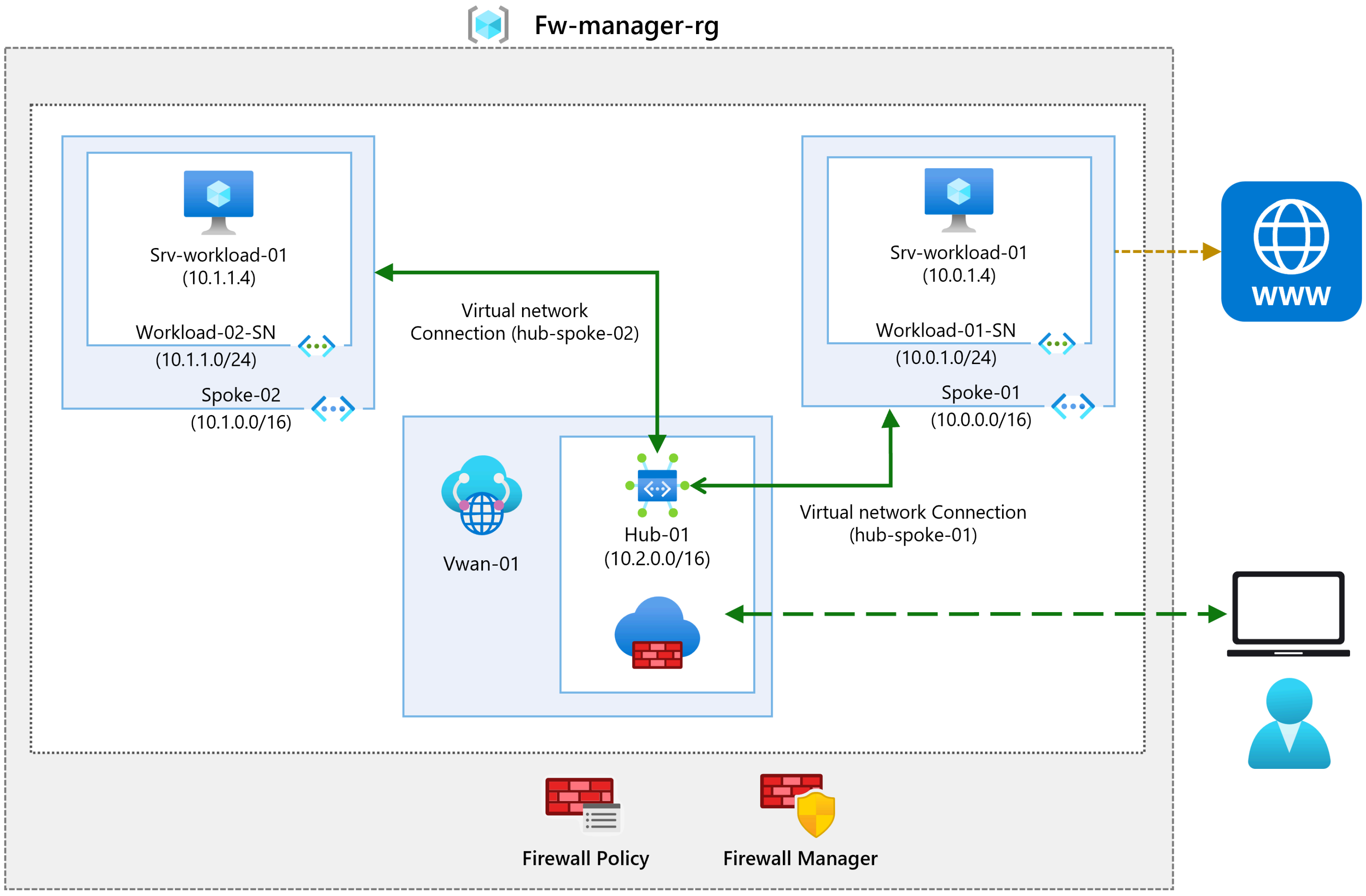
M06-Unit 9 Secure your virtual hub using Azure Firewall Manager

Exercise scenario

In this exercise, you will create the spoke virtual network and create a secured virtual hub, then you will connect the hub and spoke virtual networks and route traffic to your hub. Next you will deploy the workload servers, then create a firewall policy and secure your hub, and finally you will 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.

Create a hub and spoke architecture

In this part of the exercise, you will create the spoke virtual networks and subnets where you will place the workload servers. Then you will create the secured virtual hub and connect the hub and spoke virtual networks.

In this exercise, you will:

- Task 1: Create two spoke virtual networks and subnets
- Task 2: Create the secured virtual hub
- Task 3: Connect the hub and spoke virtual networks
- Task 4: Deploy the servers
- Task 5: Create a firewall policy and secure your hub
- Task 6: Associate the firewall policy
- Task 7: Route traffic to your hub
- Task 8: Test the application rule
- Task 9: Test the network rule
- Task 10: Clean up resources

Estimated time: 35 minutes

Task 1: Create two spoke virtual networks and subnets

In this task, you will create the two spoke virtual networks each containing a subnet that will host your workload servers.

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. In **Resource group**, select **Create new**, and enter **fw-manager-rg** as the name and select **OK**.
4. In **Name**, enter **Spoke-01**.
5. In **Region**, select your region.
6. Select **Next: IP Addresses**.
7. In **IPv4 address space**, enter **10.0.0.0/16**.
8. **Delete** any other address spaces listed here, such as **10.1.0.0/16**.
9. Under **Subnet name**, select the word **default**.
10. In the **Edit subnet** dialog box, change the name to **Workload-01-SN**.
11. Change the **Subnet address range** to **10.0.1.0/24**.
12. Select **Save**.
13. Select **Review + create**.
14. Select **Create**.

Repeat steps 1 to 14 above to create another similar virtual network and subnet but using the following information:

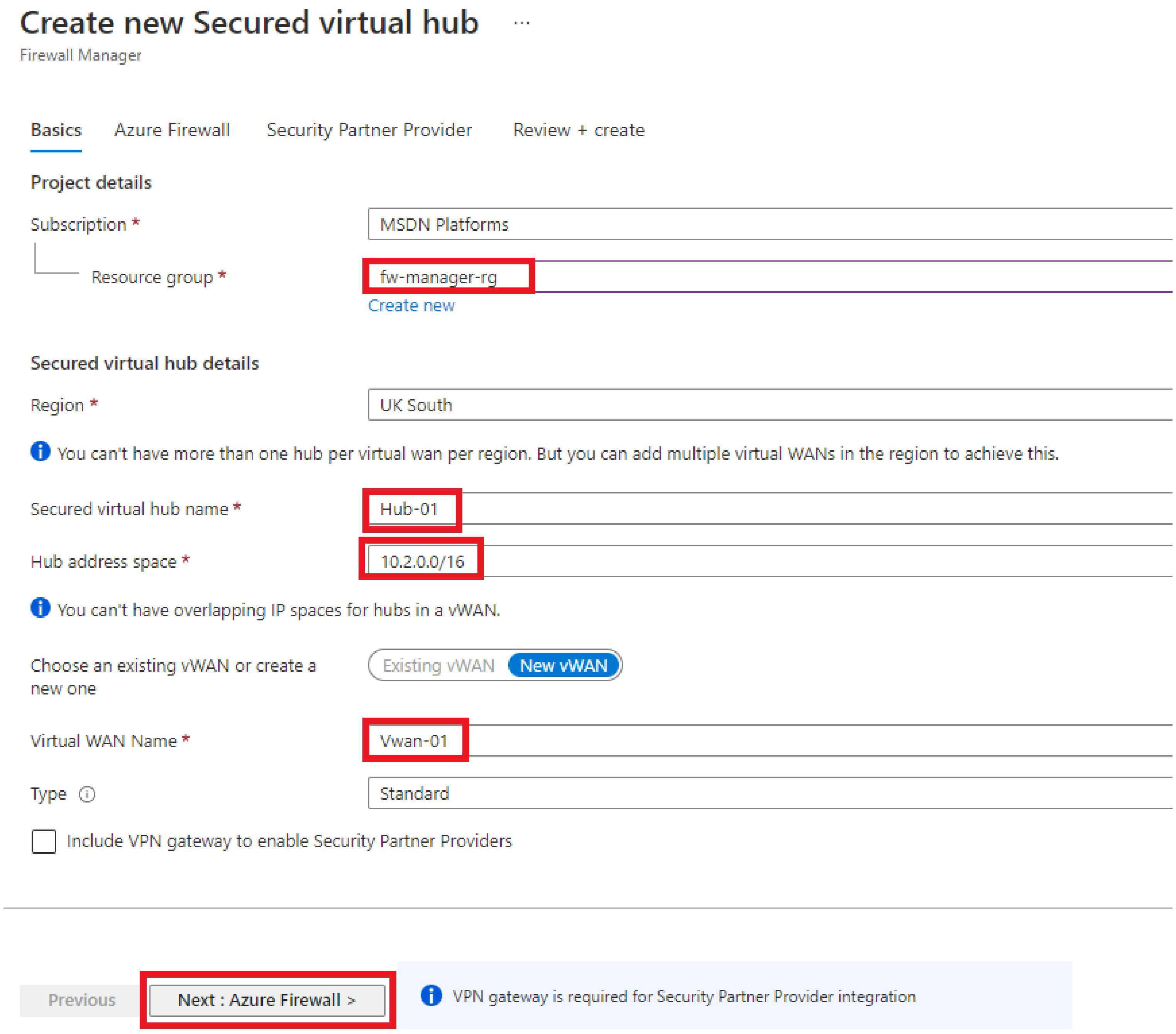
- Resource Group: **fw-manager-rg** (select existing)
- Name: **Spoke-02**
- Address space: **10.1.0.0/16** - (delete any other listed address spaces)
- Subnet name: **Workload-02-SN**
- Subnet address range: **10.1.1.0/24**

Task 2: Create the secured virtual hub

In this task you will create your secured virtual hub using Firewall Manager.

1. From the Azure portal home page, select **All services**.
2. In the search box, enter **firewall manager** and select **Firewall Manager** when it appears.
3. On the **Firewall Manager** page, from the Overview page, select **View secured virtual hubs**.
4. On the **Virtual hubs** page, select **Create new secured virtual hub**.
5. For **Resource group**, select **fw-manager-rg**.
6. For **Region**, select your region.
7. For the **Secured virtual hub name**, enter **Hub-01**.
8. For **Hub address space**, enter **10.2.0.0/16**.
9. Choose **New vWAN**.
10. In **Virtual WAN Name**, enter **Vwan-01**.

11. Select **Next: Azure Firewall**.



Create new Secured virtual hub

Firewall Manager

Project details

Subscription *: MSDN Platforms

Resource group *: fw-manager-rg

Secured virtual hub details

Region *: UK South

You can't have more than one hub per virtual wan per region. But you can add multiple virtual WANs in the region to achieve this.

Secured virtual hub name *: Hub-01

Hub address space *: 10.2.0.0/16

You can't have overlapping IP spaces for hubs in a vWAN.

Choose an existing vWAN or create a new one: Existing vWAN ● New vWAN

Virtual WAN Name *: Vwan-01

Type: Standard

□ Include VPN gateway to enable Security Partner Providers

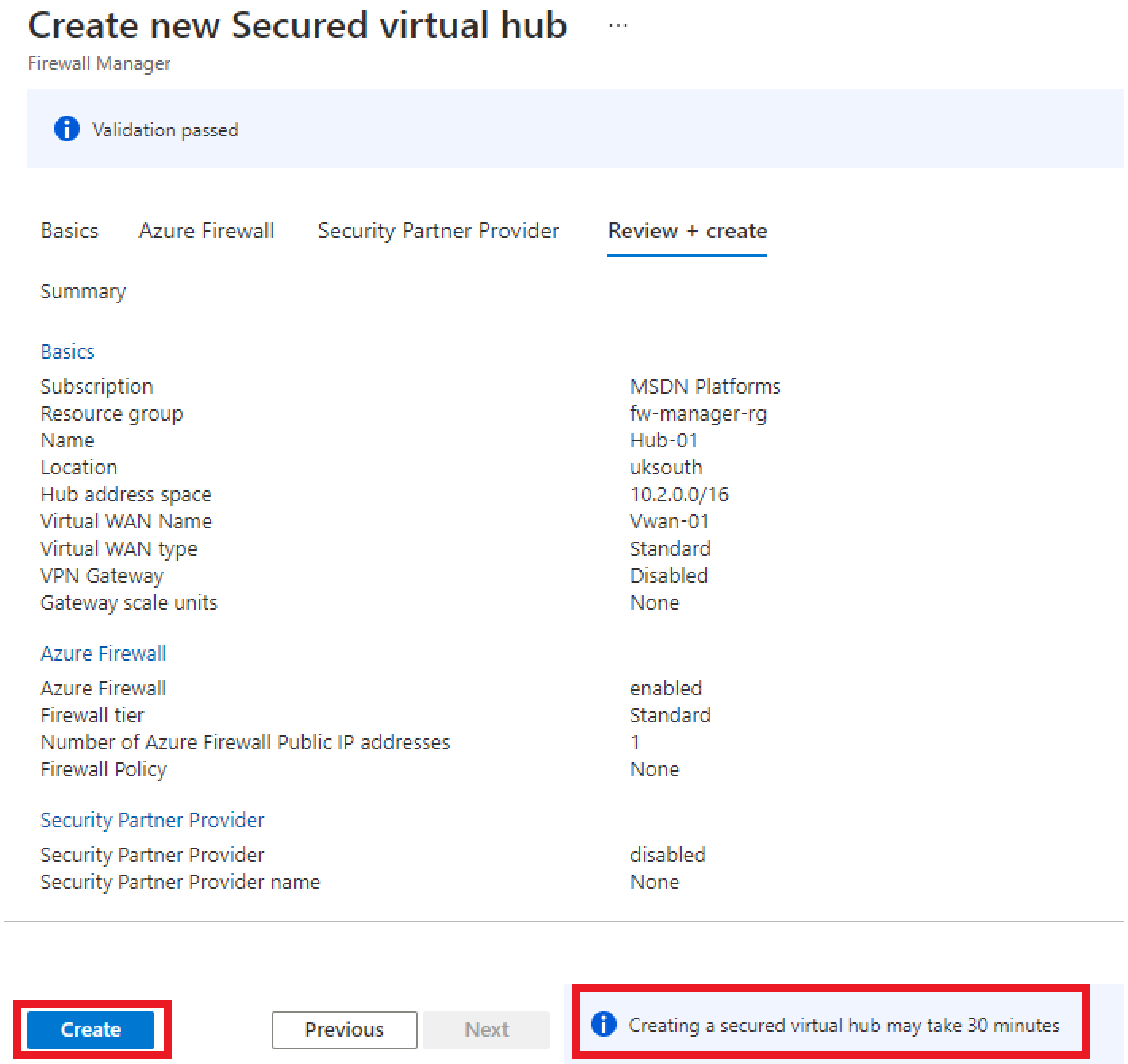
VPN gateway is required for Security Partner Provider integration

12. Select **Next: Security Partner Provider**.

13. Select **Next: Review + create.**

14. Select **Create**.

> ! **[!NOTE]** This can take up to 30 minutes to deploy.



Create new Secured virtual hub ...

Firewall Manager

Validation passed

Summary

Basics

Subscription	MSDN Platforms
Resource group	fw-manager-rg
Name	Hub-01
Location	uksouth
Hub address space	10.2.0.0/16
Virtual WAN Name	Vwan-01
Virtual WAN type	Standard
VPN Gateway	Disabled
Gateway scale units	None

Azure Firewall

Azure Firewall	enabled
Firewall tier	Standard
Number of Azure Firewall Public IP addresses	1
Firewall Policy	None

Security Partner Provider

Security Partner Provider	disabled
Security Partner Provider name	None

Creating a secured virtual hub may take 30 minutes

15. When the deployment completes, from the Azure portal home page, select **All services**.

16. In the search box, enter **firewall manager** and select **Firewall Manager** when it appears.

17. On the **Firewall Manager** page, select **Virtual hubs**.

18. Select **Hub-01**.

19. Select **Public IP configuration**.

20. Note the public IP address (e.g., **51.143.226.18**), which you will use later.

Task 3: Connect the hub and spoke virtual networks

In this task you will connect the hub and spoke virtual networks. This is commonly known as peering.

1. From the Azure portal home page, select **Resource groups**.

2. Select the **fw-manager-rg** resource group, then select the **Vwan-01** virtual WAN.

3. Under **Connectivity**, select **Virtual network connections**.

4. Select **Add connection**.

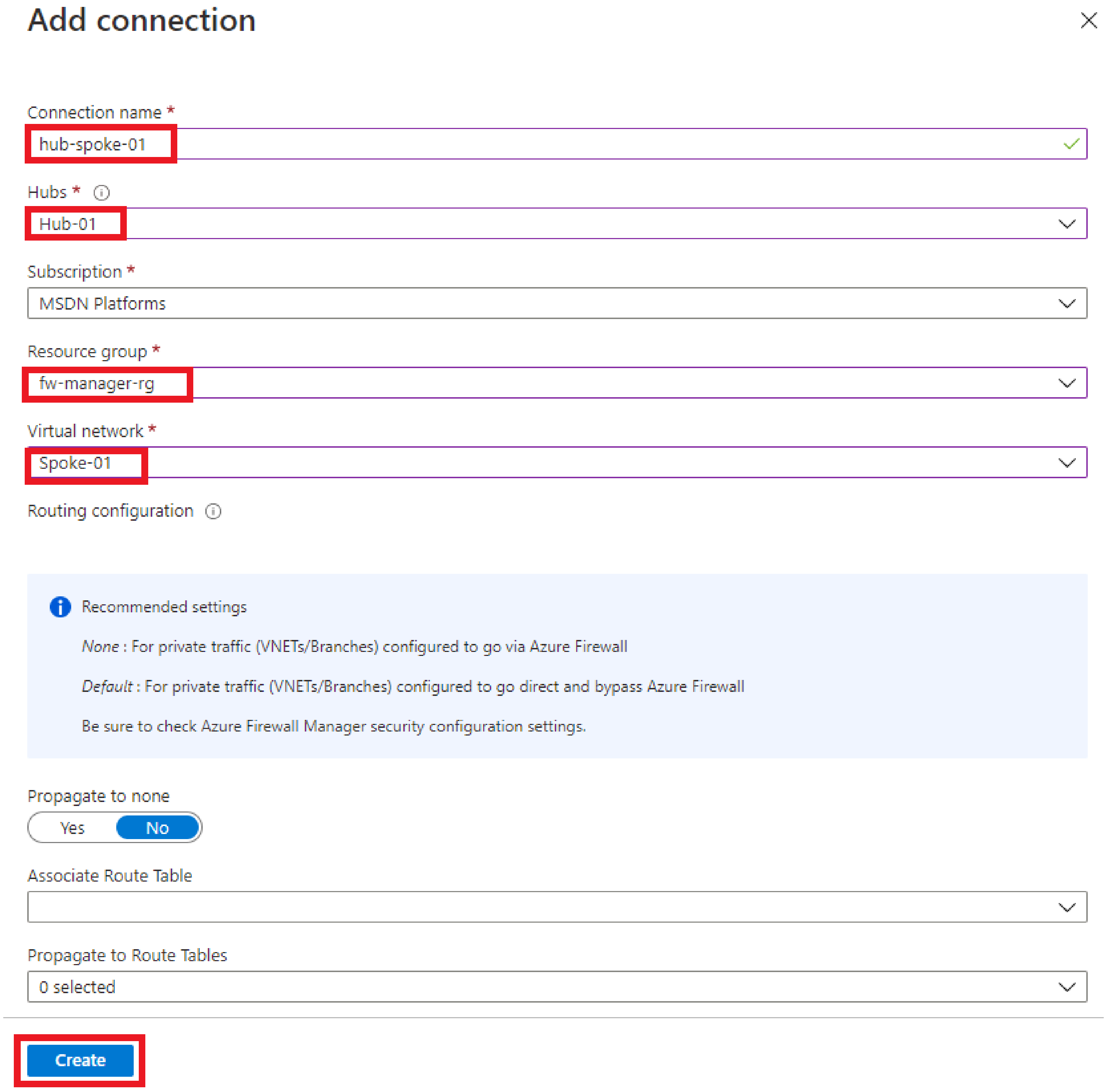
5. For **Connection name**, enter **hub-spoke-01**.

6. For **Hubs**, select **Hub-01**.

7. For **Resource group**, select **fw-manager-rg**.

8. For **Virtual network**, select **Spoke-01**.

9. Select **Create**.



Add connection

Connection name * hub-spoke-01

Hubs * Hub-01

Subscription * MSDN Platforms

Resource group * fw-manager-rg

Virtual network * Spoke-01

Routing configuration

Recommended settings

None : For private traffic (VNETs/Branches) configured to go via Azure Firewall

Default : For private traffic (VNETs/Branches) configured to go direct and bypass Azure Firewall

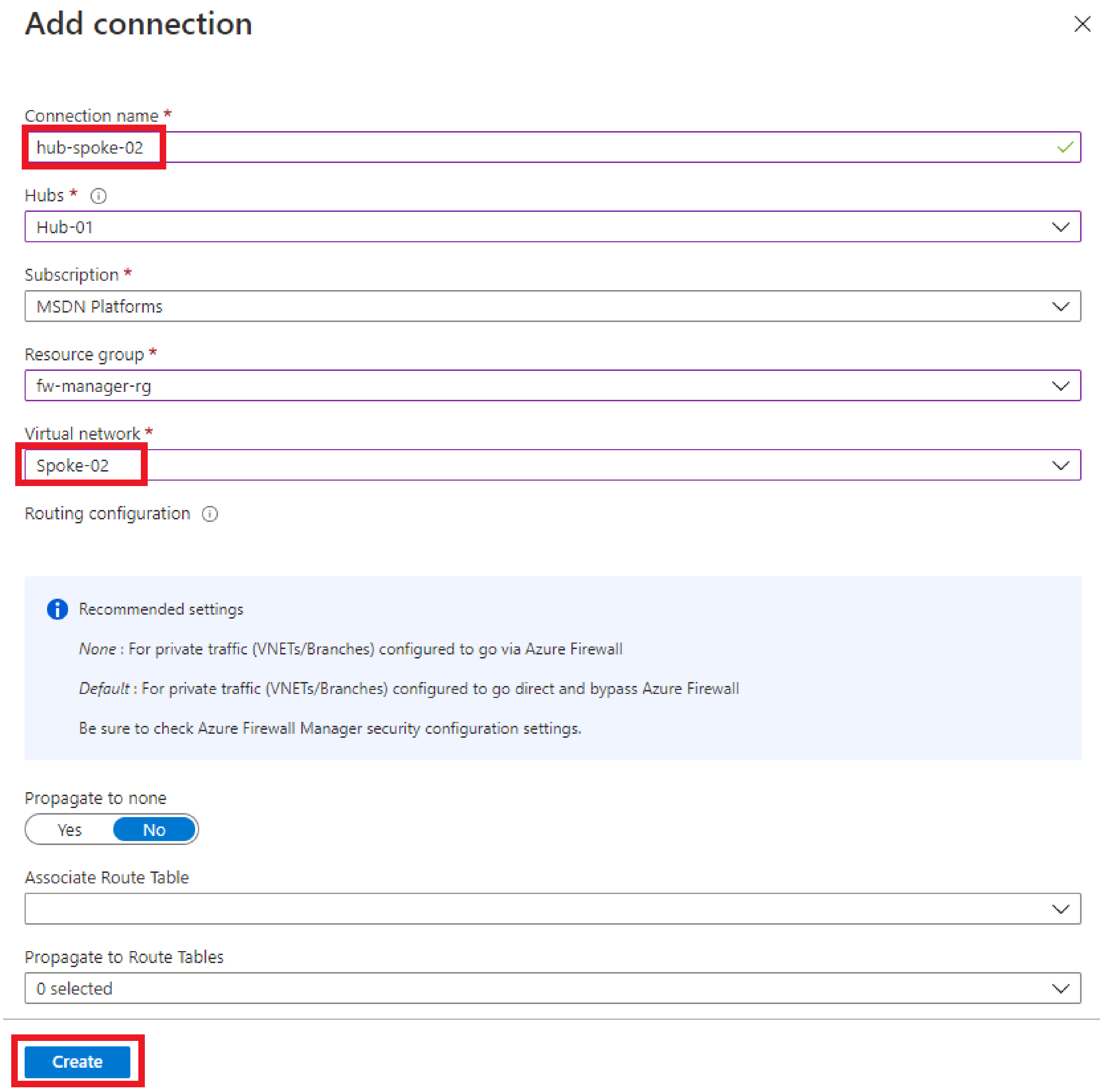
Be sure to check Azure Firewall Manager security configuration settings.

Propagate to none: Yes [✓ No]

Associate Route Table

Propagate to Route Tables: 0 selected

10. Repeat steps 4 to 9 above to create another similar connection but using the connection name of **hub-spoke-02** to connect the **Spoke-02** virtual network.



Add connection

Connection name * hub-spoke-02

Hubs * Hub-01

Subscription * MSDN Platforms

Resource group * fw-manager-rg

Virtual network * Spoke-02

Routing configuration

Recommended settings

None : For private traffic (VNETs/Branches) configured to go via Azure Firewall

Default : For private traffic (VNETs/Branches) configured to go direct and bypass Azure Firewall

Be sure to check Azure Firewall Manager security configuration settings.

Propagate to none ○ Yes ● No

Associate Route Table

Propagate to Route Tables 0 selected

Task 4: Deploy the servers

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 **FirewallManager.json** and **FirewallManager.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 = "fw-manager-rg"

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

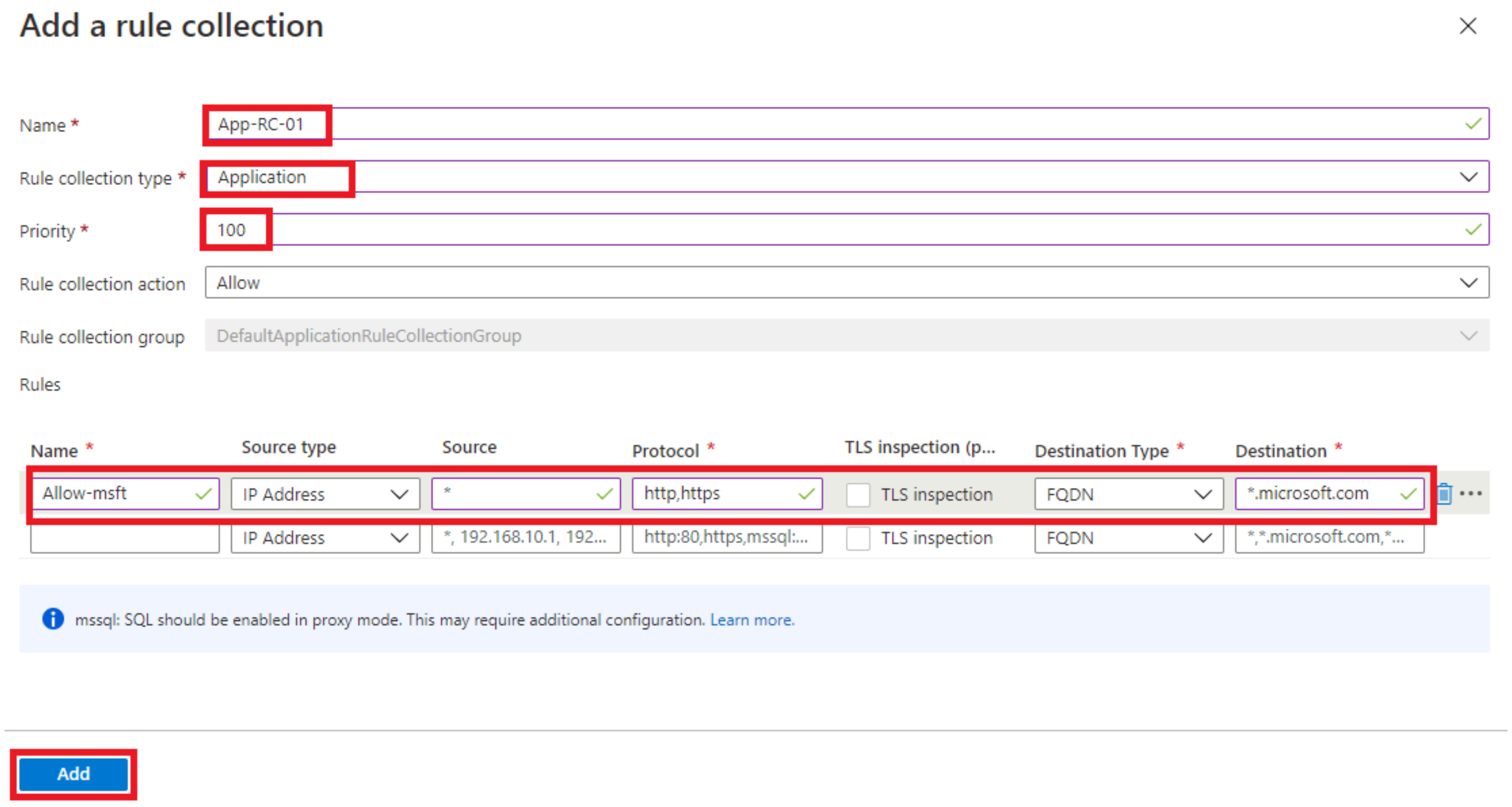
4. When the deployment is complete, go to the Azure portal home page, and then select **Virtual Machines**.
5. On the **Overview** page of **Srv-workload-01**, in the right-hand pane, under the **Networking** section, note down the **Private IP address** (e.g., **10.0.1.4**).

6. On the **Overview** page of **Srv-workload-02**, in the right-hand pane, under the **Networking** section, note down the **Private IP address** (e.g., **10.1.1.4**).

Task 5: Create a firewall policy and secure your hub

In this task you will first create your firewall policy, then secure your hub. The firewall policy will define collections of rules to direct traffic on one or more Secured virtual hubs.

1. From the Azure portal home page, select **Firewall Manager**.
    - If the Firewall Manager icon does not appear on the homepage, then select **All services**. Then in the search box, enter **firewall manager** and select **Firewall Manager** when it appears.
2. From **Firewall Manager**, from the Overview page, select **View Azure Firewall Policies**.
3. Select **Create Azure Firewall Policy**.
4. On **Resource group**, select **fw-manager-rg**.
5. Under **Policy details**, for the **Name**, enter **Policy-01**.
6. On **Region** select your region.
7. On **Policy tier**, select **Standard**.
8. Select **Next : DNS Settings**.
9. Select **Next : TLS Inspection (preview)**.
10. Select **Next : Rules**.
11. On the **Rules** tab, select **Add a rule collection**.
12. On the **Add a rule collection** page, in **Name**, enter **App-RC-01**.
13. For **Rule collection type**, select **Application**.
14. For **Priority**, enter **100**.
15. Ensure **Rule collection action** is **Allow**.
16. Under **Rules**, in **Name** enter **Allow-msft**.
17. For the **Source type**, select **IP Address**.
18. For **Source**, enter *.
19. For **Protocol**, enter **http,https**.
20. Ensure **Destination type** is **FQDN**.
21. For **Destination**, enter ***.microsoft.com**.
22. Select **Add**.



Add a rule collection

Name *	App-RC-01
Rule collection type *	Application
Priority *	100
Rule collection action	Allow
Rule collection group	DefaultApplicationRuleCollectionGroup

Rules

Name *	Source type	Source	Protocol *	TLS inspection (p...	Destination Type *	Destination *
Allow-msft	IP Address	*	http,https	□ TLS inspection	FQDN	*.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.

23. To add a DNAT rule so you can connect a remote desktop to the Srv-workload-01 VM, select **Add a rule collection**.

24. For **Name**, enter **dnat-rdp**.

25. For **Rule collection type**, select **DNAT**.

26. For **Priority**, enter **100**.

27. Under **Rules**, in **Name** enter **Allow-rdp**.

28. For the **Source type**, select **IP Address**.

29. For **Source**, enter *.

30. For **Protocol**, select **TCP**.

31. For **Destination Ports**, enter **3389**.

32. For **Destination Type**, select **IP Address**.

33. For **Destination**, enter the firewall virtual hub public IP address that you noted down earlier (e.g., **51.143.226.18**).

34. For **Translated address**, enter the private IP address for **Srv-workload-01** that you noted down earlier (e.g., **10.0.1.4**).

35. For **Translated port**, enter **3389**.

36. Select **Add**.

37. To add a Network rule so you can connect a remote desktop from Srv-workload-01 to Srv-workload-02 VM, select **Add a rule collection**.

38. For **Name**, enter **vnet-rdp**.

39. For **Rule collection type**, select **Network**.

40. For **Priority**, enter **100**.

41. For **Rule collection action**, select **Allow**.

42. Under **Rules**, in **Name** enter **Allow-vnet**.

43. For the **Source type**, select **IP Address**.

44. For **Source**, enter *.

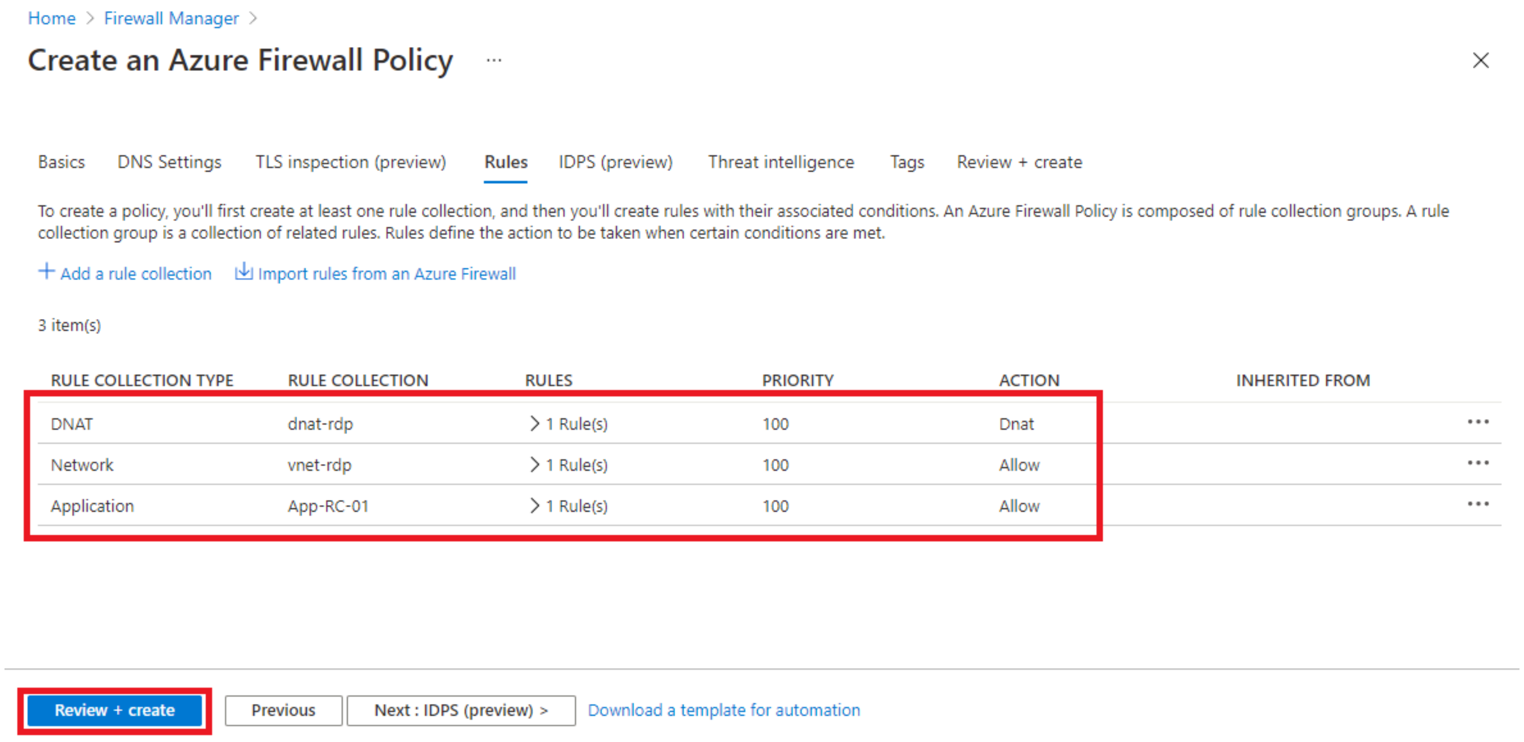
45. For **Protocol**, select **TCP**.

46. For **Destination Ports**, enter **3389**.

47. For **Destination Type**, select **IP Address**.

48. For **Destination**, enter the private IP address for **Srv-workload-02** that you noted down earlier (e.g., **10.1.1.4**).

49. Select **Add**.



Home > Firewall Manager >

Create an Azure Firewall Policy ...

Basics DNS Settings TLS inspection (preview) Rules IDPS (preview) Threat intelligence Tags Review + create

To create a policy, you'll first create at least one rule collection, and then you'll create rules with their associated conditions. An Azure Firewall Policy is composed of rule collection groups. A rule collection group is a collection of related rules. Rules define the action to be taken when certain conditions are met.

+ Add a rule collection Import rules from an Azure Firewall

3 item(s)

RULE COLLECTION TYPE	RULE COLLECTION	RULES	PRIORITY	ACTION	INHERITED FROM
DNAT	dnat-rdp	> 1 Rule(s)	100	Dnat	
Network	vnet-rdp	> 1 Rule(s)	100	Allow	
Application	App-RC-01	> 1 Rule(s)	100	Allow	

50. You should now have 3 rule collections listed.

51. Select **Review + create**.
52. Select **Create**.

Task 6: Associate the firewall policy

In this task you will associate the firewall policy with the virtual hub.

1. From the Azure portal home page, select **Firewall Manager**.

   - If the Firewall Manager icon does not appear on the homepage, then select **All services**. Then in the search box, enter **firewall manager** and select **Firewall Manager** when it appears.

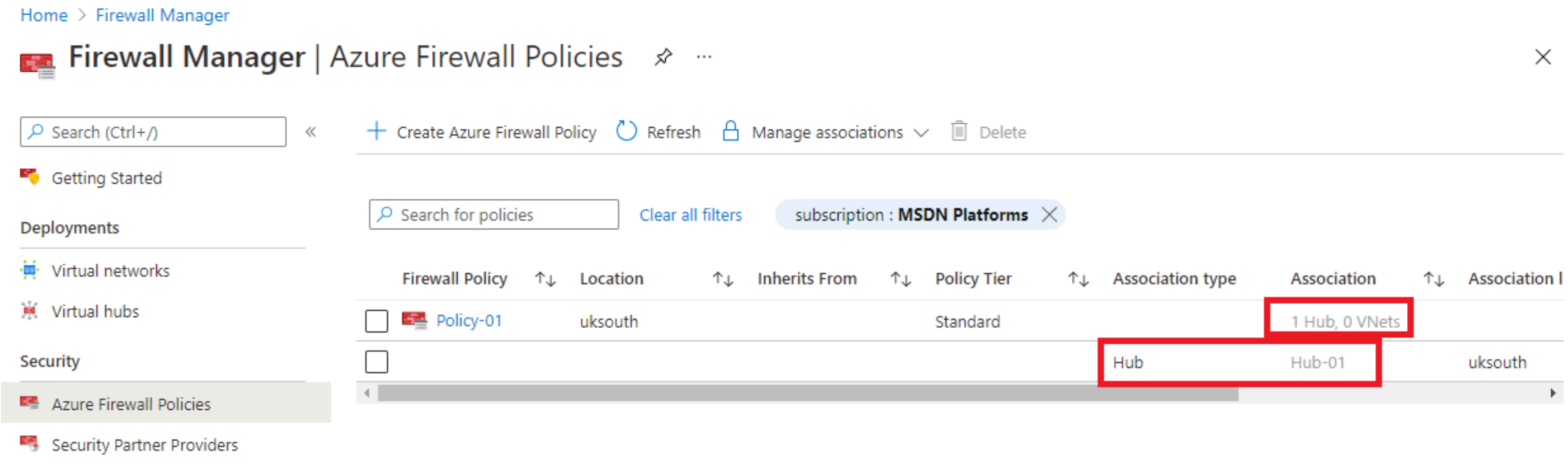
2. On **Firewall Manager**, under **Security**, select **Azure Firewall Policies**.

3. Select the checkbox for **Policy-01**.

4. Select **Manage associations>Associate hubs**.

5. Select the checkbox for **Hub-01**.

6. Select **Add**.
7. When the policy has been attached, select **Refresh**. The association should be displayed.



Home > Firewall Manager

Firewall Manager | Azure Firewall Policies

	Firewall Policy	Location	Inherits From	Policy Tier	Association type	Association	Association l
□	Policy-01	uksouth		Standard		1 Hub, 0 VNets	
□					Hub	Hub-01	uksouth

Task 7: Route traffic to your hub

In this task you will ensure that network traffic gets routed through your firewall.

1. On **Firewall Manager**, select **Virtual hubs**.

2. Select **Hub-01**.
3. Under **Settings**, select **Security configuration**.
4. On **Internet traffic**, select **Azure Firewall**.
5. On **Private traffic**, select **Send via Azure Firewall**.
6. Select **Save**.
7. This will take a few minutes to complete.
8. Once configuration has completed, ensure that under **INTERNET TRAFFIC** and **PRIVATE TRAFFIC**, it says **Secured by Azure Firewall** for both hub-spoke connections.

Task 8: Test the application rule

In this part of the exercise, you will connect a remote desktop to the firewall public IP address, which is NATed to Srv-Workload-01. You will then use a web browser to test the application rule and connect a remote desktop to Srv-Workload-02 to test the network rule.

In this task you will test the application rule to confirm that it works as expected.

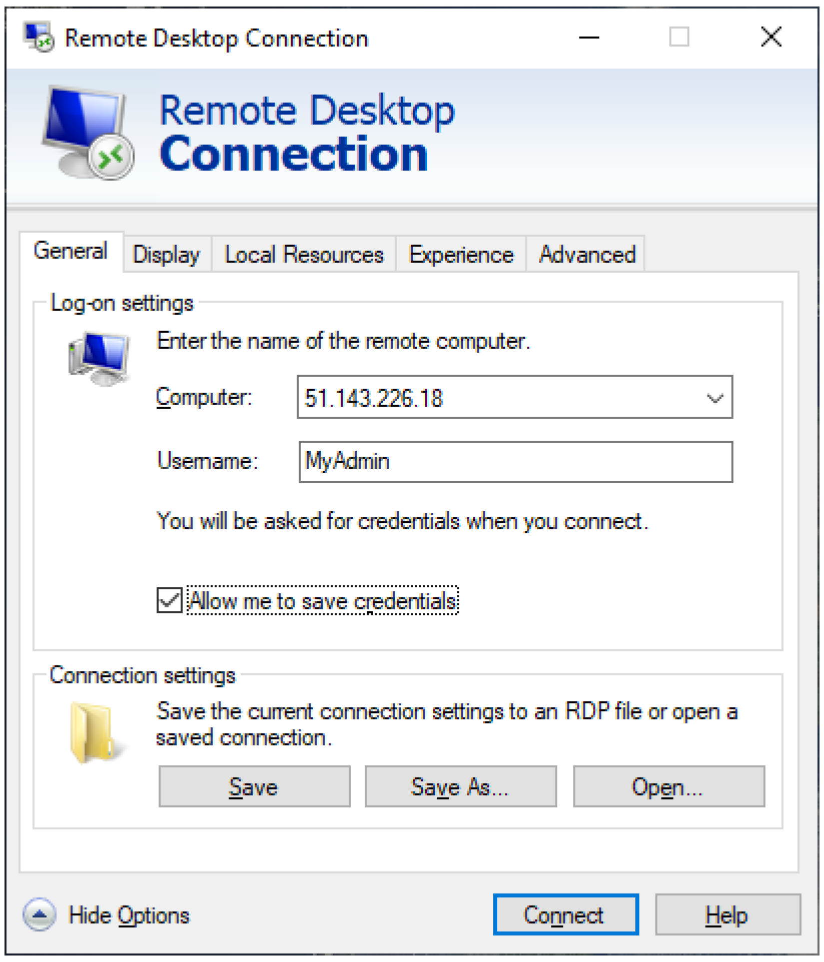
1. Open **Remote Desktop Connection** on your PC.

2. On the **Computer** box, enter the **firewall's public IP address** (e.g., **51.143.226.18**).

3. Select **Show Options**.

4. On the **Username** box, enter **TestUser**.

5. Select **Connect**.



Remote Desktop Connection

Remote Desktop Connection

General | Display | Local Resources | Experience | Advanced

Log-on settings

Enter the name of the remote computer.

Computer: 51.143.226.18

Username: MyAdmin

You will be asked for credentials when you connect.

☑ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

6. On the **Enter your credentials** dialog box, log into the **Srv-workload-01** server virtual machine, by using the password you provided during deployment.

7. Select **OK**.

8. Select **Yes** on the certificate message.

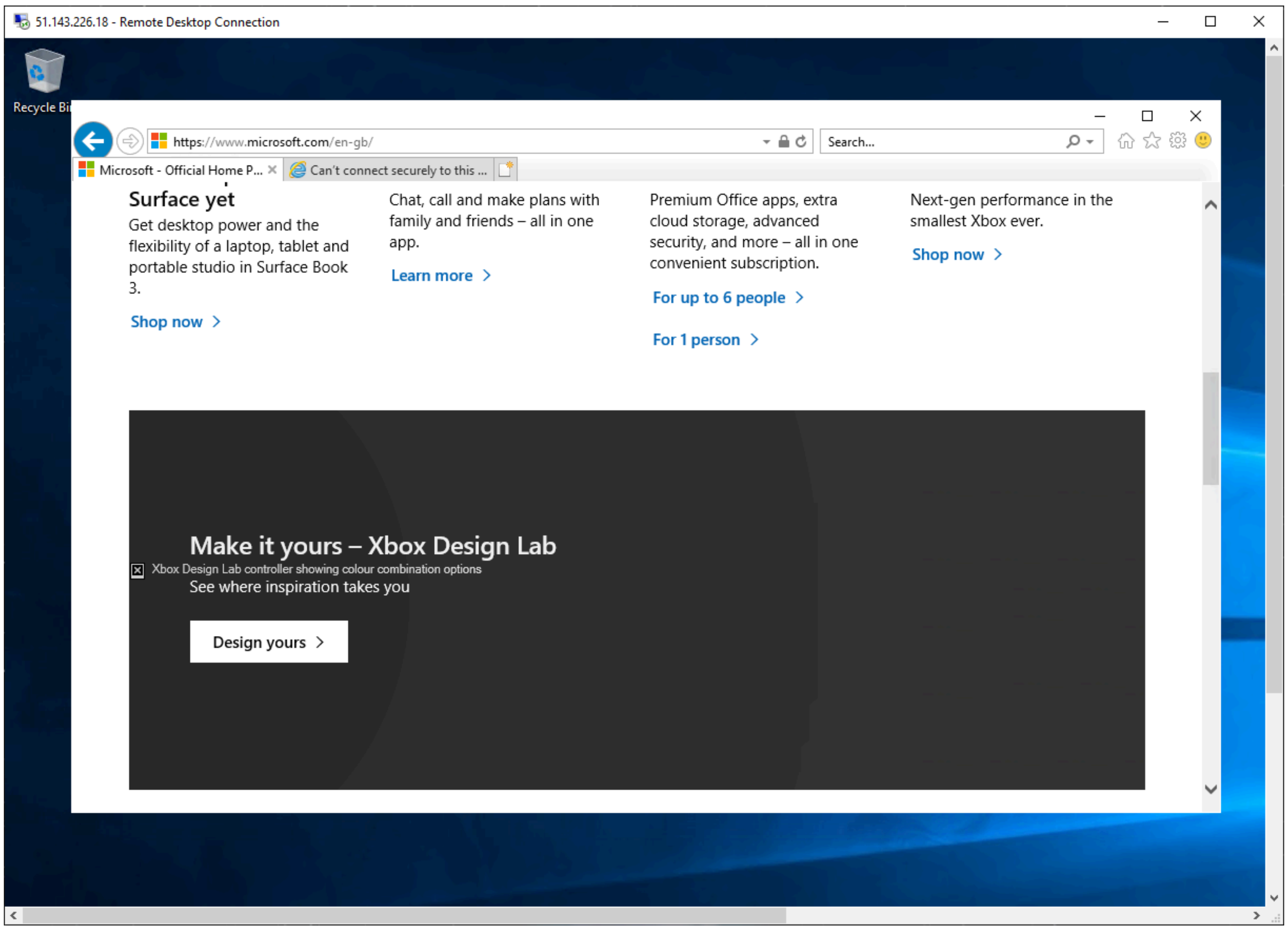
9. Open Internet Explorer and select **OK** in the **Set up Internet Explorer 11** dialog box.

10. Browse to **https://** ****.

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

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

13. You should see the Microsoft home page.


51.143.226.18 - Remote Desktop Connection
Recycle Bi
https://www.microsoft.com/en-gb/
Search...
Microsoft - Official Home P...
Can't connect securely to this ...
Shop now
Learn more
For up to 6 people
For 1 person
Shop now
Design yours

Surface yet

Get desktop power and the flexibility of a laptop, tablet and portable studio in Surface Book 3.

Chat, call and make plans with family and friends – all in one app.

Premium Office apps, extra cloud storage, advanced security, and more – all in one convenient subscription.

Next-gen performance in the smallest Xbox ever.

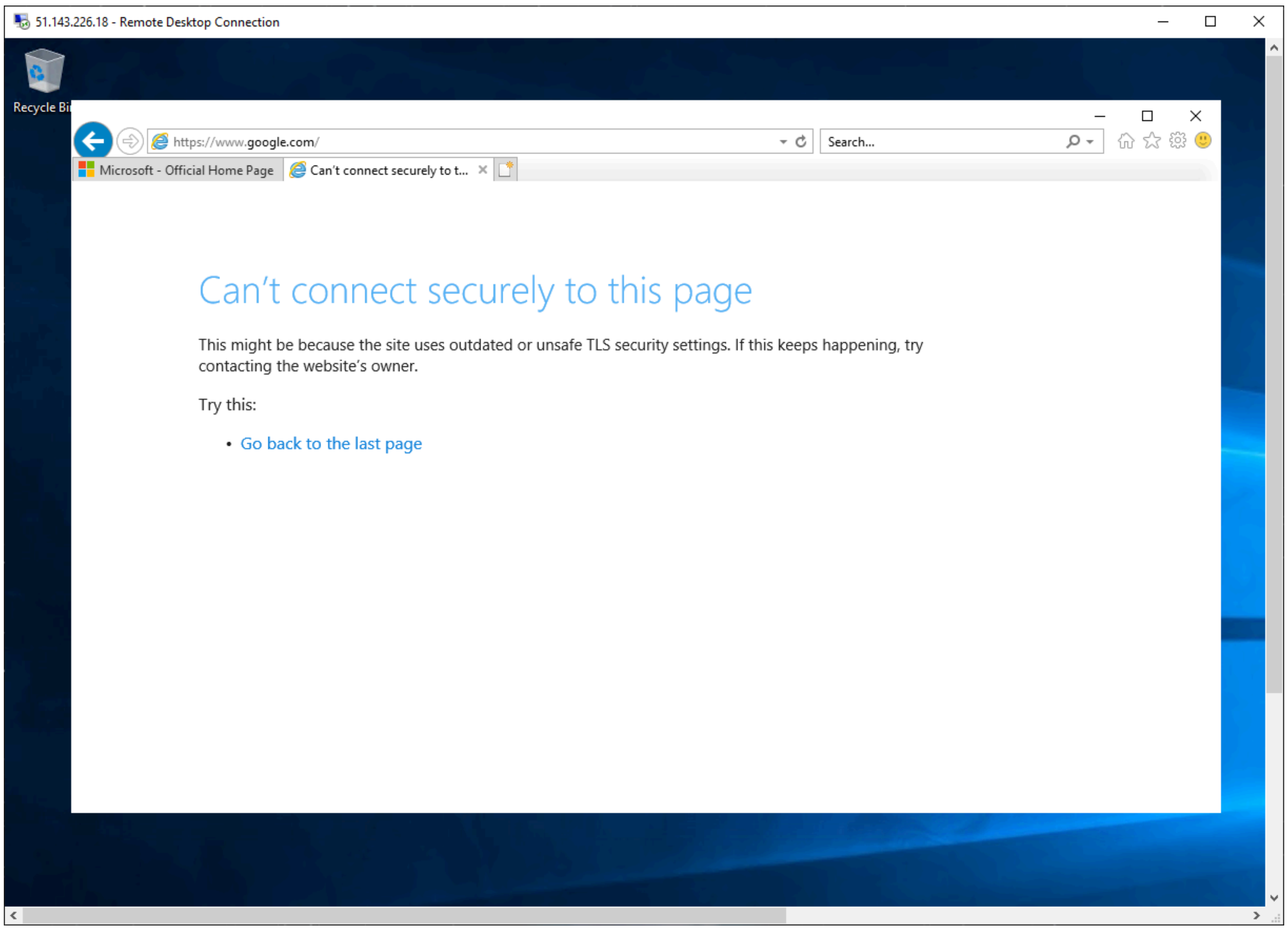
Make it yours – Xbox Design Lab

Xbox Design Lab controller showing colour combination options

See where inspiration takes you

14. Browse to **https://** ****.

15. You should be blocked by the firewall.


51.143.226.18 - Remote Desktop Connection
Recycle Bi
https://www.google.com/
Search...
Microsoft - Official Home Page
Can't connect securely to t...
Go back to the last page

Can't connect securely to this page

This might be because the site uses outdated or unsafe TLS security settings. If this keeps happening, try contacting the website's owner.

Try this:

- Go back to the last page

16. So, you have verified that you can connect to the one allowed FQDN but are blocked from all others.

Task 9: Test the network rule

In this task you will test the network rule to confirm that it works as expected.

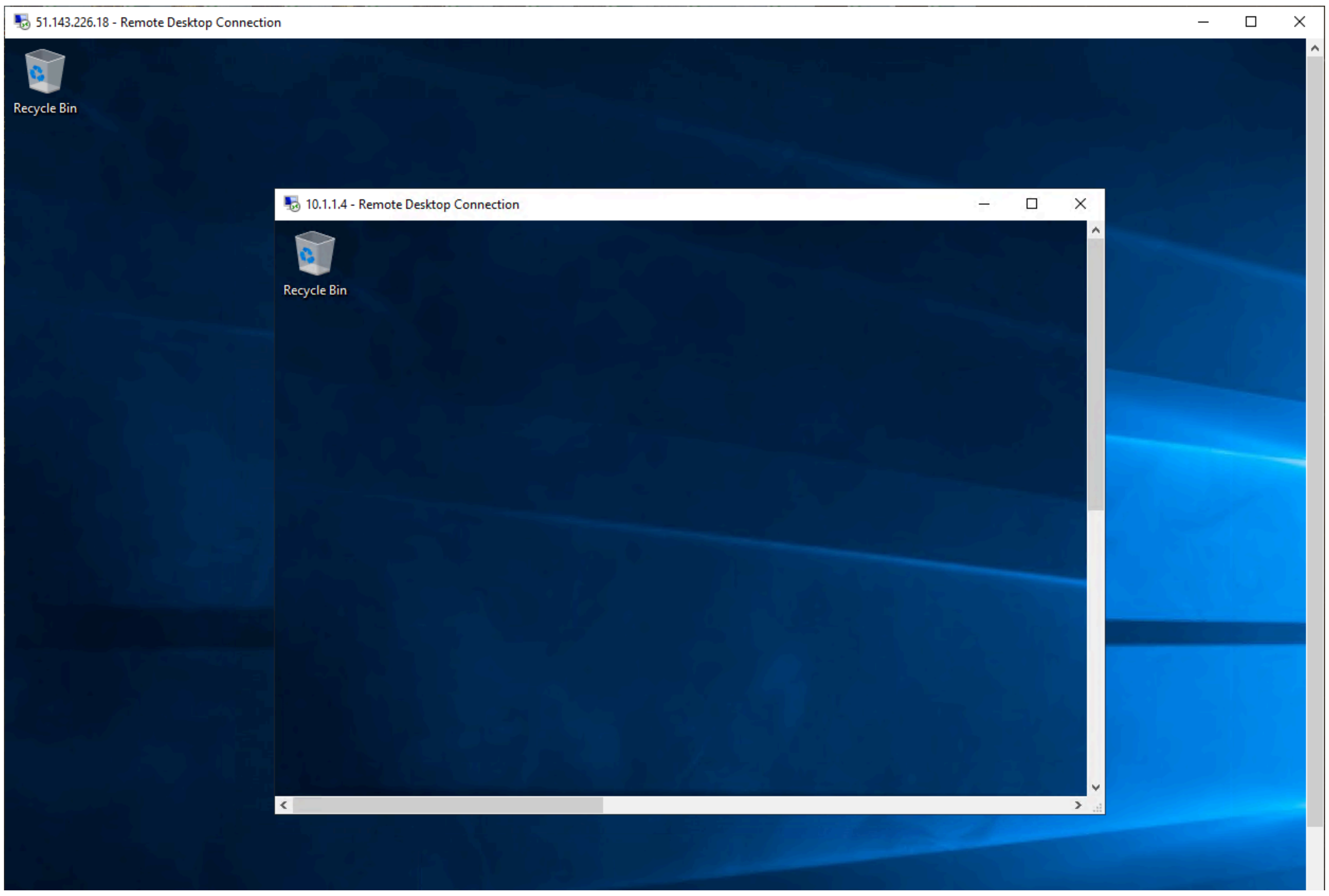
1. While still logged in to the **Srv-workload-01** RDP session, from this remote computer, open **Remote Desktop Connection**.

2. On the **Computer** box, enter the **private IP address** of **Srv-workload-02** (e.g., **10.1.1.4**).

3. On the **Enter your credentials** dialog box, log in to the **Srv-workload-02** server by using the username **TestUser**, and the password you provided during deployment.

4. Select **OK**.

5. Select **Yes** on the certificate message.


51.143.226.18 - Remote Desktop Connection
Recycle Bin
10.1.1.4 - Remote Desktop Connection
Recycle Bin

6. So, now you have verified that the firewall network rule is working, as you have connected a remote desktop from one server to another server located in another virtual network.

7. Close both RDP sessions to disconnect them.

Task 10: 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 'fw-manager-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.