

# Lab: DNS Filtering

Estimated time 15 minutes

**Note:- All steps must be completed in a single session. Once the virtual instance is closed, all configurations will be lost.**

## Introduction

In this hands-on lab, you will learn how to create an outbound rule in Windows Firewall to strengthen network security by restricting DNS requests. By completing this lab, you will gain valuable skills in managing firewall rules and controlling network traffic.

**Note:** If you try these instructions on your computer, your screens might look slightly different than what you see in this lab. Also, remember to disable or remove the outbound rule after completing the lab.

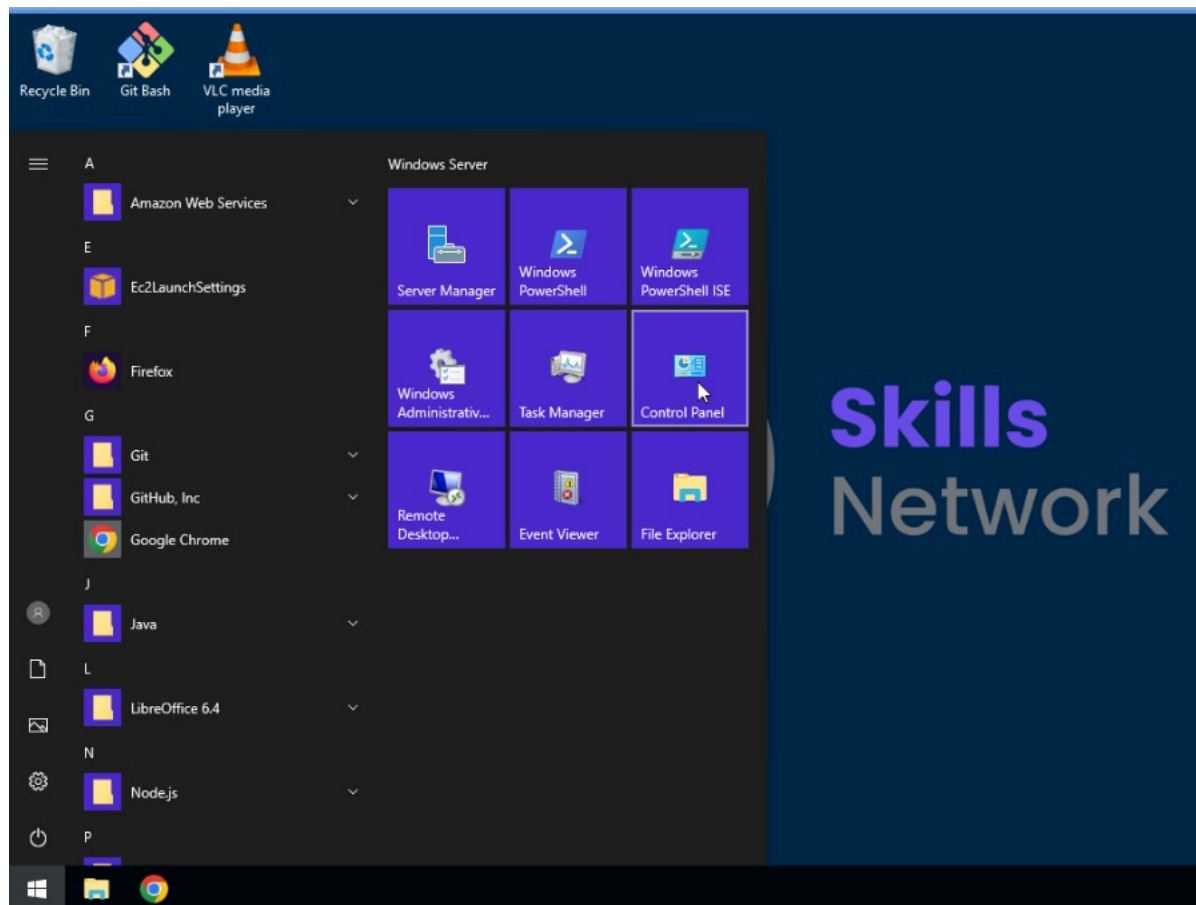
## Objectives

After completing this lab, you will be able to:

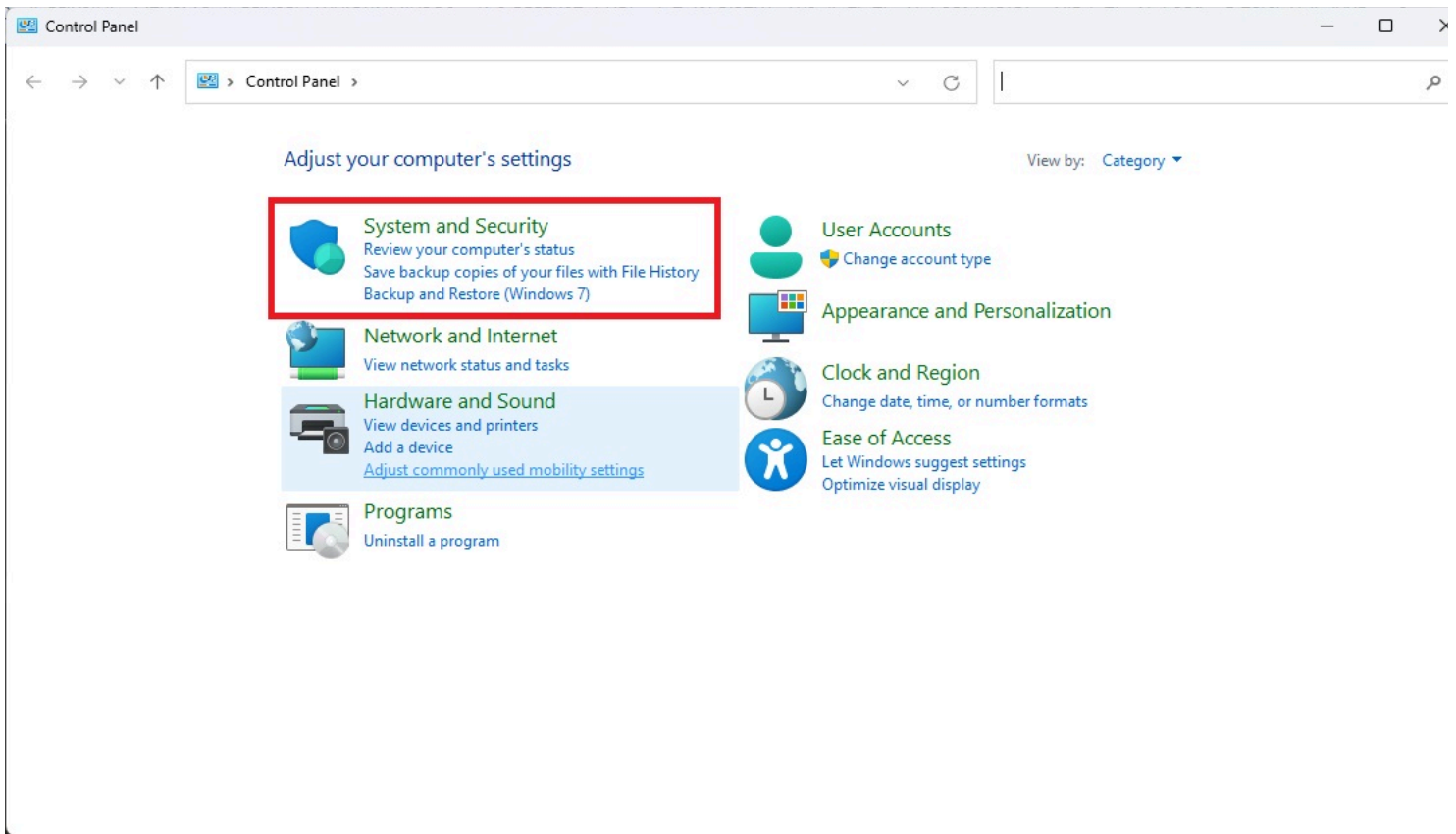
- Locate and access the Microsoft Windows Firewall interface.
- Create a new outbound rule in Windows Firewall interface to block DNS traffic
- Verify the existence and effectiveness of the new outbound rule.

## Task 1: Navigate to the Microsoft Windows Firewall interface

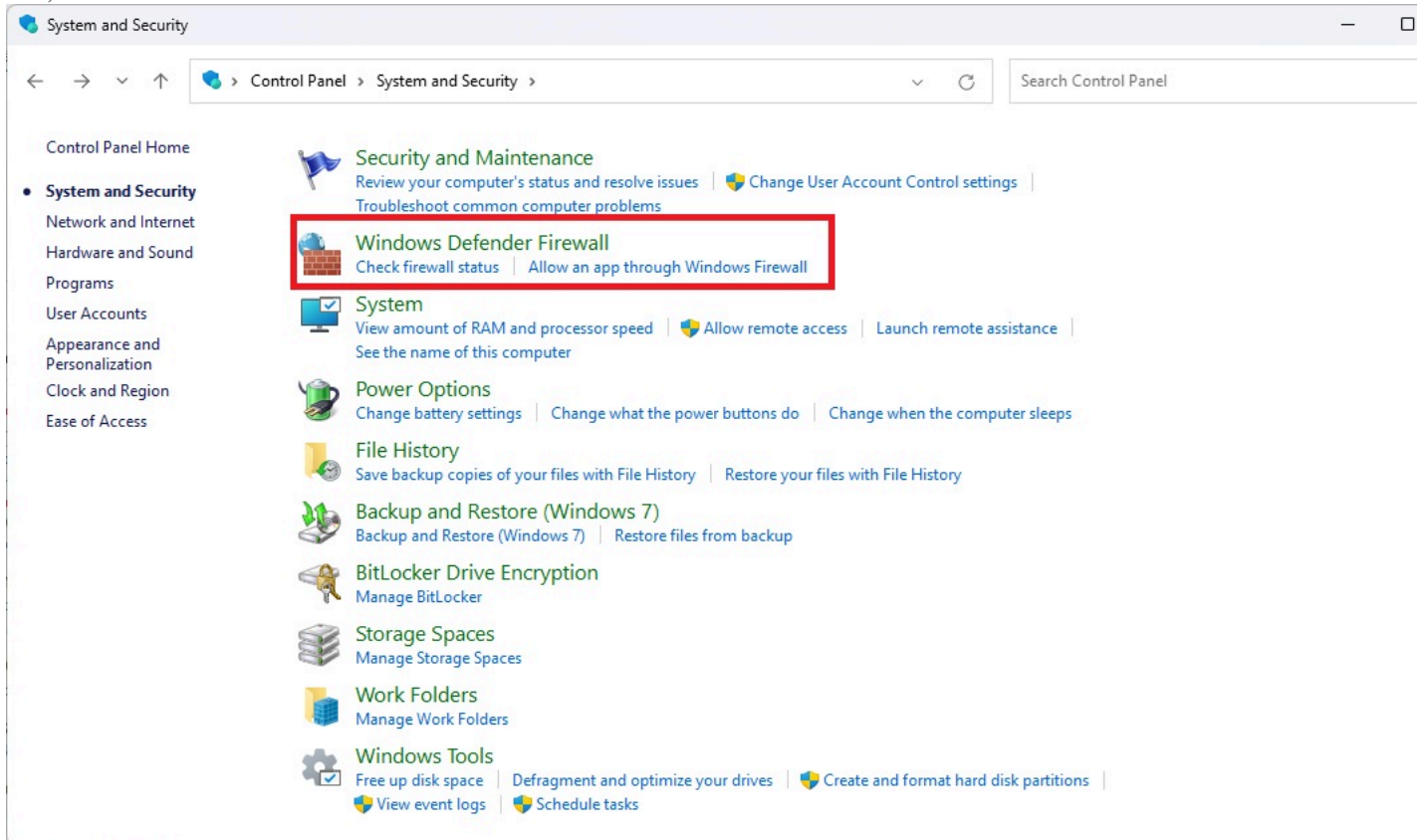
1. Click Windows Icon, and search for **Control Panel**.



2. Click on **Control Panel**.
3. Select **System and Security**.

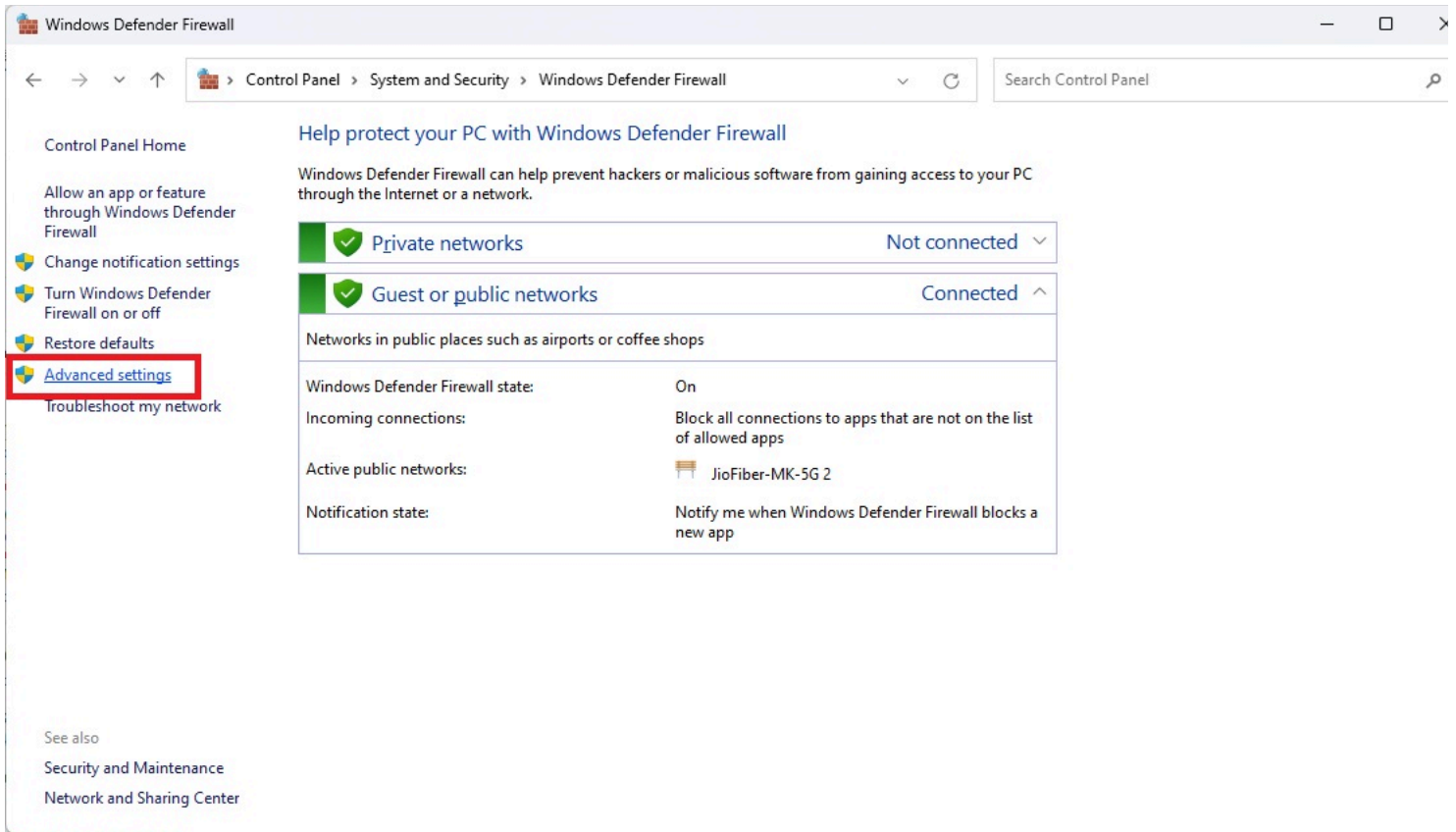


4. Next, select **Windows Defender Firewall**.

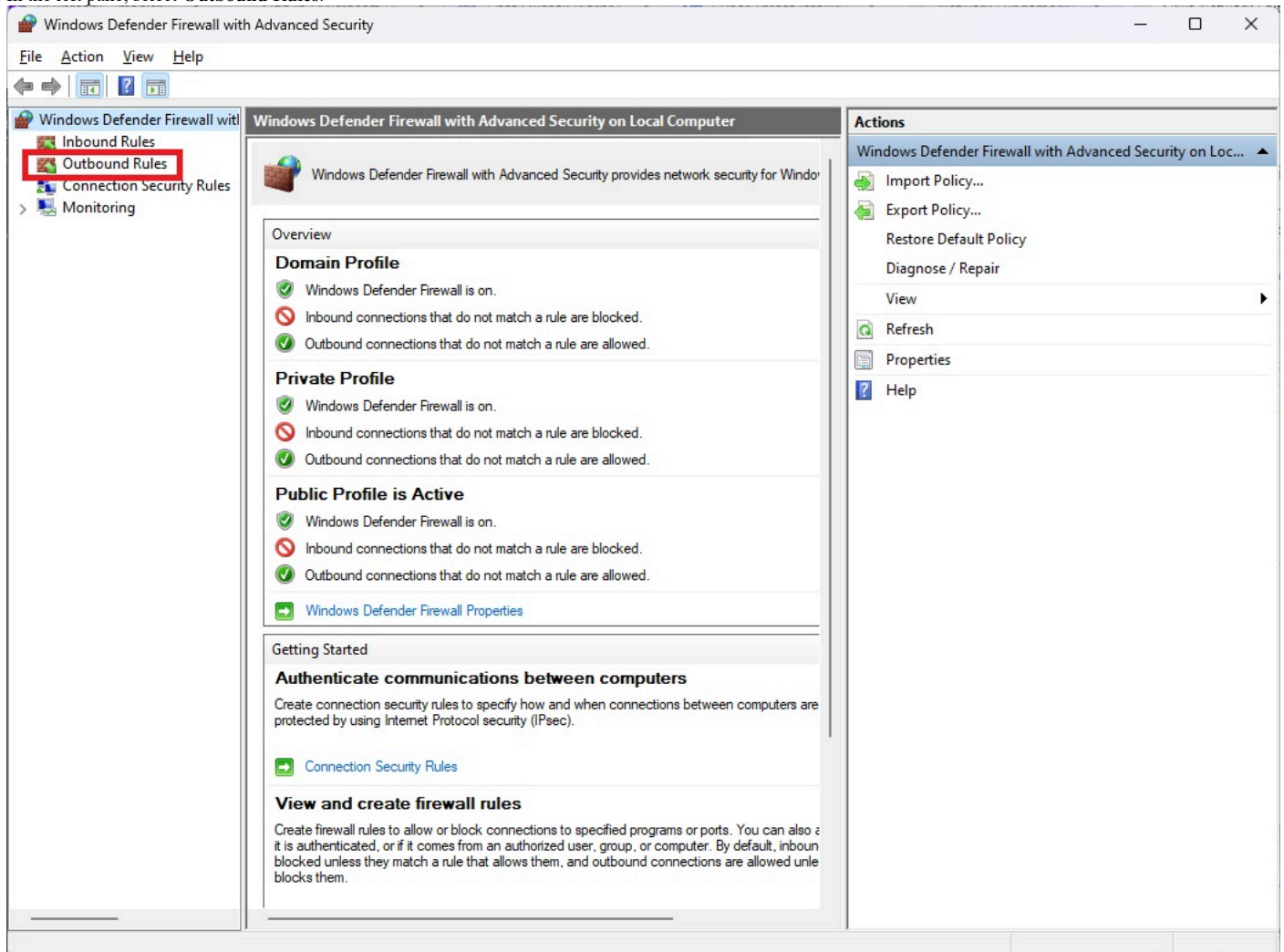


## Task 2: Create a new outbound rule

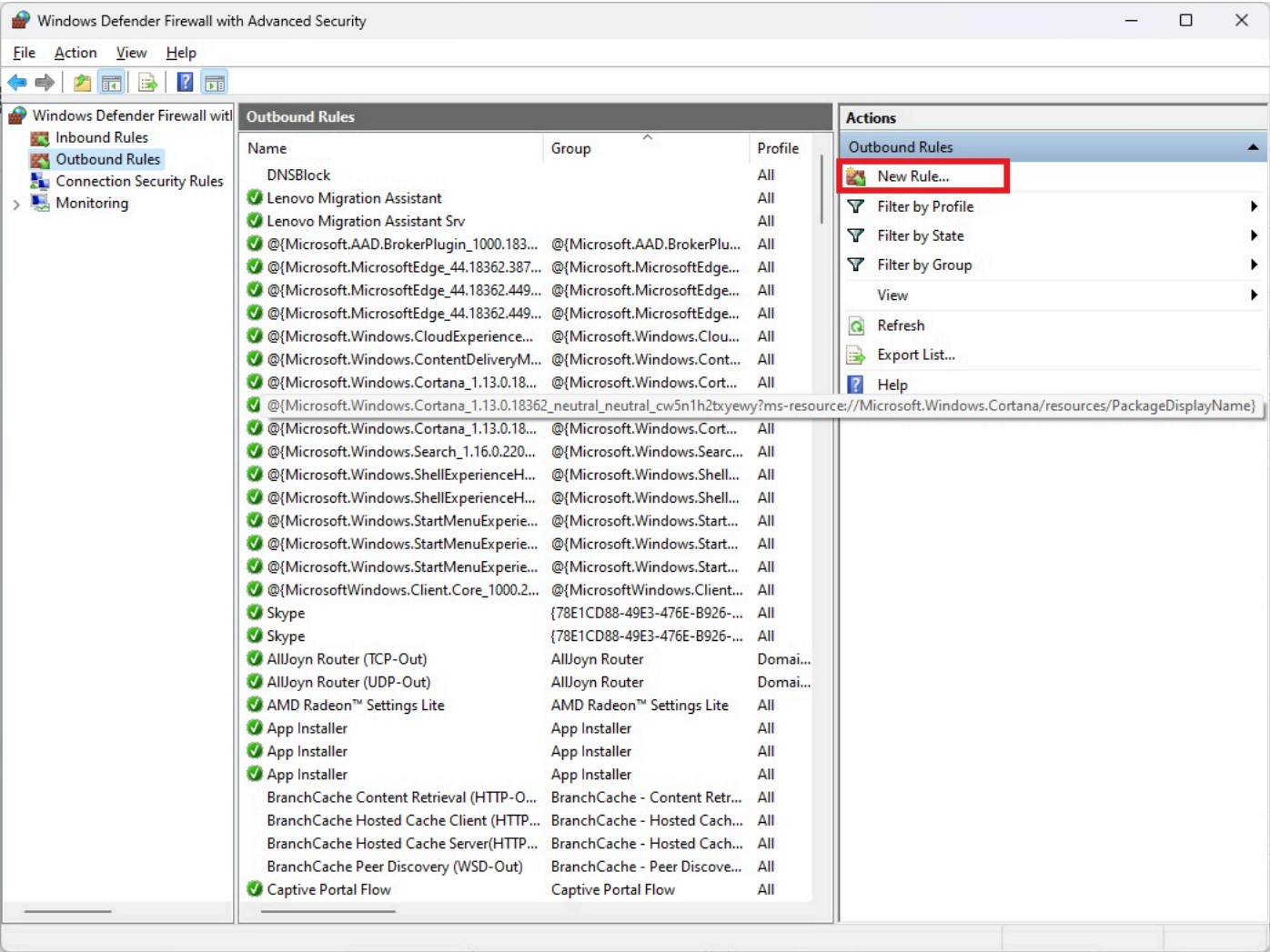
1. In the left pane, select **Advanced Settings**.



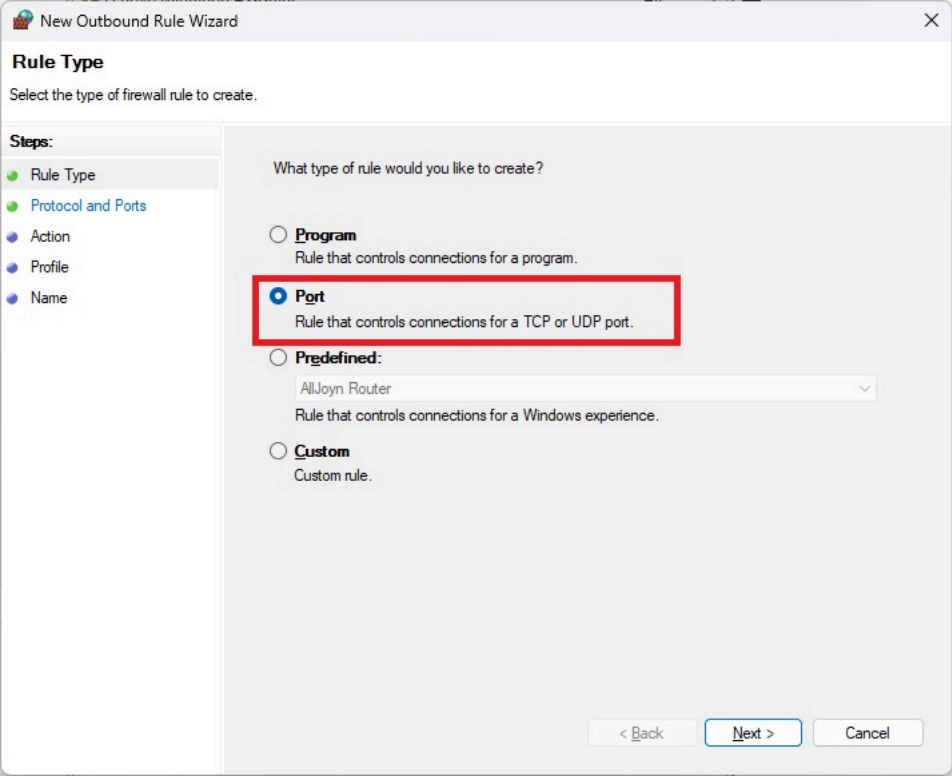
2. In the left pane, select **Outbound Rules**.



3. In the right **Actions** pane, select **New Rule**. The **Rule Type** window displays.



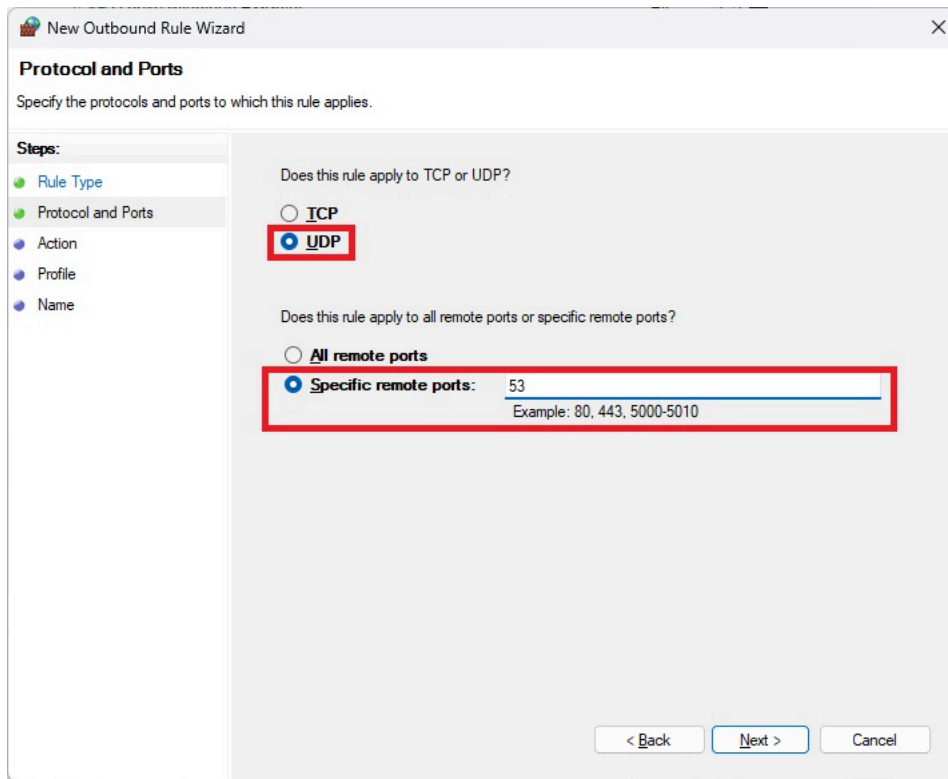
4. You now see the windows related to the **New Outbound Rule Wizard**. In the left pane, you'll see **Protocol and Ports**. Select **Port** and **Next**.





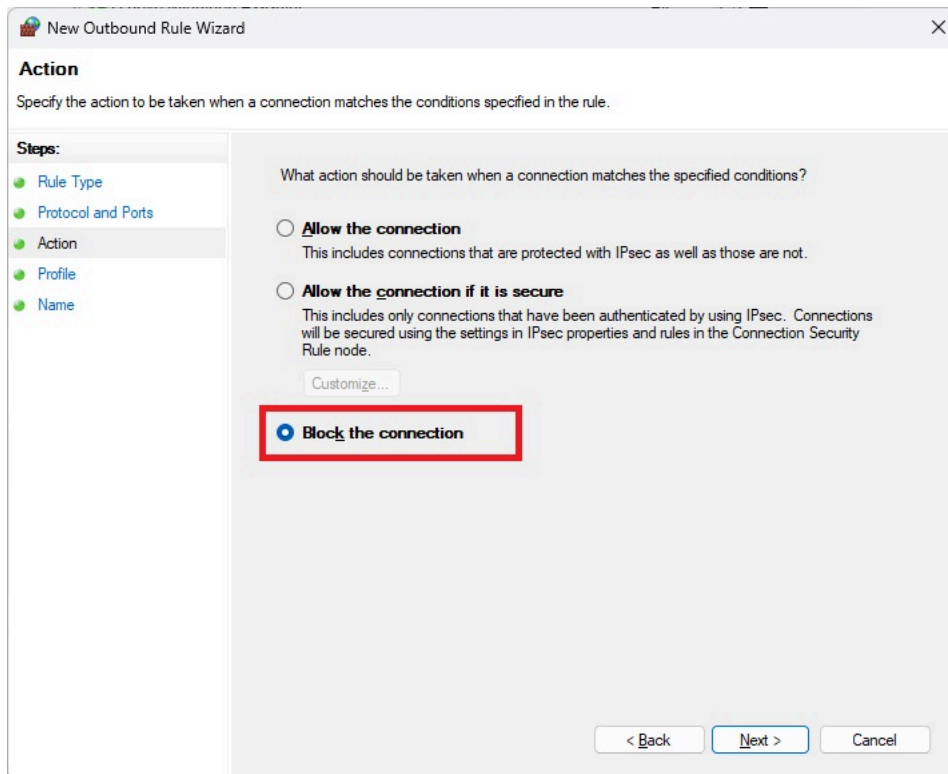
5. Next, select **UDP** radio button as the answer to the question, **Does this rule apply to TCP or UDP?**

6. Select the **Specific remote ports** radio button and type **53** (the port used for DNS requests) in the available text box. Click **Next**.



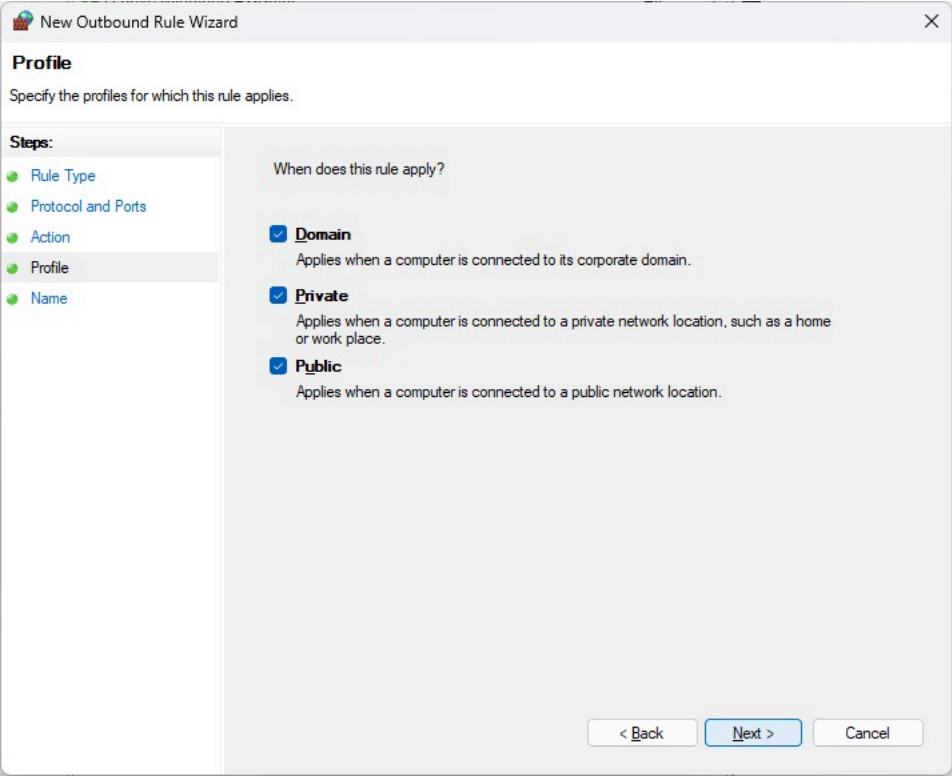
The screenshot shows the 'New Outbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action, Profile, and Name. The main area contains two questions. The first question, 'Does this rule apply to TCP or UDP?', has two radio buttons: 'TCP' and 'UDP'. The 'UDP' button is selected and highlighted with a red rectangle. The second question, 'Does this rule apply to all remote ports or specific remote ports?', also has two radio buttons: 'All remote ports' and 'Specific remote ports'. The 'Specific remote ports' button is selected and highlighted with a red rectangle. Below this button is a text box containing the number '53'. A red rectangle also highlights the text box and the 'Specific remote ports' button. Below the text box is the example text 'Example: 80, 443, 5000-5010'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

7. Next, choose the appropriate action. In this scenario, you want to stop the outbound traffic to the DNS Server. Select the radio button option, **Block the connection**.

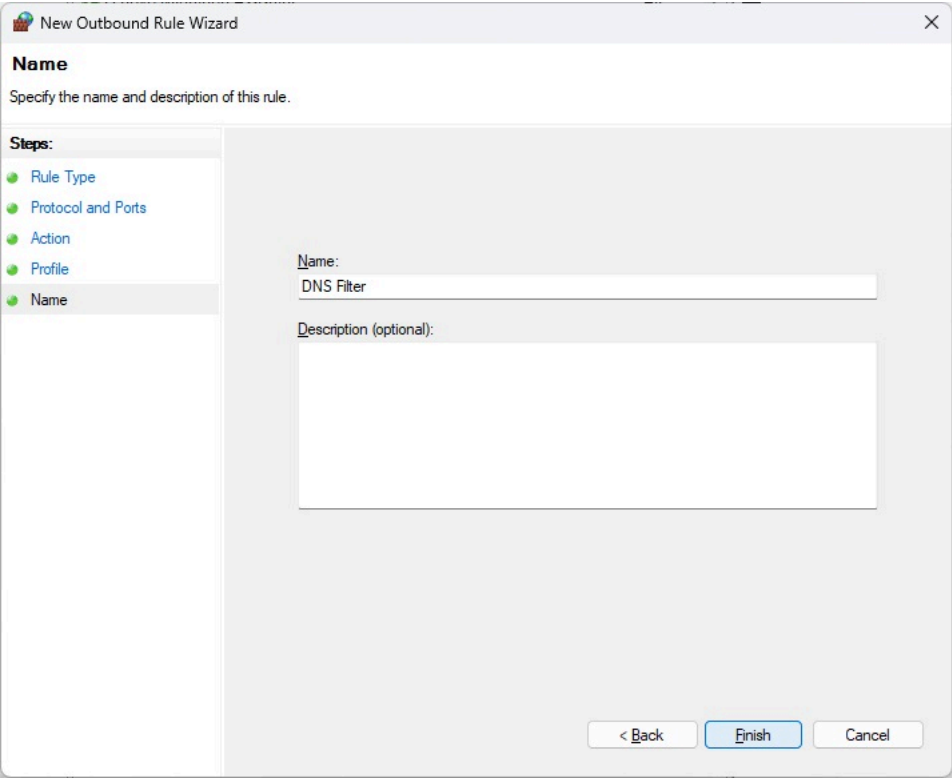


The screenshot shows the 'New Outbound Rule Wizard' window, specifically the 'Action' step. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action, Profile, and Name. The main area contains the question 'What action should be taken when a connection matches the specified conditions?'. There are three radio button options: 'Allow the connection', 'Allow the connection if it is secure', and 'Block the connection'. The 'Block the connection' option is selected and highlighted with a red rectangle. Below the 'Allow the connection' option is a description: 'This includes connections that are protected with IPsec as well as those are not.' Below the 'Allow the connection if it is secure' option is a description: 'This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.' Below the 'Block the connection' option is a 'Customize...' button. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

8. On the **Profiles** window, specify which profiles to apply this rule. Select **Domain**, **Private**, and **Public** options in this example. Select **Next**.

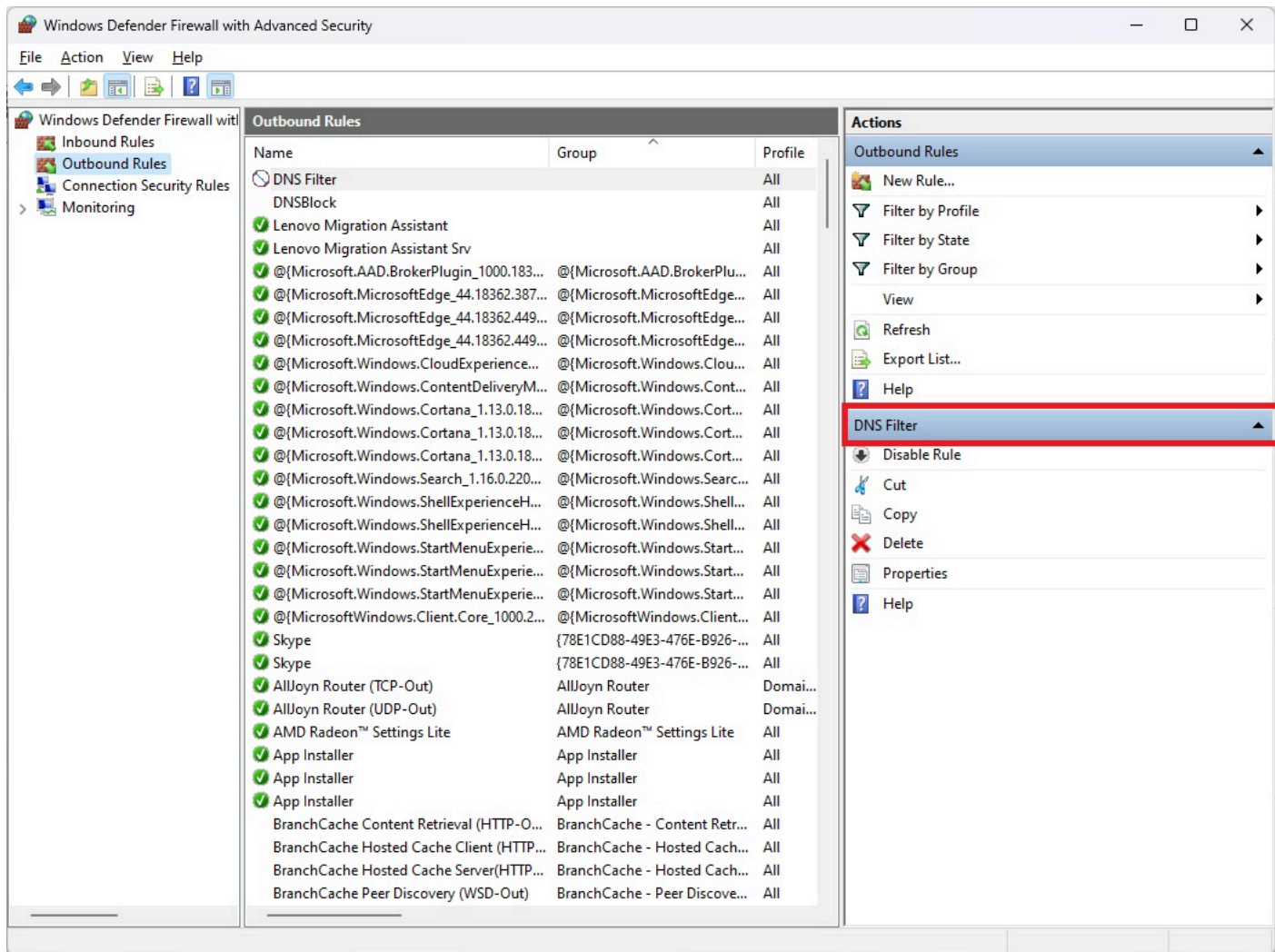


9. On the **Name** window, in the **Name** field, type a meaningful name for your rule, such as *DNS Filter*. Use the optional **Description** field to add more details when needed. Select **Finish**.



**Task 3: Verify the existence and effectiveness of the new DNS Filter rule**

1. On the Windows Defender Firewall window, view the **Actions** pane to verify that you see the *DNS Filter*.



2. Next, open a browser and try to access any website. Users cannot access any website because the rule filters all DNS access.

**Important!** If you try this rule on your computer, remember to disable or remove the rule after completing this exercise.

## Practice Exercises

Next, use these practice exercises to reinforce your learning.

### Exercise 1: Block DNS requests to specific IP addresses

**Problem Statement:** Block DNS requests to a specific DNS server's IP address, such as Google's public DNS server 8.8.8.8.

**Hint:** You will need to create an outbound rule in Windows Firewall to block traffic to the specific IP address on port 53 (DNS).

► [Click here for the solution](#)

### Exercise 2: Allow DNS requests only to specific IP addresses

**Problem Statement:** Allow DNS requests only to a specific DNS server, such as Cloudflare's DNS server 1.1.1.1, and block all other DNS servers.

**Hint:** You will need to create outbound rules to allow traffic only to the specific IP address on port 53 and block all other traffic on port 53.

► [Click here for the solution](#)

## Conclusion

You now can locate Windows Defender Firewall settings within the **Control Panel** and **Systems and Security**. You now know how to locate the **Outbound Rules** and create outbound rules, specifically how to create outbound rules that block access to external websites.

### Author

Dr. Manish Kumar



# Skills Network