THISARA KANDAGE

UNDERGRADUATE - SLIIT

E-mail LinkedIn GitHub Website

An Integrated Approach to Secure Web Application Deployment on Azure Using Bastion Access, Virtual Network Firewalls, and NGINX Reverse Proxy on Virtual Machines

Project Overview->

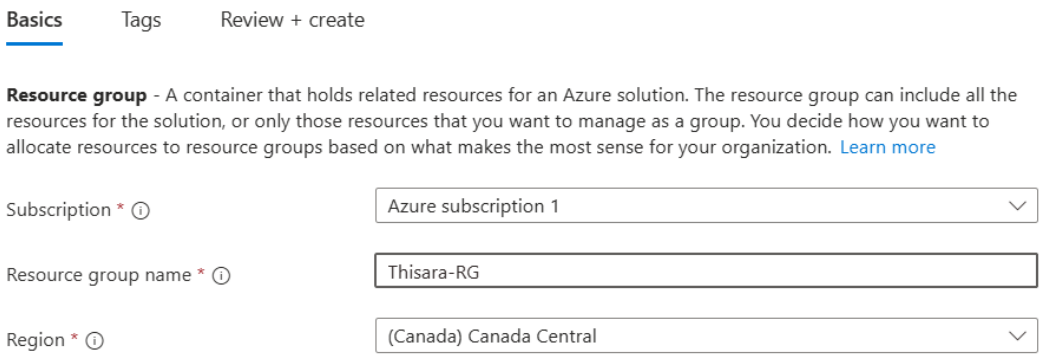
In this project, we will create a **Virtual Network (VNet)** in Azure and deploy an **Azure Firewall** to control and secure inbound and outbound traffic.

Behind the firewall, we will configure a **subnet** called **Web Application Subnet**, in which we will deploy a **Virtual Machine (VM)**. On this VM, we will install **Nginx** and host a simple HTML web page.

Since the VM will have only a **private IP address**, it will not be directly accessible from the internet. To securely connect to the VM, we will use **Azure Bastion**. This service allows secure RDP/SSH connections to the VM through the Azure Portal without exposing the VM to the public internet.

We will also configure **firewall rules** so that **authenticated users** can bypass the firewall and access the Nginx application hosted on the VM.

1. Starting with creating a resource group



THISARA KANDAGE

UNDERGRADUATE - SLIIT

E-mail LinkedIn GitHub Website

2. Create Virtual Network (VNet)

Project details

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

Subscription * Azure subscription 1

Resource group * Thisara-RG

Create new

Instance details

Virtual network name * Thisara-VNet

Region * (Canada) Canada Central

Deploy to an Azure Extended Zone

- **Create azure Bastian service**

Azure Bastion

Azure Bastion is a paid service that provides secure RDP/SSH connectivity to your virtual machines over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address. Learn more.

Learn more.

Enable Azure Bastion

Azure Bastion host name Thisara-VNet-Bastion

Azure Bastion public IP address * (New) thisara-vnet-bastion

Create a public IP address

THISARA KANDAGE

UNDERGRADUATE - SLIIT

E-mail LinkedIn GitHub Website

- **Create firewall policies**

Azure Firewall name	Thisara-VNet-Firewall
Subnet name *	AzureFirewallSubnet
Tier *	Basic
Policy *	(New) Thisara-VNet-firewall-policy Create new
Azure Firewall public IP address *	(New) thisara-vnet-firewall Create a public IP address
Management traffic public IP address *	(New) thisara-vnet-traffic-management Create a public IP address

- Subnets

Subnets	IP address range	Size	NAT gateway
WebApp	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-
AzureBastionSubnet	10.0.1.0 - 10.0.1.63	/26 (64 addresses)	-
AzureFirewallSubnet	10.0.1.64 - 10.0.1.127	/26 (64 addresses)	-
AzureFirewallManagementS	10.0.1.128 - 10.0.1.191	/26 (64 addresses)	-

THISARA KANDAGE

UNDERGRADUATE - SLIIT

E-mail LinkedIn GitHub Website

3. Azure Virtual Machine creation Steps

Project details

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

Subscription * ⓘ — Azure subscription 1

Resource group * ⓘ — Thisara-RG

Create new

Instance details

Virtual machine name * ⓘ — nginx-web

Region * ⓘ — (Canada) Canada Central

Deploy to an Azure Extended Zone

Availability options ⓘ — Availability zone

Zone options ⓘ

- (●) Self-selected zone
  Choose up to 3 availability zones, one VM per zone
- ( ) Azure-selected zone (Preview)
  Let Azure assign the best zone for your needs

Administrator account

Authentication type ⓘ

- (●) SSH public key
- ( ) Password

ⓘ Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.

Username * ⓘ — azureuser

SSH public key source — Generate new key pair

SSH Key Type

- (●) RSA SSH Format
- ( ) Ed25519 SSH Format

ⓘ Ed25519 provides a fixed security level of no more than 128 bits for 256-bit key, while RSA could offer better security with keys longer than 3072 bits.

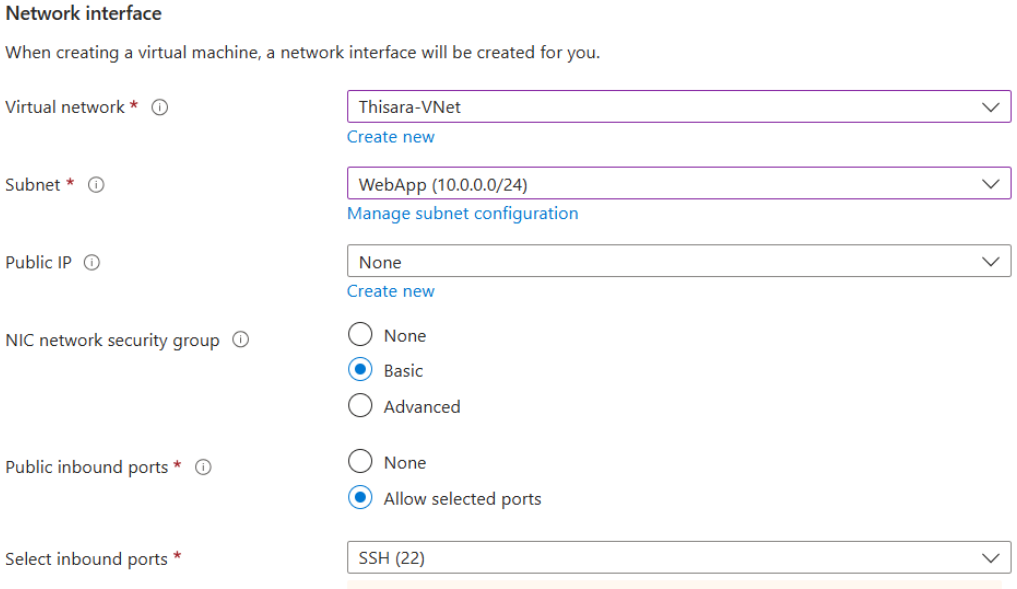
Key pair name * — nginx-web1_key

THISARA KANDAGE

UNDERGRADUATE - SLIIT

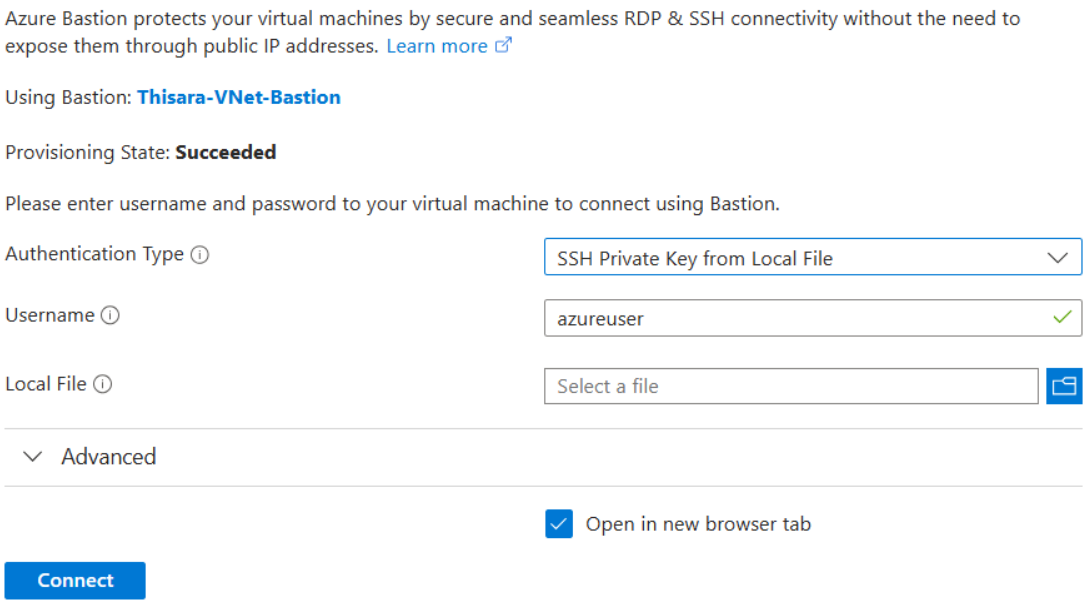
E-mail LinkedIn GitHub Website

- **Network configurations**



Without a public IP we can't SSH to the VM. so, we need to set up Bastian service

4. Connect VM via Bastian



THISARA KANDAGE

UNDERGRADUATE - SLIIT

E-mail LinkedIn GitHub Website

```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

azureuser@nginx-web1:~$
azureuser@nginx-web1:~$
azureuser@nginx-web1:~$
azureuser@nginx-web1:~$ ll
total 28
drwxr-x--- 4 azureuser azureuser 4096 Aug  8 15:30 ./
drwxr-xr-x 3 root      root      4096 Aug  8 14:58 ../
-rw-r--r-- 1 azureuser azureuser  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 azureuser azureuser 3771 Mar 31  2024 .bashrc
drwx------ 2 azureuser azureuser 4096 Aug  8 15:30 .cache/
-rw-r--r-- 1 azureuser azureuser  807 Mar 31  2024 .profile
drwx------ 2 azureuser azureuser 4096 Aug  8 14:58 .ssh/
azureuser@nginx-web1:~$
```

In here I use Bastian as a proxy

5. Connect to root

```
azureuser@nginx-web1:~$ sudo su -
root@nginx-web1:~#
root@nginx-web1:~#
root@nginx-web1:~#
root@nginx-web1:~#
```

6. Nginx installation

```
root@nginx-web1:~# apt-get install nginx -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  nginx-common
Suggested packages:
  fcgiwrap nginx-doc ssl-cert
The following NEW packages will be installed:
```

THISARA KANDAGE

UNDERGRADUATE - SLIIT

E-mail LinkedIn GitHub Website

7. Create HTML file in correct path

```
root@nginx-web1:~# cd /var/www/html
root@nginx-web1:/var/www/html#
root@nginx-web1:/var/www/html#
root@nginx-web1:/var/www/html# vim index.html
```

```
~
<!DOCTYPE html>
<html lang="en">
        <head>
                <meta charset="UTF-8">
                    <meta name="viewport" content="width=device-width, initial-scale=1.0">
                        <title>Demo Page</title>
        </head>
        <body>
                <h1> I Learnt how networking works in Azure today</h1>
        </body>
</html>
~
~
```

8. Restart Nginx

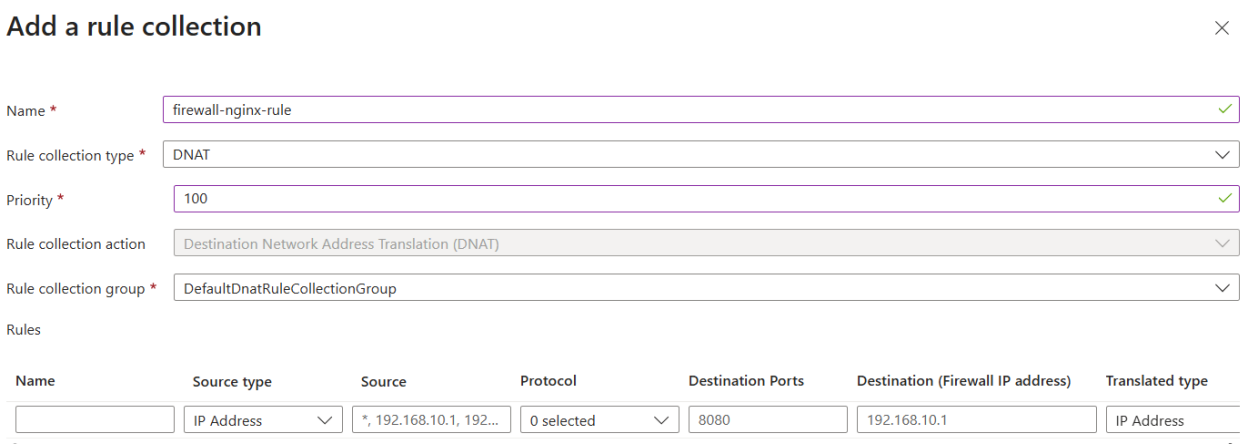
```
root@nginx-web1:/var/www/html# systemctl restart nginx
root@nginx-web1:/var/www/html#
root@nginx-web1:/var/www/html#
```

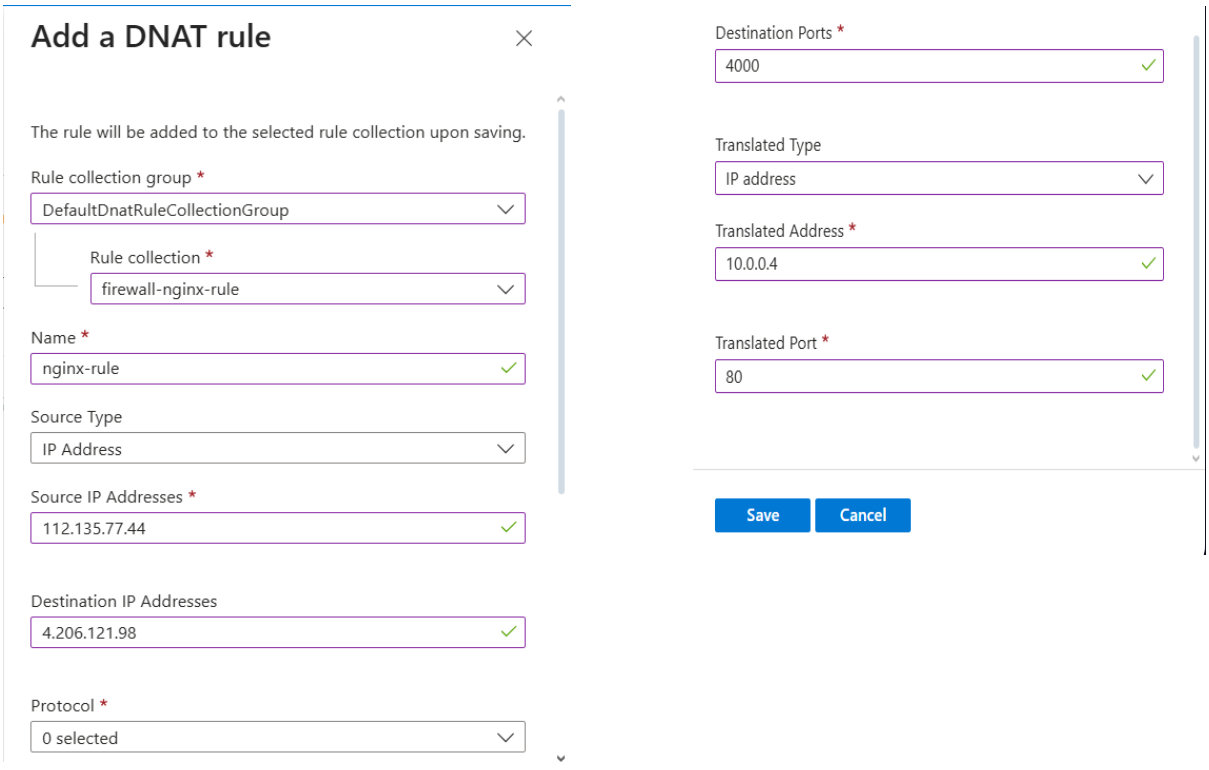
THISARA KANDAGE

UNDERGRADUATE - SLIIT

E-mail LinkedIn GitHub Website

9. Setup Firewall DNAT rules





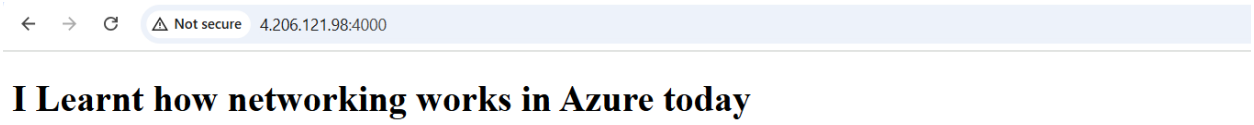
What I have done here is: if the IP address **112.135.77.44** sends a request to the firewall (**4.206.121.98**) on port **4000**, it will be translated to the IP address **10.0.0.4** (the IP of the Nginx VM) on port **80**.

THISARA KANDAGE

UNDERGRADUATE - SLIIT

E-mail LinkedIn GitHub Website

10. Access the webapp trough the browser



Summary:

I successfully set up a secure cloud infrastructure on Azure by creating and configuring:

- **Virtual Network (VNet)** for network segmentation and security.
- **Azure Bastion** to enable secure, browser-based RDP/SSH access to the VM without exposing public Ips.
- **Network Security Groups (NSGs)** and **VNet Firewall rules** to control inbound and outbound traffic.
- **Linux Virtual Machine** hosted inside the VNet.
- **NGINX** installed and configured on the VM for web server hosting.

This setup follows best practices for secure remote management and restricted network access, ensuring both **security** and **functionality** in a cloud environment.