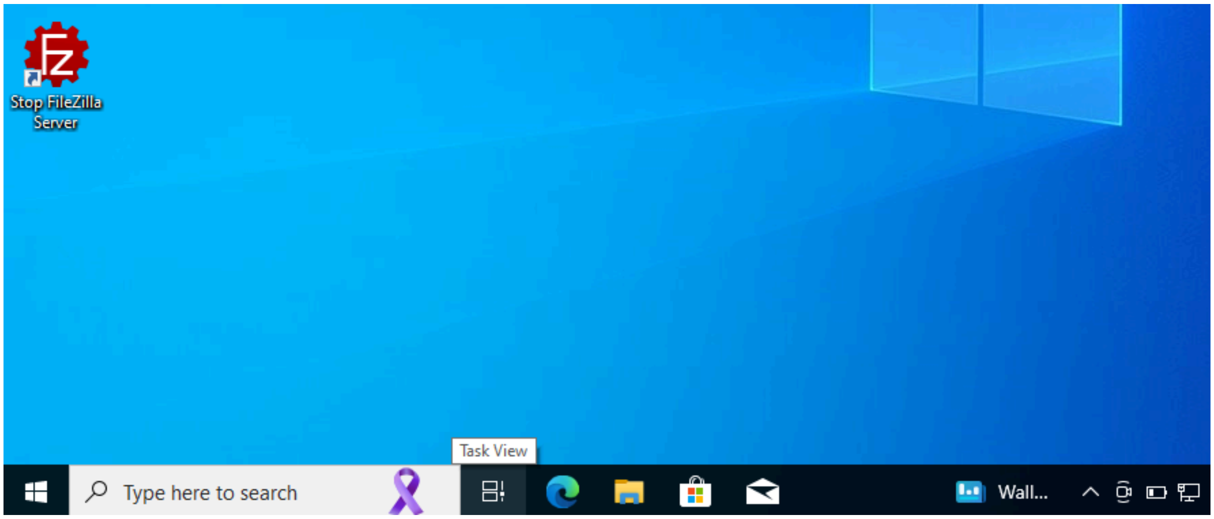
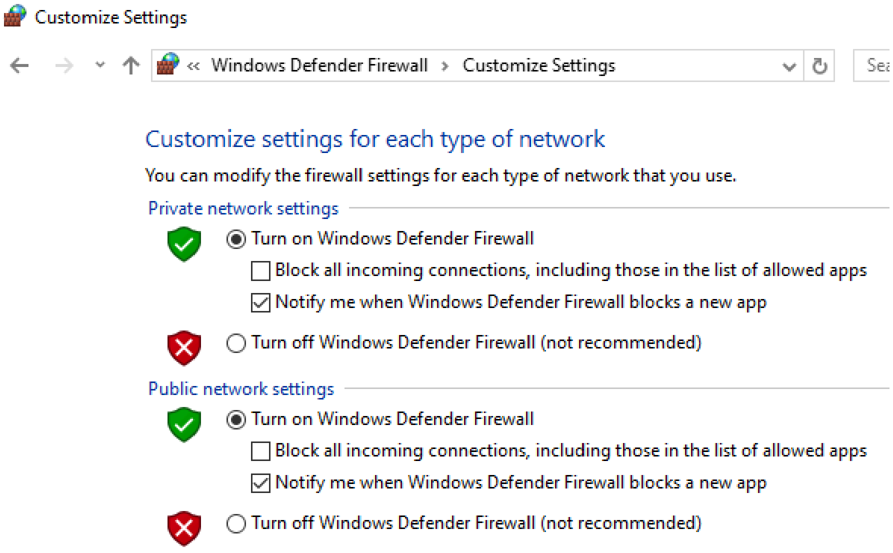
Configure Firewall rules



Step 1: Run your **Windows 10 virtual machine** using **VirtualBox**. If you haven't set it up yet, install VirtualBox, create a VM for Windows 10, and complete the OS installation. Make sure to allocate enough **RAM and storage** for smooth performance. Set the **network adapter to "Bridged Adapter"** in VirtualBox so the VM can communicate with other devices on your network.



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

● Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Public network settings

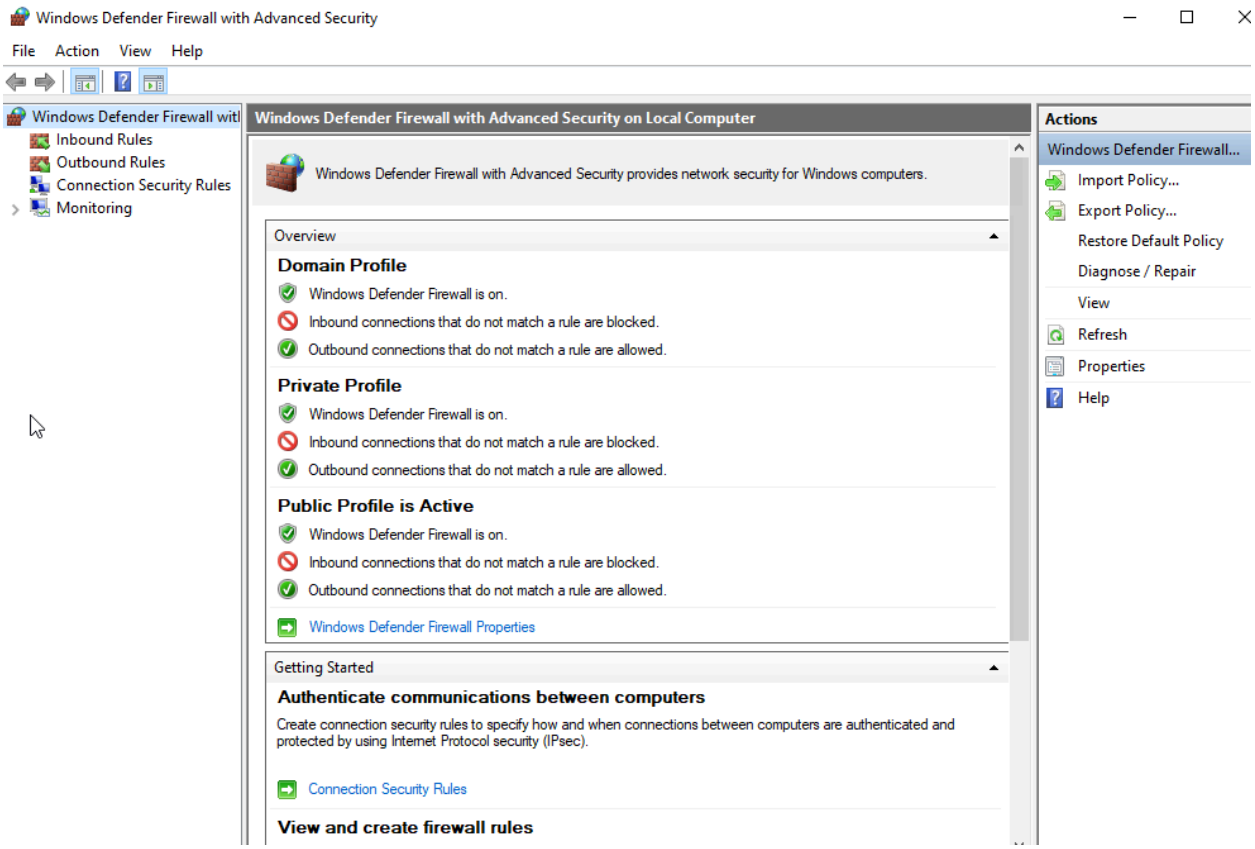
● Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

○ Turn off Windows Defender Firewall (not recommended)

Step 2: On your Windows 10 Virtual Machine, click the Windows Search Bar and type **Windows Defender Firewall**, then open it. Once you're in the app, we're going to start by learning how to turn the firewall on or off. On the left-hand side of the window, click **“Turn Windows Defender Firewall on or off.”** You’ll now see two sections: one for **Private network settings** and one for **Public network settings**. This lets you control how the firewall acts depending on whether you're connected to a private network, like your home Wi-Fi, or a public one, like in a hotel.You can choose to leave one on and turn the other off, turn both off, or turn both on. For this project, we’ll leave both turned on so the firewall is active for all network types. If either one is currently off, go ahead and select **“Turn on Windows Defender Firewall”** for both, and then click **OK** to apply the changes. This ensures your firewall is running and ready before we move on to creating and managing firewall rules.



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

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

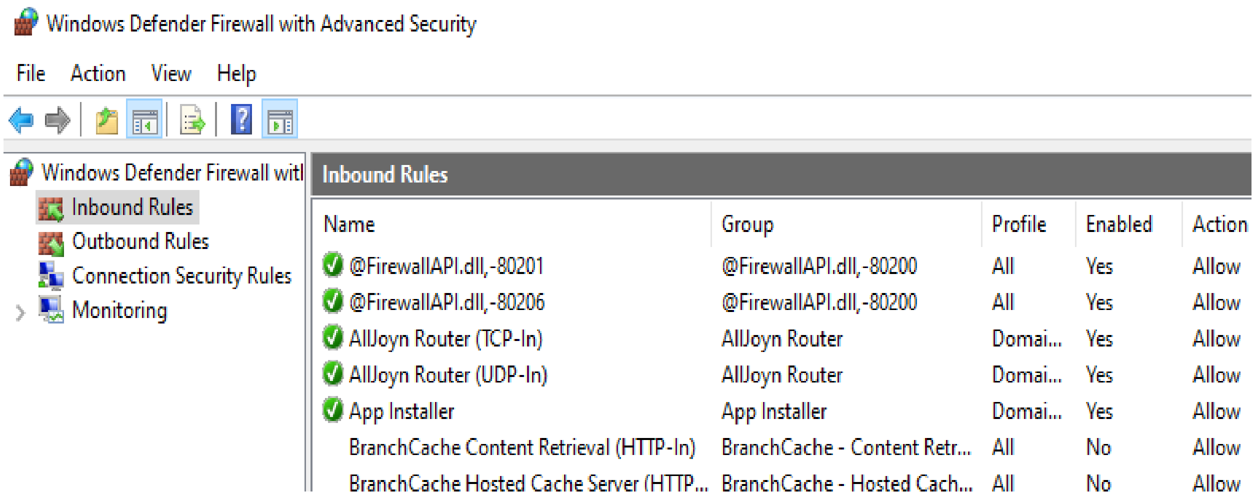
Authenticate communications between computers

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

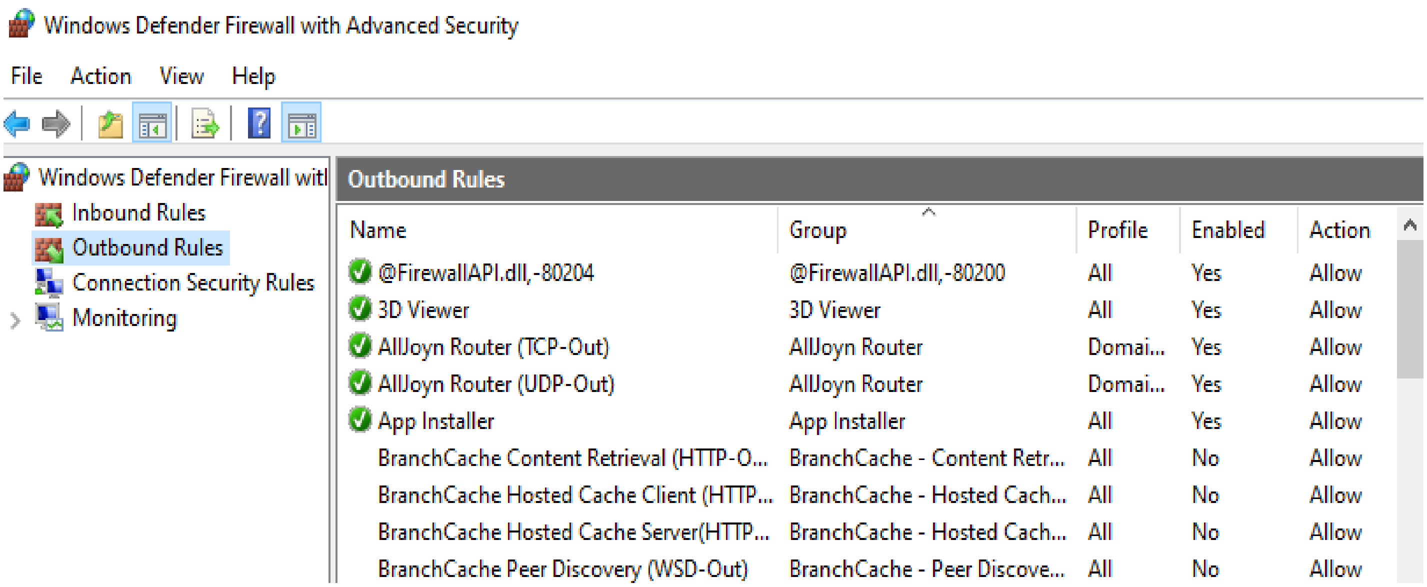
Connection Security Rules

View and create firewall rules

Step 3: Now let’s look at how to open ports in Windows Defender Firewall. If you’re trying to run an app and it’s not working the way it should, it might be because the firewall is blocking the port it needs. To fix that, go back to the main firewall window and click **“Advanced settings”** on the left. This will open up the advanced firewall panel, where you can see and control all the rules. From here, you’ll be able to create a rule to open the port you need.

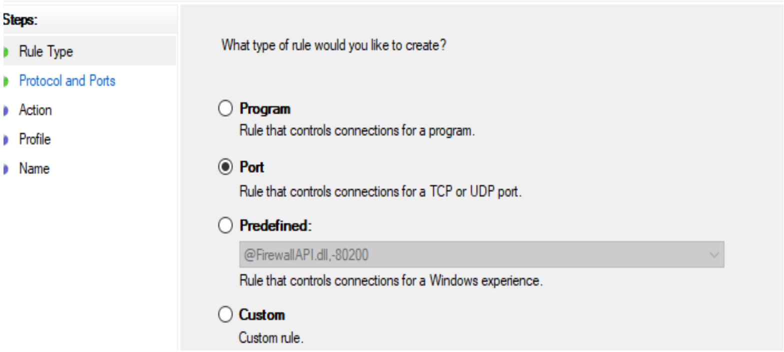

Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules

Name	Group	Profile	Enabled	Action
✓ @FirewallAPI.dll,-80201	@FirewallAPI.dll,-80200	All	Yes	Allow
✓ @FirewallAPI.dll,-80206	@FirewallAPI.dll,-80200	All	Yes	Allow
✓ AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow
✓ AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow
✓ App Installer	App Installer	Domai...	Yes	Allow
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTTP...	BranchCache - Hosted Cach...	All	No	Allow


Windows Defender Firewall with Advanced Security
File
Action
View
Help
Windows Defender Firewall witl
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Outbound Rules

Name	Group	Profile	Enabled	Action
✓ @FirewallAPI.dll,-80204	@FirewallAPI.dll,-80200	All	Yes	Allow
✓ 3D Viewer	3D Viewer	All	Yes	Allow
✓ AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow
✓ AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow
✓ App Installer	App Installer	All	Yes	Allow
BranchCache Content Retrieval (HTTP-O...	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Client (HTTP...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Hosted Cache Server(HTTP...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	All	No	Allow

Step 4: By default, the firewall blocks most traffic coming **into** your machine and allows traffic going **out**. To see this in action, click **Inbound Rules** and **Outbound Rules** on the left-hand side. This shows you exactly what the firewall is currently allowing or blocking, both for incoming and outgoing connections on your system.



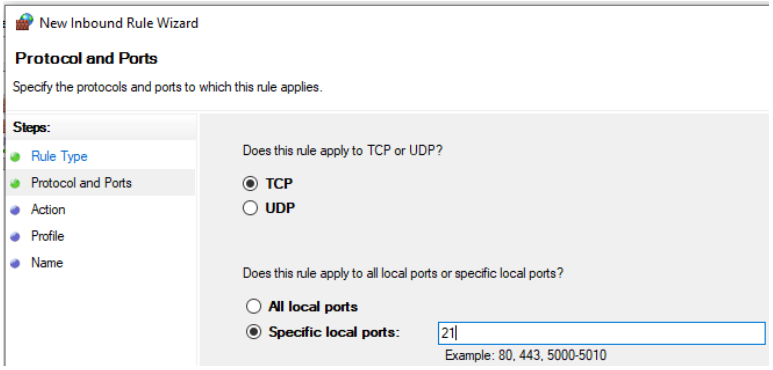
What type of rule would you like to create?

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

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

○ **Predefined:**
@FirewallAPI.dll,-80200
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.


New Inbound Rule Wizard

Protocol and Ports

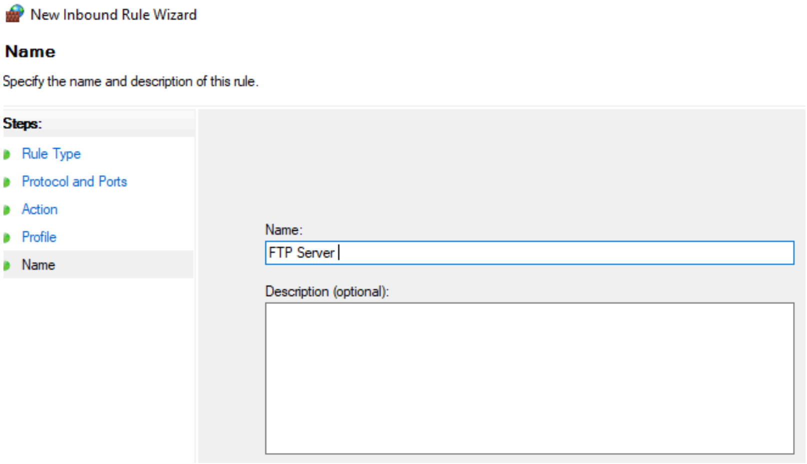
Specify the protocols and ports to which this rule applies.

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:** 21
Example: 80, 443, 5000-5010

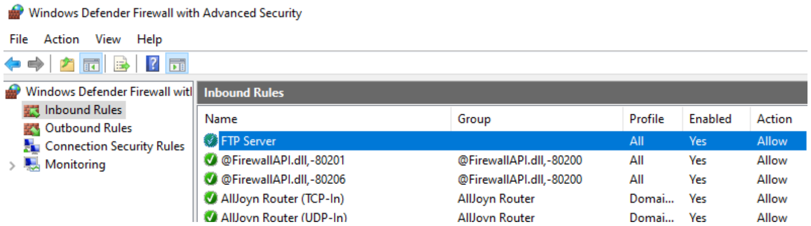

New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Name: FTP Server

Description (optional):


Windows Defender Firewall with Advanced Security

Inbound Rules

Name	Group	Profile	Enabled	Action
FTP Server		All	Yes	Allow
@FirewallAPI.dll,-80201	@FirewallAPI.dll,-80200	All	Yes	Allow
@FirewallAPI.dll,-80206	@FirewallAPI.dll,-80200	All	Yes	Allow
AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes	Allow
AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes	Allow

Step 5: By default, the firewall doesn’t allow FTP traffic in, so we need to create a rule. On the right side of the firewall window, click **“New Rule…”** and choose **“Port”**, then click **Next**.

Select **TCP**, type **21** for the specific port, and click **Next**. Choose **“Allow the connection”**, then keep clicking **Next** until you reach the name screen. Name the rule **“FTP Server”** and click **Finish**. You should now see your new rule in the inbound rules list, and FTP traffic will be allowed on this machine.

Step 6: Close All Tabs to End the Project