

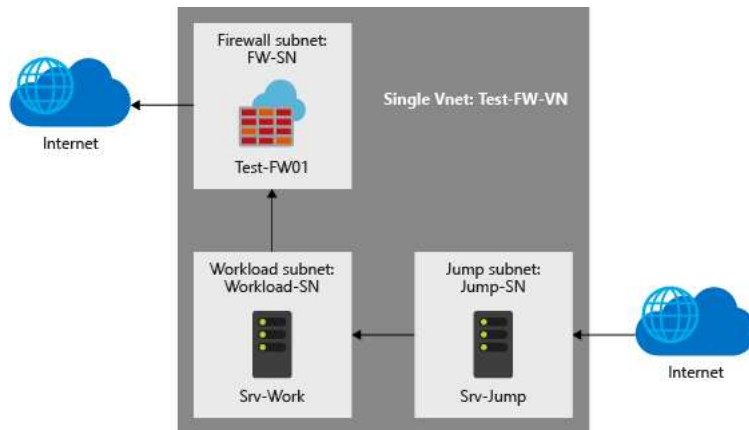
Module 5 - Lab 3: Deploy Azure Firewall

? Scenario

In this lab, you will learn how Azure Firewall can be deployed in your environment. Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources.

- Deploy Azure Firewall.
- Create default routes to change the traffic flows through the firewall and setup rules on the firewall.

? What you will build



Exercise 1: Create a Network

Task 1: Create a Virtual Network

1. Login to the **Azure Port** <https://portal.azure.com> with the username sheikhnasir4K010@gdcs4.com and password [Jb7bs02ehAtRoLsG](#)
2. Expand the portal's left navigation by clicking **Show portal menu** in the top left.

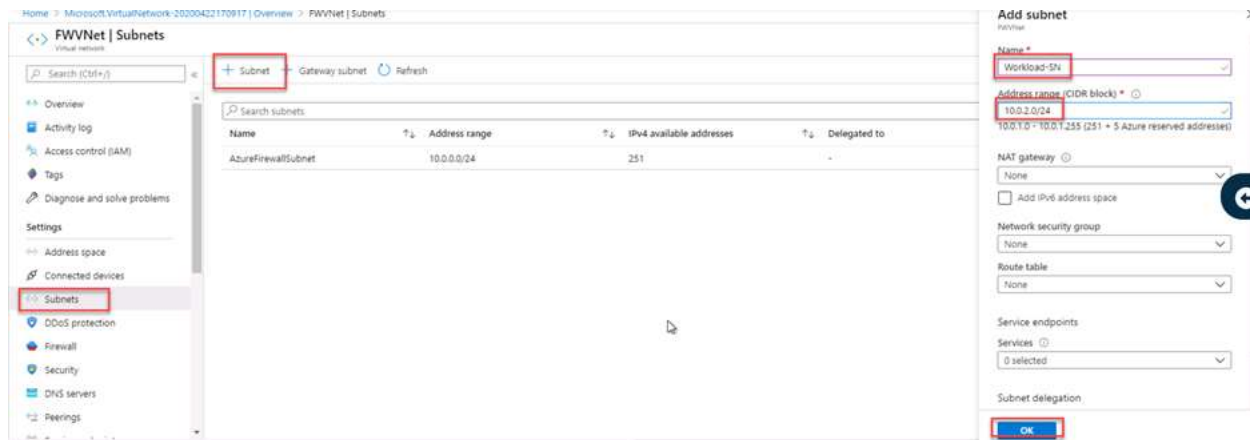


3. From within the **Azure Portal**, click + **Create a resource** and then select **Networking** -> **Virtual Network**
4. Select **+Create** and Specify the following settings for your new virtual network then click **Next: IP Addresses**.
 - Resource Group: Select **unrecognised token (\$gd.com(azure).resourceGroups(AzureFirewallRG))**
 - Name: [FWVNet](#)
 - Region: **East US**
5. Enter the following settings then click **Review + Create** then **Create**.
 - IPv4 Address Space: **10.0.0.0/16**
 - Click **Default** then enter the following configuration and click **Save**.
 - Subnet name: [AzureFirewallSubnet](#)
 - Subnet address Range: **10.0.0.0/24**

Note: We'll deploy the Azure Firewall in a later step.

Task 2: Create the subnets required

- ☐ 1. In the Azure portal, select **Virtual Networks** from the left navigation.
- ☐ 2. Select the **FWVNet** virtual network
- ☐ 3. Under **Settings** on the left, click **Subnets**. Click + **Subnet** to create a new subnet using the following settings and click **Save**.
 - Name: **Workload-SN**
 - Address range: **10.0.2.0/24**



- ☐ 4. Add another subnet using the following settings:
 - Name: **Jump-SN**
 - Address range: **10.0.3.0/24**

- ☐ 5. Accept the defaults and click **Save**.



You have now created all the necessary networking infrastructure. Next you will create a virtual machine.

Task 3: Create a virtual machine to use as a jump box

- ☐ 1. Within the Azure portal, click + **Create a Resource** and choose **Windows Server 2019 Datacenter**.
- ☐ 2. Specify the following configuration:
 - Resource Group: Select **unrecognised token (\$gd.com(azure).resourceGroups(AzureFirewallRG))**
 - Virtual machine name: **Srv-Jump**
 - Region: **East US**
 - Size: **IMPORTANT** - ensure the size is set to **Standard D2s v3**
 - Username: **localadmin**
 - Password/Confirm Password: **Jb7bs02ehAtRoLsG**
 - Inbound Port Rules: choose **Allow selected ports**, and enable **RDP (3389)**
- ☐ 3. At the top of the page click the **Networking** tab.
 - Set the Virtual Network to **FWVNet** and the subnet to **Jump-SN**
 - Public IP: If it is not already created, click **Create new** and name it **Srv-Jump-ip** and click **OK**.
- ☐ 4. Click **Review + create** and then click **Create**.

Task 4: Create a virtual machine to use as the protected server

- ☐ 1. Create another **Windows Server 2019 Datacenter** virtual machine using the following values:
 - Resource Group: **unrecognised token (\$gd.com(azure).resourceGroups(AzureFirewallRG))**
 - Virtual machine name: **Srv-Work**
 - Region: **East US**
 - Size: **IMPORTANT** - ensure the size is set to **Standard D2s v3**

- Username:  `localadmin`
- Password/Confirm Password:  `Jb7bs02ehAtRoLsG`
- On the **Networking** tab on the top.
 - Virtual Network: **FWVNet**
 - Subnet: **Workload-SN**
 - Public IP: **None**

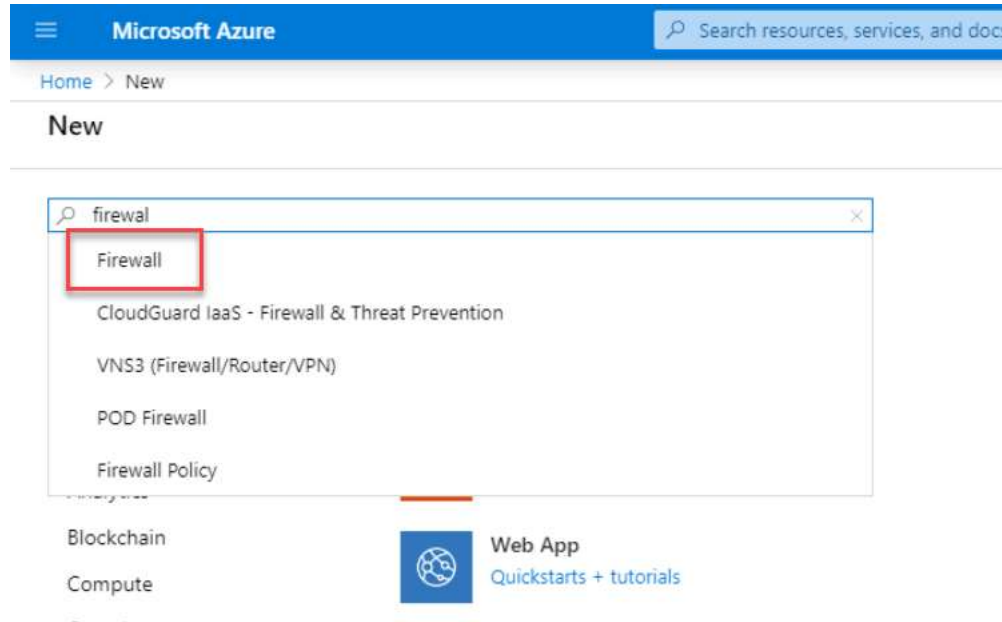
- ☐ 2. Click **Review + create** and then click **Create**.




At this point, we have all the necessary infrastructure ready and will now deploy the Azure Firewall.

Exercise 2: Deploy the Azure Firewall

Task 1: Deploy the Azure Firewall

- ☐ 1. In the portal, click + **Create a Resource** and search for Firewall. Click **Firewall** from the returned results and click **Create**.



- ☐ 2. Specify the following settings and click **Review + Create** and then **Create**.
- Resource Group: **unrecognised token (\$gd.com(azure).resourceGroups(AzureFirewallRG))**
 - Name:  `AzureFW`
 - Region: **East US**
 - Firewall Management: **Use Firewall rules (Classic) to manage this firewall**
 - Virtual network: **(use existing) FWVNet**
 - Public IP: **(create new)**  `azureFirewalls-ip`
 - Firewall Policy: **(create new)**  `azurefirewall-policy`

Create a firewall

Project details

* Subscription: OTA-PRD-731

* Resource group: AzureFirewallRG [Create new](#)

Instance details

* Name: AzureFW

* Region: (US) South Central US

Availability zone: None

Choose a virtual network: ☐ Create new ☒ Use existing

Virtual network: FWVNet (AzureFirewallRG)

* Public IP address: (New) azureFirewalls-ip [Create new](#)

[Review + create](#) [< Previous](#) [Next: Tags >](#) [Download a template for automation](#)

The Firewall will take a few minutes to deploy. Once completed we need to get the private ip address of the Firewall.

Navigate to the firewall and note the private ip address. Click **azureFirewalls-ip** then make note of the public ip addresses.

Dashboard > Resource groups > AzureFirewallRG > AzureFW

AzureFW
Firewall

Search (Ctrl+/)

Overview | Activity log | Access control (IAM) | Tags | Settings | Rules | Properties | Locks | Automation script | Monitoring | Metrics | Diagnostics logs | Support + troubleshooting | New support request

Resource group (change): AzureFirewallRG

Location: West US

Subscription (change): OTA-PRD-490

Subscription ID: 5468eb1a-0308-46e4-815b-d0247fb432fb

Tags (change): [Click here to add tags](#)

Virtual network/subnet: FWVNet/AzureFirewallSubnet

Private IP address: 10.0.0.4

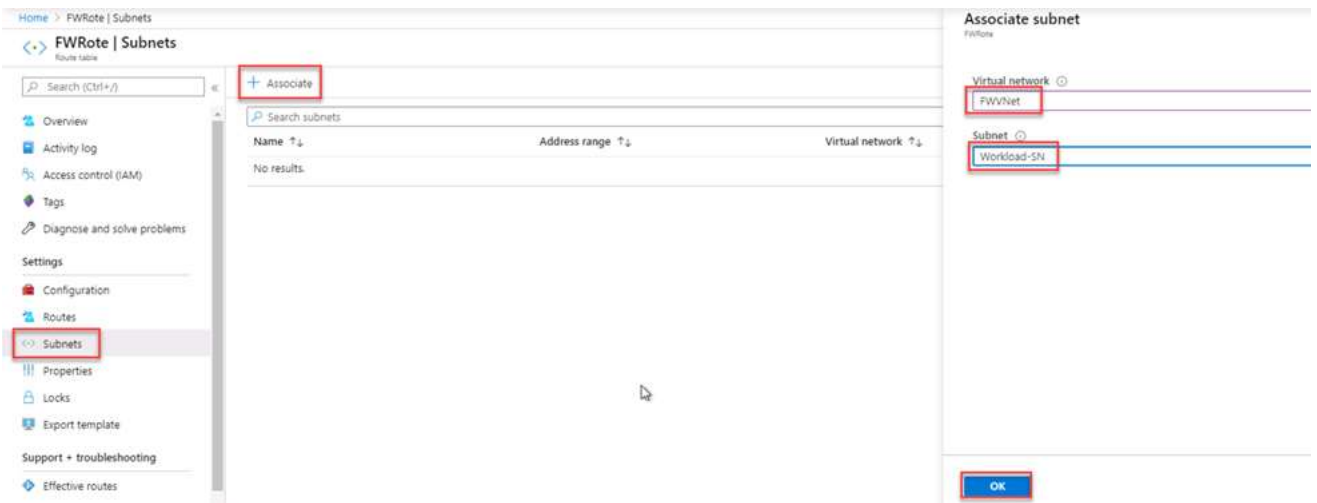
Public IP address: azureFirewalls-ip

Provisioning state: Succeeded

Task 2: Create the default route table

? We will now create the default route

- ☐ 1. In the portal, click + **Create a resource** then search for and select **Route Table** and click **Create**.
- ☐ 2. Specify the following configuration and click **Create**.
 - Name: [FW-Route](#)
 - Resource Group: **unrecognised token (\$gd.com(azure).resourceGroups(AzureFirewallRG))**
 - Location: **East US**
- ☐ 3. When the route table is created click **Go to Resource** in the notifications to open the route table you just created.
- ☐ 4. Select **Subnets** under **Settings** on the left and click + **Associate**. Choose the **FWVNet** virtual network and the **Workload-SN** subnet from the dropdowns and click **OK**.



Task 3: Add a route to the route table

- ☐ 1. Click **Routes** on the left under **Settings** and click + **Add**.
- ☐ 2. Specify the following configuration and click **OK**.
 - Route name: **FW-DG**
 - Address prefix: **0.0.0.0/0**
 - Next hop type: **Virtual appliance**
 - Next hop address: **The private ip address of your Azure firewall that you made note of earlier**

Dashboard > Resource groups > AzureFirewallRG > FW-Route - Routes > Add route

Add route

FW-Route

- * Route name: ✓
- * Address prefix: ✓
- Next hop type: ✓
- * Next hop address: ✓

Task 4: Configure an application rule

? You will now configure an application rule on the firewall.

- ☐ 1. Open the **AzureFirewallRG** resource group and select the AzureFW.
- ☐ 2. Under **Settings** on the left, click **Rules**.
- ☐ 3. Click **Application rule collection** then click + **Add application rule collection**
- ☐ 4. Specify the following configuration and click **Add**.
 - Name: **App-Coll01**
 - Priority: **200**
 - Action: **Allow**
 - Target FQDNs
 - Name: **AllowGH**
 - Source Addresses: **10.0.2.0/24**
 - Protocol: **http_https**
 - Target FQDN: **github.com**

Home > Resource groups > OpsTestAz

Test-FW - Firewall

Search (Ctrl+/)

Overview

Activity log

Access control (I

Tags

Settings

Rules

Properties

Locks

Automation scrip

Monitoring

Metrics

Diagnostics logs

Support + troublesho

Add application rule collection

* Name: App-Coll01

* Priority: 200

* Action: Allow

Rules

FQDN tags

NAME	SOURCE ADDRESSES
	* 192.168.10.1, 192.168.10.0/24, 192.168.10.2 - 192.16...

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

Target FQDNs

NAME	SOURCE ADDRESSES	PROTOCOL:PORT
AllowGH	10.0.2.0/24	http, https
	* 192.168.10.1, 192.168.10.0/24, 192.168...	http, http:8080, https

Add

You will now configure a network rule.

Task 5: Configure a network rule

- ☐ 1. Click **Network rule collection** then click + **Add network rule collection**
- ☐ 2. Specify the following configuration and click **Add**:
 - Name: **Net-Coll01**
 - Priority: **200**
 - Action: **Allow**
 - Rules (IP Addresses):
 - Name: **Allow-DNS**
 - Protocol: **UDP**
 - Source address: **10.0.2.0/24**
 - Destination Addresses: **8.8.8.8,1.1.1.1**
 - Destination port: **53**

Add network rule collection

Name *

Priority *

Action *

Rules

IP Addresses

name		Protocol	Source type	Source		Destination type	Destination
Allow-DNS	✓	UDP	IP address	10.0.2.0/24	✓	IP address	8.8.8.8, 1.1.1.1
		0 selected	IP address	*, 192.168.10.1, 192...		IP address	*, 192.168...

Service Tags

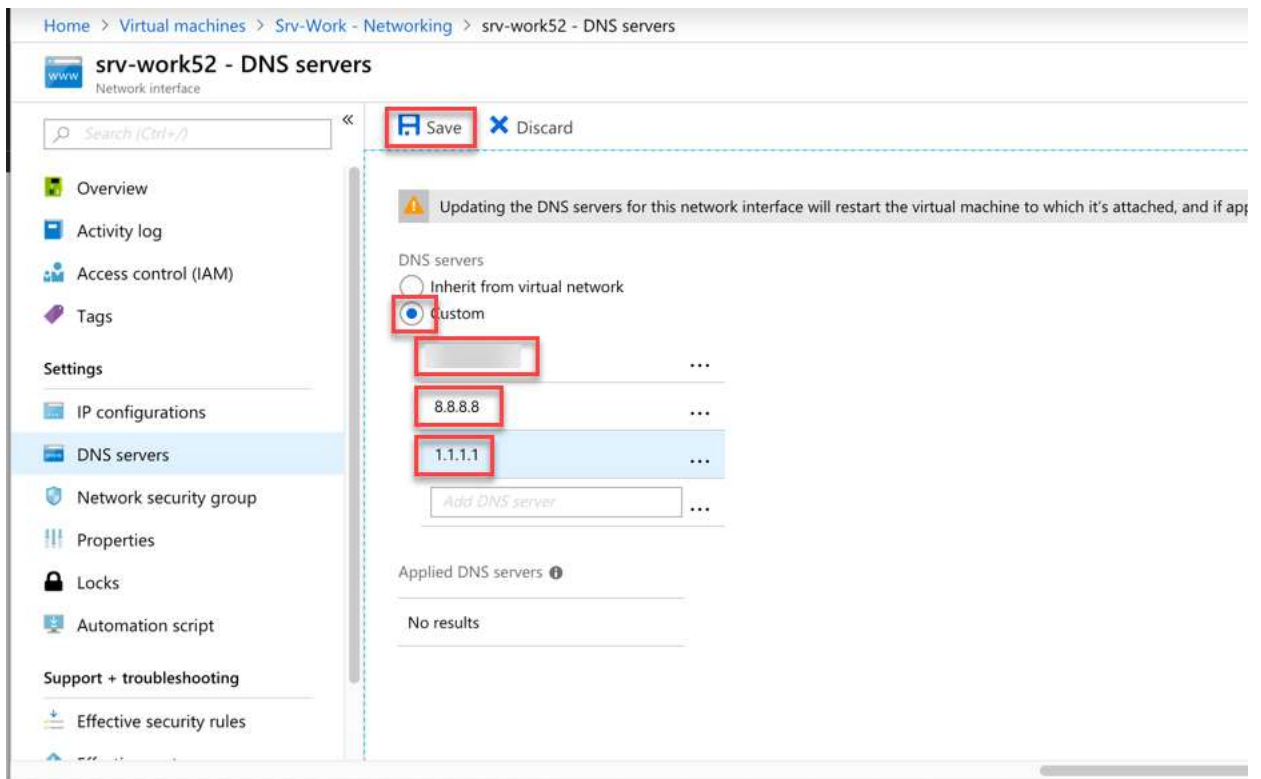
name		Protocol	Source type	Source		Service Tags
		0 selected	IP address	*, 192.168.10.1, 192.168...		0 selected



You will now change the DNS servers on the Srv-Work NIC

Task 6: Change DNS for Srv-Work NIC

- ☐ 1. Within the **Azure portal**, click **Virtual Machines** on the left navigation and open the **Srv-Work** VM.
- ☐ 2. Click **Networking** on the left under **Settings** then by where it says **Network Interface**; click **srv-workXXX** to open the network interface configuration.
- ☐ 3. Under **Settings** on the left click **DNS Servers** then click **Custom**.
- ☐ 4. Add the following DNS servers and click **Save**.
 - The AzureFW public IP address you noted earlier
 - 8.8.8.8
 - 1.1.1.1

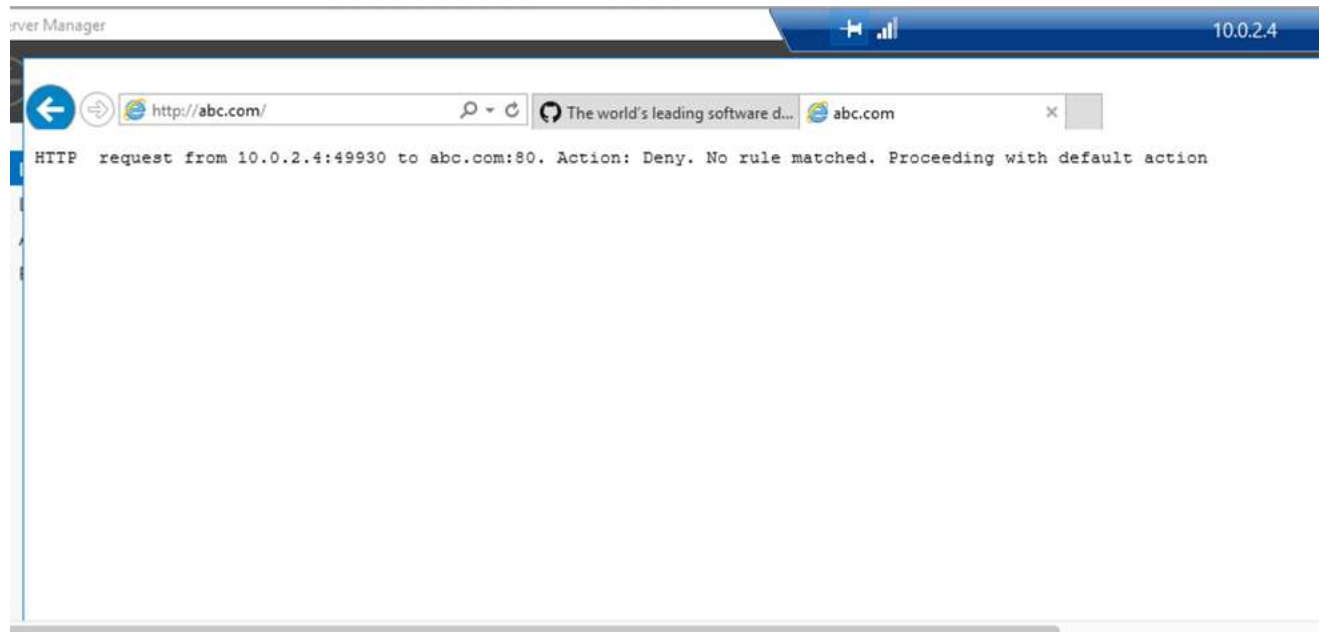


- ☐ 5. Upon completion restart the **Srv-Work** virtual machine by clicking **Restart** on the virtual machine overview page.

You will now test the firewall

Task 7: Testing

- ☐ 1. Note the private ip address of the Srv-Work VM on the **Overview** blade.
- ☐ 2. Click **Connect** then **RDP**. Download and open the RDP file, click **Connect** and login using:
 - Username: [localadmin](#)
 - Password: [Jb7bs02ehAtRoLsG](#)
- ☐ 3. From within **Srv-Jump** launch the remote desktop client by clicking the Windows start button, then search for and select **mstsc.exe**.
- ☐ 4. Enter the private ip address of **Srv-Work**, click **Connect** and login using the following credentials:
 - Username: [localadmin](#)
 - Password: [Jb7bs02ehAtRoLsG](#)
- ☐ 5. In the **Srv-Work** VM, start Internet Explorer and navigate to: <https://github.com>
- ☐ 6. This works (you will receive an error that GitHub no longer supports IE and several warnings - you can ignore all of them)
- ☐ 7. Now try another site: <http://abc.com>
- ☐ 8. This is blocked because no rule matched.



- ✓ **Results:** In this lab, you deployed a jump box and a simulated production server and then configured the Azure Firewall to only allow access to GitHub.com from the production server. You then tested by accessing the production server from a Jumpbox and connected to GitHub successfully and abc.com unsuccessfully because it is blocked.