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:

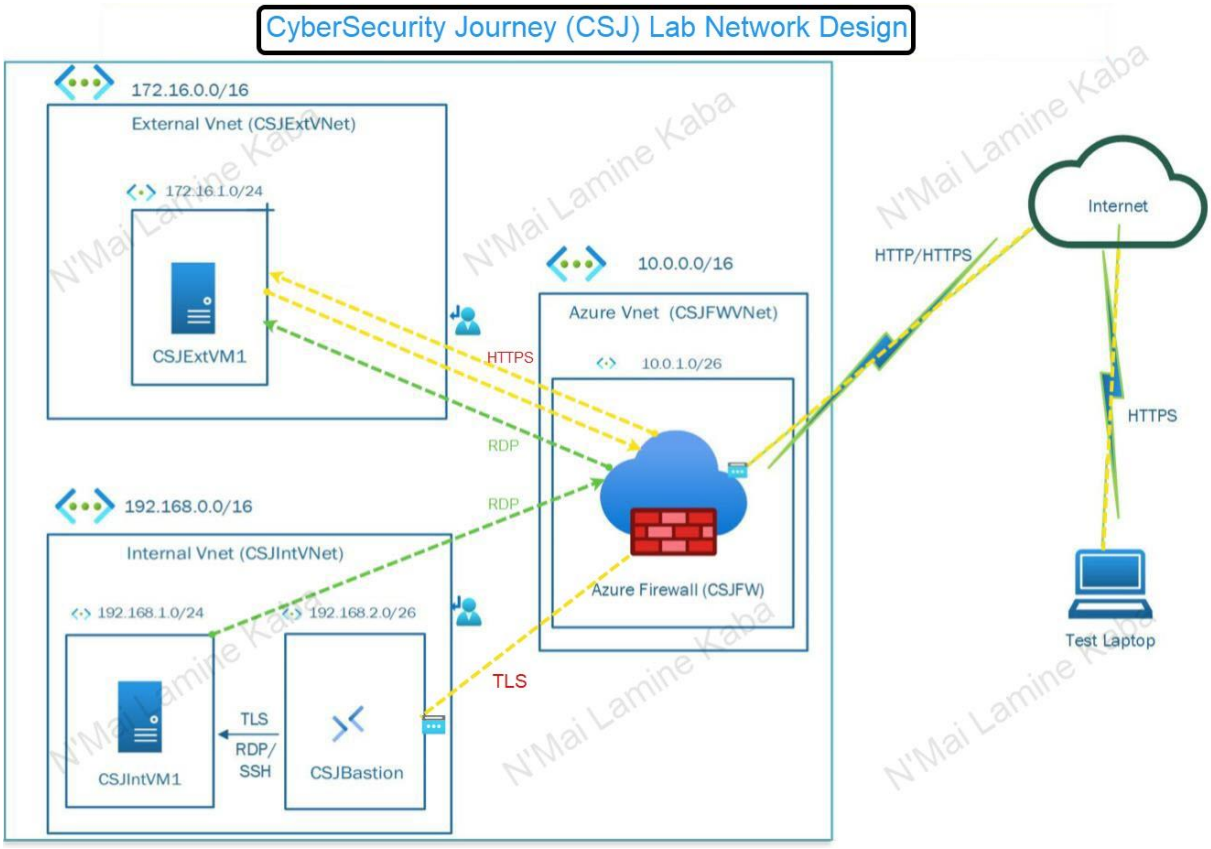
- Perform connectivity tests to ensure proper routing and firewall rule enforcement.

- 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

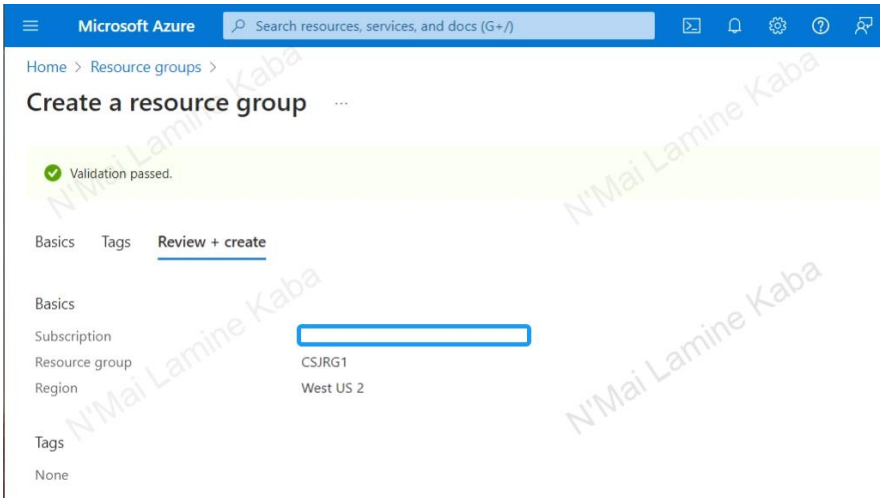
Navigate to **Resource Groups** in the Azure portal.

Click + **Create**.

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

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

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

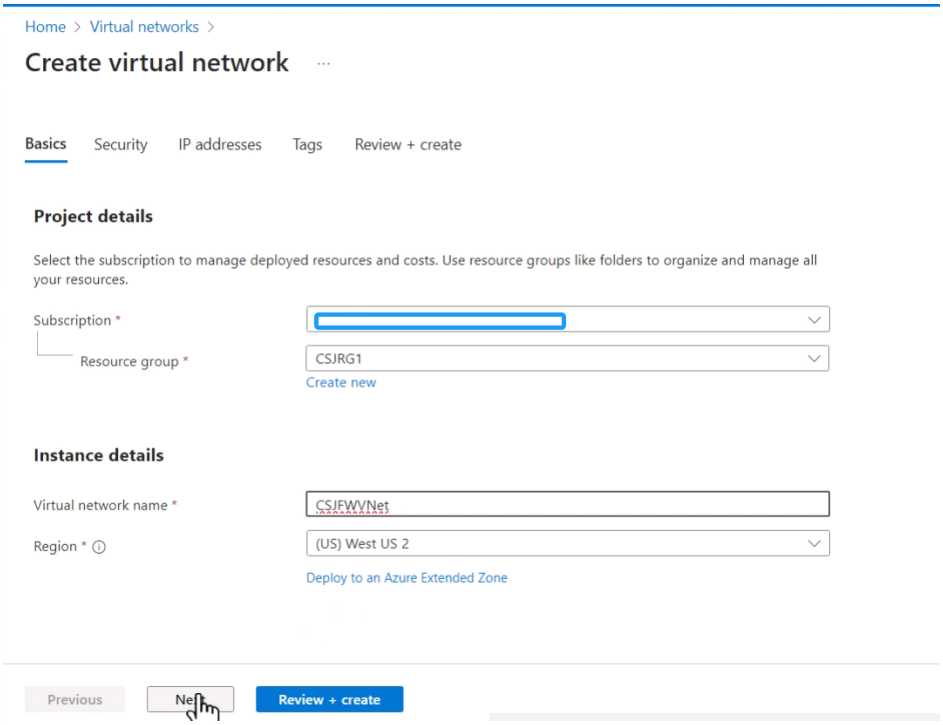


Step 2: Set Up Firewall Virtual Network (VNet)

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**`

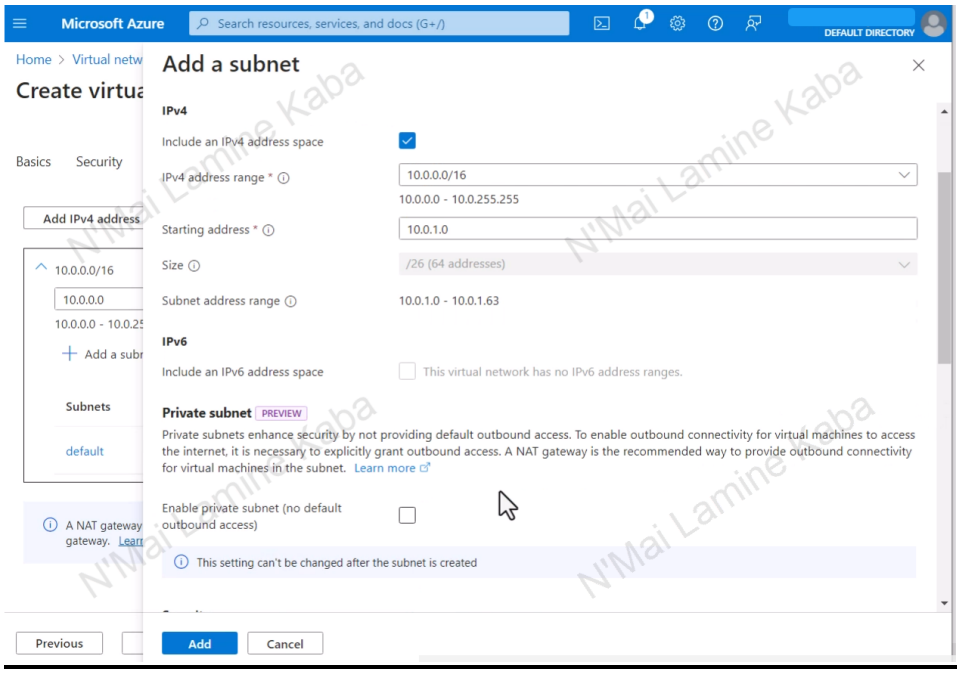


Under **IP addresses tab,** Click + **Add a subnet**.

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**.



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)**

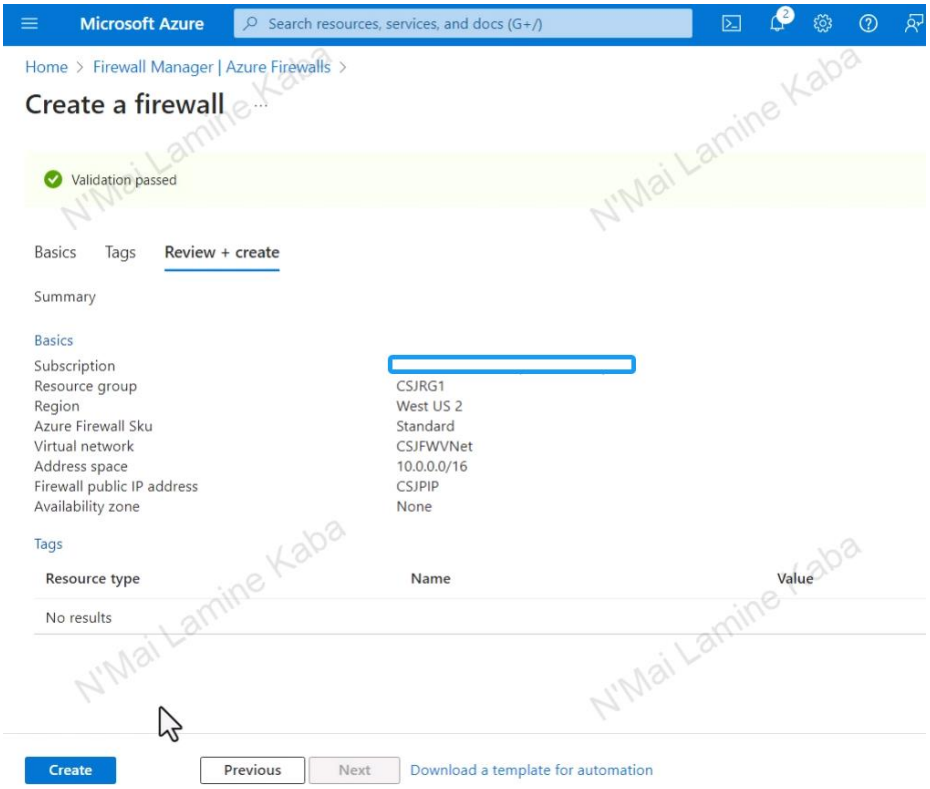
Choose a virtual network: `**Use existing**`

Under Virtual Network:

- Select **CSJFWVNet**

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

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



Step 4: Create the Internal Virtual Network (VNet)

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

Enter the following details:

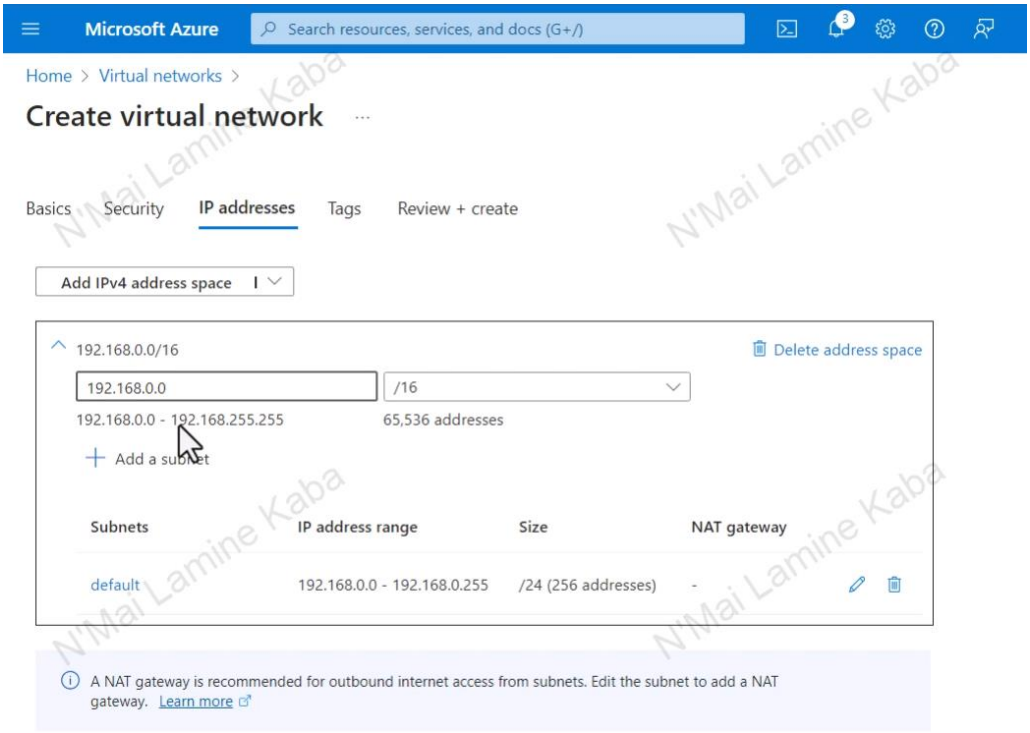
- Subscription: **Choose your subscription**

- Resource Group: `**CSJRG1**`

- Name: `**CSJIntVNet**`

  - Region: `**West US 2**`

  - Address Space: `**192.168.0.0/16**`



Click + **Add Subnet**.

Enter the following details:

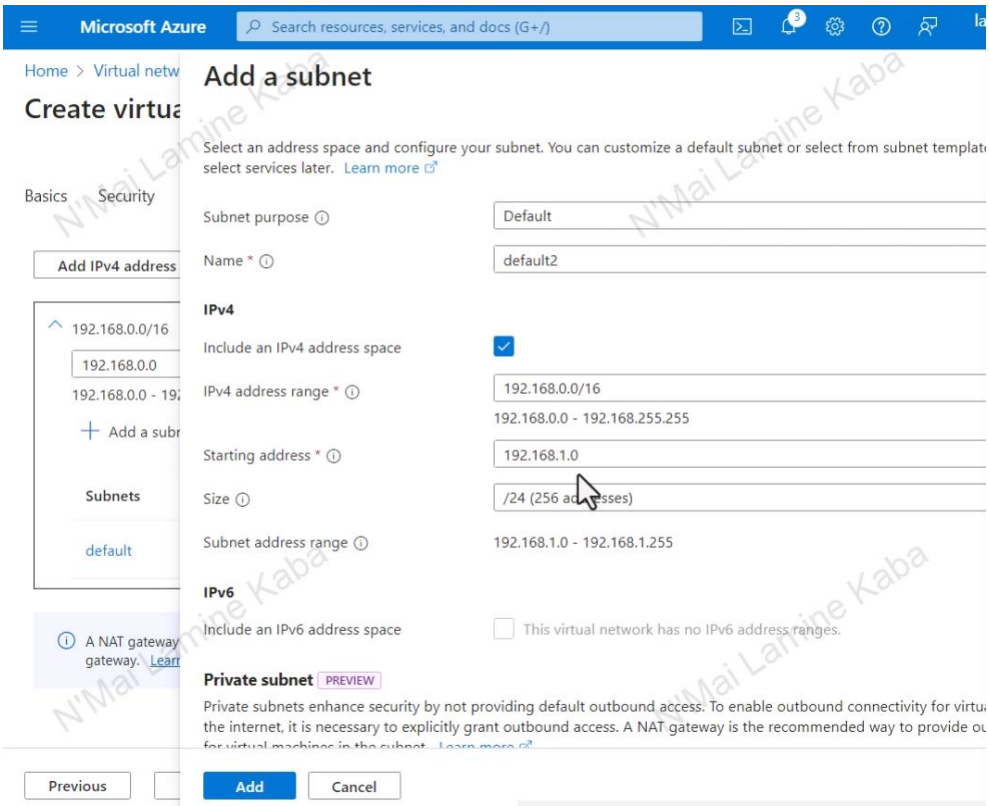
  - Subnet Purpose: Select`**Default**`

  - 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**.



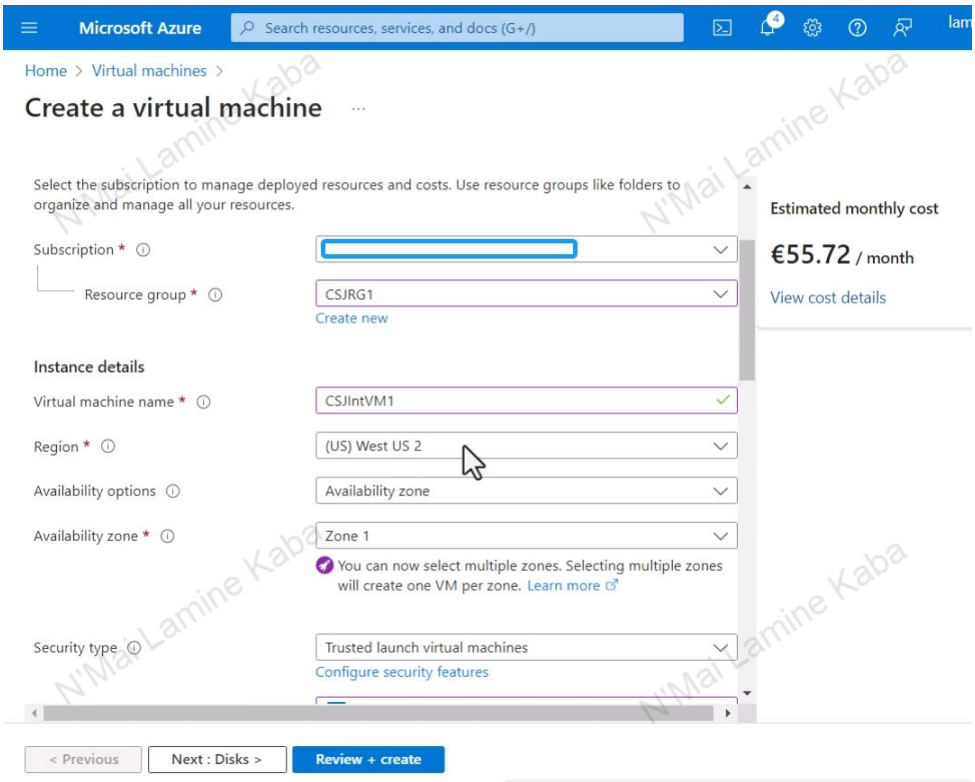
Step 5: Deploy Internal Server in CSJIntVNet

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**`

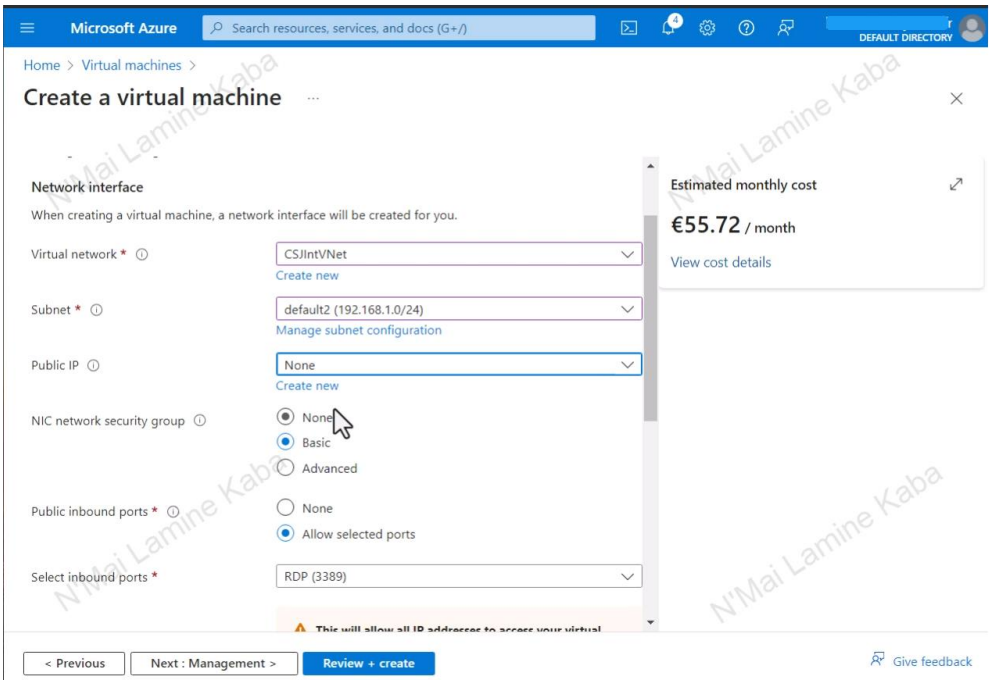
Under **Inbound Port Rules**: Allow selected ports `**RDP**`



Under the **Networking** tab:

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

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



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**`

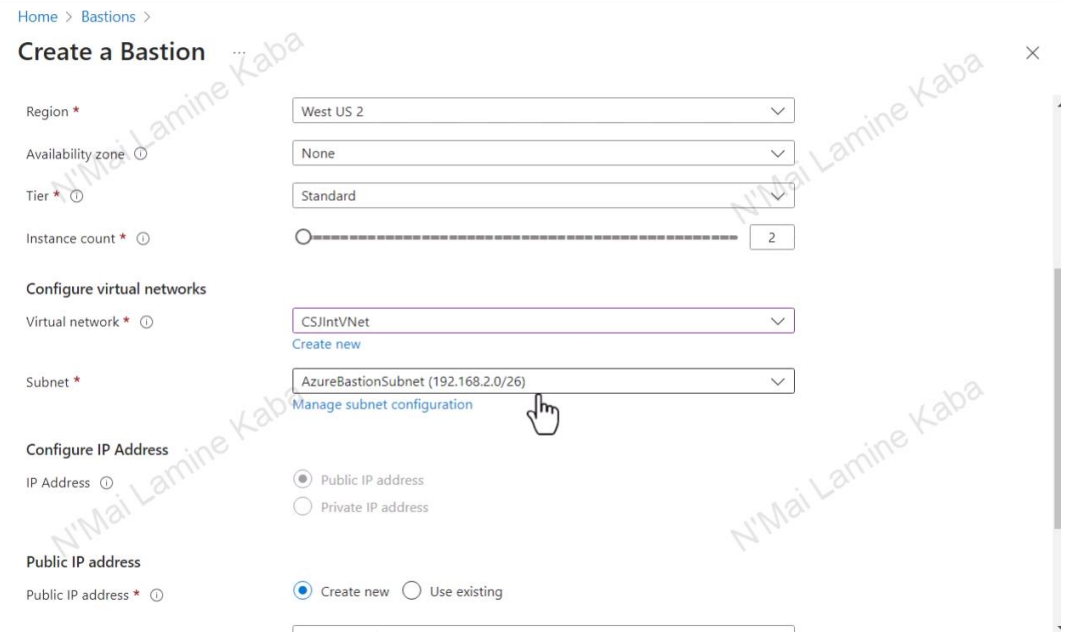
Under **IPv4**,

- 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**.



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,**

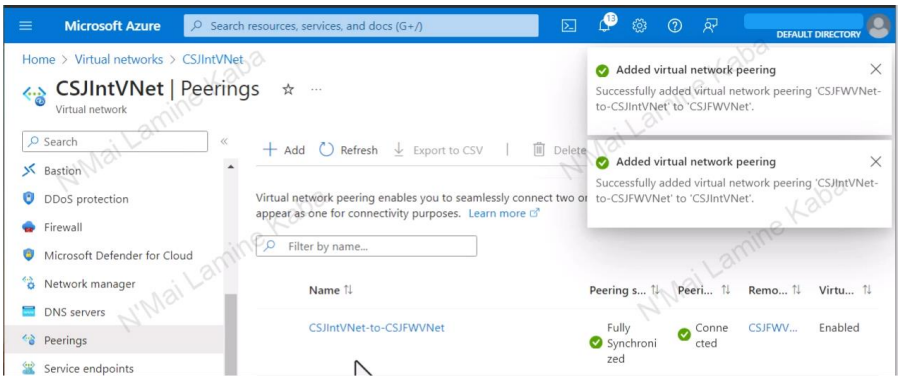
Enter the following details:

- 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**.

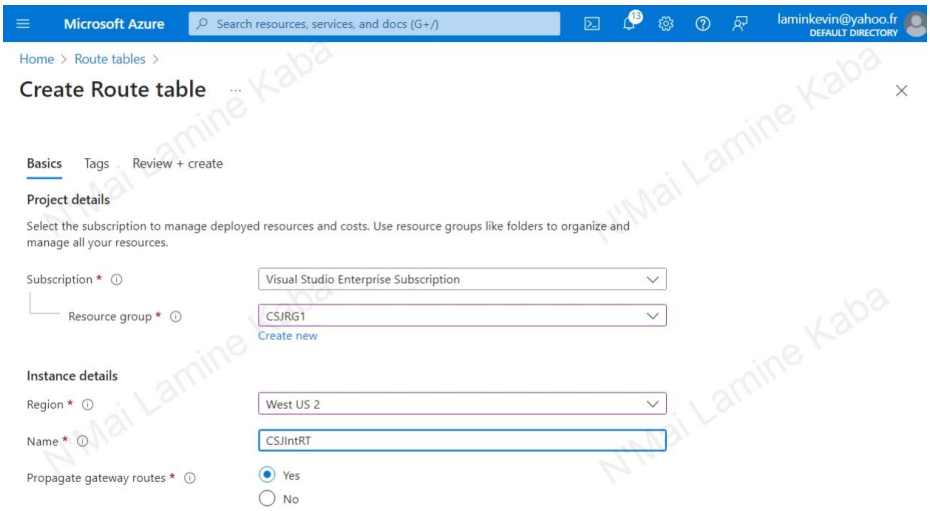
Enter the following details:

- Resource Group: `**CSJRG1**`

- Region: `**West US 2**`

- Name: `**CSJIntRT**`

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



8.2: Add Route to Route Table

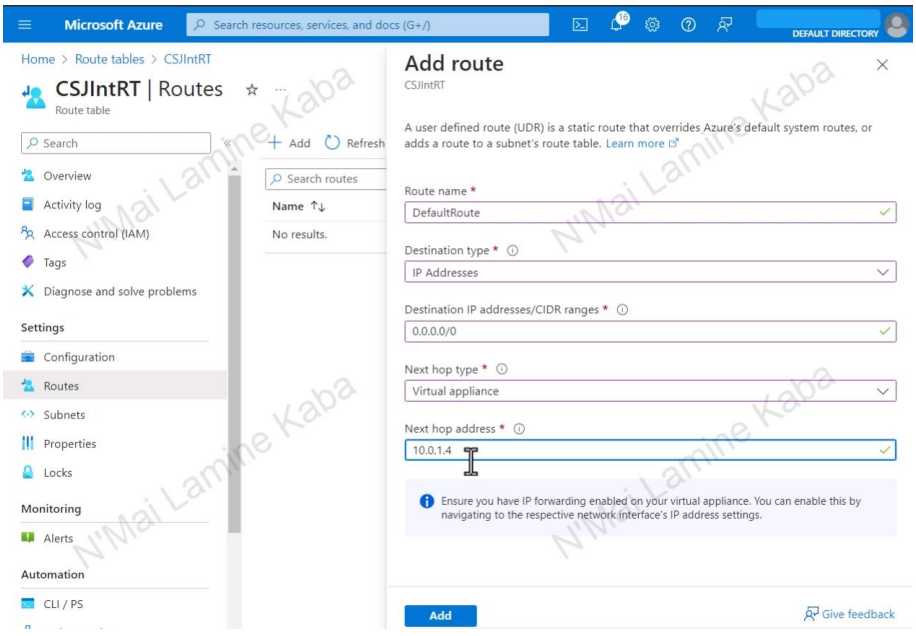
Select the newly created route table (`**CSJIntRT**`).

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**.



Step 8.3: Associate Route Table with Subnet

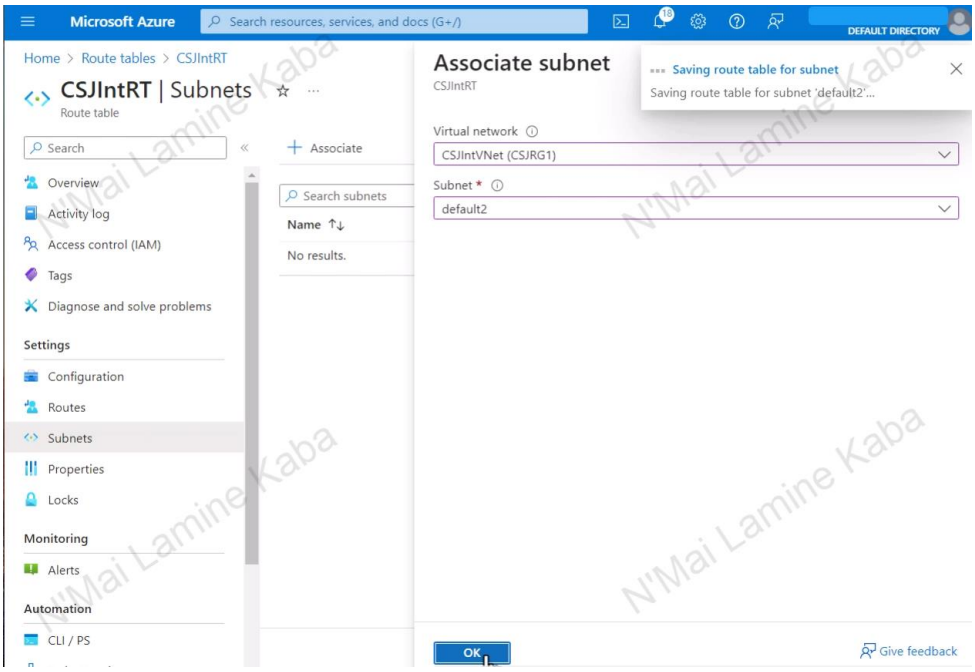
In the route table (`**CSJIntRT**`), under **Settings**, select **Subnets**.

Click + **Associate**.

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

Select the Subnet: `**Default2**`.

Click **OK**.

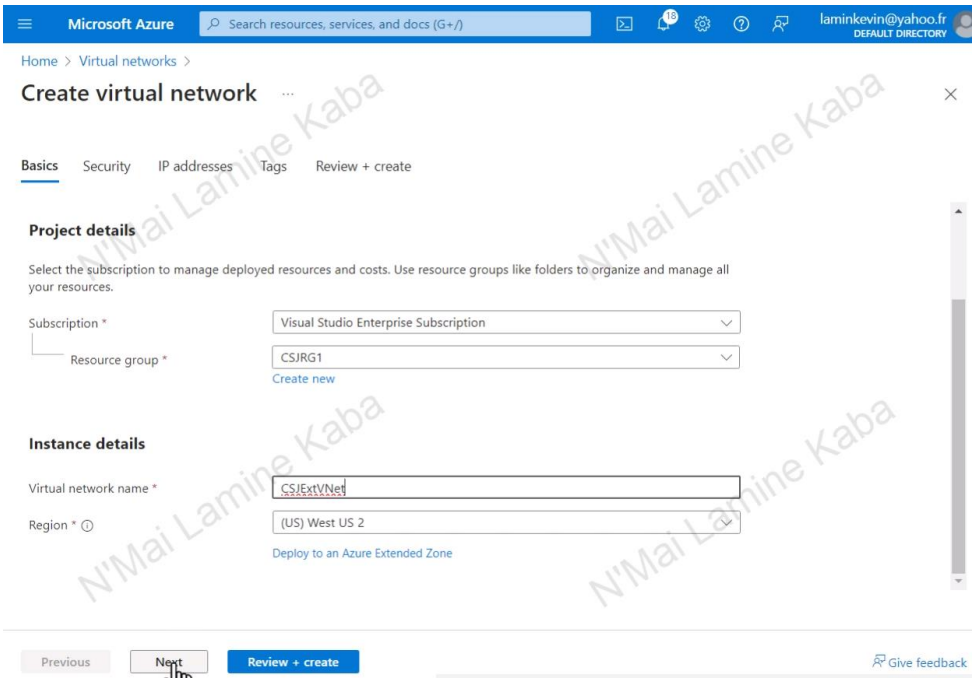


Step 9: Create the External VNet

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

Enter the following details:

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



Under the IP addresses tab,

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

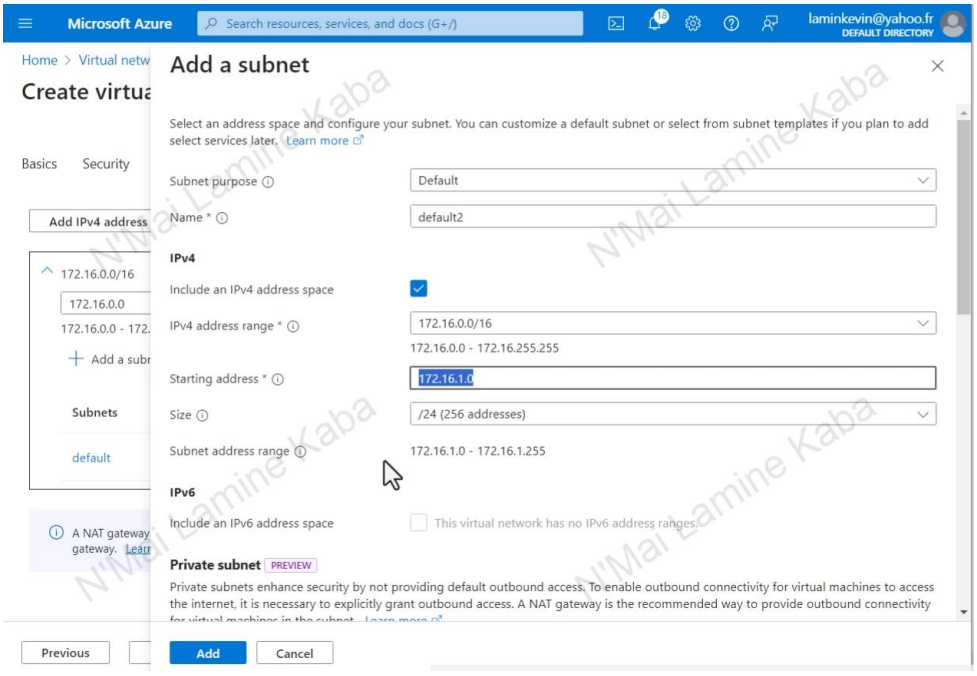
- Click + **Add Subnet**.

Enter the following details:

- Name: `**default2**`

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

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

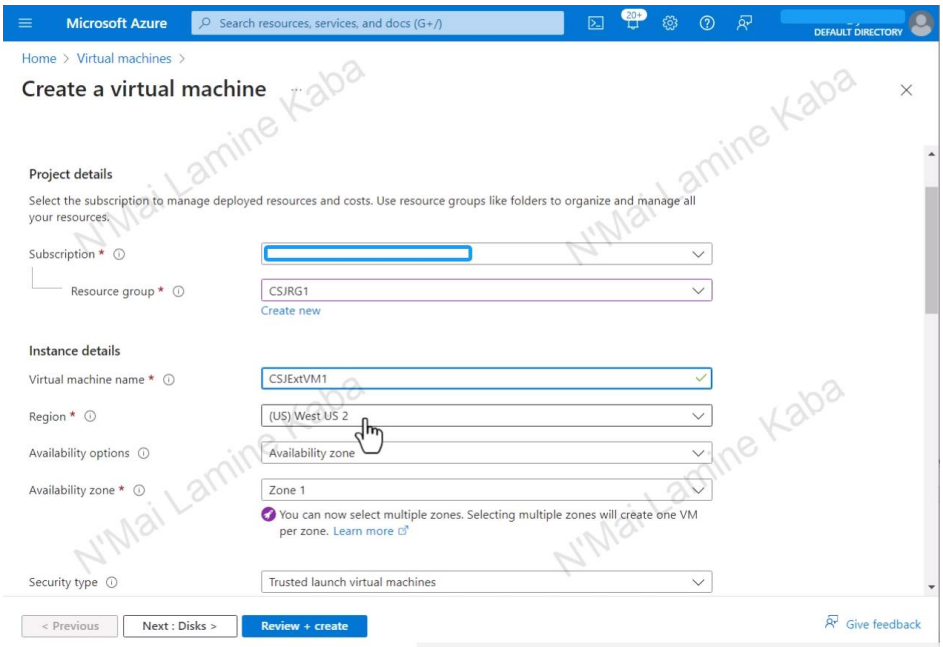


Step 10: Deploy External Server in CSJExtVNet

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**`



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

Under the **Networking**tab:

- Ensure the VM is connected to `C**SJExtVNet**` 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,**

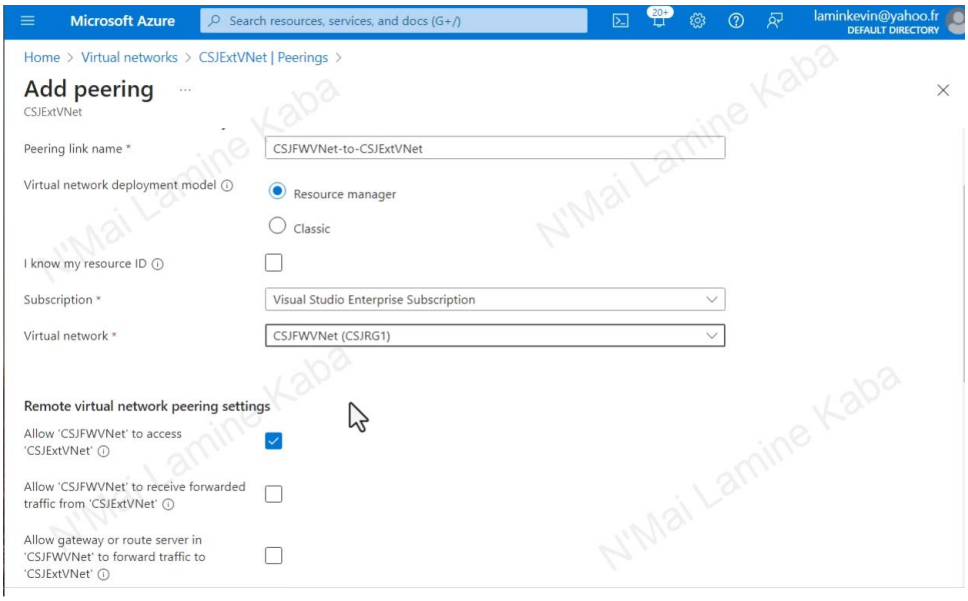
Enter the following details:

- Peering link Name: `**CSJExtVNet-to-CSJFWVNet**`

- Remote Virtual Network: `**CSJFWVNet**`

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

Click **Add.**



Step 12: Configure Routing from External VNet to Firewall VNet

12.1: Create Route Table

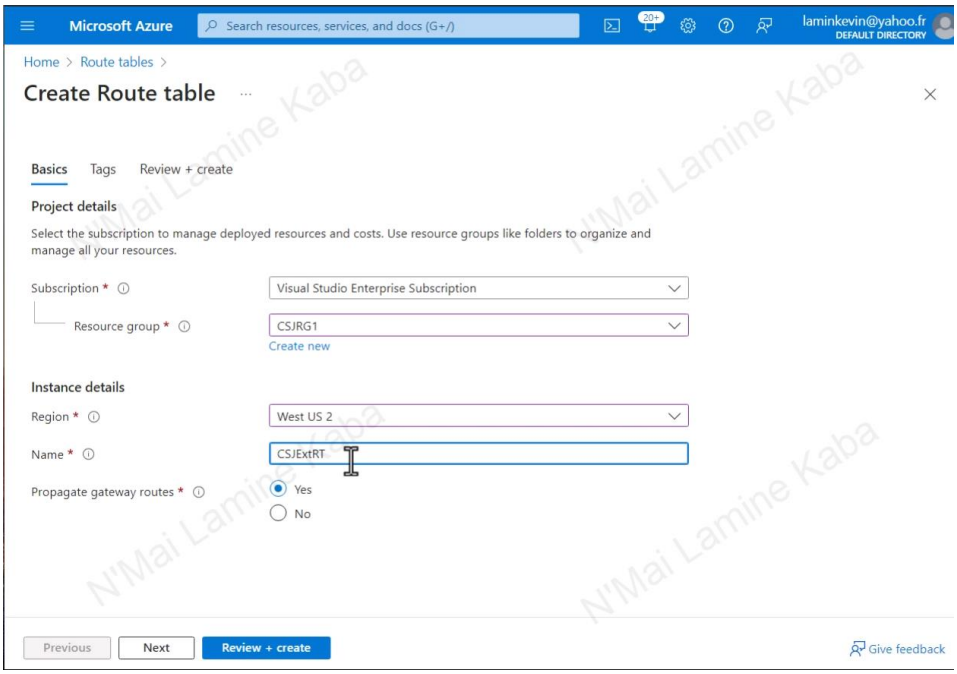
In the Azure portal, search for and select **Route tables**.

Click + **Create**.

Enter the following details:

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

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



12.2: Add Route to Route Table

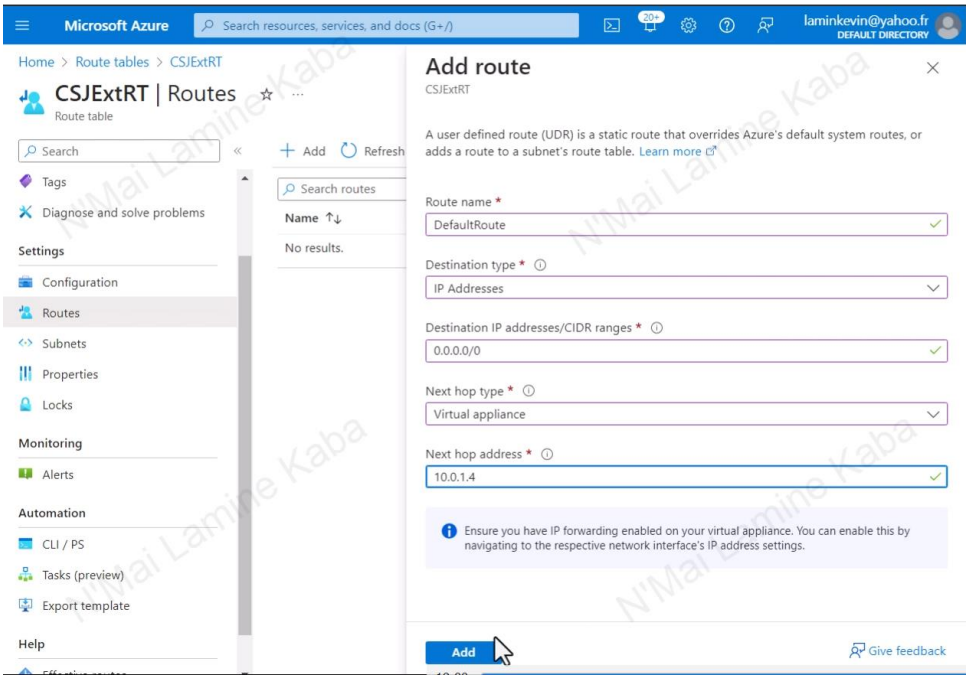
Select the newly created route table (`**CSJExtRT**`).

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

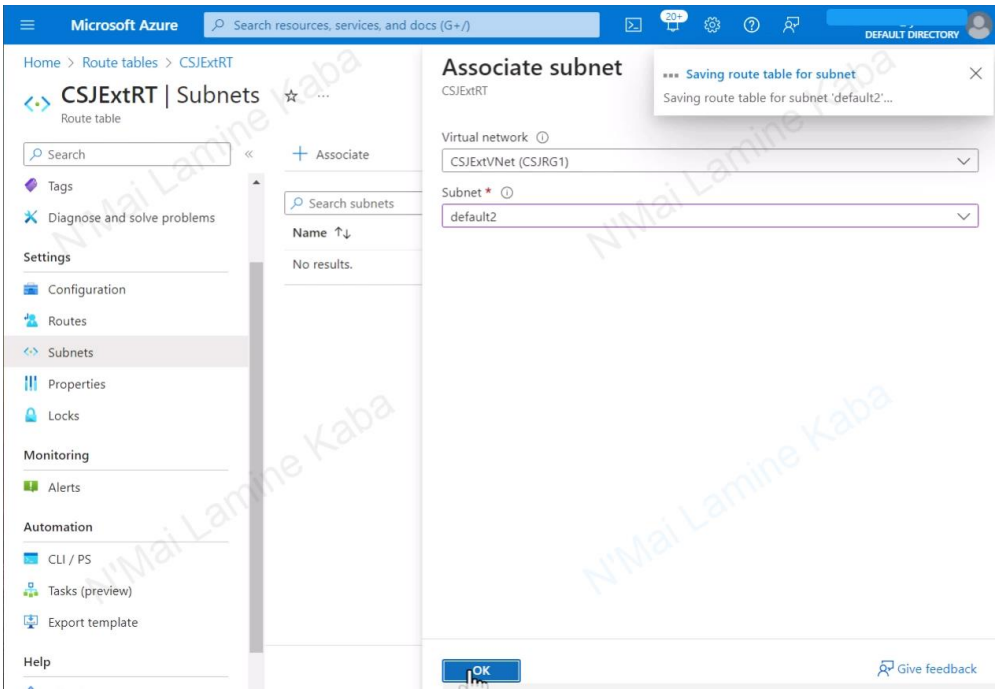
In the route table (`**CSJExtRT**`), under **Settings**, select **Subnets**.

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**.

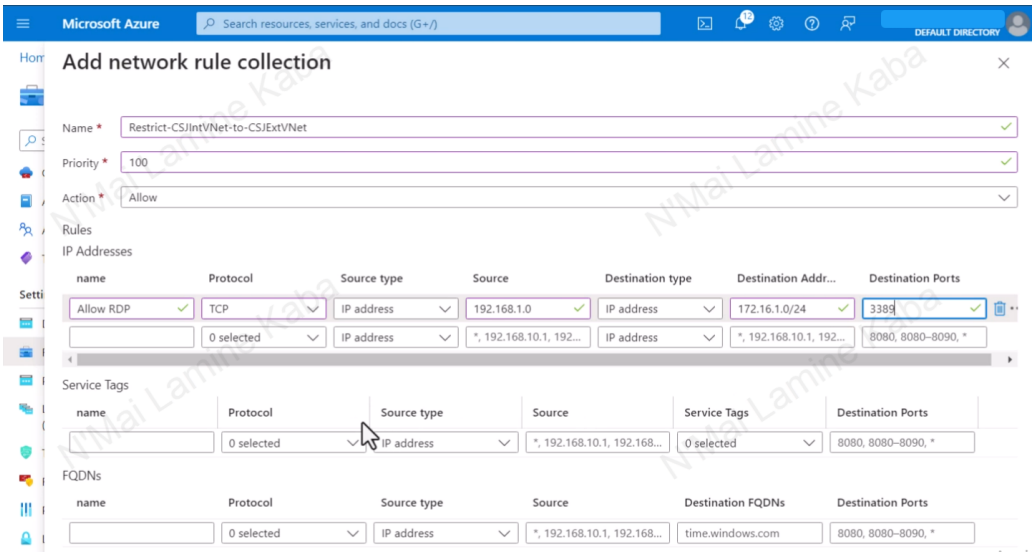
Enter the following details:

- 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**`

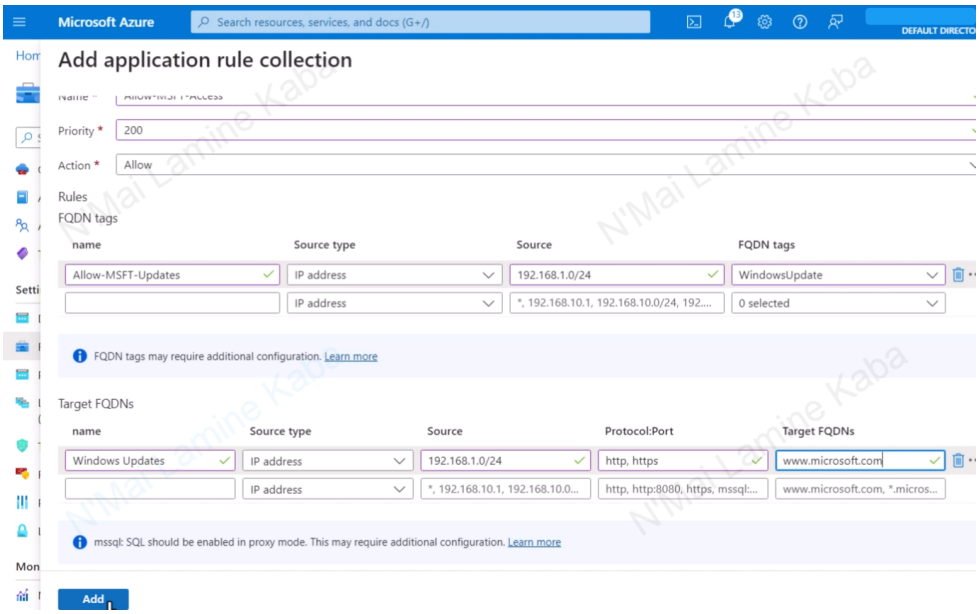
Under **FQDN tags**, enter the following:

- 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**.



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**.

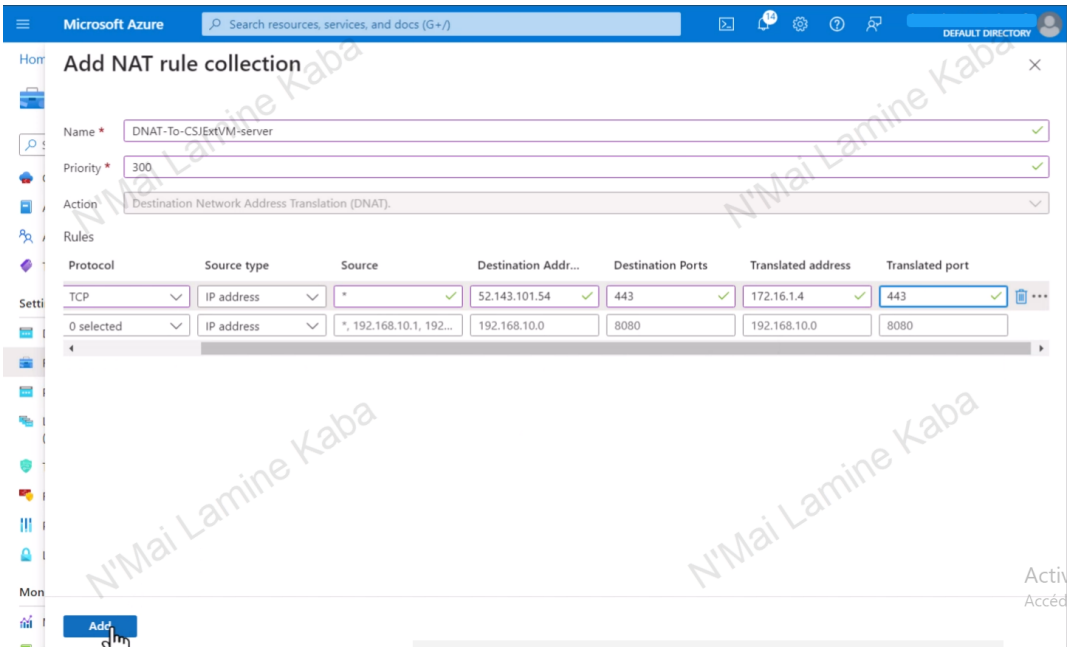
Enter the following details:

- 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**.



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.

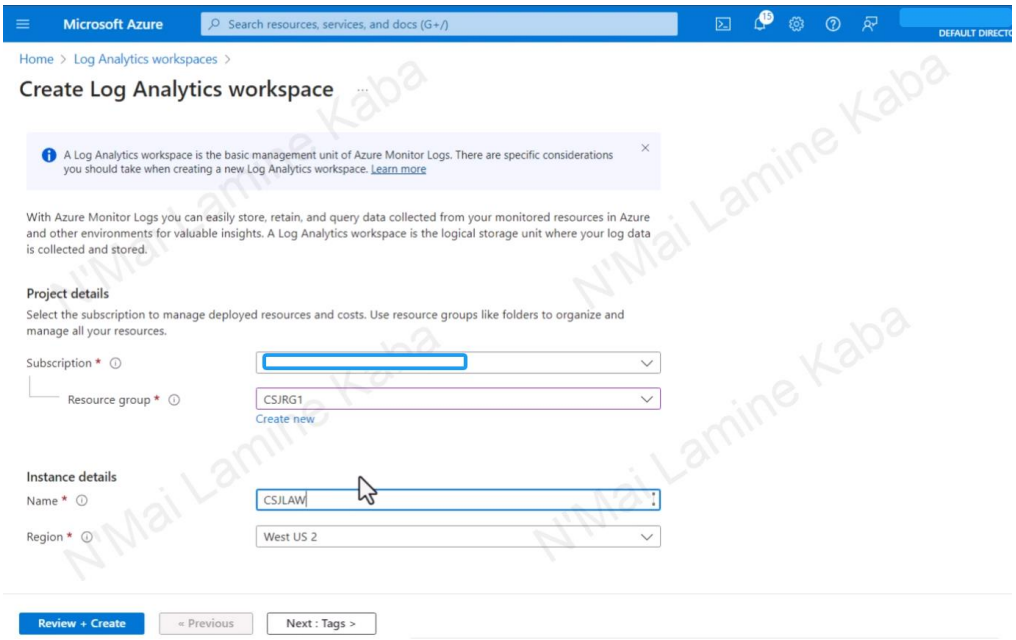
14.1: Create Log Analytics Workspace

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**.



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

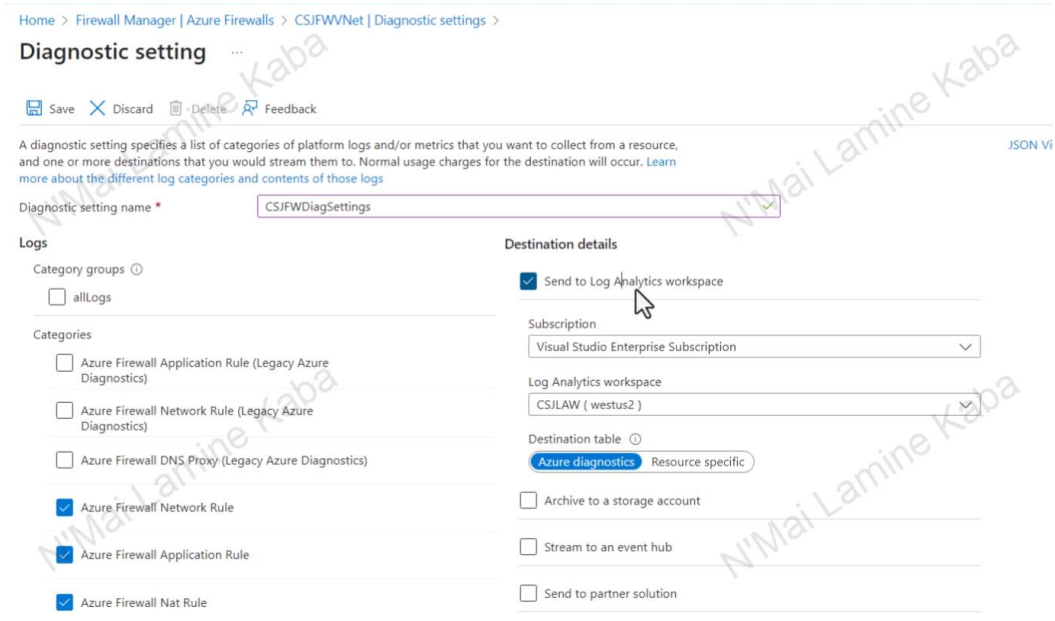
Navigate to **Firewalls** and select `**CSJFW**`.

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**.



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:

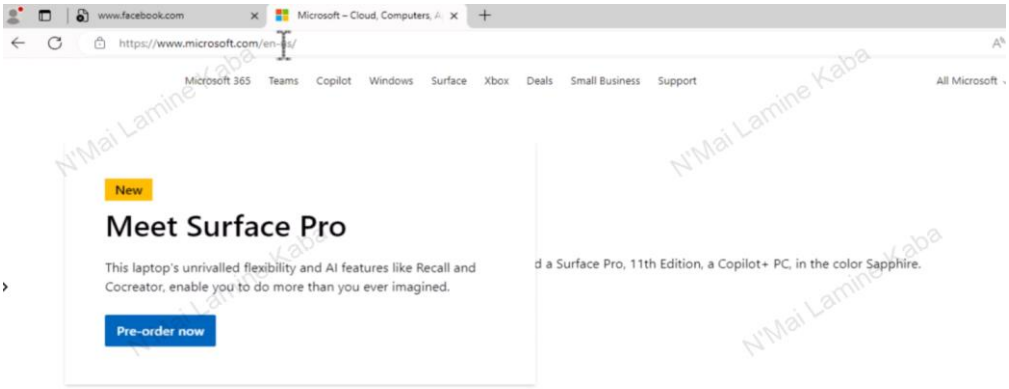
www.youtube.com/@CybersecJourneywithLamine

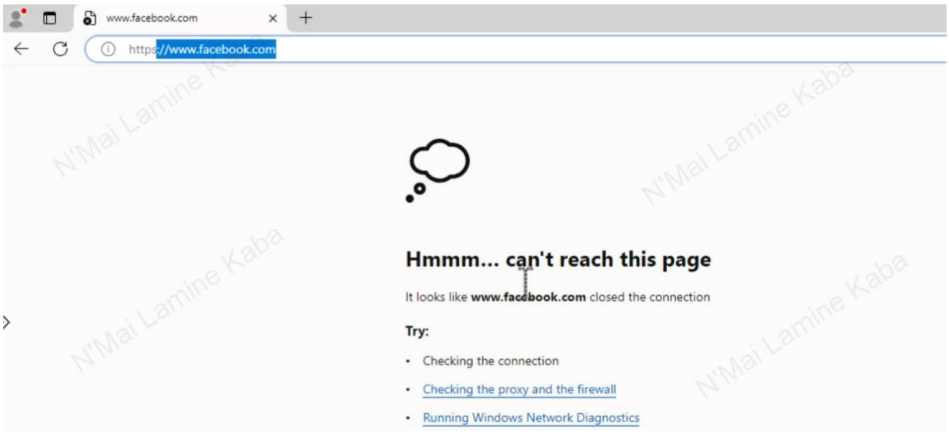
Step 15.2: Test Internet Access from CSJIntVNet

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).



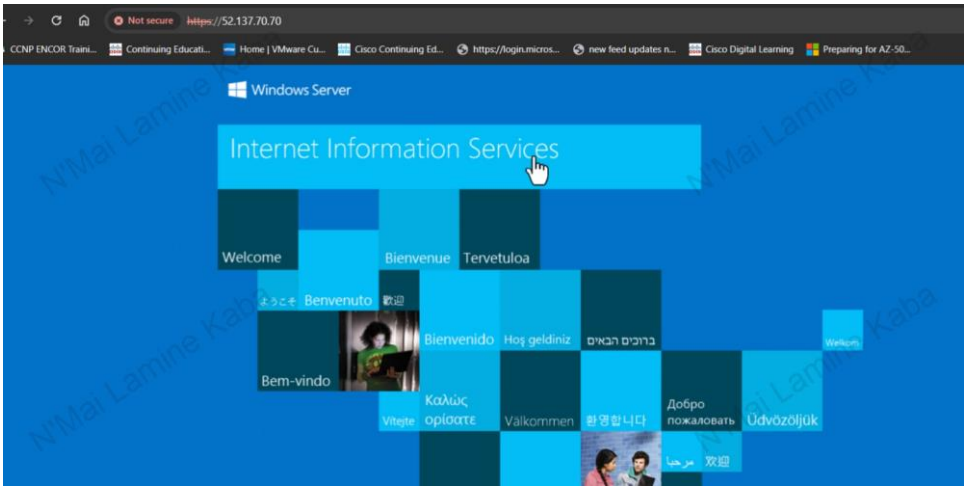


Step 15.3: Test DNAT Configuration (Internet to Internal VM)

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:

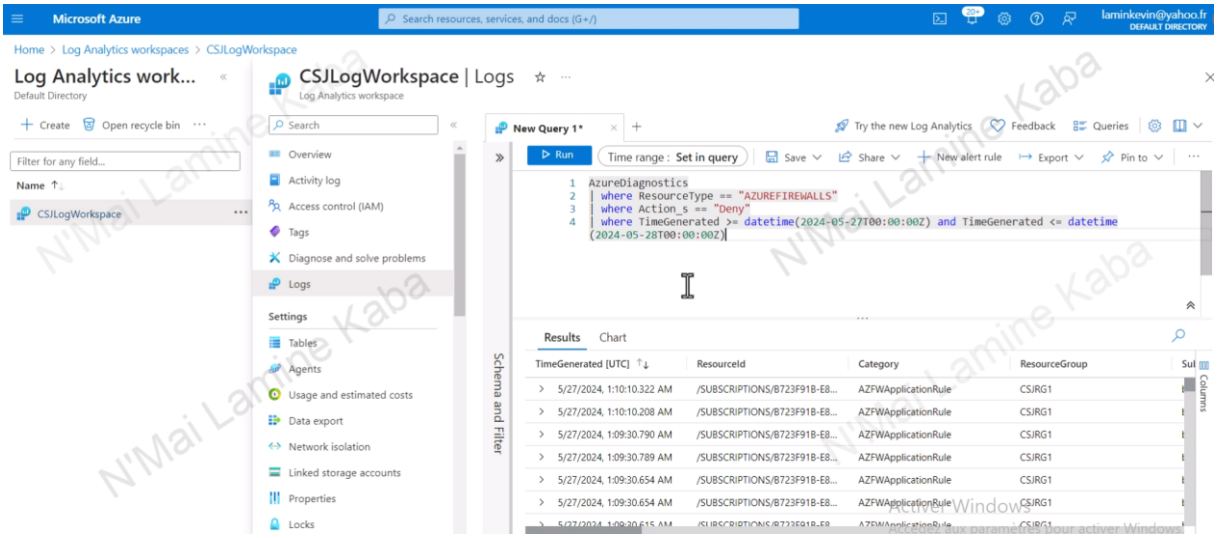
Query for Denied Connections:

```
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

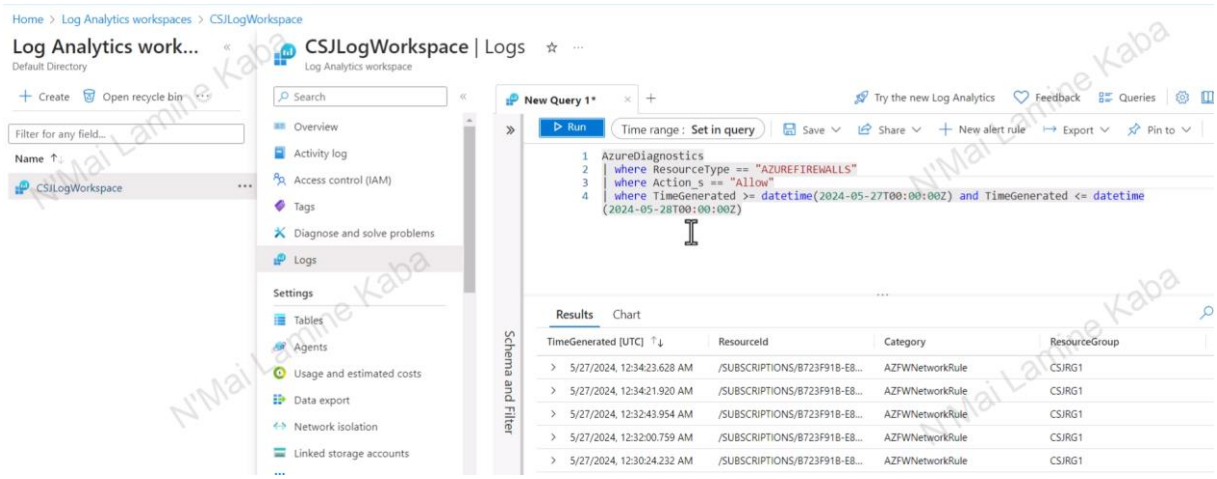


Query for Allowed Connections:

AzureDiagnostics

| where ResourceType == "AZUREFIREWALLS"

| where Action == "Allow"



| 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.