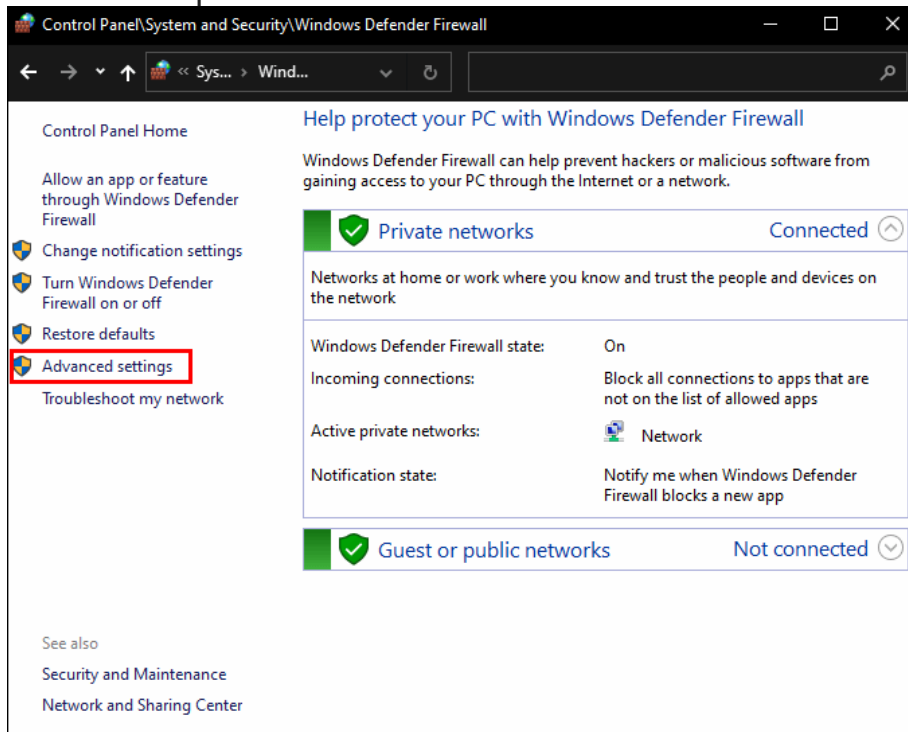
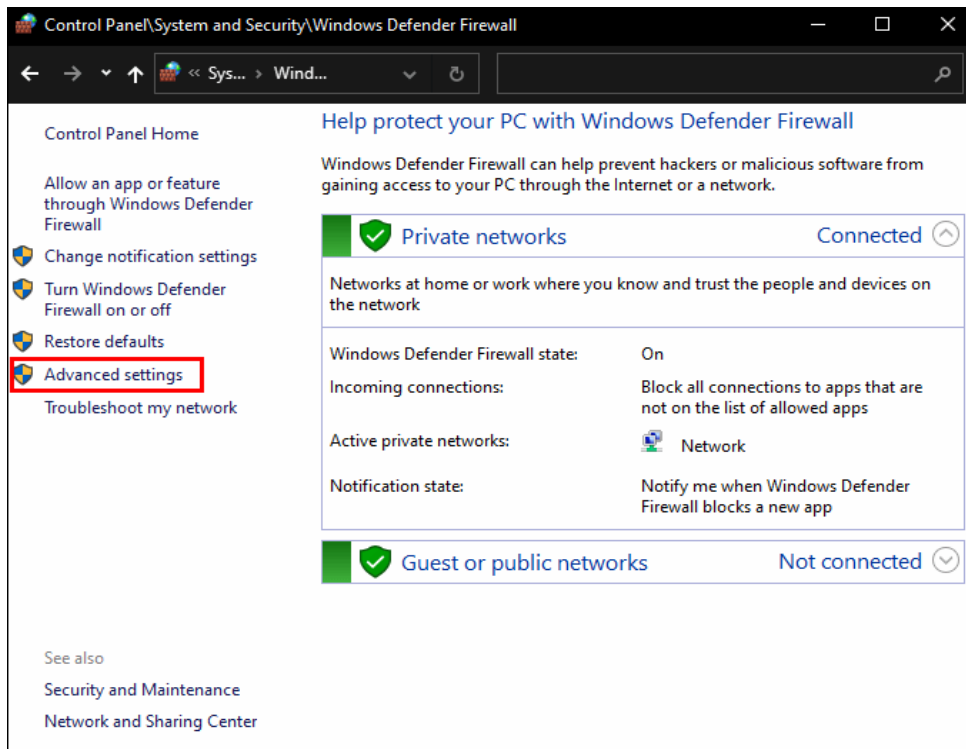


## Lab Program 8: Block the website using the Windows Defender Firewall in Windows 10

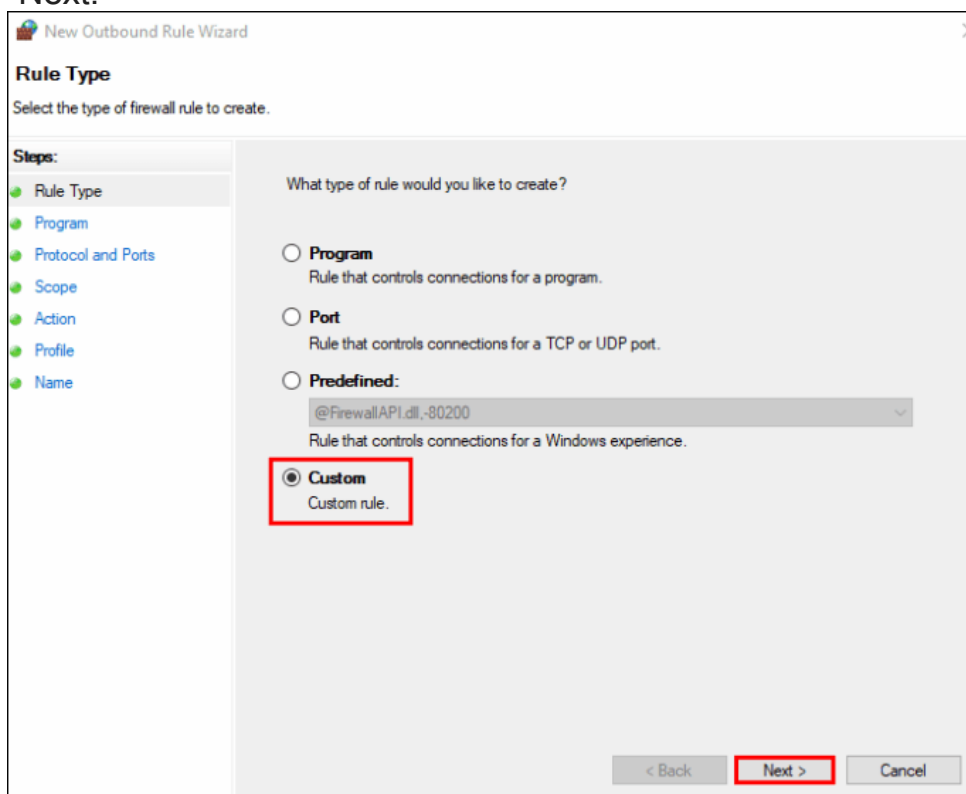
1. Launch the Control Panel on your computer.
2. Select “Windows Defender Firewall” followed by “Advanced Settings” on the left-side pane.



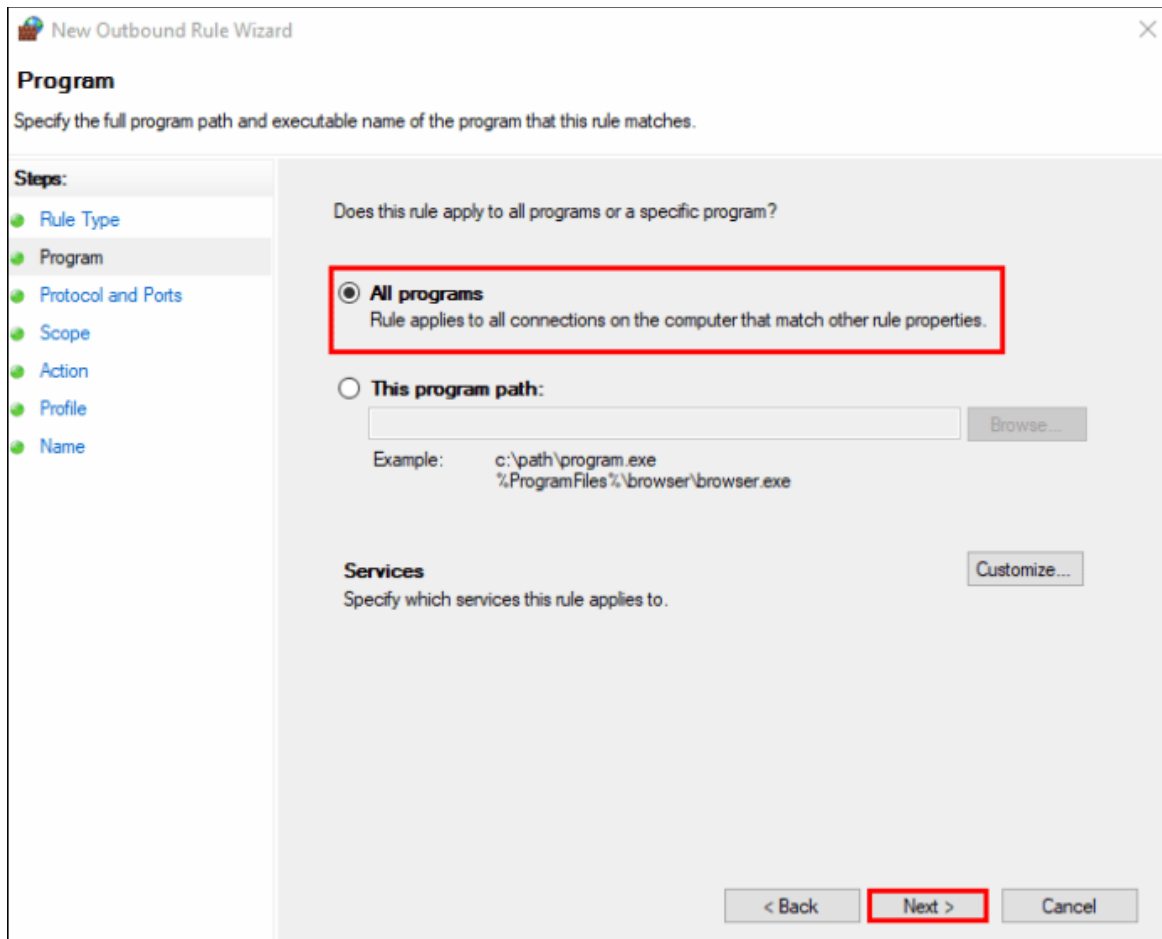
3. Right-click on “Outbound Rules” from the menu on the left and select “New Rule.”



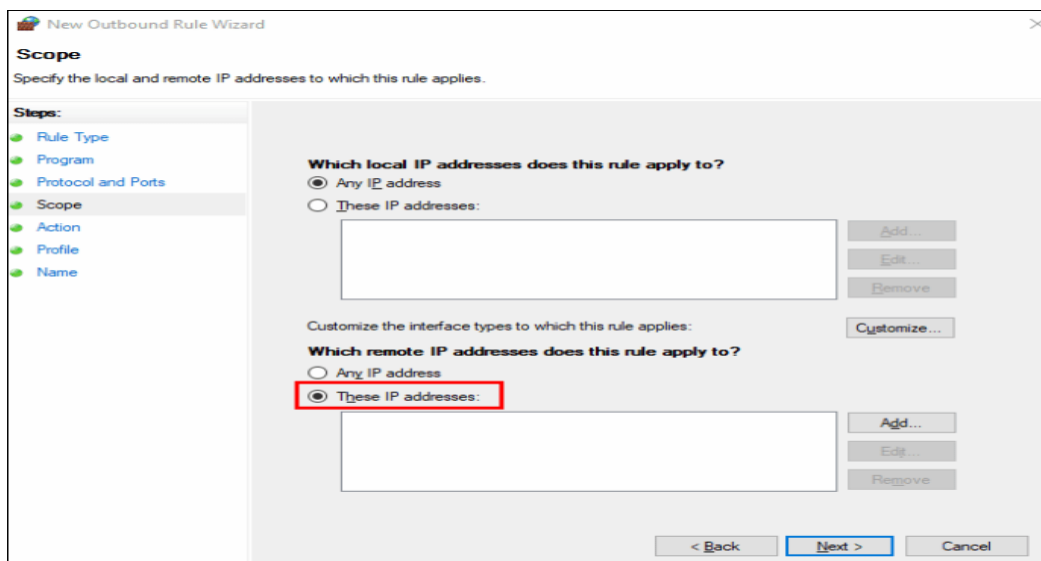
4. When a new window pops up, select the “Custom” option followed by “Next.”



5. On the next window, select “All programs” and again select “Next.”



6. Select the "These IP addresses" option under "Which remote IP addresses does this rule apply to?"



7. Click on "Add" and enter the IP addresses you want to block. Then select "Next."

New Outbound Rule Wizard

### Scope

Specify the local and remote IP addresses to which this rule applies.

**Steps:**

- Rule Type
- Program
- Protocol and Ports
- Scope**
- Action
- Profile
- Name

**Which local IP addresses does this rule apply to?**

☒ Any IP address

☐ These IP addresses:

Add...  
Edit...  
Remove

Customize the interface types to which this rule applies: Customize...

**Which remote IP addresses does this rule apply to?**

☐ Any IP address

☒ These IP addresses:

192.168.0.1

Add...  
**Edit...**  
Remove

< Back **Next >** Cancel

8. Make sure to choose the “Block the connection” option and click on “Next.”

New Outbound Rule Wizard

**Action**

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

**Steps:**

- Rule Type
- Program
- Protocol and Ports
- Scope
- 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.

[Customize...](#)

☒ **Block the connection**

< Back   **Next >**   Cancel

9. Choose whether the rule applies to Domain, Private, or Public. You can also select all three.

New Outbound Rule Wizard

**Profile**

Specify the profiles for which this rule applies.

**Steps:**

- Rule Type
- Program
- Protocol and Ports
- Scope
- 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.

< Back   **Next >**   Cancel

10. Select "Next," add a name or description for this rule, and select "Finish" to complete the action.

New Outbound Rule Wizard

**Name**

Specify the name and description of this rule.

**Steps:**

- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name**

Name:  
Blocking

Description (optional):

< Back Finish Cancel

**To check whether the website is blocked:**

**Go to search bar-> type cmd -> Right click -> Run as administrator**

```
C:\Users\alphr>nslookup www.facebook.com
Server: UnKnown
Address: 192.168.0.1

Non-authoritative answer:
Name: star-mini.c10r.facebook.com
Addresses: 2a03:2880:f15a:83:face:b00c:0:25de
           31.13.77.35
Aliases: www.facebook.com

C:\Users\alphr>
```

**Scope**

Specify the local and remote IP addresses to which this rule applies.

**Steps:**

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

**Which local IP addresses does this rule apply to?**

☒ Any IP address

☐ These IP addresses:

[Add...](#)[Edit...](#)[Remove](#)

Customize the interface types to which this rule applies:

[Customize...](#)**Which remote IP addresses does this rule apply to?**

☐ Any IP address

☒ These IP addresses:

192.168.0.1  
2a03:2880f15a:83face:b00c:0:25de

[Add...](#)[Edit...](#)[Remove](#)[< Back](#)[Next >](#)[Cancel](#)