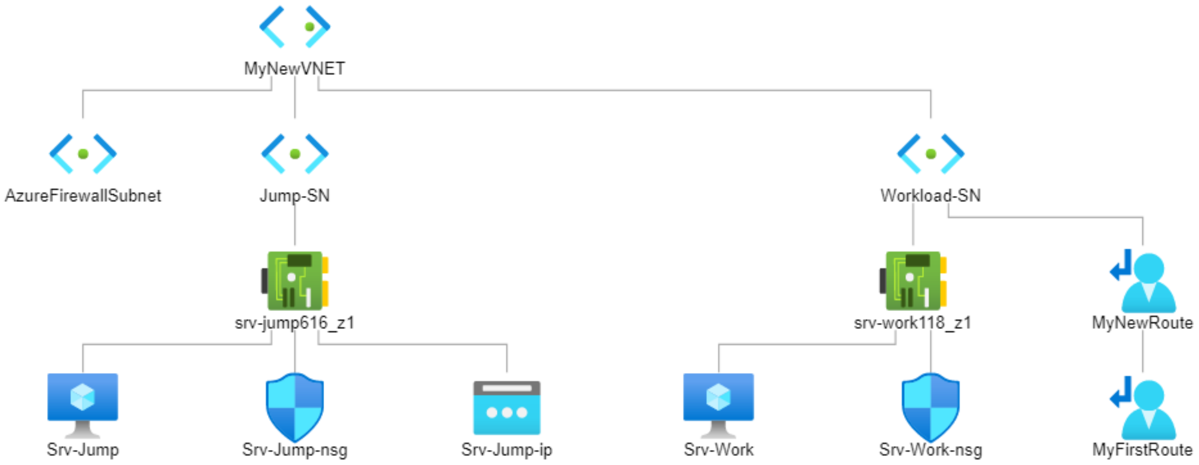
Install a Firewall and configure rules with Firewall Manager. This will help the organization to control inbound and outbound traffic which is an essential part of the overall network security plan. Specifically, I would like you to create and test the following infrastructure components:

- **A virtual network with a workload subnet and a jump host subnet.**
- **A virtual machine in each subnet.**
- **A custom route that ensures all outbound workload traffic from the workload subnet uses the firewall.**
- **Firewall Application rules that only allow outbound traffic to www.microsoft.com.**
- **Firewall Network rules that allow external DNS server lookups.**

The network overview:

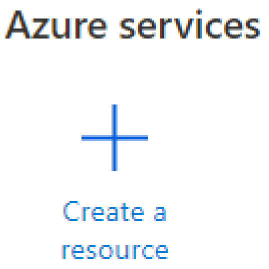


Tasks

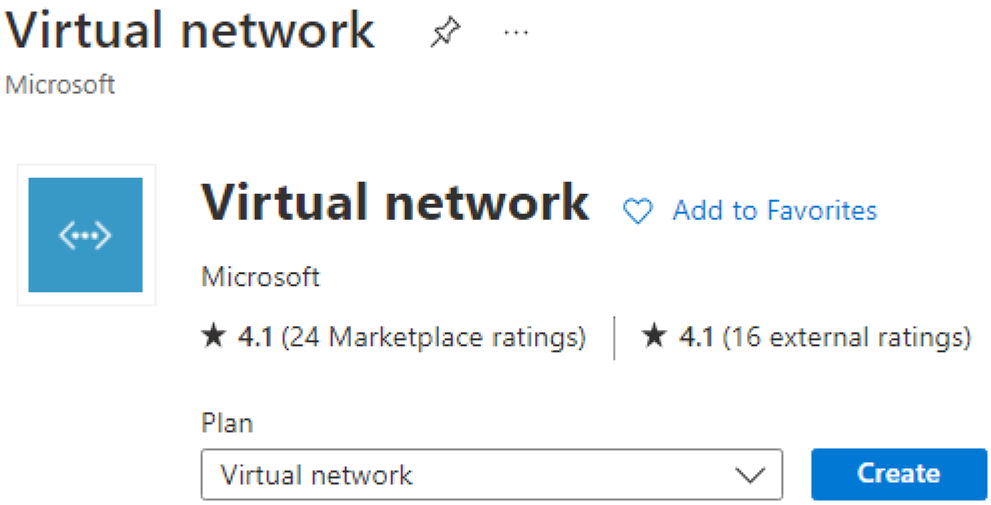
1. Create a Virtual network

You need some VNETs before you can set up and use Azure Firewall and Azure Firewall Manager.

1. From the Azure Portal, click on **Create** a resource button:



2. In the search box, enter **Virtual Network**:



Virtual network

Microsoft

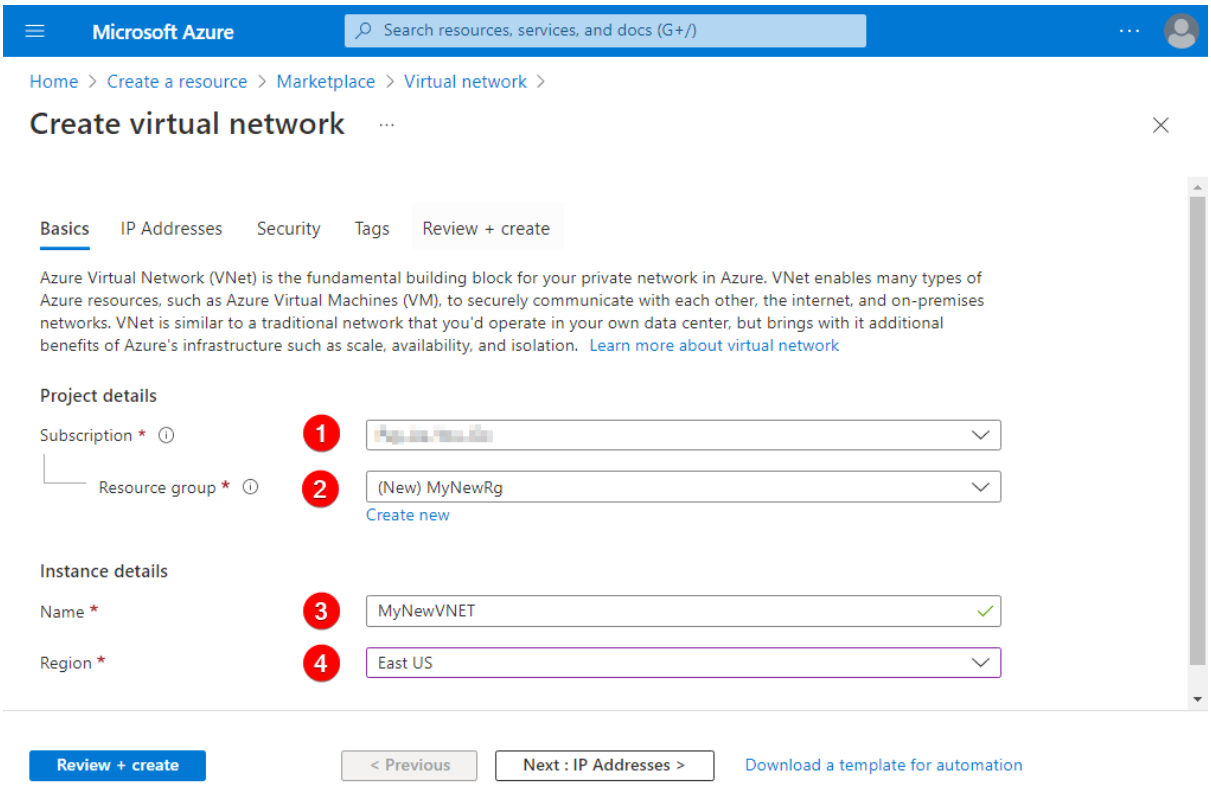
Virtual network

Microsoft

★ 4.1 (24 Marketplace ratings) | ★ 4.1 (16 external ratings)

Plan: Virtual network

3. Select **Create** and enter the following values in the **Basics tab**:



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Create a resource > Marketplace > Virtual network >

Create virtual network

Basics
IP Addresses
Security
Tags
Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. Learn more about virtual network

Project details

Subscription * 1

Resource group * 2 (New) MyNewRg

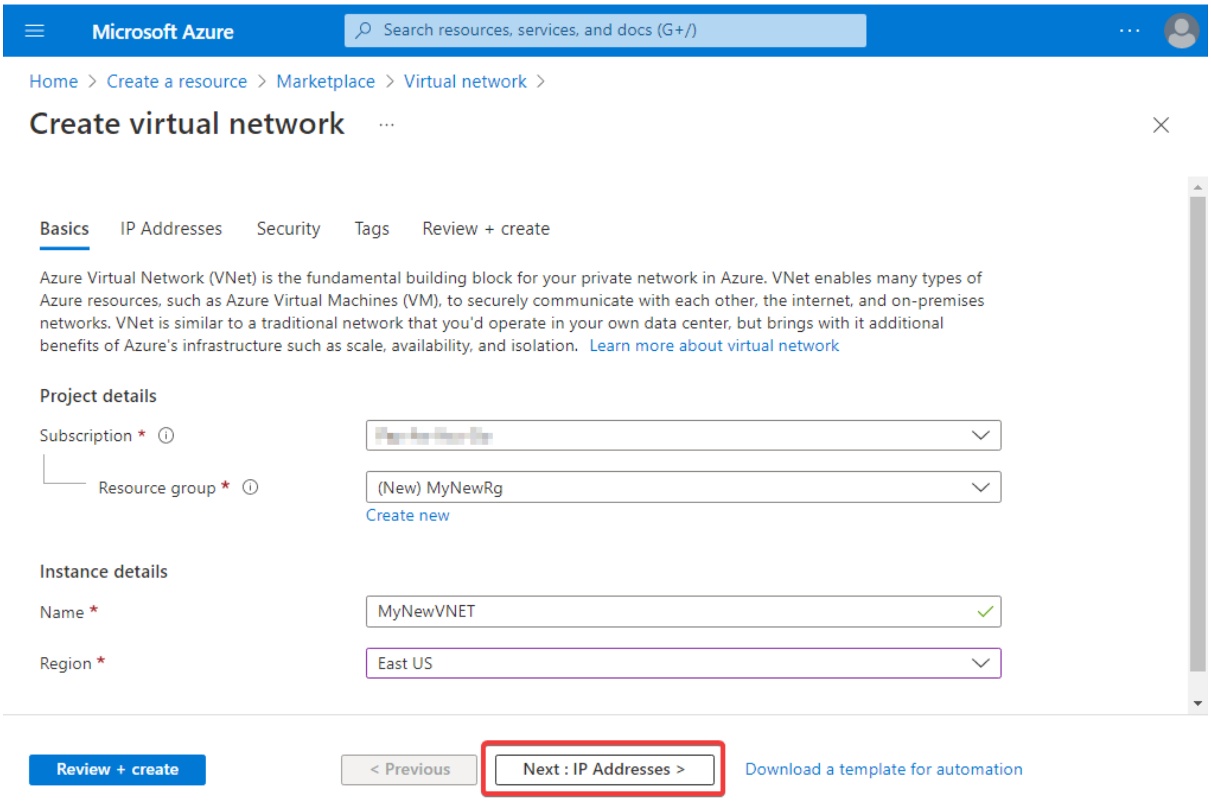
Create new

Instance details

Name * 3 MyNewVNET

Region * 4 East US

4. Click on the **Next: IP Addresses** button:



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Create a resource > Marketplace > Virtual network >

Create virtual network

Basics
IP Addresses
Security
Tags
Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. Learn more about virtual network

Project details

Subscription *

Resource group * (New) MyNewRg

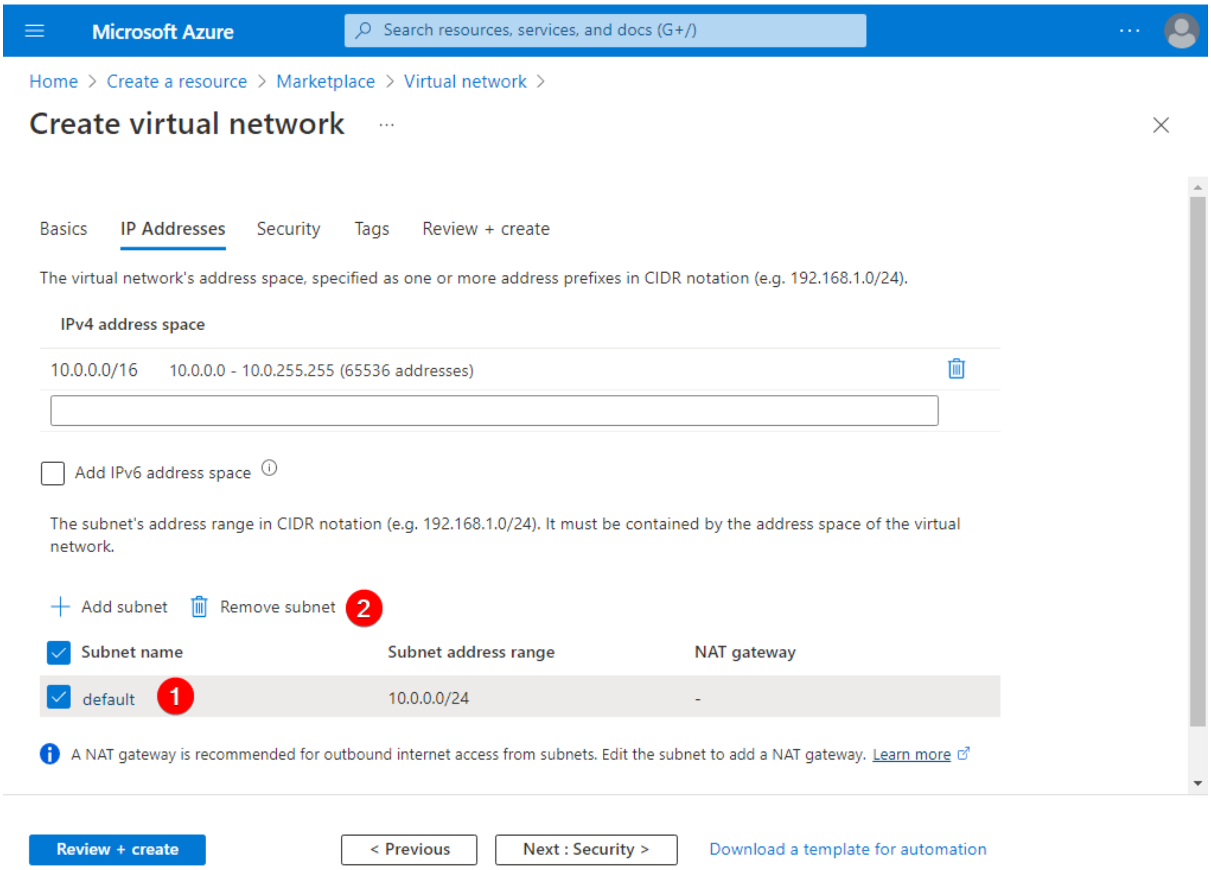
Create new

Instance details

Name * MyNewVNET

Region * East US

5. Check the box of the **default** subnet, and click on the **Remove Subnet** button:



Home > Create a resource > Marketplace > Virtual network >

Create virtual network

Basics | IP Addresses | Security | Tags | Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space	
10.0.0.0/16	10.0.0.0 - 10.0.255.255 (65536 addresses)

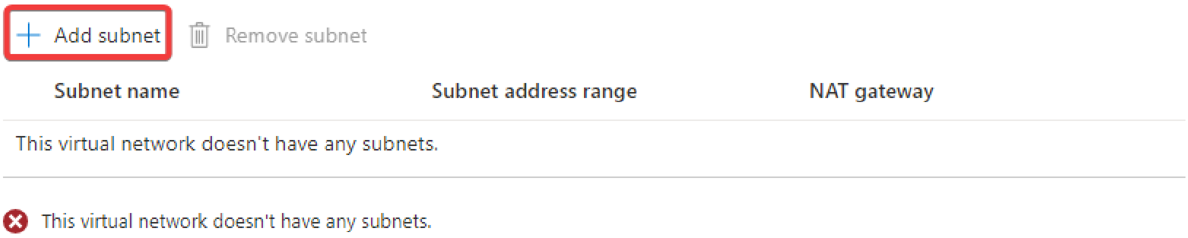
□ Add IPv6 address space

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

☑ Subnet name	Subnet address range	NAT gateway
☑ default	10.0.0.0/24	-

A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. Learn more

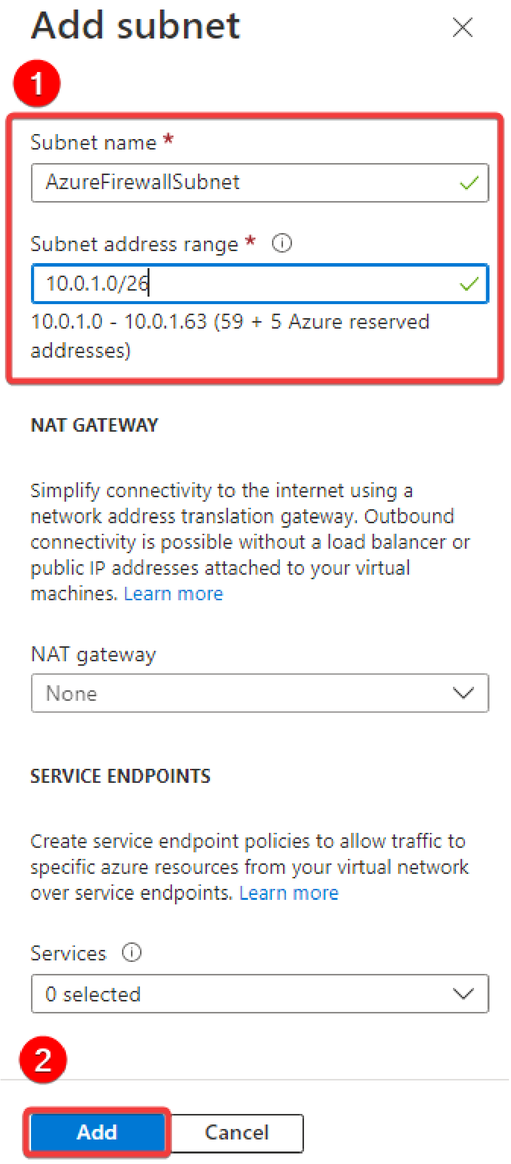
6. Now, click on the **+Add Subnet** button:



Subnet name	Subnet address range	NAT gateway
This virtual network doesn't have any subnets.		

This virtual network doesn't have any subnets.

7. On the **Add Subnet** page, enter the following details and click on **Add**:



Add subnet

1

Subnet name *

AzureFirewallSubnet ✓

Subnet address range * ⓘ

10.0.1.0/26 ✓

10.0.1.0 - 10.0.1.63 (59 + 5 Azure reserved addresses)

NAT GATEWAY

Simplify connectivity to the internet using a network address translation gateway. Outbound connectivity is possible without a load balancer or public IP addresses attached to your virtual machines. Learn more

NAT gateway

None

SERVICE ENDPOINTS

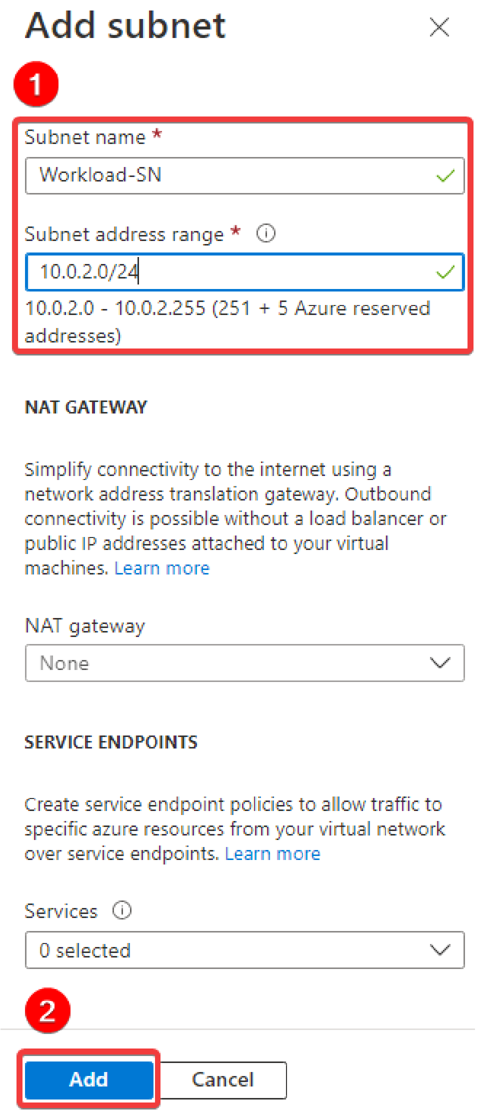
Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more

Services ⓘ

0 selected

2

8. Click on the **+Add Subnet** button and enter or select the following details on the **Add Subnet page** and click on **Add**:



Add subnet

Subnet name *

Workload-SN ✓

Subnet address range * ⓘ

10.0.2.0/24 ✓

10.0.2.0 - 10.0.2.255 (251 + 5 Azure reserved addresses)

NAT GATEWAY

Simplify connectivity to the internet using a network address translation gateway. Outbound connectivity is possible without a load balancer or public IP addresses attached to your virtual machines. Learn more

NAT gateway

None

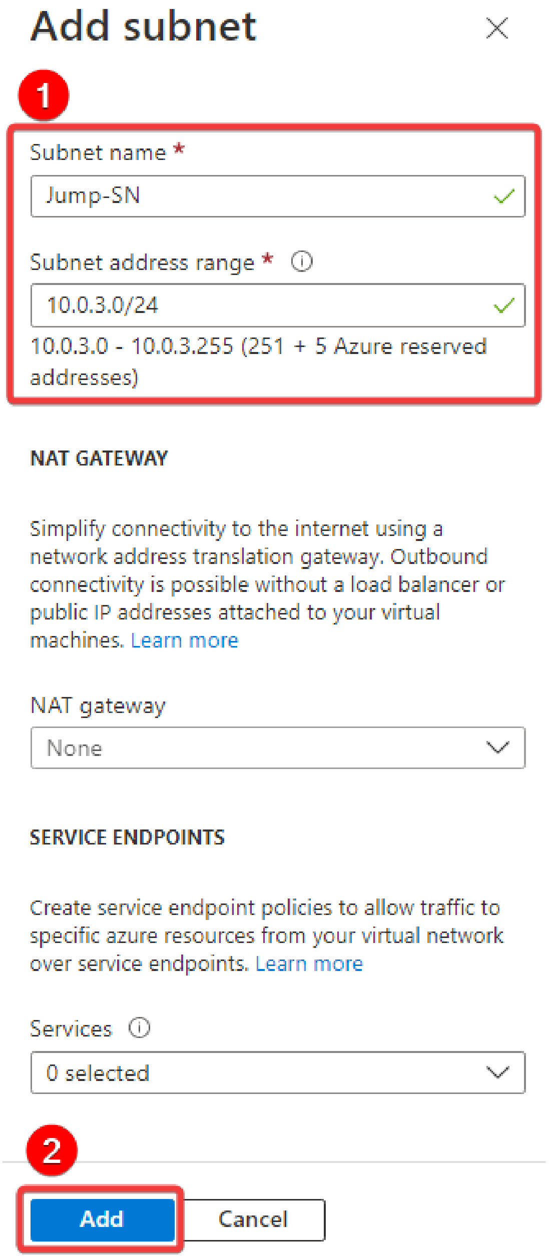
SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more

Services ⓘ

0 selected

9. Click on the **+Add Subnet** button and enter or select the following details on the **Add Subnet page** and click on **Add**:



Add subnet

Subnet name *

Jump-SN

Subnet address range *

10.0.3.0/24

10.0.3.0 - 10.0.3.255 (251 + 5 Azure reserved addresses)

NAT GATEWAY

Simplify connectivity to the internet using a network address translation gateway. Outbound connectivity is possible without a load balancer or public IP addresses attached to your virtual machines. Learn more

NAT gateway

None

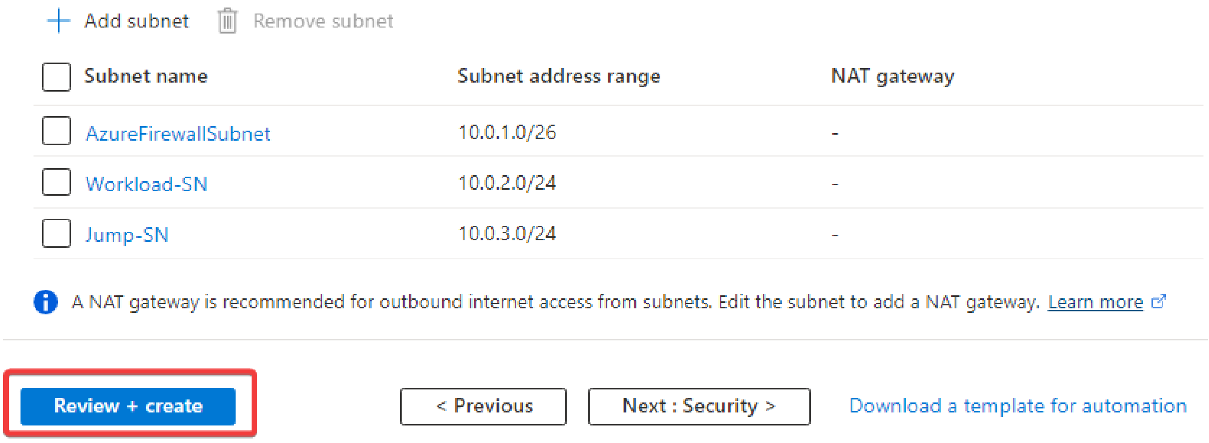
SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more

Services

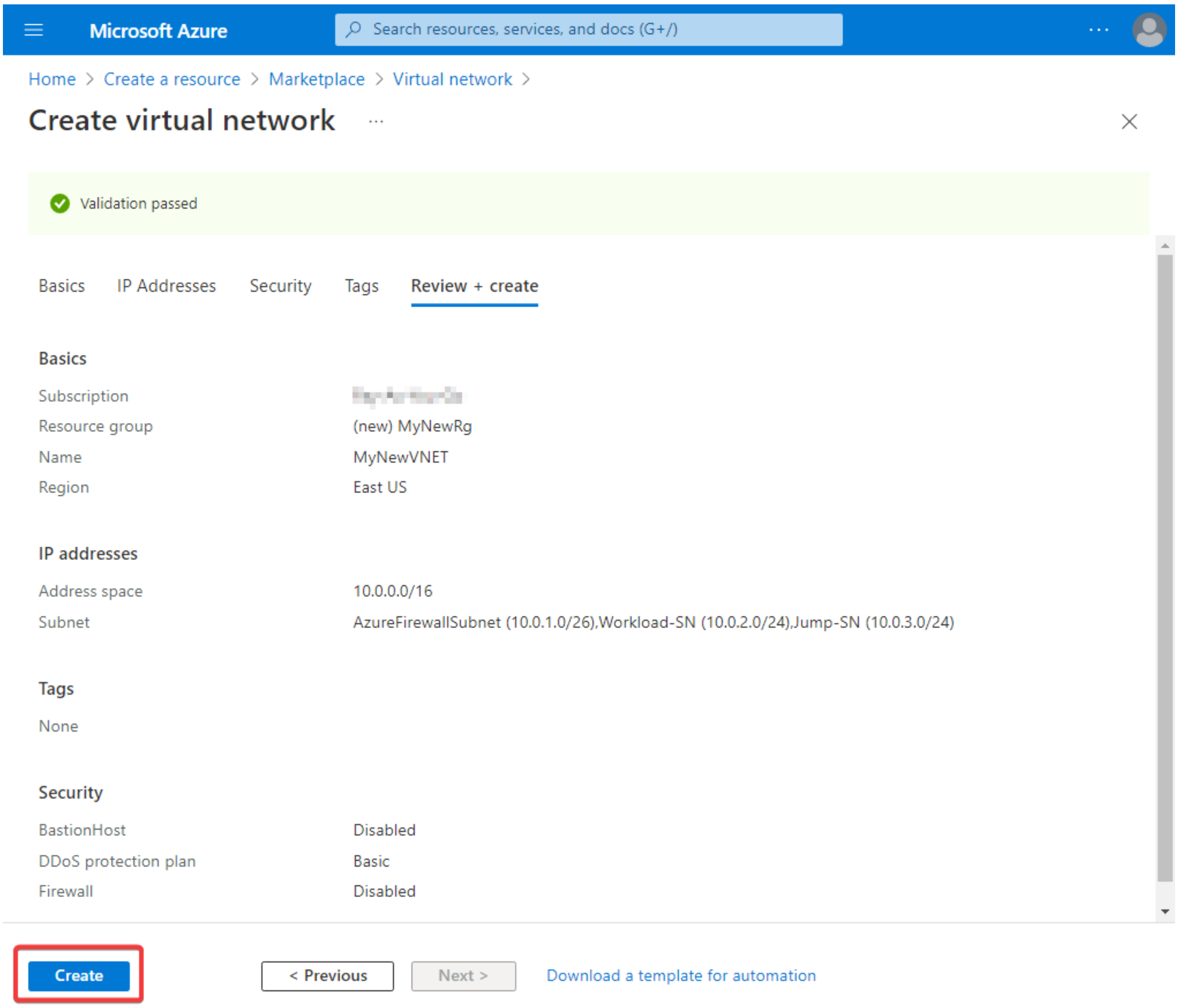
0 selected

10. Select **Review + Create** and then select **Create**.



□ Subnet name	Subnet address range	NAT gateway
□ AzureFirewallSubnet	10.0.1.0/26	-
□ Workload-SN	10.0.2.0/24	-
□ Jump-SN	10.0.3.0/24	-

A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. Learn more



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Create a resource > Marketplace > Virtual network >

Create virtual network

Validation passed

Basics
IP Addresses
Security
Tags
Review + create

Basics

Subscription [redacted]
Resource group (new) MyNewRg
Name MyNewVNET
Region East US

IP addresses

Address space 10.0.0.0/16
Subnet AzureFirewallSubnet (10.0.1.0/26),Workload-SN (10.0.2.0/24),Jump-SN (10.0.3.0/24)

Tags

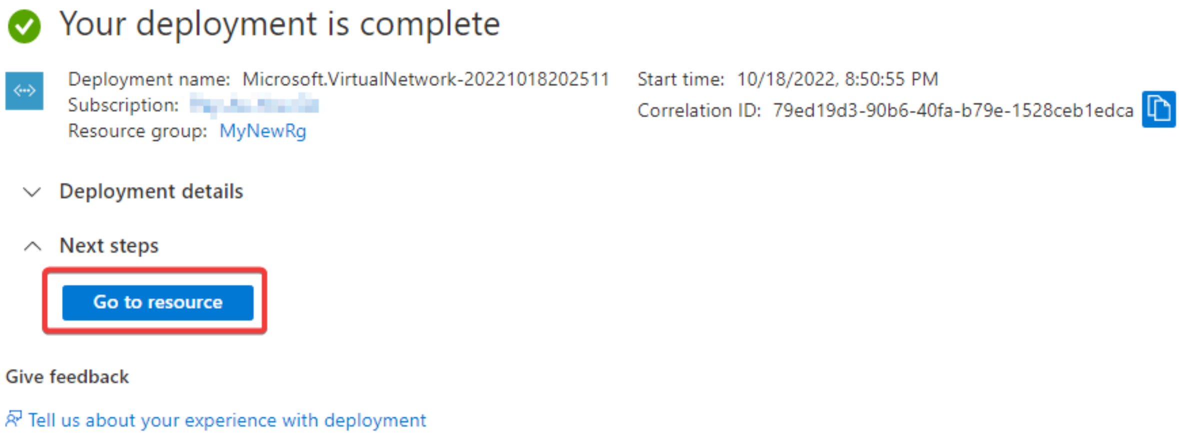
None

Security

BastionHost Disabled
DDoS protection plan Basic
Firewall Disabled

Create
< Previous
Next >
Download a template for automation

11. Click on **Go to resource:**



Your deployment is complete

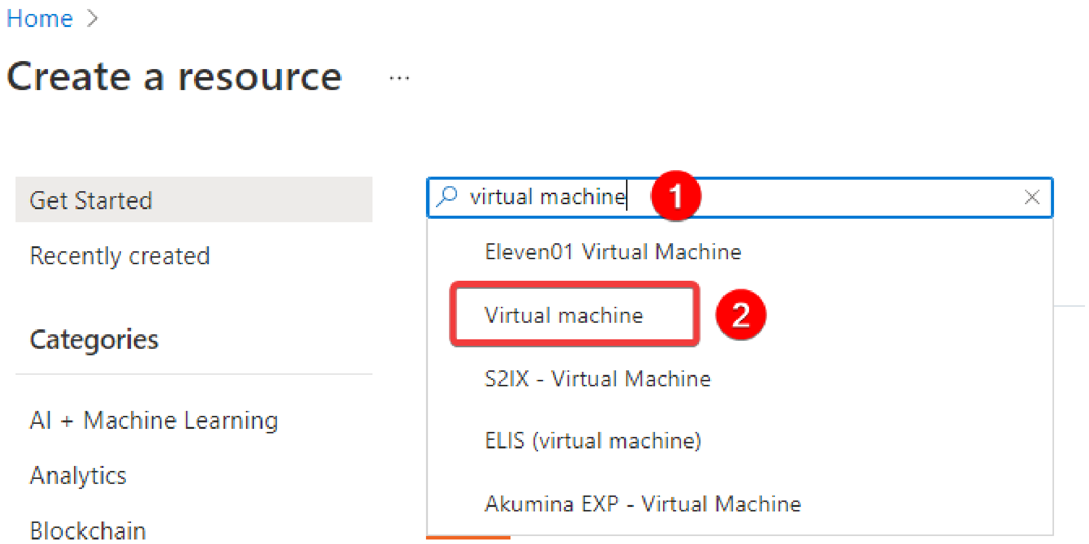
Deployment name: Microsoft.VirtualNetwork-20221018202511
Subscription: [redacted]
Resource group: MyNewRg

Start time: 10/18/2022, 8:50:55 PM
Correlation ID: 79ed19d3-90b6-40fa-b79e-1528ceb1edca

2. Deploy the Virtual Machines

The network isn't complete without Virtual Machines and a Firewall is useless without a compute resource. I need you to create them:

1. In the search box at the top of the Azure Portal, search for **Virtual Machines** and select it from the list:

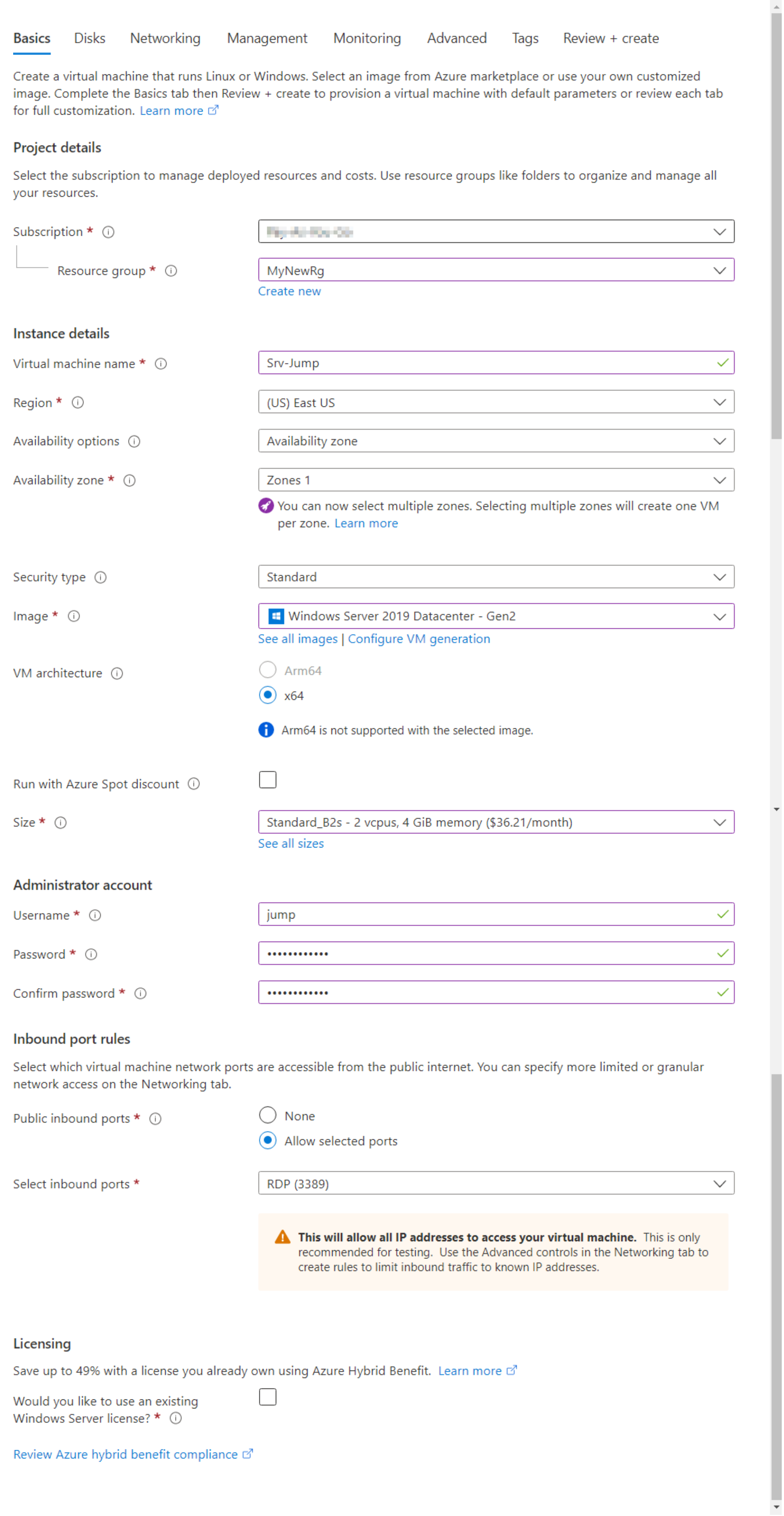


Home >

Create a resource ...

virtual machine

2. On the **Basics** tab, enter or select the following details:



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. Learn more

Project details

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

Subscription * ⓘ [redacted]

Resource group * ⓘ MyNewRg

Create new

Instance details

Virtual machine name * ⓘ Srv-Jump ✓

Region * ⓘ (US) East US

Availability options ⓘ Availability zone

Availability zone * ⓘ Zones 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more

Security type ⓘ Standard

Image * ⓘ Windows Server 2019 Datacenter - Gen2

See all images | Configure VM generation

VM architecture ⓘ ○ Arm64 ● x64

ⓘ Arm64 is not supported with the selected image.

Run with Azure Spot discount ⓘ □

Size * ⓘ Standard_B2s - 2 vcpus, 4 GiB memory ($36.21/month)

See all sizes

Administrator account

Username * ⓘ jump ✓

Password * ⓘ •••••••••••• ✓

Confirm password * ⓘ •••••••••••• ✓

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)

⚠ **This will allow all IP addresses to access your virtual machine.** This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

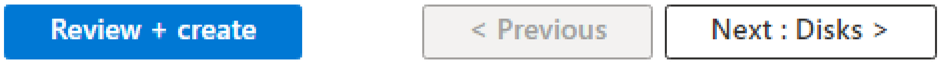
Licensing

Save up to 49% with a license you already own using Azure Hybrid Benefit. Learn more

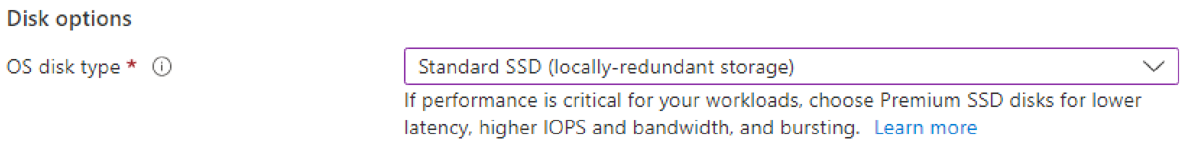
Would you like to use an existing Windows Server license? * ⓘ □

Review Azure hybrid benefit compliance

3. Click on the **Next: Disks** button at the bottom:



4. Select the following:

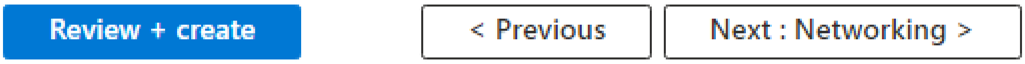


Disk options

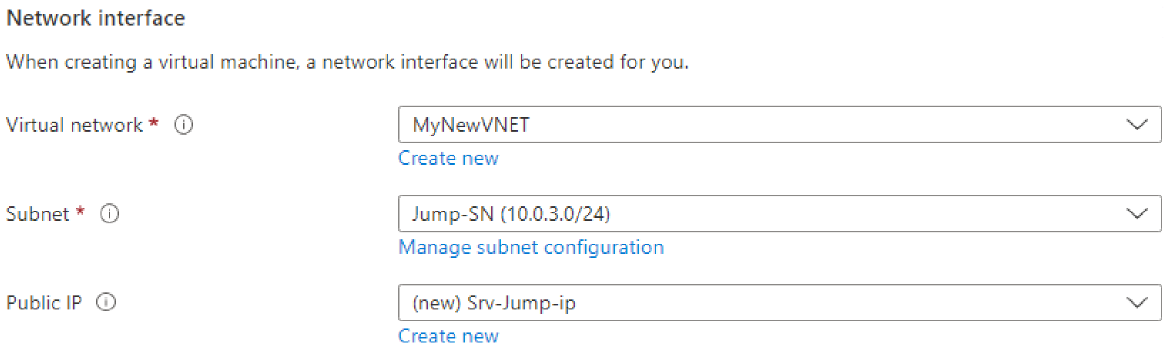
OS disk type * ⓘ Standard SSD (locally-redundant storage)

If performance is critical for your workloads, choose Premium SSD disks for lower latency, higher IOPS and bandwidth, and bursting. Learn more

5. At the bottom, click on the **Next: Networking** button:



6. Select the following details and leave the rest as default:



Network interface

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

Virtual network * ⓘ MyNewVNET

Create new

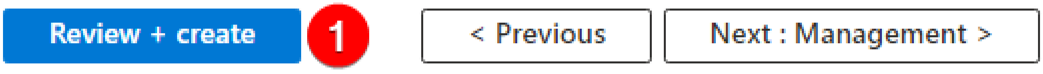
Subnet * ⓘ Jump-SN (10.0.3.0/24)

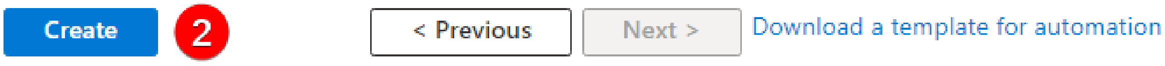
Manage subnet configuration

Public IP ⓘ (new) Srv-Jump-ip

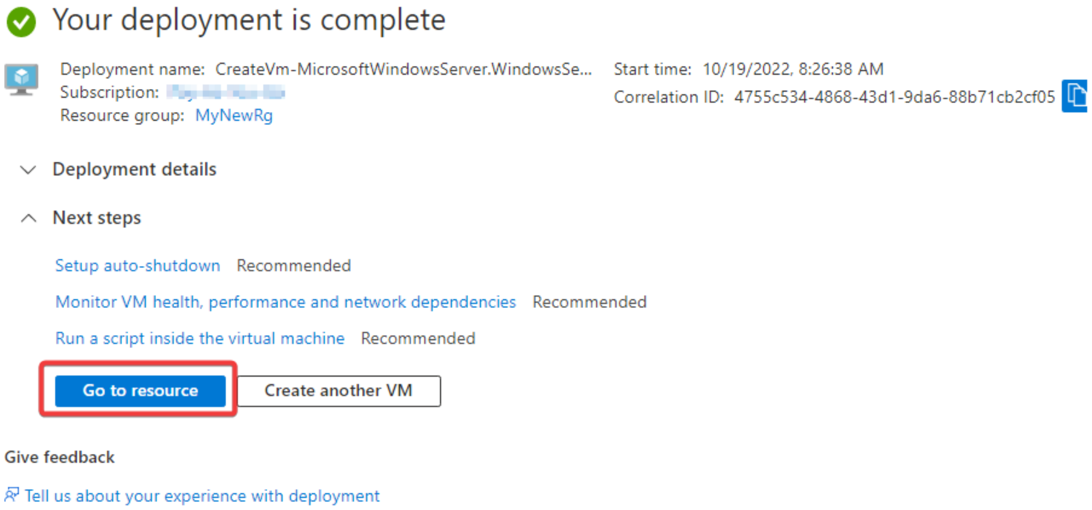
Create new

7. At the bottom, click on the **Review + Create** button and then select **Create**:





8. Click on the **Go to resource** button and copy the Private IP address:



Your deployment is complete

Deployment name: CreateVm-MicrosoftWindowsServer.WindowsSe...
Subscription: [redacted]
Resource group: MyNewRg

Start time: 10/19/2022, 8:26:38 AM
Correlation ID: 4755c534-4868-43d1-9da6-88b71cb2cf05

Deployment details

Next steps

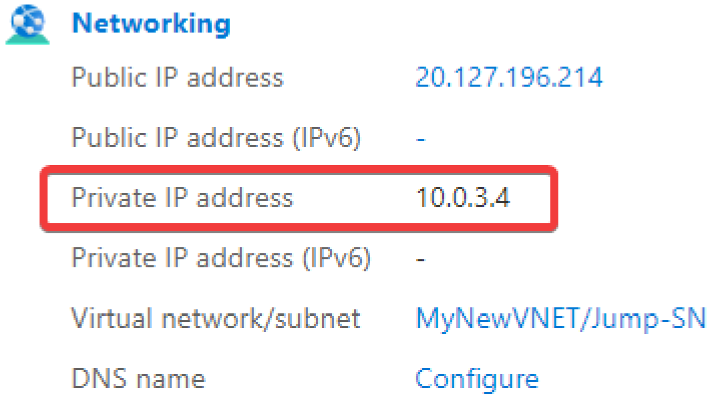
Setup auto-shutdown Recommended

Monitor VM health, performance and network dependencies Recommended

Run a script inside the virtual machine Recommended

Give feedback

Tell us about your experience with deployment



Networking

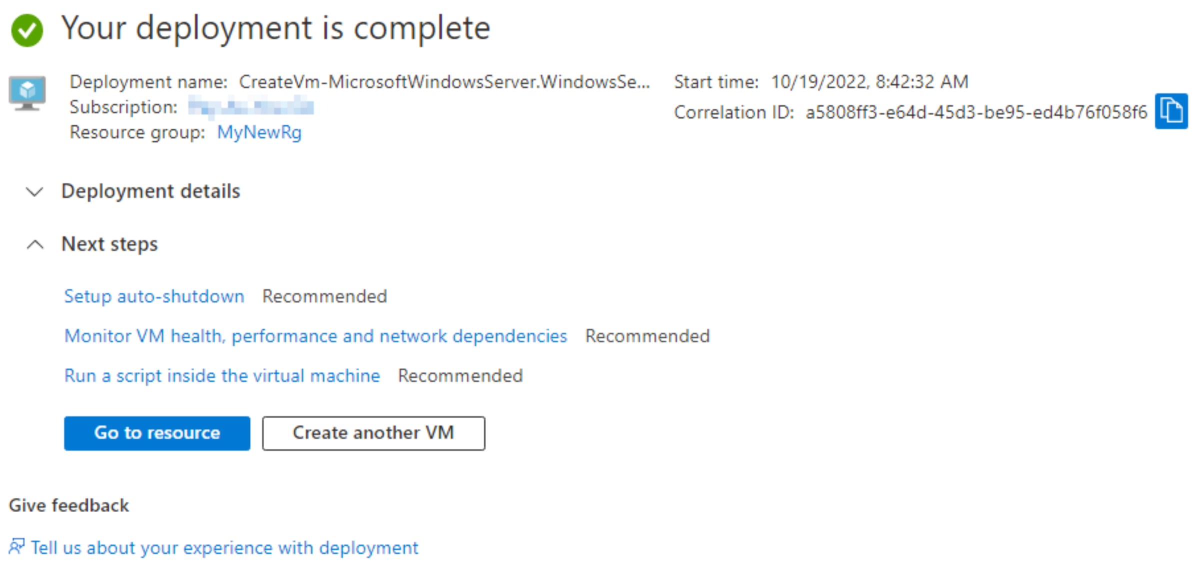
Public IP address	20.127.196.214
Public IP address (IPv6)	-
Private IP address	10.0.3.4
Private IP address (IPv6)	-
Virtual network/subnet	MyNewVNET/Jump-SN
DNS name	Configure

9. Repeat steps 1 - 7 to deploy another VM and enter or select the following details:

- Basics tab:
  - Resource group: **MyNewRg**
  - Instance details:
    - Virtual Machine Name: **Srv-Work**
    - Region: **East US**
    - Image: **Windows Server 2019 Datacenter - Gen2**
    - Azure Spot instance: **Leave the default (unchecked)**
    - Size: **Standard_B2s**
  - Administrator Account:
    - Username: **work**
    - Password: Enter a password
    - Confirm password: Re-enter password
  - Inbound Port rules:
    - Public inbound ports: **None**

- Disks tab:
    - OS disk type: **Standard SSD**

- Networking tab:
    - Network Interface:
        - Virtual Network: **MyNewVNET**
        - Subnet: **Workload-SN**
        - Public IP: **None**



Your deployment is complete

Deployment name: CreateVm-MicrosoftWindowsServer.WindowsSe...
Subscription: [redacted]
Resource group: MyNewRg
Start time: 10/19/2022, 8:42:32 AM
Correlation ID: a5808ff3-e64d-45d3-be95-ed4b76f058f6

Deployment details

Next steps

Setup auto-shutdown Recommended
Monitor VM health, performance and network dependencies Recommended
Run a script inside the virtual machine Recommended

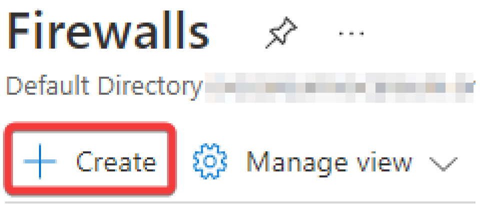
Give feedback

Tell us about your experience with deployment

3. Deploy Azure Firewall

You need the Azure Firewall to protect the network against threats. I want you to create the firewall:

1. In the search box at the top of the Azure Portal, search for **Firewalls**, select **Firewall,** and then select **Create**:



Firewalls

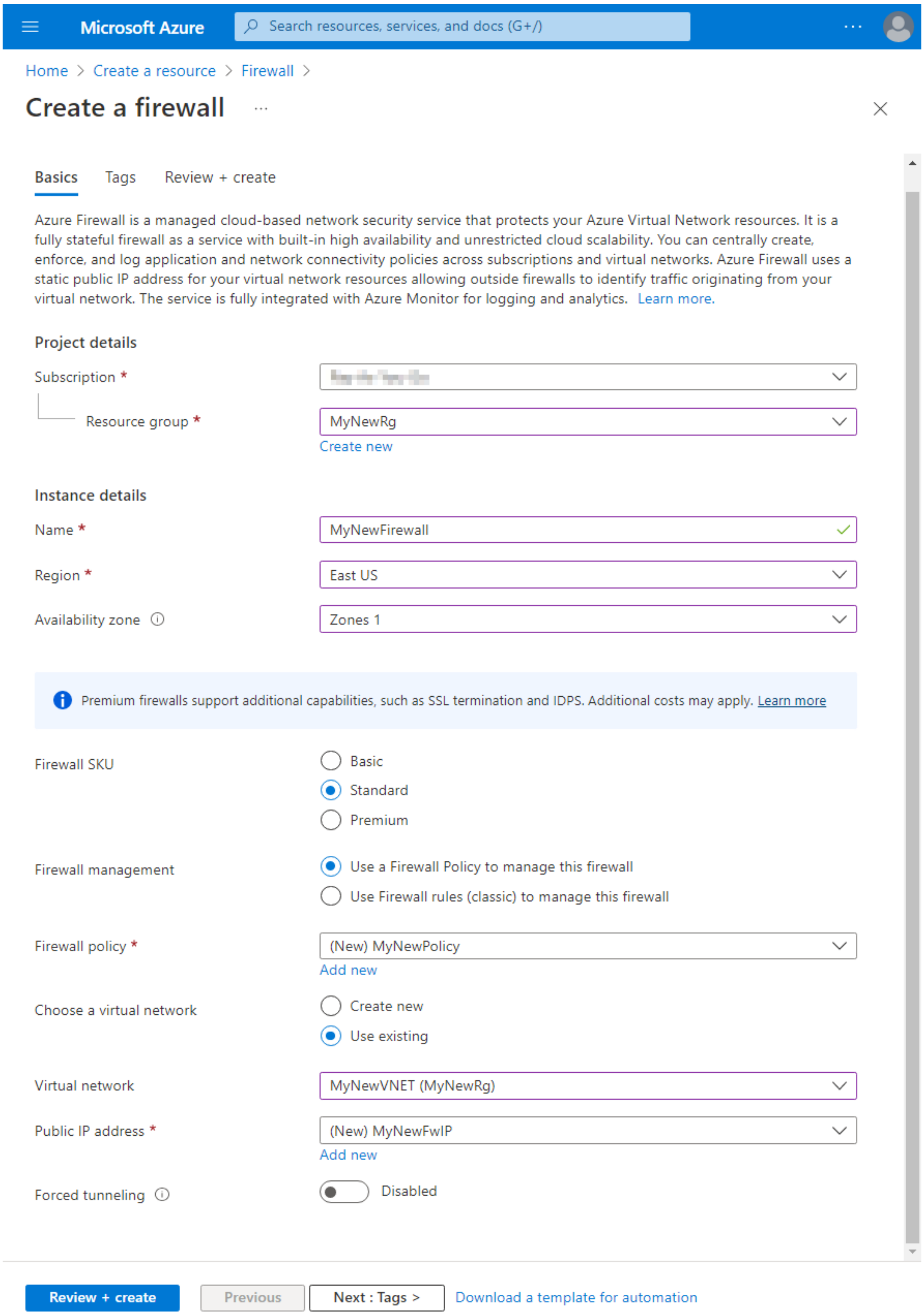
Default Directory [redacted]

2. On the **Basics** tab, enter or select the following details:

- Resource group: **MyNewRG**
- Instance details:
    - Name: **MyNewFirewall**
    - Region: **East US**
    - Availability Zone: **Zone 1**
    - Firewall tier: **Standard**
    - Firewall management: **Use a Firewall Policy to manage this firewall**
    - Firewall Policy: **Add new**
        - Policy name: **MyNewPolicy**

- Region: **East US**

- Choose a Virtual Network: **Use existing**
- Virtual Network: **MyNewVNET**
- Public IP address: **Add new**
  - Name: **MyNewFwIP**



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Create a resource > Firewall >

Create a firewall

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 * : [redacted]

Resource group * : MyNewRg (Create new)

Instance details

Name * : MyNewFirewall ✓

Region * : East US

Availability zone ⓘ : Zones 1

ⓘ Premium firewalls support additional capabilities, such as SSL termination and IDPS. Additional costs may apply. Learn more

Firewall SKU: ○ Basic ● Standard ○ Premium

Firewall management: ● Use a Firewall Policy to manage this firewall ○ Use Firewall rules (classic) to manage this firewall

Firewall policy * : (New) MyNewPolicy (Add new)

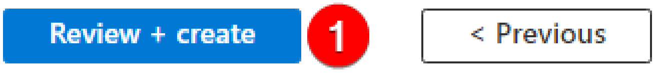
Choose a virtual network: ○ Create new ● Use existing

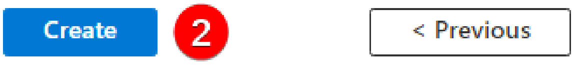
Virtual network: MyNewVNET (MyNewRg)

Public IP address * : (New) MyNewFwIP (Add new)

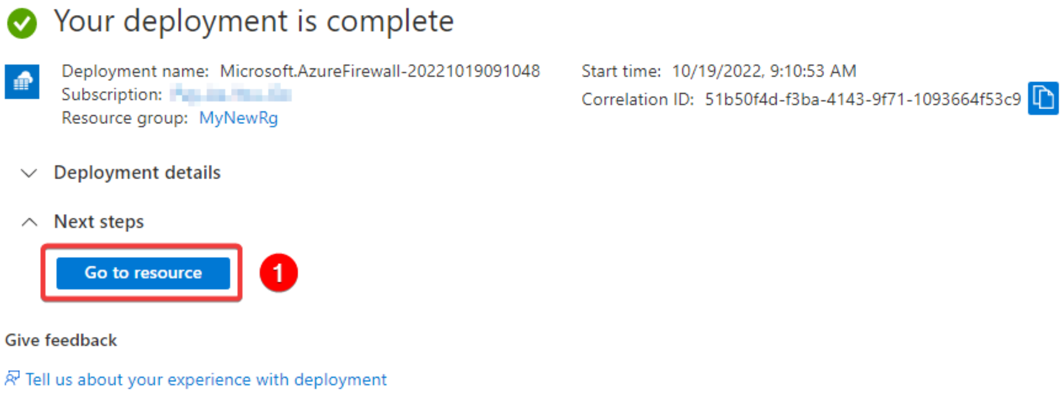
Forced tunneling ⓘ : Disabled

3. Click on the **Review + Create** button and then select **Create**.





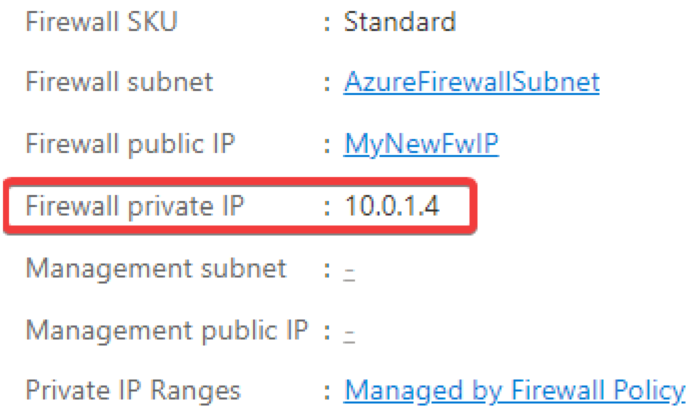
4. Click on the **Go to resource** button and copy the Firewall Private IP:.



Your deployment is complete

Deployment name: Microsoft.AzureFirewall-20221019091048
Subscription: [redacted]
Resource group: MyNewRg

Start time: 10/19/2022, 9:10:53 AM
Correlation ID: 51b50f4d-f3ba-4143-9f71-1093664f53c9



Firewall SKU : Standard

Firewall subnet : AzureFirewallSubnet

Firewall public IP : MyNewFwIP

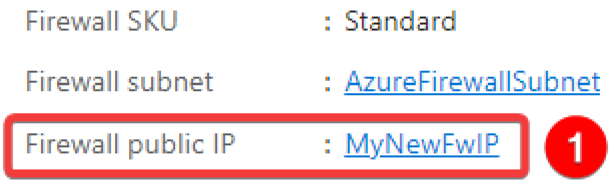
Firewall private IP : 10.0.1.4

Management subnet : -

Management public IP : -

Private IP Ranges : Managed by Firewall Policy

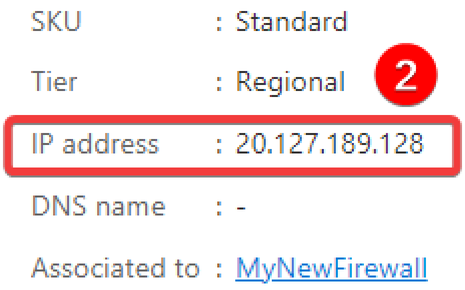
5. Click on **MyNewFwIP** and copy the public ip address of the firewall:



Firewall SKU : Standard

Firewall subnet : AzureFirewallSubnet

Firewall public IP : MyNewFwIP



SKU : Standard

Tier : Regional

IP address : 20.127.189.128

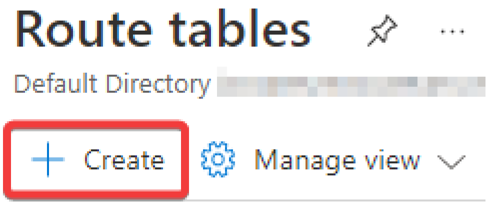
DNS name : -

Associated to : MyNewFirewall

3. Create a default route

We want to route traffic through the Azure Firewall, I need you to create a default route for that.

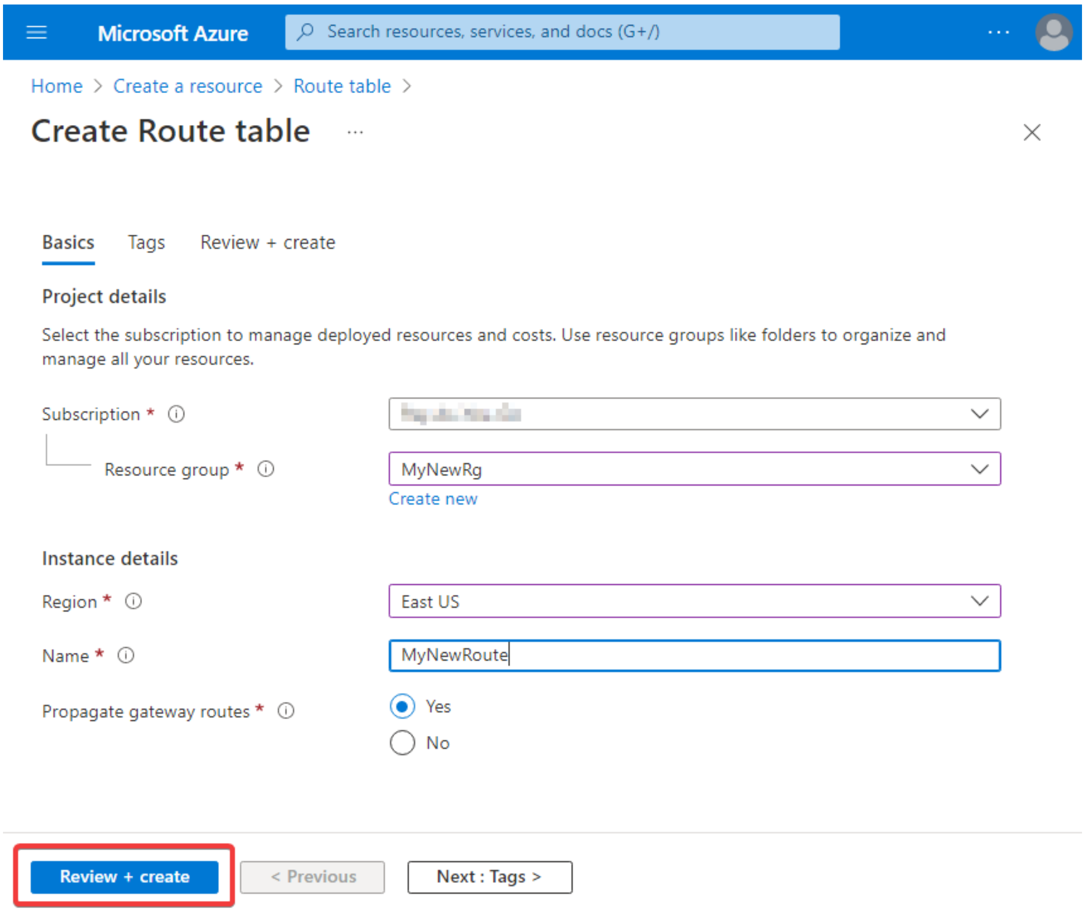
1. In the search box at the top of the Azure Portal, search for **Route Tables** and select it from the dropdown. Select **Create** after that:



Route tables

Default Directory [redacted]

2. On the **Basics** tab, enter or select the following details and click on **Review + create**:



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Create a resource > Route table >

Create Route table

Project details

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

Subscription * [redacted]

Resource group * MyNewRg

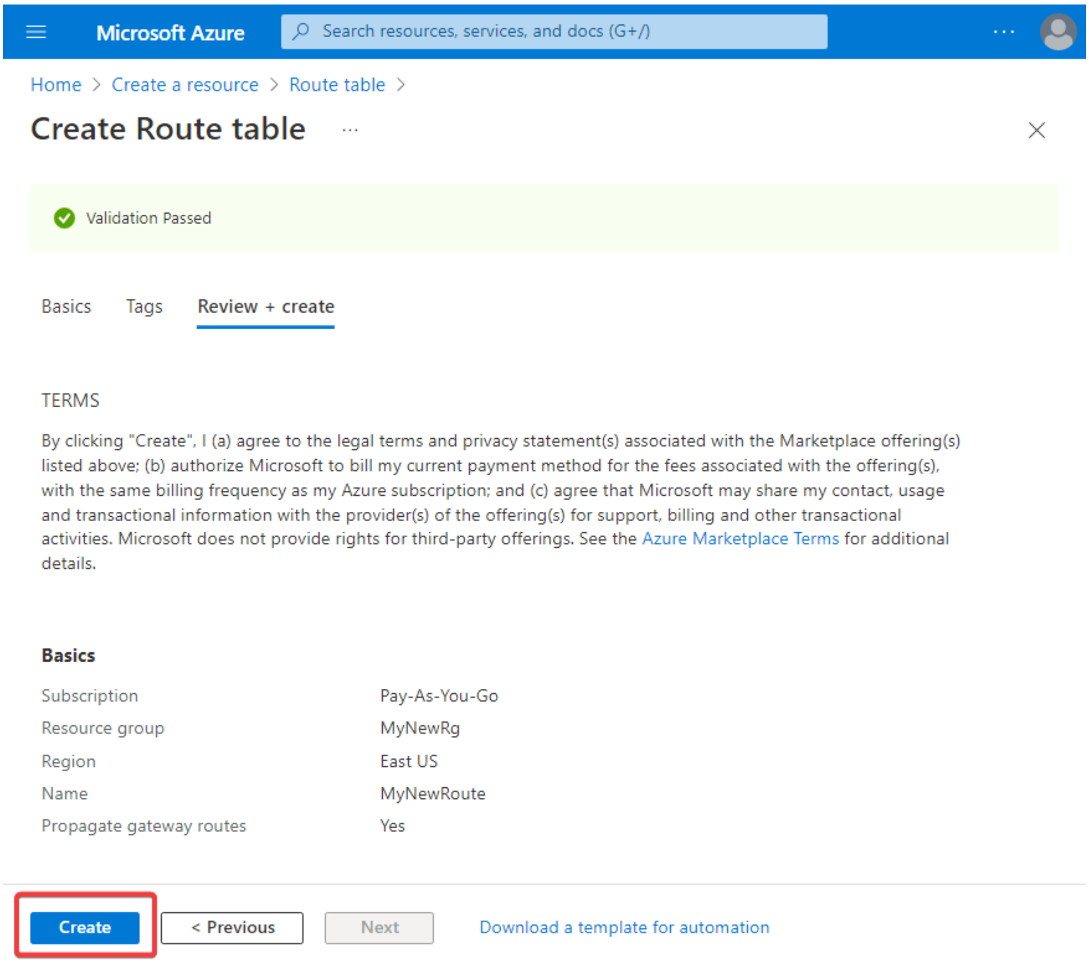
Instance details

Region * East US

Name * MyNewRoute

Propagate gateway routes * ● Yes ○ No

3. Click on **Create**:


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Create a resource > Route table >
Basics
Tags
Review + create
Create
< Previous
Next
Download a template for automation

Create Route table

Validation Passed

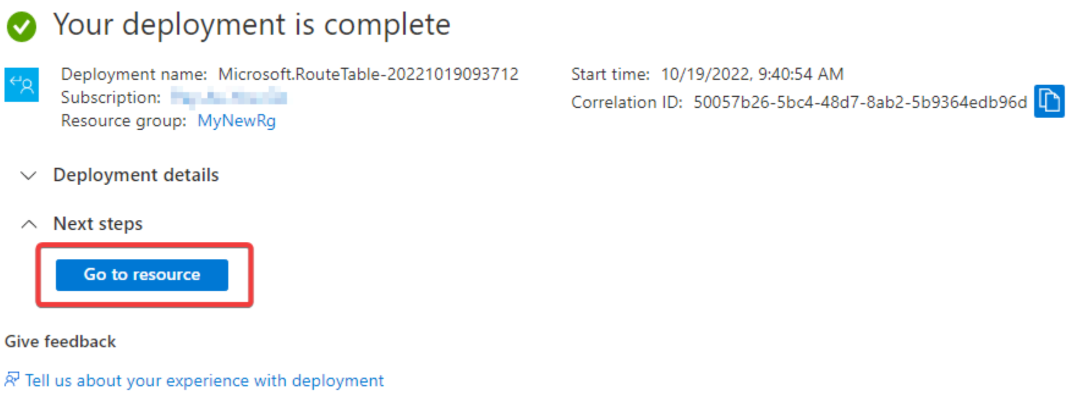
TERMS

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	Pay-As-You-Go
Resource group	MyNewRg
Region	East US
Name	MyNewRoute
Propagate gateway routes	Yes

4. Click on **Go to resource**:

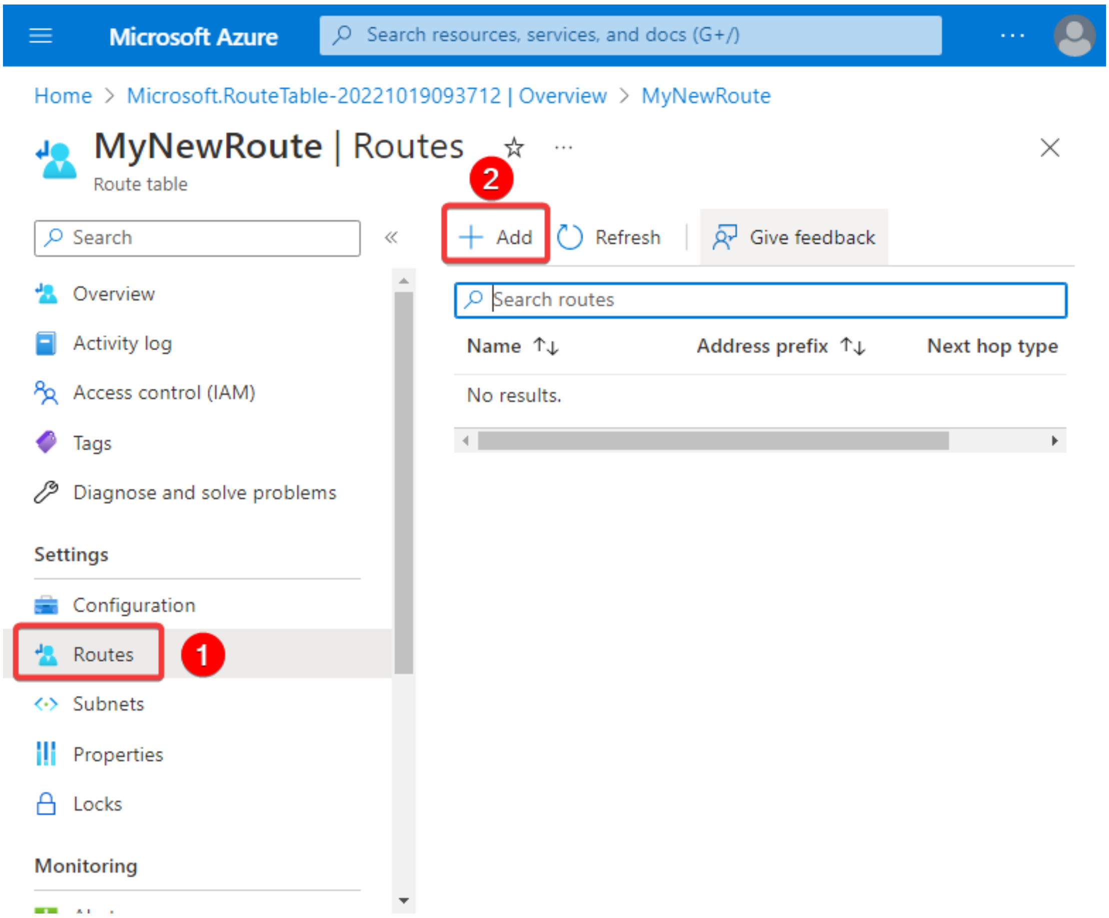


Your deployment is complete

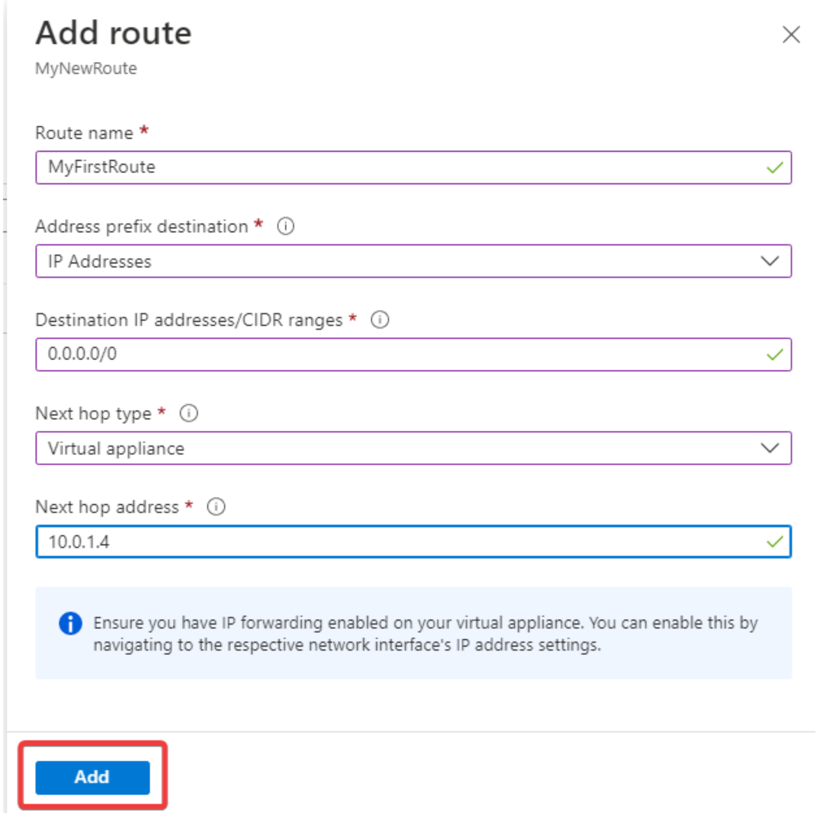
Deployment name: Microsoft.RouteTable-20221019093712
Subscription: [redacted]
Resource group: MyNewRg

Start time: 10/19/2022, 9:40:54 AM
Correlation ID: 50057b26-5bc4-48d7-8ab2-5b9364edb96d

5. From the left menu, select **Routes** and then select **+Add**:



6. On the **Add route** page, enter or select the following details and click **Add**.
    - Route name: **MyFirstRoute**
    - Address prefix source: **IP Addresses**
    - Destination IP Addresses/CIDR ranges: **0.0.0.0/0**
    - Next hop type: **Virtual appliance**
    - Next hop address: Paste the private IP address of **MyNewFirewall** (10.0.1.4)



Add route

MyNewRoute

Route name * MyFirstRoute

Address prefix destination * IP Addresses

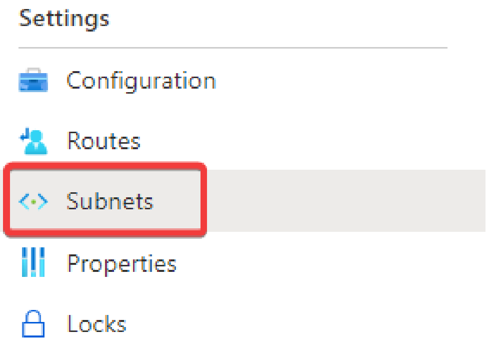
Destination IP addresses/CIDR ranges * 0.0.0.0/0

Next hop type * Virtual appliance

Next hop address * 10.0.1.4

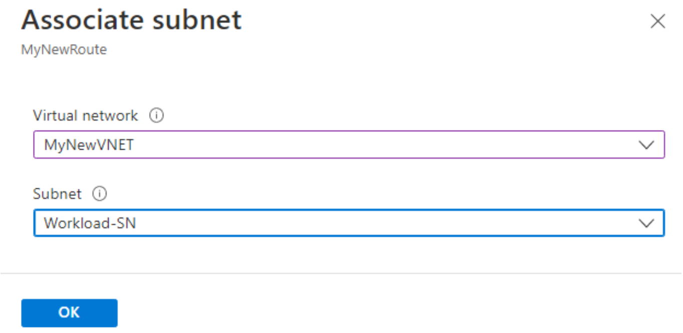
Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.

7. From the left menu, select **Subnets**:



8. Click on the **+Associate** button, enter or select the following details on the **Associate Subnet** page and click **Ok:**

   - Virtual Network: **MyNewVNET**
   - Subnet: **Workload-SN**



Associate subnet

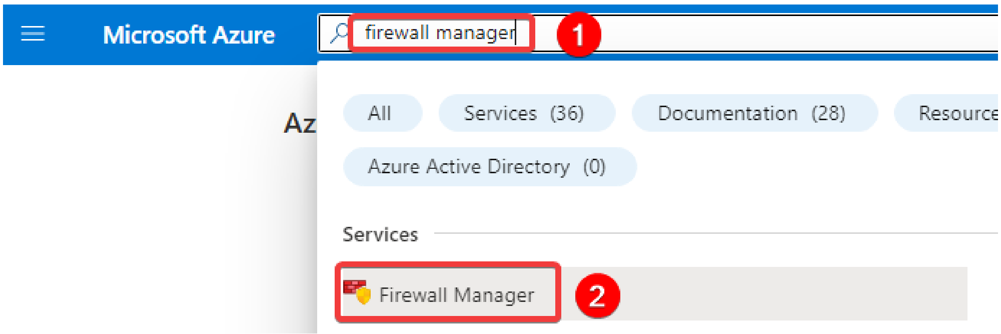
MyNewRoute

Virtual network MyNewVNET

Subnet Workload-SN

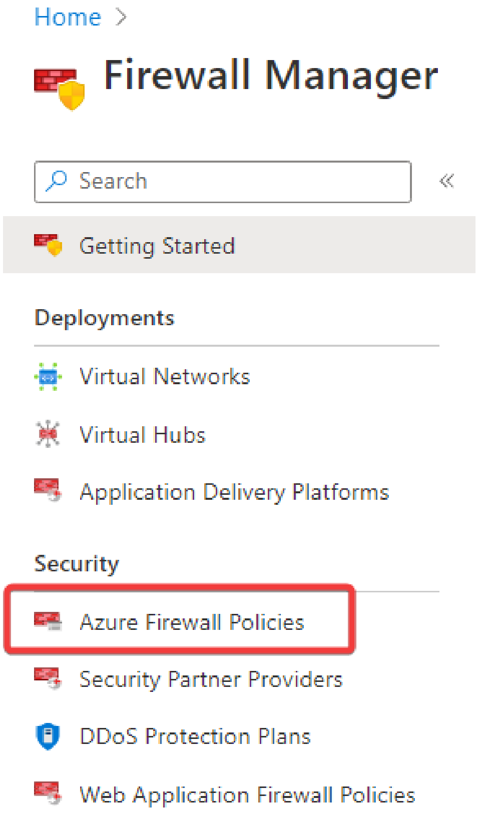
4. Create the Application rule

1. In the search box at the top of the Azure Portal, search for **Firewall Manager** and select it from the dropdown list:

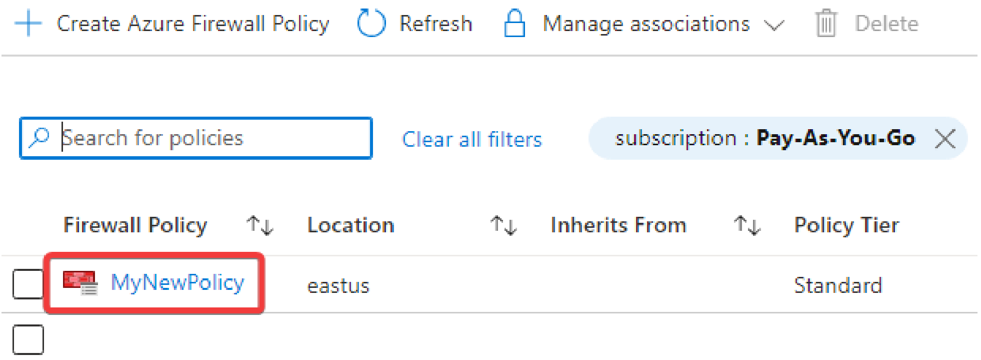


firewall manager

2. From the left menu, click on **Azure Firewall Policies**:

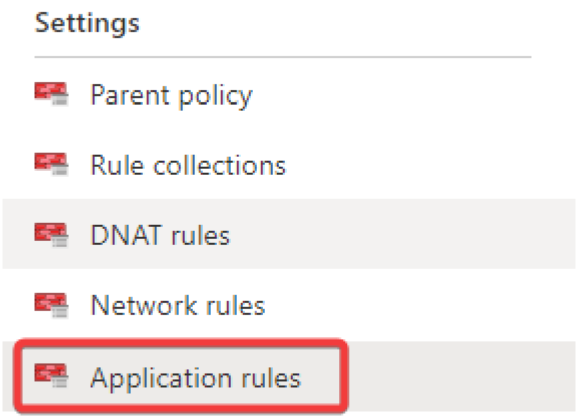


3. Since we already created a policy, click on **MyNewPolicy:**

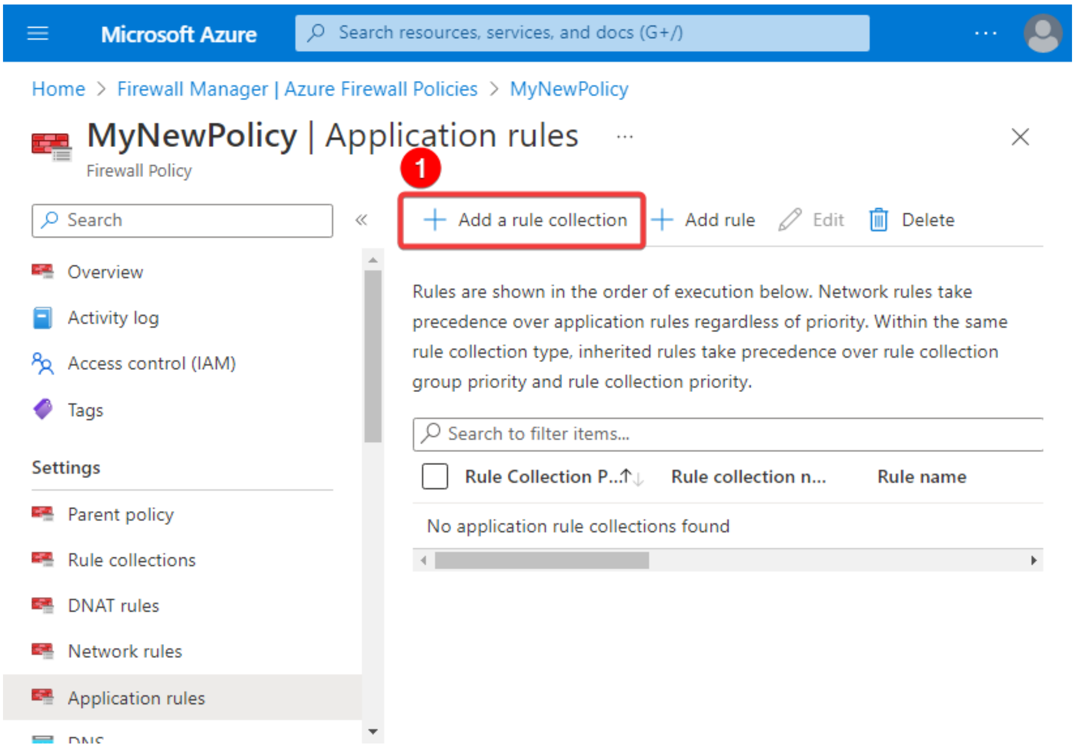


	Firewall Policy ↑↓	Location ↑↓	Inherits From ↑↓	Policy Tier
□	MyNewPolicy	eastus		Standard
□				

4. From the left menu, click on **Application rules**:



5. Click on the **+Add a rule collection** button:

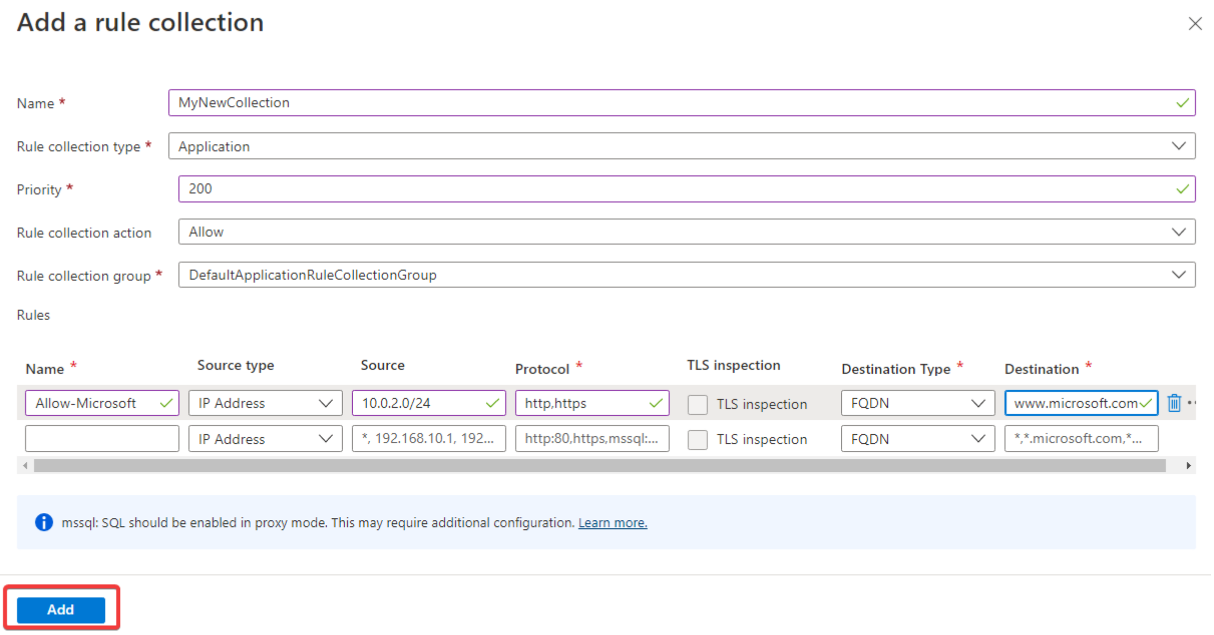


Rules are shown in the order of execution below. Network rules take precedence over application rules regardless of priority. Within the same rule collection type, inherited rules take precedence over rule collection group priority and rule collection priority.

No application rule collections found

6. Enter or select the following details on the Add a rule collection page and click on **Add**:
   - Name: **MyNewCollection**
   - Rule Collection type: **Application**
   - Priority: **200**
   - Rule Collection action: **Allow**
   - Rule Collection group: **DefaultApplicationRuleCollectionGroup**
   - Rules:
     - Name: **Allow-Microsoft**
     - Source type: **IP Address**
     - Source: Private IP of Workload-SN (**10.0.2.0/24**)
     - Protocol: **http,https**
     - Destination type: **FQDN**

- Destination: www.microsoft.com



Add a rule collection

Name *	MyNewCollection
Rule collection type *	Application
Priority *	200
Rule collection action	Allow
Rule collection group *	DefaultApplicationRuleCollectionGroup

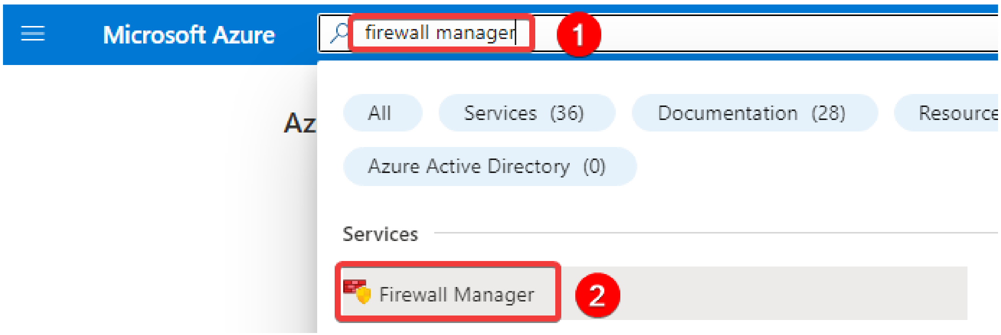
Rules

Name *	Source type	Source	Protocol *	TLS inspection	Destination Type *	Destination *
Allow-Microsoft	IP Address	10.0.2.0/24	http,https	☐ TLS inspection	FQDN	www.microsoft.com
	IP Address	*, 192.168.10.1, 192...	http:80,https,mssql:...	☐ TLS inspection	FQDN	*,*.microsoft.com,*...

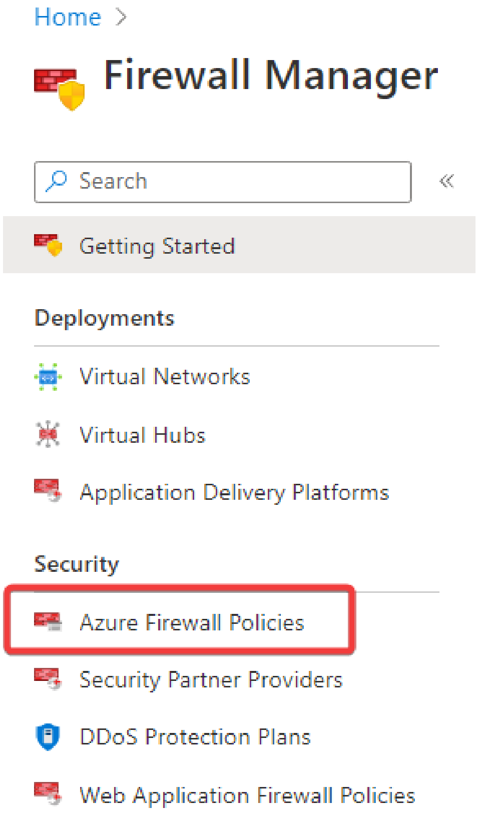
mssql: SQL should be enabled in proxy mode. This may require additional configuration. Learn more.

5. Create the Network rule

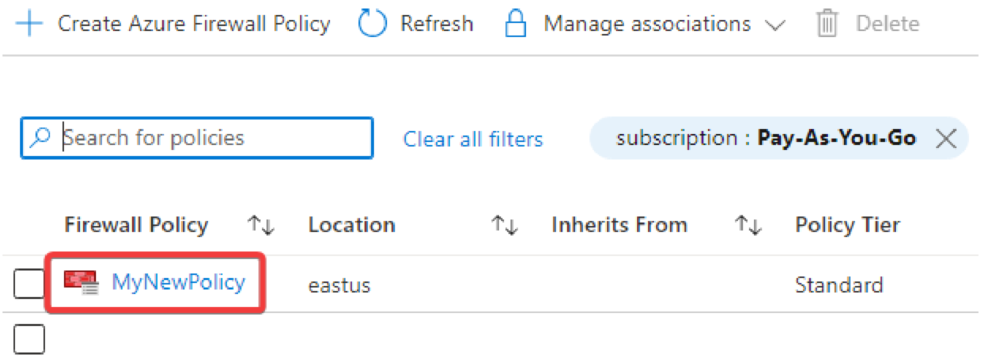
1. In the search box at the top of the Azure Portal, search for **Firewall Manager** and select it from the dropdown list:



2. From the left menu, click on **Azure Firewall Policies**:

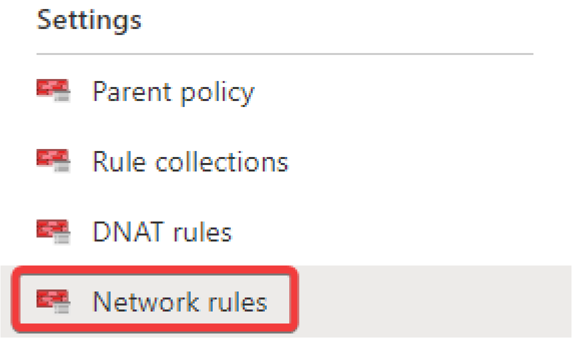


3. Since we already created a policy, click on **MyNewPolicy:**

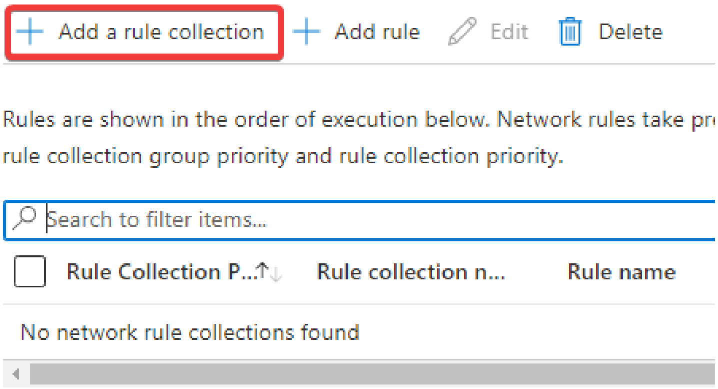


	Firewall Policy	Location	Inherits From	Policy Tier
□	MyNewPolicy	eastus		Standard
□				

4. From the left menu, click on **Network rules**:



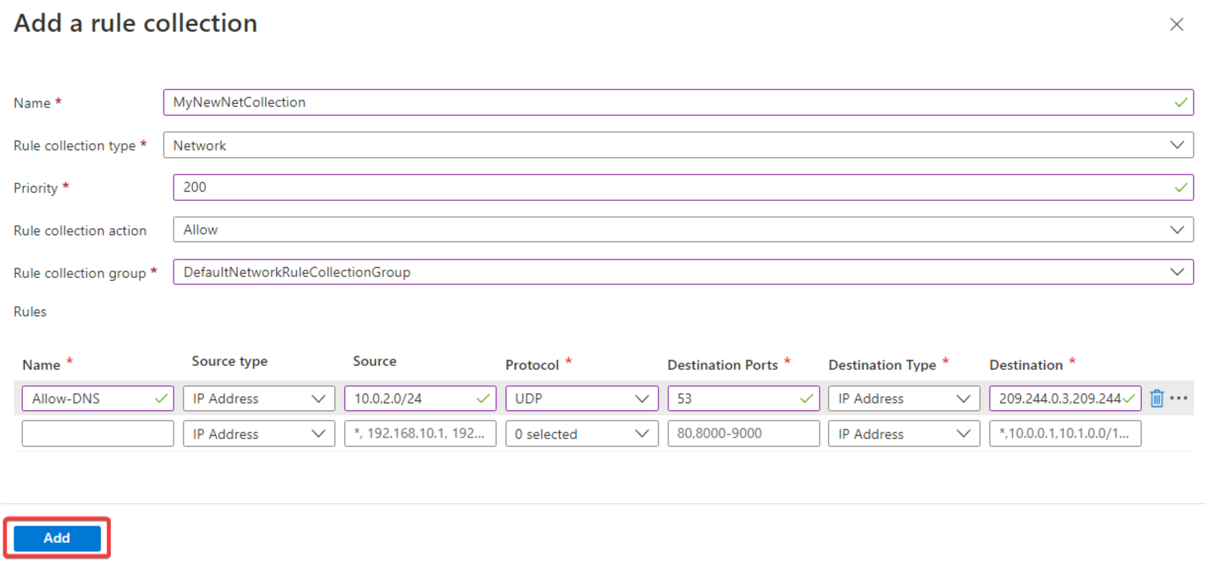
5. Click on the **+Add a rule collection** button:



Rules are shown in the order of execution below. Network rules take pr
rule collection group priority and rule collection priority.

□	Rule Collection P...↑↓	Rule collection n...	Rule name
No network rule collections found			

6. Enter or select the following details on the Add a rule collection page and click on **Add**:
    - Name: **MyNewNetCollection**
    - Rule Collection type: **Network**
    - Priority: **200**
    - Rule Collection action: **Allow**
    - Rule Collection group: **DefaultNetworkRuleCollectionGroup**
    - Rules:
        - Name: **Allow-DNS**
        - Source type: **IP Address**
        - Source: Private IP of Workload-SN (**10.0.2.0/24**)
        - Protocol: **UDP**
        - Destination ports: **53**
        - Destination type: **IP Address**
        - Destination: **209.244.0.3,209.244.0.4**



Add a rule collection

Name * MyNewNetCollection

Rule collection type * Network

Priority * 200

Rule collection action Allow

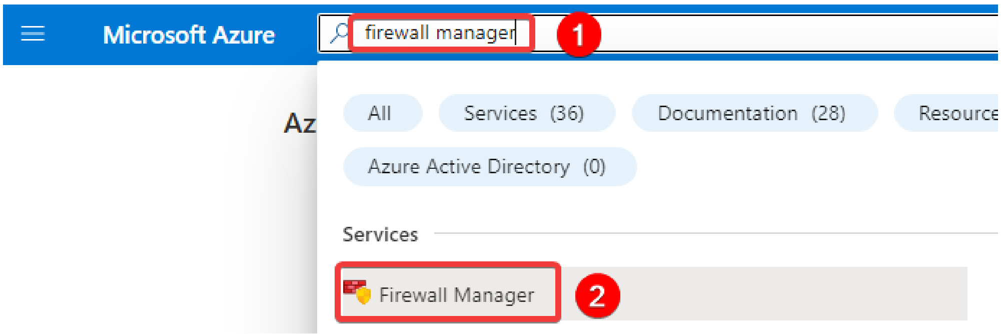
Rule collection group * DefaultNetworkRuleCollectionGroup

Rules

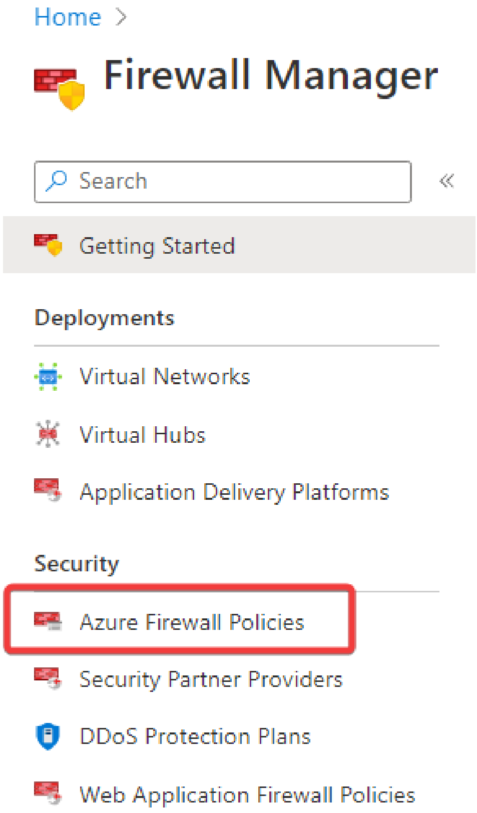
Name *	Source type	Source	Protocol *	Destination Ports *	Destination Type *	Destination *
Allow-DNS	IP Address	10.0.2.0/24	UDP	53	IP Address	209.244.0.3,209.244
	IP Address	*, 192.168.10.1, 192...	0 selected	80,8000-9000	IP Address	*,10.0.0.1,10.1.0.0/1...

5. Create the DNAT rule

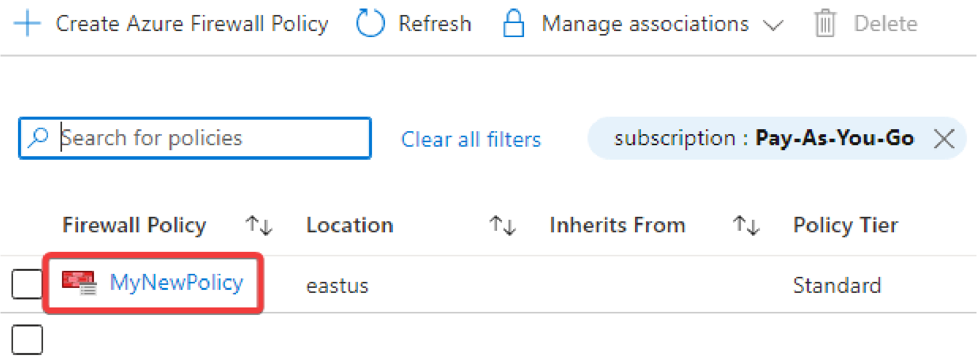
1. In the search box at the top of the Azure Portal, search for **Firewall Manager** and select it from the dropdown list:



2. From the left menu, click on **Azure Firewall Policies**:

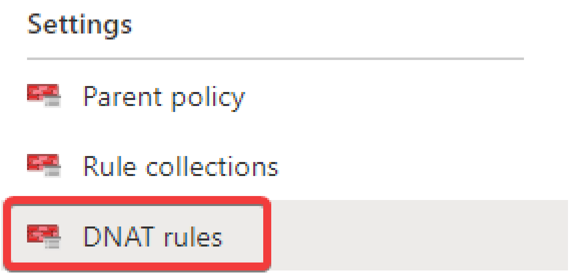


3. Since we already created a policy, click on **MyNewPolicy:**

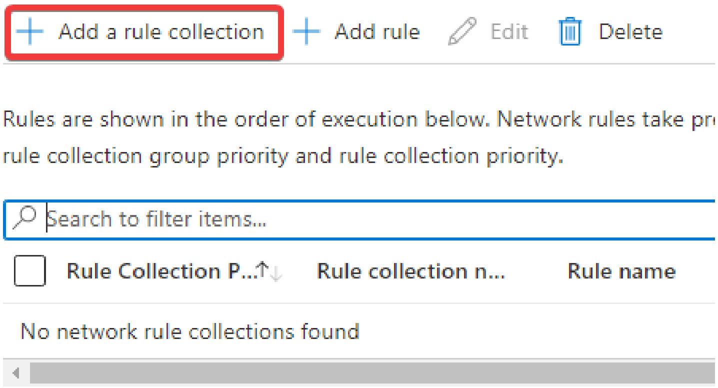


	Firewall Policy ↑↓	Location ↑↓	Inherits From ↑↓	Policy Tier
□	MyNewPolicy	eastus		Standard
□				

4. From the left menu, click on **DNAT rules**:



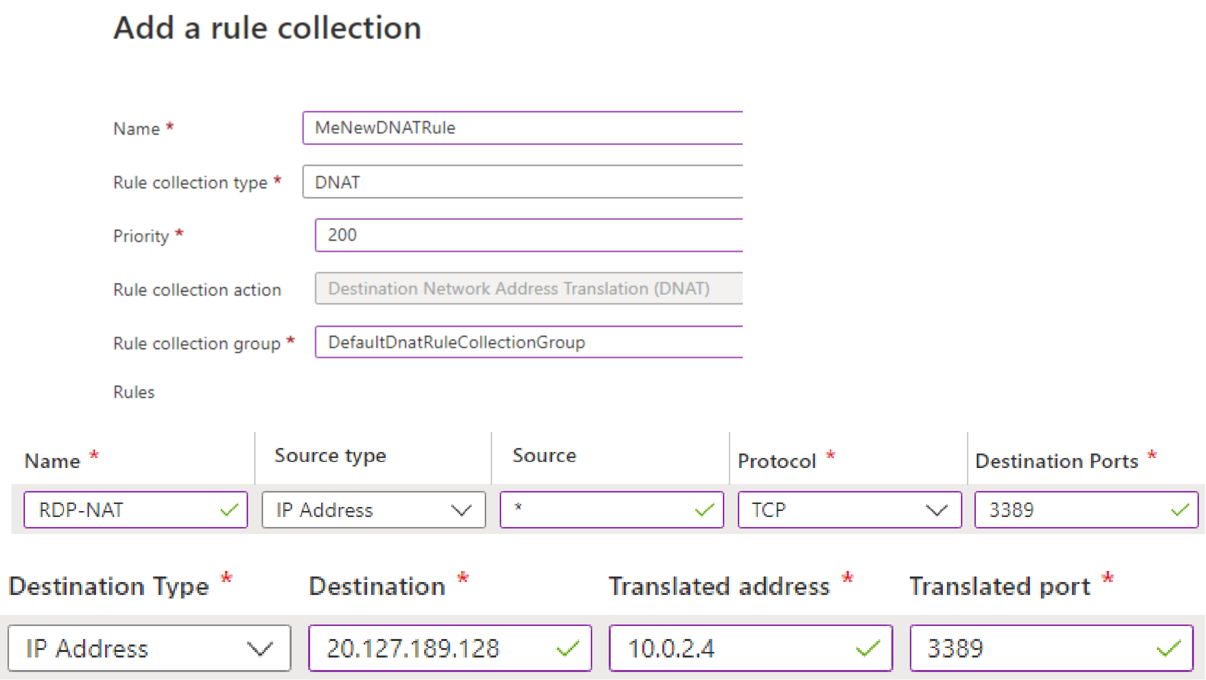
5. Select **+Add a rule collection**:



Rules are shown in the order of execution below. Network rules take pr
rule collection group priority and rule collection priority.

No network rule collections found

6. Enter or select the following details on Add a rule collection page and click on **Add**:
   - Name: **MyNewDNATRule**
   - Rule Collection type: **DNAT**
   - Priority: **200**
   - Rule Collection group: **DefaultDnatRuleCollectionGroup**
   - Rules:
     - Name: **RDP-NAT**
     - Source type: **IP Address**
     - Source: *****
     - Protocol: **TCP**
     - Destination ports: **3389**
     - Destination type: **IP Address**
     - Destination: **The public IP of MyNewFirewall**
     - Translated Address: The private IP of Srv-work (**10.0.2.4**)
     - Translated port: **3389**



Add a rule collection

Name *	MeNewDNATRule
Rule collection type *	DNAT
Priority *	200
Rule collection action	Destination Network Address Translation (DNAT)
Rule collection group *	DefaultDnatRuleCollectionGroup

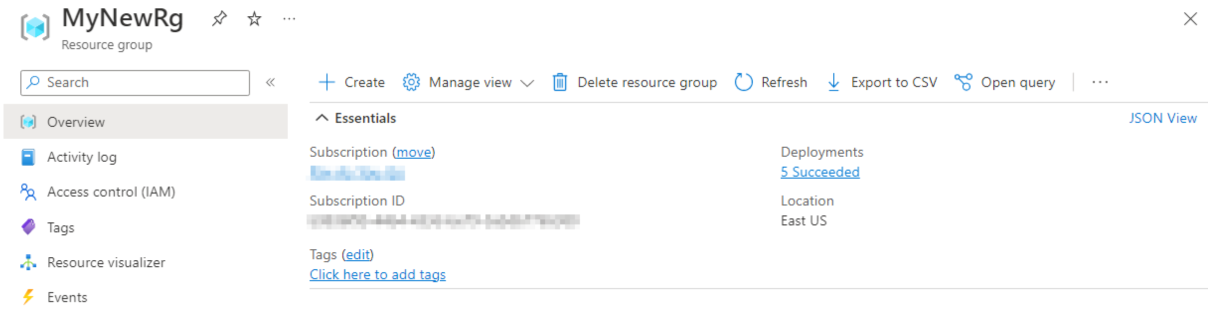
Rules

Name *	Source type	Source	Protocol *	Destination Ports *
RDP-NAT	IP Address	*	TCP	3389

Destination Type *	Destination *	Translated address *	Translated port *
IP Address	20.127.189.128	10.0.2.4	3389

6. Change DNS settings and test the firewall

1. In the search box at the top of the Azure Portal, search for **Resource Groups** and click on your Resource group:



Subscription (move)
[redacted]

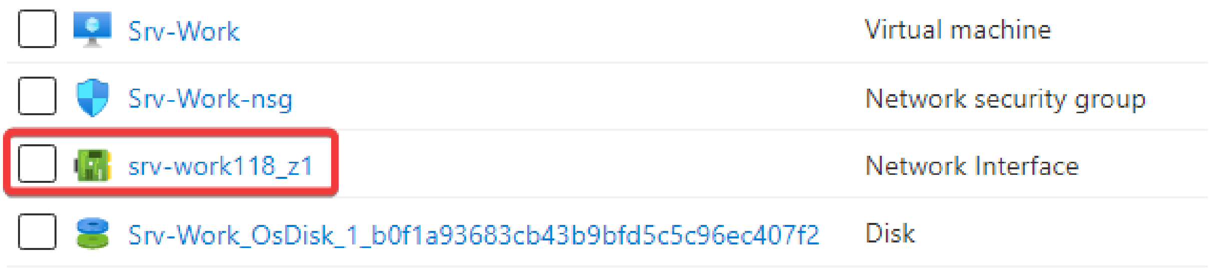
Subscription ID
[redacted]

Tags (edit)
Click here to add tags

Deployments
5 Succeeded

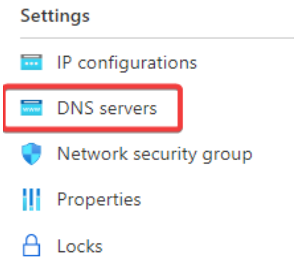
Location
East US

2. Scroll down and select the **network interface** of **Srv-work**:

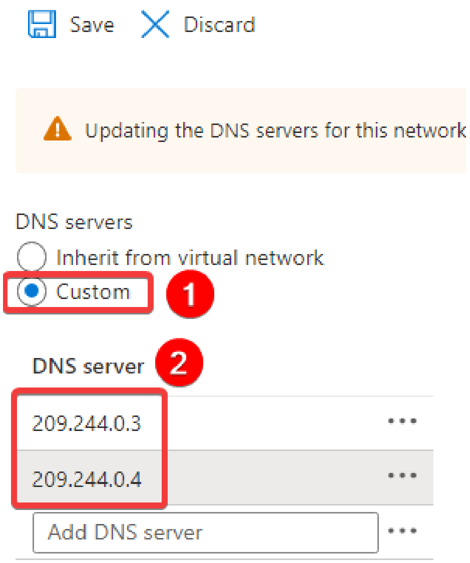


□ Srv-Work	Virtual machine
□ Srv-Work-nsg	Network security group
□ srv-work118_z1	Network Interface
□ Srv-Work_OsDisk_1_b0f1a93683cb43b9bfd5c5c96ec407f2	Disk

3. From the left menu, select **DNS servers** under settings:



4. Select **Custom,** add the following DNS servers and click on save:

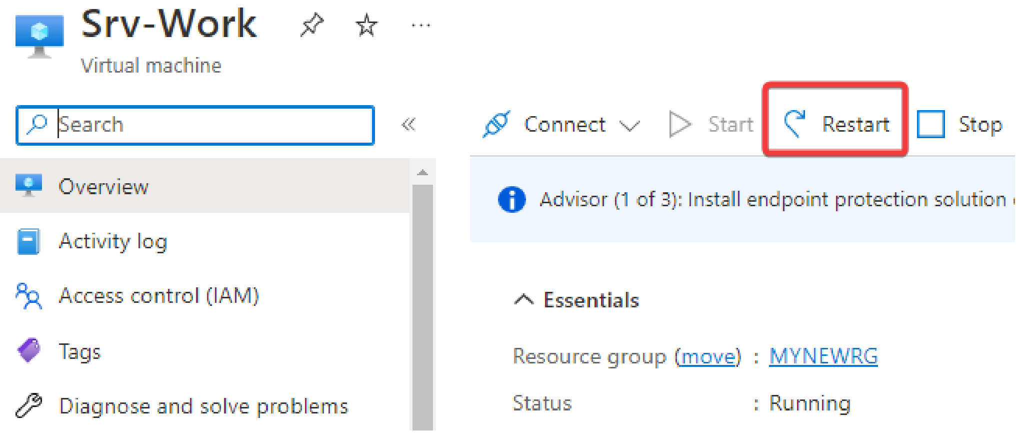


Updating the DNS servers for this network

DNS servers
○ Inherit from virtual network
● Custom

DNS server
209.244.0.3
209.244.0.4
Add DNS server

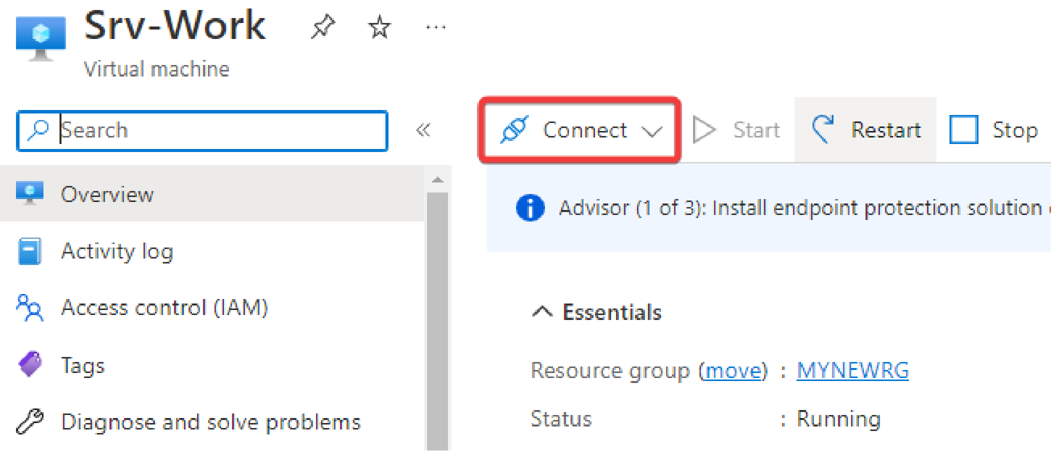
5. In the search box at the top of the Azure Portal, search for **Virtual Machines**, click on **Srv-work** and click on **Restart**:



Advisor (1 of 3): Install endpoint protection solution

Resource group (move) : MYNEWRG
Status : Running

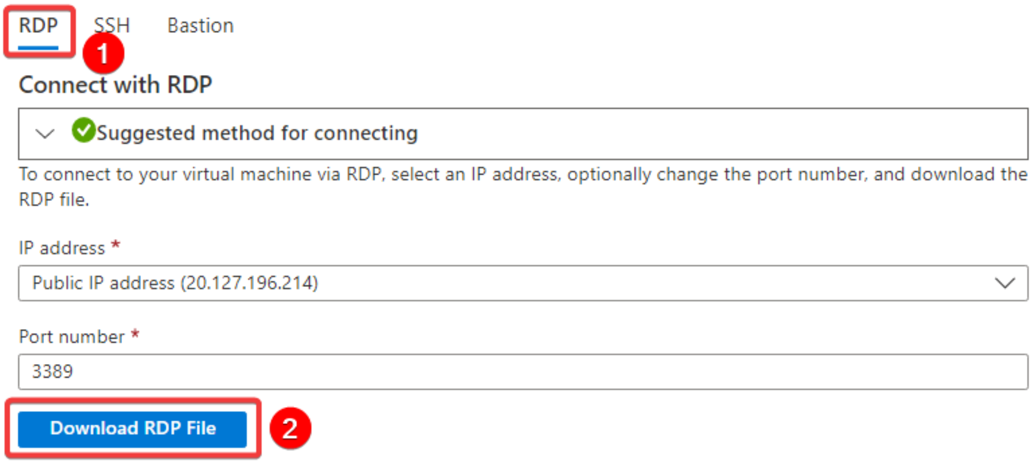
6. In the search box at the top of the Azure Portal, search for **Virtual Machines** and select **Srv-Work** from the list and click on **Connect**:



Advisor (1 of 3): Install endpoint protection solution

Resource group (move) : MYNEWRG
Status : Running

7. Click on **RDP** and click on the **Download RDP File** button:



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

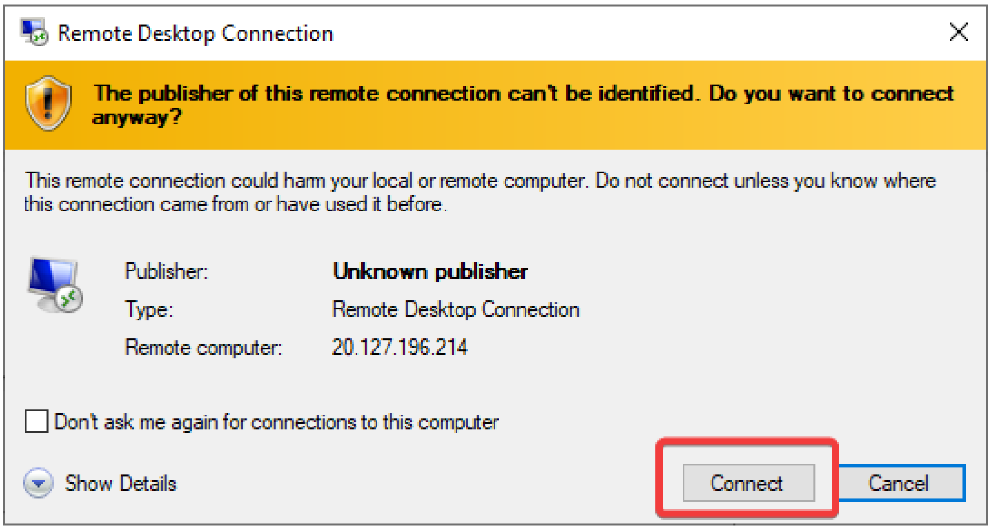
IP address *

Public IP address (20.127.196.214)

Port number *

3389

8. Open the downloaded **RDP** file and click on **Connect**:



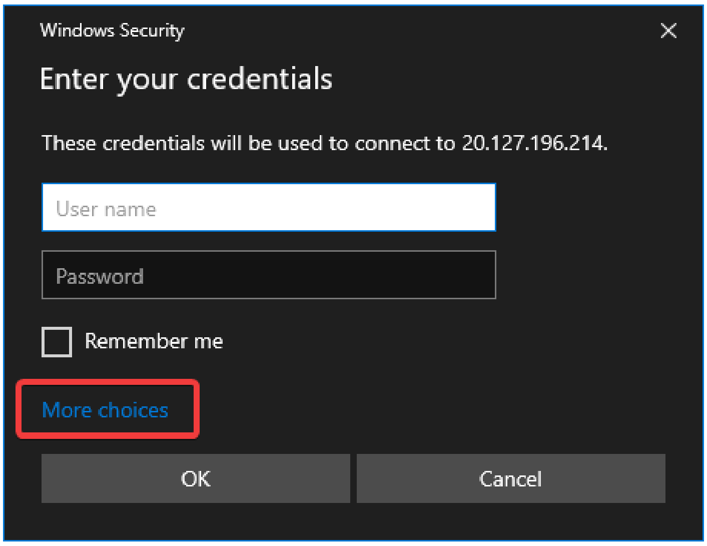
The publisher of this remote connection can't be identified. Do you want to connect anyway?

This remote connection could harm your local or remote computer. Do not connect unless you know where this connection came from or have used it before.

Publisher:	**Unknown publisher**
Type:	Remote Desktop Connection
Remote computer:	20.127.196.214

□ Don't ask me again for connections to this computer

9. On the **Windows Security** prompt, click on **More choices:**

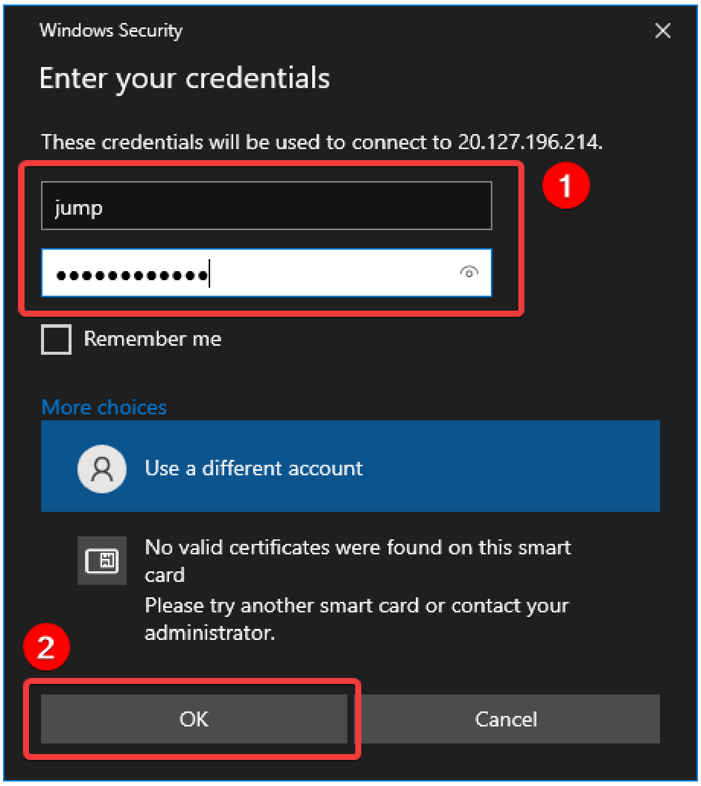


Enter your credentials

These credentials will be used to connect to 20.127.196.214.

□ Remember me

10. Click on **Use a different account** and enter the username and password you specified while creating the Virtual Machine and select **OK**:



Windows Security

Enter your credentials

These credentials will be used to connect to 20.127.196.214.

jump

••••••••••••

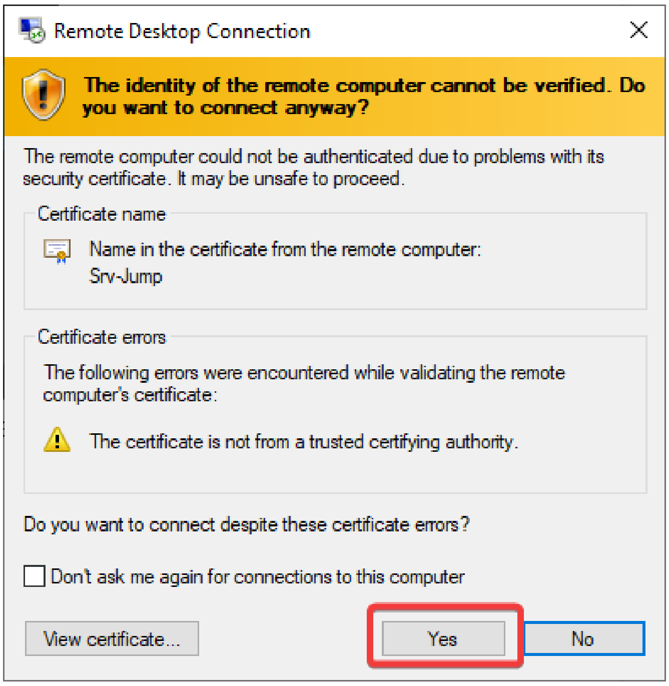
□ Remember me

More choices

Use a different account

No valid certificates were found on this smart card
Please try another smart card or contact your administrator.

11. You may receive a certificate warning during the sign-in process. Click **Yes** to continue:



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
Srv-Jump

Certificate errors

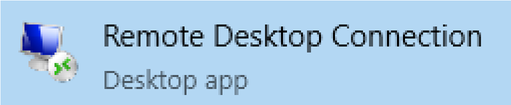
The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

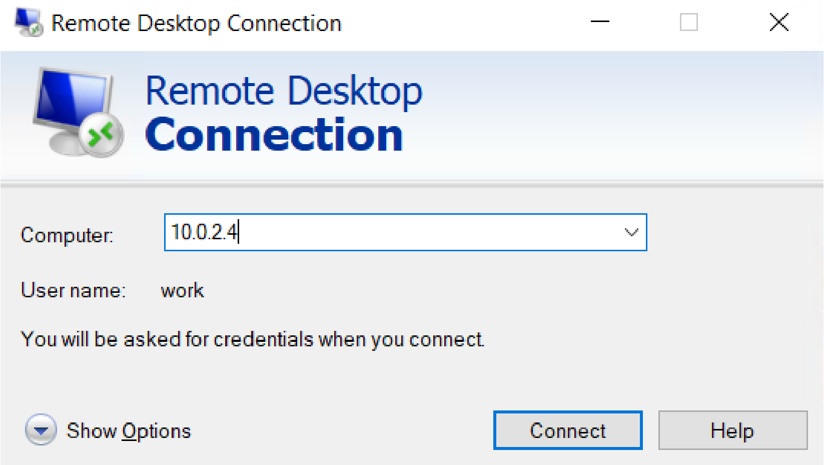
□ Don't ask me again for connections to this computer

12. On the **Srv-work** virtual machine, look for the **Remote Desktop Connection** app and open it:



Remote Desktop Connection
Desktop app

13. Type the Private IP address of the **Srv-work** virtual machine (10.0.2.4) and click on **Connect**:



Remote Desktop Connection

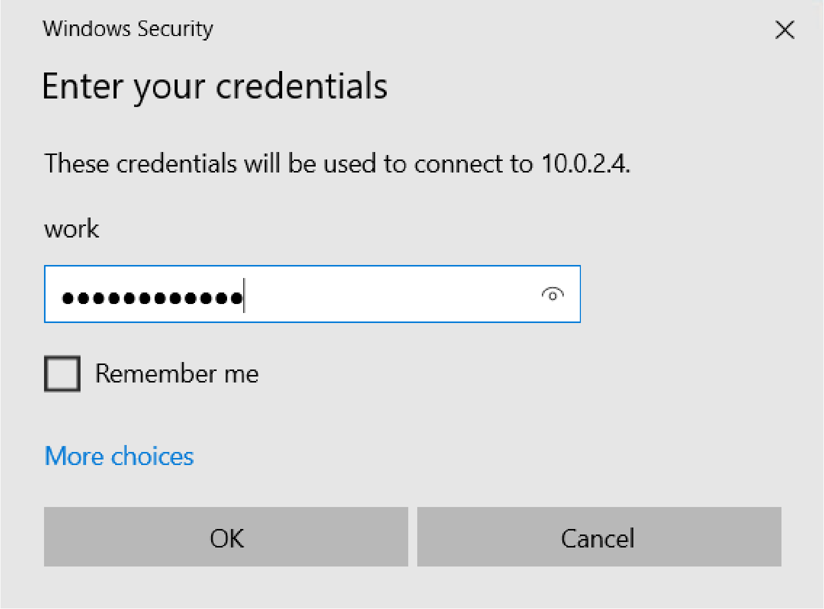
Remote Desktop **Connection**

Computer: 10.0.2.4

User name: work

You will be asked for credentials when you connect.

14. Now enter the password of the **Srv-work** virtual machine and click on **Ok**:



Windows Security

Enter your credentials

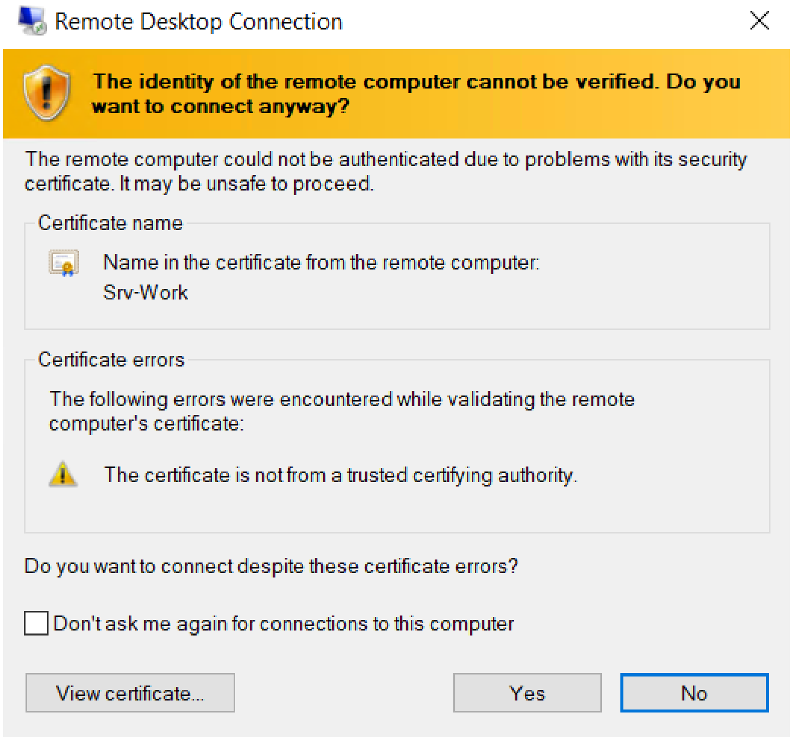
These credentials will be used to connect to 10.0.2.4.

work

●●●●●●●●●●●●

□ Remember me

15. You may receive a certificate warning during the sign-in process. Click **Yes** to continue:



Remote Desktop Connection

The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
Srv-Work

Certificate errors

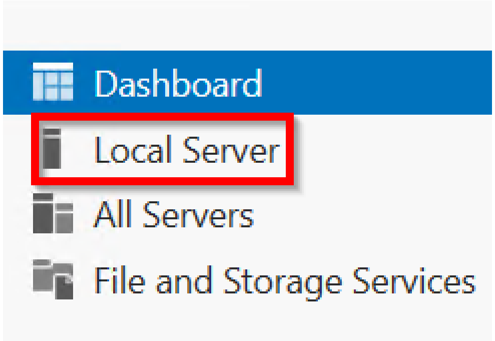
The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

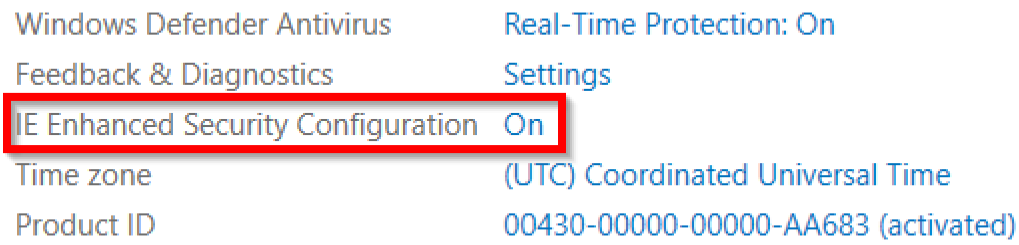
Do you want to connect despite these certificate errors?

□ Don't ask me again for connections to this computer

16. In the **Srv-work** virtual machine, click on **Local Server** from the left menu of the Server Manager dashboard:

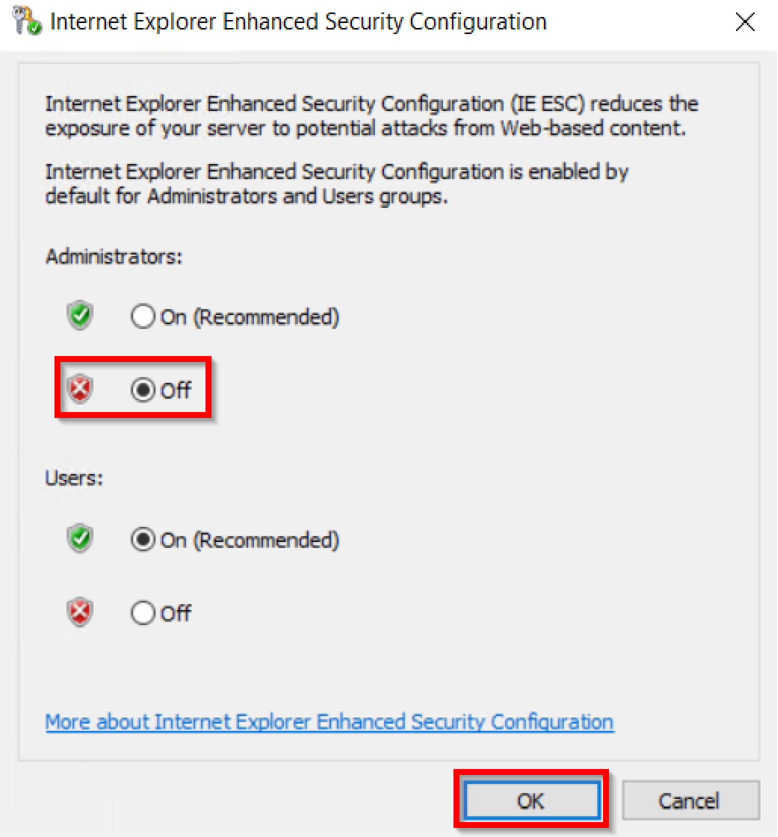


17. Turn off the **IE Enhanced Security Configuration**:



Windows Defender Antivirus	Real-Time Protection: On
Feedback & Diagnostics	Settings
IE Enhanced Security Configuration	On
Time zone	(UTC) Coordinated Universal Time
Product ID	00430-00000-00000-AA683 (activated)

18. Click on **Ok**:



Internet Explorer Enhanced Security Configuration

Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.

Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.

Administrators:

○ On (Recommended)

● Off

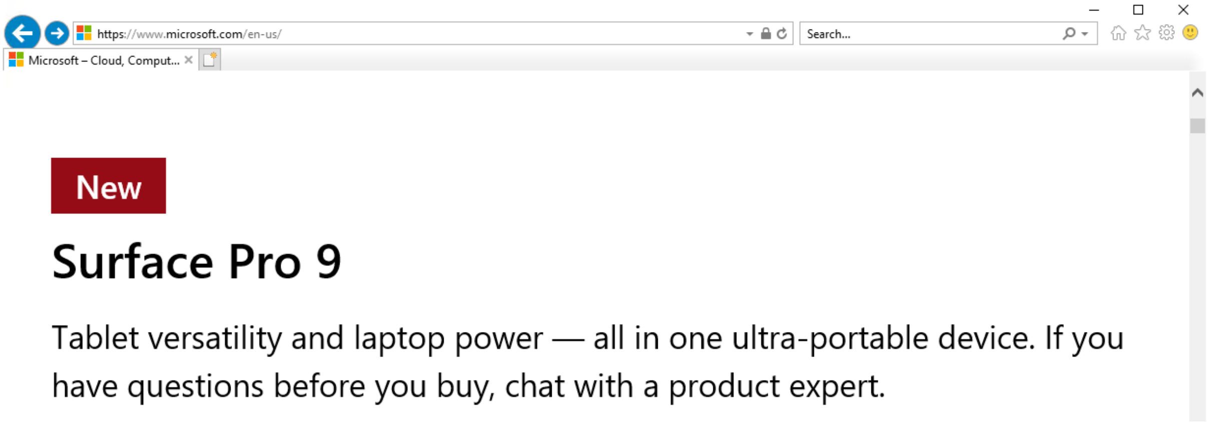
Users:

● On (Recommended)

○ Off

More about Internet Explorer Enhanced Security Configuration

19. Open Internet Explorer and browse to www.microsoft.com:



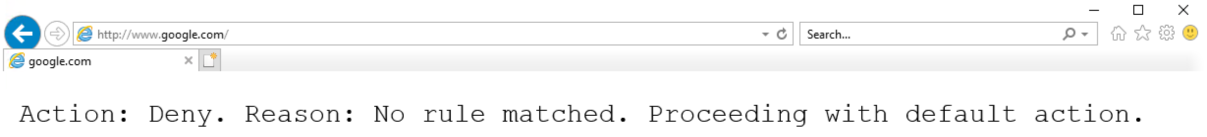
https://www.microsoft.com/en-us/
Search...
Microsoft – Cloud, Comput...

New

Surface Pro 9

Tablet versatility and laptop power — all in one ultra-portable device. If you have questions before you buy, chat with a product expert.

20. Browse to **www.google.com**, you will be blocked by the firewall:



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