which are necessary to selectively enforce MFA. To perform this, I would require an Azure AD Premium P1 or P2 licence.

- MFA Simulation

With Azure AD Premium, the following steps would have been followed:

1. Targeted AD Groups for MFA Enforcement:
    - Grp-Management
    - Grp-Finance
    - Grp-IT-Admins
    - Grp-Rnd
2. Policy Configuration:
    - Policy Name: “Require MFA for Sensitive Departments
    - Scope: The above AD groups
    - Cloud Apps: All cloud apps
    - Status: Enabled

3. Expected Behaviour:
    - Upon sign-in, users in these groups would be prompted to register for MFA using either the Microsoft Authenticator app, SMS, or a phone call.
    - Users in Marketing would be exempt from being prompted for MFA.

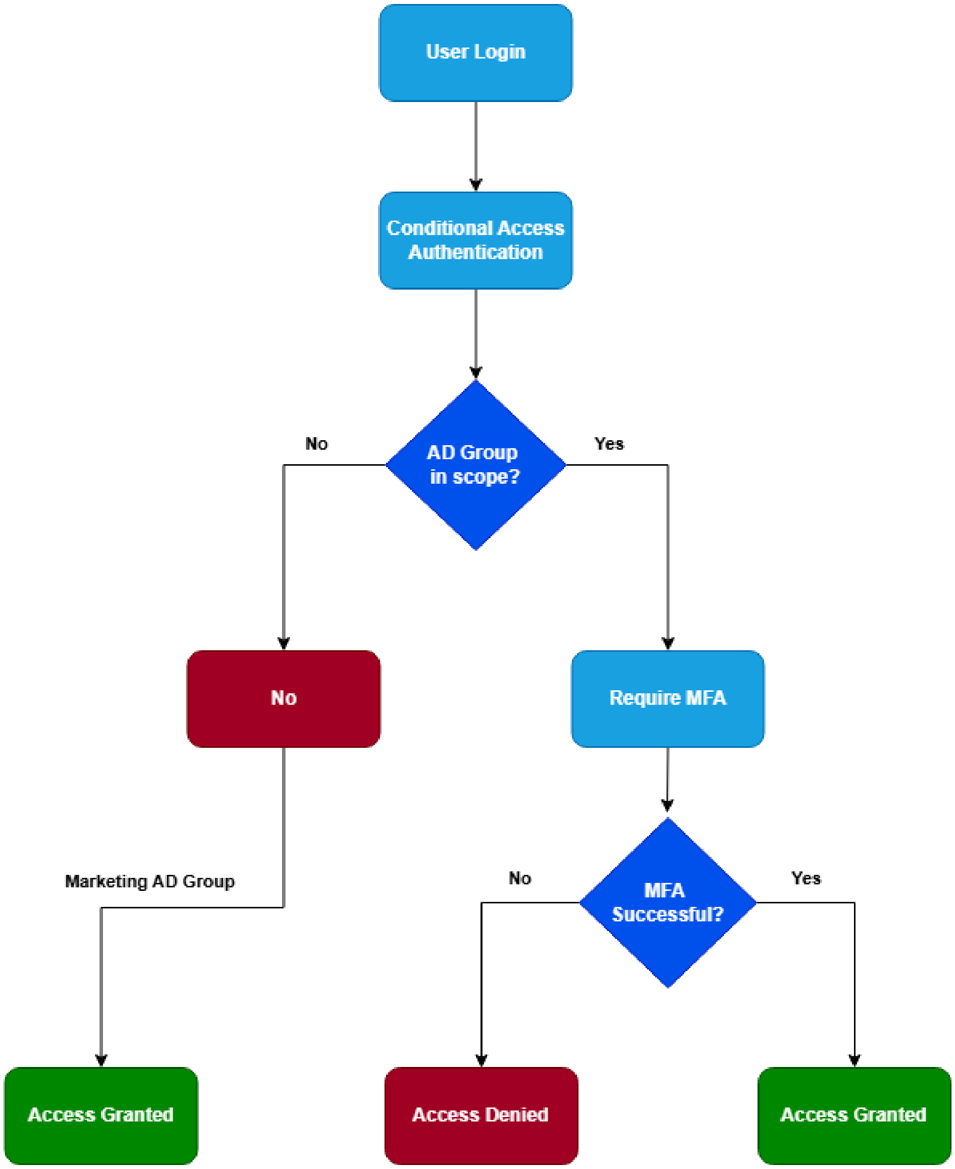


Figure 1.8: Conditional Access Flowchart (AD Group Context)

1.5. IAM Test Cases

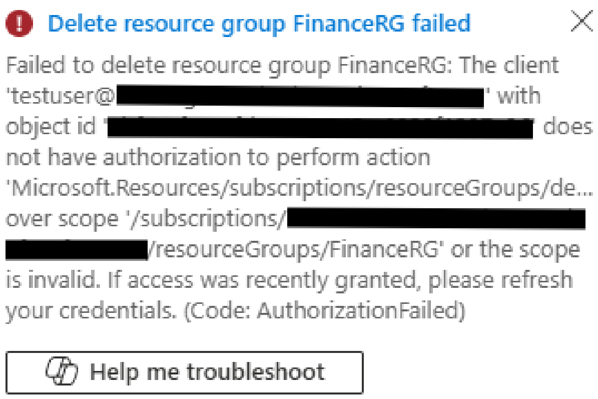
1.5.1. Test Case 1: Reader Role - Grp-Management on MarketingRG

Objective: To validate that users in Grp-Management, assigned the ***Reader*** role on MarketingRG, have view-only access and cannot perform any modifications.

- User: test.user@mydomain.com
- Group: Grp-Management
- Role: **Reader**
- Scope: MarketingRG

Test Step	Expected Result	Actual Result	Pass/Fail
Sign in via the Azure portal	Access granted	Success	Pass ✅
View resources in MarketingRG	Allowed	Success	Pass ✅
Create a new resource	Blocked	Blocked	Pass ✅
Delete a resource	Blocked	Blocked	Pass ✅
Edit Resource	Blocked	Blocked	Pass ✅
Assign an IAM role to a user/group	Blocked	Blocked	Pass ✅

*Table 1.7: Confirms that **Reader** access behaves as intended. Management users were only able to view resources, but were unable to modify or manage them.*



Delete resource group FinanceRG failed

Failed to delete resource group FinanceRG: The client 'testuser@[redacted]' with object id '[redacted] does not have authorization to perform action 'Microsoft.Resources/subscriptions/resourceGroups/de... over scope '/subscriptions/[redacted]/resourceGroups/FinanceRG' or the scope is invalid. If access was recently granted, please refresh your credentials. (Code: AuthorizationFailed)

Figure 1.9: Attempted deletion of FinanceRG from a Grp-Management user

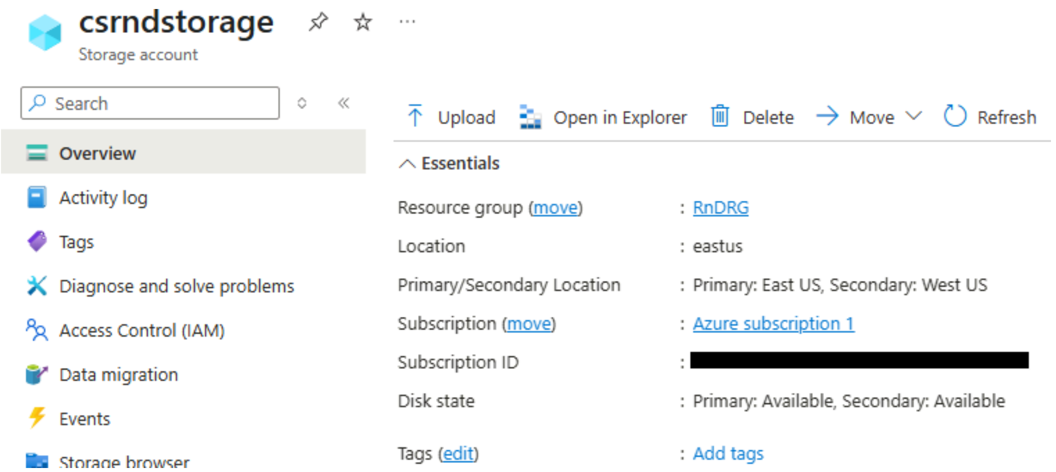
1.5.2. Test Case 2: Contributor Role - Grp-RnD on RnDRG

Objective: To confirm that users in Grp-RnD assigned the ***Contributor*** role on RnDRG can manage resources, but not assign roles.

- User: test.user@mydomain.com
- Group: Grp-RnD
- Role: **Contributor**
- Scope: RnDRG

Test Step	Expected Result	Actual Result	Pass/Fail
Sign in to Azure portal	Access granted	Success	Pass ✅
View and navigate resources in RG	Allowed	Success	Pass ✅
Create a new storage account	Allowed	Success	Pass ✅
Modify resource settings	Allowed	Success	Pass ✅
Delete a resource	Allowed	Success	Pass ✅
Assign an IAM role to a user/group	Blocked	Blocked	Pass ✅

*Table 1.8: Confirms that the **Contributor** role allows full resource management, excluding IAM access (RBAC).*



Resource group (move) : RnDRG

Location : eastus

Primary/Secondary Location : Primary: East US, Secondary: West US

Subscription (move) : Azure subscription 1

Subscription ID : [redacted]

Disk state : Primary: Available, Secondary: Available

Tags (edit) : Add tags

Figure 1.10: Successful creation of a storage account for the RnDRG

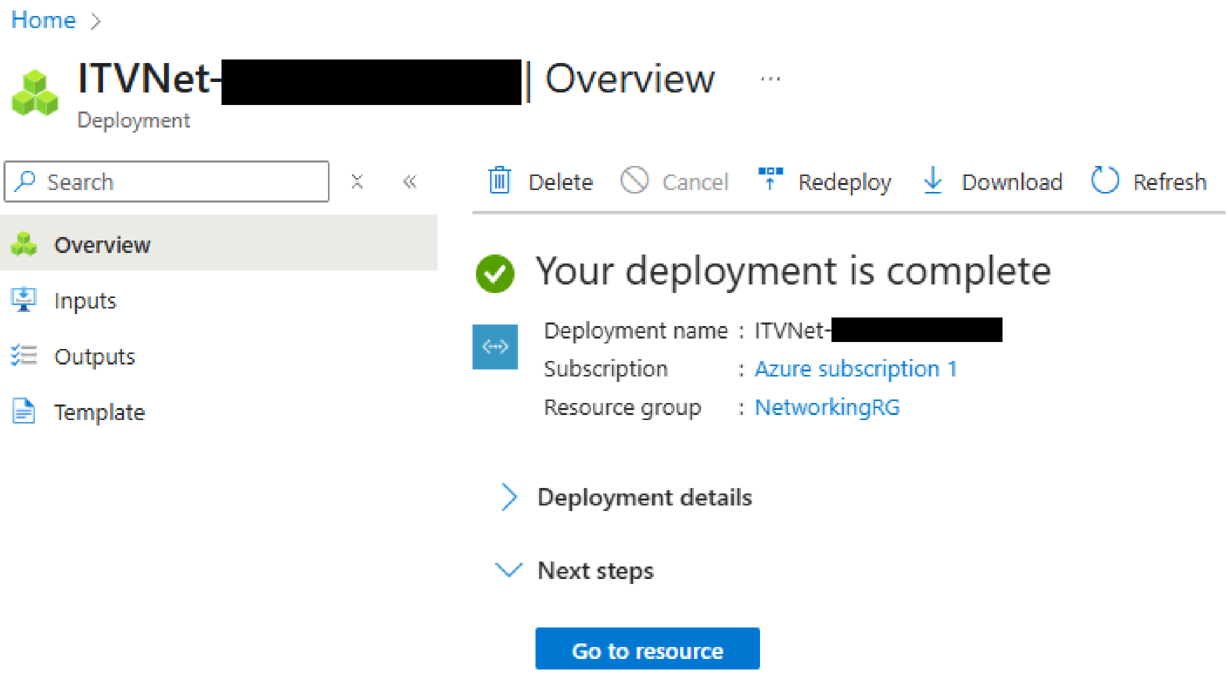
1.5.3. Test Case 3: Owner Role - Grp-IT-Admins on ITRG

Objective: To confirm that IT Admins assigned the ***Owner*** role on ITRG can fully manage resources and assign IAM roles.

- User: test.user@mydoamin.com
- Group: Grp-IT-Admins
- Role: **Owner**
- Scope: ITRG

Test Step	Expected Result	Actual Result	Pass/Fail
Sign in to Azure portal	Access granted	Success	Pass ✅
Create new resources in ITRG	Allowed	Success	Pass ✅
Modify and delete resources	Allowed	Success	Pass ✅
Assign an IAM role to a user/group	Allowed	Success	Pass ✅

*Table 1.9: Confirms the **Owner** role provides full access to resources and assignment of roles*



ITVNet-[redacted] | Overview ...

Deployment

Your deployment is complete

Deployment name : ITVNet-[redacted]
Subscription : Azure subscription 1
Resource group : NetworkingRG

Figure 1.11: IT admin user successfully created a Virtual Network in ITRG.

1.5.4. Test Case 4: MFA Simulation - Management, IT, Finance and R&D

Objective: To simulate the enforcement of MFA for sensitive departments via Conditional Access policies, despite the free-tier limitation in Azure.

Targeted Groups:

- Grp-Management
- Grp-Finance
- Grp-IT-Admins
- Grp-RnD

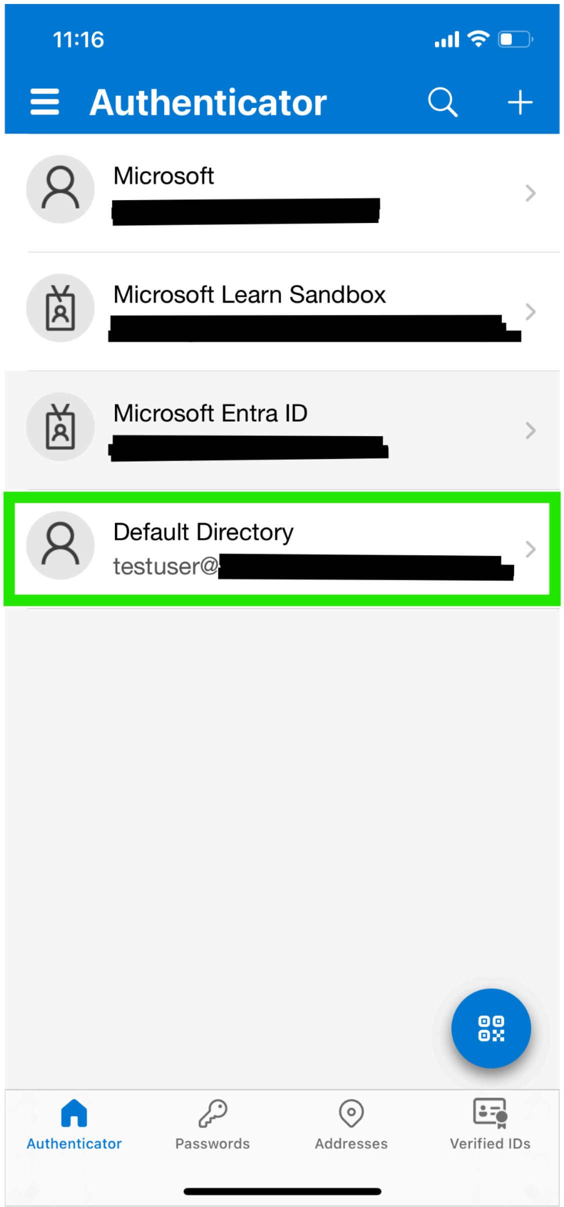
Method:

- Conditional Access (Simulated)

Test Step	Expected Result	Actual Result	Pass/Fail
Apply Conditional Access to AD groups	Policy created and enforced	Not Implemented (Free Tier)	Simulated ✅
Attempt login from IT user	Promoted for MFA	Simulated via Security Defaults	Simulated ✅
Attempt login from RnD user	Prompted for MFA	Simulated via Security Defaults	Simulated ✅
Attempt login from Marketing user	No MFA prompt	Simulated (Not Enforced	Simulated ✅

Table 1.10: Conditional Access per MFA requirement

Note:
Due to free-tier limitations, Conditional Access and MFA enforcement could not be directly implemented. The policy design was documented and would be applied in a licensed production environment.



Microsoft
[redacted]

Microsoft Learn Sandbox
[redacted]

Microsoft Entra ID
[redacted]

Default Directory
testuser@[redacted]

Table 1.12: Microsoft Authenticator app confirming that the testuser@mydomain.com has been registered for MFA under my Default Directory.

Note:

- While Conditional Access could not be configured due to licensing limitations, MFA enforcement was still triggered using Microsoft's Security Defaults, which apply tenant-wide MFA for all users.
- This screenshot helps support the idea that MFA registration was completed for the test user in the Azure environment.

2. Phase 2 Objectives — Network Segmentation & Security Infrastructure

1. Design and Deploy Azure Virtual Network (VNet)

- Define address space
- Plan and create departmental subnets

2. Segment Departments Using Subnets

- One subnet per department
- Ensure future scalability

3. Create and Apply Network Security Groups (NSGs)

- One NSG per subnet
- Define inbound/outbound rules per department
- Implement custom rules for cross-subnet access and admin exceptions

4. Deploy Virtual Machines (VMs) for Testing

- One VM per subnet (where applicable)
- Associate VMs with the correct subnets and NSGs
- Remove auto-created NSGs from NICs (VM)

5. Test NSG Rules Across Subnets

- Validate that rules permit/deny traffic as expected
- Use PowerShell for testing access
- Verify access for Admin IPs and ITVM

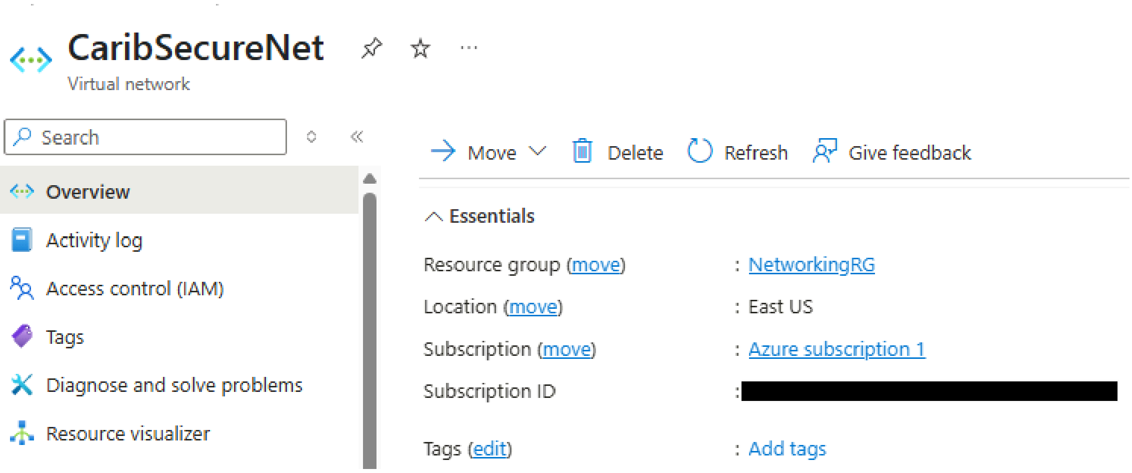
2.1. Design and Deploy Azure Virtual Network (VNet)

Objective: Create a scalable virtual network to serve as a foundation for subnet segmentation and secure communication between departments.

Configuration Summary Table

Setting	Value
VNet Name	CaribSecureNet
Region	East US
Address Space	10.0.0.0/16
Subnet Count	6
Subnet Addressing	/24 block per dept.

Table 2.1: CaribSecureNet was created in the East US region to provide an isolated and secure environment for deploying Azure resources. Although the organisation currently has fewer than 100 employees, the VNet uses an address space of 10.0.0.0/16, which allows for up to 256 (/24) subnets, offering flexibility and room for organisational growth, better separation of duties, and scalable design. With this address range, it is ideal for segmenting departments and enforcing access boundaries using subnet-level Network Security Groups (NSGs). Each department will be assigned its subnet to support network isolation and Zero Trust architecture principles.



Resource group (move) : NetworkingRG

Location (move) : East US

Subscription (move) : Azure subscription 1

Subscription ID : [redacted]

Tags (edit) : Add tags

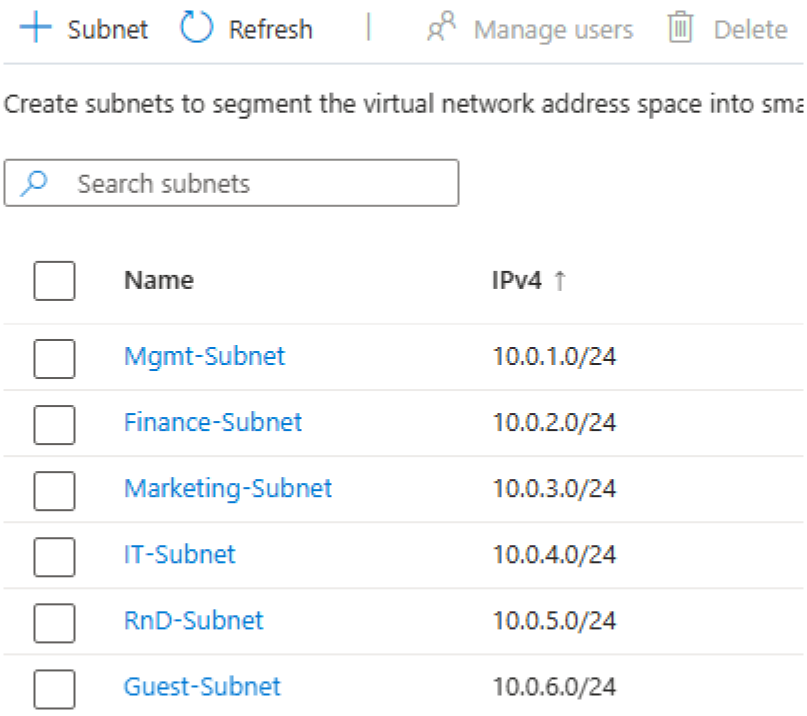
Figure 2.1: CaribSecureNet Virtual Network

2.2. Segment Departments Using Subnets

Objective: Logically separate departments using dedicated subnets to support Zero Trust principles and subnet-level security.

Subnet Name	Address Range	Department
Mgmt-Subnet	10.0.1.0	Management
Finance-Subnet	10.0.2.0	Finance
Marketing-Subnet	10.0.3.0	Marketing
IT-Subnet	10.0.4.0	IT
RnD-Subnet	10.0.5.0	R&D
Guest-Subnet	10.0.6.0	Guest Wi-Fi

Table 2.2: Subnet Configuration



Create subnets to segment the virtual network address space into sma

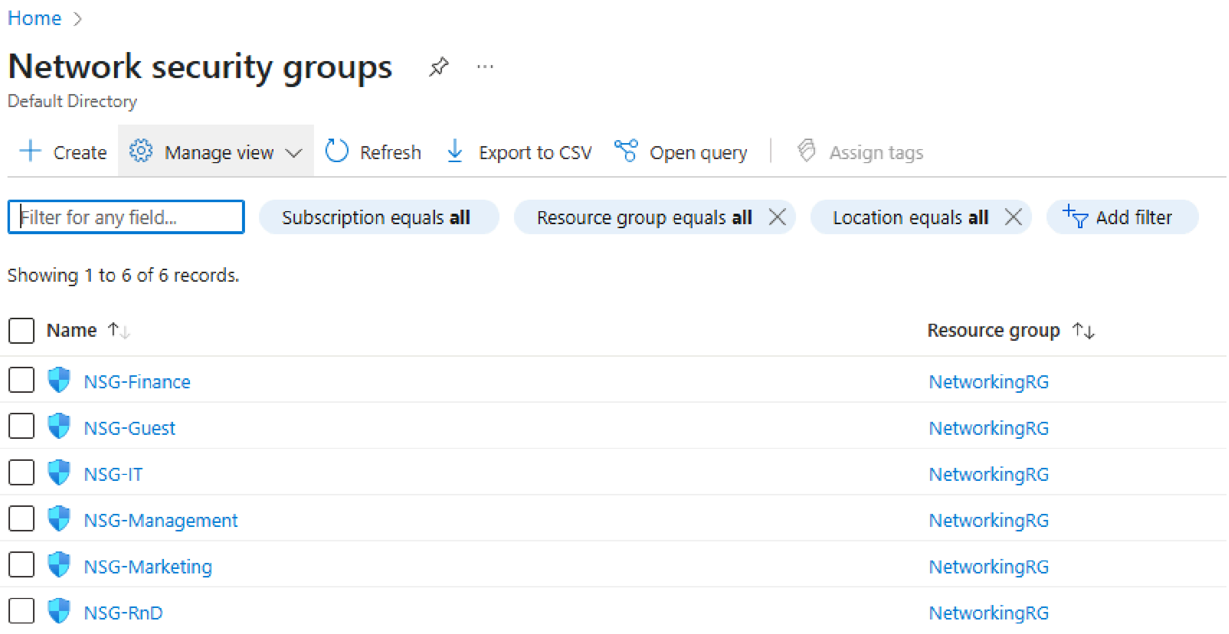
□	Name	IPv4 ↑
□	Mgmt-Subnet	10.0.1.0/24
□	Finance-Subnet	10.0.2.0/24
□	Marketing-Subnet	10.0.3.0/24
□	IT-Subnet	10.0.4.0/24
□	RnD-Subnet	10.0.5.0/24
□	Guest-Subnet	10.0.6.0/24

Figure 2.2: Subnet layout within CaribSecureNet VNet

2.3. Create and Apply Network Security Groups (NSGs)

2.3.1. Create Network Security Groups

Objective: Control traffic between and within subnets using NSGs, with custom rules for administrative access and inter-departmental isolation.



Subscription equals **all**

Resource group equals **all**

Location equals **all**

Showing 1 to 6 of 6 records.

Name	Resource group
NSG-Finance	NetworkingRG
NSG-Guest	NetworkingRG
NSG-IT	NetworkingRG
NSG-Management	NetworkingRG
NSG-Marketing	NetworkingRG
NSG-RnD	NetworkingRG

Figure 2.3: Each NSG is configured to allow or deny traffic based on the needs of each department

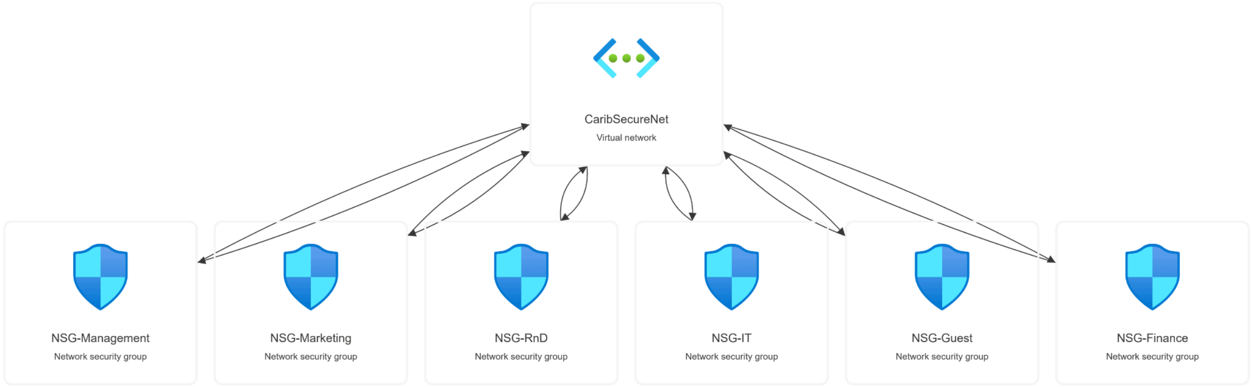


Figure 2.4: CaribSecure Virtual Network Diagram

2.3.2. Azure NSG Default Rules

2.3.2.1. Default Inbound rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancer	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Purpose for each

- **AllowVnetInBound**

Allows communications between VMs and services running on the same virtual network. Without this, internal traffic between subnets or virtual machines would be blocked.

- **AllowAzureLoadBalancer**

Allows traffic from Azure's internal load balancer, which is utilised for distribution and health probes.

- **DenyAllInBound**

Blocks any traffic that isn't explicitly allowed above. It aims to prevent unintended external access.

2.3.2.2. Default Outbound Rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Purpose for each

- **AllowVnetOutBound**

Allows communications between VMs and services running on the same virtual network. Without this, internal traffic between subnets or virtual machines would be blocked.

- **AllowInternetOutBound**

Allows VMs to access the public Internet for browsing, downloading software, updates, etc. This is critical for communication and updates.

- **DenyAllOutBound**

Blocks all outbound traffic that wasn’t previously allowed above. This prevents any accidental data leakage or unintended external connections.

2.3.3. My Custom NSG Rules

1. <u>Management NSG</u>

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow-IT-RDP	3389	TCP	10.0.4.0/24	10.0.1.0/24	Allow
110	Allow-RnD	Any	Any	10.0.5.0/24	10.0.1.0/24	Allow
120	Allow-Mgmt	Any	Any	10.0.1.0/24	10.0.1.0/24	Allow
200	Deny-Finance	Any	Any	10.0.2.0/24	10.0.1.0/24	Deny
210	Deny-Marketing	Any	Any	10.0.3.0/24	10.0.1.0/24	Deny
220	Deny-Guest	Any	Any	10.0.6.0/24	10.0.1.0/24	Deny

2. <u>Finance NSG</u>

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow-IT-RDP	3389	TCP	10.0.4.0/24	10.0.2.0/24	Allow
110	Allow-Finance	Any	Any	10.0.2.0/24	10.0.2.0/24	Allow
200	Deny-RnD	Any	Any	10.0.5.0/24	10.0.2.0/24	Deny
210	Deny-Marketing	Any	Any	10.0.3.0/24	10.0.2.0/24	Deny
220	Deny-Mgmt	Any	Any	10.0.1.0/24	10.0.2.0/24	Deny
230	Deny-Guest	Any	Any	10.0.6.0/24	10.0.2.0/24	Deny

3. Marketing NSG

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow-IT-RDP	3389	TCP	10.0.4.0/24	10.0.3.0/24	Allow
110	Allow-Marketing	Any	Any	10.0.3.0/24	10.0.3.0/24	Allow
200	Deny-Mgmt	Any	Any	10.0.1.0/24	10.0.3.0/24	Deny
210	Deny-Finance	Any	Any	10.0.2.0/24	10.0.3.0/24	Deny
220	Deny-RnD	Any	Any	10.0.5.0/24	10.0.3.0/24	Deny
230	Deny-Guest	Any	Any	10.0.6.0/24	10.0.3.0/24	Deny

4. IT NSG

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow-IT	Any	Any	10.0.4.0/24	10.0.4.0/24	Allow
110	Allow-AdminIP	3389	TCP	My IP Address	10.0.4.0/24	Allow

5. RnD NSG (Research & Development)

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow-Mgmt	Any	Any	10.0.1.0/24	10.0.5.0/24	Allow
110	Allow-IT-RDP	3389	TCP	10.0.4.0/24	10.0.5.0/24	Allow
120	Allow-RnD	Any	Any	10.0.5.0/24	10.0.5.0/24	Allow
130	Allow-Admin-RDP	3389	TCP	My IP Address	10.0.5.0/24	Allow
200	Deny-Finance	Any	Any	10.0.2.0/24	10.0.5.0/24	Deny
210	Deny-Marketing	Any	Any	10.0.3.0/24	10.0.5.0/24	Deny
220	Deny-Guest	Any	Any	10.0.6.0/24	10.0.5.0/24	Deny

6. Guest NSG

Inbound Rules

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow-Internet	443	TCP	Any	Any	Allow
110	Allow-Guest	Any	Any	10.0.5.0/24	10.0.6.0/24	Allow
120	Allow-Admin-RDP	3389	TCP	My IP Address	10.0.6.0/24	Allow
200	Deny-VNet	Any	Any	10.0.0.0/24	10.0.6.0/24	Deny

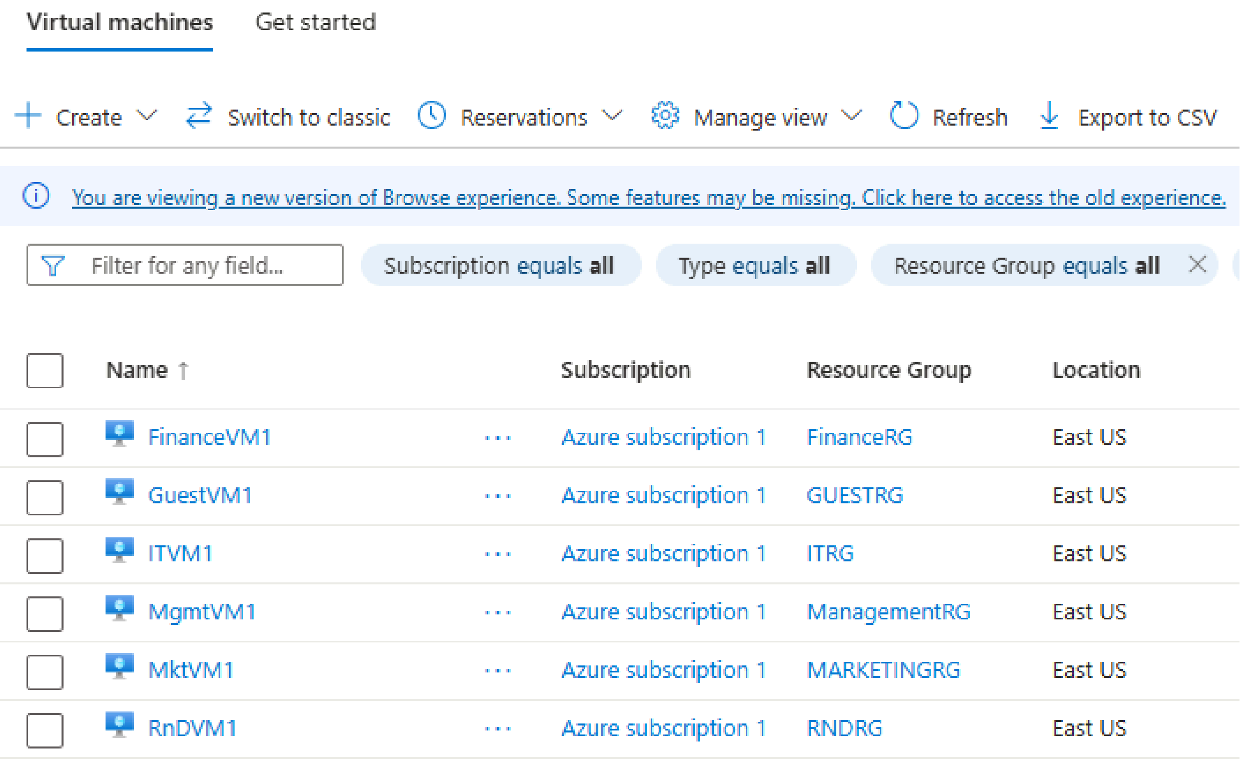
Outbound Rules

Priority	Name	Port	Protocol	Source	Destination	Action
100	Deny-Internal	Any	Any	10.0.6.0/24	10.0.0.0/16	Deny
110	Allow-Internet-Outbound	443	TCP	10.0.6.0/24	Any	Allow

2.4. Deploy Virtual Machines (VMs) for Testing

Objective: Deploy VMs across subnets to simulate department workloads and validate NSG rules.

- Create VMs



You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.

Subscription equals **all** | Type equals **all** | Resource Group equals **all**

□	Name ↑		Subscription	Resource Group	Location
□	FinanceVM1	···	Azure subscription 1	FinanceRG	East US
□	GuestVM1	···	Azure subscription 1	GUESTRG	East US
□	ITVM1	···	Azure subscription 1	ITRG	East US
□	MgmtVM1	···	Azure subscription 1	ManagementRG	East US
□	MktVM1	···	Azure subscription 1	MARKETINGRG	East US
□	RnDVM1	···	Azure subscription 1	RNDRG	East US

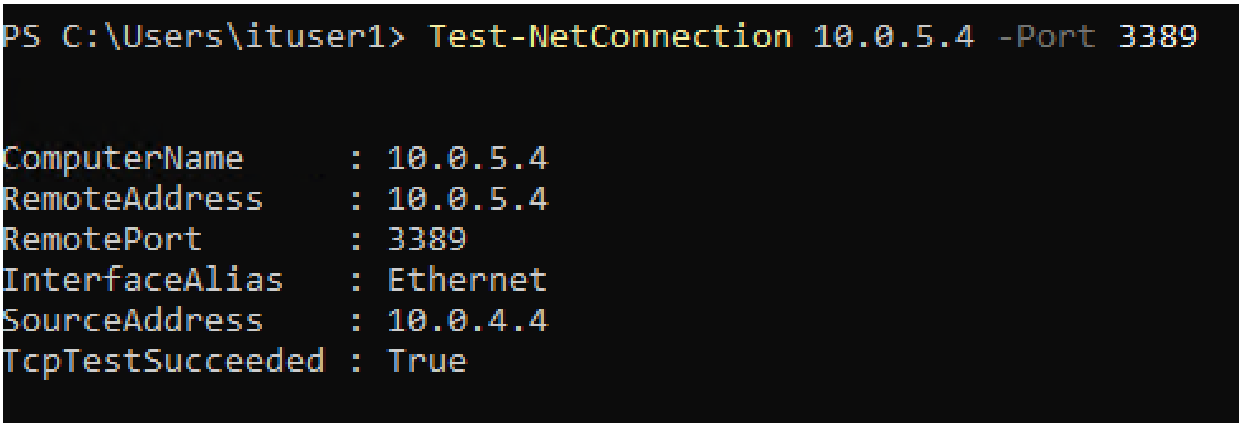
Figure 2.5: VM Deployment per subnet

2.5. Test NSG Rules Across Subnets

2.5.1. Test Case 1 - ITVM Can RDP into RnDVM

Objective: Verify that the IT department can access R&D over RDP (port 3389), based on the *Allow-IT-RDP* rule in the RnD NSG.

Step	Expected Result	Actual Result	Pass/Fail
Log in to ITVM	Success	Success	Pass ✅
Run **Test-NetConnection 10.0.5.4 -Port 3389**	TCP test succeeds	Succeeded	Pass ✅
RDP from ITVM to RnDVM	RDP connects successfully	Connected	Pass ✅



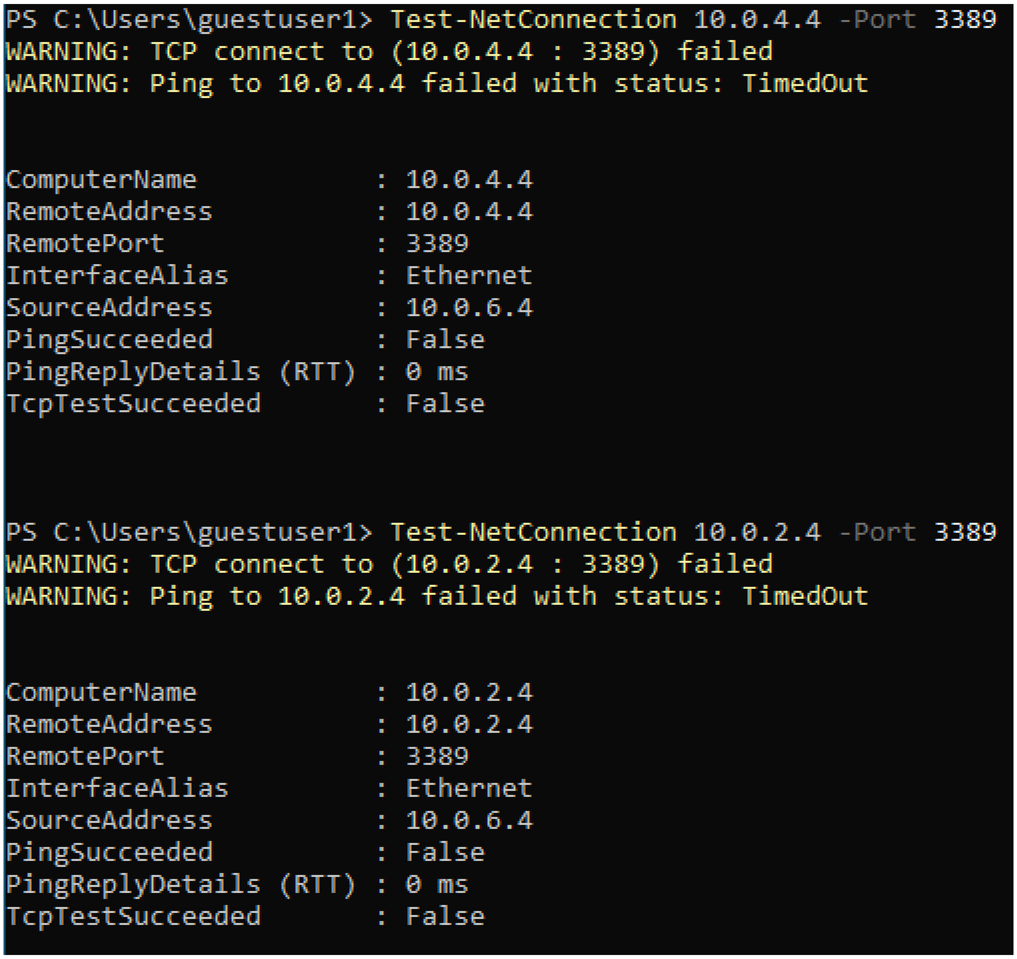
```
PS C:\Users\ituser1> Test-NetConnection 10.0.5.4 -Port 3389


ComputerName     : 10.0.5.4
RemoteAddress    : 10.0.5.4
RemotePort       : 3389
InterfaceAlias   : Ethernet
SourceAddress    : 10.0.4.4
TcpTestSucceeded : True
```

Figure 2.6: PowerShell output showing successful RDP test from ITVM to RnDVM

2.5.2. Test Case 2 - GuestVM Cannot Access Internal Subnets

Objective: Ensure the Guest subnet (10.0.6.0/24) cannot communicate with internal subnets (e.g IT, Finance).

Step	Expected Result	Actual Result	Pass/Fail
Log in to GuestVM	Success	Succes	Pass ✅
Run **Test-NetConnection 10.0.4.4 -Port 3389** (ITVM)	TCP test fails	Failed	Pass ✅
Run **Test-NetConnection 10.0.2.4 -Port 3389** (FinanceVM)	TCP test fails	Failed	Pass ✅



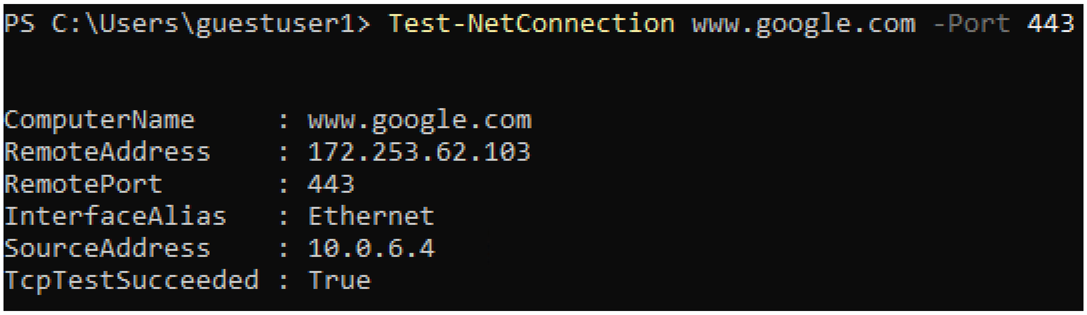
```
PS C:\Users\guestuser1> Test-NetConnection 10.0.4.4 -Port 3389
WARNING: TCP connect to (10.0.4.4 : 3389) failed
WARNING: Ping to 10.0.4.4 failed with status: TimedOut


ComputerName           : 10.0.4.4
RemoteAddress          : 10.0.4.4
RemotePort             : 3389
InterfaceAlias         : Ethernet
SourceAddress          : 10.0.6.4
PingSucceeded          : False
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded       : False



PS C:\Users\guestuser1> Test-NetConnection 10.0.2.4 -Port 3389
WARNING: TCP connect to (10.0.2.4 : 3389) failed
WARNING: Ping to 10.0.2.4 failed with status: TimedOut


ComputerName           : 10.0.2.4
RemoteAddress          : 10.0.2.4
RemotePort             : 3389
InterfaceAlias         : Ethernet
SourceAddress          : 10.0.6.4
PingSucceeded          : False
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded       : False
```

Figure 2.7: PowerShell output from Guest VM showing failed connections to IT and Finance, respectively.

2.5.3. Test Case 3 - GuestVM Can Access the Internet

Objective: Ensure Guest VM can access external internet services (e.g., port 443), simulating public Wi-Fi behaviour.

Step	Expected Result	Actual Result	Pass/Fail
Log in to GuestVM	Success	Success	Pass ✅
Run Test-NetConnection www.google.com -Port 443	TCP test succeeds	Success	Pass ✅
Open a browser to google.com	Page loads	Page loads	Pass ✅



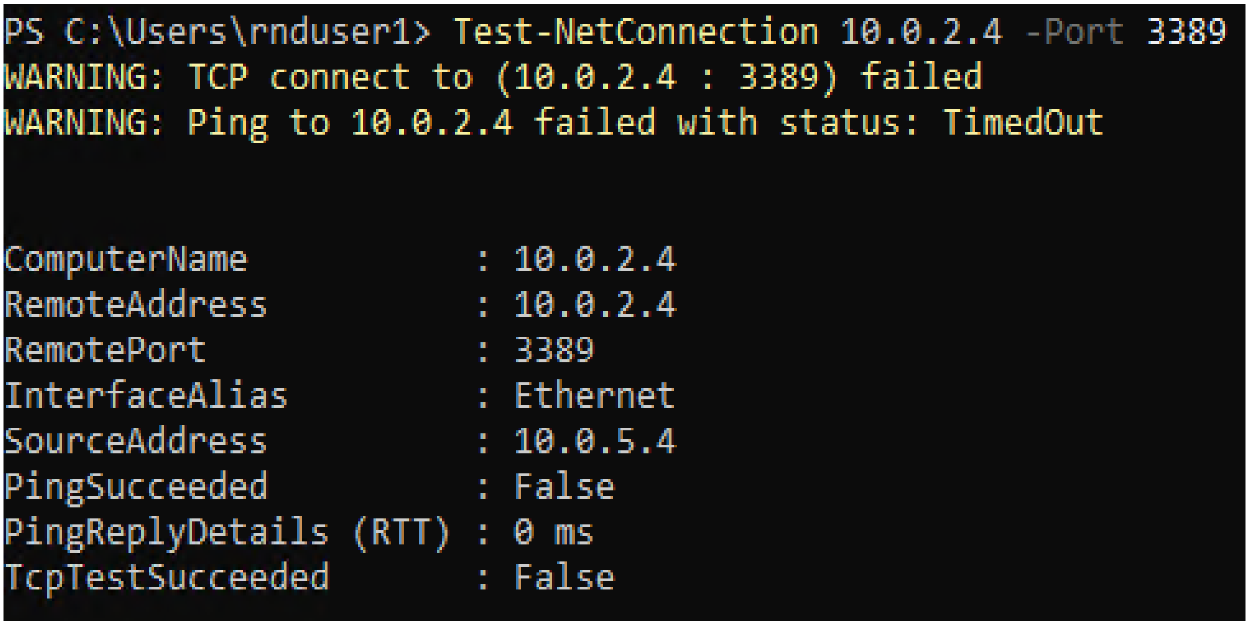
```
PS C:\Users\guestuser1> Test-NetConnection www.google.com -Port 443


ComputerName     : www.google.com
RemoteAddress    : 172.253.62.103
RemotePort       : 443
InterfaceAlias   : Ethernet
SourceAddress    : 10.0.6.4
TcpTestSucceeded : True
```

Figure 2.8: PowerShell test showing internet access from GuestVM

2.5.4. Test Case 4 - RnDVM Cannot Access Finance Subnet

Objective: Verify that RnD subnet (10.0.5.0/24) cannot access the Finance subnet (10.0.2.0/24).

Step	Expected Result	Actual Result	Pass/Fail
Log in to RnDVM	Success	Success	Pass ✅
Run **Test-NetConnection 10.0.2.4 -Port 3389**	TCP test fails	Failed	Pass ✅
Attempt ping or any other connection	Failed	Failed	Pass ✅



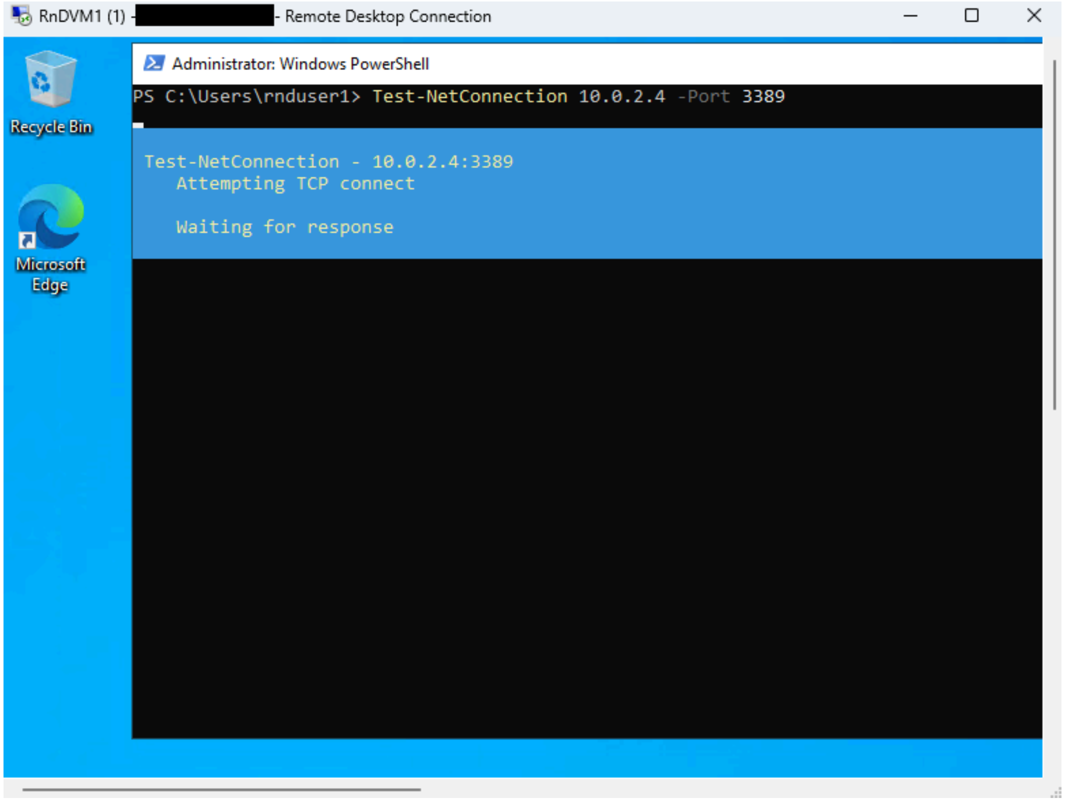
```
PS C:\Users\rnduser1> Test-NetConnection 10.0.2.4 -Port 3389
WARNING: TCP connect to (10.0.2.4 : 3389) failed
WARNING: Ping to 10.0.2.4 failed with status: TimedOut


ComputerName           : 10.0.2.4
RemoteAddress          : 10.0.2.4
RemotePort             : 3389
InterfaceAlias         : Ethernet
SourceAddress          : 10.0.5.4
PingSucceeded          : False
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded       : False
```

Figure 2.9: PowerShell output from RnDVM showing blocked connection to Finance.

2.5.5. Test Case 5 - Admin IP Can RDP into RnD and IT

Objective: To confirm that the administrator’s public IP address can access RnDVM and ITVVM over RDP (port 3389), based on the Allow-Admin-RDP rule configured for the respective NSG.

Step	Expected Result	Actual Result	Pass/Fail
Ensure NSG rule Allow-Admin-RDP is present in NSG-IT	Confirmed	Confirmed	Pass ✅
Ensure NSG rule Allow-Admin-RDP is present in NSG-RnD	Confirmed	Confirmed	Pass ✅
Connect to ITVM from Admin PC using RDP	RDP connects successfully	RDP session launched	Pass ✅
Connect to RnDVM from Admin PC using RDP	RDP connects successfully	RDP session launched	Pass ✅



RnDVM1 (1) - [redacted] - Remote Desktop Connection

Administrator: Windows PowerShell

```
PS C:\Users\rnduser1> Test-NetConnection 10.0.2.4 -Port 3389

Test-NetConnection - 10.0.2.4:3389
   Attempting TCP connect

   Waiting for response
```

Figure 2.10: Screenshot showing successful RDP login from Admin IP into RnDVM. Shows the admin attempting a TCP connection to FinanceVM.