

Valerie Kivayiru Jarenga
Cloud Security Specialist - C2 – 2025

Task 1: Use a template to deploy the lab environment.

The screenshot shows the Microsoft Azure portal interface. The main content area displays the deployment details for a template named 'Microsoft.Template-20250527151147'. The deployment is marked as 'complete'. The details include the deployment name, subscription (MOC Subscription-Iod50647090), resource group (AZ500LAB08), start time (5/27/2025, 3:12:16 PM), and correlation ID (ceabc695-e12d-49af-a447-53652ac4c691). The right sidebar shows the 'Azure Firewall' task with instructions and a progress bar. The instructions include steps for identifying Azure regions and clicking 'Review + create'.

Microsoft Azure

Home > Microsoft.Template-20250527151147 | Overview

Deployment

Inputs

Outputs

✓ Your deployment is complete

Deployment name : Microsoft.Template-20250527151147

Subscription : MOC Subscription-Iod50647090

Resource group : AZ500LAB08

Start time : 5/27/2025, 3:12:16 PM

Correlation ID : ceabc695-e12d-49af-a447-53652ac4c691

Deployment details

Next steps

Go to resource group

Azure Firewall

2 Hr 49 Min Remaining

Instructions Resources Help 110%

adminPassword

To identify Azure regions where you can provision Azure VMs, refer to <https://azure.microsoft.com/en-us/regions/offers/>

7. Click **Review + create**, and then click **Create**.

Wait for the deployment to complete. This should take about 2 minutes.

Task 2: Deploy the Azure firewall

15% Tasks Complete

Previous End

Task 2: Deploy the Azure firewall

The screenshot shows the Microsoft Azure portal interface. The main content area displays the details for the 'Test-FW01' firewall resource. The details include the resource group (AZ500LAB08), location (East US), subscription (MOC Subscription-Iod50647090), subscription ID (f3061296-e5d8-4956-8234-b13be138c986), virtual network (Test-FW-VN), and provisioning state (Succeeded). The right sidebar shows the 'Azure Firewall' task with instructions and a progress bar. The instructions include steps for identifying the 'Test-FW01' firewall and identifying the 'Private IP' address.

Home > Resource groups > AZ500LAB08 > Test-FW01

Firewall

Search

Migrate to firewall policy Delete Lock Change SKU

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Monitoring

Automation

Help

Essentials

Resource group (move) AZ500LAB08

Location East US

Subscription (move) MOC Subscription-Iod50647090

Subscription ID f3061296-e5d8-4956-8234-b13be138c986

Virtual network Test-FW-VN

Provisioning state Succeeded

SKU Standard(change)

Subnet AzureFirewallSubnet

Public IP TEST-FW-PIP

Private IP 10.0.1.4

Management subnet

Management public IP

Private IP Ranges IANA RFC 1918

Route Server (preview) Add

Azure Firewall

2 Hr 39 Min Remaining

Instructions Resources Help 110%

can sort by Type.

7. In the list of resources, click the entry representing the **Test-FW01** firewall.

8. On the **Test-FW01** blade, identify the **Private IP** address that was assigned to the firewall.

You will need this information in the next task.

Task 3: Create a default route

In this task, you will create a default route for the **Workload-SN** subnet. This route will configure outbound traffic through the firewall.

1. In the Azure portal, in the **Search resources**.

28% Tasks Complete

Previous End

Task 3: Create a default route

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Route tables > Firewall-route

Firewall-route | Routes

Route table

+ Add

Refresh

Give feedback

Search routes

Name ↑↓	Address prefix ↑↓	Next hop type ↑↓	Next hop IP address
FW-DG	0.0.0.0/0	VirtualAppliance	10.0.1.4

Azure Firewall

2 Hr 33 Min Remaining

Instructions Resources Help

Next hop type **Virtual appliance**

Next hop address the private IP address of the firewall that you identified in the previous task

Azure Firewall is actually a managed service, but virtual appliance works in this situation.

11. Click **Add** to add the route.

Task 4: Configure an application rule

46% Tasks Complete

Previous End

Task 4: Configure an application rule

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home > Firewall Manager | Azure Firewalls > Test-FW01

Test-FW01 | Rules (classic)

Firewall

Refresh

Updating firewall

NAT rule collection

Network rule collection

Application rule collection

+ Add application rule collection

Priority	Name	Action	Rules
200	App-Coll01	Allow	> 1 rule.

Azure infrastructure application rule collection is enabled by default. [Learn more](#)

Azure Firewall

2 Hr 30 Min Remaining

Instructions Resources Help

Protocol port **http, https**

Target FQDNS **www.bing.com**

6. Click **Add** to add the Target FQDNS-based application rule.

Azure Firewall includes a built-in rule collection for infrastructure FQDNS that are allowed by default. These FQDNS are specific for the platform and can't be used for other purposes.

Task 5: Configure a network rule

In this task, you will create a network rule that allows outbound access to two IP addresses on port 53 (DNS).

56% Tasks Complete

Previous End

Task 5: Configure a network rule

Microsoft Azure

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

Copilot

Home > Firewall Manager | Azure Firewalls > Test-FW01

Test-FW01 | Rules (classic)

Firewall

Refresh

Updating firewall

NAT rule collection

Network rule collection

Application rule collection

+ Add network rule collection

Priority	Name	Action	Rules
200	Net-Coll01	Allow	> 1 rule.

Instructions

Resources

Help

110%

Destination Ports

T 53

5. Click **Add** to add the network rule.

The destination addresses used in this case are known public DNS servers.

Task 6: Configure the virtual machine DNS servers

In this task, you will configure the primary and secondary DNS addresses for the virtual machine. This is not a firewall requirement.

1. In the Azure portal, navigate back to the **AZ500LAB08** resource group.

65% Tasks Complete

Task 7: Test the firewall

labclient.labondemand.com/LabClient/9969a58b-8cbd-4271-8fce-53bd6c31f200

Server Manager

172.191.193.7

http://www.microsoft.com/

microsoft.com

Action: Deny. Reason: No rule matched. Proceeding with default action.

Azure Firewall

2 Hr 10 Min Remaining

Instructions

Resources

Help

110%

The website should successfully display. The firewall allows you access.

10. Browse to

T http://www.microsoft.com/

Within the browser page, you should receive a message with text resembling the following:

T HTTP request from 10.0.2.4:xxxxx to microsoft.com:80. Action: Deny. No rule matched. Proceeding with default action.

This is expected, since the firewall blocks access to this website.

93% Tasks Complete

< Previous

End >

labclient.labondemand.com/LabClient/9969a58b-8cbd-4271-8fce-53bd6c31f200

Server Manager 172.191.193.7

http://www.microsoft.com/ microsoft.com

Action: Deny. Reason: No rule matched. Proceeding with default action.

Azure Firewall
2 Hr 10 Min Remaining

Instructions Resources Help 110%

The website should successfully display. The firewall allows you access.

10. Browse to `http://www.microsoft.com/`

Within the browser page, you should receive a message with text resembling the following:

HTTP request from 10.0.2.4:xxxxx to microsoft.com:80. Action: Deny. No rule matched. Proceeding with default action.

This is expected, since the firewall blocks access to this website.

93% Tasks Complete

Previous End

Azure Firewall - Google Chrome

labclient.labondemand.com/LabClient/9969a58b-8cbd-4271-8fce-53bd6c31f200

Admin

Reset password

Admin

Student

ENG

Azure Firewall
2 Hr 7 Min Remaining

Instructions Resources Help 110%

2. Ensure **PowerShell** is selected in the drop-down menu in the upper-left corner of the Cloud Shell pane.

3. In the PowerShell session within the Cloud Shell pane, run the following to remove the resource group you created in this lab:

```
powershell  
Remove-AzResourceGroup -Name "AZ"
```

4. Close the **Cloud Shell** pane.

Congratulations

100% Tasks Complete

Previous End

