Secure Firewall Configuration and Management

Module 07

Lab 1

Designing Firewall Rules on a Windows Firewall

The Windows Firewall is a software component of Microsoft Windows that provides firewalling and packet filtering functions.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Firewall rules are created to put restriction on sending traffic to, or receiving traffic from, programs, system services, computers, or users. Configuring inbound and outbound traffic rules on a firewall is one of the important tasks in network security. These rules are configured based on the organizational policy. It prevents malicious traffic from entering into the network. As a network administrator, you should be able to configure inbound and outbound rules in a Windows firewall.

Lab Objectives

The objective of this lab is to demonstrate you how to create inbound and outbound rules in a Windows firewall.

Lab Environment

To perform this lab, you need:

- A virtual machine running **Windows 10**
- Administrative Privileges

Lab Duration

Time: 25 Minutes

Overview of Firewall Rules

Firewall rules can be created for either inbound or outbound traffic.

- An inbound firewall rule protects the network against incoming malicious traffic from the Internet or other network segments.

- An outbound firewall protects against outgoing traffic originating inside an enterprise network.

The rule can be configured to specify the computers, users, program, service, port and protocol.

Lab Tasks

TASK 1

Launch Windows Firewall

1. Logon to the **Windows 10** virtual machine, right-click on the **Windows** icon, and select **Control Panel**.

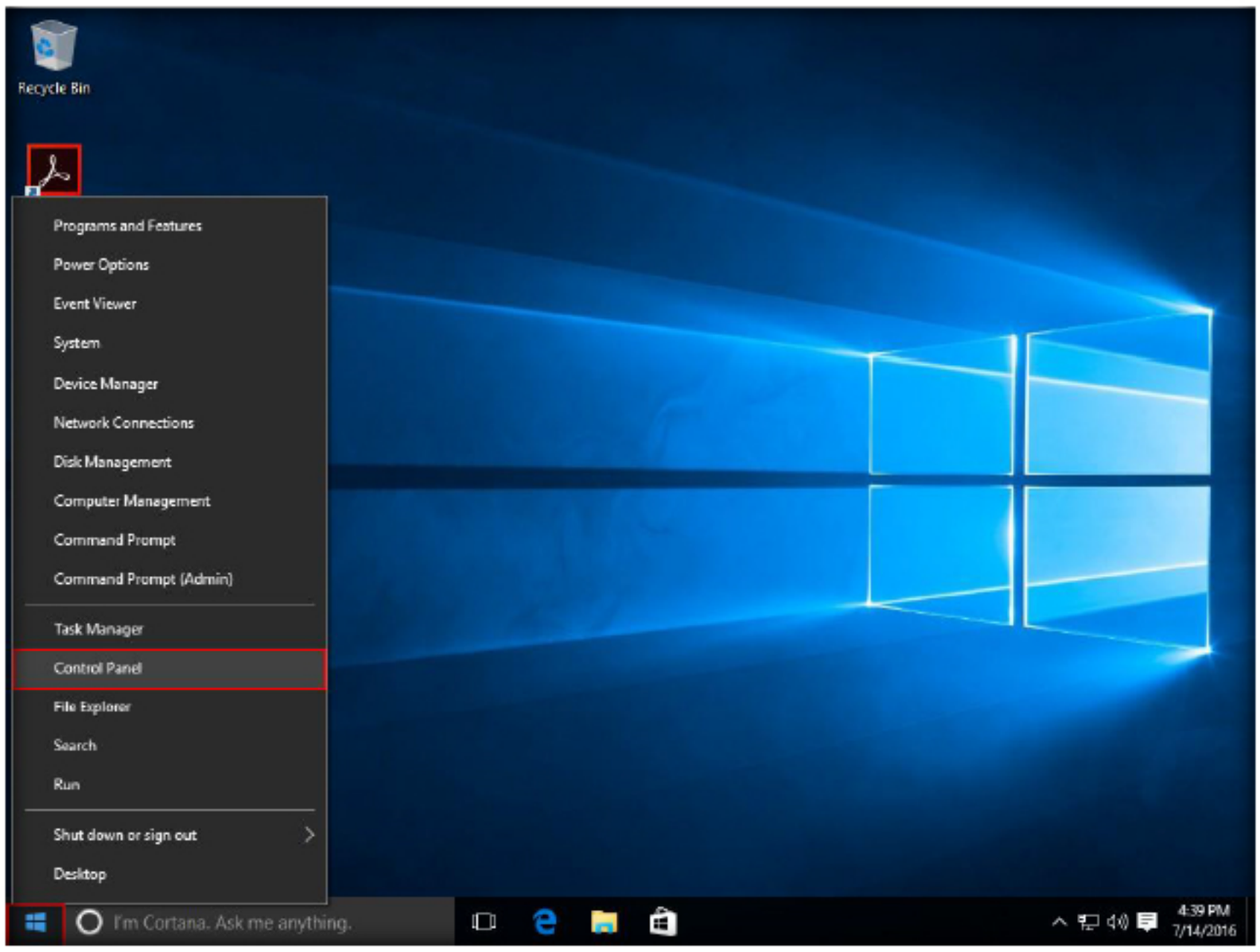


FIGURE 1.1: Navigating to the Control panel

2. **Control Panel** appears; if you are in category view, you may switch to the **Large icons** view by selecting **Large icons** from the **Category** drop-down list.

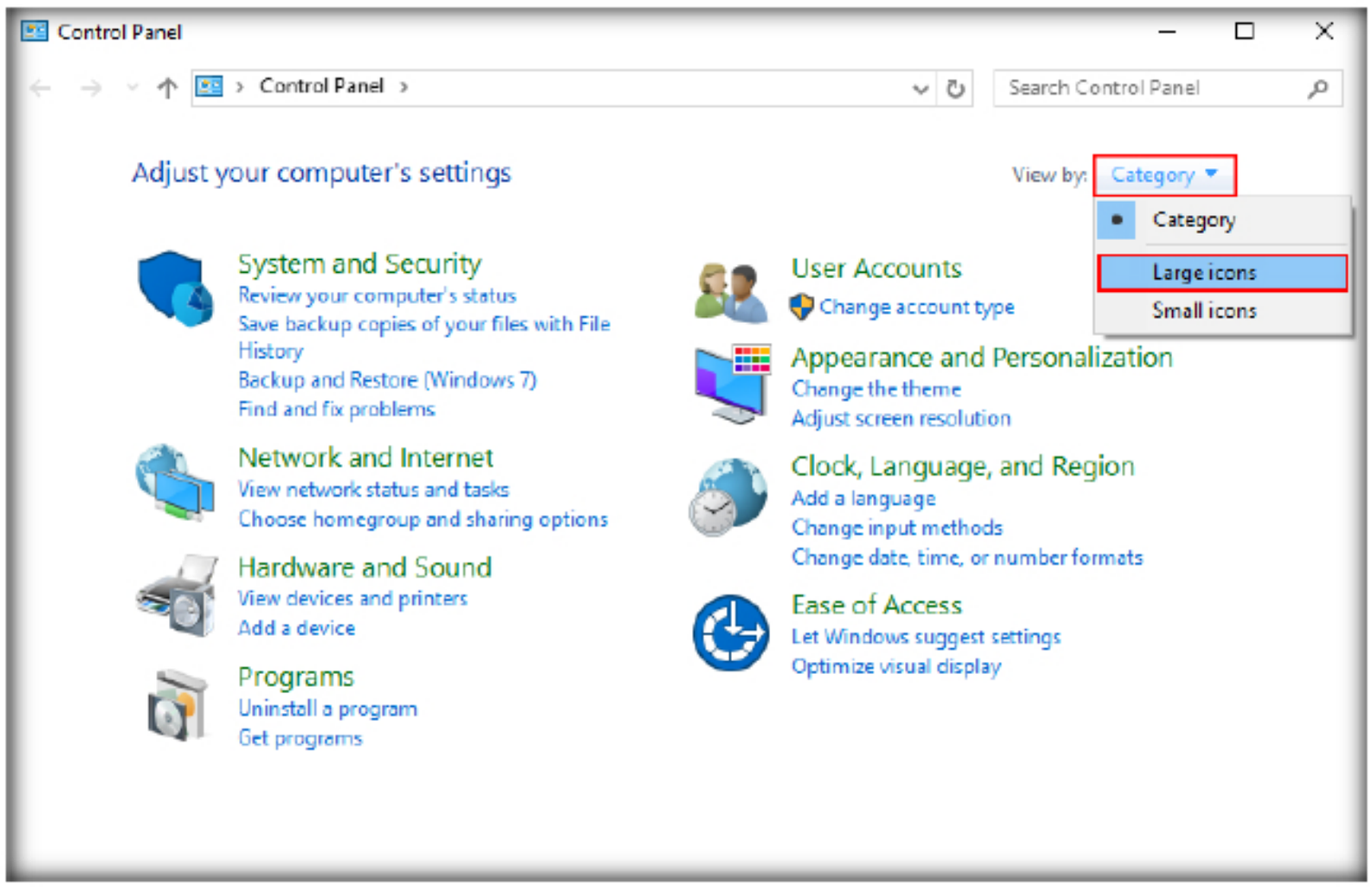


FIGURE 1.2: Switching to the Large icons view

3. The **All Control Panel Items** window appears, scroll the window down and click on the **Windows Firewall.**

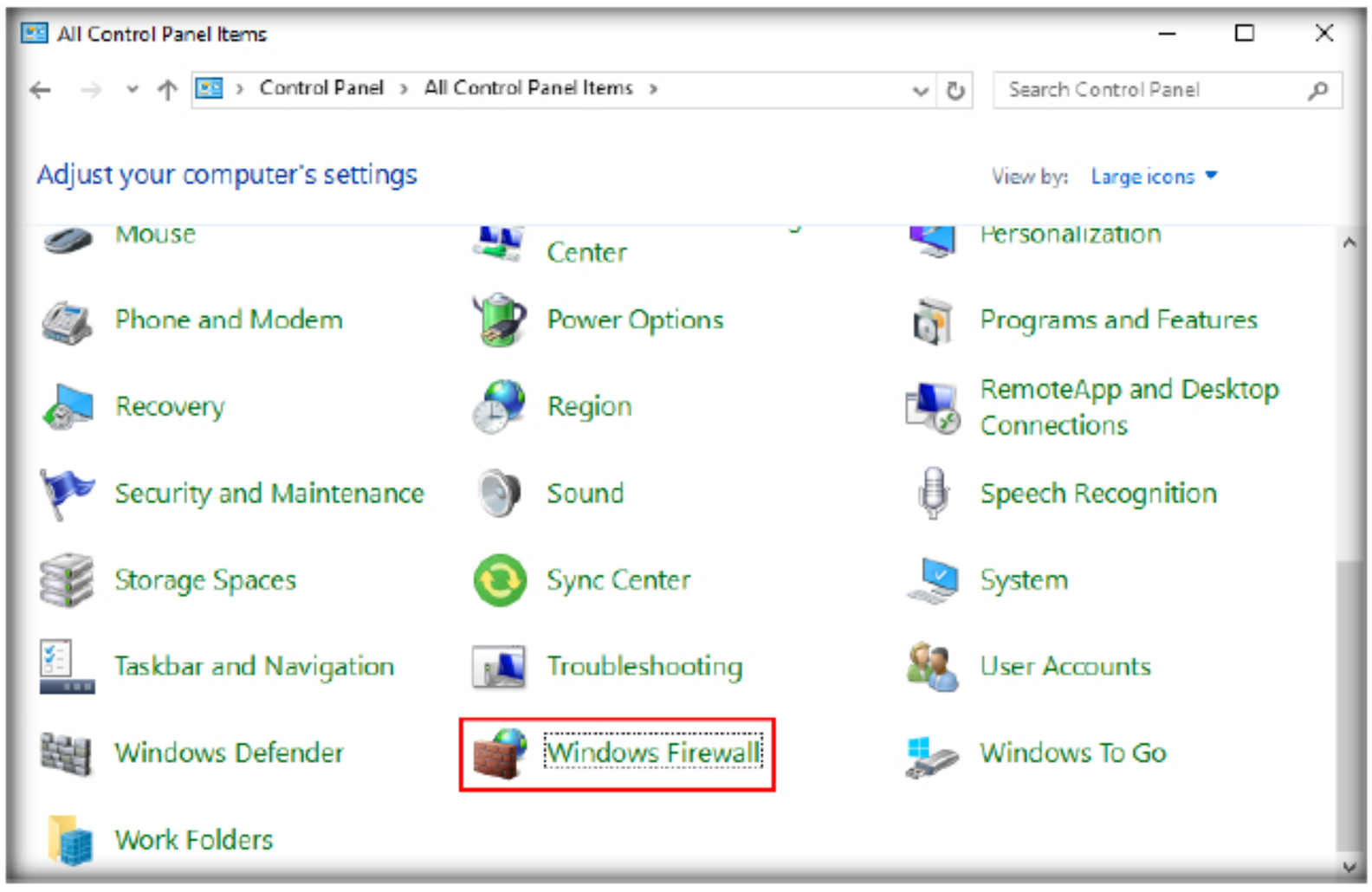


FIGURE 1.3: Opening the Windows Firewall

4. **The Windows Firewall** setting window will be displayed. Click **Advanced Settings** in the left pane.

📖 You can use the Windows Firewall with Advanced Security to help protect the computers on your network.

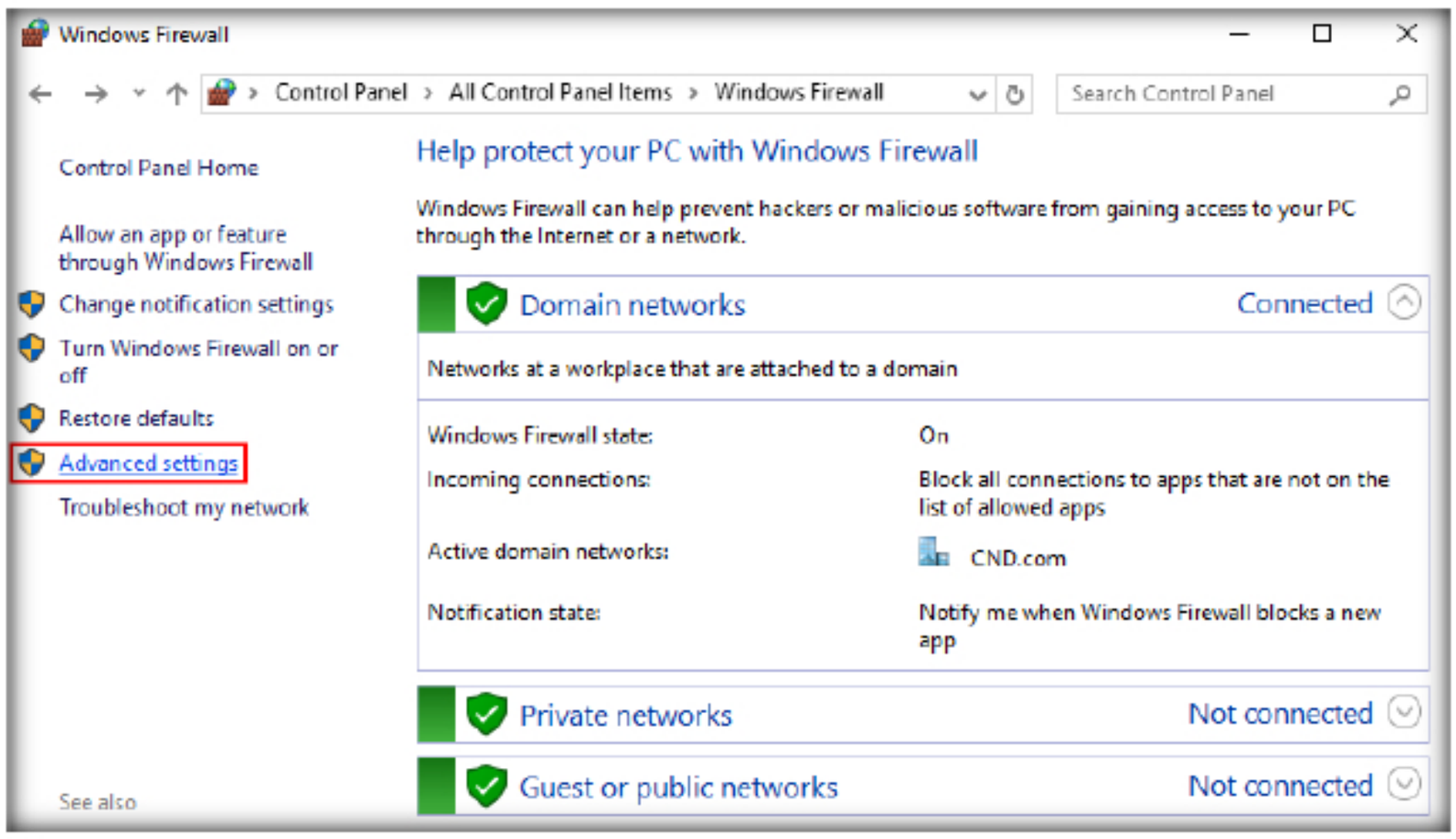


FIGURE 1.4: Navigating to Advanced Settings in Window Firewall

5. The Advanced Settings operate at three levels described below:
   a. **Domain**: Applies to the network adapter, when the device is part of a Domain
   b. **Private**: Applies to a network adapter when the device is connected to a network indirectly through a router or some other security device
   c. **Public**: Applies to a network adapter when the device is directly connected to a network. This is the default profile.

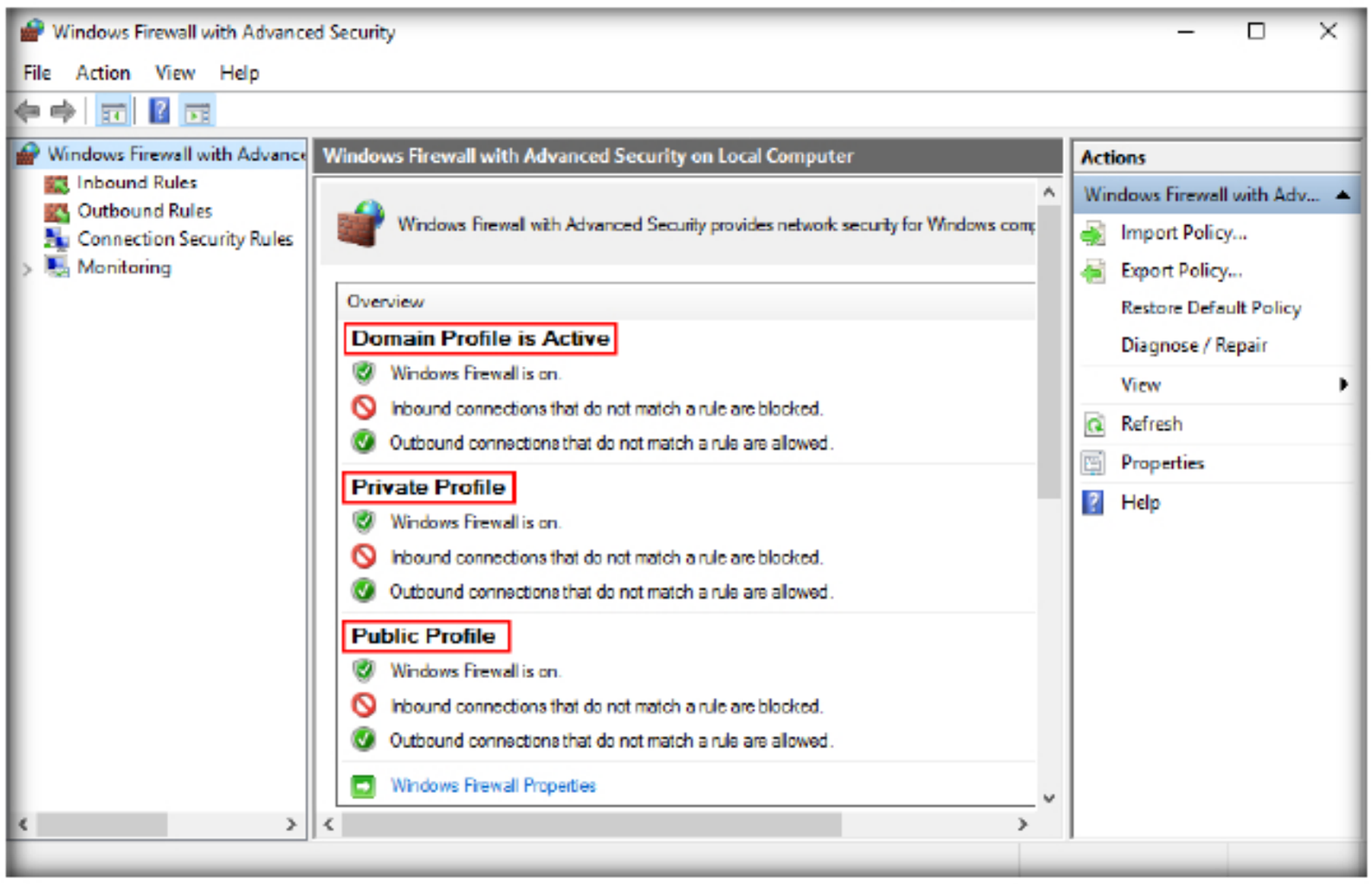


FIGURE 1.5: Three levels at which Advanced settings operate

TASK 2

Changing Firewall Settings

Windows Firewall with Advanced Security includes a stateful firewall that allows you to determine which network traffic is permitted to pass between your computer and the network

6. Click **Windows Firewall Properties**

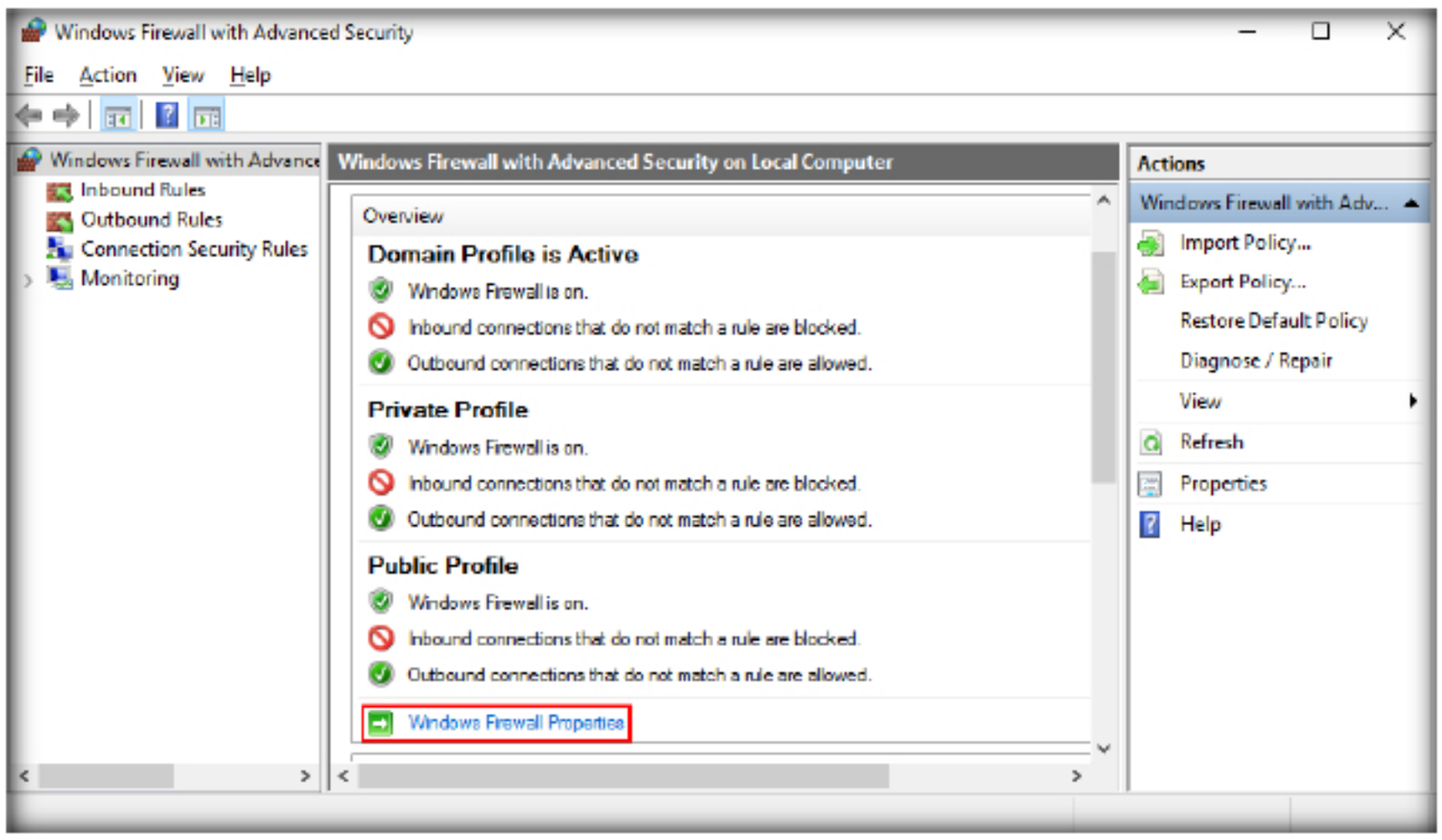


FIGURE 1.6: The Window Firewall Properties window

7. The Windows Firewall Properties window allows you to view and configure the firewall properties for a **Domain**, **Private** and **Public Profiles**. Click **OK** to close the window.

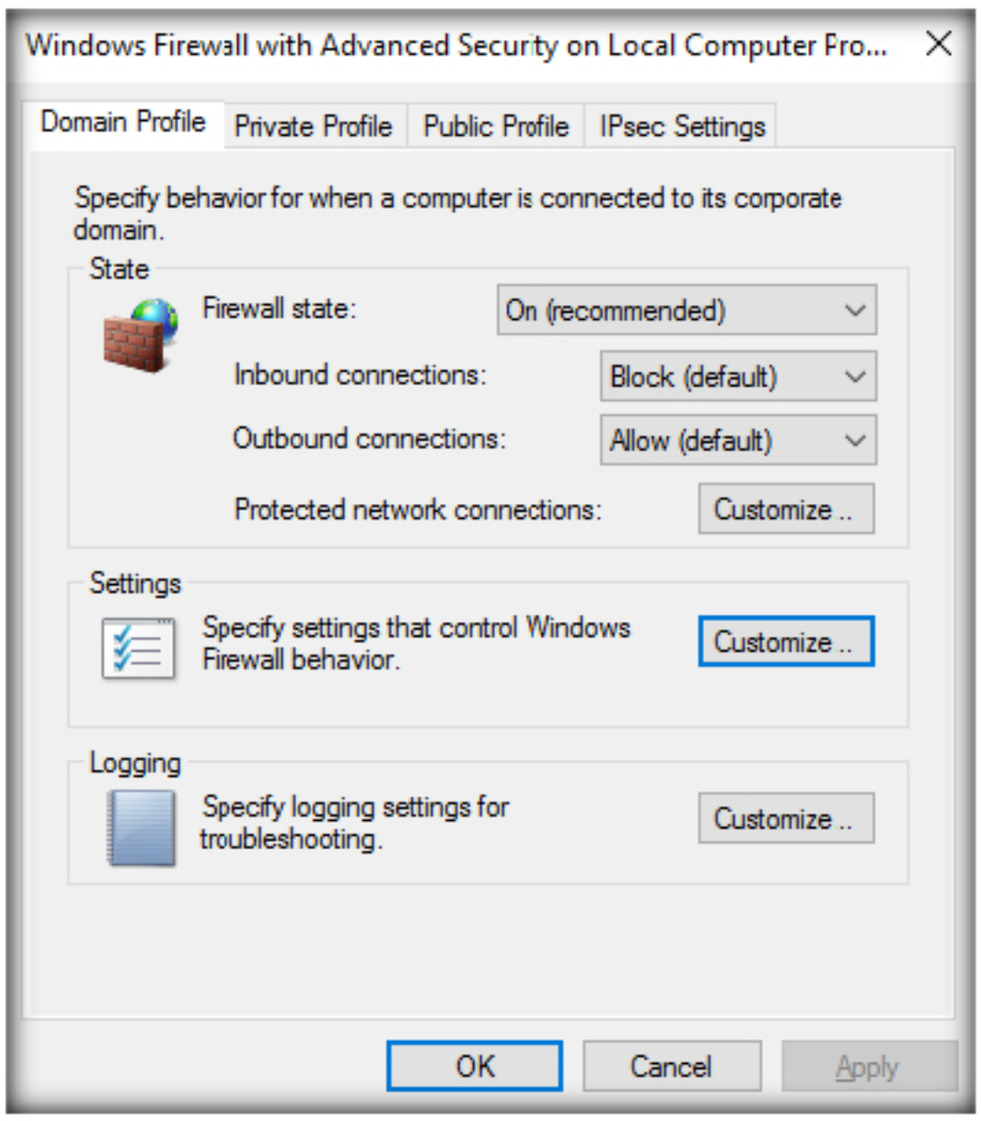


FIGURE 1.7: Default settings for Domain profile

Note: It is recommended that you do not alter the default settings for any of the profiles.

8. Now, keep the **Windows Firewall with Advanced Security** window intact, switch to the **Ubuntu** virtual machine and login.
9. Once you are logged on to the machine, launch a command line terminal, type **ftp 10.10.10.10** in the command line terminal and press **Enter**. You will notice the connection has timed out, which means, the firewall in Windows 10 is preventing the Ubuntu machine from accessing it. Type **bye** and press **Enter** to exit the **ftp** shell.

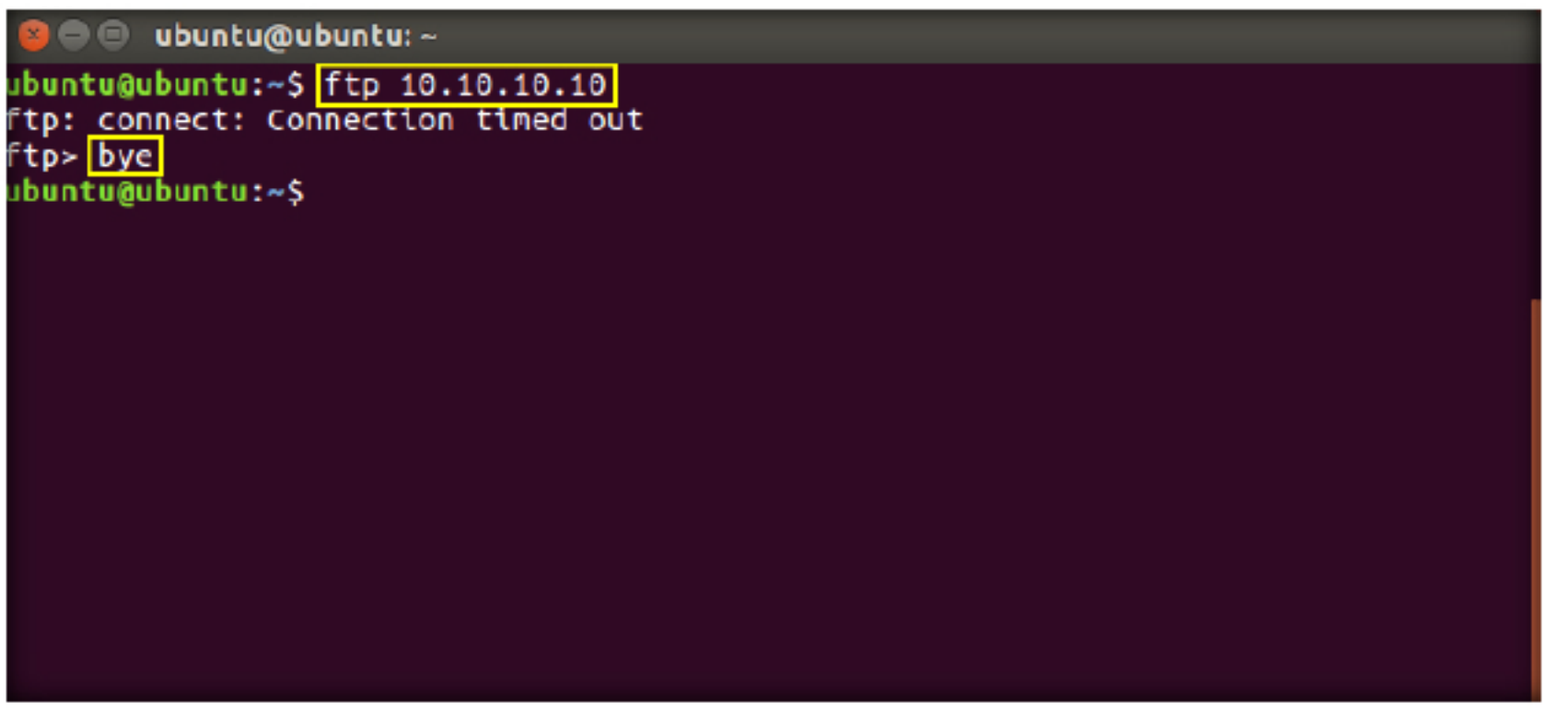


FIGURE 1.8: Establishing FTP Connection

10. Next, we will add an inbound Firewall rule in Windows 10 to allow ftp to access the computers in the domain. To add the rule, switch back to Windows 10 and click **Inbound Rules** in the left pane.

TASK 3

Creating Inbound Rules

Inbound rules explicitly allow, or explicitly block, inbound network traffic that matches the criteria in the rule.

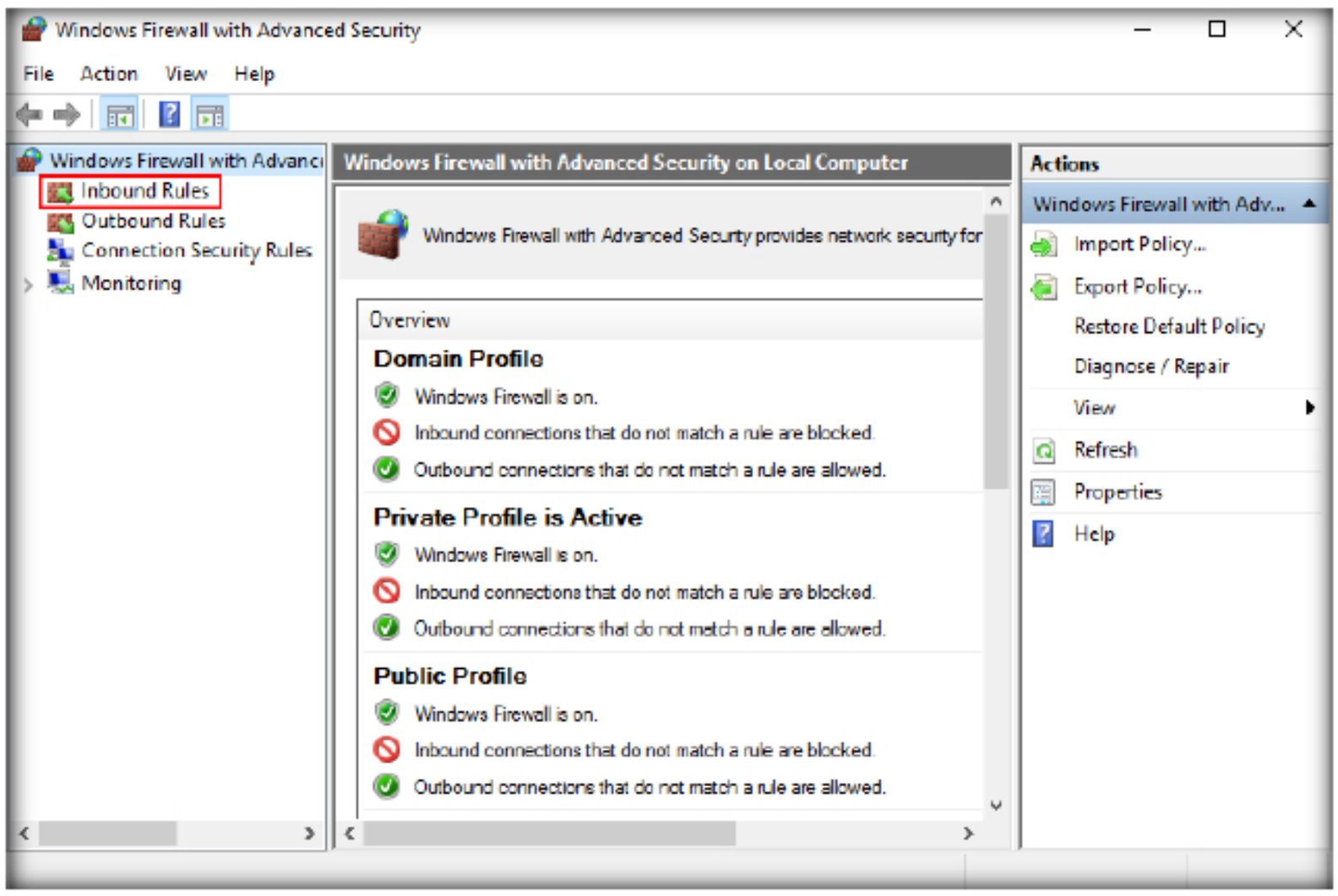


FIGURE 1.9: Navigating to Inbound rule

11. Click **New Rule...** in the right pane

📖 Inbound rules filter traffic passing from the network to the local computer based on the filtering conditions specified in the rule. Conversely, outbound rules filter traffic passing from the local computer to the network based on the filtering conditions specified in the rule. Both inbound and outbound rules can be configured to allow or block traffic as needed.

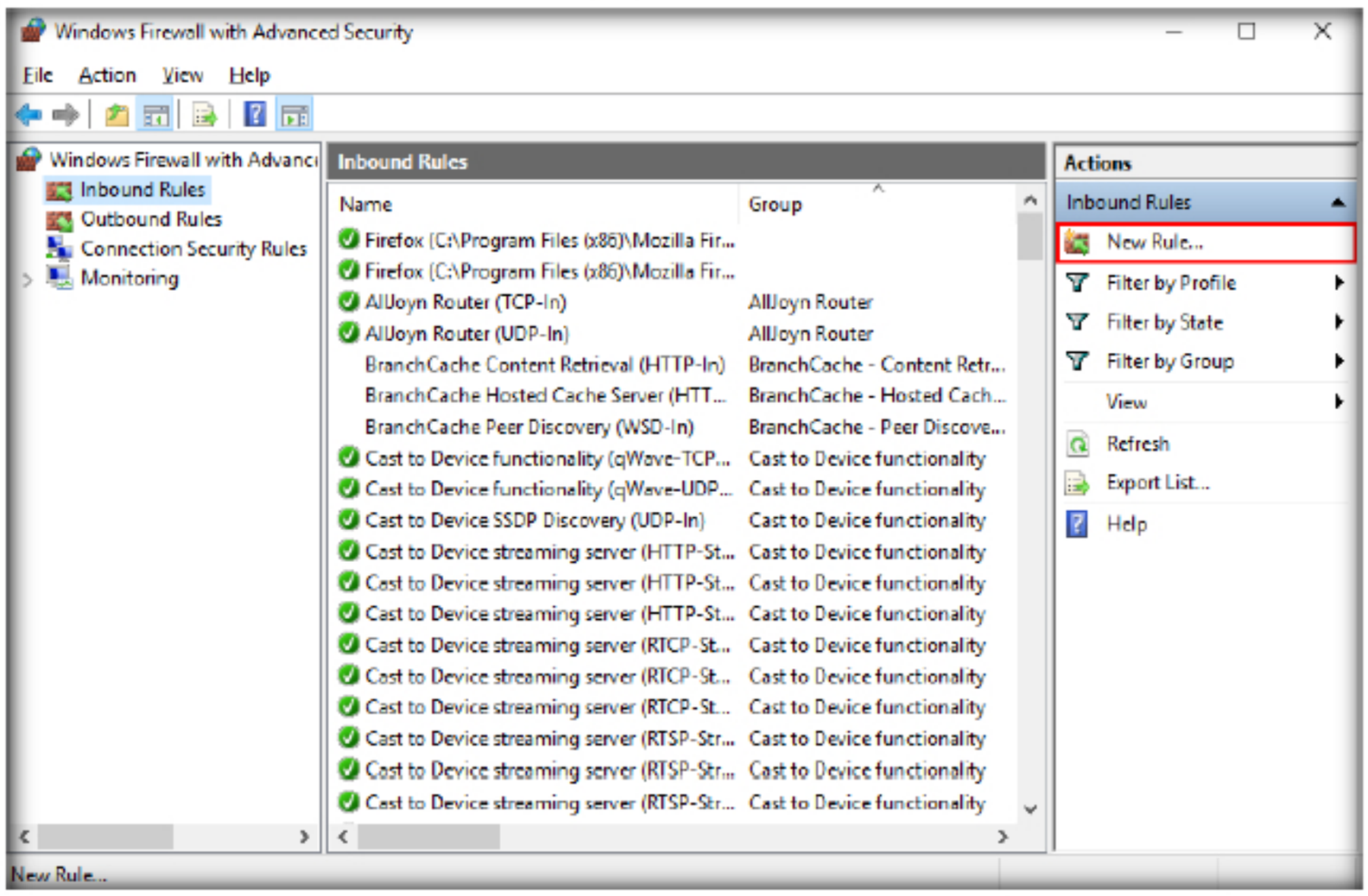


FIGURE 1.10: Creating a New Rule

12. The **New Inbound Rule Wizard** window appears, select the **Port** radio button and click **Next**

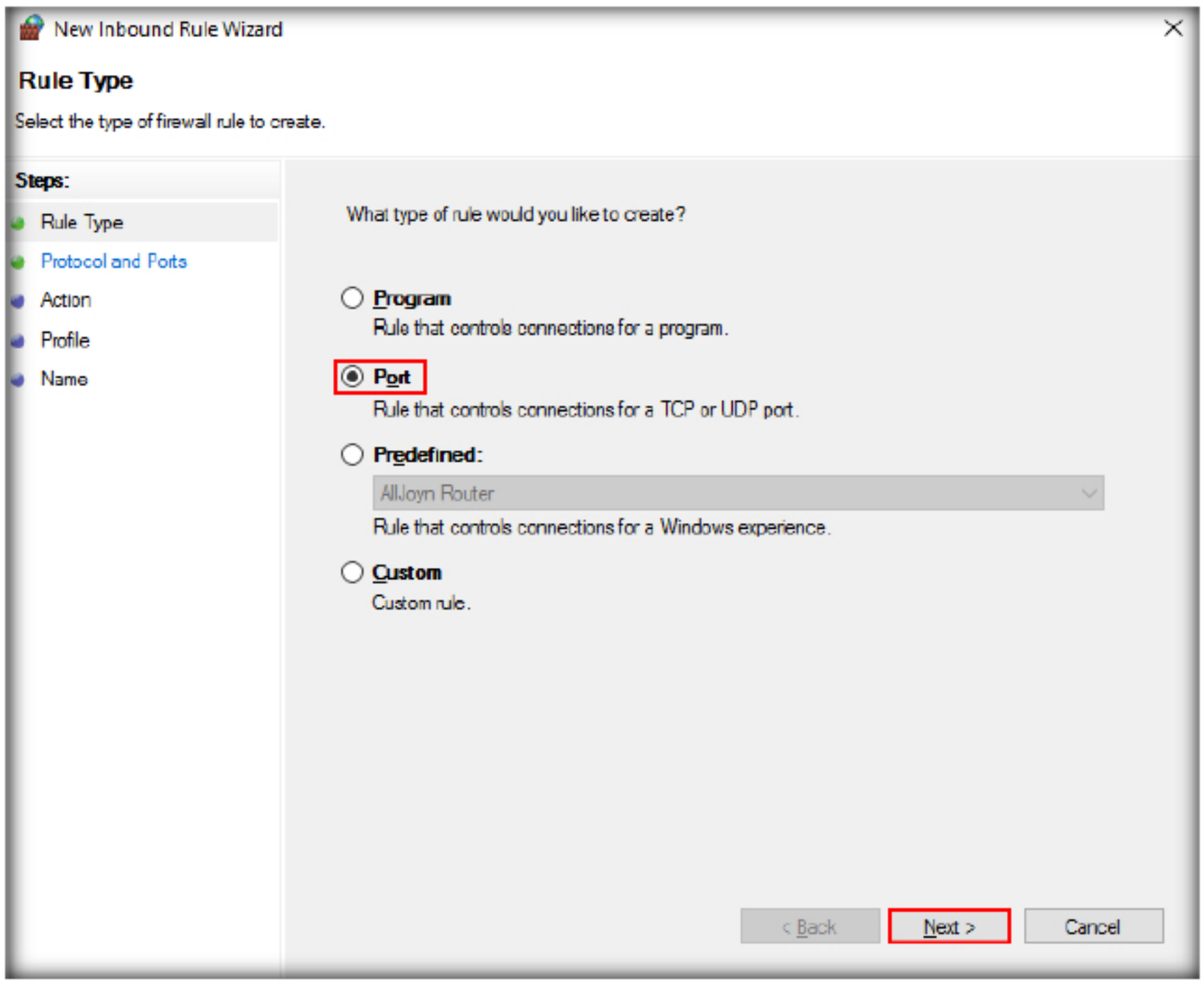
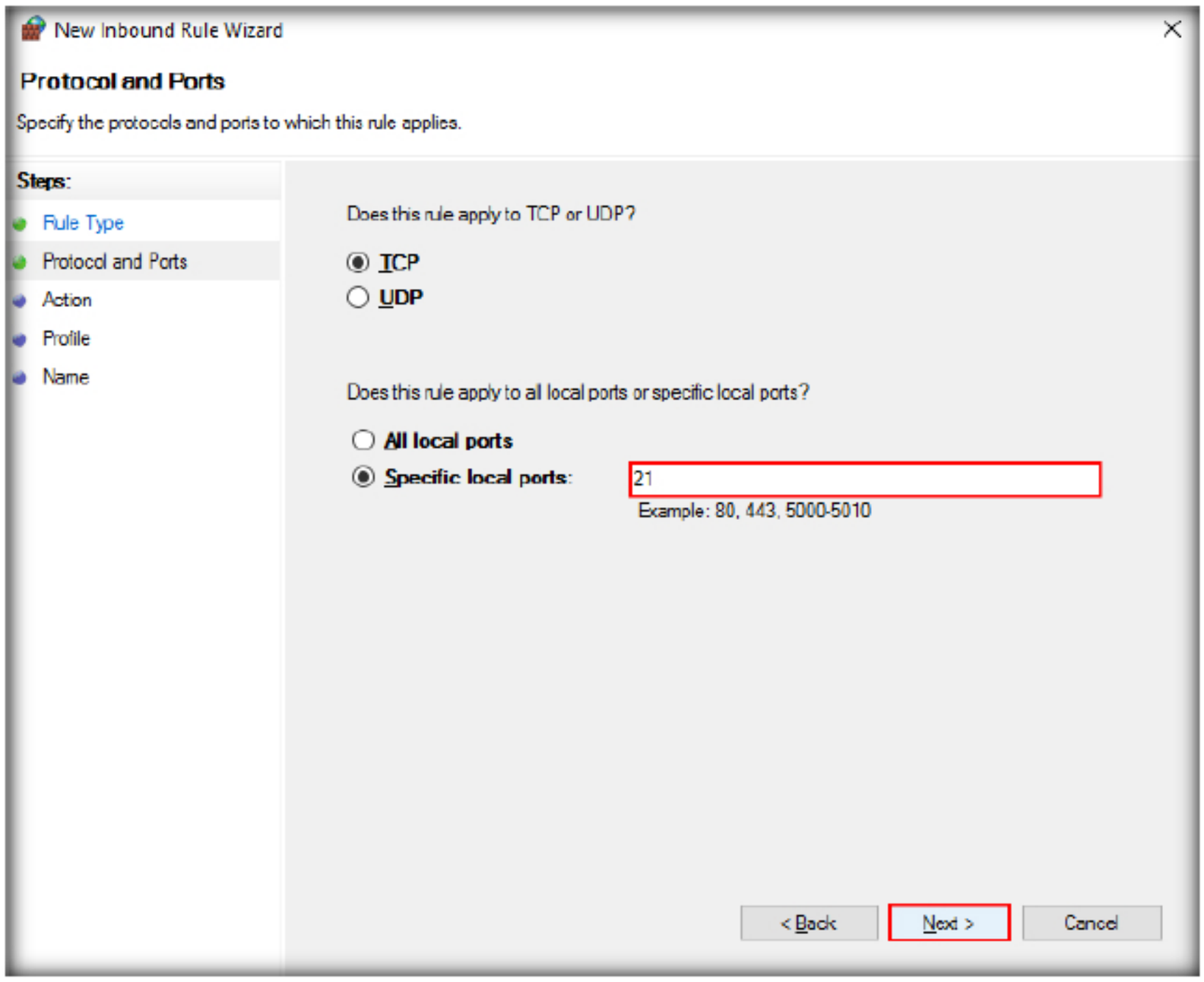


FIGURE 1.11: Creating an Inbound Rule for Allowing a Port

13. There are **four types** of rules you can create with a Windows firewall:
    a. **Program**: Related to programs and controls connections to programs installed on the device
    b. **Port**: These rules govern the access to TCP and UDP ports on the system
    c. **Predefined**: These rules govern the connections related to any Windows feature
    d. **Custom**: It applies to any specific program or service
14. **Protocols and Ports** section appears, enter port **21** in the **Specific local ports** field and click **Next**



📖 To allow a certain type of unsolicited inbound traffic, you must create an inbound rule that describes that traffic. For example, if you want to run a Web server, then you must create a rule that allows unsolicited inbound network traffic on TCP port 80.

FIGURE 1.12: Specifying a Port

15. The **Action** section appears, select the **Allow the connection** radio button and click **Next**.

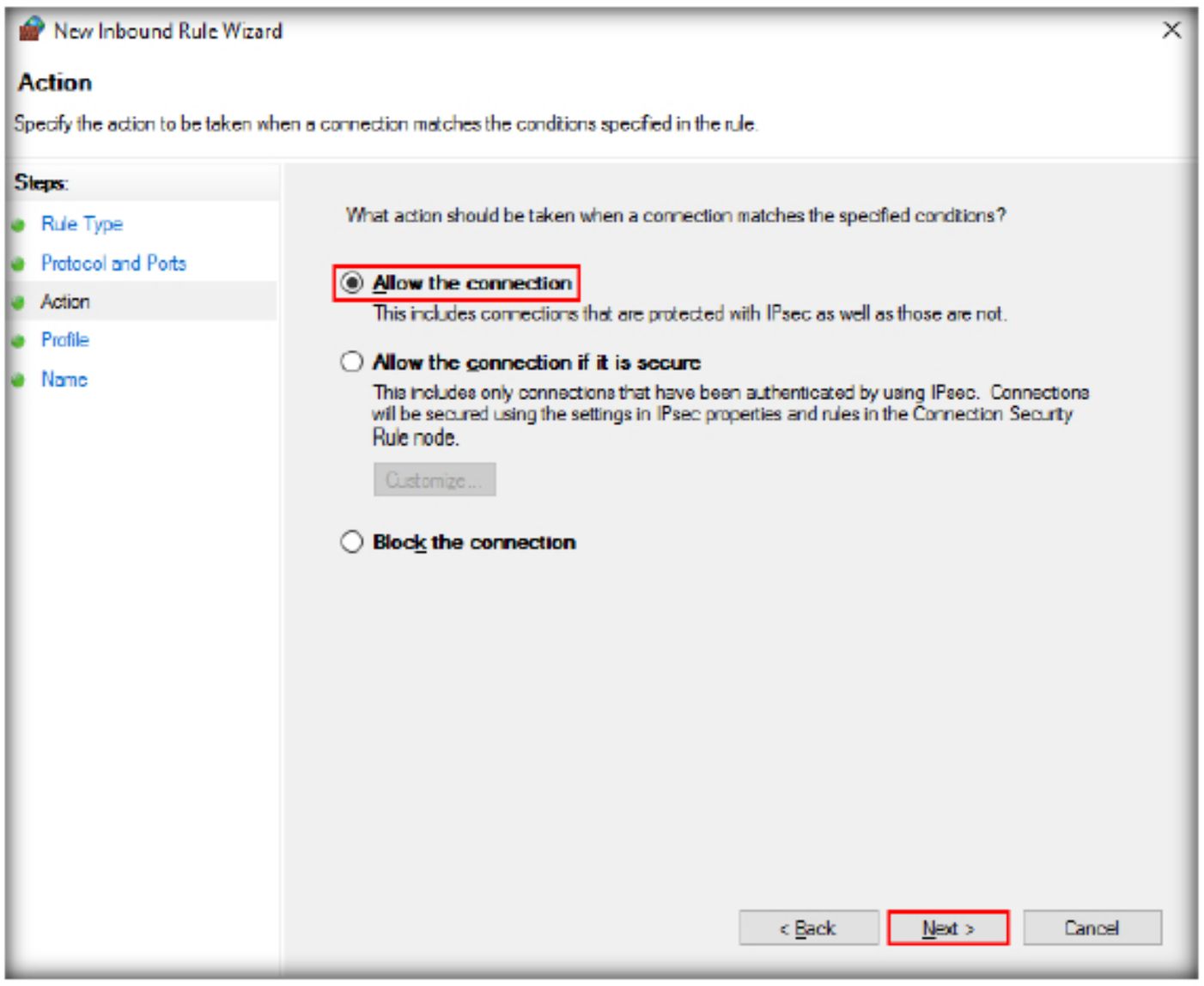


FIGURE 1.13: Allowing the Connection

16. The **Profile** section appears, check the **Domain** option, uncheck both the **Private** and **Public** options, then click **Next**.

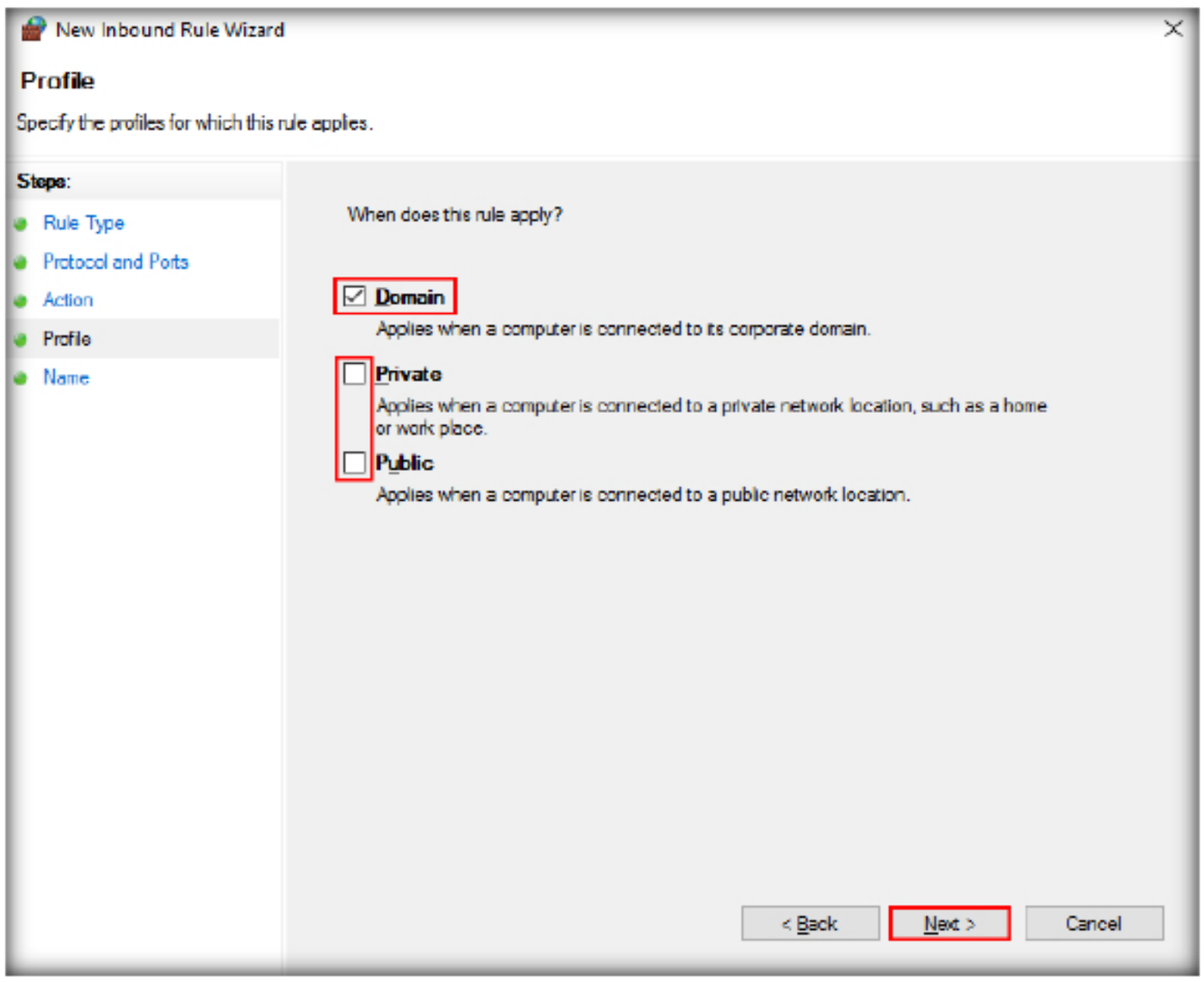


FIGURE 1.14: Choosing the Profiles

📖 The default behavior of Firewall is to block unsolicited inbound network traffic, but to allow all outbound network traffic. You can change the default behavior on the Domain Profile, Private Profile, and Public Profile tabs of the Windows Firewall with Advanced Security Properties dialog box.

📖 **Domain Profile:** Applied to a network adapter when it is connected to a network on which it can detect a domain controller of the domain to which the computer is joined.

17. The **Name** section appears, enter the name as **Port 21 Opened**, then click **Finish**.

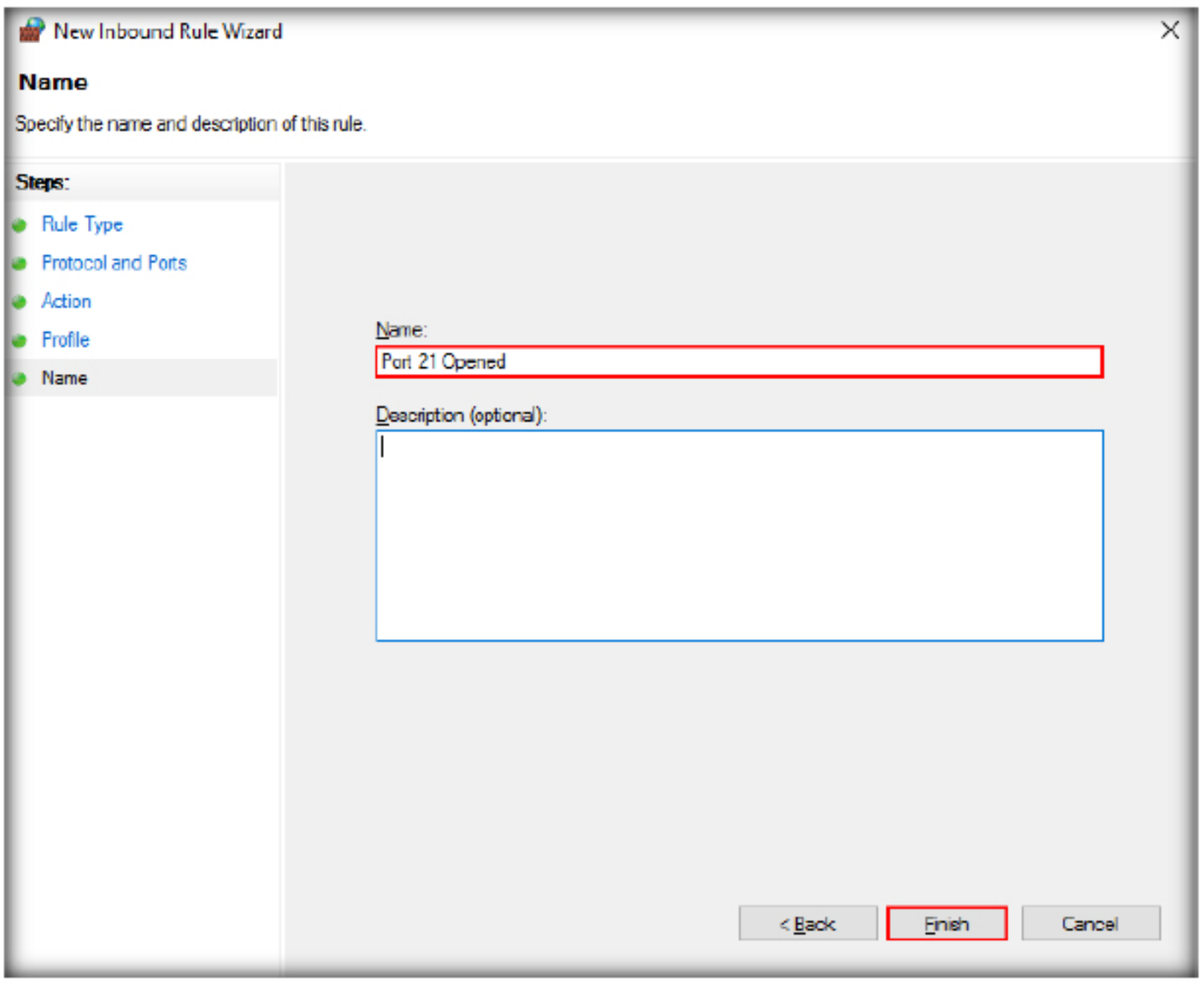


FIGURE 1.15: Finalizing the Rule

📖 **Private Profile:** Applied to a network adapter when it is connected to a network that is identified by the user or administrator as a private network. A private network is one that is not connected directly to the Internet, but is behind some kind of security device, such as a network address translation (NAT) router or hardware firewall.

18. The added rule appears under the list of inbound rules as shown in the following screenshot:

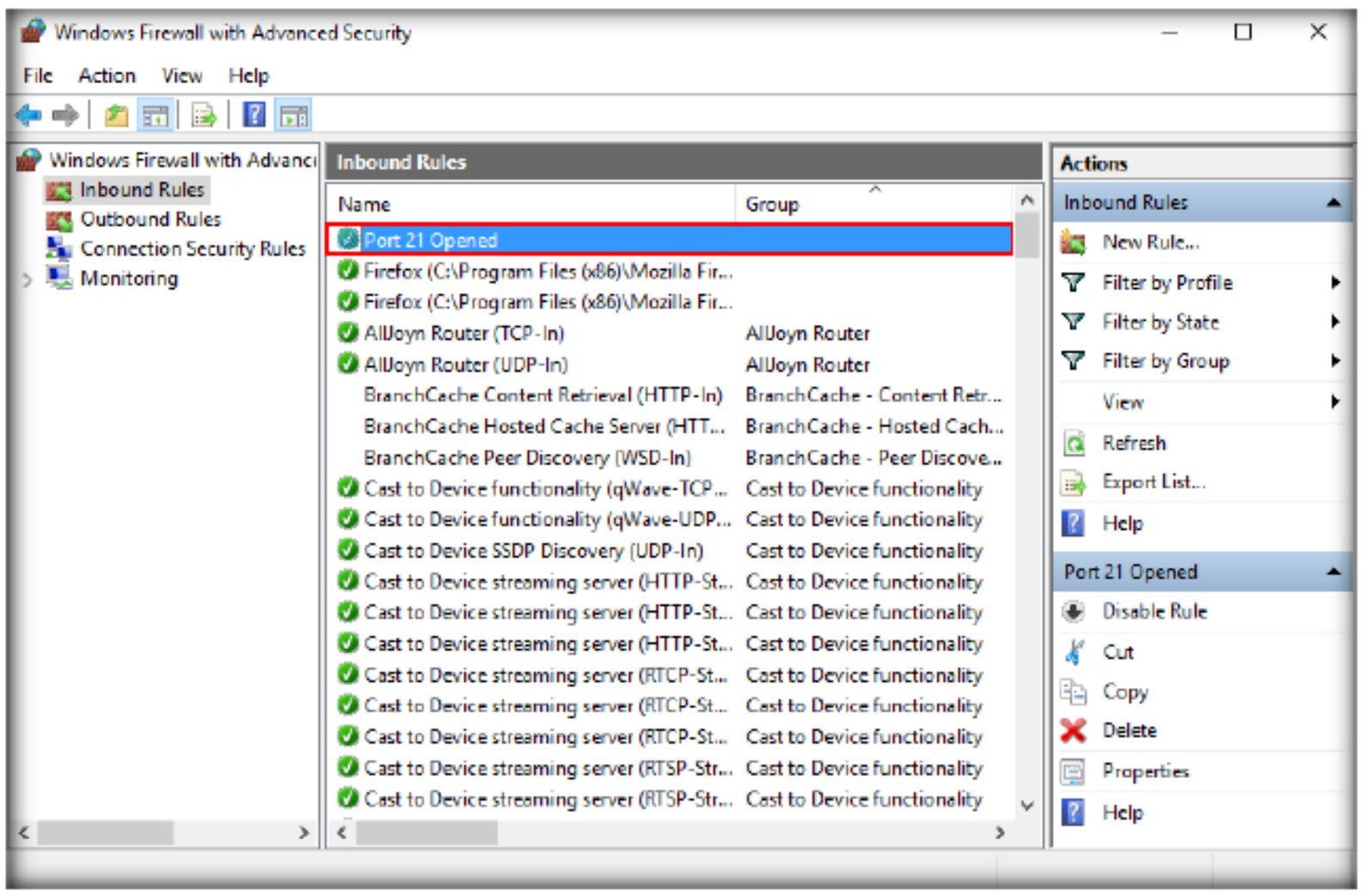


FIGURE 1.16: New Rule Created Successfully

📖 **Public Profile:** Applied to a network adapter when it is connected to a public network such as those available in airports and coffee shops. When the profile is not set to Domain or Private, the default profile is Public.

19. Now, switch to the **Ubuntu** virtual machine, type **ftp 10.10.10.10** in the command line terminal and press **Enter**.

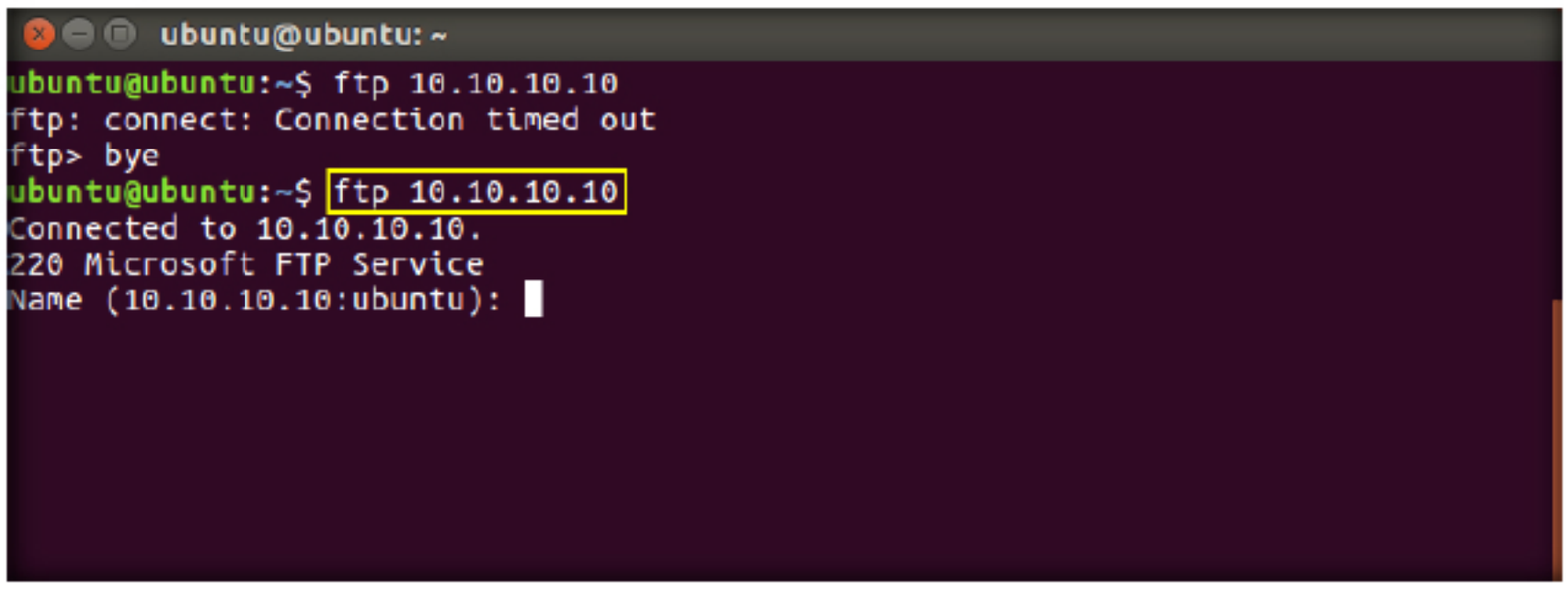


FIGURE 1.17: FTP Connection Attained Successfully

20. It is evident that you are able to connect to the FTP server hosted on the Windows 10 machine, by adding an inbound rule to open port **21**
21. In the same way, you may create inbound rules to allow or block access to ports, programs and services on the machine
22. Now, switch to the **Windows 10** virtual machine, minimize the **Windows Firewall with Advanced Security** window, launch a web browser, type **http://www.certifiedhacker.com** in the address bar and press **Enter**. You will be able to access the webpage as shown in the following screenshot:

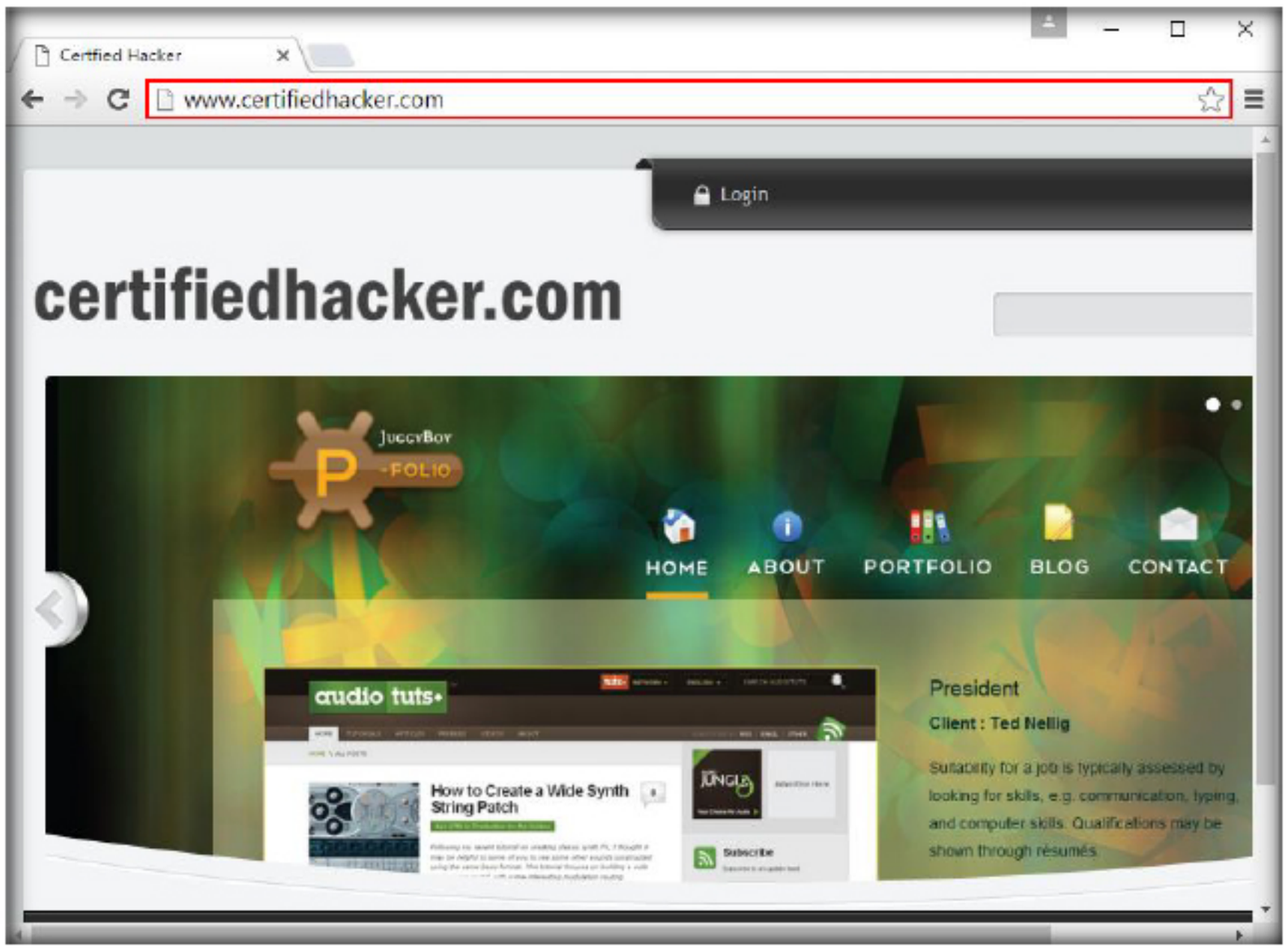


FIGURE 1.18: Browsing an HTTP Webpage

TASK 4

Creating Outbound rule

23. Now, we shall create an outbound rule to restrict a user from accessing HTTP enabled websites (by blocking port **80**), so that they will access only https enabled websites on the Internet.
24. Minimize the web browser, maximize the **Windows Firewall with Advanced Security** window, and click **Outbound Rules** in the left pane.
25. The **Outbound Rules** window appears, click **New rule** in the right pane.

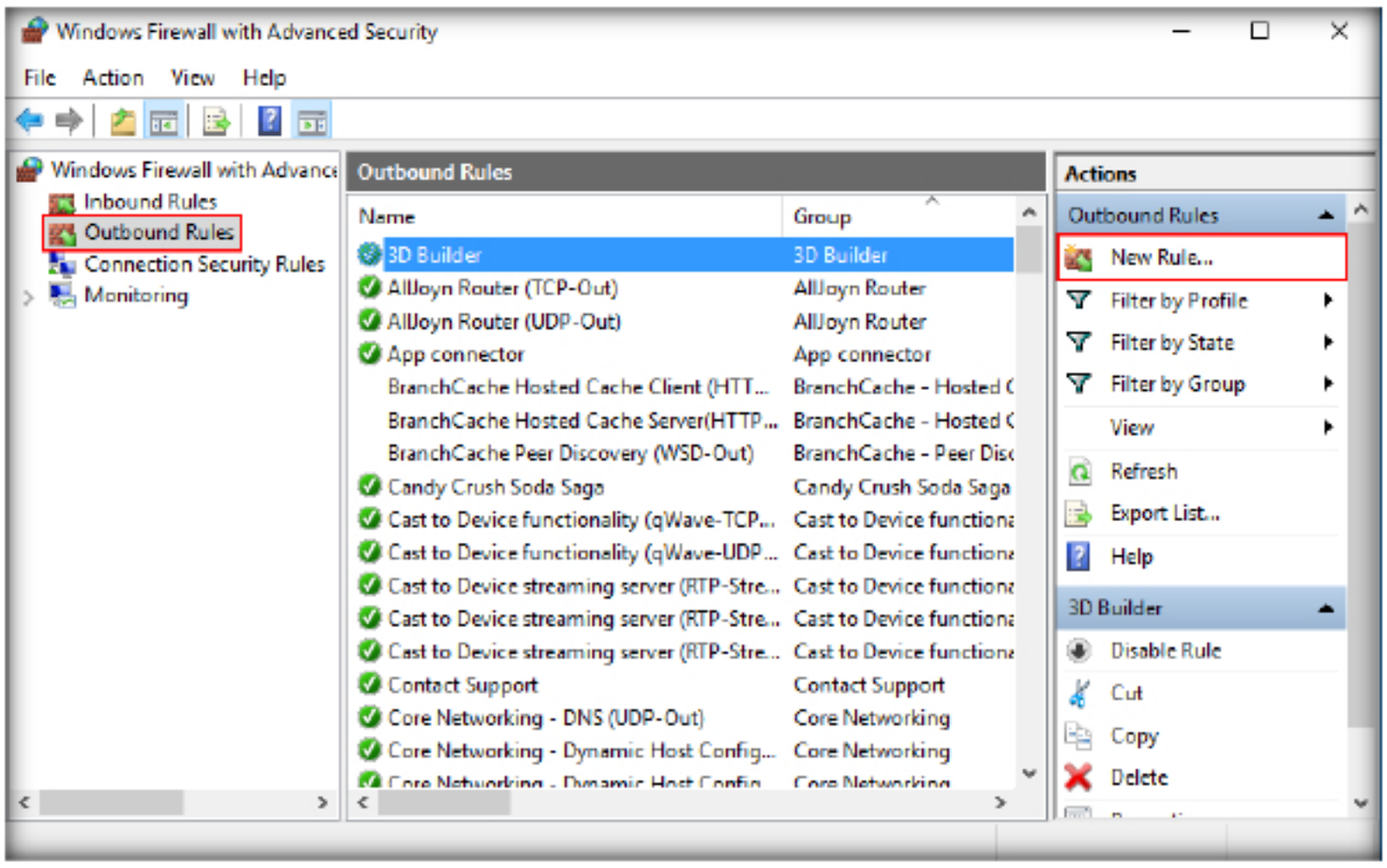


FIGURE 1.19: Navigating towards creation of a New Outbound Rule

26. The **New Outlook Rule Wizard** appears, select the **Port** radio button and click **Next**.

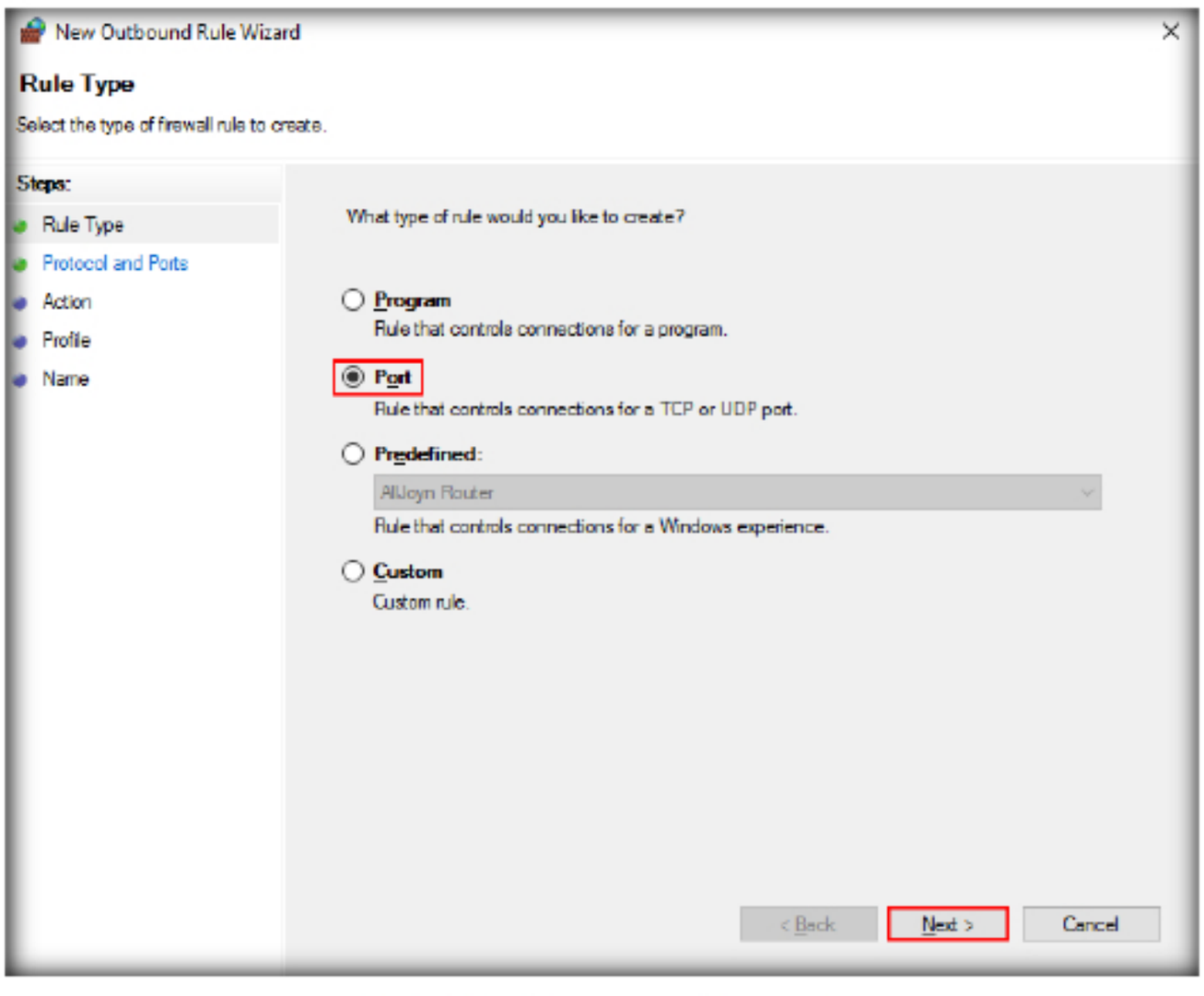


FIGURE 1.20: Creating a new Program rule

📖 Outbound rules explicitly allow, or explicitly block, network traffic originating from the computer that matches the criteria in the rule. For example, you can configure a rule to explicitly block outbound traffic to a computer (by IP address) through the firewall, but allow the same traffic for other computers.

📖 You can also configure the default action the Windows Firewall with Advanced Security takes, whether outbound connections are allowed or blocked, when no outbound rule applies.

27. The **Ports and Protocols** section appears, enter port **80** for the **Specific remote ports** field and click **Next**.

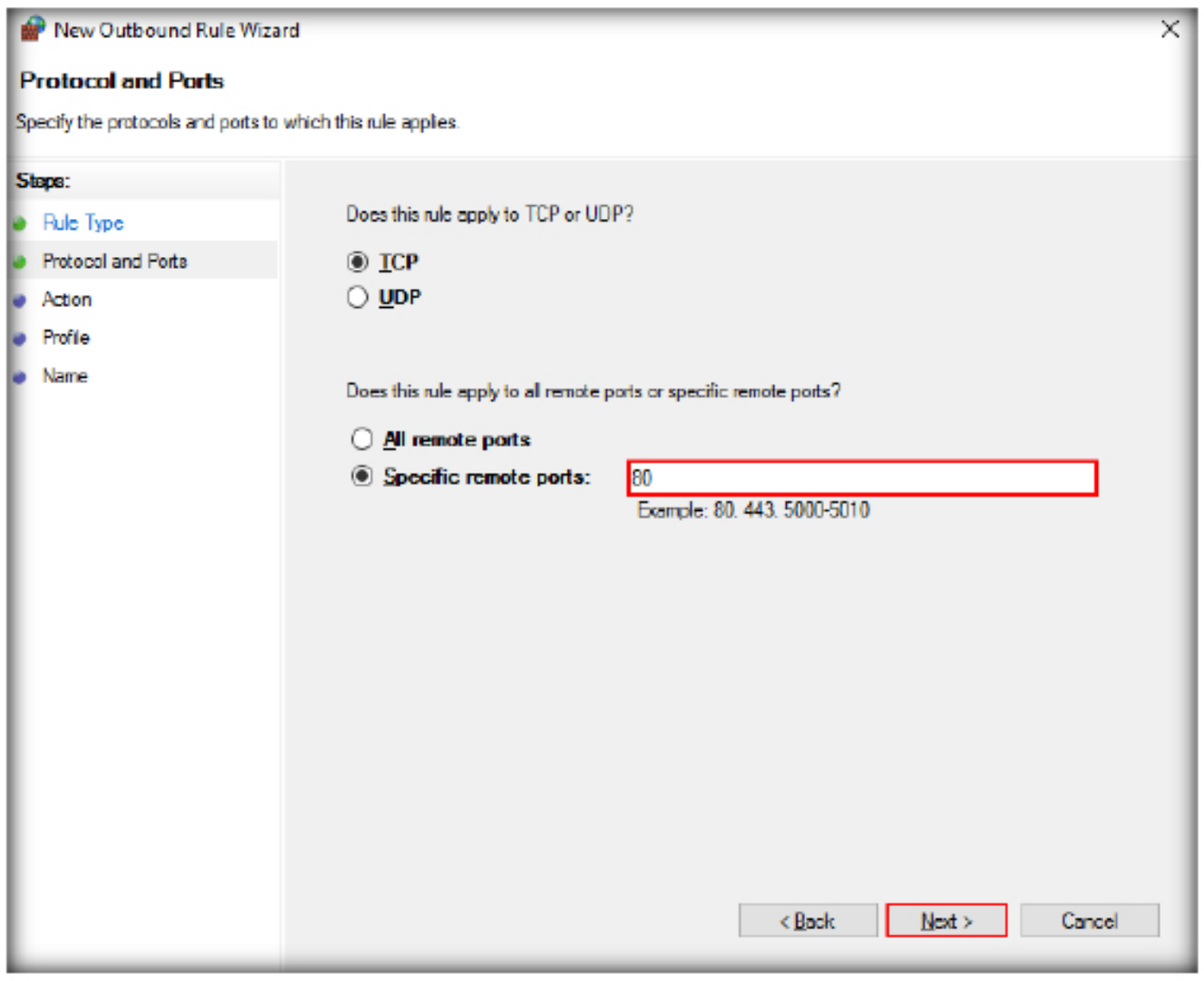


FIGURE 1.21: Specifying a Port

28. In the **Action** section, select the **Block the connection** radio button and click **Next**.

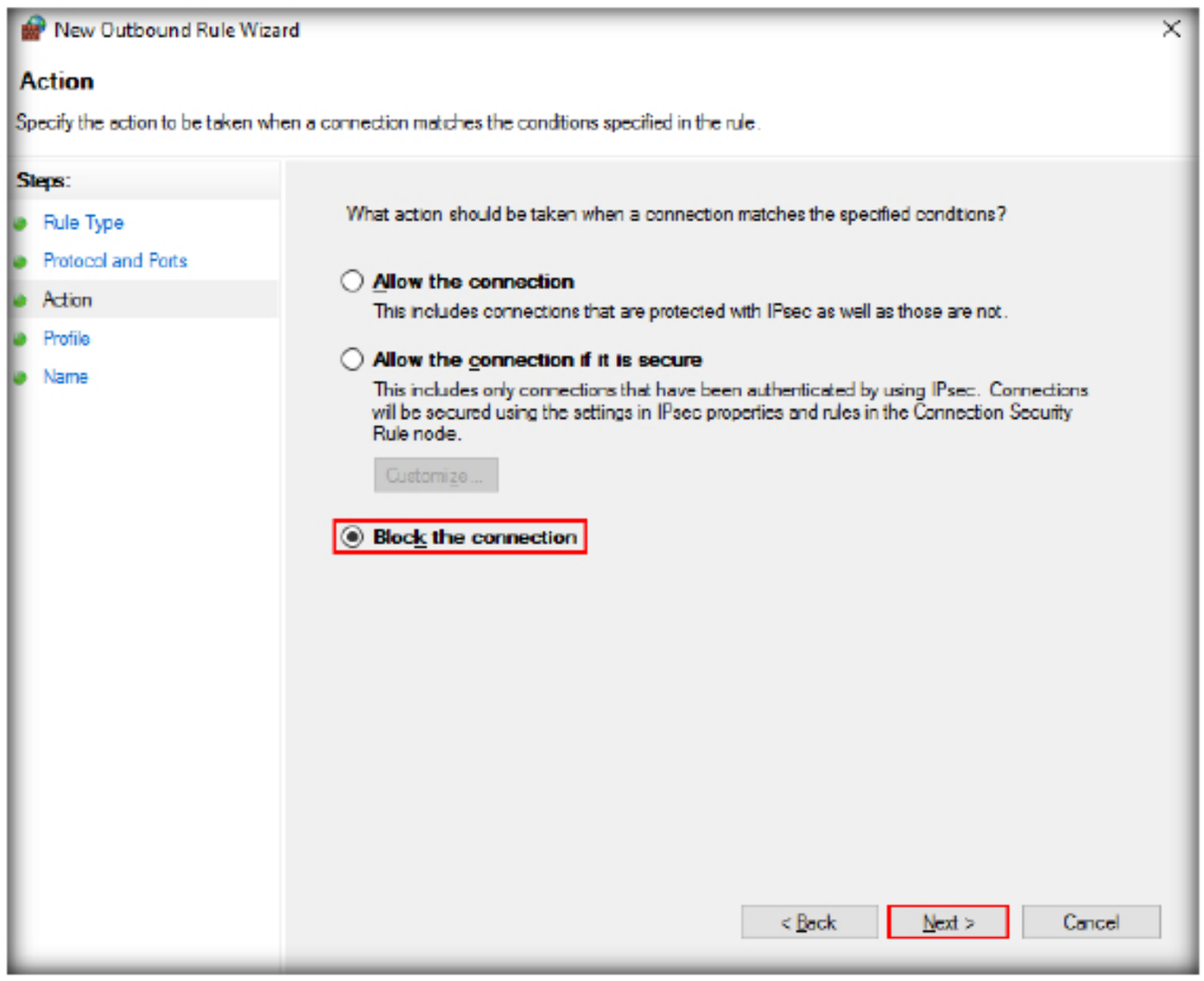


FIGURE 1.22: Blocking the Rule

29. The **Profile** section appears, check the **Domain**, **Private** and **Public** options, then click **Next**.

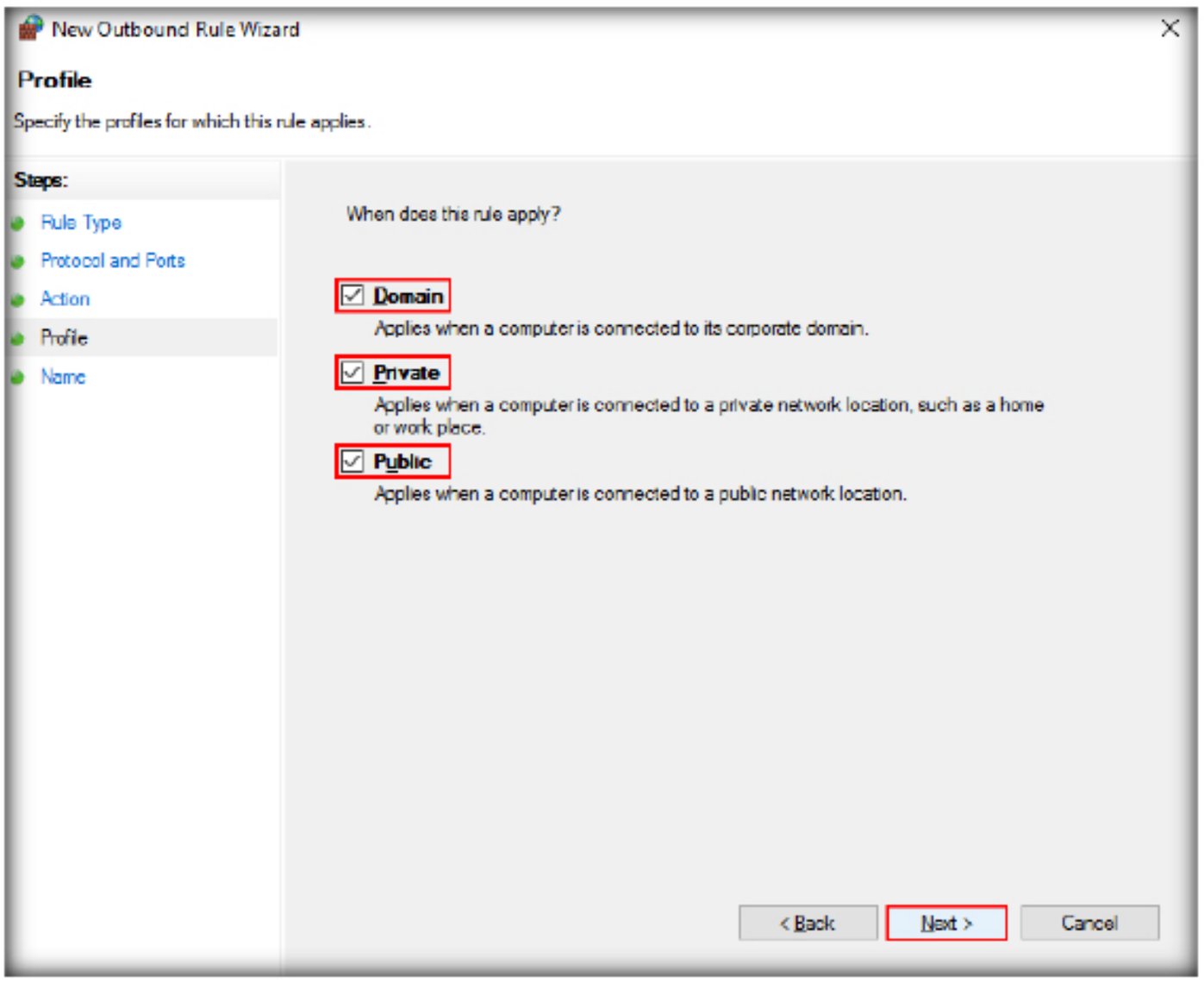


FIGURE 1.23: Selecting the Profiles

30. The **Name** section appears, enter the name as **Port 80 Blocked**, and click **Finish**.

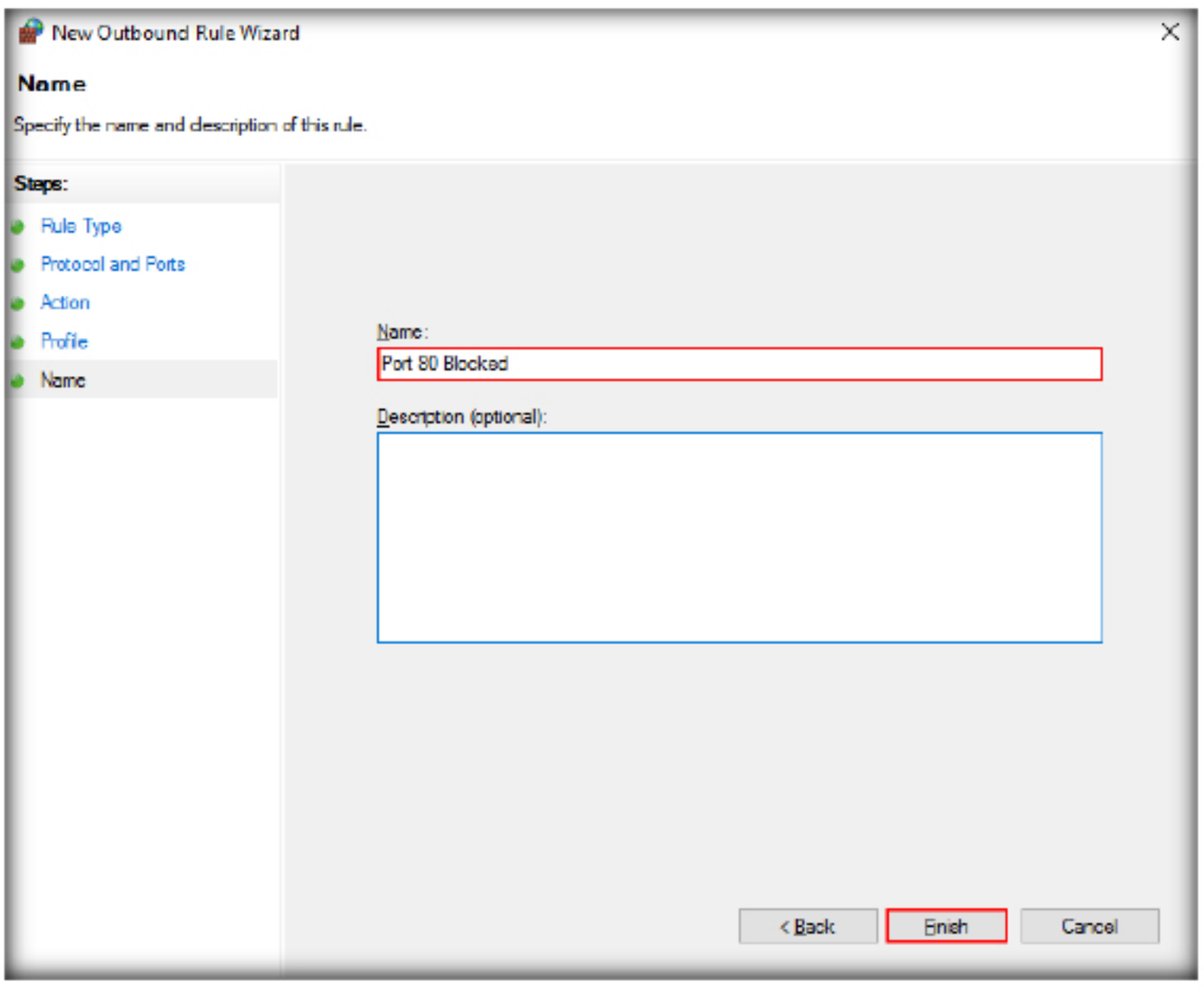


FIGURE 1.24: Finalizing the Rule

31. The added rule appears under the list of outbound rules as shown in the following screenshot:

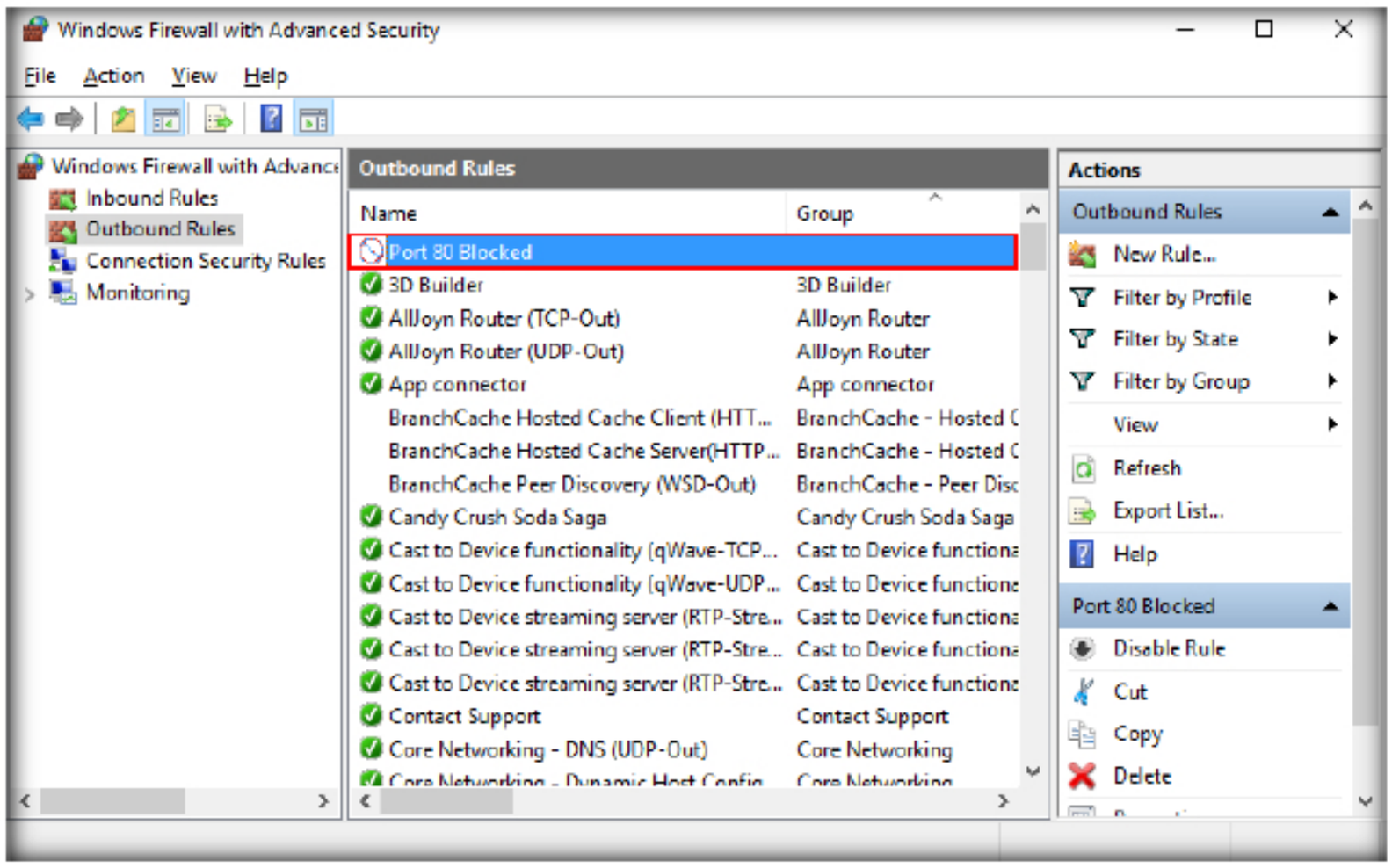


FIGURE 1.25: New Rule created successfully

32. Now, maximize the web browser, and reload the **certifiedhacker** website. You will notice the Internet access is blocked, stating the firewall or antivirus has blocked the connection as shown in the following screenshot:

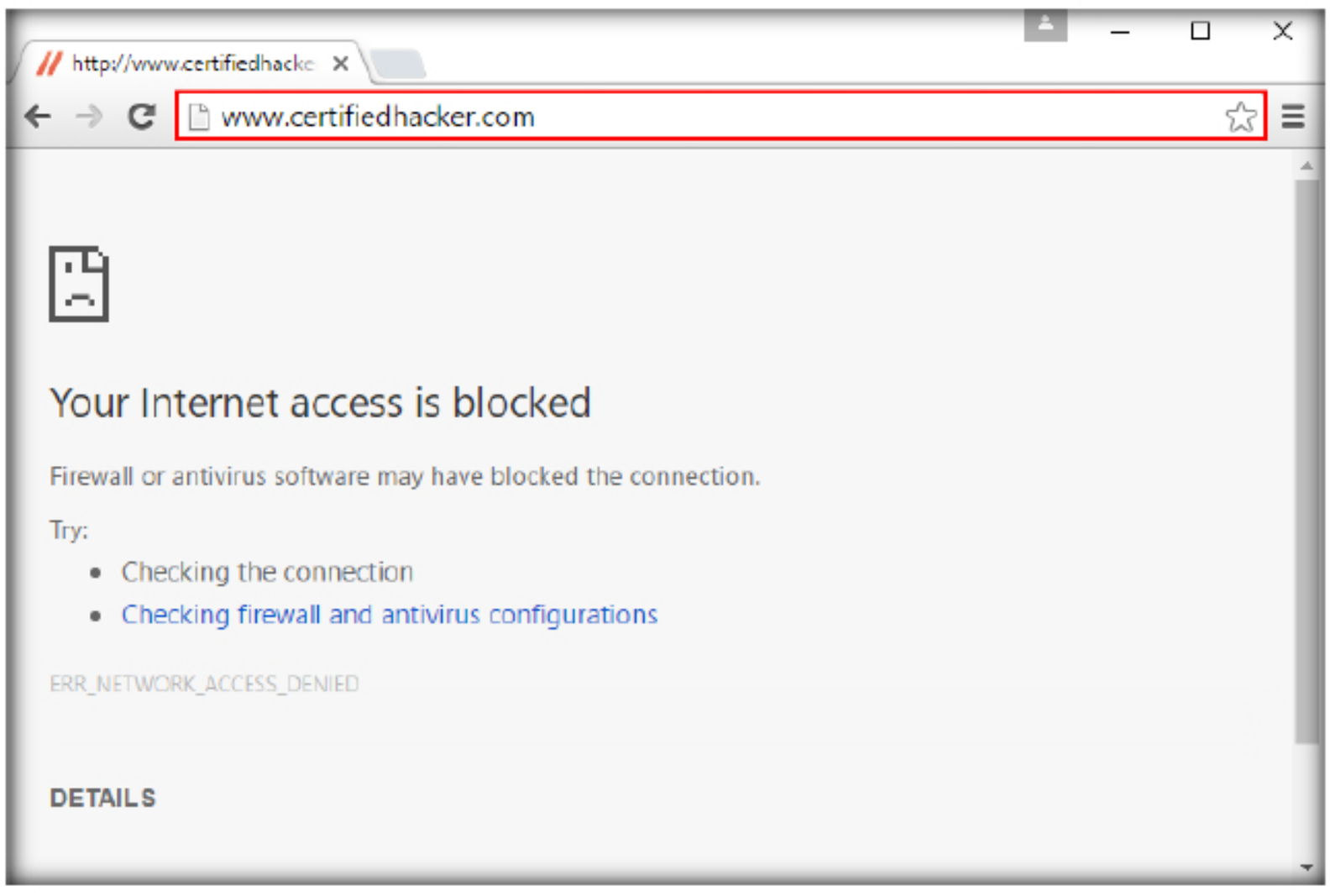


FIGURE 1.26: Website Restricted by Firewall

33. Open a new tab, type **https://www.eccouncil.org** and press **Enter**. You will be able to browse the website as shown in the following screenshot:

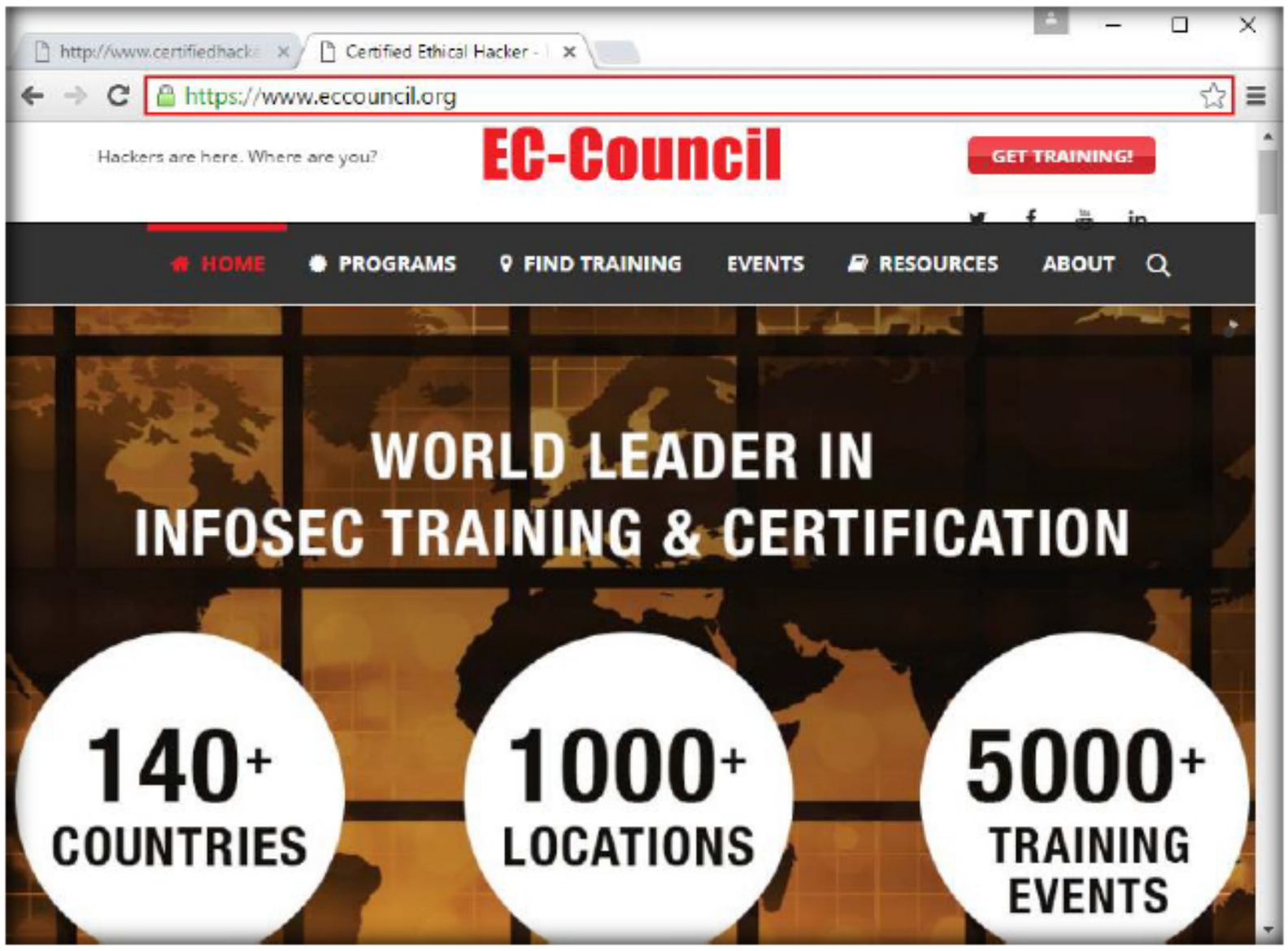


FIGURE 1.27: HTTPS Website Successfully Accessed

34. This signifies the firewall is blocking all websites that can be accessed through port 80, and allowing only websites using https, ensuring that the data is not flowing in plain-text.

Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs