

Implementation of Secure Network Infrastructure Using Azure Firewall

Created by: N'mai Lamine Kaba.

E-mail: laminkevin@yahoo.fr

Tel: +44 7442701850

Linkedin: <https://www.linkedin.com/in/n-mai-lamine-kaba-5b28ba32/>

YouTube: www.youtube.com/@CybersecJourneywithLamine

Introduction:

In today's digital era, securing network infrastructure is a critical task for any organization. This project focuses on building a robust and secure network infrastructure on Microsoft Azure using Azure Firewall. By implementing multiple virtual networks (VNets) with VNet peering, configuring Azure Firewall with specific rules, and setting up comprehensive logging and monitoring, we aim to ensure a secure and efficient network environment.

Project Overview:

1) Design and Deploy Secure Network Infrastructure:

- Create and configure multiple virtual networks (VNets) with specific address spaces.
- Establish VNet peering to enable communication between VNets.

2) Implement Azure Firewall:

- Deploy Azure Firewall and configure custom network, application, and DNAT rules to control traffic flow and protect network resources.
- Set up internal and external virtual machines and configure secure routing through the firewall.

3) Utilize Azure Bastion for Secure Access:

- Deploy Azure Bastion to provide secure and seamless RDP access to virtual machines without exposing public IPs.

4) Integrate Azure Log Analytics:

- Set up an Azure Log Analytics Workspace to collect and analyze logs from the Azure Firewall and other network resources.
- Use KQL (Kusto Query Language) to query and visualize firewall logs for better insights and decision-making.

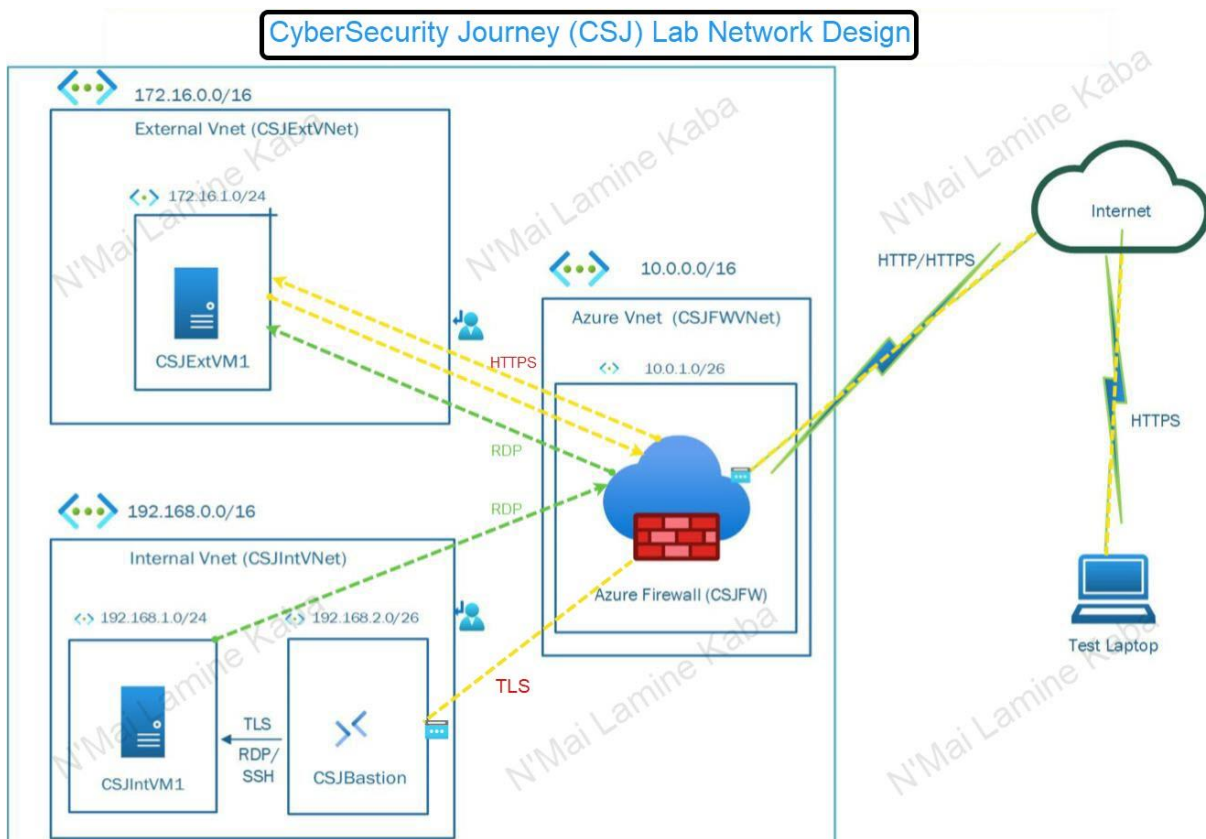
5) Test and Validate Security Configurations:

- Perform connectivity tests to ensure proper routing and firewall rule enforcement.
- Validate that the firewall rules are correctly blocking or allowing traffic as intended.

Prerequisites:

1. Azure Subscription: Have an active Azure subscription.
2. Azure Portal Access: Be familiar with the Azure portal.
3. Expected level: Have at least a foundational level of Microsoft Azure

Lab diagram:



Lab Steps:

Step 1: Create a Resource Group

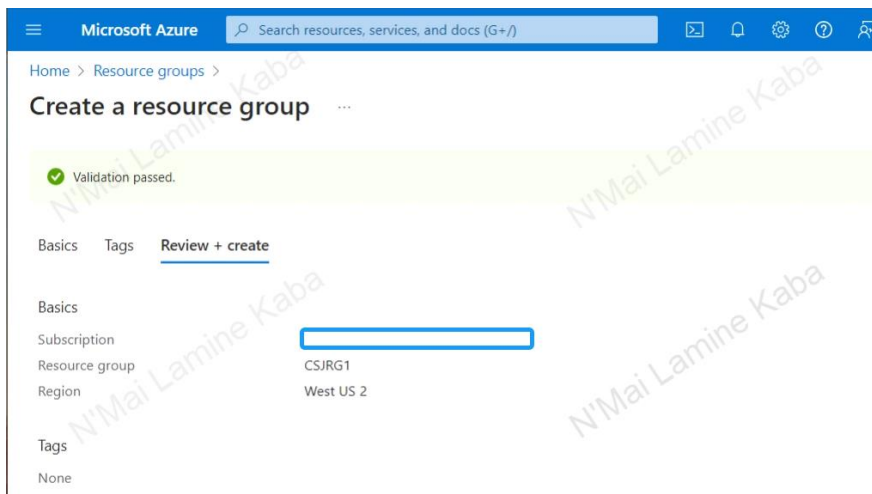
Navigate to **Resource Groups** in the Azure portal.

Click + **Create**.

Enter the Resource Group Name: **`CSJRG1`**

Select the Region: **`West US 2`**

Click **Review + Create** and then Create.



Step 2: Set Up Firewall Virtual Network (VNet)

Go to Virtual Networks and click + **Create**.

Enter the following details:

- Subscription: **Choose your subscription**
- Resource Group: **`CSJRG1`**
- Name: **`CSJFWVNet`**
- Region: **`West US 2`**
- Address Space: **`10.0.0.0/16`**

Home > Virtual networks >

Create virtual network ...

Basics Security IP addresses Tags Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Instance details

Virtual network name *

Region * [Deploy to an Azure Extended Zone](#)

[Previous](#) [Next](#) [Review + create](#)

Under **IP addresses** tab, Click **+ Add a subnet**.

Enter the following details:

- Subnet Purpose: Select **Azure FirewallSubnet**
- Check Include an IPv4 address space
- Starting Address: **10.0.1.0**

Click **Review + Create** and then **Create**.

Microsoft Azure Search resources, services, and docs (G+/)

Home > Virtual networks > Create virtual network

Add a subnet

Basics Security

[Add IPv4 address](#)

10.0.0.0/16

10.0.0.0

10.0.0.0 - 10.0.255.255

[+ Add a subnet](#)

Subnets

default

[A NAT gateway gateway. Learn more](#)

[Previous](#) [Add](#) [Cancel](#)

IPv4

Include an IPv4 address space ☒

IPv4 address range * 10.0.0.0 - 10.0.255.255

Starting address *

Size

Subnet address range

IPv6

Include an IPv6 address space ☐ This virtual network has no IPv6 address ranges.

Private subnet [PREVIEW](#)

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Enable private subnet (no default outbound access) ☐

[This setting can't be changed after the subnet is created](#)

Step 3: Deploy Azure Firewall

From the Azure portal, search/navigate to **Firewalls** and click + **Create**

Enter the following details:

- Subscription: **Choose your subscription**
- Resource Group: **`CSJRG1`**
- Name: **`CSJFW`**
- Region: **`West US 2`**
- Availability: **`None`**
- Firewall SKU: **`Standard`**

Under **Firewall management**:

- Select **Use firewall rules (classic)**

Choose a virtual network: **`Use existing`**

Under Virtual Network:

- Select **CSJFWVNet**

Public IP address: Add New, Name: `CSJPIP`, OK

Click **Review + Create** and then **Create**.

The screenshot shows the 'Create a firewall' page in the Azure portal, specifically the 'Review + create' tab. The page displays a summary of the configuration details for the firewall. A green checkmark indicates that validation has passed. The configuration details are as follows:

Resource type	Name	Value
Subscription		CSJRG1
Resource group		West US 2
Region		Standard
Azure Firewall Sku		CSJFWVNet
Virtual network		10.0.0.0/16
Address space		CSJPIP
Firewall public IP address		None
Availability zone		

Below the configuration details, there is a section for 'Tags' which shows 'No results'. At the bottom of the page, there are buttons for 'Create', 'Previous', 'Next', and a link to 'Download a template for automation'. A mouse cursor is pointing at the 'Create' button.

Step 4: Create the Internal Virtual Network (VNet)

Go to Virtual Networks and click + **Create**.

Enter the following details:

- Subscription: **Choose your subscription**
- Resource Group: **`CSJRG1`**
- Name: **`CSJIntVNet`**
- Region: **`West US 2`**
- Address Space: **`192.168.0.0/16`**

The screenshot shows the 'Create virtual network' page in the Microsoft Azure portal, specifically the 'IP addresses' tab. The page is for creating a new VNet with the address space 192.168.0.0/16. A subnet named 'default' is already added with the IP range 192.168.0.0 - 192.168.0.255 and a size of /24 (256 addresses). A button '+ Add a subnet' is visible. A note at the bottom states: 'A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. [Learn more](#)'.

Subnets	IP address range	Size	NAT gateway
default	192.168.0.0 - 192.168.0.255	/24 (256 addresses)	-

Click + **Add Subnet**.

Enter the following details:

- Subnet Purpose: Select **`Default`**
- Check Include an IPv4 address space
- Starting Address: - Name: **`Default2`**
- Subnet address range: **`192.168.1.0/24`**

Click **Add**, then **Review + Create**, and then **Create**.

Microsoft Azure Search resources, services, and docs (G+/)

Home > Virtual network > **Add a subnet**

Create virtual network

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates to select services later. [Learn more](#)

Basics Security

Add IPv4 address

Subnet purpose

Name *

IPv4

Include an IPv4 address space ☒

IPv4 address range *

192.168.0.0 - 192.168.255.255

Starting address *

Size

Subnet address range

IPv6

Include an IPv6 address space ☐ This virtual network has no IPv6 address ranges.

Private subnet PREVIEW

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines in the subnet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more](#)

Step 5: Deploy Internal Server in CSJIntVNet

Navigate to **Virtual Machines** and click **+ Create**.

Enter the following details:

- Resource group: **`CSJRG1`**
- Name: **`CSJIntVM1`**
- Region: **`West US 2`**
- Availability Option: **`Availability Zone`**
- Availability Zone: **`Zone 1`**
- Security type: **`Standard`**
- Image: **`Windows Server 2022`**
- Size: **Choose a cost-effective VM size**
- Username: **`CSJAdmin`**
- Password: **`CSJP@ssword123`**

Under **Inbound Port Rules**: Allow selected ports **`RDP`**

Microsoft Azure Search resources, services, and docs (G+/I)

Home > Virtual machines >

Create a virtual machine

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource group * ⓘ CSJRG1 [Create new](#)

Instance details

Virtual machine name * ⓘ CSJIntVM1 ✓

Region * ⓘ (US) West US 2

Availability options ⓘ Availability zone

Availability zone * ⓘ Zone 1

☒ You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

Security type ⓘ Trusted launch virtual machines [Configure security features](#)

Estimated monthly cost
€55.72 / month
[View cost details](#)

< Previous Next : Disks > **Review + create**

Under the **Networking** tab:

- Virtual network `CSJIntVNet` and
- Subnet `default2`.
- Set **Public IP** to `None`.

Click **Review + Create** and then **Create**.

Microsoft Azure Search resources, services, and docs (G+/I) DEFAULT DIRECTORY

Home > Virtual machines >

Create a virtual machine

Network interface
When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ CSJIntVNet [Create new](#)

Subnet * ⓘ default2 (192.168.1.0/24) [Manage subnet configuration](#)

Public IP ⓘ None [Create new](#)

NIC network security group ⓘ ☒ None ☐ Basic ☐ Advanced

Public inbound ports * ⓘ ☐ None ☒ Allow selected ports

Select inbound ports * RDP (3389)

This will allow all IP addresses to access your virtual machine.

Estimated monthly cost
€55.72 / month
[View cost details](#)

< Previous Next : Management > **Review + create** [Give feedback](#)

Step 6: Deploy Azure Bastion Host

Navigate to **Bastions** and click **+ Create**.

Enter the following details:

- Resource Group: **`CSJRG1`**
- Name: **`CSJBastion`**
- Region: **`West US 2`**
- Availability: **`None`**
- Tier: **`Standard`**
- Instance count: **2**
- Virtual Network: **`CSJIntVNet`**
- Subnet: Click **Manage subnet configuration**. Then **+Subnet**
- Subnet purpose: **`Azure Bastion`**

Under **IPv4**,

- Starting address: **`192.168.2.0/26`**.

Click **Add**,

Back to the **Create a Bastion** page, under Subnet, select the newly created subnet.

Click **Review + Create** and then **Create**.

Home > Bastions >

Create a Bastion

Region * West US 2

Availability zone ① None

Tier * ① Standard

Instance count * ① 2

Configure virtual networks

Virtual network * ① CSJIntVNet
[Create new](#)

Subnet * AzureBastionSubnet (192.168.2.0/26)
[Manage subnet configuration](#)

Configure IP Address

IP Address ① ☒ Public IP address ☐ Private IP address

Public IP address

Public IP address * ① ☒ Create new ☐ Use existing

Step 7: Establish VNet Peering between Internal Server VNet and Firewall VNet

Navigate to Virtual Networks and select 'CSJIntVNet'.

Under Settings, go to **Peerings** and click + **Add**.

Under **Remote virtual network summary**,

Enter the following details:

- Peering link name: 'CSJFWVNet-to-CSJIntVNet'
- Subscription: Your subscription name
- Virtual Network: CSJFWVNet (CSJRG1)

Check Allow 'CSJFWVNet' to receive forwarded traffic from 'CSJExtVNet'

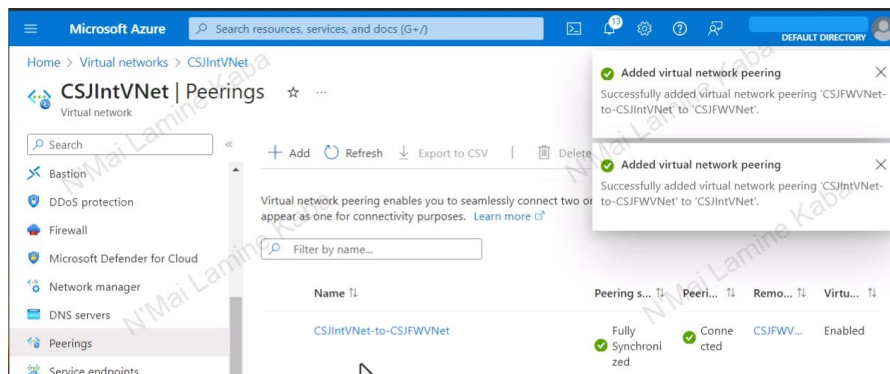
Under **Local virtual network summary**,

Enter the following details:

- Peering link Name: 'CSJIntVNet-to-CSJFWVNet'
- Remote Virtual Network: 'CSJFWVNet'

Check Allow 'CSJExtVNet' to receive forwarded traffic from 'CSJFWVNet'

Click **Add**.



Step 8: Configure Routing from Internal VNet to Firewall VNet

8.1: Create Route Table

In the Azure portal, search for and select **Route tables**. Click + **Create**.

Enter the following details:

- Resource Group: 'CSJRG1'
- Region: 'West US 2'
- Name: 'CSJIntRT'

Click **Review + Create** and then **Create**.

Microsoft Azure | Search resources, services, and docs (G+)

Home > Route tables >

Create Route table

Basics | Tags | Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Instance details

Region *

Name *

Propagate gateway routes * ☒ Yes ☐ No

8.2: Add Route to Route Table

Select the newly created route table ('CSJIntRT').

Under **Settings**, select **Routes** and click + **Add**.

Enter the following details:

- Route name: '**DefaultRoute**'
- Destination Type: '**IP address**'
- IP Addresses: '**0.0.0.0/0**'
- Next hop type: '**Virtual appliance**'
- Next hop address: Enter the **private IP** address of the Azure Firewall in '**CSJFWVNet**'.

Click **OK**.

Microsoft Azure | Search resources, services, and docs (G+)

Home > Route tables > CSJIntRT

CSJIntRT | Routes

+ Add + Refresh

Search routes

Name ↑↓

No results.

Add route

CSJIntRT

A user defined route (UDR) is a static route that overrides Azure's default system routes, or adds a route to a subnet's route table. [Learn more](#)

Route name *

Destination type *

Destination IP addresses/CIDR ranges *

Next hop type *

Next hop address *

Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.

Add

Give feedback

Step 8.3: Associate Route Table with Subnet

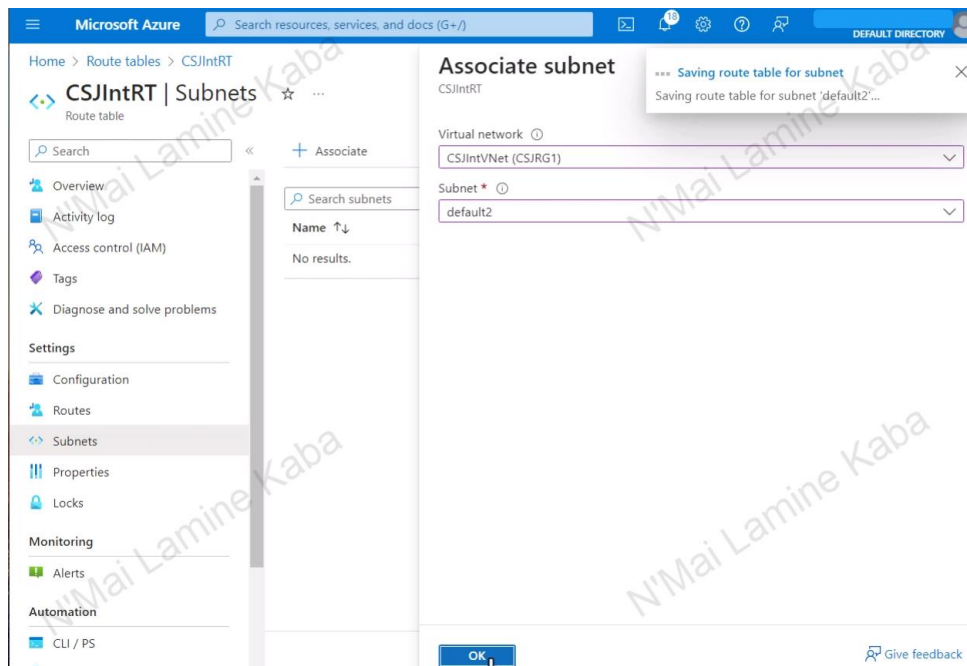
In the route table ('CSJIntRT'), under **Settings**, select **Subnets**.

Click + **Associate**.

Select the **Virtual Network**: 'CSJIntVNet'.

Select the Subnet: 'Default2'.

Click **OK**.



Step 9: Create the External VNet

Go to **Virtual Networks** and click + **Create**.

Enter the following details:

- Resource Group: 'CSJRG1'
- Name: 'CSJExtVNet'
- Region: 'West US 2'

Microsoft Azure

Home > Virtual networks >

Create virtual network

Basics Security IP addresses Tags Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Visual Studio Enterprise Subscription

Resource group * CSJRG1 [Create new](#)

Instance details

Virtual network name * CSJExtVNet

Region * (US) West US 2 [Deploy to an Azure Extended Zone](#)

Previous Next **Review + create** [Give feedback](#)

Under the IP addresses tab,

- Address Space: use ``172.16.0.0/16``

- Click + **Add Subnet**.

Enter the following details:

- Name: ``default2``

- Subnet address range: ``172.16.1.0/24``

Click **Add**, then **Review + Create**, and then **Create**.

Microsoft Azure

Home > Virtual network >

Create virtual network

Basics Security

Add IPv4 address

172.16.0.0/16

172.16.0.0

172.16.0.0 - 172.16.0.255

+ Add a subnet

Subnets

default

A NAT gateway gateway. [Learn more](#)

Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more](#)

Subnet purpose ⓘ Default

Name * ⓘ default2

IPv4

Include an IPv4 address space ☒

IPv4 address range * ⓘ 172.16.0.0/16

172.16.0.0 - 172.16.255.255

Starting address * ⓘ 172.16.1.0

Size ⓘ /24 (256 addresses)

Subnet address range ⓘ 172.16.1.0 - 172.16.1.255

IPv6

Include an IPv6 address space ☐ This virtual network has no IPv6 address ranges.

Private subnet [PREVIEW](#)

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in this subnet. [Learn more](#)

Previous **Add** Cancel

Step 10: Deploy External Server in CSJExtVNet

Navigate to **Virtual Machines** and click **+ Create**.

Enter the following details:

- Resource group: **`CSJRG1`**
- Name: **`CSJExtVM1`**
- Region: **`West US 2`**
- Availability Option: **`Availability Zone`**
- Availability Zone: **`Zone 1`**
- Security type: **`Standard`**
- Image: **`Windows Server 2022`**
- Size: **Choose a cost-effective VM size**
- Username: **`CSJAdmin`**
- Password: **`CSJP@ssword123`**

Microsoft Azure

Home > Virtual machines >

Create a virtual machine

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Instance details

Virtual machine name *

Region *

Availability options

Availability zone *

☒ You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

Security type

[< Previous](#) [Next: Disks >](#) [Review + create](#) [Give feedback](#)

Under **Inbound Port Rules**: Allow selected ports **`RDP`**

Under the **Networking** tab:

- Ensure the VM is connected to **`CSJExtVNet`** and **`default2`**.
- Set Public IP to **`None`**.

Click **Review + Create** and then **Create**.

Step 11: Create VNet Peering between External VNet and Firewall VNet

Navigate to **Virtual Networks** and select '**CSJExtVNet**'.

Under Settings, go to **Peerings** and click **+ Add**.

Under **Remote virtual network summary**,

Enter the following details:

- Peering link name: **CSJFWVNet-to-CSJExtVNet**
- Subscription: **Your subscription name**
- Virtual Network: **CSJFWVNet (CSJRG1)**

Check **Allow 'CSJFWVNet' to receive forwarded traffic from 'CSJExtVNet'**

Under **Local virtual network summary**,

Enter the following details:

- Peering link Name: '**CSJExtVNet-to-CSJFWVNet**'
- Remote Virtual Network: '**CSJFWVNet**'

Check **Allow 'CSJExtVNet' to receive forwarded traffic from 'CSJFWVNet'**

Click **Add**.

The screenshot shows the 'Add peering' configuration page in the Microsoft Azure portal. The page is titled 'Add peering' and is for the virtual network 'CSJExtVNet'. The configuration details are as follows:

- Peering link name ***: CSJFWVNet-to-CSJExtVNet
- Virtual network deployment model**: ☒ Resource manager, ☐ Classic
- I know my resource ID**: ☐
- Subscription ***: Visual Studio Enterprise Subscription
- Virtual network ***: CSJFWVNet (CSJRG1)
- Remote virtual network peering settings**:
 - Allow 'CSJFWVNet' to access 'CSJExtVNet'**: ☒
 - Allow 'CSJFWVNet' to receive forwarded traffic from 'CSJExtVNet'**: ☐
 - Allow gateway or route server in 'CSJFWVNet' to forward traffic to 'CSJExtVNet'**: ☐

Step 12: Configure Routing from External VNet to Firewall VNet

12.1: Create Route Table

In the Azure portal, search for and select **Route tables**.

Click **+ Create**.

Enter the following details:

- Resource Group: **`CSJRG1`**
- Region: **`West US 2`**
- Name: **`CSJExtRT`**

Click **Review + Create** and then **Create**.

The screenshot shows the 'Create Route table' wizard in the Microsoft Azure portal. The 'Project details' section is active, showing the subscription 'Visual Studio Enterprise Subscription' and resource group 'CSJRG1'. The 'Instance details' section shows the region 'West US 2' and the name 'CSJExtRT'. The 'Propagate gateway routes' option is set to 'Yes'. The 'Review + create' button is highlighted in blue.

12.2: Add Route to Route Table

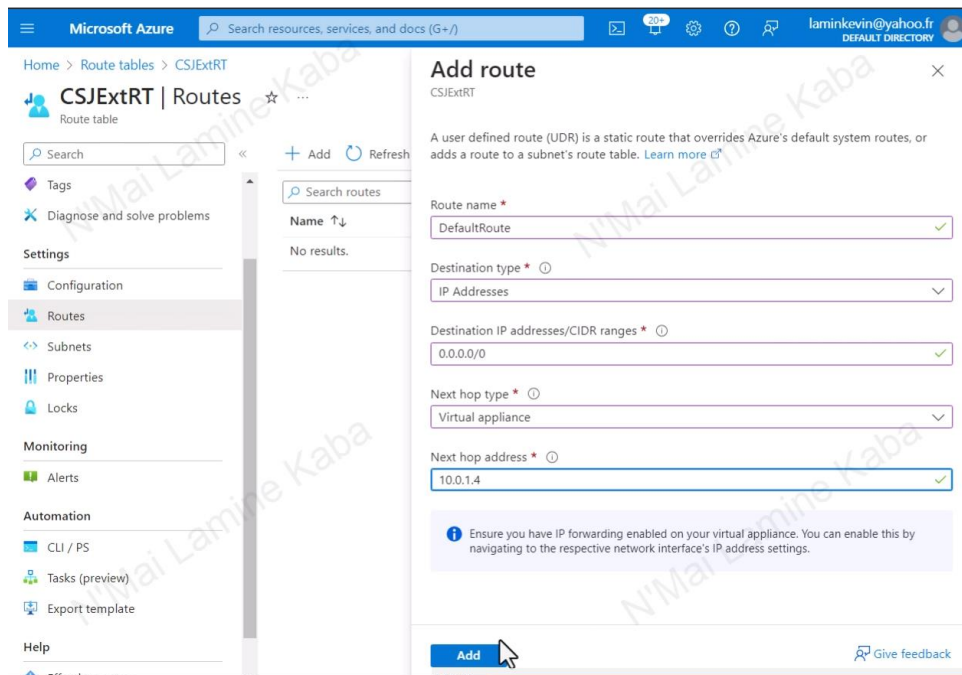
Select the newly created route table (**`CSJExtRT`**).

Under **Settings**, select **Routes** and click **+ Add**.

Enter the following details:

- Route name: **`DefaultRoute`**
- Destination type: **`IP addresses`**
- Destination IP Addresses: **`0.0.0.0/0`**
- Next hop type: **`Virtual appliance`**
- Next hop address: Enter the **private IP** address of the Azure Firewall in **`CSJFWVNet`**.

Click **OK**.



12.3: Associate Route Table with Subnet

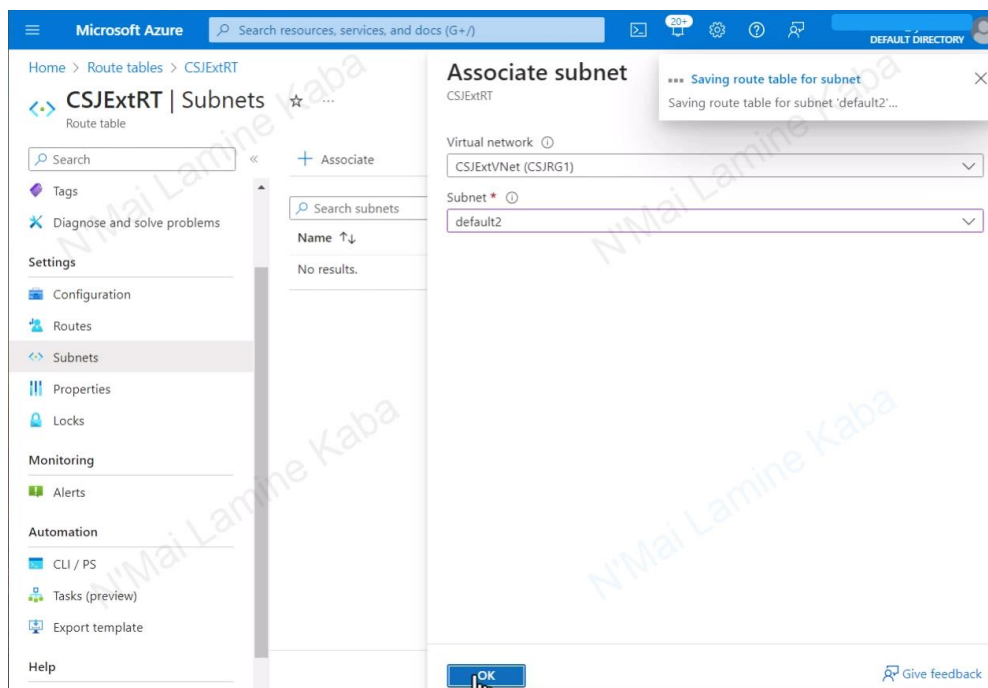
In the route table ('CSJExtRT'), under **Settings**, select **Subnets**.

Click **+ Associate**.

Select the **Virtual Network**: 'CSJExtVNet'.

Select the **Subnet**: 'Default2'.

Click **OK**.



Step 13: Configure Azure Firewall Rules

13.1: Network Rules

Explanation: This network rule allows TCP traffic from any IP address in the 192.168.1.0/24 subnet (internal network) to any IP address in the 172.16.1.0/24 subnet (external network) on port 3389, which is typically used for Remote Desktop Protocol (RDP). This rule permits internal servers to initiate RDP connections to external servers.

Navigate to **Firewalls** and select **'CSJFW'**.

Go to **Rules** and click on the **Network rule collection** tab.

Click + **Add network rule collection**.

Enter the following details:

- Name: **'Restrict-CSJIntVNet-to-CSJExtVNet'**
- Priority: **'100'**
- Action: **'Allow'**

Under **Rules**, enter the following:

- Name: **'Allow RDP'**
- Protocol: **'TCP'**
- Source type: **'IP Address'**
- Source: **'192.168.1.0/24'** (CSJIntVNet subnet)
- Destination type: **'IP Address'**
- Destination: **'172.16.1.0/24'** (CSJExtVNet subnet)
- Destination Ports: **3389**

Click **Add**.

13.2: Application Rules

Explanation: This application rule allows HTTP and HTTPS traffic from any IP address in the 192.168.1.0/24 subnet to the domain www.microsoft.com. It enables internal servers to access Microsoft's website, which may be necessary for software updates or other services.

Navigate to **Rules** and click on the **Application rule collection** tab. Click + **Add application rule collection**.

Enter the following details:

- Name: **`Allow-MSFT-Access`**
- Priority: **`200`**
- Action: **`Allow`**

Under **FQDN tags**, enter the following:

- Name: **`Allow-MSFT-Updates`**
- Source type: **`IP Address`**
- Source: **`192.168.1.0/24`** (CSJIntVNet subnet)
- FQDN tags: **`Windows Updates`**

Under FQDN tags, enter the following:

- Name: **`Allow-MSFT-Access`**
- Source type: **`IP Address`**
- Source: **`192.168.1.0/24`** (CSJIntVNet subnet)
- Protocol: **`http, https`**
- Target FQDNs: **`www.microsoft.com`**

Click **Add**.

Add application rule collection

Priority * 200

Action * Allow

Rules

name	Source type	Source	FQDN tags
Allow-MSFT-Updates	IP address	192.168.1.0/24	WindowsUpdate
	IP address	*, 192.168.10.1, 192.168.10.0/24, 192...	0 selected

FQDN tags may require additional configuration. [Learn more](#)

Target FQDNs

name	Source type	Source	Protocol:Port	Target FQDNs
Windows Updates	IP address	192.168.1.0/24	http, https	www.microsoft.com
	IP address	*, 192.168.10.1, 192.168.10.0...	http, http:8080, https, mssql:...	www.microsoft.com, *.micro...

mssql: SQL should be enabled in proxy mode. This may require additional configuration. [Learn more](#)

Add

13.3: DNAT Rules

Explanation: This DNAT rule translates inbound TCP traffic destined for the firewall's public IP on port 443 to the private IP address of CSJExtVM1 on the same port. It allows external clients to securely connect to the internal server via HTTPS through the firewall.

Navigate to **Rules** and click on the **NAT rule collection** tab.

Click + **Add NAT rule collection**.

Enter the following details:

- Name: **`DNAT-To-CSJExtVM-server`**
- Priority: **`300`**
- Action: **`Destination Network Address Translation (DNAT)`**

Under **Rules**, click + **Add rule** and configure:

- Name: **`HTTPS-To-CSJExtVM-server`**
- Protocol: **`TCP`**
- Source type: **`IP Address`**
- Source: **`*`**
- Destination Address: **Public IP of `CSJFW`**
- Destination Ports: **`443`**
- Translated Address: **Private IP of `CSJExtVM1`**
- Translated Port: **`443`**

Click **Add**.

Microsoft Azure Search resources, services, and docs (G+)

Add NAT rule collection

Name * DNAT-To-CSJExtVM-server ✓

Priority * 300 ✓

Action Destination Network Address Translation (DNAT).

Rules

Protocol	Source type	Source	Destination Addr...	Destination Ports	Translated address	Translated port
TCP	IP address	*	52.143.101.54 ✓	443 ✓	172.16.1.4 ✓	443 ✓
0 selected	IP address	*, 192.168.10.1, 192...	192.168.10.0	8080	192.168.10.0	8080

Activ Accèd

Step 14: Monitoring and Logging

Explanation: Log Analytics provides a powerful query language (KQL - Kusto Query Language) to filter and analyze log data. By running specific queries, you can extract valuable insights about your network traffic and firewall rule processing. For instance, querying for denied connections helps identify potential security threats, while querying for allowed connections ensures that legitimate traffic is flowing as expected.

14.1: Create Log Analytics Workspace

Navigate to the Azure portal and search for **Log Analytics workspaces**. Click **+ Create**.

Enter the following details:

- Resource Group: **`CSJRG1`**
- Name: **`CSJLAW`**
- Region: **`West US`**

Click **Review + Create** and then **Create**.

Microsoft Azure Search resources, services, and docs (G+)

Home > Log Analytics workspaces >

Create Log Analytics workspace

Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Instance details

Name *

Region *

[Review + Create](#) [< Previous](#) [Next: Tags >](#)

14.2: Configure Azure Firewall to Send Logs to Log Analytics Workspace

Navigate to **Firewalls** and select 'CSJFW'.

Under **Monitoring**, click **Diagnostic settings**. Click + **Add diagnostic setting**.

Enter the following details:

- Name: 'CSJFWDiagSettings'
- Logs: Select the logs you want to collect (e.g., **Firewall, Application, and NetworkRule**)
- Destination details: Select **Send to Log Analytics** and choose 'CSJLogWorkspace'

Click **Save**.

Home > Firewall Manager | Azure Firewalls > CSJFWNet | Diagnostic settings >

Diagnostic setting

[Save](#) [Discard](#) [Delete](#) [Feedback](#)

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name *

Logs

Category groups ☐ allLogs

Categories

- ☐ Azure Firewall Application Rule (Legacy Azure Diagnostics)
- ☐ Azure Firewall Network Rule (Legacy Azure Diagnostics)
- ☐ Azure Firewall DNS Proxy (Legacy Azure Diagnostics)
- ☒ Azure Firewall Network Rule
- ☒ Azure Firewall Application Rule
- ☒ Azure Firewall Nat Rule

Destination details

- ☒ Send to Log Analytics workspace
 - Subscription:
 - Log Analytics workspace:
 - Destination table [Resource specific](#)
- ☐ Archive to a storage account
- ☐ Stream to an event hub
- ☐ Send to partner solution

Step 15: Test Connectivity

Step 15.1: Test Connectivity from CSJIntVNet to CSJExtVNet

Log in to `CSJIntVM1` via the bastion host.

Open **Remote Desktop Connection** and enter the private IP of `CSJExtVM1`.

Enter admin credentials: `.\CSJAdmin`.



PS: After successfully connecting to CSJExtVM1, Install **IIS** (web service), generate a certificate using the public IP of the firewall for instance, and bind the certificate to the default site. You can find these steps on the video version of this lab on my YouTube channel:

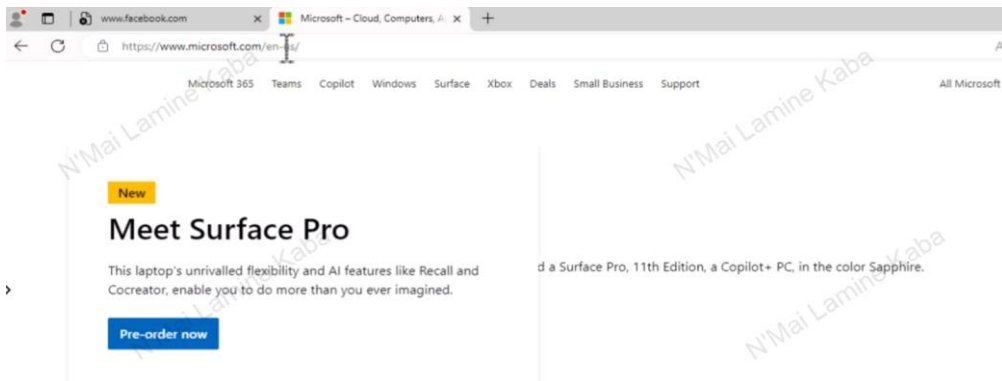
www.youtube.com/@CybersecJourneywithLamine

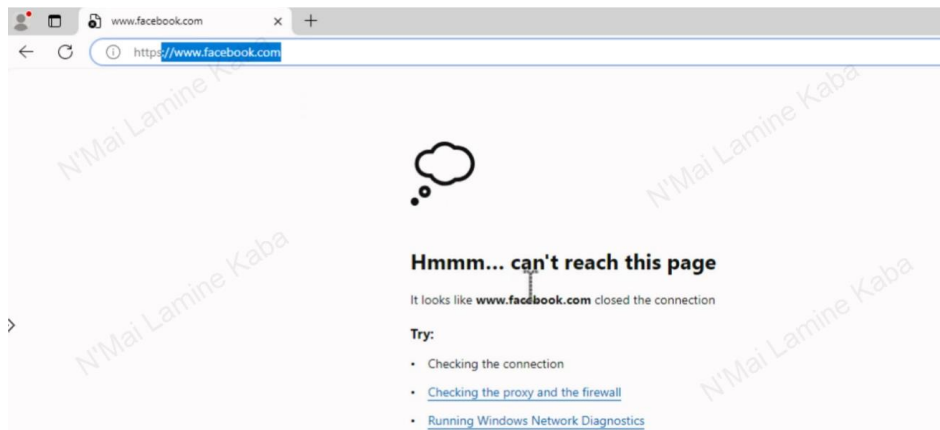
Step 15.2: Test Internet Access from CSJIntVNet

Log in to `CSJIntVM1` via the bastion host.

Open a web browser on `CSJIntVM1`.

Navigate to **https://www.microsoft.com** (should work) and **https://www.facebook.com** (should be blocked).

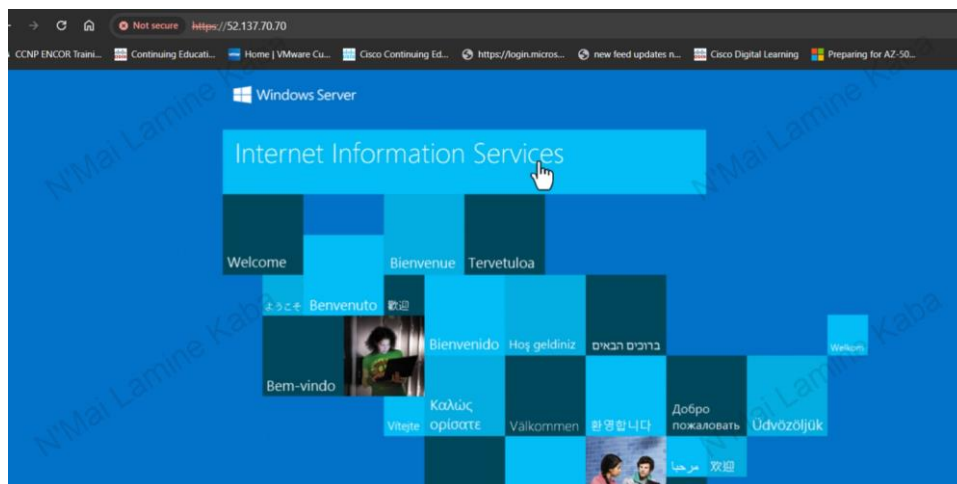




Step 15.3: Test DNAT Configuration (Internet to Internal VM)

From an external network, perform the following tests:

- Open a web browser and navigate to `http://<Azure_Firewall_Public_IP>` (should not work).
- Navigate to `https://<Azure_Firewall_Public_IP>` (should work).



Step 16: Accessing Logs in Log Analytics Workspace

Go to the Azure portal, search for, and select **Log Analytics workspaces**.

Choose the Log Analytics workspace (`CSJLogWorkspace`).

Use queries to filter and retrieve specific log entries:

Example Queries:

Query for Denied Connections:

AzureDiagnostics

| where ResourceType == "AZUREFIREWALLS"

| where Action == "Deny"

| where TimeGenerated >= datetime(2024-05-27T00:00:00Z) and TimeGenerated <= datetime(2024-05-28T00:00:00Z)

| limit 10

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Log Analytics workspaces' sidebar is visible, with 'CSJLogWorkspace' selected. The main pane displays the 'Logs' view for 'CSJLogWorkspace'. A query editor is open, showing a query for 'AzureDiagnostics' logs where the 'Action_s' is 'Deny' and the 'TimeGenerated' is between 2024-05-27T00:00:00Z and 2024-05-28T00:00:00Z. The query is limited to 10 results. The results table shows 10 entries, all with 'Action_s' set to 'Deny' and 'TimeGenerated' values ranging from 2024-05-27T00:00:00Z to 2024-05-28T00:00:00Z.

TimeGenerated [UTC]	ResourceId	Category	ResourceGroup
5/27/2024, 1:10:10.322 AM	/SUBSCRIPTIONS/8723F91B-E8...	AZFWApplicationRule	CSJRG1
5/27/2024, 1:10:10.208 AM	/SUBSCRIPTIONS/8723F91B-E8...	AZFWApplicationRule	CSJRG1
5/27/2024, 1:09:30.790 AM	/SUBSCRIPTIONS/8723F91B-E8...	AZFWApplicationRule	CSJRG1
5/27/2024, 1:09:30.789 AM	/SUBSCRIPTIONS/8723F91B-E8...	AZFWApplicationRule	CSJRG1
5/27/2024, 1:09:30.654 AM	/SUBSCRIPTIONS/8723F91B-E8...	AZFWApplicationRule	CSJRG1
5/27/2024, 1:09:30.654 AM	/SUBSCRIPTIONS/8723F91B-E8...	AZFWApplicationRule	CSJRG1
5/27/2024, 1:09:30.615 AM	/SUBSCRIPTIONS/8723F91B-E8...	AZFWApplicationRule	CSJRG1
5/27/2024, 1:09:30.615 AM	/SUBSCRIPTIONS/8723F91B-E8...	AZFWApplicationRule	CSJRG1
5/27/2024, 1:09:30.615 AM	/SUBSCRIPTIONS/8723F91B-E8...	AZFWApplicationRule	CSJRG1
5/27/2024, 1:09:30.615 AM	/SUBSCRIPTIONS/8723F91B-E8...	AZFWApplicationRule	CSJRG1

Query for Allowed Connections:

AzureDiagnostics

| where ResourceType == "AZUREFIREWALLS"

| where Action == "Allow"

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Log Analytics workspaces' sidebar is visible, with 'CSJLogWorkspace' selected. The main pane displays the 'Logs' view for 'CSJLogWorkspace'. A query editor is open, showing a query for 'AzureDiagnostics' logs where the 'ResourceType' is 'AZUREFIREWALLS', the 'Action_s' is 'Allow', and the 'TimeGenerated' is between 2024-05-27T00:00:00Z and 2024-05-28T00:00:00Z. The query is limited to 10 results. The results table shows 10 entries, all with 'Action_s' set to 'Allow' and 'TimeGenerated' values ranging from 2024-05-27T00:00:00Z to 2024-05-28T00:00:00Z.

TimeGenerated [UTC]	ResourceId	Category	ResourceGroup
5/27/2024, 12:34:23.628 AM	/SUBSCRIPTIONS/8723F91B-E8...	AZFWNetworkRule	CSJRG1
5/27/2024, 12:34:21.920 AM	/SUBSCRIPTIONS/8723F91B-E8...	AZFWNetworkRule	CSJRG1
5/27/2024, 12:32:43.954 AM	/SUBSCRIPTIONS/8723F91B-E8...	AZFWNetworkRule	CSJRG1
5/27/2024, 12:32:00.759 AM	/SUBSCRIPTIONS/8723F91B-E8...	AZFWNetworkRule	CSJRG1
5/27/2024, 12:30:24.232 AM	/SUBSCRIPTIONS/8723F91B-E8...	AZFWNetworkRule	CSJRG1

| where TimeGenerated >= datetime(2024-05-27T00:00:00Z) and TimeGenerated <= datetime(2024-05-28T00:00:00Z)

| limit 10

PS: replace the date and time with your testing date and time.

Conclusion:

The successful implementation of a secure network infrastructure using Azure Firewall demonstrates a comprehensive understanding of cloud networking, security, and resource management on the Azure platform. This project involved creating and configuring multiple virtual networks, establishing secure communication through VNet peering, and implementing robust firewall rules to control traffic flow and ensure security compliance.

By integrating Azure Bastion and Log Analytics, the project not only ensured secure and efficient access to internal resources but also provided a detailed monitoring and logging system for ongoing management and analysis. The project highlights my proficiency in deploying and managing Azure resources, my ability to design and implement security measures, and my skills in troubleshooting and optimizing cloud environments.

Overall, this project has significantly enhanced my expertise in Azure infrastructure and security, preparing me for advanced roles in cloud architecture and cybersecurity.

Future Work: Integrating Azure firewall with Azure Sentinel

Building upon this project, the future work aims to enhance security monitoring and incident response capabilities by integrating Azure Sentinel, a cloud-native SIEM (Security Information and Event Management) solution.