

Implement an Azure Firewall using Azure Portal

Use Case:

From a network architecture perspective, we will create a single Virtual Network (VNET) which will contain three subnets. The three subnets will be

- AzureFirewallSubnet: Contains Azure Firewall and all workload server traffic will be routed through Azure Firewall.
- Workload-SN: Contains the Workload server i.e. a server where a production application would run. We create a default route so that this subnet's network traffic is configured to go through the firewall. The workload server will not have a publicly accessible connection available to it and will only be accessible via a *Jump server(Jump box)*. We will configure Azure Firewall to allow the workload server to access DNS servers over port 53 to allow it access web sites on the internet.
- Jump-SN: Contains a *Jump server* which has a public IP address that you can connect to using Remote Desktop. From there, you can then connect to (using another Remote Desktop) the workload server.

Prerequisites:

You require need an Azure subscription to perform these steps. If you don't have one you can create one by following the steps outlined on the [Create your Azure free account today](#) webpage.

Steps:

Create Resource group

1. Sign in to the Azure portal at <https://portal.azure.com>
2. On the Azure portal home page, click **Resource groups** > **Add** and use the following details and click **Review and Create** and then **Create**.

The screenshot displays the Azure portal's 'Resource groups' section. At the top, under 'Azure services', there are icons for 'Create a resource', 'Resource groups', 'Virtual networks', and 'Advisor'. Below this, the 'Recent resources' section lists various services like 'te', 'la', 'Co', 'cc', and 'cc'. A 'Navigate' section shows a 'Subscription' icon. A dropdown menu for 'Resource groups' is open, showing options to '+ Create' and 'View'. It also lists 'Recents' with 'CodeSizzlerIoTFactory-rg' from 4 days ago. Below that, it offers 'Free training from Microsoft' with a link to 'Control and organize Azure resources with Azu...' (8 units, 46 min). At the bottom of the dropdown are 'Useful links' for 'Overview' and 'Get Started'. The main content area is titled 'Resource groups' for 'JIJI TECHNOLOGIES PRIVATE LIMITED'. At the bottom, there is a toolbar with buttons for '+ Add', 'Edit columns', 'Refresh', 'Export to CSV', 'Assign tags', and 'Feedback'.

Azure services

- Create a resource
- Resource groups
- Virtual networks
- Advisor

Recent resources

- te
- la
- Co
- cc
- cc

Navigate

- Subscription

Resource groups ★

- + Create View

Recents

- CodeSizzlerIoTFactory-rg
4 d ago

Free training from Microsoft

- [Control and organize Azure resources with Azu...](#)
8 units · 46 min


Useful links

- [Overview](#)
- [Get Started](#)

Resource groups
JIJI TECHNOLOGIES PRIVATE LIMITED

+ Add Edit columns Refresh Export to CSV Assign tags Feedback

- **Subscription:** < select your own subscription >
- **Resource group:** az900-rg
- **Region:** < select a Datacenter location nearest to you. Note: All subsequent resources that you create must be in the same location. >

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](#) 

Project details

Subscription * 

Visual Studio Enterprise – MPN

Resource group * 

az900-rg

Resource details

Region * 

Southeas

Recommended 

(Asia Pacific) Southeast Asia

Other 

Click on create button.

ode \$izzler

Home > Resource groups > Create a resource group

Create a resource group

Create

✓ Validation passed.

Basics Tags Review + create

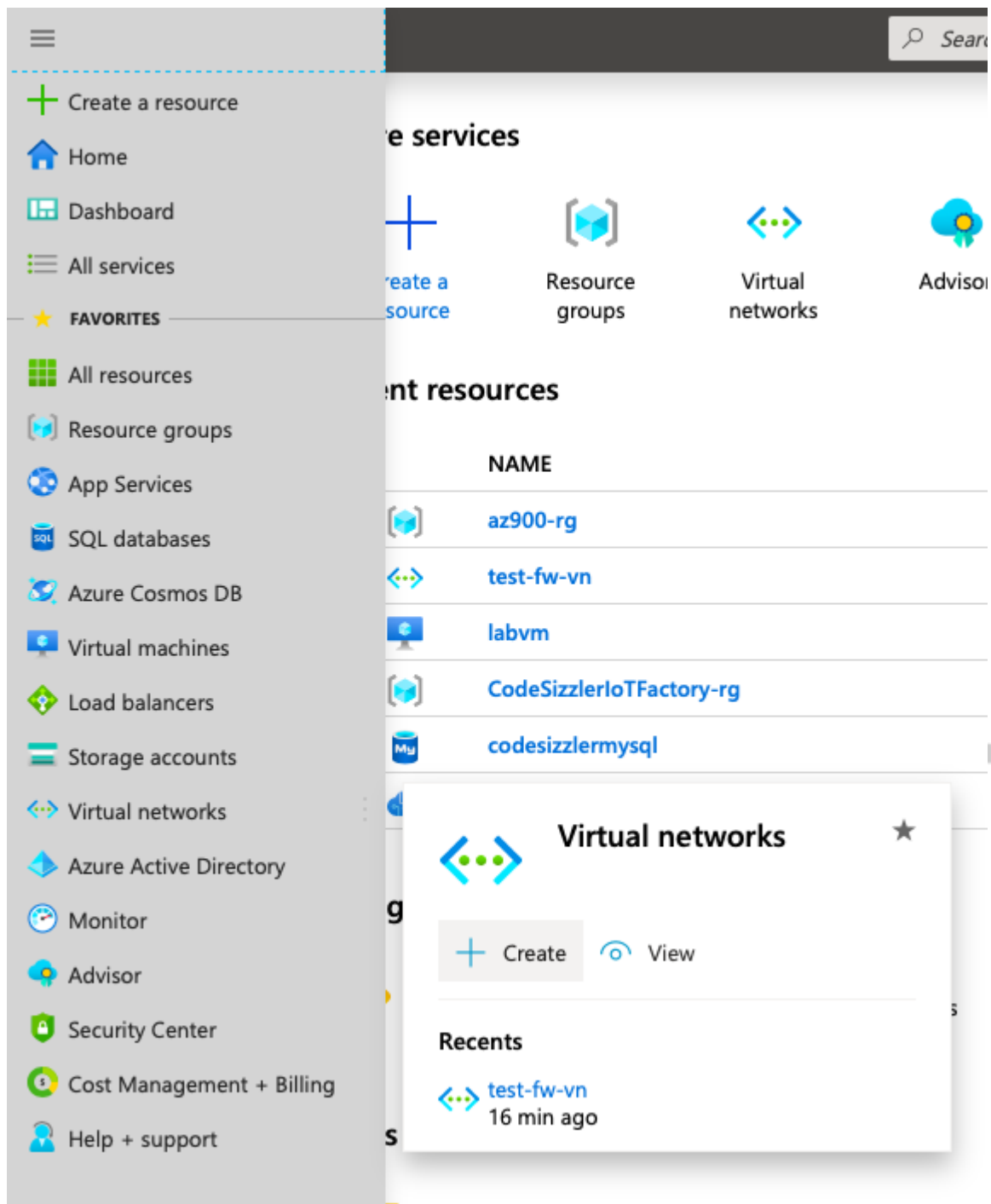
Basics

Subscription	Visual Studio Enterprise – MPN
Resource group	az900-rg
Region	(Asia Pacific) Southeast Asia

Create < Previous Next >

Create a VNET

1. From the Azure portal home page, click **All services** > **Networking** > **Virtual networks**.



2. Click **Add** and use the following details, leaving any other values as their default and click **Create** when finished

- **Name:** Test-FW-VN

Name *

Test-FW-VN ✓

- **Address space:** 10.0.0.0/16

Address space * ⓘ

10.0.0.0/16 ✓

10.0.0.0 - 10.0.255.255 (65536 addresses)

- **Subscription** : < select your subscription >

Subscription *

Visual Studio Enterprise – MPN ✓

- **Resource group**: < select resource group created earlier az900-rg >

Resource group *

az900-rg ✓

[Create new](#)

- **Location**: < select the same location that you used previously >

Location *

(Asia Pacific) Southeast Asia ✓

- **Subnet**>
- **Name**: AzureFirewallSubnet (The firewall will be in this subnet, and the subnet name must be AzureFirewallSubnet).
- **Address range**: 10.0.1.0/24

Subnet

Name *

AzureFirewallSubnet ✓

Address range * ⓘ

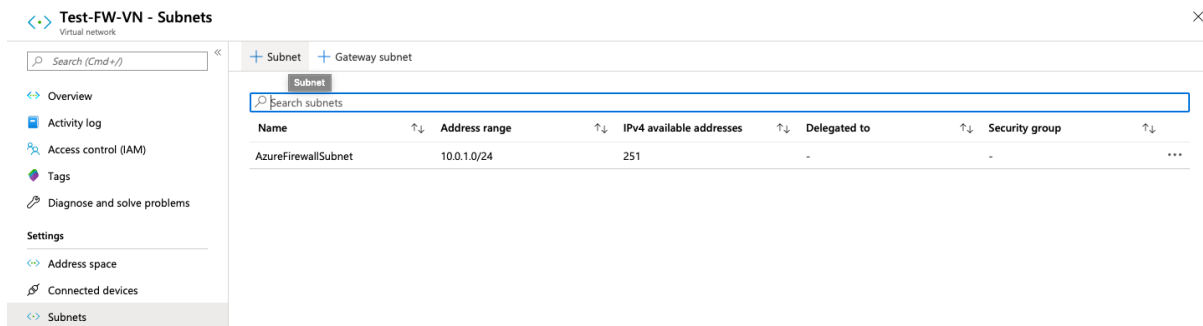
10.0.1.0/24 ✓

10.0.1.0 - 10.0.1.255 (256 addresses)

Create additional subnets

Next we will create some additional subnets, into which we will subsequently place two virtual machines.

1. On the Azure portal home page, click **Resource groups** > **az900-rg**.
2. Click the **Test-FW-VN** virtual network.
3. Click **Subnets** > **+ Subnet** and use the following details, leaving the remaining items at their default values and click **OK** when completed



- **Name:** Workload-SN
- **Address range:** 10.0.2.0/24

Name *

Workload-SN

Address range (CIDR block) * ⓘ

10.0.2.0/24

10.0.2.0 - 10.0.2.255 (251 + 5 Azure reserved addresses)

4. Create another subnet by repeating steps 1-3 above, using the values

- **Name:** Jump-SN
- **Address range:** 10.0.3.0/24

Add subnet

Test-FW-VN

Name *

Jump-SN

Address range (CIDR block) * ⓘ

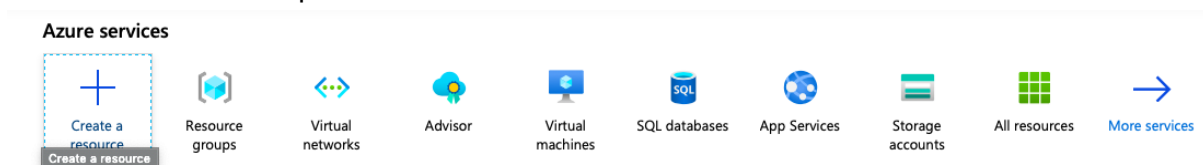
10.0.3.0/24

10.0.3.0 - 10.0.3.255 (251 + 5 Azure reserved addresses)

Create a virtual machine in each subnet

Now we will create two virtual machines and place them in the two additional subnets created in the previous section, one for the Jump-SN subnet, and one for the Workload-SN subnet.

1. On the Azure portal, click **Create a resource**.



2. Click **Compute** and then select **Windows Server 2016 Datacenter** in the Featured list.



Windows Server 2016 Datacenter

Quickstart tutorial

3. Enter these values for the virtual machine, accepting the default values for items not listed below. When finished click **Review + Create**, then click **Create**

- **Basic:**
- **Subscription:** < select your subscription >
- **Resource group:** Test-FW-RG < the resource group you created earlier >
- **Virtual machine name:** Srv-Jump
- **Region:** < The region you selected earlier >
- **Size** – Standard DS1 V2
- **Username:** demouser
- **Password:** demo@pass123

[Home](#) > [New](#) > Create a virtual machine

Create a virtual machine

Looking for classic VMs? [Create VM from Azure Marketplace](#)

Project details

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

Subscription * ⓘ

Visual Studio Enterprise – MPN



Resource group * ⓘ

az900-rg

[Create new](#)

Instance details

Virtual machine name * ⓘ

Srv-Jump

Region * ⓘ

(Asia Pacific) Southeast Asia

Availability options ⓘ

No infrastructure redundancy required

Image * ⓘ

Windows Server 2016 Datacenter

[Browse all public and private images](#)

Size * ⓘ

Standard DS1 v2

1 vcpu, 3.5 GiB memory

[Change size](#)

Administrator account

Username * ⓘ

demouser

Password * ⓘ

Confirm password * ⓘ

- **Public inbound ports:** RDP (3389).

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ

☐ None ☒ Allow selected ports

Select inbound ports *

RDP (3389) ▼

- **Disks:**
- **Disk options** – OS disk type: Premium SSD

Disk options

OS disk type * ⓘ

Premium SSD ▼

- **Networking:**
- Virtual Network: Test-FW-VN
- Subnet: Jump-SN
- Public IP: click Create new then type Srv-Jump-PIP for the public IP address name and click OK.

Network interface

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

Virtual network * ⓘ

Test-FW-VN ▼

[Create new](#)

Subnet * ⓘ

Jump-SN (10.0.3.0/24) ▼

[Manage subnet configuration](#)

Public IP ⓘ

(new) Srv-Jump-ip ▼

[Create new](#)

- **Management:**
- Boot diagnostics: Off

Monitoring

Boot diagnostics ⓘ

☐ On ☒ Off

- Click on create button.
4. While the virtual machine is being created, repeat steps 1-3 above to create another virtual machine with the following settings:

Azure services



Resource groups



Virtual networks



Advisor



Virtual machines



SQL databases



App Services



Storage accounts



All resources



[More services](#)

New

Azure Marketplace [See all](#)

Popular

Get started

Recently created



[Windows Server 2016 Datacenter](#)

[Quickstart tutorial](#)

- **Basics:**
- **Subscription:** < select your subscription >
- **Resource group:** az900-rg < the resource group you created earlier >
- **Virtual machine name:** Srv-Work
- **Region:** < The region you selected earlier >
- **Username:** demouser
- **Password:** demo@pass123
- **Public inbound ports:** None

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Advanced](#) [Tags](#) [Review + create](#)

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image.

Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization.

Looking for classic VMs? [Create VM from Azure Marketplace](#)

Project details

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

Subscription * ⓘ

Visual Studio Enterprise – MPN

Resource group * ⓘ

az900-rg

[Create new](#)

Instance details

Virtual machine name * ⓘ

Srv-Work

Region * ⓘ

(Asia Pacific) Southeast Asia

Availability options ⓘ

No infrastructure redundancy required

Image * ⓘ

Windows Server 2016 Datacenter

[Browse all public and private images](#)

Size * ⓘ

Standard DS1 v2

1 vcpu, 3.5 GiB memory

[Change size](#)

Administrator account

Username * ⓘ	<input type="text" value="demouser"/>	✓
Password * ⓘ	<input type="password" value="*****"/>	✓
Confirm password * ⓘ	<input type="password" value="*****"/>	✓

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ ☒ None ☐ Allow selected ports

Select inbound ports

i All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Save money

Save up to 49% with a license you already own using Azure Hybrid Benefit. [Learn more](#)

Already have a Windows Server license? * ☐ Yes ☒ No ⓘ

[Review + create](#)

[< Previous](#)

[Next : Disks >](#)

- **Disks:**
- **Disk options – OS disk type:** Premium SSD

Disk options

OS disk type * ⓘ

- **Networking:**
- **Virtual Network:** Test-FW-VN
- **Subnet:** Workload-SN
- **Public IP:** None

Network interface

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

Virtual network * ⓘ Test-FW-VN ▼
[Create new](#)

Subnet * ⓘ Workload-SN (10.0.2.0/24) ▼
[Manage subnet configuration](#)

Public IP ⓘ None ▼
[Create new](#)

NIC network security group ⓘ ☐ None ☒ Basic ☐ Advanced

Public inbound ports * ⓘ ☒ None ☐ Allow selected ports

Select inbound ports Select one or more ports ▼

i All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Accelerated networking ⓘ ☐ On ☒ Off

The selected VM size does not support accelerated networking.

[Review + create](#)

[< Previous](#)

[Next : Management >](#)

- **Management:**
- **Boot diagnostics:** Off

Monitoring

Boot diagnostics ⓘ ☐ On ☒ Off

- Click on create button.

Create a virtual machine

✓ Validation passed

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Advanced](#) [Tags](#) [Review + create](#)

PRODUCT DETAILS

Standard DS1 v2

by Microsoft

[Terms of use](#) | [Privacy policy](#)

Subscription credits apply ⓘ

5.2216 INR/hr

[Pricing for other VM sizes](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Basics

Subscription	Visual Studio Enterprise – MPN
Resource group	az900-rg
Virtual machine name	Srv-Work
Region	(Asia Pacific) Southeast Asia
Availability options	No infrastructure redundancy required
Username	demouser
Public inbound ports	None
Already have a Windows Server license?	No

Disks

OS disk type	Premium SSD
--------------	-------------

Create

< Previous

Next >

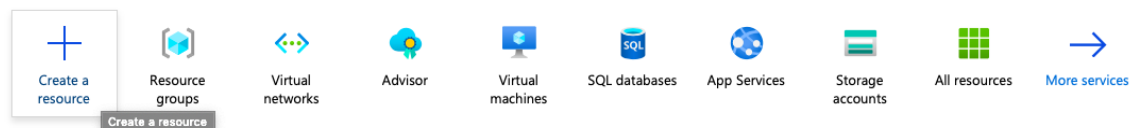
[Download a template for automation](#)

Create

Deploy the Firewall into the VNET

1. From the portal home page, click **Create a resource** and in the **New** pane type **Firewall**, then click **Create**

Azure services



2. Click **Networking** and in the **Featured** section click **See all > Firewall > Create**.

Firewall

Microsoft



Firewall [Save for later](#)

Create

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics.

Useful Links

[Learn more](#)

[Documentation](#)

[Pricing](#)

- **Subscription:** < your Azure subscription >
- **Resource group:** az900-rg < the resource group you created earlier >
- **Name:** Test-FW01
- **Region:** < Select the same location that you used previously >
- **Choose a virtual network:** Test-FW-VN < the VNET you created earlier >
- **Public IP address:** < select **Create new** radio button >
- **Public IP address:** < accept the default value >
- **Public IP address SKU:** Standard

Basics Tags Review + create

Azure Firewall is a managed cloud-based network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics. [Learn more.](#)

Project details

Subscription *	Visual Studio Enterprise – MPN
Resource group *	az900-rg

[Create new](#)

Instance details

Name *	Test-FW01
Region *	(Asia Pacific) Southeast Asia
Availability zone ⓘ	None
Choose a virtual network	<input type="radio"/> Create new <input checked="" type="radio"/> Use existing
Virtual network	Test-FW-VN (az900-rg)
Public IP address *	(New) azpip

[Create new](#)

Click on create button.

Create a firewall

 Validation passed

[Basics](#) [Tags](#) [Review + create](#)

Summary

Basics

Subscription	Visual Studio Enterprise – MPN
Resource group	az900-rg
Region	(Asia Pacific) Southeast Asia
Virtual network	Test-FW-VN
Address space	10.0.0.0/16
Availability zone	None
Public IP address	azpip

Create

< Previous

Next >

[Download a template for automation](#)

- After deployment completes, go to the **Test-FW-RG** resource group, and click the **Test-FW01** firewall.

Home > Microsoft.AzureFirewall-20191028123650 - Overview

Microsoft.AzureFirewall-20191028123650 - Overview

Deployment

Search (Cmd+/) << Delete Cancel Redeploy Refresh

- Overview
- Inputs
- Outputs
- Template

✓ **Your deployment is complete**

Deployment name: Microsoft.AzureFirewall-20191028123650
Subscription: [Visual Studio Enterprise – MPN](#)
Resource group: [az900-rg](#)

Start time: 10/28/2019, 12:37:03 PM
Correlation ID: 84899623-4750-4b5b-8216-4d4eb74db5d7

Deployment details (Download)

Next steps

[Go to resource](#)

Create a default route

1. From the Azure portal home page, click **All services**. Under **Networking**, click **Route tables**.

Azure services

Create a resource Create a resource Virtual networks Advisor Virtual machines SQL databases App Services Storage accounts All resources More services

Home > New > Route table

Route table

Microsoft

← Create

Route table Save for later

Microsoft

Create

A route table contains a set of rules, called routes, that specifies how packets should be routed in a virtual network. Route tables are associated to subnets, and each packet leaving a subnet is handled based on the associated route table. Each route table can be associated to multiple subnets, but a subnet can only be associated to a single route table.

Packets are matched to routes using the destination. This can be an IP address, a virtual network gateway, a virtual appliance, or the internet. If a matching route can't be found, then the packet is dropped. By default, every subnet in a virtual network is associated with a set of built-in routes. These allow traffic between virtual machines in a virtual network; virtual machines and an address space as defined by a local network gateway; and virtual machines and the internet.

There are no additional charges for creating route tables in Microsoft Azure.

Useful Links
[Service overview](#)
[Documentation](#)

2. In the Route tables pane click + **Add** and enter the following details and when finished click **Create**
 - **Name:** Firewall-route
 - **Subscription:** < select your subscription >
 - **Resource group:** az900-rg < the resource group you created earlier >
 - **Location:** < select the same location that you used previously >
 - Click on create button.

Home > New > Route table > Create route table

Create route table

You can add routes to this table after it's created.

Name *

Firewall-route ✓

Subscription *

Visual Studio Enterprise – MPN

Resource group *

az900-rg

[Create new](#)

Location *

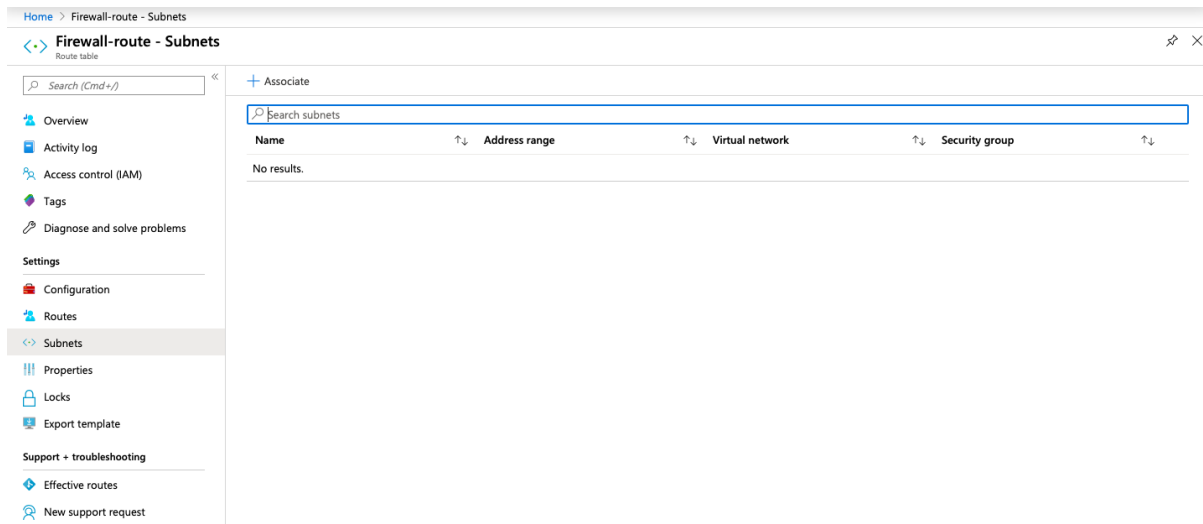
(Asia Pacific) Southeast Asia

Virtual network gateway route propagation

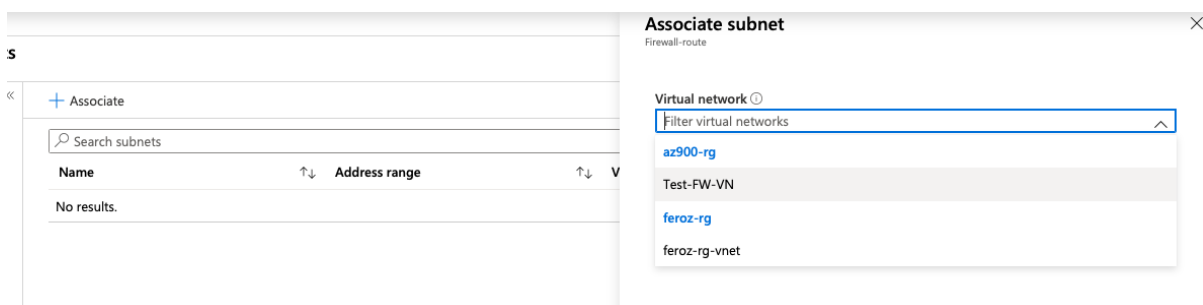
Disabled **Enabled**

Create [Automation options](#)

3. When it is finished click **Refresh**, and then click the **Firewall-route** route table.
4. Click **Subnets** > **+ Associate**.



5. Click **Virtual network** > **Test-FW-VN**.



6. For **Subnet**, click **Workload-SN**. Make sure that you select **only** the **Workload-SN** subnet for this route, otherwise your firewall won't work correctly.

7. Click OK.

Associate subnet



Firewall-route

Virtual network ⓘ

Test-FW-VN



Subnet ⓘ

Workload-SN



OK

- Click **Routes** > **+ Add** and enter the following details and click **OK** when finished

Home > Firewall-route - Routes

Firewall-route - Routes

Route table

+ Add

Add

Routes

Name
No results.

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Routes

Subnets

- **Route name:** FW-DG
- **Address prefix:** 0.0.0.0/0
- **Next hop type:** Virtual appliance. (Azure Firewall is actually a managed service, but *virtual appliance* works in this situation.)
- **Next hop address** < enter the private IP address for the firewall that you noted previously >

Add route

Firewall-route

Route name *

FW-DG



Address prefix * ⓘ

0.0.0.0/0



Next hop type ⓘ

Virtual appliance



Next hop address * ⓘ

10.0.1.4



Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.

OK

Configure an application rule

1. Open the **az900-rg**, and click the **Test-FW01** firewall.\

Home > az900-rg > Test-FW01 > az900-rg

az900-rg
Resource group

Search (Cmd+/)

+ Add Edit columns Delete resource group Refresh Move Export to CSV Assign tags Delete Export template Feedback

Subscription (change): Visual Studio Enterprise - MPN
Subscription ID: 7bd726dd-0a34-4060-9168-b1e496983db8
Deployments: 5 Succeeded

Tags (change): Click here to add tags

Filter by name... Type == all Location == all Add filter

Showing 1 to 13 of 13 records. Show hidden types

Name	Type	Location
azpip	Public IP address	Southeast Asia
Firewall-route	Route table	Southeast Asia
Srv-Jump	Virtual machine	Southeast Asia
Srv-Jump-ip	Public IP address	Southeast Asia
Srv-Jump-nsg	Network security group	Southeast Asia
srv-jump91	Network interface	Southeast Asia
Srv-Jump_OsDisk_1_e3821e81c6da4ace8ab05b3cae0500f	Disk	Southeast Asia
Srv-Work	Virtual machine	Southeast Asia
Srv-Work-nsg	Network security group	Southeast Asia
srv-work324	Network interface	Southeast Asia
Srv-Work_OsDisk_1_4d3187865abb4db68832ca07b7a7a48	Disk	Southeast Asia
Test-FW-VN	Virtual network	Southeast Asia
Test-FW01	Firewall	Southeast Asia

2. On the Test-FW01 page, under Settings, click Rules.

Settings

- Rules
- Public IP Configuration
- Threat intelligence
- Properties
- Locks
- Export template

3. Click the **Application rule collection** tab.

NAT rule collection Network rule collection **Application rule collection**

+ Add application rule collection

4. Click + **Add application rule collection** and enter the following values, then click **Add** when finished

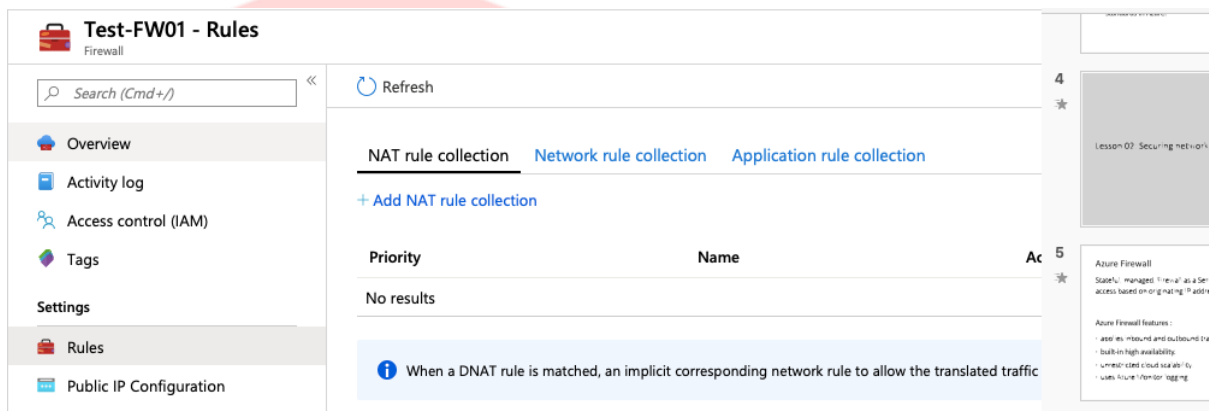
- **Name:** App-Coll01
- **Priority:** 200
- **Action:** Allow
- **Rules:**
 - **Name:** AllowWebsite
 - **Source Address:** 10.0.2.0/24.
 - **Protocol:Port:** http, https.

- **Target FQDNS:** www.microsoft.com (You can specify part of all or a URL, including wild characters, or just a single wild character to indicate all internet sites)

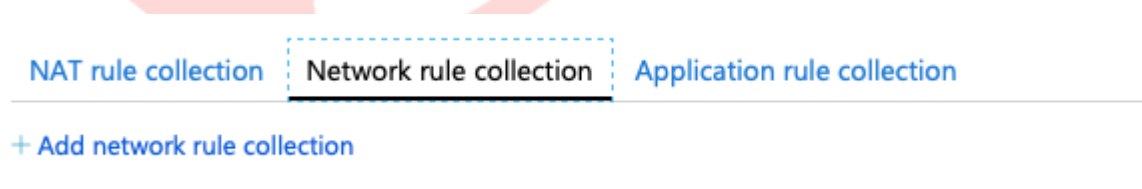
Note: Azure Firewall includes a built-in rule collection for infrastructure FQDNs that are allowed by default. These FQDNs are specific for the platform and can't be used for other purposes. For more information, see [Infrastructure FQDNs](#). You can also use [FQDN tags](#) to represent a group of fully qualified domain names (FQDNs) associated with well known Microsoft services, such as Windows Update, Azure Backup etc.

Configure a network rule:

1. Open the **az900-rg**, and click the **Test-FW01** firewall.
2. On the **Test-FW01** page, under **Settings**, click **Rules**>Click the **Network rule collection** tab.



3. Click + **Add network rule collection** and enter the following details, when finished click **Add**



- **Name:** Net-Coll01
- **Priority:** 200
- **Action:** Allow
- **Rules:**
- **IP Addresses:**
- **Name:** AllowDNS
- **Protocol:** UDP
- **Source Addresses:** 10.0.2.0/24
- **Destination Addresses:** 209.244.0.3,209.244.0.4
- **Destination Port::** 53

Add network rule collection

Name *
Net-Coll01

Priority *
200

Action *
Allow

Rules

IP Addresses

name	Protocol	Source Addresses	Destination Addresses	Destination Ports
AllowDNS	UDP	10.0.2.0/24	209.244.0.3,209.244.0.4	53
	0 selected	*, 192.168.10.1, 192.168.10.0/...	*, 192.168.10.1, 192.168.10.0/...	8080, 8080-8090, *

Service Tags

name	Protocol	Source Addresses	Service Tags	Destination Ports
	0 selected	*, 192.168.10.1, 192.168.10.0/...	0 selected	8080, 8080-8090, *

Add

Change the primary and secondary DNS address for the Srv-Work network interface

- From the Azure portal, open the **az900-rg** resource group.
- Click the **network interface** for the **Srv-Work** virtual machine, it should be named something like *Srv-Work-xyz*.

az900-rg
Resource group

Search (Cmd+/)

+ Add
Edit columns
Delete resource group
Refresh
Move
Export to CSV
Assign tags
Delete
Export template
Feedback

Overview
Activity log
Access control (IAM)
Tags
Events
Settings
Quickstart
Deployments
Policies
Properties
Locks
Export template
Cost Management
Cost analysis
Cost alerts
Budgets
Advisor recommendations
Monitoring
Insights (preview)

Subscription (change) : Visual Studio Enterprise - MPN
Deployments : 5 Succeeded

Subscription ID : 7bd726dd-0a34-4060-9168-b1e496983db8
Tags (change) : Click here to add tags

Filter by name...
Type == all
Location == all
Add filter

Showing 1 to 13 of 13 records.
Show hidden types
No grouping

Name	Type	Location
azzip	Public IP address	Southeast Asia
Firewall-route	Route table	Southeast Asia
Srv-Jump	Virtual machine	Southeast Asia
Srv-Jump-ip	Public IP address	Southeast Asia
Srv-Jump-nsg	Network security group	Southeast Asia
srv-jump91	Network interface	Southeast Asia
Srv-Jump_OsDisk_1_e3821e81c6da4ace8ab05b3caeb0500f	Disk	Southeast Asia
Srv-Work	Virtual machine	Southeast Asia
Srv-Work-nsg	Network security group	Southeast Asia
srv-work324	Network interface	Southeast Asia
Srv-Work_OsDisk_1_4d3187865abb4db68832ca07b7af7a48	Disk	Southeast Asia
Test-FW-VN	Virtual network	Southeast Asia
Test-FW01	Firewall	Southeast Asia

3. Under **Settings**, click **DNS servers**.> click **Custom** and add the following details and click **Save** when finished.

- **Box 1 - Add DNS Server:** 209.244.0.3
- **Box 2 - Add DNS Server:** 209.244.0.4

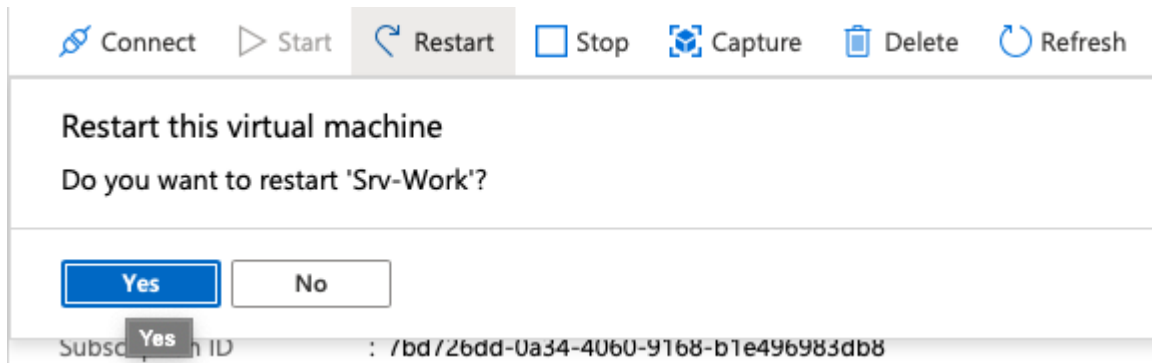
The screenshot shows the Azure portal interface for configuring DNS servers on a network interface. The left sidebar shows the 'az900-rg' resource group. The main pane is titled 'srv-work324 - DNS servers'. Under the 'Settings' tab, the 'DNS servers' section is expanded, showing the 'Custom' option selected. Two DNS servers are listed: 209.244.0.3 and 209.244.0.4. A warning message at the top right states: 'Updating the DNS servers for this network interface will restart the virtual machine to which it's attached'.

Note: Updating the DNS records for the Network interface will automatically restart the virtual machine to which it is attached, you should see a message indicating such. Also the IP Addresses we are adding here are pre-existing publicly accessible DNS Server addresses. When our virtual machine looks for an external address it will refer to these DNS servers for the address details.

4. Go to the Srv-Work virtual machine and ensure it has a status of running, if it is de-allocated click **Start**, or if it has not re-started click **Restart**

The screenshot shows the Azure portal interface for managing virtual machines. The left sidebar shows the 'Virtual machines' section. The main pane displays a table of virtual machines. The table has columns: Name, Type, Status, Resource group, Location, Source, Maintenance status, and Subscription. Three VMs are listed: labvm (Stopped), Srv-Jump (Running), and Srv-Work (Running). The Srv-Work VM is highlighted, showing its details.

Name	Type	Status	Resource group	Location	Source	Maintenance status	Subscription
labvm	Virtual machine	Stopped (deallocated)	feroz-rg	Southeast Asia	Marketplace	-	Visual Studio Enterprise...
Srv-Jump	Virtual machine	Running	az900-rg	Southeast Asia	Marketplace	-	Visual Studio Enterprise...
Srv-Work	Virtual machine	Running	az900-rg	Southeast Asia	Marketplace	-	Visual Studio Enterprise...



Test the firewall

1. From the Azure portal, review the network settings for the **Srv-Work** virtual machine and note the private IP address.

<input type="checkbox"/> Srv-Jump	Virtual machine	Running	az900-rg	Southeast Asia	Marketplace	-	Visual Studio Enterprise...
<input type="checkbox"/> Srv-Work	Virtual machine	Running	az900-rg	Southeast Asia	Marketplace	-	Visual Studio Enterprise...

Ephemeral OS disk : N/A

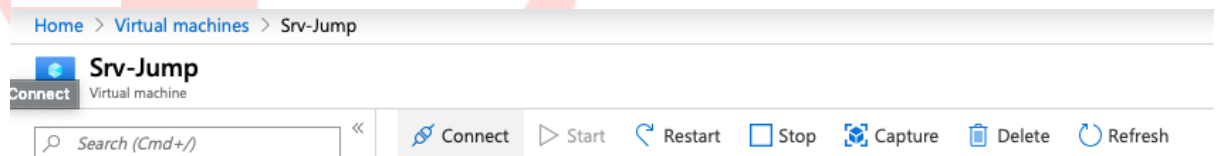
Public IP address : 13.76.193

Private IP address : 10.0.3.4

Virtual network/subnet : Test-FW-VN/Jump-SN

Copy to clipboard

2. In the Azure Portal go to the **Srv-Jump** virtual machine and click **Connect**, followed by **Download RDP File** to open an RDP session to the **SRV-Jump** virtual machine, using the credentials you specified earlier when creating the VM.



Connect to virtual machine

Srv-Jump

To improve security, enable just-in-time access on this VM. →

RDP

SSH

BASTION

To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the RDP file.

IP address *

Public IP address (13.76.193.100) ▼

Port number *

3389

Download RDP File

Download RDP File

Having trouble connecting to this VM?

- From within the **Srv-Jump** virtual machine open a remote desktop connection to the **Srv-Work** private IP address that you noted earlier.

Server Manager - Local Server

PROPERTIES
For Srv-Jump

Computer name	Srv-Jump	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Install updates automatically using Windows Update
		Last checked for updates	Never
Windows Firewall	Private: On	Windows Defender	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Enabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC) Coordinated Universal Time
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00376-40000-00000-AA947 (activated)
Operating system version	Microsoft Windows Server 2016 Datacenter	Processors	Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz
Hardware information	Microsoft Corporation Virtual Machine	Installed memory (RAM)	3.5 GB
		Total disk space	133.51 GB

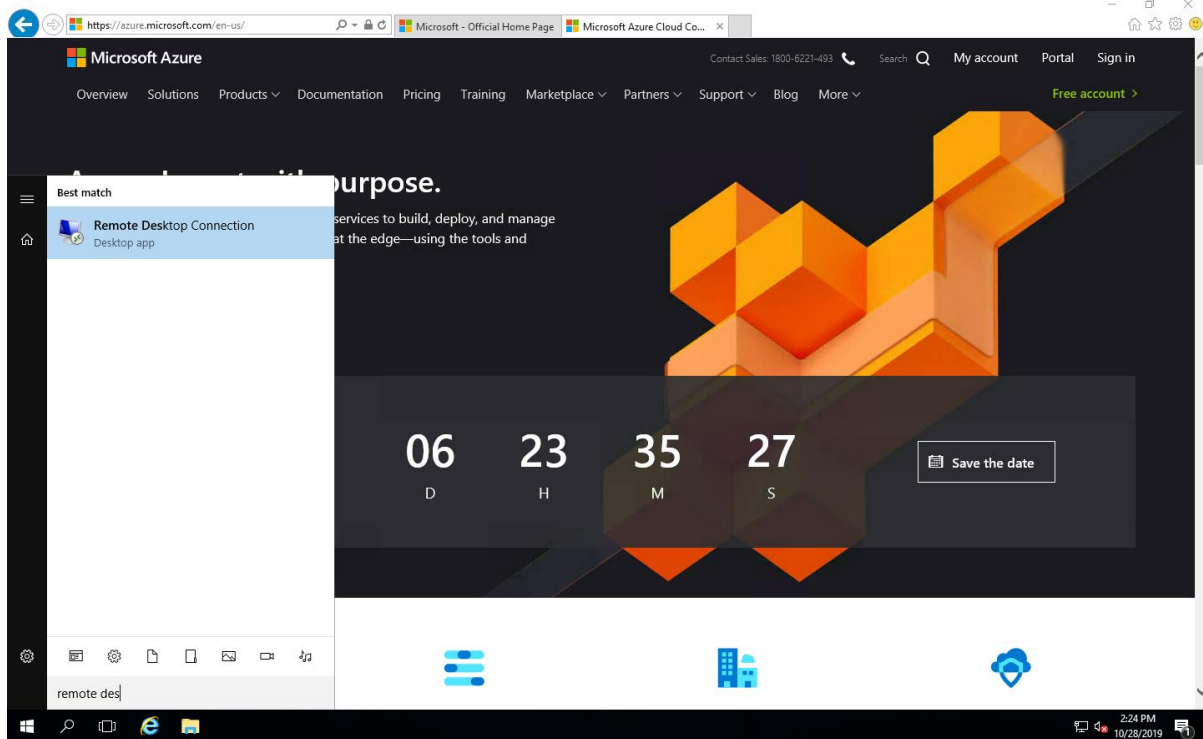
EVENTS
All events | 9 total

Server Name	ID	Severity	Source	Log	Date and Time
Srv-Jump	2004	Warning	Microsoft-Windows-Resource-Exhaustion-Detector	System	10/28/2019 12:33:02 PM
Srv-Jump	2004	Warning	Microsoft-Windows-Resource-Exhaustion-Detector	System	10/28/2019 11:28:15 AM
Srv-Jump	2004	Warning	Microsoft-Windows-Resource-Exhaustion-Detector	System	10/28/2019 8:31:51 AM
Srv-Jump	10016	Error	Microsoft-Windows-DistributedCOM	System	10/28/2019 8:26:31 AM
Srv-Jump	2004	Warning	Microsoft-Windows-Resource-Exhaustion-Detector	System	10/28/2019 8:26:16 AM
Srv-Jump	1534	Warning	Microsoft-Windows-User Profile Service	Application	10/28/2019 8:25:58 AM
Srv-Jump	2004	Warning	Microsoft-Windows-Resource-Exhaustion-Detector	System	10/28/2019 7:27:54 AM

- Once logged into the SRV-Jump virtual machine, allow **Server Manager** to open, which it will do after log in automatically, then go to **Local server** and turn off **IE Enhanced Security Configuration**.

Note: In production environments you would not do this, this is to allow use access the workload server a bit more easily in this test scenario and reduce and prevent pop-ups. In a production you may use a workload server with no GUI environment present.

5. Open **Internet Explorer** and browse to <https://www.microsoft.com>



6. Click **OK > Close** on the security alerts that may pop-up.