



# 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

### Basics

### Tags

### Review + create

**Resource group** - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

Subscription \* ⓘ

Azure subscription 1

Resource group name \* ⓘ

Thisara-RG

Region \* ⓘ

(Canada) Canada Central



## 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.](#)

Enable Azure Bastion ⓘ

☒

Learn more.

Azure Bastion host name

Thisara-VNet-Bastion

Azure Bastion public IP address \*

(New) thisara-vnet-bastion

Create a public IP address



• 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)	-	
AzureFirewallManagement	10.0.1.128 - 10.0.1.191	/26 (64 addresses)	-	



## 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 *	<input type="text" value="Azure subscription 1"/>
Resource group *	<input type="text" value="Thisara-RG"/>

[Create new](#)

### Instance details

Virtual machine name *	<input type="text" value="nginx-web"/>
Region *	<input type="text" value="(Canada) Canada Central"/>
Availability options	<input type="text" value="Availability zone"/>
Zone options	<div><div><input checked="" type="radio"/> Self-selected zone</div><div>Choose up to 3 availability zones, one VM per zone</div><div><input type="radio"/> Azure-selected zone (Preview)</div><div>Let Azure assign the best zone for your needs</div></div>

### Administrator account

Authentication type	<div><div><input checked="" type="radio"/> SSH public key</div><div><input type="radio"/> Password</div></div> <div><div><div><b>i</b></div><div>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.</div></div></div>
Username *	<input type="text" value="azureuser"/>
SSH public key source	<input type="text" value="Generate new key pair"/>
SSH Key Type	<div><div><input checked="" type="radio"/> RSA SSH Format</div><div><input type="radio"/> Ed25519 SSH Format</div></div> <div><div><b>i</b></div><div>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.</div></div>
Key pair name *	<input type="text" value="nginx-web1_key"/>



- **Network configurations**

## Network interface

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

Virtual network * ⓘ	<div>Thisara-VNet</div> <div>Create new</div>
Subnet * ⓘ	<div>WebApp (10.0.0.0/24)</div> <div>Manage subnet configuration</div>
Public IP ⓘ	<div>None</div> <div>Create new</div>
NIC network security group ⓘ	<div><input type="radio"/> None</div> <div><input checked="" type="radio"/> Basic</div> <div><input type="radio"/> Advanced</div>
Public inbound ports * ⓘ	<div><input type="radio"/> None</div> <div><input checked="" type="radio"/> Allow selected ports</div>
Select inbound ports *	<div>SSH (22)</div>

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

## 4. Connect VM via Bastian

Azure Bastion protects your virtual machines by secure and seamless RDP & SSH connectivity without the need to expose them through public IP addresses. [Learn more](#)

Using Bastion: **Thisara-VNet-Bastion**

Provisioning State: **Succeeded**

Please enter username and password to your virtual machine to connect using Bastion.

Authentication Type ⓘ	<div>SSH Private Key from Local File</div>
Username ⓘ	<div>azureuser</div>
Local File ⓘ	<div>Select a file</div>

Advanced

☒ Open in new browser tab

Connect



```
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:  
  nginx nginx-common
```



## 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#
```



## 9. Setup Firewall DNAT rules

### Add a rule collection

Name \*

Rule collection type \*

Priority \*

Rule collection action

Rule collection group \*

Rules

Name	Source type	Source	Protocol	Destination Ports	Destination (Firewall IP address)	Translated type
<input type="text"/>	<input type="text" value="IP Address"/>	<input type="text" value="*, 192.168.10.1, 192..."/>	<input type="text" value="0 selected"/>	<input type="text" value="8080"/>	<input type="text" value="192.168.10.1"/>	<input type="text" value="IP Address"/>

### Add a DNAT rule

The rule will be added to the selected rule collection upon saving.

Rule collection group \*

Rule collection \*

Name \*

Source Type

Source IP Addresses \*

Destination IP Addresses

Protocol \*

Destination Ports \*

Translated Type

Translated Address \*

Translated Port \*

Save

Cancel

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**.





## 10. Access the webapp trough the browser



**I Learnt how networking works in Azure today**

### 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.