

5. Create a new Azure Firewall and configure rules to control inbound and outbound traffic.

Create a resource group

- Sign in to the Azure portal. On the Azure portal menu, select Resource groups or search for and select Resource groups from any page, then select Add. Enter or select the following values:
 - Subscription Select your Azure subscription.
 - Resource group Enter- TestFwRg
 - Region Select a region. All other resources that you create must be in the same region.
- Select Review + create.
- Select Create.

Create a VNet

This VNet will have two subnets.

- On the Azure portal menu or from the Home page, select Create a resource. Select Networking. Search for Virtual network and select it. Select Create, then enter or select the following values:
 - Subscription Select your Azure subscription.
 - Resource group -Select TestFwRg
 - Name Enter TestFwVn
- Region Select the same location that you used previously.
- Select Next: IP addresses.
- For IPv4 Address space, accept the default 10.0.0.0/16.
- Under Subnet, select default.
- For Subnet name change the name to AzureFirewallSubnet.
- The firewall will be in this subnet, and the subnet name must be AzureFirewallSubnet.
- For Address range, type 10.0.1.0/26.
- Select Save.
- Next, create a subnet for the workload server.
- Select Add subnet.
- For Subnet name, type Workload-SN.
- For Subnet address range, type 10.0.2.0/24.
- Select Add.
- Select Review + create. Select Create.

Create a virtual machine

Now create the workload virtual machine, and place it in the Workload-SN subnet.

- On the Azure portal menu or from the Home page, select Create a resource.
- Select Windows Server 2019 Datacenter.
- Enter or select these values for the virtual machine:
 - Setting Value
 - Subscription Select your Azure subscription.
 - Resource group Select TestFwRg
 - Virtual machine name Enter Srv-Work.
 - Region Select the same location that you used previously.
 - Username Enter a username.
 - Password Enter a password.
 - Under Inbound port rules, Public inbound ports, select None.
 - Accept the other defaults and select Next: Disks.
 - Accept the disk defaults and select Next: Networking.
 - Make sure that Test-FW-VN is selected for the virtual network and the subnet is Workload-SN.
 - For Public IP, select None.
 - Accept the other defaults and select Next: Management.
 - Select Disable to disable boot diagnostics. Accept the other defaults and select Review + create.
 - Review the settings on the summary page, and then select Create.
 - After the deployment completes, select the Srv-Work resource and note the private IP address for later use- 10.0.2.4

Deploy the firewall and policy

- Deploy the firewall into the VNet
- On the Azure portal menu or from the Home page, select Create a resource.
- Type firewall in the search box and press Enter.
- Select Firewall and then select Create.
- On the Create a Firewall page, use the following table to configure the firewall:
 - Subscription Select your Azure subscription.
 - Resource group Select TestFwRg.
 - Name Enter Test-FW01.
 - Region Select the same location that you used previously.
 - Firewall management Select Use a Firewall Policy to manage this firewall.
 - Firewall policy Select Add new, and enter fw-test-pol.
 - Select the same region that you used previously.
 - Choose a virtual network Select Use existing, and then select TestFwVn.
 - Public IP address Select Add new, and enter fw-pip for the Name.
- Accept the other default values, then select Review + create.
- Review the summary, and then select Create to create the firewall.

- This will take a few minutes to deploy.
- After deployment completes, go to the TestFwRg resource group, and select the Test-FW01 firewall.
- Note the firewall private and public IP addresses. You'll use these addresses later.
20.198.114.243 10.0.1.4

The screenshot shows the 'Create a firewall' wizard in the Microsoft Azure portal. The 'Review + create' tab is selected, showing a summary of the configuration. A green banner at the top indicates 'Validation passed'. The configuration details are as follows:

Basics	
Subscription	Free Trial
Resource group	TestFwRg
Region	Central India
Azure Firewall Sku	Standard
Firewall Policy Name	fw-test-pol
Firewall Policy Sku	Standard
Virtual network	TestFwVn
Address space	10.0.0.0/16
Firewall public IP address	fw-pip
Availability zone	None

Below the basics section, there is a 'Tags' section with a table that shows 'No results'.

Resource type	Name	Value
No results		

At the bottom, there are buttons for 'Create', 'Previous', and 'Next', along with a link to 'Download a template for automation'.

Create a default route

For the Workload-SN subnet, configure the outbound default route to go through the firewall.

- On the Azure portal menu, select All services or search for and select All services from any page.
- Under Networking, select Route tables.
- Select Create, then enter or select the following values:
 - Subscription Select your Azure subscription.
 - Resource group Select TestFwRg.
 - Region Select the same location that you used previously.
 - Name Enter Firewall-route.
- Select Review + create.
- Select Create.

Create Route table

Basics | Tags | Review + create

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

Subscription * ⓘ Free Trial

Resource group * ⓘ TestFwRg
[Create new](#)

Instance details

Region * ⓘ Central India

Name * ⓘ Firewall-route ✓

Propagate gateway routes * ⓘ ☒ Yes ☐ No

[Previous](#) [Next](#) [Review + create](#)

After deployment completes, select Go to resource.

- On the Firewall-route page, select Subnets and then select Associate.
- Select Virtual network > TestFwVn
- For Subnet, select Workload-SN. Make sure that you select only the Workload-SN subnet for this route, otherwise your firewall won't work correctly.
- Select OK.

Firewall-route | Subnets

Route table

Search << + Associate

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Configuration

Routes

Subnets

Name ↑↓	Address range ↑↓	Virtual network ↑↓	Security group ↑↓
Workload-SN	10.0.2.0/24	TestFwVn	-

- Select Routes and then select Add.
- For Route name, enter fw-dg.
- For Address prefix, enter 0.0.0.0/0.

- For Next hop type, select Virtual appliance. Azure Firewall is actually a managed service, but virtual appliance works in this situation.
- For Next hop address, enter the private IP address for the firewall that you noted previously.
- Select OK.

The screenshot shows the Microsoft Azure portal interface. On the left, the navigation pane is open, showing the 'Routes' section under 'Firewall-route | Routes'. The main area displays the 'Add route' form for a 'Firewall-route'. The form includes the following fields:

- Route name ***: fw-dg (with a green checkmark)
- Destination type ***: IP Addresses (with a dropdown arrow)
- Destination IP addresses/CIDR ranges ***: 0.0.0.0/0 (with a green checkmark)
- Next hop type ***: Virtual appliance (with a dropdown arrow)
- Next hop address ***: 10.0.1.4 (with a green checkmark)

Below the form, there is a blue information box with a question mark icon and the text: "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." At the bottom right of the form, there is a blue 'Add' button and a 'Give feedback' link.

Configure an application rule

This is the application rule that allows outbound access to www.google.com.

- Open the TestFwRg resource group, and select the fw-test-pol firewall policy.
- Select Application rules.
- Select Add a rule collection.
- For Name, enter App-Coll01.
- For Priority, enter 200.
- For Rule collection action, select Allow.
- Under Rules, for Name, enter Allow-Google.
- For Source type, select IP address.
- For Source, enter 10.0.2.0/24.
- For Protocol:port, enter http, https.
- For Destination Type, select FQDN.
- For Destination, enter www.google.com
- Select Add.

Add a rule collection

Name * App-Co1101 ✓

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-Google ✓	IP Address	10.0.2.0/24 ✓	http,https ✓	<input type="checkbox"/> TLS inspection	FQDN	www.google.com ✓
	IP Address	*, 192.168.10.1, 192...	http:80,https,mssql...	<input type="checkbox"/> TLS inspection	FQDN	*.microsoft.com,*...

mssql: SQL should be enabled in proxy mode. This may require additional configuration. [Learn more](#)

Add

Configure a network rule

This is the network rule that allows outbound access to two IP addresses at port 53 (DNS).

- Select Network rules.
- Select Add a rule collection.
- For Name, enter Net-Coll01.
- For Priority, enter 200.
- For Rule collection action, select Allow.
- For Rule collection group, select DefaultNetworkRuleCollectionGroup.
- Under Rules, for Name, enter Allow-DNS.
- For Source type, select IP Address.
- For Source, enter 10.0.2.0/24.
- For Protocol, select UDP.
- For Destination Ports, enter 53.
- For Destination type select IP address.
- For Destination, enter 209.244.0.3,209.244.0.4.
- These are public DNS servers operated by CenturyLink.

Microsoft Azure Search resources, services, and docs (G+) krsureshit@live.com DEFAULT DIRECTORY

Add a rule collection

Name *

Rule collection type *

Priority *

Rule collection action

Rule collection group *

Rules

Name *	Source type	Source	Protocol *	Destination Ports *	Destination Type *	Destination *
Allow-DNS	IP Address	10.0.2.0/24	UDP	53	IP Address	209.244.0.3,209.2...
	IP Address	*, 192.168.10.1, 192...	0 selected	80,8000-9000	IP Address	*, 10.0.0.1, 10.1.0.0/1...

[Add](#)

Configure a DNAT rule

This rule allows you to connect a remote desktop to the Srv-Work virtual machine through the firewall.

- Select the DNAT rules.
- Select Add a rule collection.
- For Name, enter rdp.
- For Priority, enter 200.
- For Rule collection group, select DefaultDnatRuleCollectionGroup.
- Under Rules, for Name, enter rdp-nat.
- For Source type, select IP address.
- For Source, enter *.
- For Protocol, select TCP.
- For Destination Ports, enter 3389.
- For Destination Type, select IP Address.
- For Destination, enter the firewall public IP address.
- For Translated address, enter the Srv-work private IP address.
- For Translated port, enter 3389.
- Select Add.

[+ Add a rule collection](#) [+ Add rule](#) [Edit](#) [Delete](#)

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.

Search to filter items...

<input checked="" type="checkbox"/>	Rule Collection P...	Rule collection n...	Rule name	Source	Port	Protocol	Destination	Translated Addre...	Translated Port
Rule Collection Group: DefaultDnatRuleCollectionGroup with priority 100.									
<input checked="" type="checkbox"/>	200	RDP	rdp-nat	* ⓘ	3389	TCP	20.198.114.243 ⓘ	10.0.2.4	3389

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

For testing purposes, configure the server's primary and secondary DNS addresses.

On the Azure portal menu, select **Resource groups** or search for and select *Resource groups* from any page. Select the TestFwRg resource group.

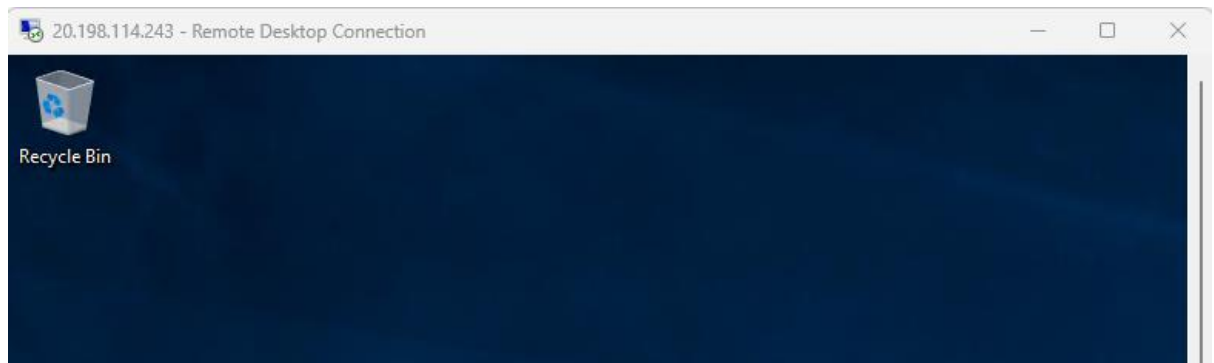
- Select the network interface for the **Srv-Work** virtual machine.
- Under **Settings**, select **DNS servers**.
- Under **DNS servers**, select **Custom**.
- Enter *209.244.0.3* in the **Add DNS server** text box, and *209.244.0.4* in the next text box.
- Select **Save**.
- Restart the **Srv-Work** virtual machine.

The screenshot shows the Azure portal interface for the 'srv-work283' network interface. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Settings (with sub-links for IP configurations, DNS servers, Network security group, Properties, and Locks), and Monitoring (with sub-links for Insights, Alerts, Metrics, and Diagnostic settings). The main content area is titled 'srv-work283 | DNS servers'. It features a search bar, 'Save' and 'Discard' buttons, and a warning message: 'Updating the DNS servers for this network interface may restart the virtual machine to which it's attached, and if applicable, any other virtual machines in the same availability set.' Below this, the 'DNS servers' section has radio buttons for 'Inherit from virtual network' and 'Custom' (selected). The 'DNS server' list shows two entries: '209.244.0.3' and '209.244.0.4', each with a delete icon. An 'Add DNS server' button is at the bottom. The 'Applied DNS servers' section includes an information icon, a descriptive text: 'For virtual machines in an availability set, the list of applied DNS servers is the union of all DNS servers from all network interfaces that are a part of the availability set.', and a table with the header 'Applied DNS servers' and one row containing 'No results'.

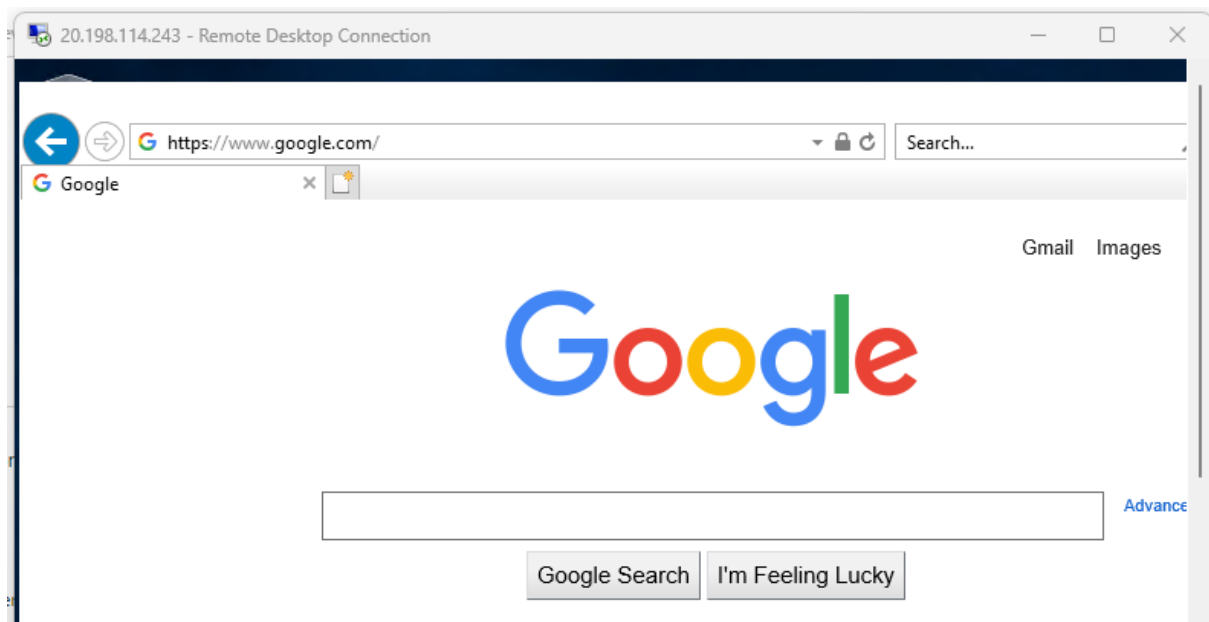
Test the firewall

Now, test the firewall to confirm that it works as expected.

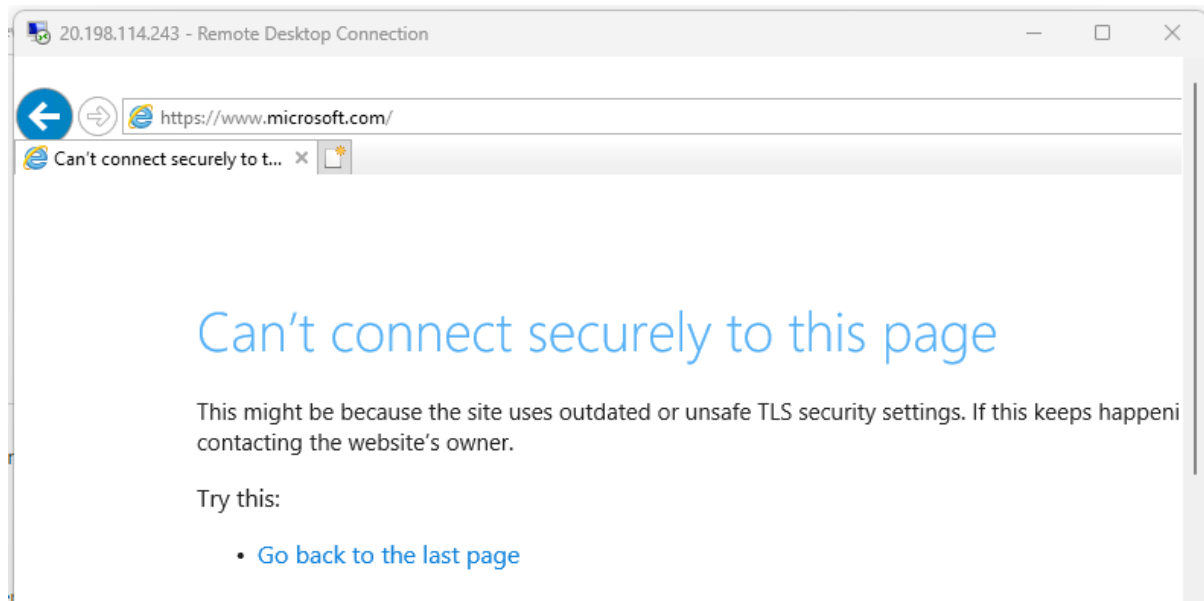
- Connect a remote desktop to firewall public IP address(20.198.114.243) and sign in to the Srv-Work virtual machine.



- Open Internet Explorer and browse to <https://www.google.com>.
- Select OK > Close on the Internet Explorer security alerts.
- You should see the Google home page.



- Browse to <https://www.microsoft.com>.
- You should be blocked by the firewall.
-



So now you've verified that the firewall rules are working:

- You can browse to the one allowed FQDN, but not to any others.
- You can resolve DNS names using the configured external DNS server