DNS Filtering

Introduction

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

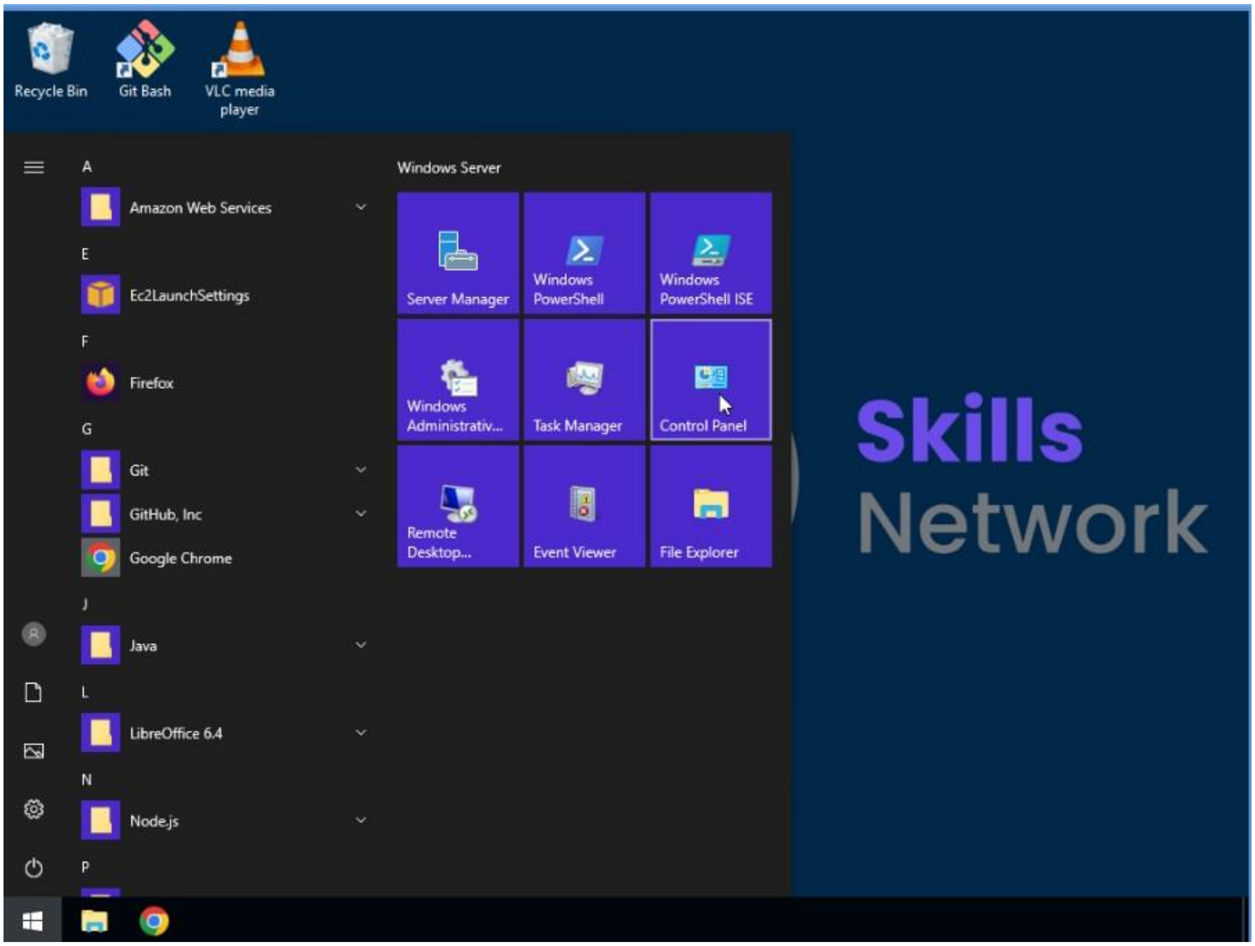
Objectives

After completing this project, 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.

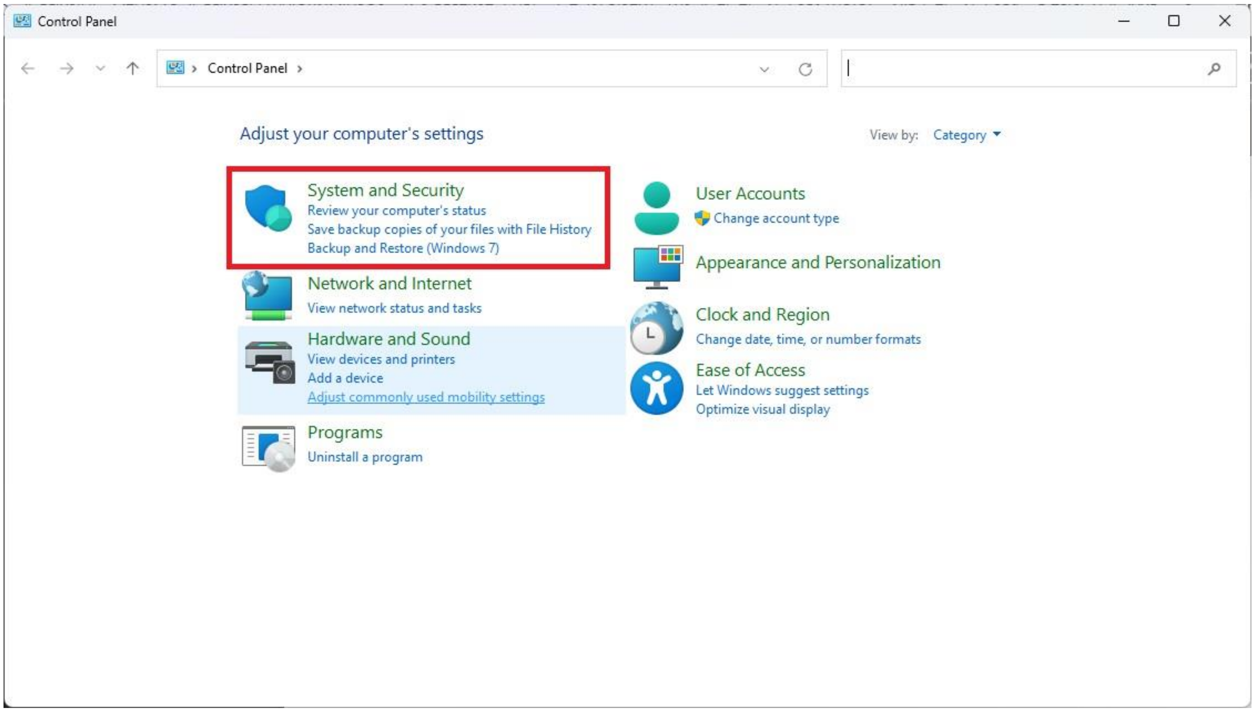
Task 1: Navigate to the Microsoft Windows Firewall interface

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

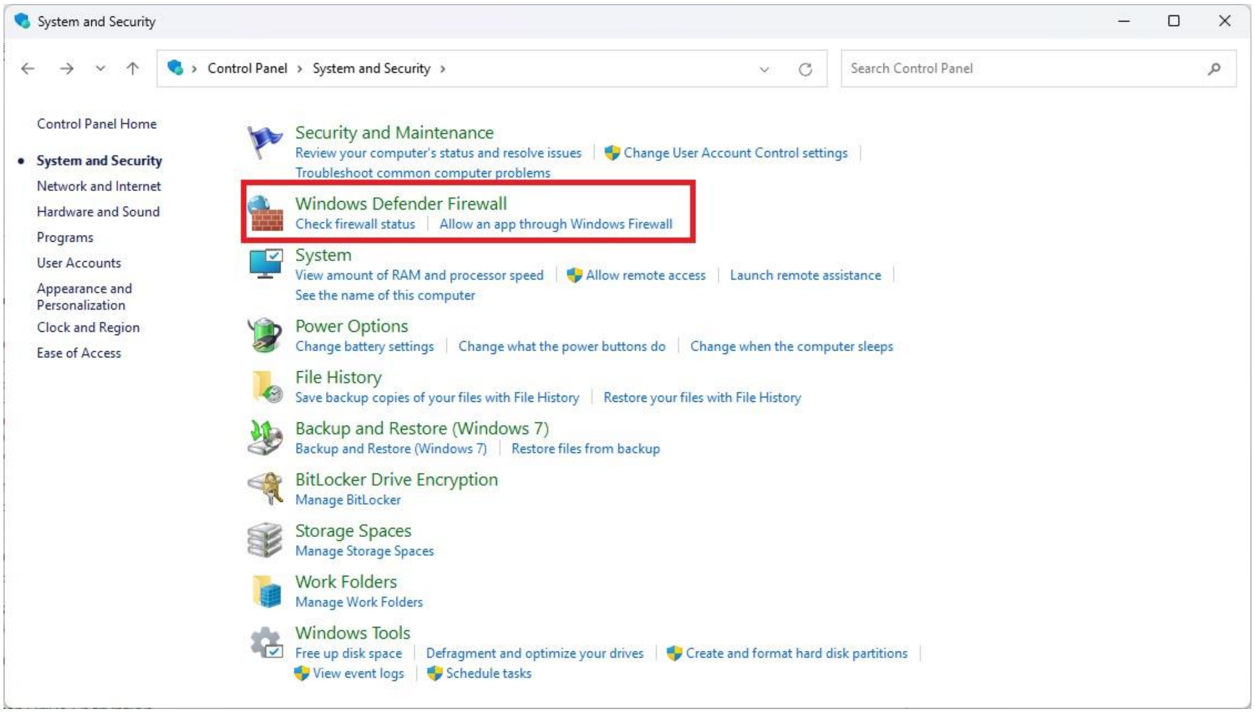


2. Click on **Control Panel**.

3. Select **System and Security**.

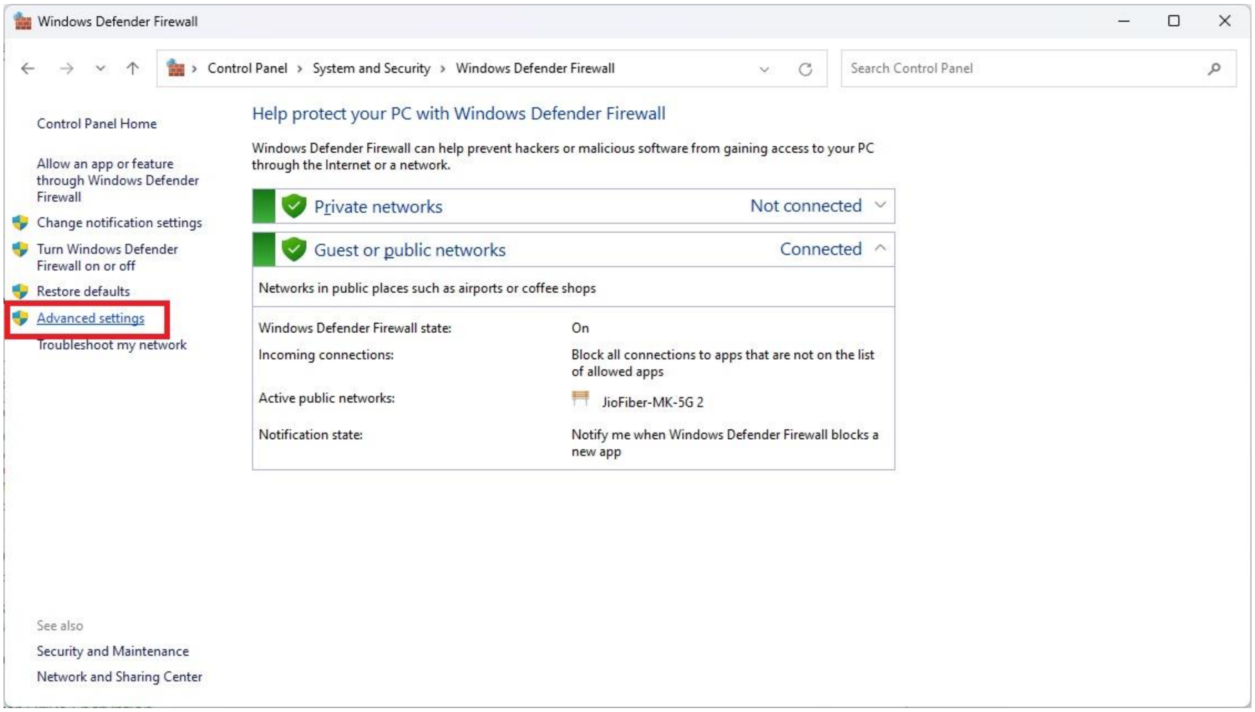

Control Panel
Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalization
Clock and Region
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display

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


System and Security
Control Panel > System and Security >
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock and Region
Ease of Access
Security and Maintenance
Review your computer's status and resolve issues
Change User Account Control settings
Troubleshoot common computer problems
Windows Defender Firewall
Check firewall status
Allow an app through Windows Firewall
System
View amount of RAM and processor speed
Allow remote access
Launch remote assistance
See the name of this computer
Power Options
Change battery settings
Change what the power buttons do
Change when the computer sleeps
File History
Save backup copies of your files with File History
Restore your files with File History
Backup and Restore (Windows 7)
Backup and Restore (Windows 7)
Restore files from backup
BitLocker Drive Encryption
Manage BitLocker
Storage Spaces
Manage Storage Spaces
Work Folders
Manage Work Folders
Windows Tools
Free up disk space
Defragment and optimize your drives
Create and format hard disk partitions
View event logs
Schedule tasks

Task 2: Create a new outbound rule

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



Windows Defender Firewall

Control Panel > System and Security > Windows Defender Firewall

Search Control Panel

Control Panel Home

Allow an app or feature through Windows Defender Firewall

Change notification settings

Turn Windows Defender Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

See also

Security and Maintenance

Network and Sharing Center

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

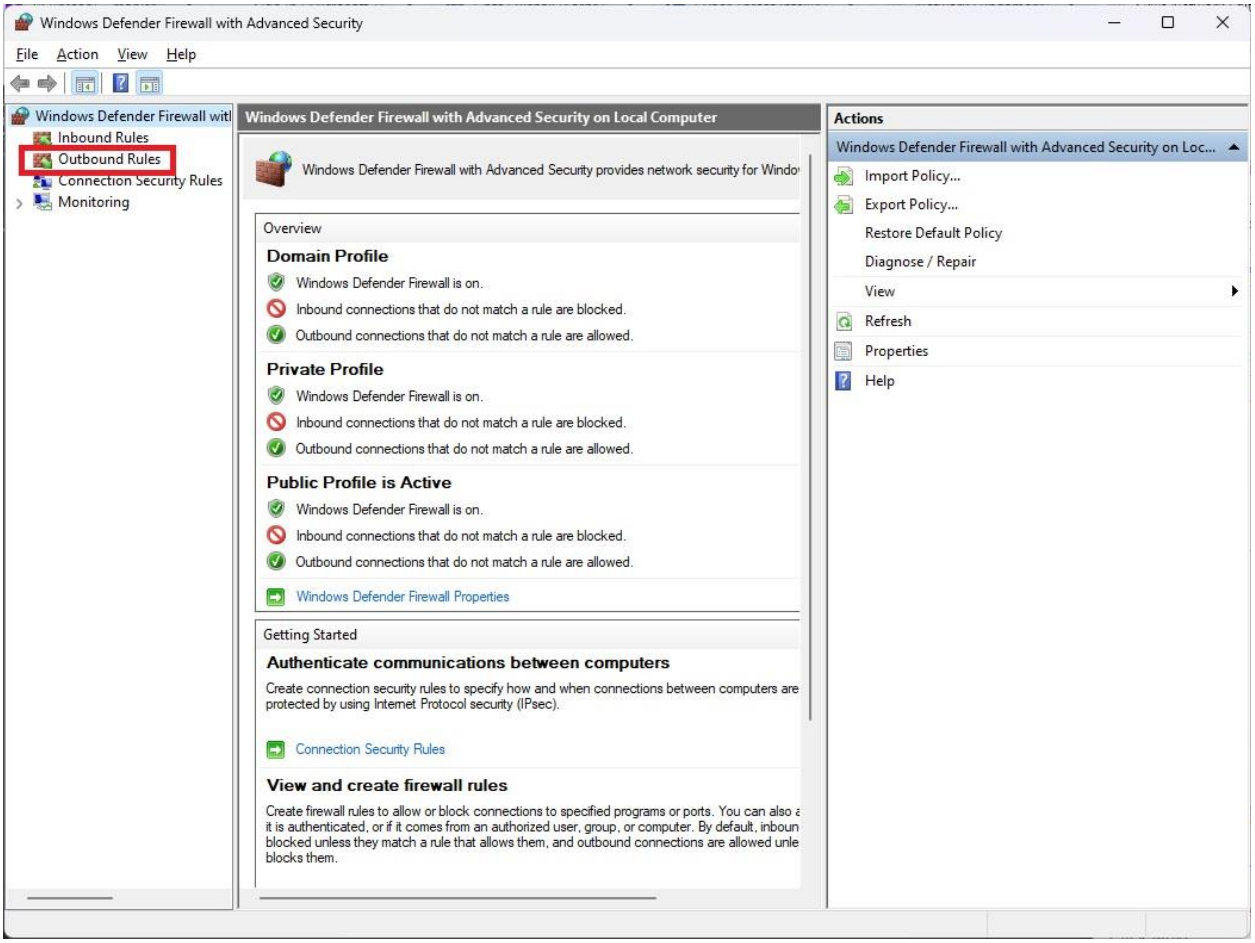
Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	JioFiber-MK-5G 2
Notification state:	Notify me when Windows Defender Firewall blocks a new app

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



Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Actions
Windows Defender Firewall with Advanced Security on Loc...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help

Windows Defender Firewall with Advanced Security provides network security for Windo

Overview

Domain Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile is Active

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

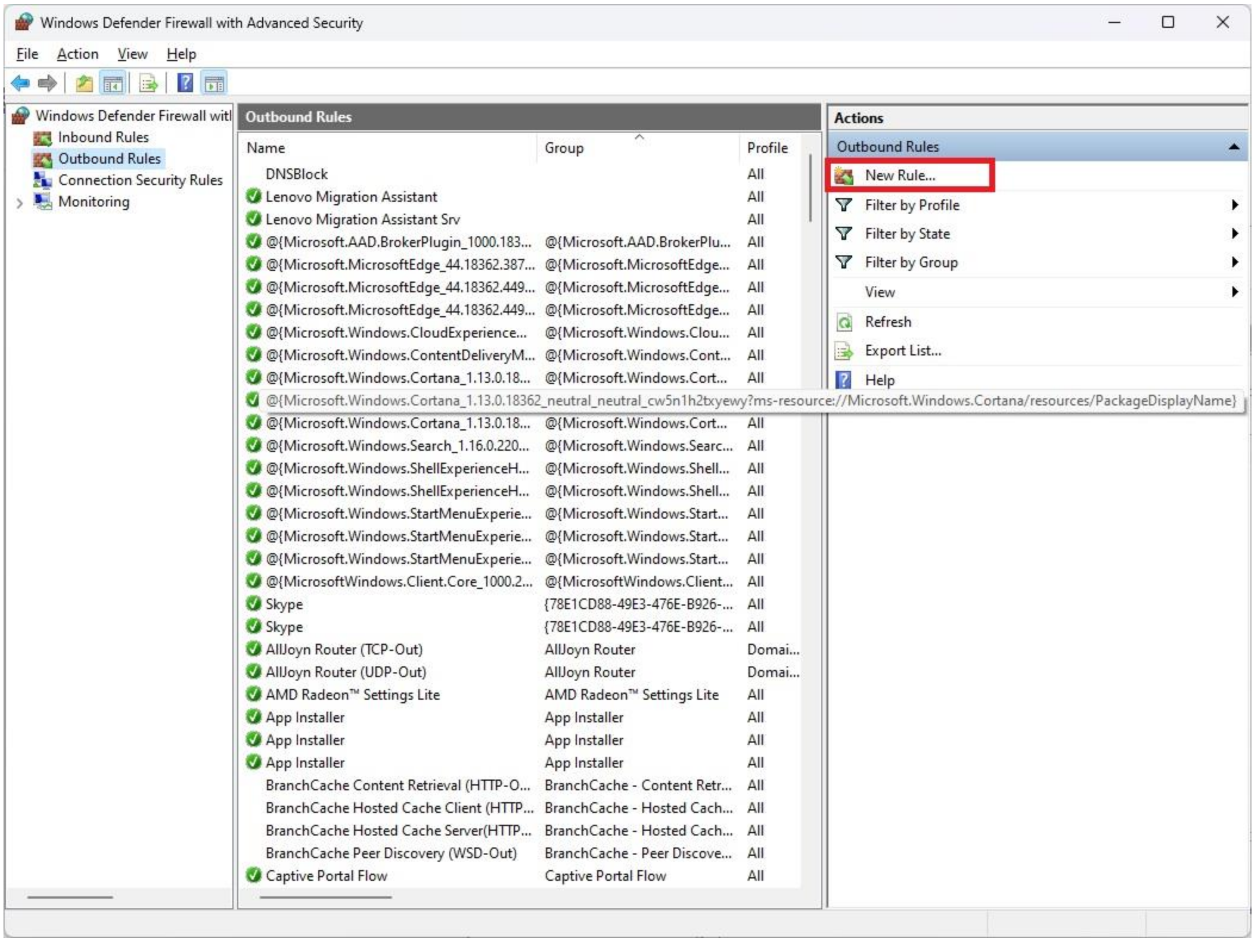
Create connection security rules to specify how and when connections between computers are protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

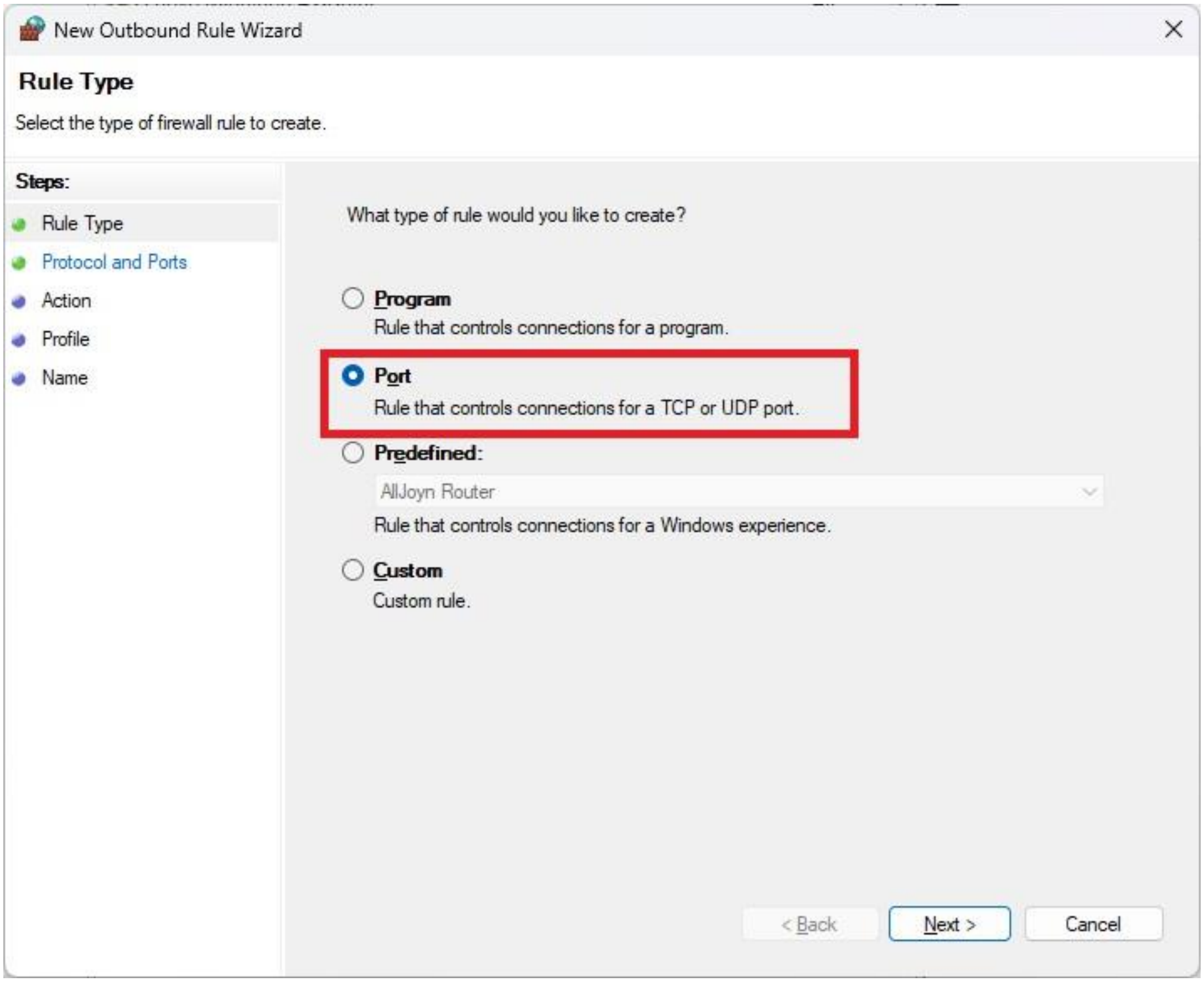
Create firewall rules to allow or block connections to specified programs or ports. You can also a it is authenticated, or if it comes from an authorized user, group, or computer. By default, inboun blocked unless they match a rule that allows them, and outbound connections are allowed unle blocks them.

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



Name	Group	Profile
DNSBlock		All
✓ Lenovo Migration Assistant		All
✓ Lenovo Migration Assistant Srv		All
✓ @{Microsoft.AAD.BrokerPlugin_1000.183...	@{Microsoft.AAD.BrokerPlu...	All
✓ @{Microsoft.MicrosoftEdge_44.18362.387...	@{Microsoft.MicrosoftEdge...	All
✓ @{Microsoft.MicrosoftEdge_44.18362.449...	@{Microsoft.MicrosoftEdge...	All
✓ @{Microsoft.MicrosoftEdge_44.18362.449...	@{Microsoft.MicrosoftEdge...	All
✓ @{Microsoft.Windows.CloudExperience...	@{Microsoft.Windows.Clou...	All
✓ @{Microsoft.Windows.ContentDeliveryM...	@{Microsoft.Windows.Cont...	All
✓ @{Microsoft.Windows.Cortana_1.13.0.18...	@{Microsoft.Windows.Cort...	All
✓ @{Microsoft.Windows.Cortana_1.13.0.18362_neutral_neutral_cw5n1h2txyewy?ms-resource://Microsoft.Windows.Cortana/resources/PackageDisplayName}		
✓ @{Microsoft.Windows.Cortana_1.13.0.18...	@{Microsoft.Windows.Cort...	All
✓ @{Microsoft.Windows.Search_1.16.0.220...	@{Microsoft.Windows.Searc...	All
✓ @{Microsoft.Windows.ShellExperienceH...	@{Microsoft.Windows.Shell...	All
✓ @{Microsoft.Windows.ShellExperienceH...	@{Microsoft.Windows.Shell...	All
✓ @{Microsoft.Windows.StartMenuExperie...	@{Microsoft.Windows.Start...	All
✓ @{Microsoft.Windows.StartMenuExperie...	@{Microsoft.Windows.Start...	All
✓ @{Microsoft.Windows.StartMenuExperie...	@{Microsoft.Windows.Start...	All
✓ @{MicrosoftWindows.Client.Core_1000.2...	@{MicrosoftWindows.Client...	All
✓ Skype	{78E1CD88-49E3-476E-B926-...	All
✓ Skype	{78E1CD88-49E3-476E-B926-...	All
✓ AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...
✓ AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...
✓ AMD Radeon™ Settings Lite	AMD Radeon™ Settings Lite	All
✓ App Installer	App Installer	All
✓ App Installer	App Installer	All
✓ App Installer	App Installer	All
BranchCache Content Retrieval (HTTP-O...	BranchCache - Content Retr...	All
BranchCache Hosted Cache Client (HTTP...	BranchCache - Hosted Cach...	All
BranchCache Hosted Cache Server(HTTP...	BranchCache - Hosted Cach...	All
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	All
✓ Captive Portal Flow	Captive Portal Flow	All

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**.



New Outbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

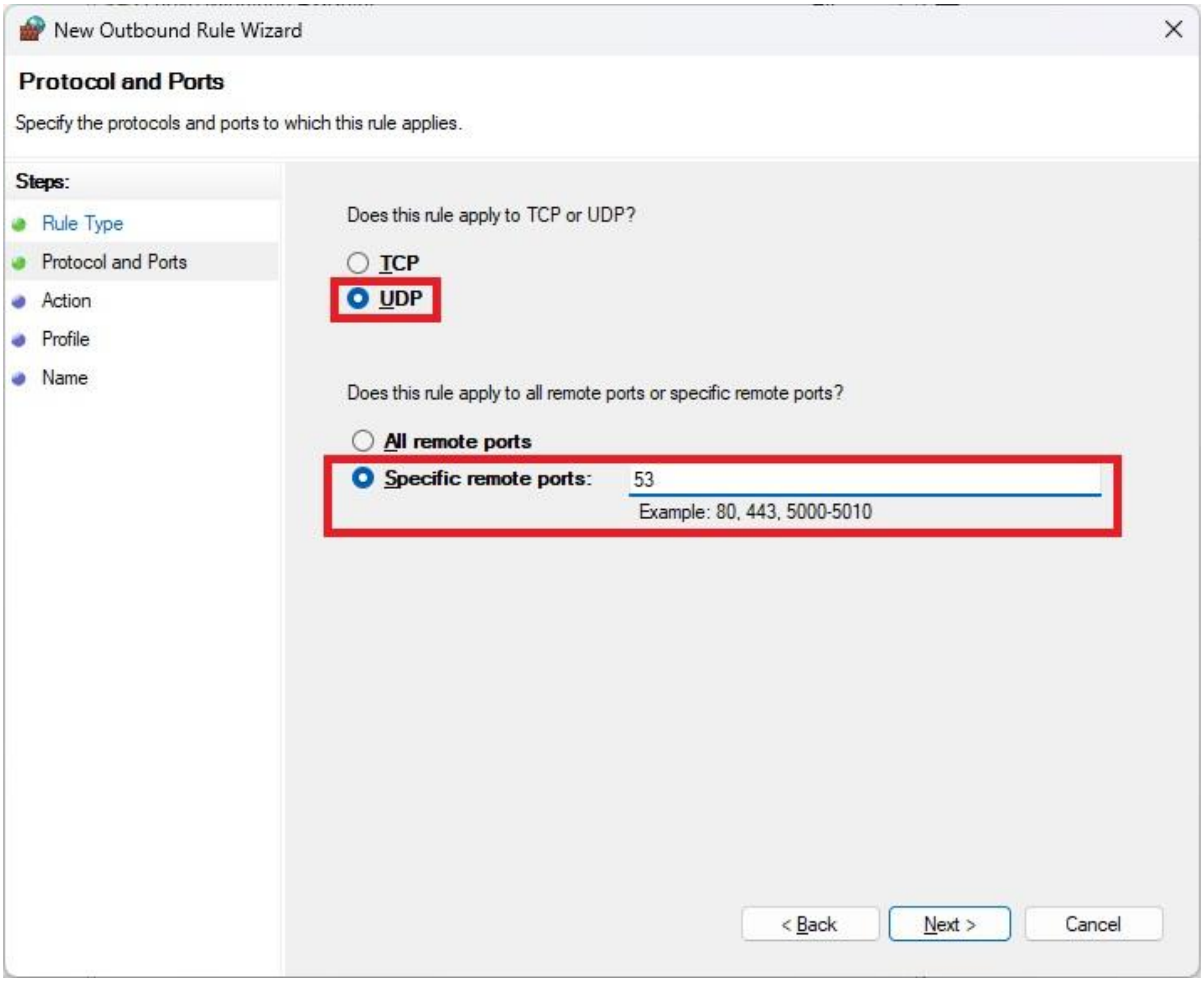
○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

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**.



New Outbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

○ TCP

● UDP

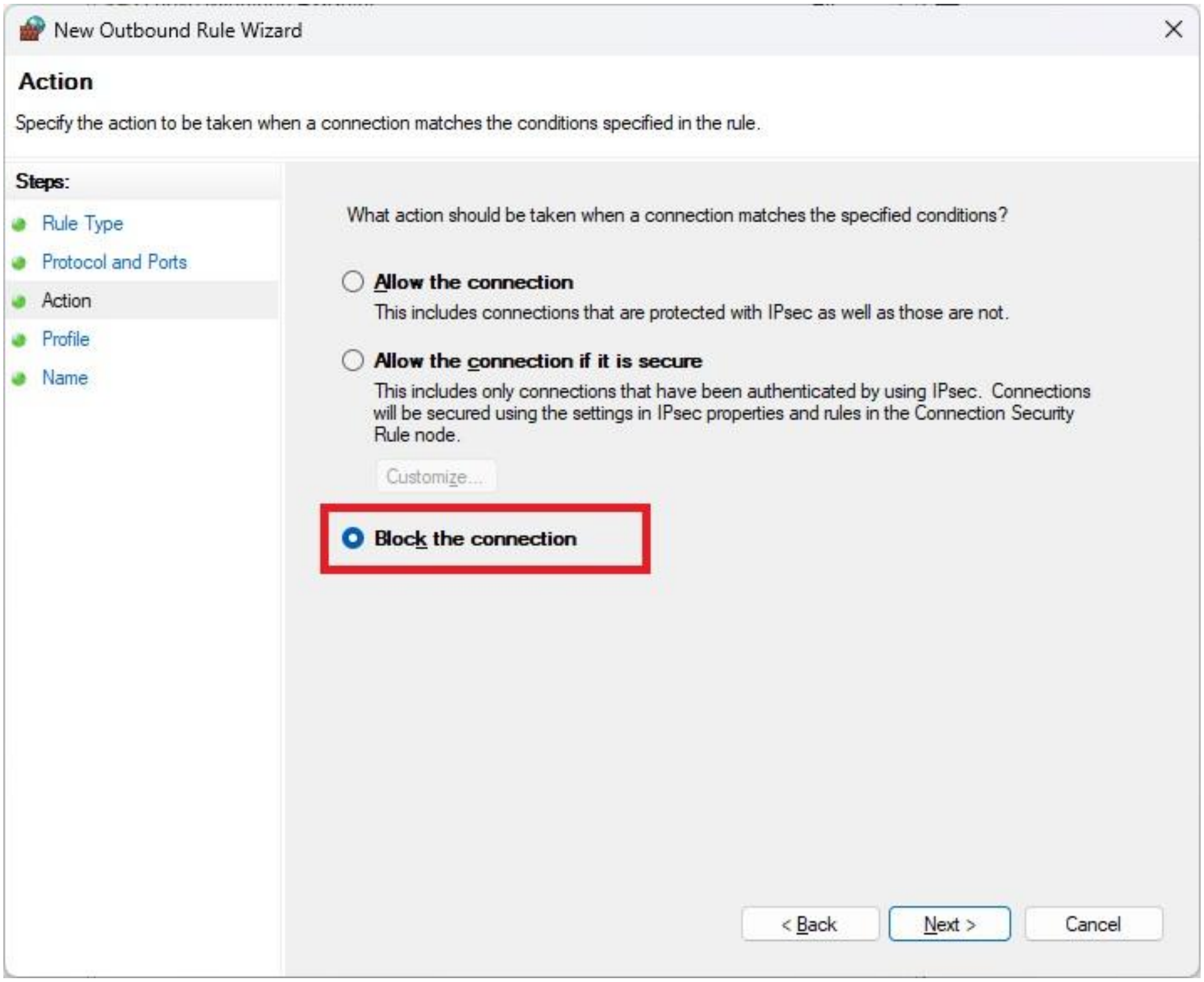
Does this rule apply to all remote ports or specific remote ports?

○ **All remote ports**

● **Specific remote ports:** 53

Example: 80, 443, 5000-5010

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**.



New Outbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

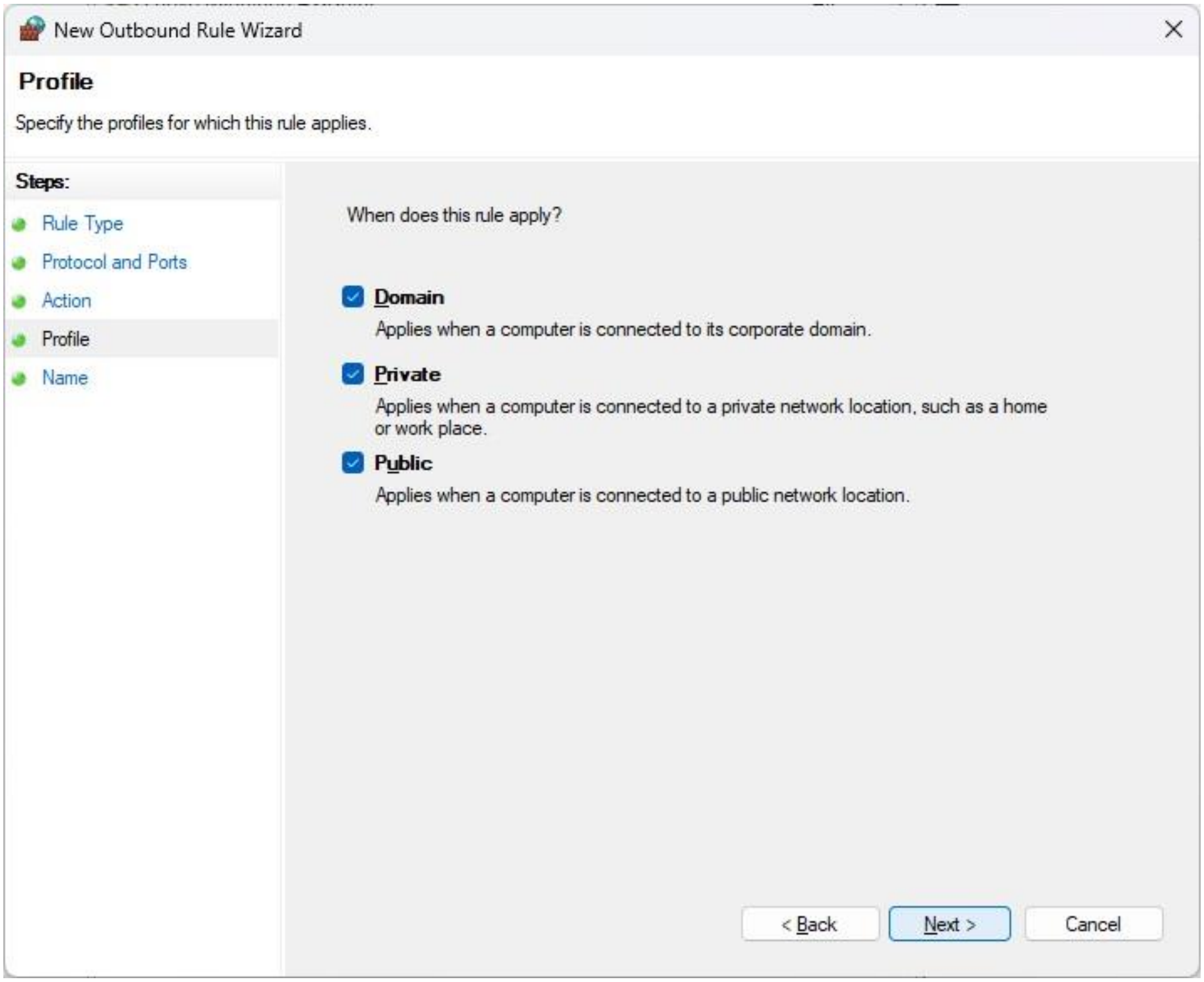
What action should be taken when a connection matches the specified conditions?

○ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
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.

● **Block the connection**

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



New Outbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

When does this rule apply?

☑ Domain

Applies when a computer is connected to its corporate domain.

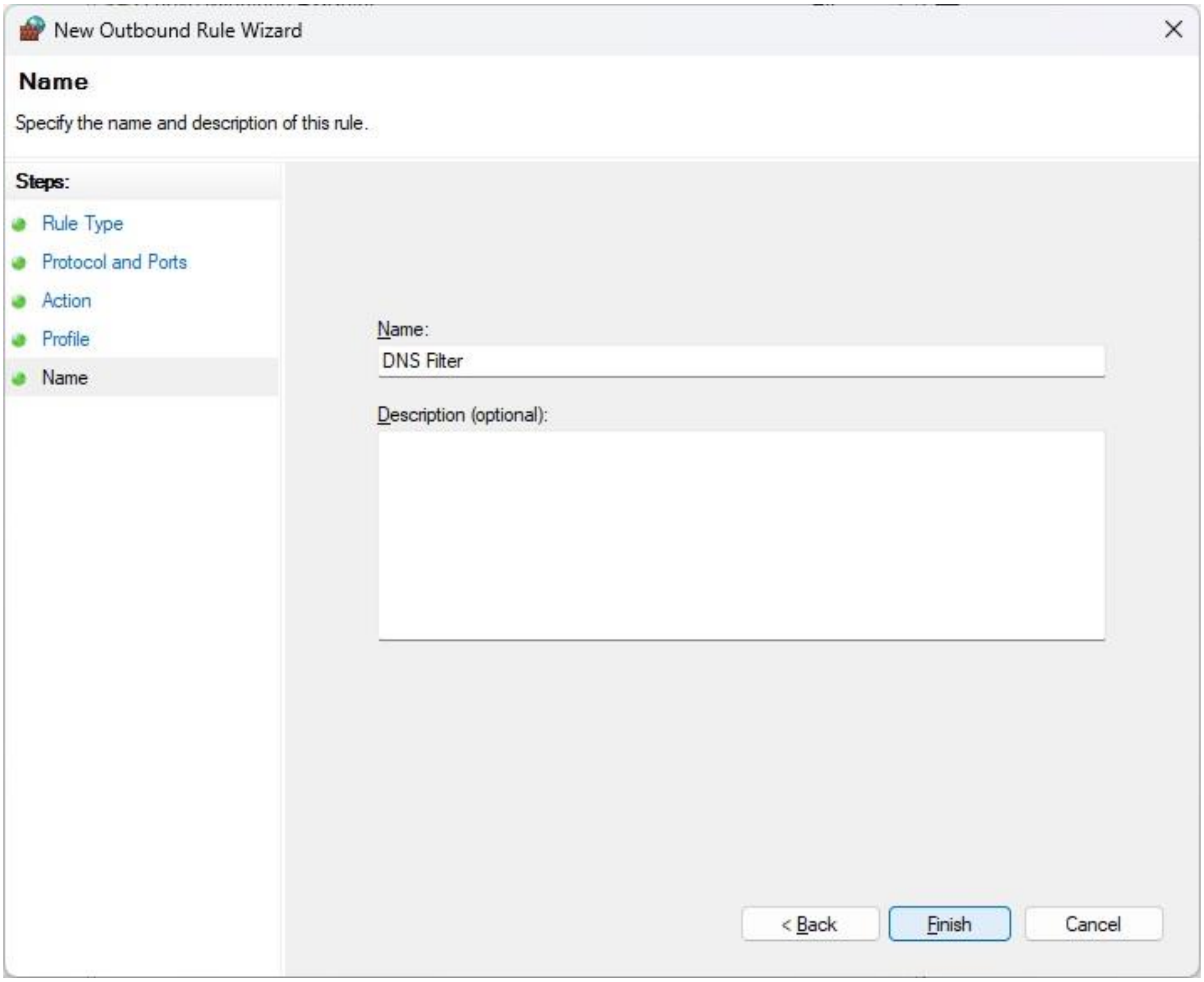
☑ Private

Applies when a computer is connected to a private network location, such as a home or work place.

☑ Public

Applies when a computer is connected to a public network location.

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**.

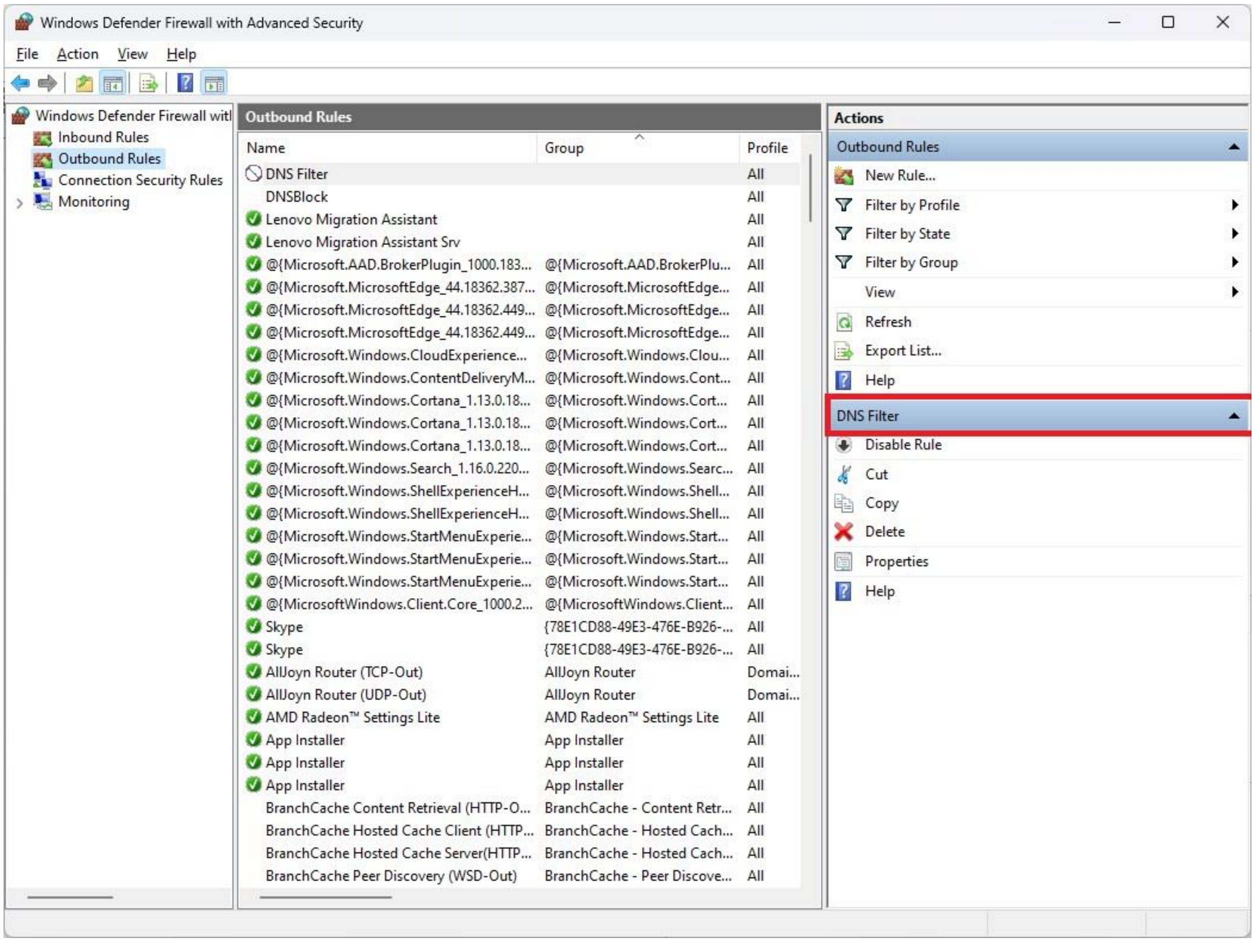


Name: DNS Filter

Description (optional):

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*.



Name	Group	Profile
DNS Filter		All
DNSBlock		All
Lenovo Migration Assistant		All
Lenovo Migration Assistant Srv		All
@{Microsoft.AAD.BrokerPlugin_1000.183...	@{Microsoft.AAD.BrokerPlu...	All
@{Microsoft.MicrosoftEdge_44.18362.387...	@{Microsoft.MicrosoftEdge...	All
@{Microsoft.MicrosoftEdge_44.18362.449...	@{Microsoft.MicrosoftEdge...	All
@{Microsoft.MicrosoftEdge_44.18362.449...	@{Microsoft.MicrosoftEdge...	All
@{Microsoft.Windows.CloudExperience...	@{Microsoft.Windows.Clou...	All
@{Microsoft.Windows.ContentDeliveryM...	@{Microsoft.Windows.Cont...	All
@{Microsoft.Windows.Cortana_1.13.0.18...	@{Microsoft.Windows.Cort...	All
@{Microsoft.Windows.Cortana_1.13.0.18...	@{Microsoft.Windows.Cort...	All
@{Microsoft.Windows.Cortana_1.13.0.18...	@{Microsoft.Windows.Cort...	All
@{Microsoft.Windows.Search_1.16.0.220...	@{Microsoft.Windows.Searc...	All
@{Microsoft.Windows.ShellExperienceH...	@{Microsoft.Windows.Shell...	All
@{Microsoft.Windows.ShellExperienceH...	@{Microsoft.Windows.Shell...	All
@{Microsoft.Windows.StartMenuExperie...	@{Microsoft.Windows.Start...	All
@{Microsoft.Windows.StartMenuExperie...	@{Microsoft.Windows.Start...	All
@{Microsoft.Windows.StartMenuExperie...	@{Microsoft.Windows.Start...	All
@{MicrosoftWindows.Client.Core_1000.2...	@{MicrosoftWindows.Client...	All
Skype	{78E1CD88-49E3-476E-B926-...	All
Skype	{78E1CD88-49E3-476E-B926-...	All
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...
AMD Radeon™ Settings Lite	AMD Radeon™ Settings Lite	All
App Installer	App Installer	All
App Installer	App Installer	All
App Installer	App Installer	All
BranchCache Content Retrieval (HTTP-O...	BranchCache - Content Retr...	All
BranchCache Hosted Cache Client (HTTP...	BranchCache - Hosted Cach...	All
BranchCache Hosted Cache Server(HTTP...	BranchCache - Hosted Cach...	All
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	All

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

Conclusion

This hands-on project guide provided a foundational understanding of creating and managing outbound rules in Windows Defender Firewall to enhance network security. By focusing on DNS traffic control, you developed essential skills to manage network traffic effectively and protect systems from potential security threats.

Key Outcomes:

1. **Locating Windows Defender Firewall Settings:**
    a. Navigated through the Control Panel to access the advanced settings of Windows Defender Firewall.

    b. Understood the structure and purpose of outbound rules in network security.

2. **Creating Outbound Rules to Block DNS Traffic:**
    a. Configured an outbound rule to block DNS requests by targeting UDP traffic on port 53.
    b. Applied the rule across all network profiles (Domain, Private, and Public) to ensure comprehensive coverage.
    c. Assigned meaningful names and descriptions to the rules for easy identification and management.
3. **Verifying Rule Effectiveness:**
    a. Successfully tested the rule by attempting to access websites, confirming that DNS requests were blocked.
    b. Gained insights into troubleshooting and verifying rule behavior using Windows Defender Firewall.
4. **Practice Exercises for Advanced Scenarios:**
    a. **Exercise 1:** Explored how to block DNS traffic to specific IP addresses (e.g., Google's public DNS server 8.8.8.8).
    b. **Exercise 2:** Learned to allow DNS traffic only to specific servers (e.g., Cloudflare's DNS server 1.1.1.1) while blocking all others, demonstrating a fine-grained approach to traffic control.

Key Takeaways:

- **Granular Traffic Management:** Windows Defender Firewall enables precise control over DNS traffic, allowing administrators to permit or restrict access to specific servers.
- **Enhanced Security Posture:** Blocking unauthorized DNS requests mitigates the risk of DNS-based attacks and unauthorized network traffic.
- **Importance of Cleanup:** After testing, removing or disabling temporary rules ensures no unintended impact on network functionality.

By mastering these configurations, users can apply DNS filtering techniques to safeguard network integrity and enforce organizational security policies.