# Overview

In this guided practice, you will install the Remote Access role on a Windows Server machine and then configure NAT (Network Address Translation) to allow the computers on your internal network to access the Internet.

# Prerequisites

* Guided practice – **Computer Setup** is complete

# Scenario

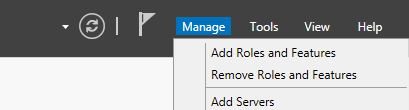
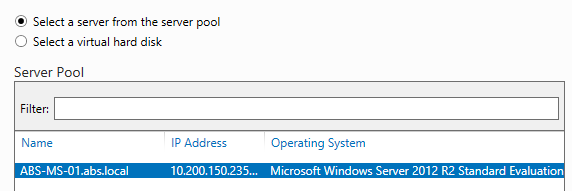
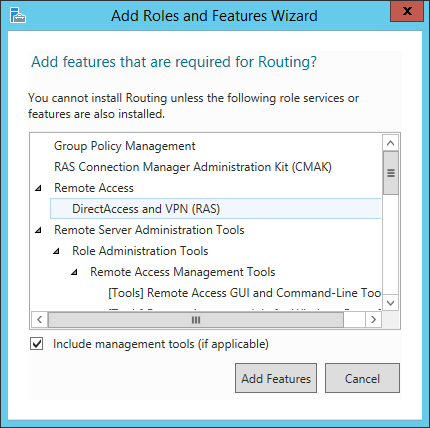
In modern business, a connection to the Internet is vital for communication and basic working tasks. ABS Corporation has just signed a contract with an Internet Service Provider and needs you to configure its router/firewall to allow traffic to the Internet. To do this, you will need to install the routing service on the Router machine and enable NAT in order to translate the private IP addresses you are using internally to the public IP address assigned to the router’s WAN connection.

# Tasks

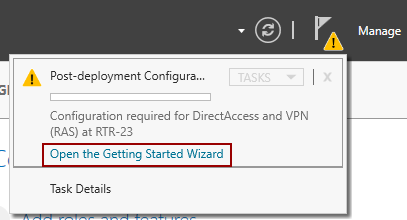
Note: This procedure must be completed on the **CIS256-RTR** virtual machine

## Installing the Remote Access Role

Use the following procedure to install the Routing and Remote Access service on your router virtual machine:

1. Logon to the **CIS256-RTR** virtual machine as the administrator
2. In **Server Manager**, select the **Add** **Roles and Features** from the **Manage** menu.
3. On the **Before You Begin** page of the **Add Roles and Features Wizard**, select **Skip this page by default** radio button and then **click** the **Next** button.
4. On the **Select installation type** page of the **Add Roles and Features Wizard**, select the **Role-based or feature-based installation** option, and then **click** the **Next** button.
5. On the **Select destination server** page of the **Add Roles and Features Wizard**, verify the **Select a server from the server pool** option is selected and your server is highlighted in the **Server Pool** list. **Click** the **Next** button.
6. On the **Select server roles** page of the **Add Roles and Features Wizard**, select the **Remote Access** checkbox. Click **Next.**
7. On the **Select features** page of the **Add Roles and Features Wizard**, click **Next.**
8. On the **Remote Access** page of the **Add Roles and Features Wizard**, read the page and click **Next.**
9. ****On the **Select role services** page of the **Add Roles and Features Wizard**, **select** the **Routing** checkbox. When prompted to Add features that are required for Routing **click** the **Add Features** button. You should see the Direct Access and VPN (RA) option selected also. **Click** the **Next** button.
10. On the **Web Server Role (IIS)** page of the **Add Roles and Features Wizard**, read the information and click **Next.**
11. On the **Select role services** page of the **Add Roles and Features Wizard**, click **Next.**
12. On the **Confirm installation selections** page of the **Add Roles and Features Wizard**, **select** the **Restart the destination server automatically if required** option and click **Install.**
13. On the **Installation Progress** page of the **Add Roles and Features Wizard**, verify that the installation was successful and click **Close.**

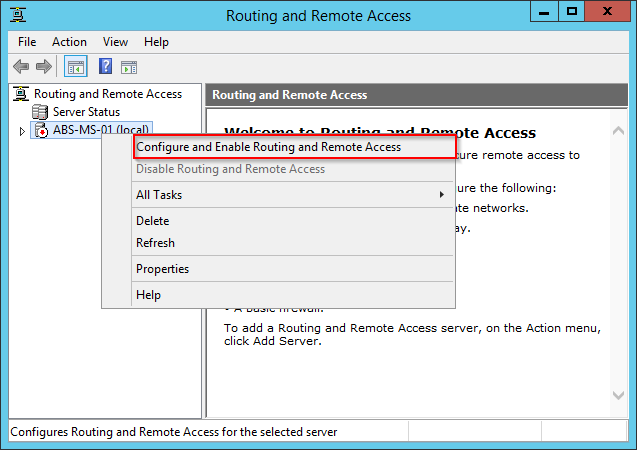
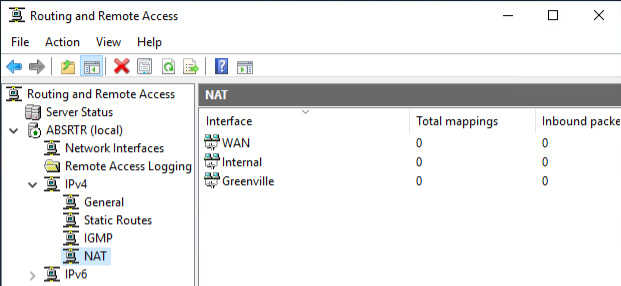
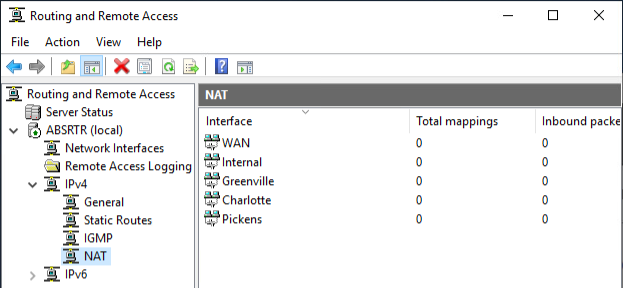
## Routing POST Installation ConfiguRation

Many of the roles in Windows have a post configuration wizard that needs to be accomplished after the installation of the role. To complete the post installation configuration for the DirectAccess and VPN roles, perform the following:

1. **Open Server Manager**
2. **Click** the **notification** icon
3. **Click** the **Open the Getting Started Wizard** link as shown in the figure. This will launch a wizard, but it may be behind **Server Manager,** and it make take a minute or longer to launch…patience.
4. In the **Configure Remote Access** wizard, **click** the **Deploy VPN** **only** option.
5. When this is done the **Routing and Remote Access** console will open and you can proceed to the next section

## Configuring and Enabling the Routing and Remote Access Service

Use the following procedure to enable the routing and remote access service and configure NAT:

1. In the **Routing and Remote Access** option from the **Tools** menu. This will launch the **Routing and Remote Access management** console.
2. **Right-Click** your server in the **Routing and Remote Access** console and choose **Configure and Enable Routing and Remote Access** from the context menu. This will launch a wizard.
3. On the **Welcome to the Routing and Remote Access Server Setup Wizard** page, click **Next**.
4. On the **Configuration** page, select **Network address translation (NAT)** radio button. Click **Next**.
5. On the **NAT Internet Connection** page, select the **WAN** network interface to be the public interface. Click **Next**.
6. On the **Network Selection** page, select the **Greenville** network interface and **click** **Next**
7. On the **Completing the Routing and Remote Access Server Setup Wizard** page, verify the settings. Click **Finish**.
8. The routing and remote access service will start, and you should see a green up arrow on the **Routing and Remote Access** snap-in indicating the service is running.
9. **Browse** to the **NAT** node and you should see something like the figure to the right.
10. **Right** **click** on the **NAT** **node** and select **New Interface…** from the **context** **menu** and **add** the **Charlotte** interface **as** a **private** interface.
11. **Repeat** the **step** above to **add** the **Pickens** interface.
12. When you are done the NAT node should look like the figure below.

## Verify the Configuration Changes

1. Verify that all your server virtual machines can now access the Internet by ping 1.1.1.1.

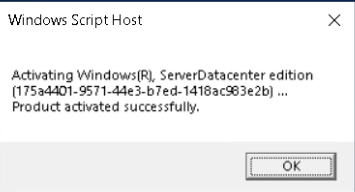
## Activate SERVER VMs and VM-Host

1. The KMS server for ECPI is located at **10.10.6.20**. In **Windows PowerShell (admin)**, issue the following commands to activate the Windows server systems.

slmgr /skms 10.10.6.20

slmgr /ato

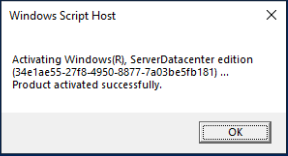
The expected response is **Product activated successfully**.



1. If the response from **slmgr /ato** is ***The activation server determined that the specified product key could not be used***, issue the following commands

slmgr /ipk WMDGN-G9PQG-XVVXX-R3X43-63DFG

slmgr /ato



## Submission Requirements

1. **Download** the **grading** **script** from the assignment page to the **C:\Scripts** folder.
2. Check your lab by running the following command:

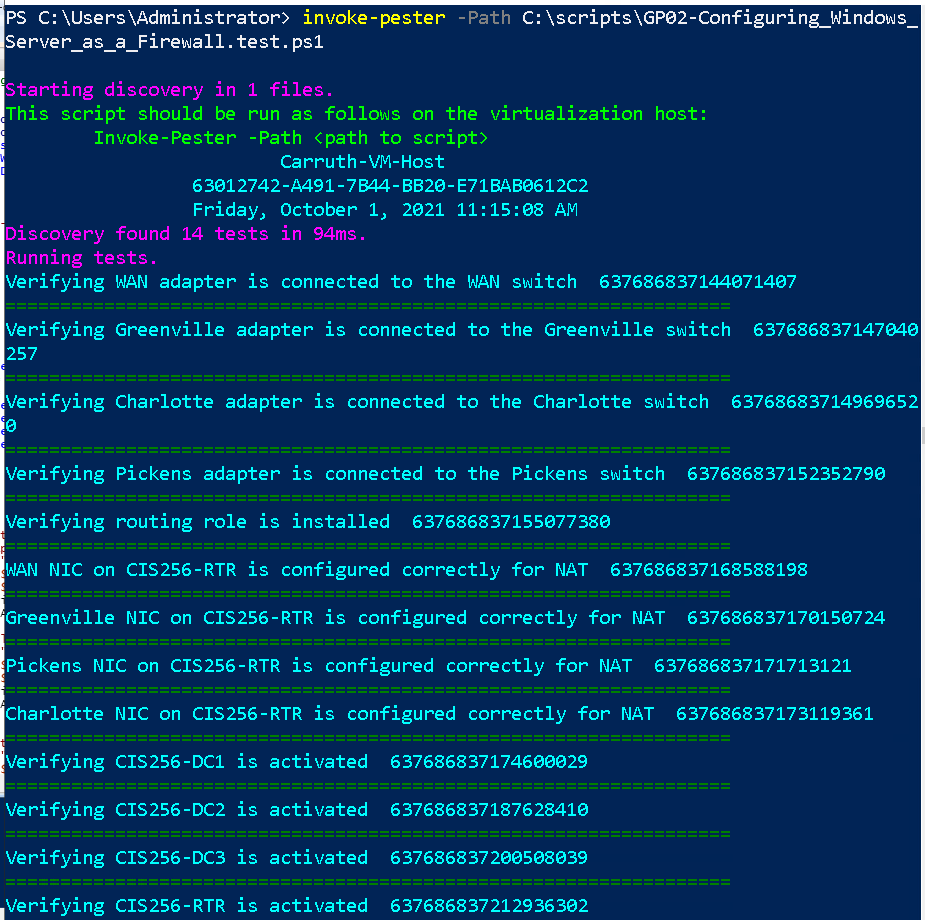
Invoke-Pester -Path C:\Scripts\GP02-Configuring\_Windows\_Server\_ as\_a\_Firewall.test.ps1

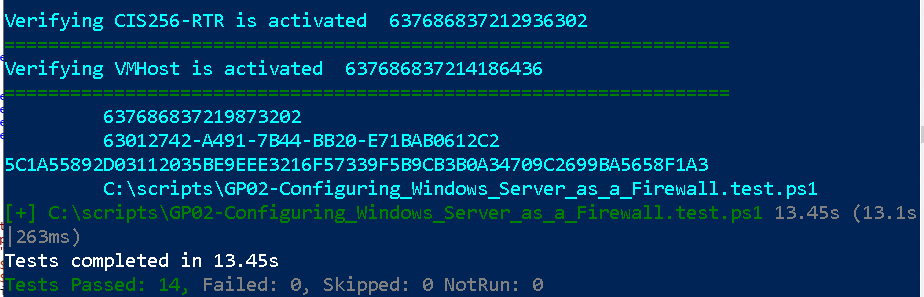
**Note**: You will see a security warning when running the script. Enter **R** to run the script.

If you want to see more detail, add **-Output Detailed** to the command. This may assist you with troubleshooting

Invoke-Pester -Path C:\Scripts\GP02-Configuring\_Windows\_Server\_ as\_a\_Firewall.test.ps1 -Output Detailed

1. You should not see any red in the output. Red in the PowerShell way of telling you that an error condition exists. Most of the time, the output will tell you what is wrong. If it is not obvious, contact your teacher and ask for assistance. You will be learning PowerShell during this term. **Correct** any **errors** you may have and run the script until all the output has no red. You should see the output like the images below.





1. Capture a snippet that shows the PowerShell Command and all its output. If you must use more than one snippet to capture the output, you must have at least **one line of overlap** in the snippets. The text in the snippets **must be legible** when pasted into the Word document. Paste the snippet(s) into a **new** **Word** **document.**
2. **Upload** the **document** in the submission area for the assignment.