BICOL UNIVERSITY
POLANGUI
Polangui, Albay

IT 123 – System Administration and Maintenance

1^{st} Semester 2025-2026

Week 10 Laboratory – Firewall and VPN Configuration

John Omar C. Clutario
Simone Andreas M. Mannhuel M. Nate
Joshua A. Obstaculo
BSIT – 4B

Guillermo V. Red, DIT
Instructor

Lab Objectives:

• Understand how to configure and manage firewall rules in Windows Defender Firewall.

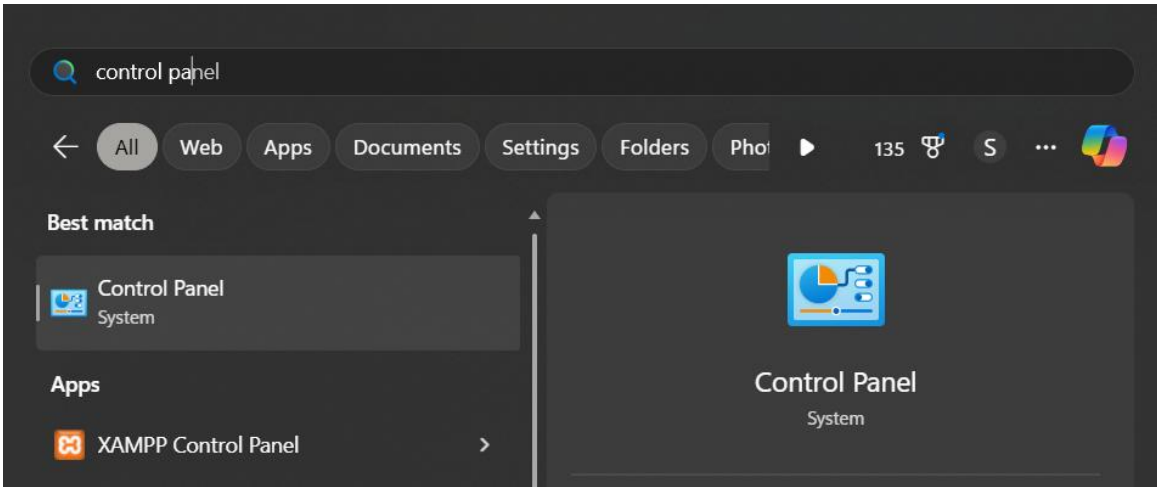
• Learn to set up and manage a Virtual Private Network (VPN) connection in Windows OS.

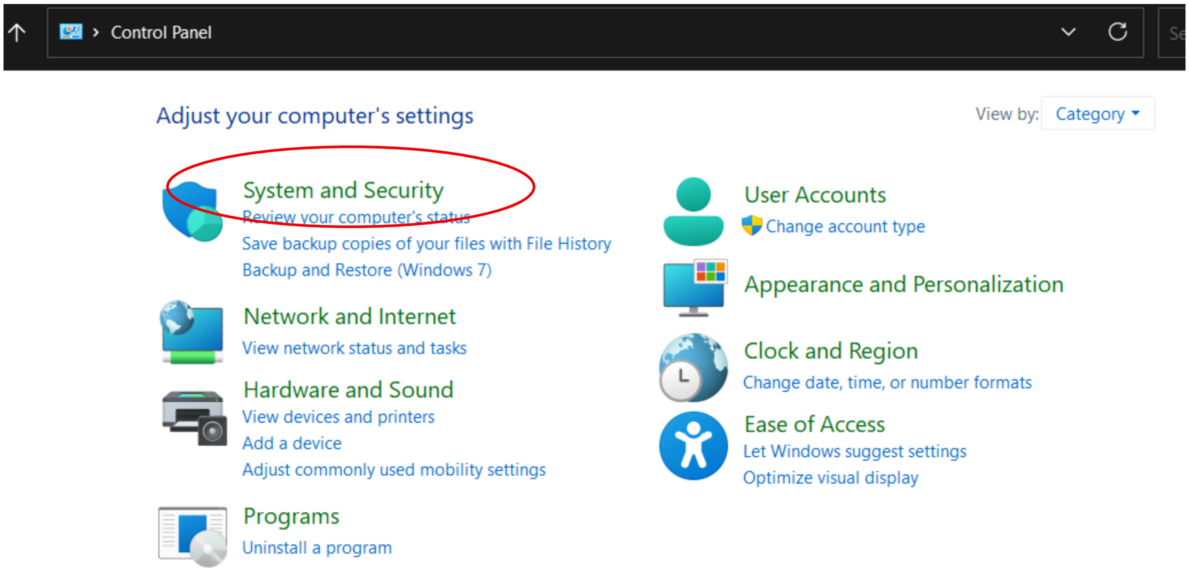
• Gain hands-on experience with securing a Windows environment.

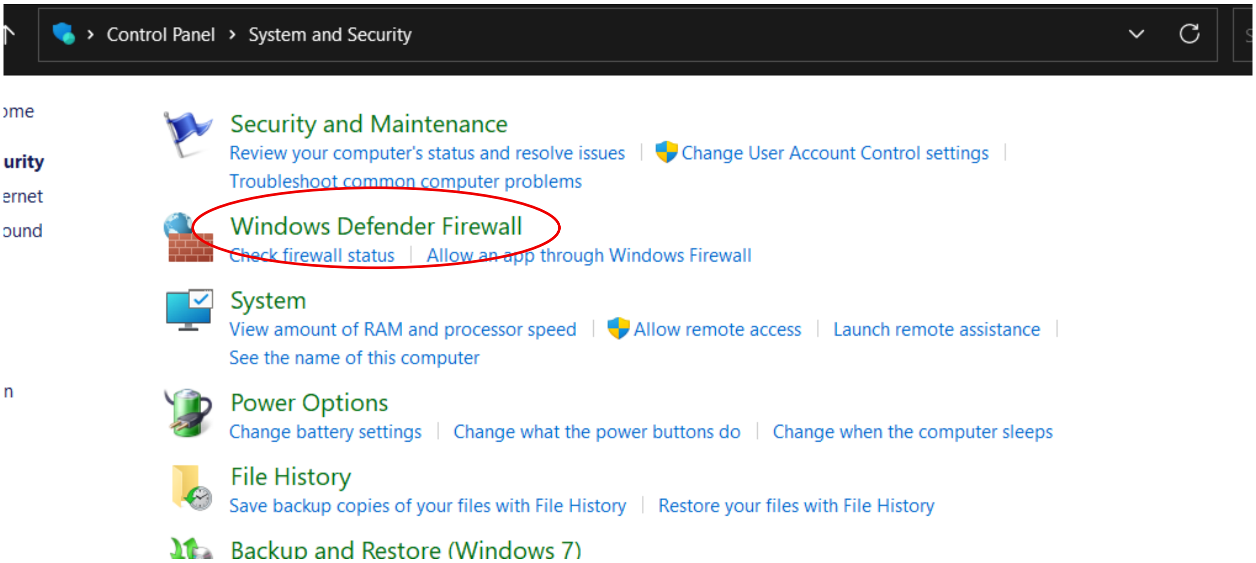
Step 1:

1. Open the Control Panel.

2. Navigate to System and Security → Windows Defender Firewall.




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



Control Panel › System and Security

ome
urity
ernet
ound
n

Security and Maintenance
Review your computer's status and resolve issues | Change User Account Control settings | Troubleshoot common computer problems

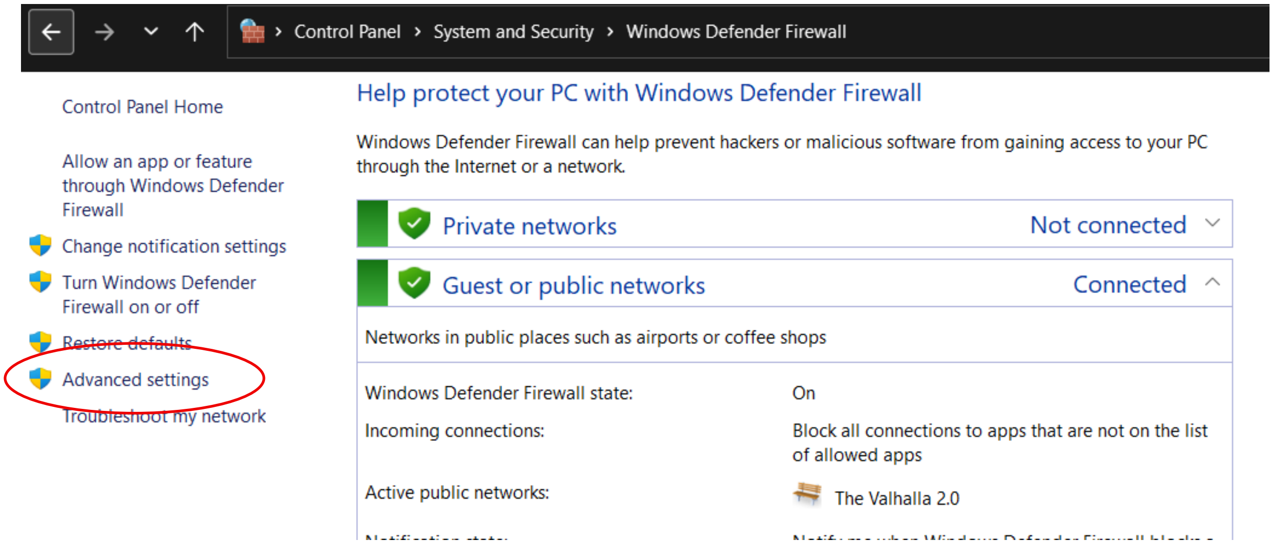
Windows Defender Firewall
Check firewall status | Allow an app through Windows Firewall

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)



Control Panel › System and Security › Windows Defender Firewall

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

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.

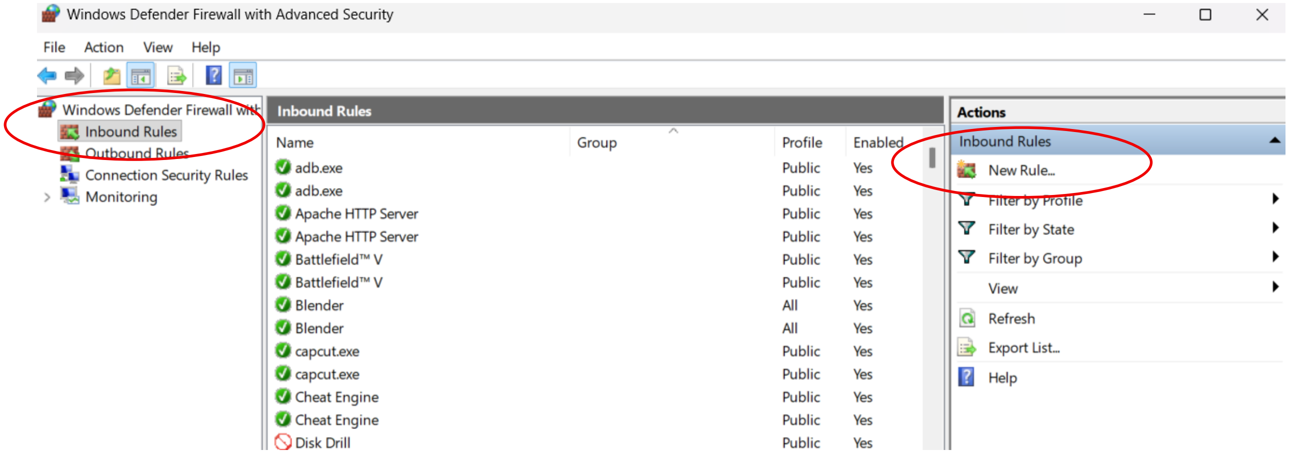
Private networks — Not connected

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:	The Valhalla 2.0

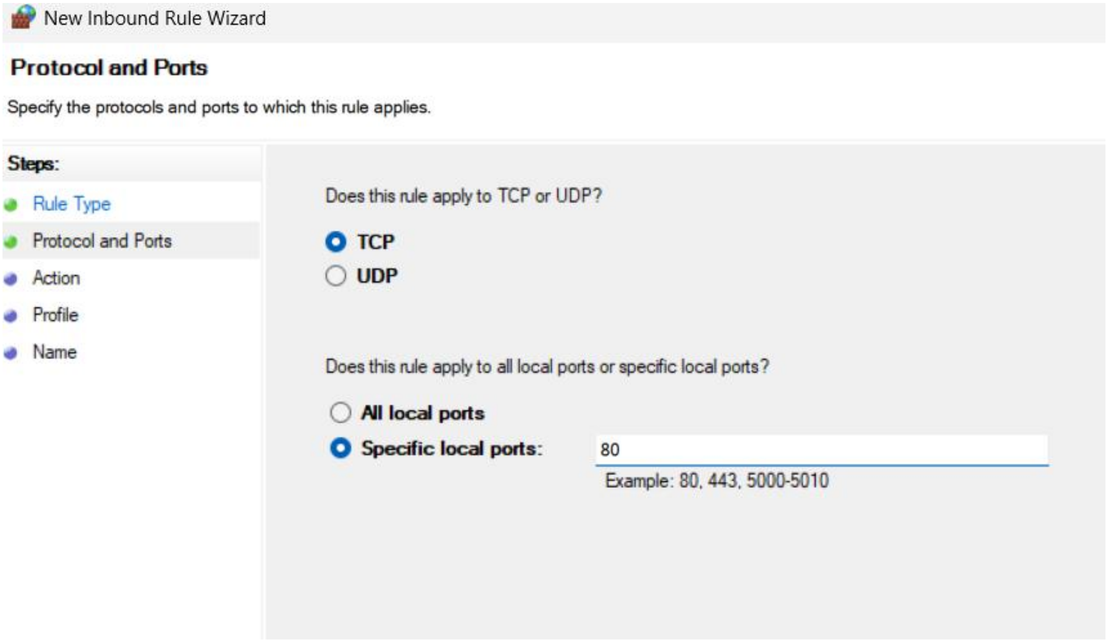
Step 2: Create an Inbound Rule



Windows Defender Firewall with Advanced Security

Inbound Rules

Name	Group	Profile	Enabled
adb.exe		Public	Yes
adb.exe		Public	Yes
Apache HTTP Server		Public	Yes
Apache HTTP Server		Public	Yes
Battlefield™ V		Public	Yes
Battlefield™ V		Public	Yes
Blender		All	Yes
Blender		All	Yes
capcut.exe		Public	Yes
capcut.exe		Public	Yes
Cheat Engine		Public	Yes
Cheat Engine		Public	Yes
Disk Drill		Public	Yes



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

● **TCP**

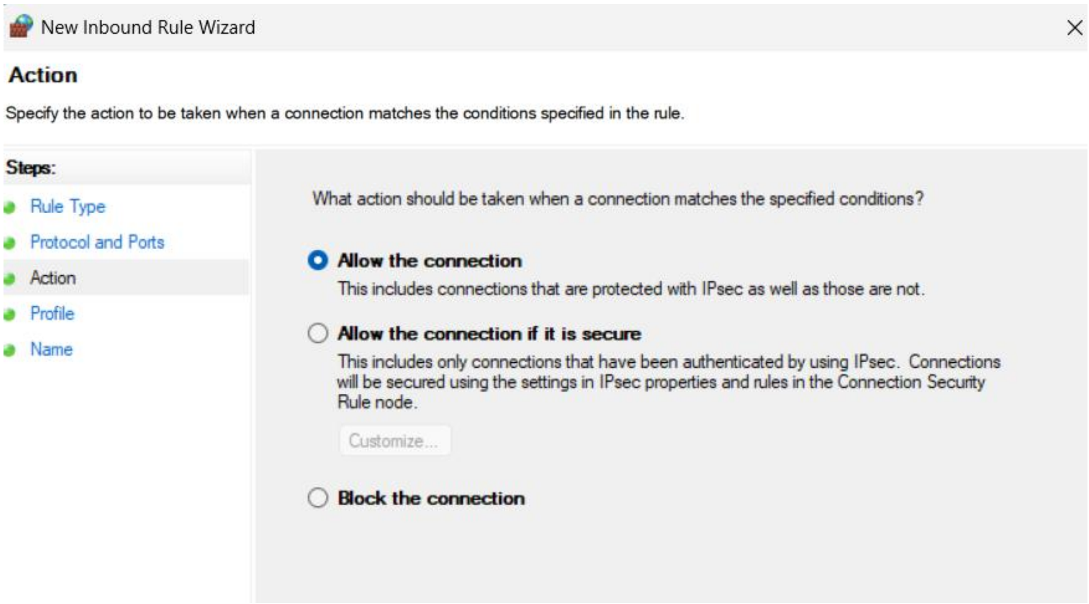
○ **UDP**

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

○ **All local ports**

● **Specific local ports:** 80

Example: 80, 443, 5000-5010



New Inbound Rule Wizard

Action

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

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

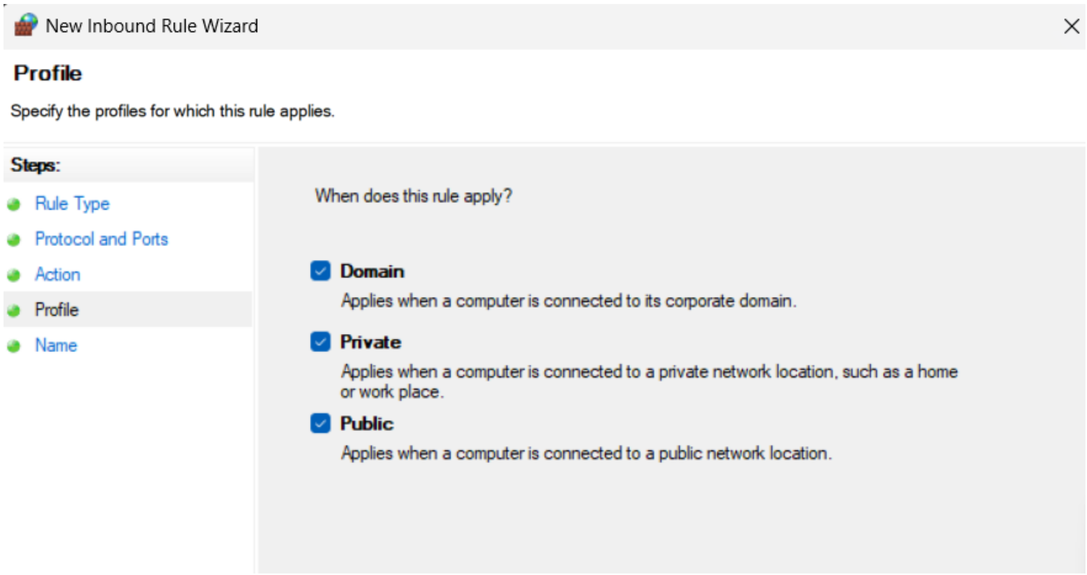
● **Allow the connection**

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**



New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

When does this rule apply?

☑ **Domain**

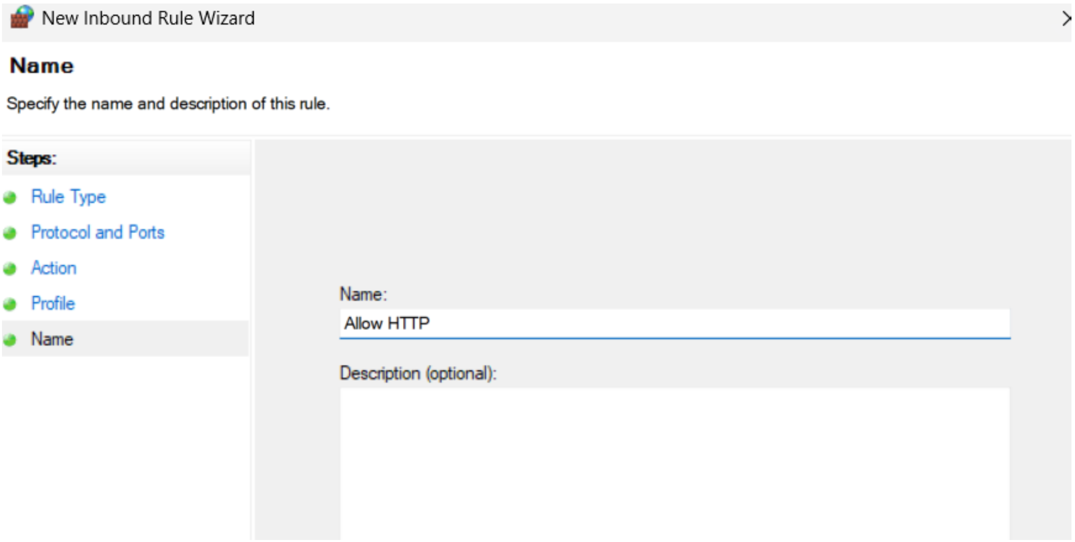
Applies when a computer is connected to its corporate domain.

☑ **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.



New Inbound Rule Wizard

Name

Specify the name and description of this rule.

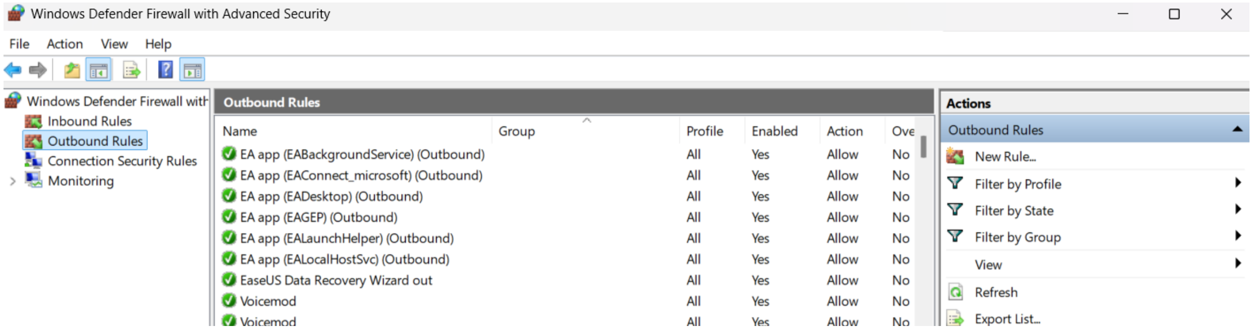
Steps:

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

Name: Allow HTTP

Description (optional):

Step 3: Create an Outbound Rule



Windows Defender Firewall with Advanced Security

- Windows Defender Firewall with
  - Inbound Rules
  - Outbound Rules
  - Connection Security Rules
  - Monitoring

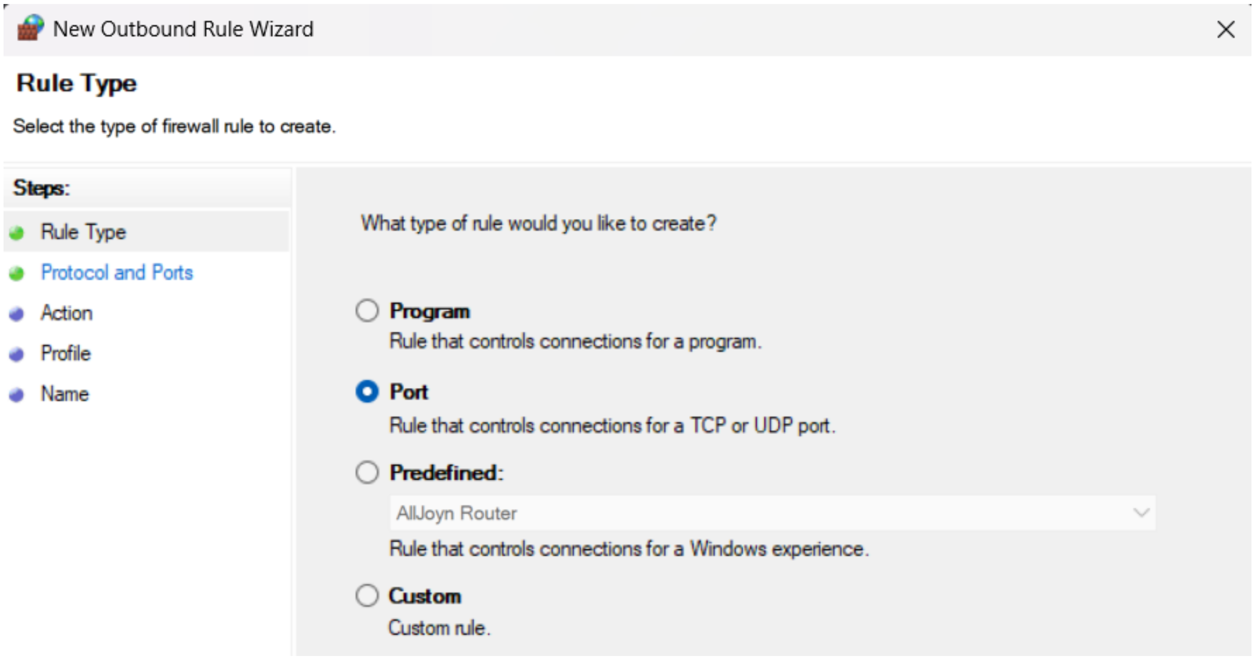
Outbound Rules

Name	Group	Profile	Enabled	Action	Ove
✓ EA app (EABackgroundService) (Outbound)		All	Yes	Allow	No
✓ EA app (EAConnect_microsoft) (Outbound)		All	Yes	Allow	No
✓ EA app (EADesktop) (Outbound)		All	Yes	Allow	No
✓ EA app (EAGEP) (Outbound)		All	Yes	Allow	No
✓ EA app (EALaunchHelper) (Outbound)		All	Yes	Allow	No
✓ EA app (EALocalHostSvc) (Outbound)		All	Yes	Allow	No
✓ EaseUS Data Recovery Wizard out		All	Yes	Allow	No
✓ Voicemod		All	Yes	Allow	No
✓ Voicemod		All	Yes	Allow	No

Actions

Outbound Rules

- New Rule...
- Filter by Profile
- Filter by State
- Filter by Group
- View
- Refresh
- Export List...



New Outbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

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

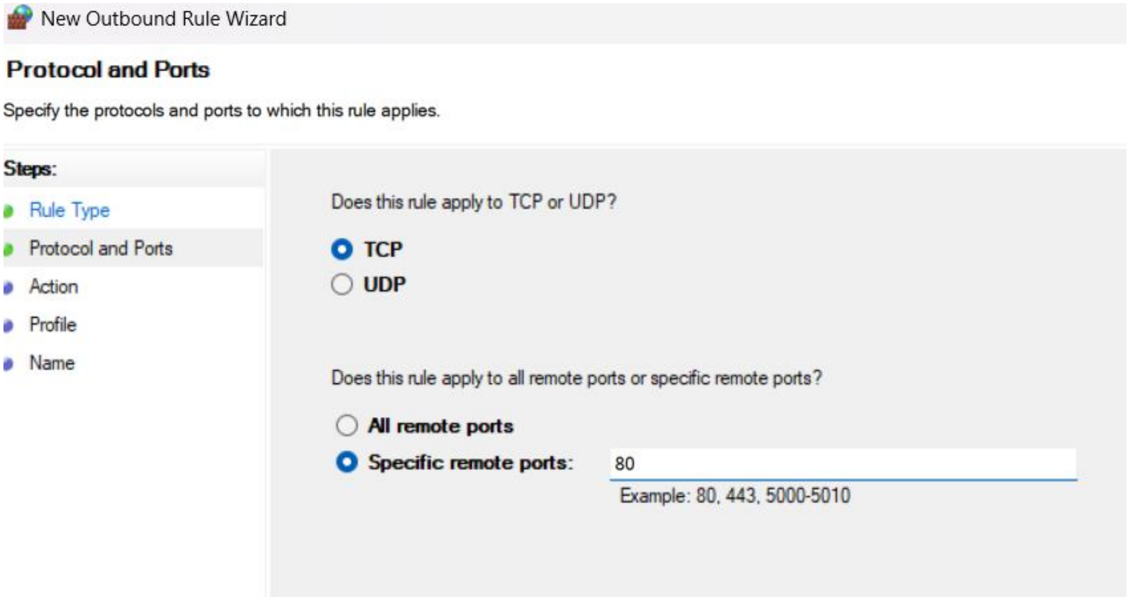
What type of rule would you like to create?

○ **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.



New Outbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

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

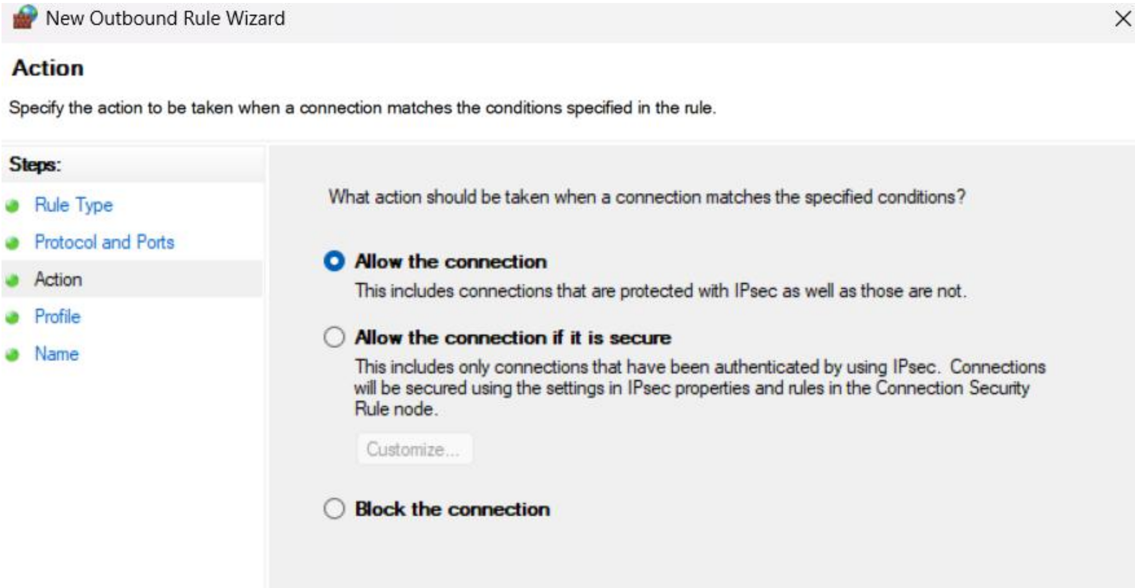
Does this rule apply to TCP or UDP?

● TCP
○ UDP

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

○ All remote ports
● Specific remote ports: 80

Example: 80, 443, 5000-5010



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?

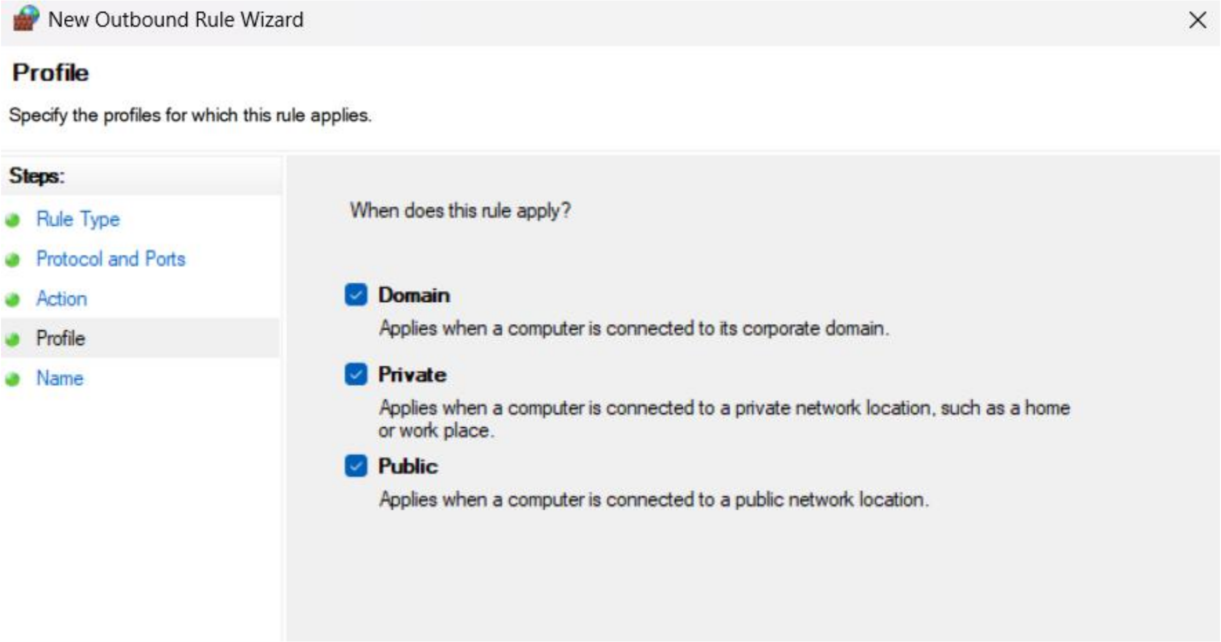
● Allow the connection

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



New Outbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

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

When does this rule apply?

☑ Domain

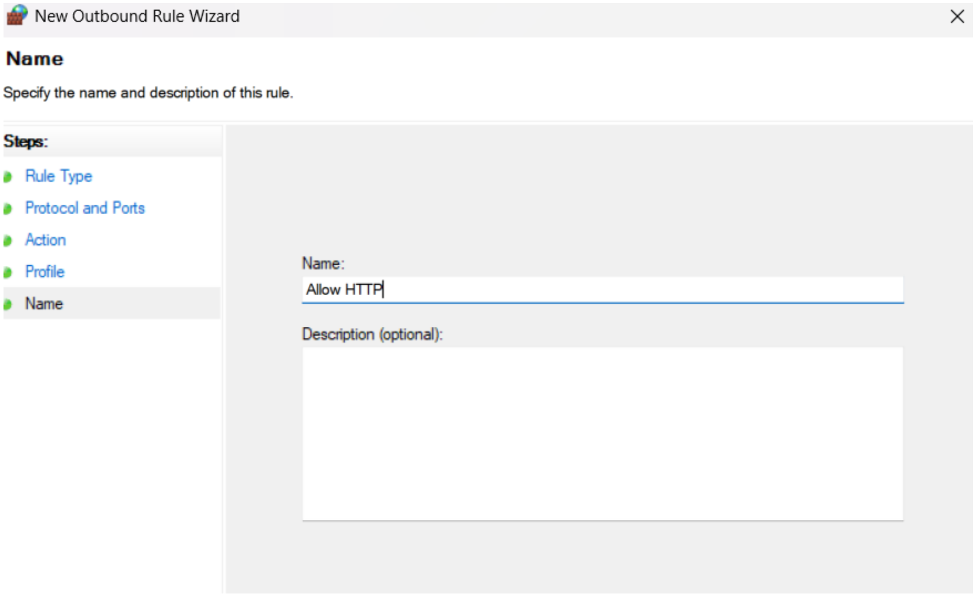
Applies when a computer is connected to its corporate domain.

☑ 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.



New Outbound Rule Wizard

Name

Specify the name and description of this rule.

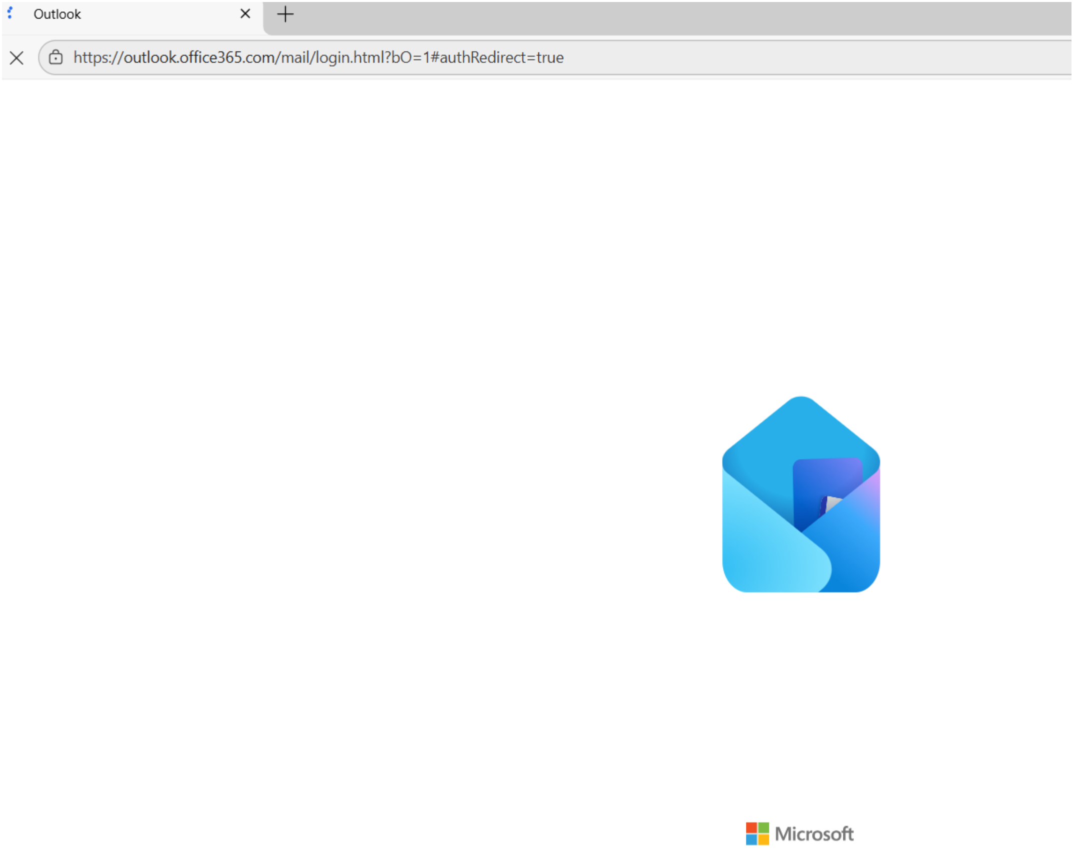
Name:
Allow HTTP

Description (optional):

Step 4:

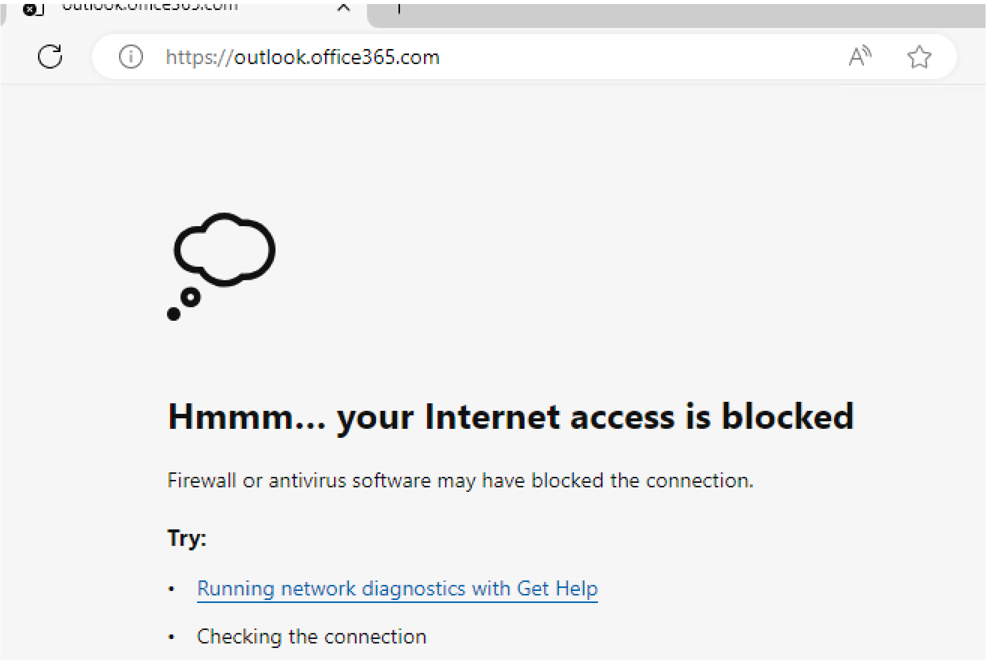
Open a browser or application that uses the configured port.

Verify the connection works when the rule is enabled.



https://outlook.office365.com/mail/login.html?bO=1#authRedirect=true

Disable the rule and check that the connection is blocked



https://outlook.office365.com

Hmmm… your Internet access is blocked

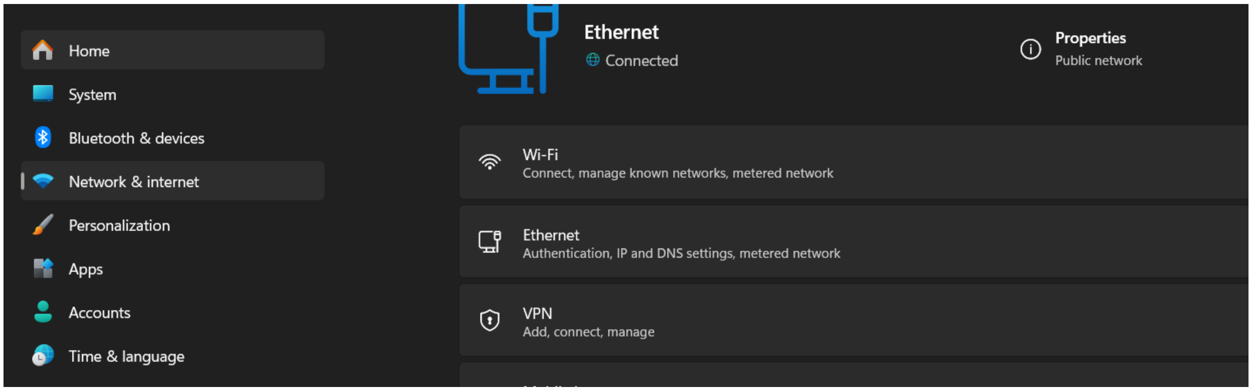
Firewall or antivirus software may have blocked the connection.

Try:

- Running network diagnostics with Get Help
- Checking the connection

Task 2: Setting Up a VPN in Windows

Step 1: Access VPN Setting



Ethernet
Connected

Properties
Public network

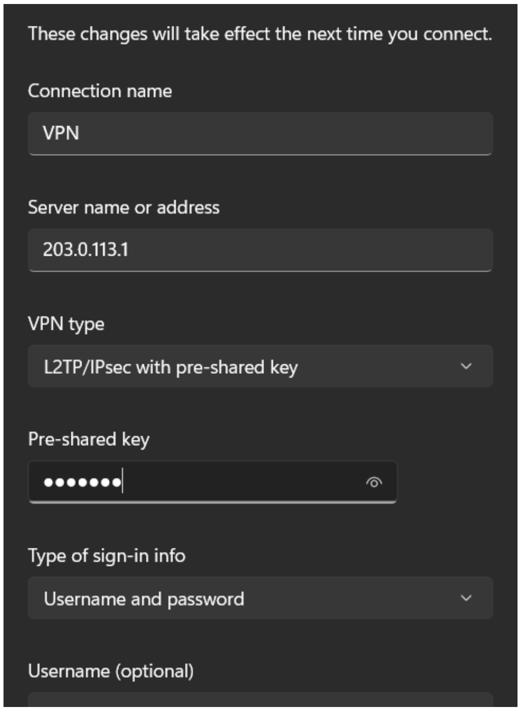
Wi-Fi
Connect, manage known networks, metered network

Ethernet
Authentication, IP and DNS settings, metered network

VPN
Add, connect, manage

Step 2: Fill in the required fields:

- VPN Provider: Windows (built-in).
- Connection Name: Example VPN.
- Server Name or Address: Enter the VPN server's public IP or domain name.
- VPN Type: Select L2TP/IPSec or as instructed by your VPN provider.
- Type of Sign-in Info: Select Username and Password.



These changes will take effect the next time you connect.

Connection name: VPN

Server name or address: 203.0.113.1

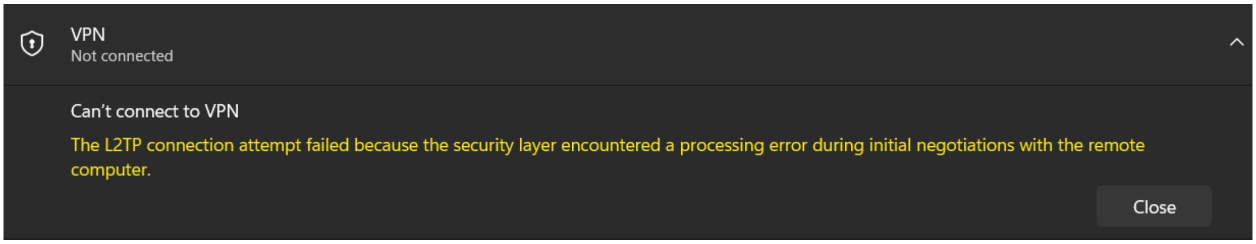
VPN type: L2TP/IPsec with pre-shared key

Pre-shared key: •••••••

Type of sign-in info: Username and password

Username (optional)

Step 3: Connect to the VPN

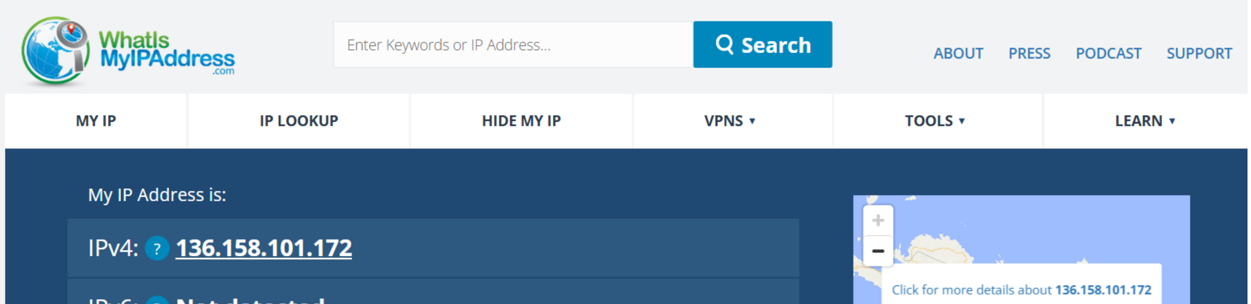


VPN
Not connected

Can't connect to VPN

The L2TP connection attempt failed because the security layer encountered a processing error during initial negotiations with the remote computer.

The VPN connection attempt failed because the server IP used was a placeholder for demonstration purposes and does not actually exist. In a real-world scenario, this error could occur if the server address, VPN type, or credentials are incorrect, or if network/firewall settings block the connection. For this lab, the error is expected and serves to illustrate the VPN configuration process.



My IP Address is:

IPv4: ? 136.158.101.172

IPv6: ? Not detected

Click for more details about 136.158.101.172

Task 3: Testing and Documenting Configurations

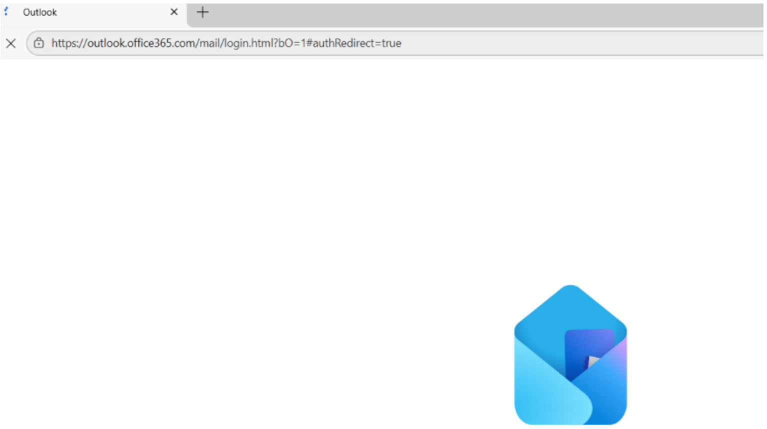
Firewall Testing

1. Use the browser or applications to test the inbound and outbound rules.

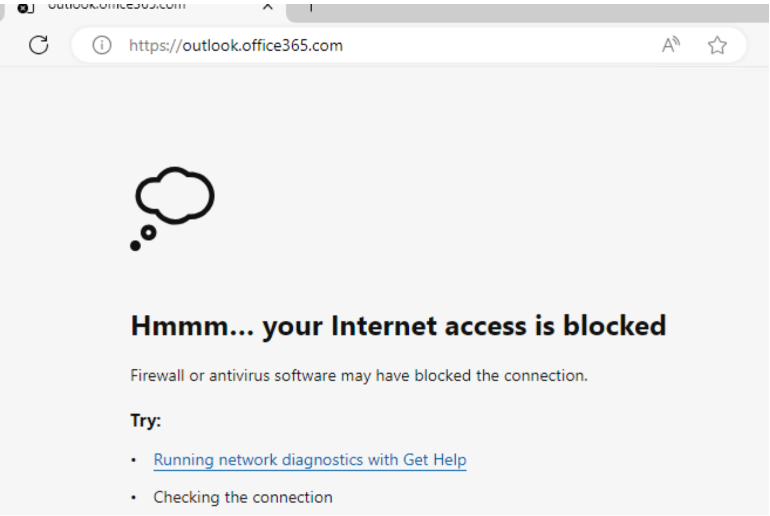
2. Document each test with:

- A description of the test performed.

- Screenshots of the application behavior when the rule is enabled and disabled.



https://outlook.office365.com/mail/login.html?bO=1#authRedirect=true



https://outlook.office365.com

Hmmm… your Internet access is blocked

Firewall or antivirus software may have blocked the connection.

Try:

- Running network diagnostics with Get Help
- Checking the connection

When the outbound rule was enabled, the system could access websites without any issues, which is why the outlook page loaded correctly in the first screenshot. Once the rule was disabled, the server lost the ability to reach external sites. The second screenshot demonstrates the browser blocking access, confirming that internet traffic was restricted. This noticeable difference in behavior highlights that the outbound firewall rule directly governs the server's ability to connect to the internet.

VPN Testing

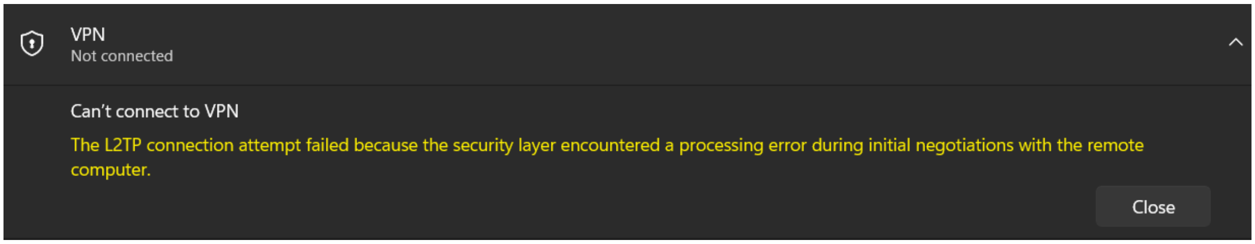
1. Connect to the VPN and verify secure access to a network resource or website.

2. Disconnect and ensure resources are inaccessible without the VPN.

3. Document the VPN connection process with:

- A description of the setup.

- Screenshots showing the VPN status



VPN
Not connected

Can't connect to VPN

The L2TP connection attempt failed because the security layer encountered a processing error during initial negotiations with the remote computer.

The VPN connection did not succeed because the server IP used was only a placeholder for demonstration purposes and isn't a real address. In real-world situations, this error can occur if the server address, VPN type, or credentials are incorrect, or if network or firewall settings block access. In this lab, the error is expected to demonstrate the VPN configuration process