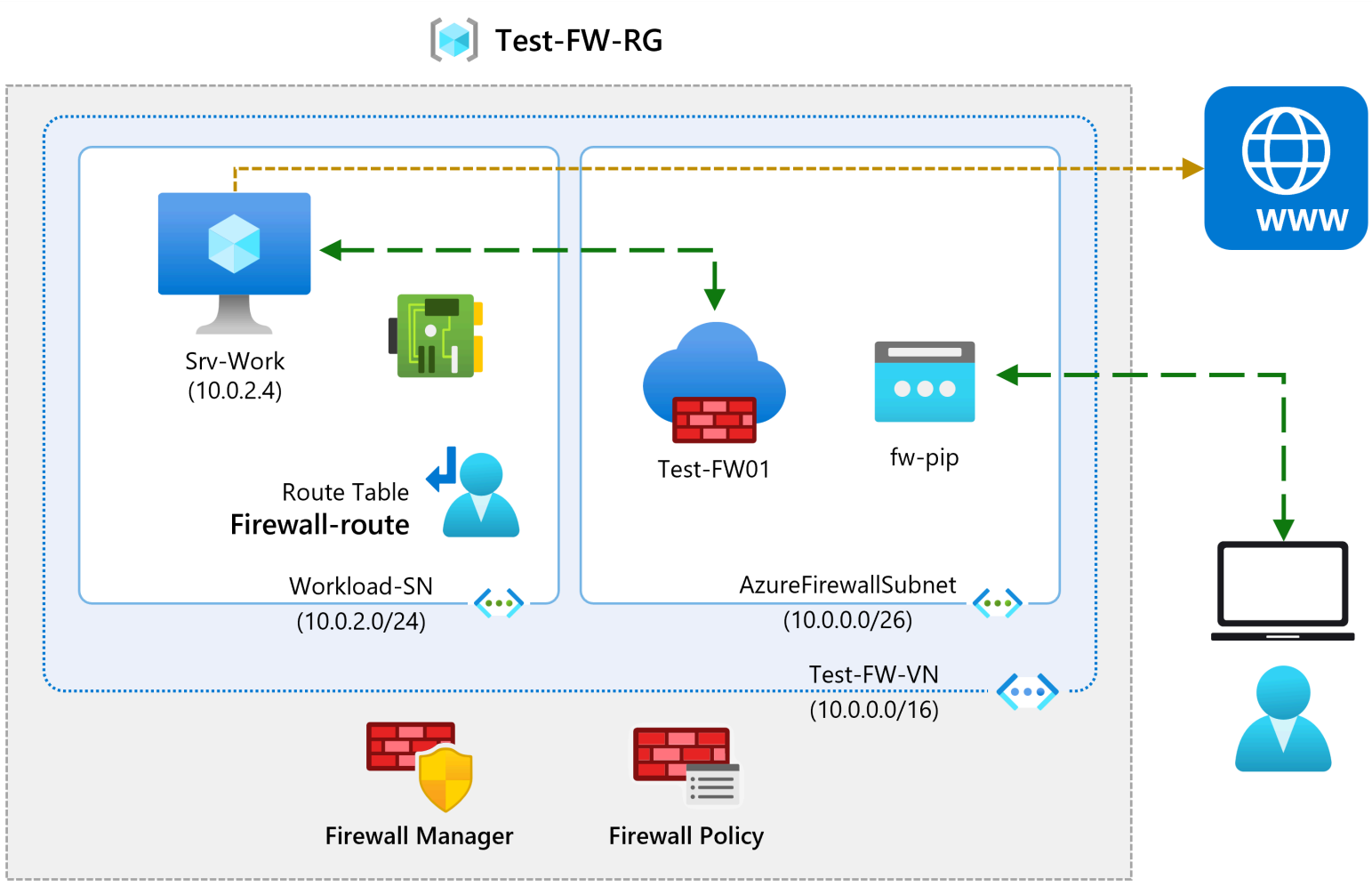
M06-Unit 7 Deploy and configure Azure Firewall using the Azure portal

Exercise scenario

Being part of the Network Security team at Contoso, your next task is to create firewall rules to allow/deny access to certain websites. The following steps walk you through creating a resource group, a virtual network and subnets, and a virtual machine as environment preparation tasks, and then deploying a firewall and firewall policy, configuring default routes and application, network and DNAT rules, and finally testing the firewall.



In this exercise, you will:

- Task 1: Create a resource group
- Task 2: Create a virtual network and subnets
- Task 3: Create a virtual machine
- Task 4: Deploy the firewall and firewall policy
- Task 5: Create a default route
- Task 6: Configure an application rule
- Task 7: Configure a network rule
- Task 8: Configure a Destination NAT (DNAT) rule
- Task 9: Change the primary and secondary DNS address for the server's network interface
- Task 10: Test the firewall

> **Note**: An **interactive lab simulation** is available that allows you to click through this lab at your own pace. You may find slight differences between the interactive simulation and the hosted lab, but the core concepts and ideas being demonstrated are the same.

Estimated time: 60 minutes

Task 1: Create a resource group

In this task, you will create a new resource group.

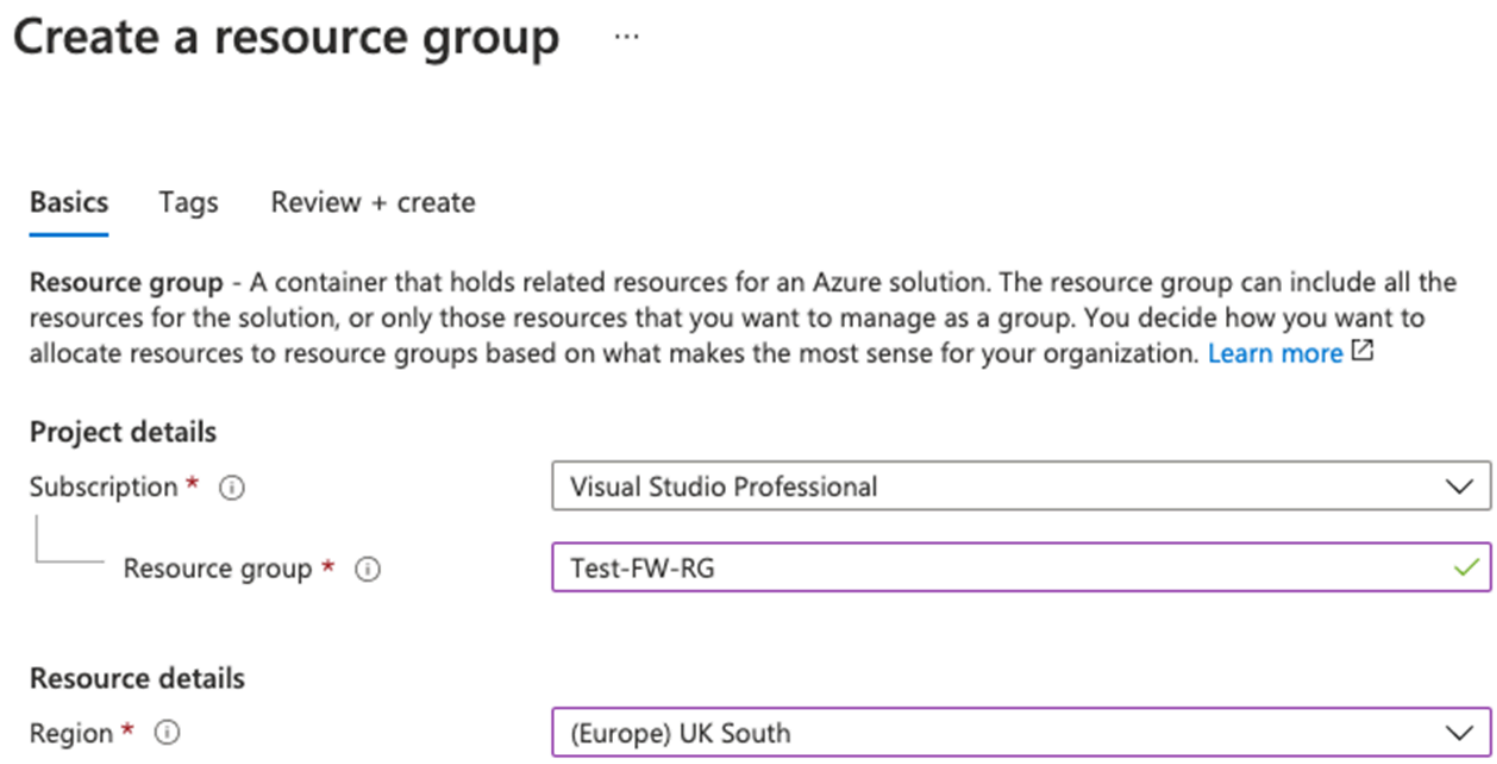
1. Log in to your Azure account.

2. On the Azure portal home page, select **Resource groups**.

3. Select **Create**.

4. On the **Basics** tab, in **Resource group**, enter **Test-FW-RG**.

5. On the **Region**, select your region from the list.



6. Select **Review + create**.

7. Select **Create**.

Task 2: Create a virtual network and subnets

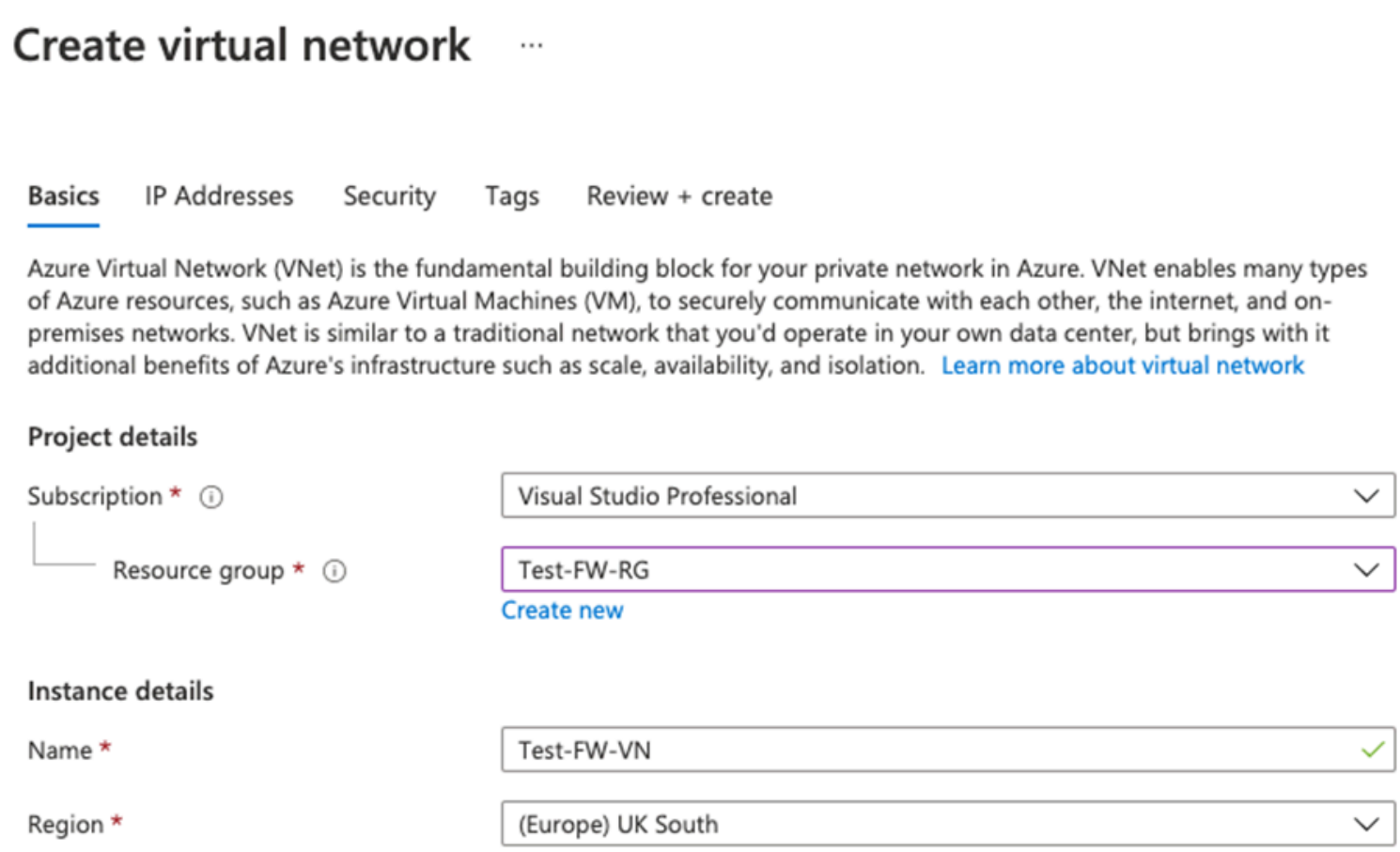
In this task, you will create a single virtual network with two subnets.

1. On the Azure portal home page, in the search box, enter **virtual network** and select **Virtual Network** when it appears.

2. Select **Create**.

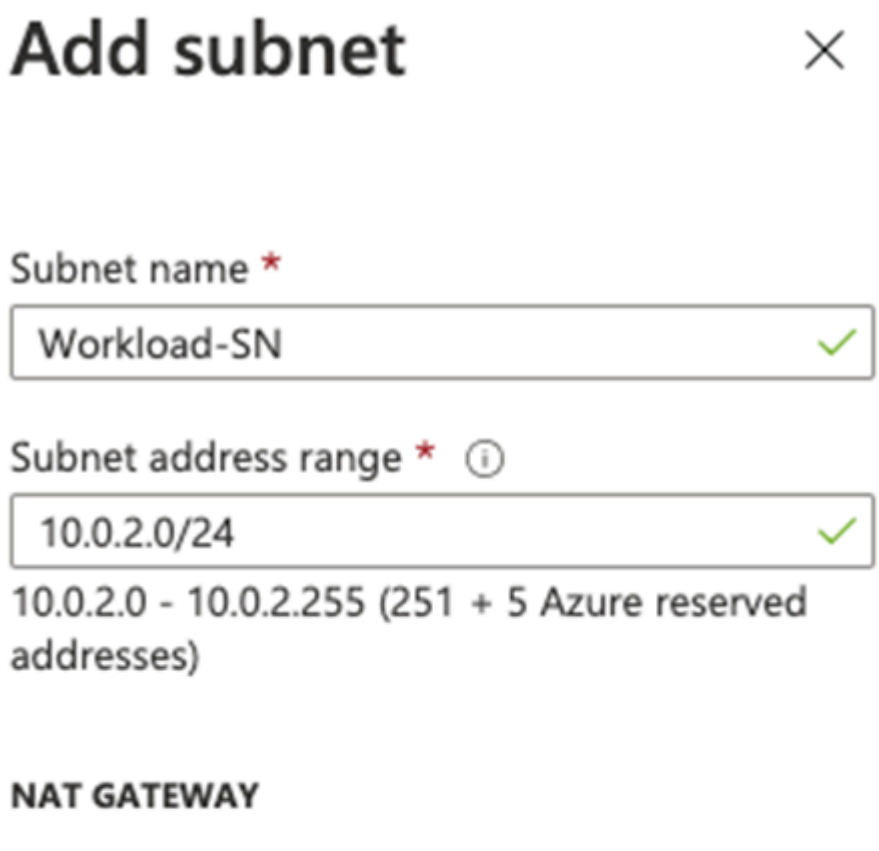
3. Select the **Test-FW-RG** resource group you created previously.

4. In the **Name** box, enter **Test-FW-VN**.



5. Select **Next: IP Addresses**. Enter IPv4 address space 10.0.0.0/16 if not already there by default.

6. Under **Subnet name**, select the word **default**.
7. In the **Edit subnet** dialog box, change the name to **AzureFirewallSubnet**.
8. Change the **Subnet address range** to **10.0.1.0/26**.
9. Select **Save**.
10. Select **Add subnet**, to create another subnet, which will host the workload server that you will create shortly.



11. In the **Edit subnet** dialog box, change the name to **Workload-SN**.
12. Change the **Subnet address range** to **10.0.2.0/24**.
13. Select **Add**.
14. Select **Review + create**.
15. Select **Create**.

Task 3: Create a virtual machine

In this task, you will create the workload virtual machine and place it in the Workload-SN subnet created previously.

1. In the Azure portal, select the Cloud Shell icon (top right). If necessary, configure the shell.
   - Select **PowerShell**.
   - Select **No Storage Account required** and your **Subscription**, then select **Apply**.
   - Wait for the terminal to create and a prompt to be displayed.
2. In the toolbar of the Cloud Shell pane, select the **Manage files** icon, in the drop-down menu, select **Upload** and upload the following files **firewall.json** and **firewall.parameters.json** into the Cloud Shell home directory one by one from the source folder **F:\Allfiles\Exercises\M06**.
3. Deploy the following ARM templates to create the VM needed for this exercise:

   > **Note**: You will be prompted to provide an Admin password.

   Code Copy

   ```
   $RGName = "Test-FW-RG"

   New-AzResourceGroupDeployment -ResourceGroupName $RGName -TemplateFile firewall.json -
   TemplateParameterFile firewall.parameters.json
   ```

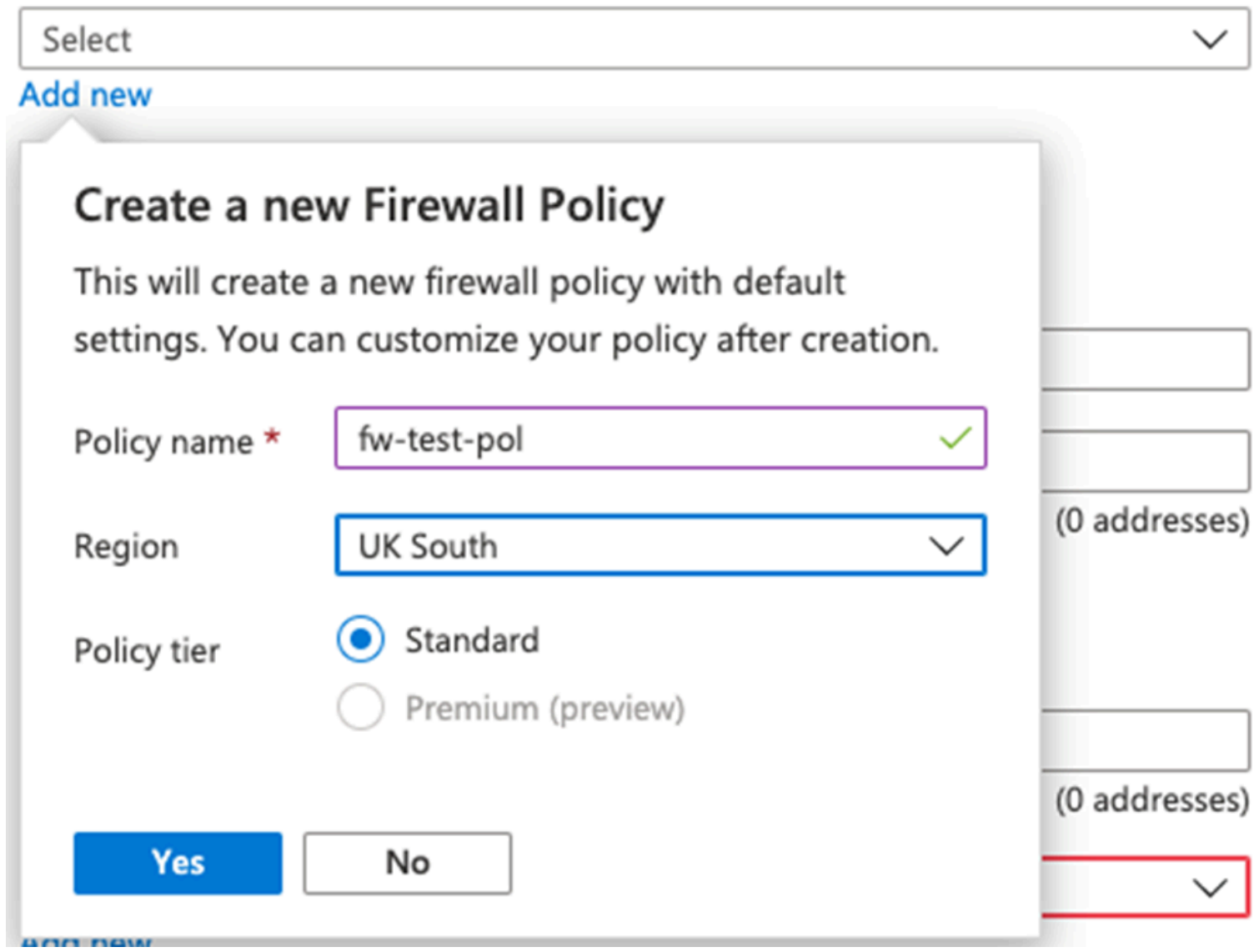
4. When the deployment is complete, go to the Azure portal home page, and then select **Virtual Machines**.
5. Verify that the virtual machine has been created.
6. On the **Overview** page of **Srv-Work**, on the right of the page under **Networking**, take a note of the **Private IP address** for this VM (e.g., **10.0.2.4**).

Task 4: Deploy the firewall and firewall policy

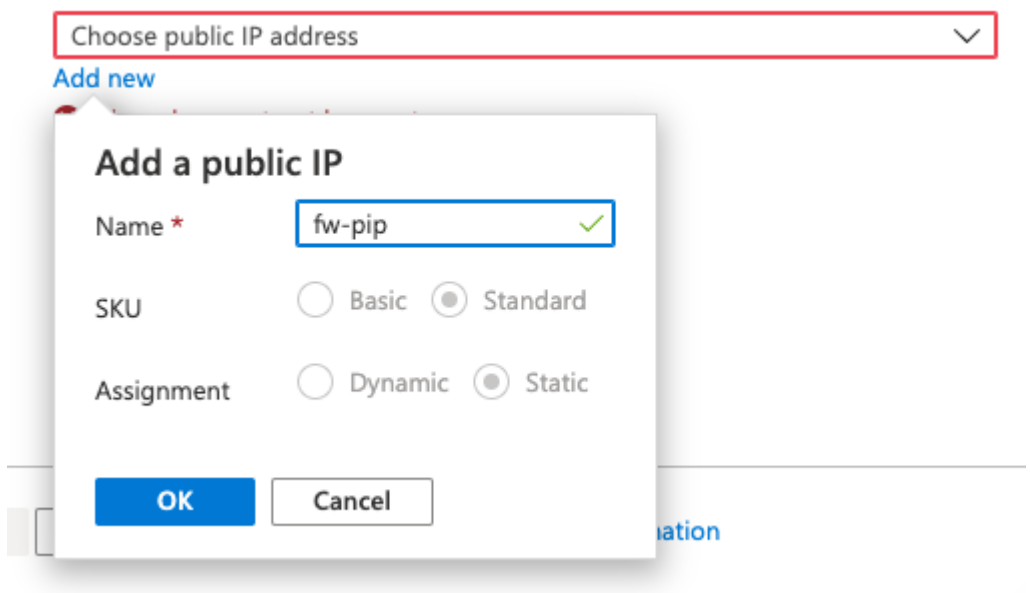
In this task, you will deploy the firewall into the virtual network with a firewall policy configured.

1. On the Azure portal home page, select **Create a resource**, then in the search box, enter **firewall** and select **Firewall** when it appears.
2. On the **Firewall** page, select **Create**.
3. On the **Basics** tab, create a firewall using the information in the table below.

Setting	Value
Subscription	Select your subscription
Resource group	**Test-FW-RG**
Firewall name	**Test-FW01**
Region	Your region
Firewall SKU	**Standard**
Firewall management	**Use a Firewall Policy to manage this firewall**
Firewall policy	Select **Add new** Name: **fw-test-pol** Region: **your region**

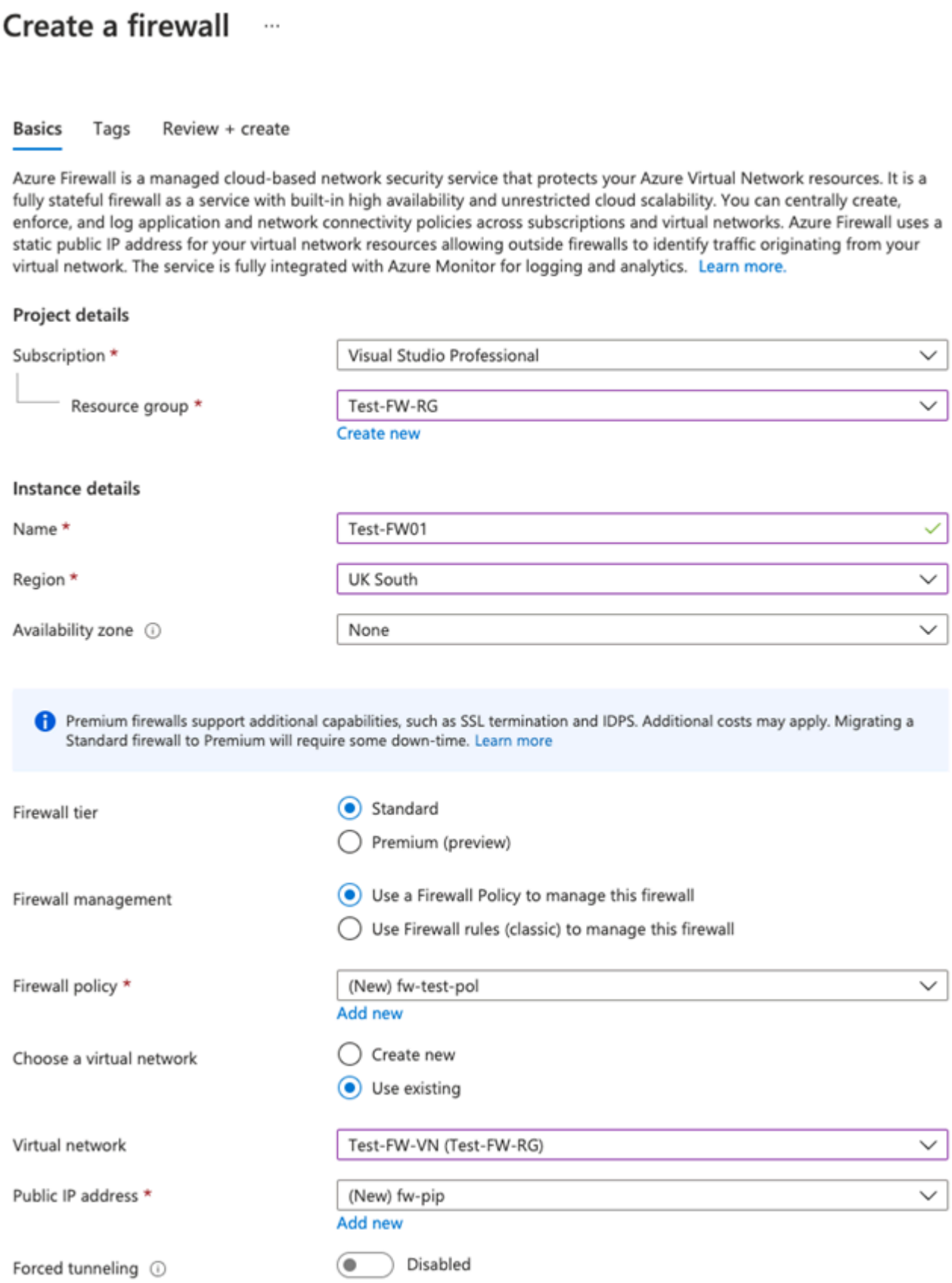


Choose a virtual network	**Use existing**
Virtual network	**Test-FW-VN**
Public IP address	Select **Add new** Name: **fw-pip**



4. We are not using the Firewall Manager so uncheck the box for **Enable Firewall Management NIC**.

5. Review your settings.



6. Proceed to **Review + create** and then **Create**.

7. Wait for the firewall deployment to complete.

8. When deployment of the firewall is completed, select **Go to resource**.

9. On the **Overview** page of **Test-FW01**, on the right of the page, take a note of the **Firewall private IP** for this firewall (e.g., **10.0.1.4**).

10. In the menu on the left, under **Settings**, select **Public IP configuration**.

11. Take a note of the address under **IP Address** for the **fw-pip** public IP configuration (e.g., **20.90.136.51**).

Task 5: Create a default route

In this task, on the Workload-SN subnet, you will configure the outbound default route to go through the firewall.

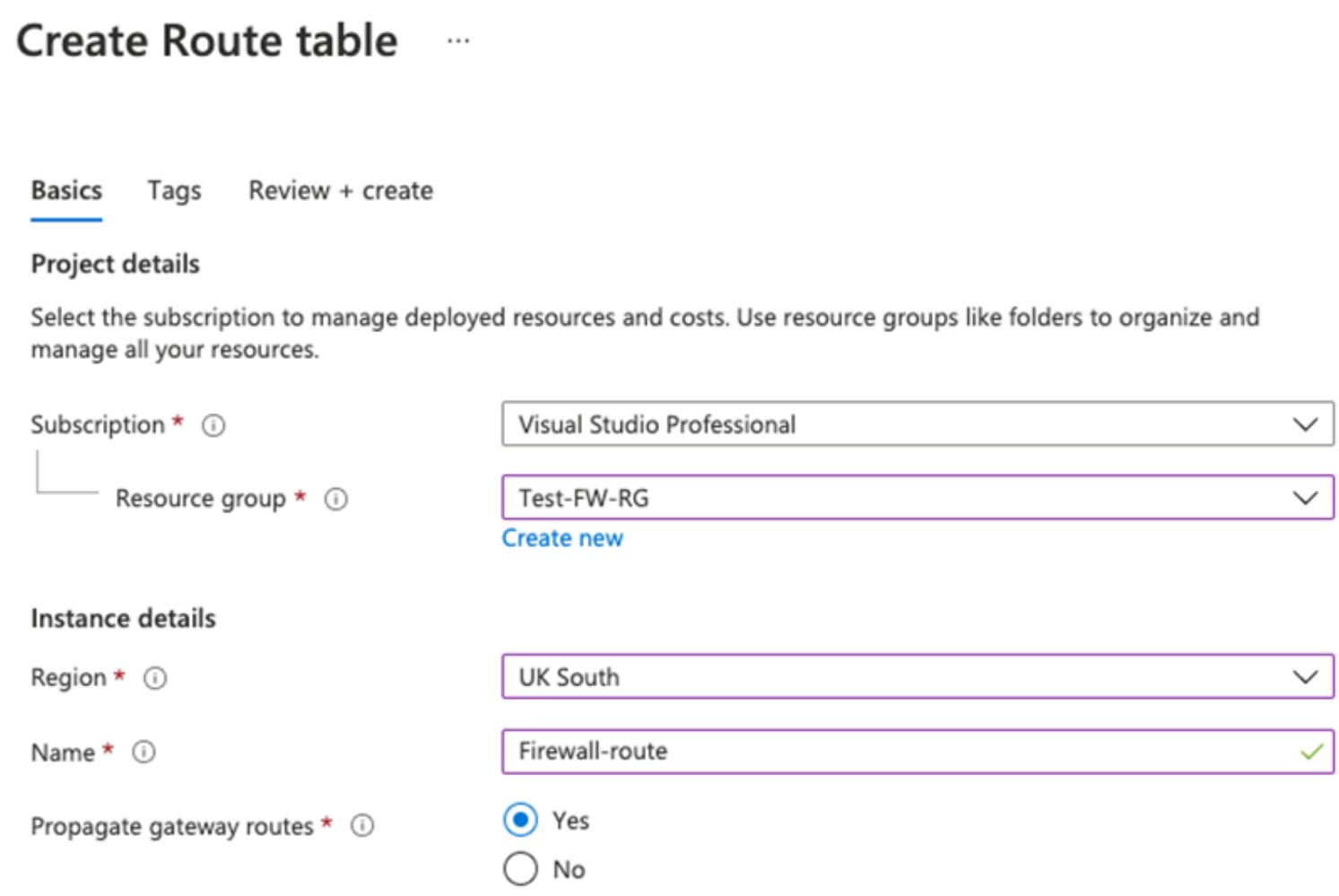
1. On the Azure portal home page, select **Create a resource**, then in the search box, enter **route** and select **Route table** when it appears.

2. On the **Route table** page, select **Create**.

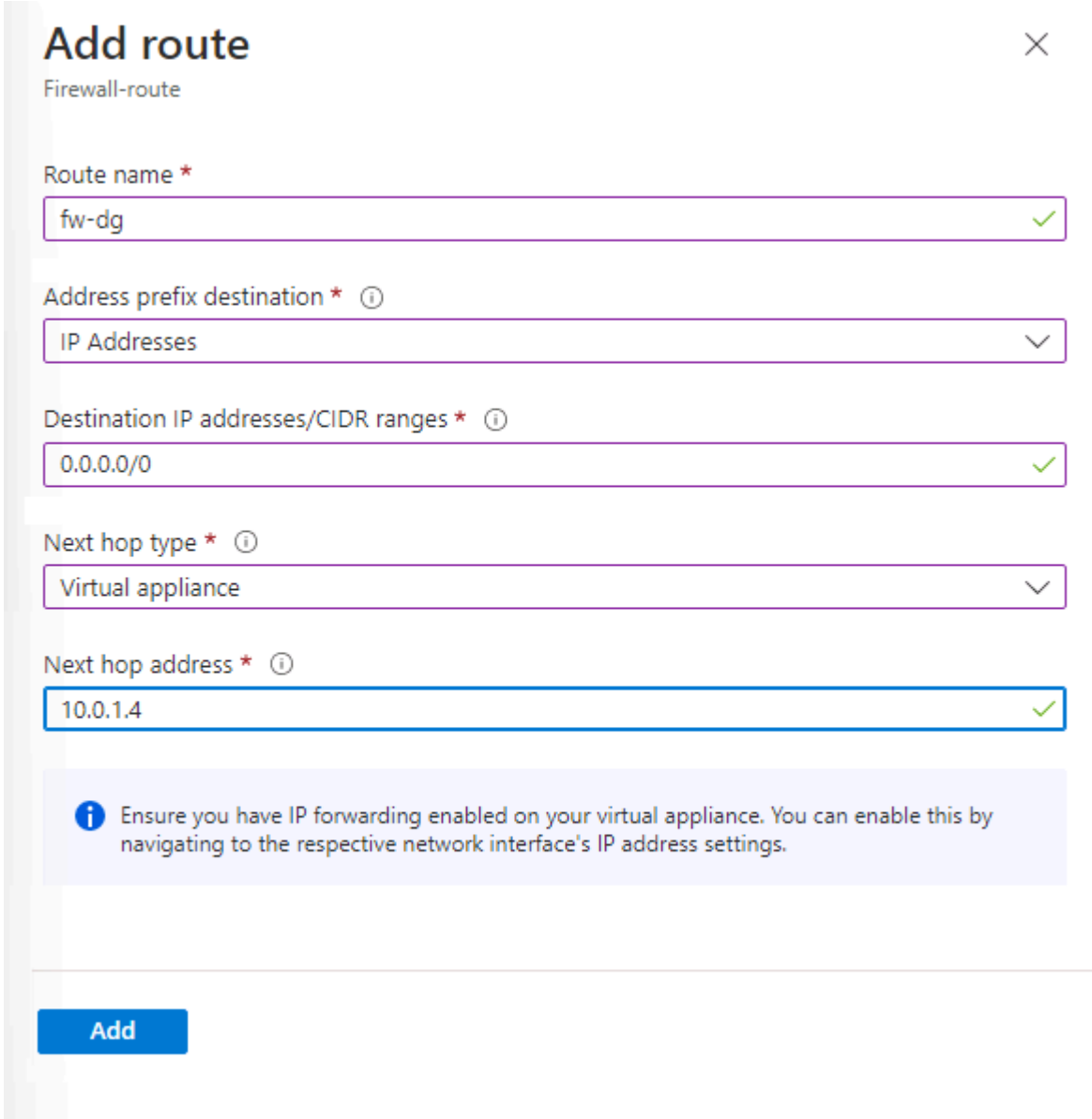
3. On the **Basics** tab, create a new route table using the information in the table below.

Setting	Value
Subscription	Select your subscription
Resource group	**Test-FW-RG**
Region	Your region
Name	**Firewall-route**
Propagate gateway routes	**Yes**

4. Select **Review + create**.
5. Select **Create**.



6. After deployment completes, select **Go to resource**.
7. On the **Firewall-route** page, under **Settings**, select **Subnets** and then select **Associate**.
8. On **Virtual network**, select **Test-FW-VN**.
9. On **Subnet**, select **Workload-SN**. Make sure that you select only the Workload-SN subnet for this route, otherwise your firewall won't work correctly.
10. Select **OK**.
11. Under **Settings**, select **Routes** and then select **Add**.
12. On **Route name**, enter **fw-dg**.
13. On **Address prefix destination**, enter **0.0.0.0/0**.
14. On **Next hop type**, select **Virtual appliance**.
15. On **Next hop address**, enter the private IP address for the firewall that you noted previously (e.g., **10.0.1.4**)
16. Select **Add**.

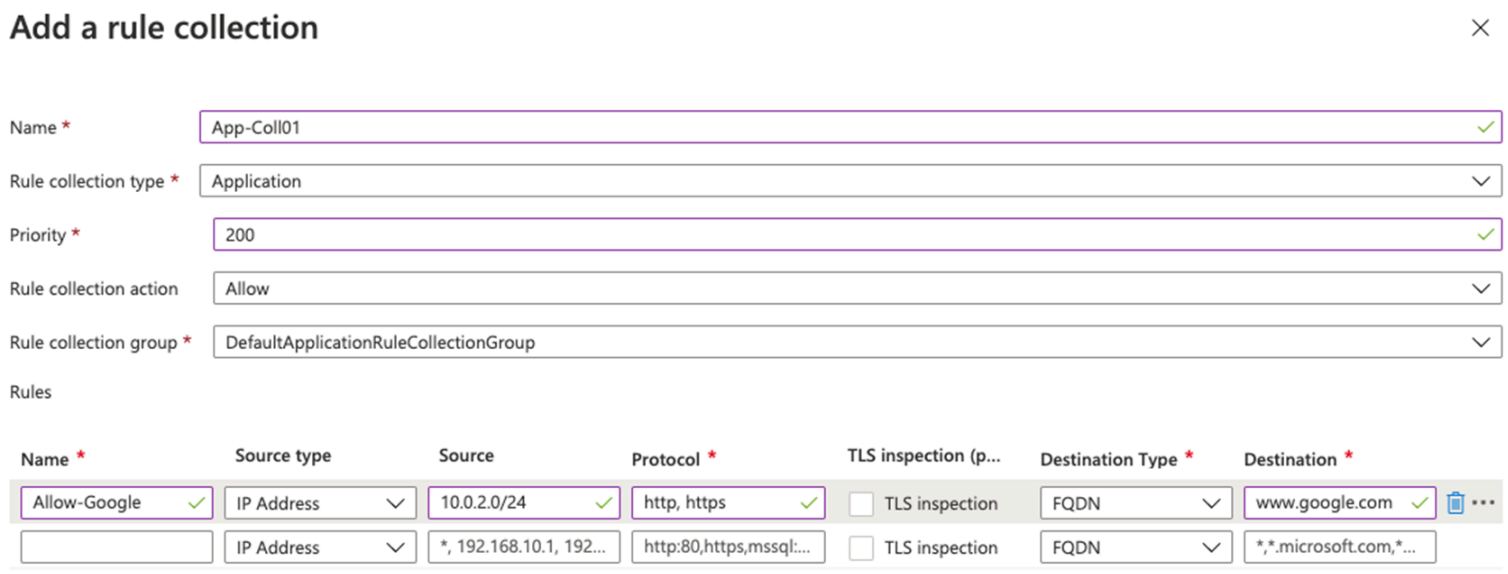


Task 6: Configure an application rule

In this task, you will add an application rule that allows outbound access to .

1. On the Azure portal home page, select **All resources**.
2. In the list of resources, select your firewall policy, **fw-test-pol**.
3. Under **Settings**, select **Application Rules**.
4. Select **Add a rule collection**.
5. On the **Add a rule collection** page, create a new application rule using the information in the table below.

Setting	Value
Name	**App-Coll01**
Rule collection type	**Application**
Priority	**200**
Rule collection action	**Allow**
Rule collection group	**DefaultApplicationRuleCollectionGroup**
Rules Section	
Name	**Allow-Google**
Source type	**IP Address**
Source	**10.0.2.0/24**
Protocol	**http,https**
Destination type	**FQDN**
Destination	****



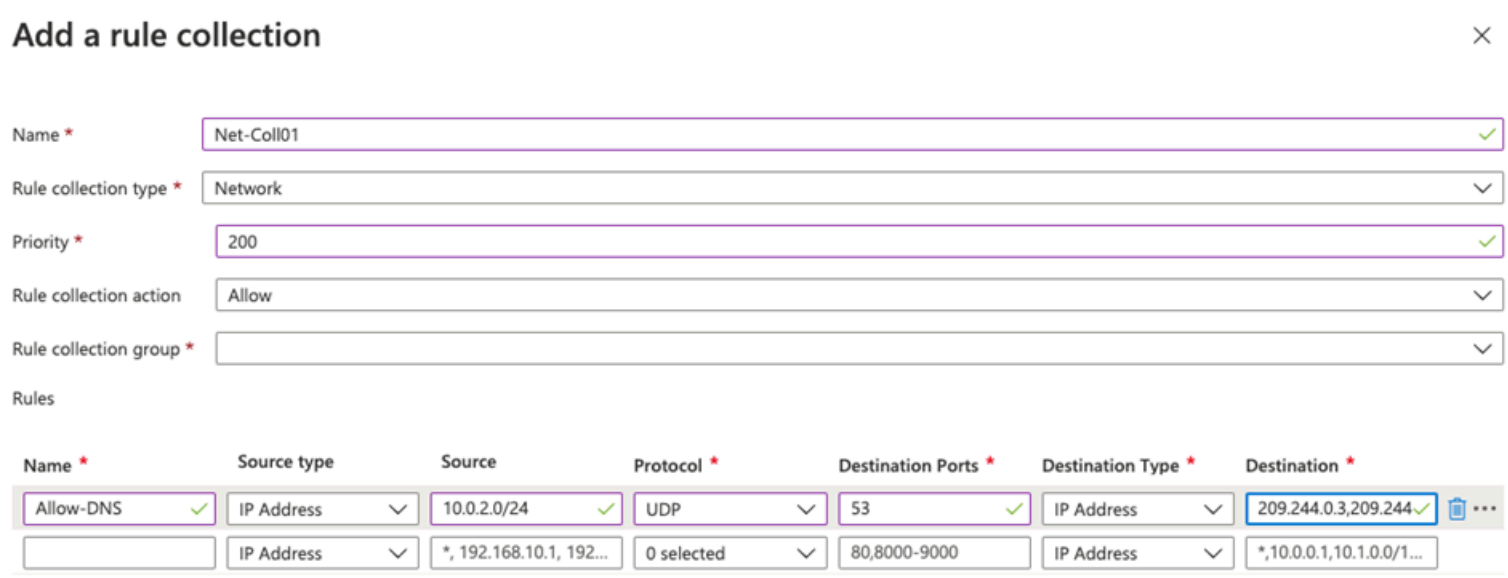
6. Select **Add**.

Task 7: Configure a network rule

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

1. On the **fw-test-pol** page, under **Settings**, select **Network Rules**.
2. Select **Add a rule collection**.
3. On the **Add a rule collection** page, create a new network rule using the information in the table below.

Setting	Value
Name	**Net-Coll01**
Rule collection type	**Network**
Priority	**200**
Rule collection action	**Allow**
Rule collection group	**DefaultNetworkRuleCollectionGroup**
Rules Section	
Name	**Allow-DNS**
Source type	**IP Address**
Source	**10.0.2.0/24**
Protocol	**UDP**
Destination Ports	**53**
Destination Type	**IP Address**
Destination	**209.244.0.3, 209.244.0.4** These are public DNS servers operated by Century Link



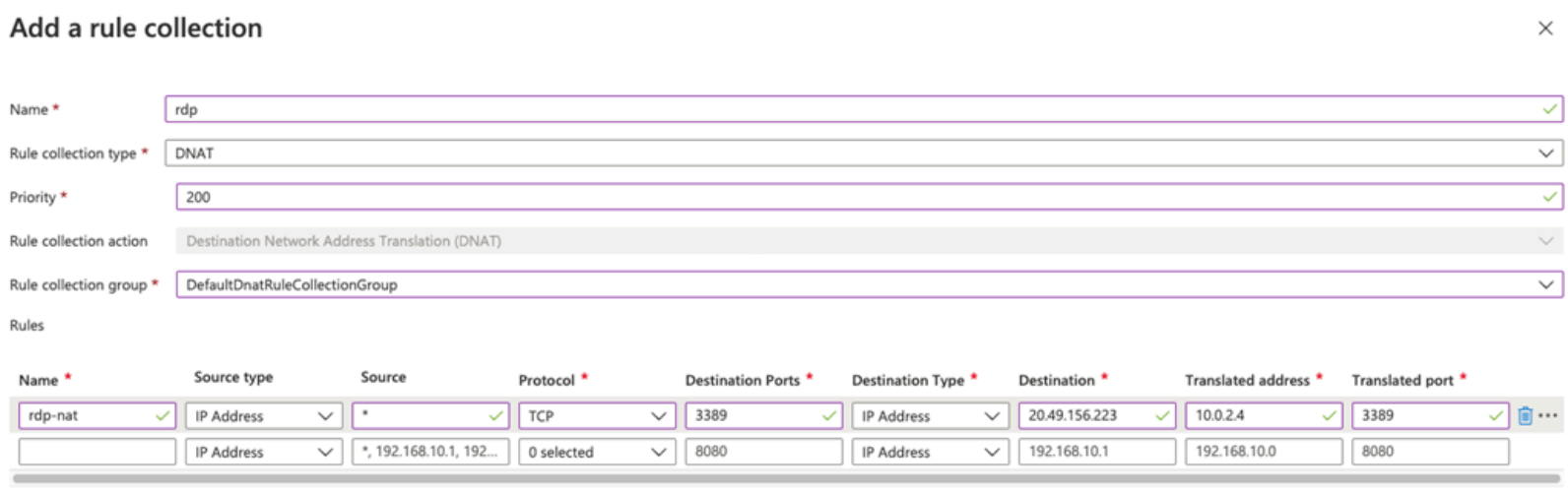
4. Select **Add**.

Task 8: Configure a Destination NAT (DNAT) rule

In this task, you will add a DNAT rule that allows you to connect a remote desktop to the Srv-Work virtual machine through the firewall.

1. On the **fw-test-pol** page, under **Settings**, select **DNAT Rules**.
2. Select **Add a rule collection**.
3. On the **Add a rule collection** page, create a new DNAT rule using the information in the table below.

Setting	Value
Name	**rdp**
Rule collection type	**DNAT**
Priority	**200**
Rule collection group	**DefaultDnatRuleCollectionGroup**
Rules Section	
Name	**rdp-nat**
Source type	**IP Address**
Source	*
Protocol	**TCP**
Destination Ports	**3389**
Destination Type	**IP Address**
Destination	Enter the firewall public IP address from **fw-pip** that you noted earlier. **e.g. - 20.90.136.51**
Translated address	Enter the private IP address from **Srv-Work** that you noted earlier. **e.g. - 10.0.2.4**
Translated port	**3389**

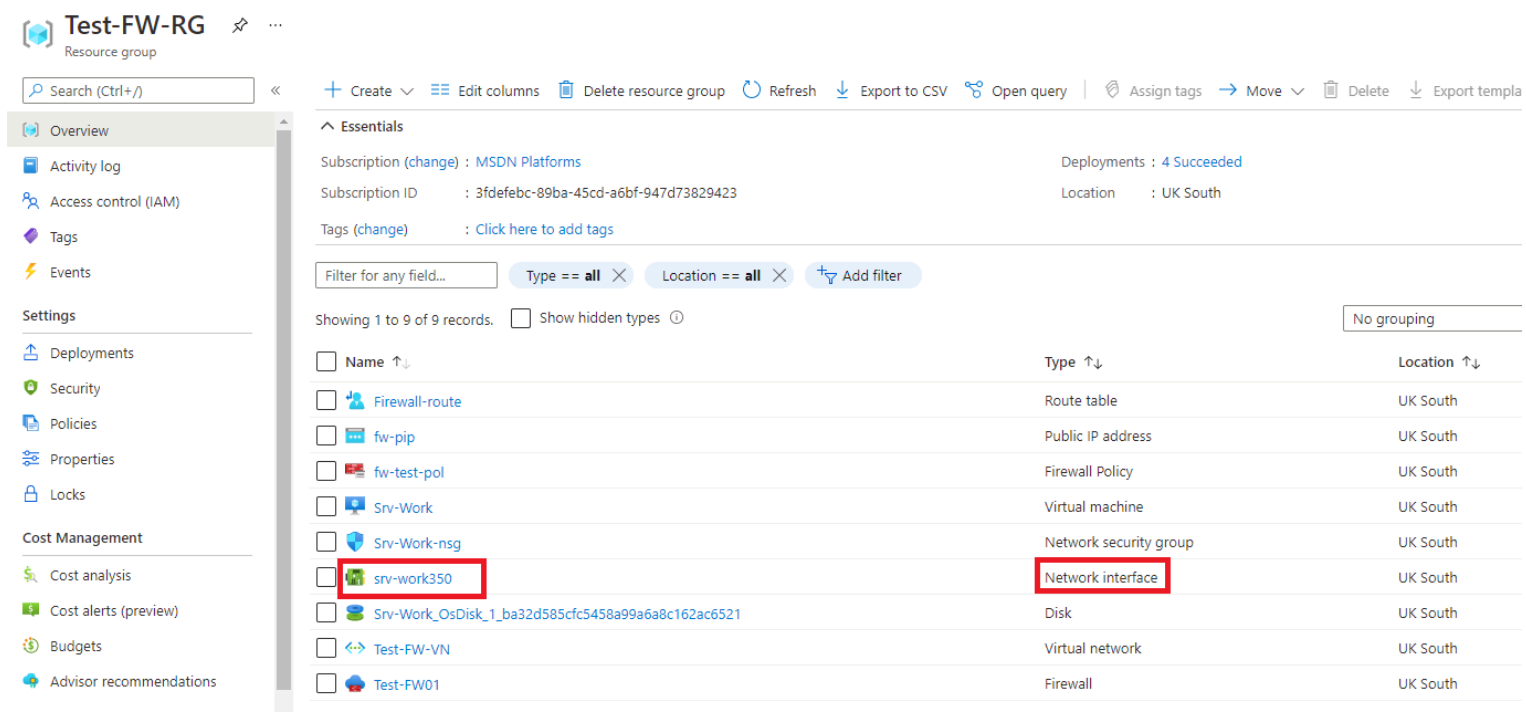


1. Select **Add**.

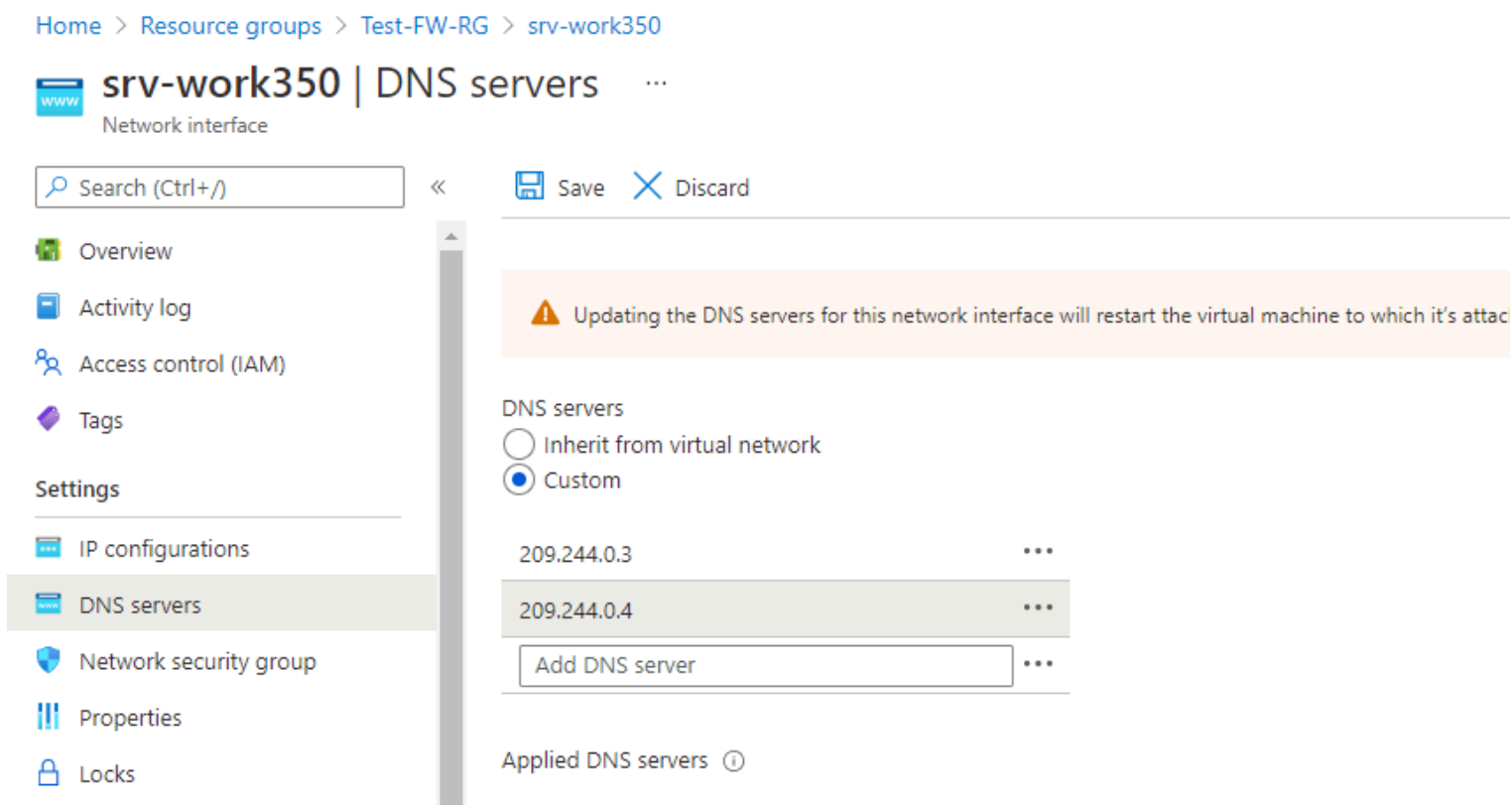
Task 9: Change the primary and secondary DNS address for the server's network interface

For testing purposes in this exercise, in this task, you will configure the Srv-Work server's primary and secondary DNS addresses. However, this is not a general Azure Firewall requirement.

1. On the Azure portal home page, select **Resource groups**.
2. In the list of resource groups, select your resource group, **Test-FW-RG**.
3. In the list of resources in this resource group, select the network interface for the **Srv-Work** virtual machine (e.g., **srv-work350**).



4. Under **Settings**, select **DNS servers**.
5. Under **DNS servers**, select **Custom**.
6. enter **209.244.0.3** in the **Add DNS server** text box, and **209.244.0.4** in the next text box.
7. Select **Save**.

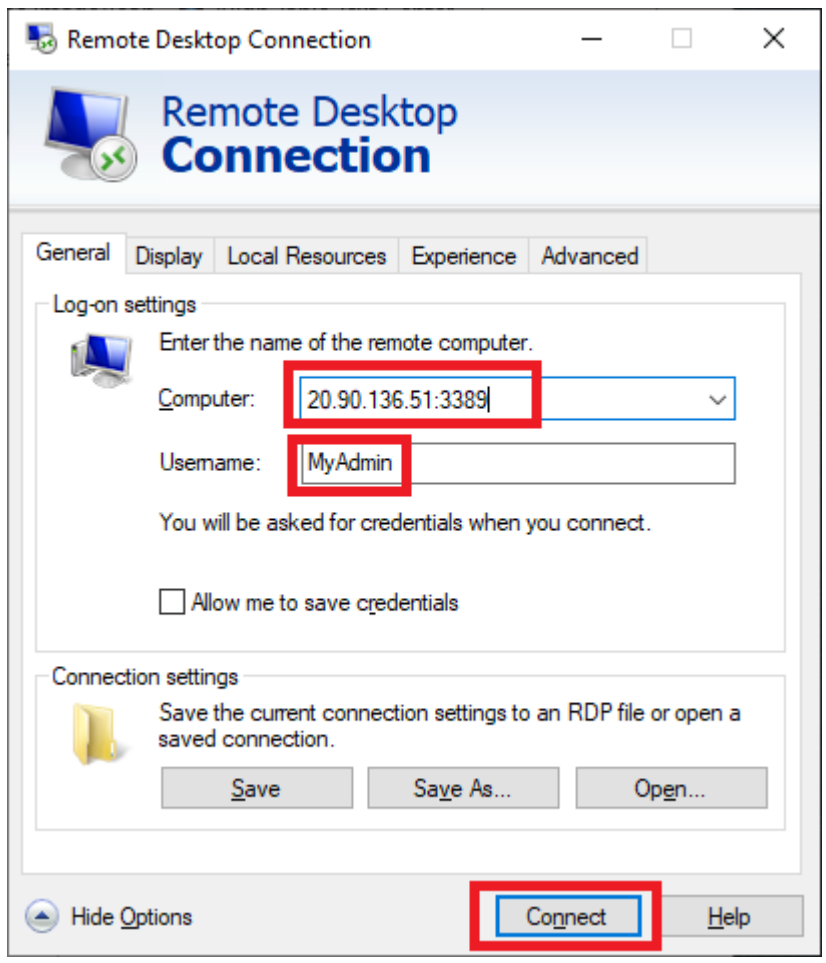


8. Restart the **Srv-Work** virtual machine.

Task 10: Test the firewall

In this final task, you will test the firewall to verify that the rules are configured correctly and working as expected. This configuration will enable you to connect a remote desktop connection to the Srv-Work virtual machine through the firewall, via the firewall's public IP address.

1. Open **Remote Desktop Connection** on your PC.
2. On the **Computer** box, enter the firewall's public IP address (e.g., **20.90.136.51**) followed by **:3389** (e.g., **20.90.136.51:3389**).
3. On the **Username** box, enter **TestUser**.
4. Select **Connect**.

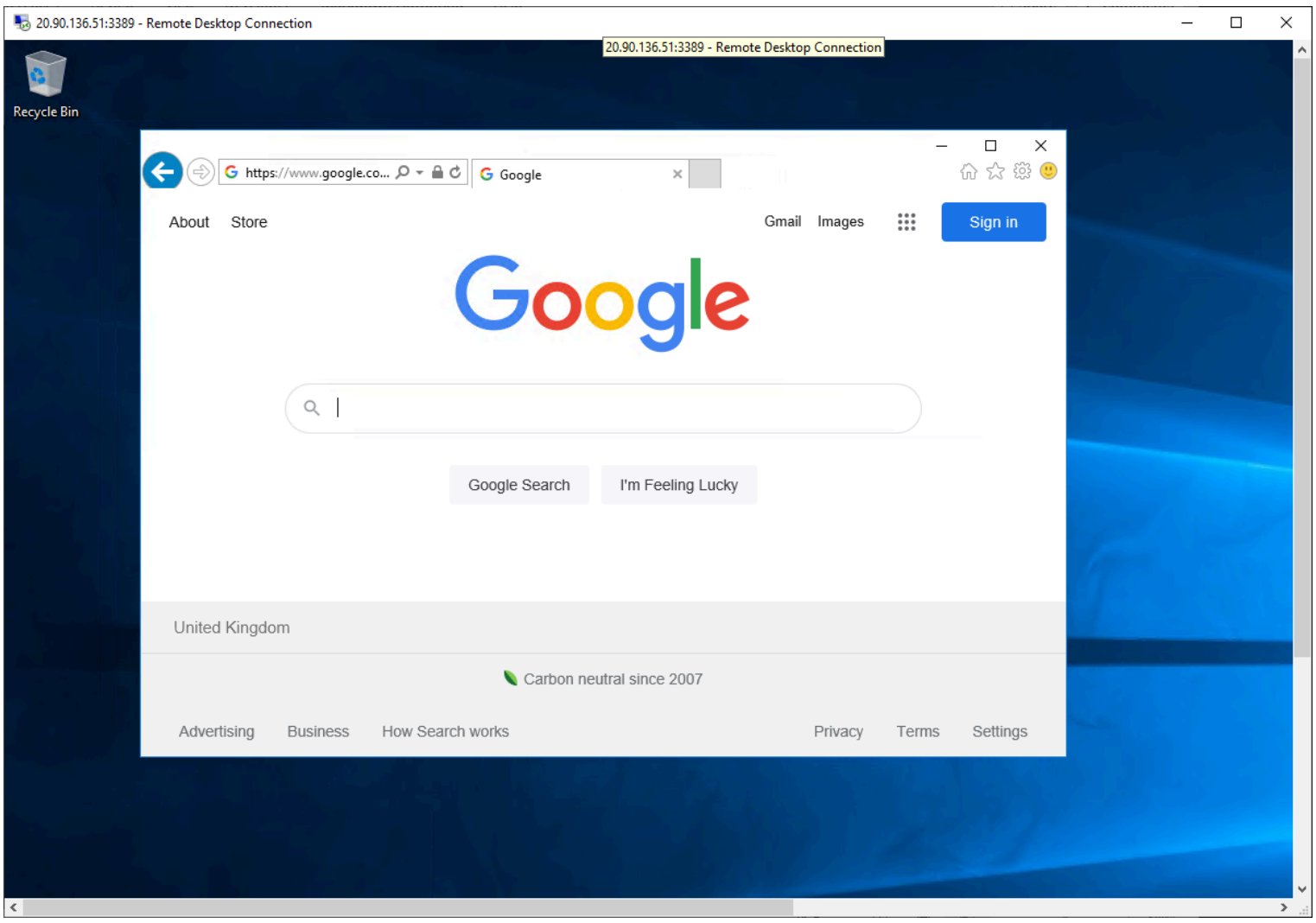


5. On the **Enter your credentials** dialog box, log into the **Srv-Work** server virtual machine, by using the password you provided during deployment.
6. Select **OK**.
7. Select **Yes** on the certificate message.
8. Open Internet Explorer and browse to **https://www.google.com**.

9. On the **Security Alert** dialog box, select **OK**.

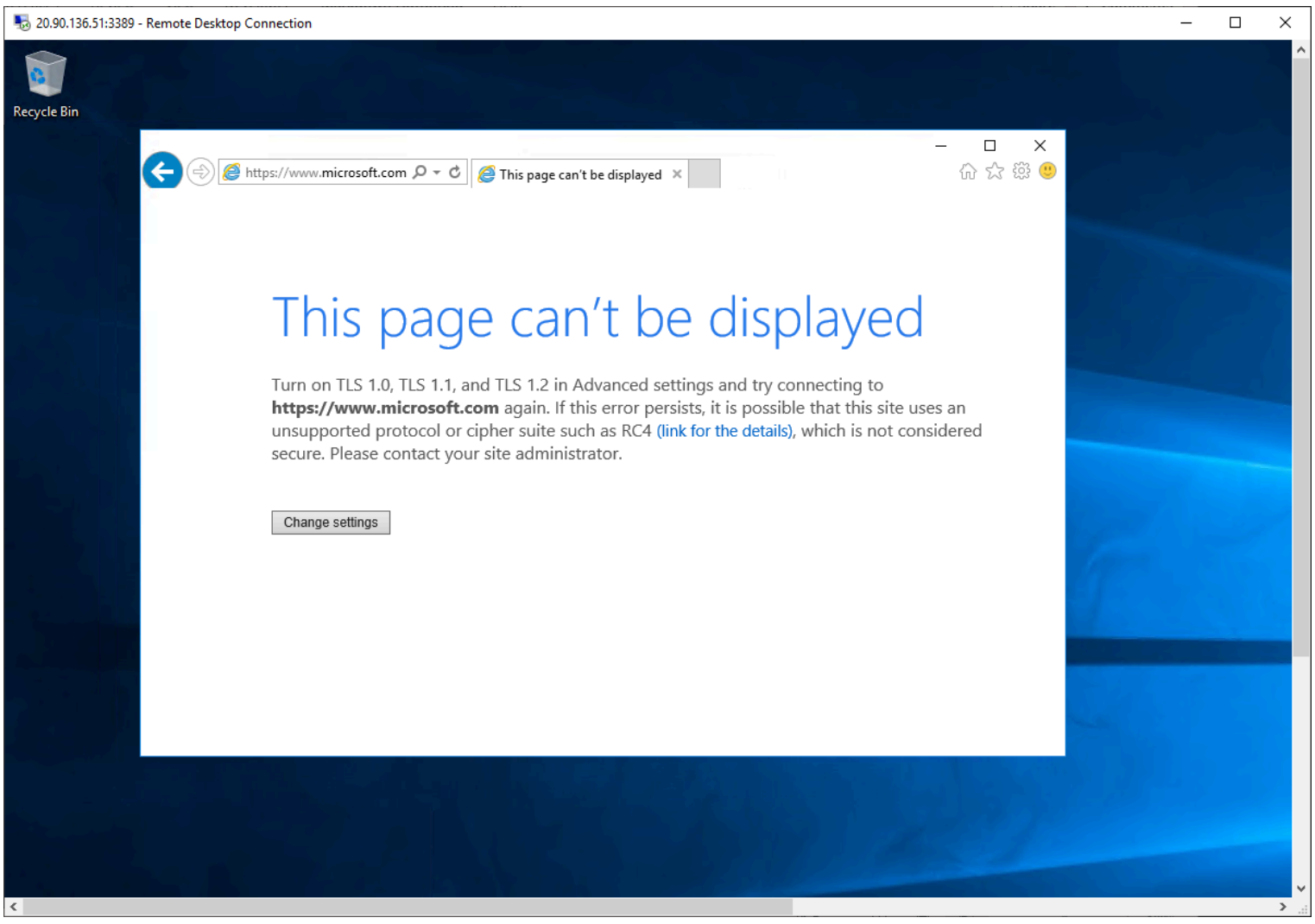
10. Select **Close** on the Internet Explorer security alerts that may pop-up.

11. You should see the Google home page.



12. Browse to **https://www.microsoft.com**.

13. You should be blocked by the firewall.



Clean up resources

> **Note**: Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not see unexpected charges.

1. On the Azure portal, open the **PowerShell** session within the **Cloud Shell** pane.

2. Delete all resource groups you created throughout the labs of this module by running the following command:

Code Copy

```
Remove-AzResourceGroup -Name 'Test-FW-RG' -Force -AsJob
```

> **Note**: The command executes asynchronously (as determined by the -AsJob parameter), so while you will be able to run another PowerShell command immediately afterwards within the same PowerShell session, it will take a few minutes before the resource groups are actually removed.

Extend your learning with Copilot

Copilot can assist you in learning how to use the Azure scripting tools. Copilot can also assist in areas not covered in the lab or where you need more information. Open an Edge browser and choose Copilot (top right) or navigate to *copilot.microsoft.com*. Take a few minutes to try these prompts.

- Provide three common usage scenarios for firewalls.
- Provide a table comparing the features of the Azure Firewall SKUs.
- Describe the three types of rules you can create for an Azure Firewall.

Learn more with self-paced training

- Introduction to Azure Firewall. In this module, you learn how Azure Firewall protects Azure virtual network resources including features, rules, and deployment options.
- Introduction to Azure Firewall Manager. In this module, you learn how Azure Firewall Manager provides central security policy and route management for cloud-based security perimeters.

Key takeaways

Congratulations on completing the lab. Here are the main takeaways for this lab.

- A firewall is a network security feature that sits between a trusted network and an untrusted network, such as the internet. The firewall's job is to analyze and then allow or deny network traffic.
- Azure Firewall is a cloud-based firewall service. In most configurations, Azure Firewall is provisioned inside a hub virtual network. Traffic to and from the spoke virtual networks and the on-premises network is directed to the firewall.
- Firewall rules evaulate the network traffic. Azure Firewall has three types of rules: Application, Network, and NAT.
- Azure Firewall is offered in three SKUs: Standard, Premium, and Basic.