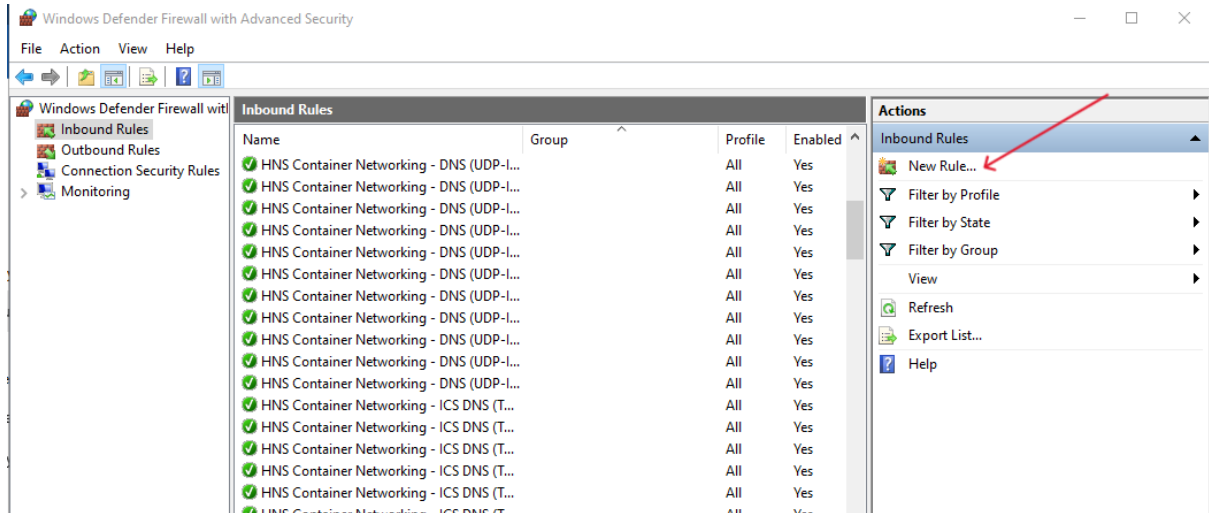


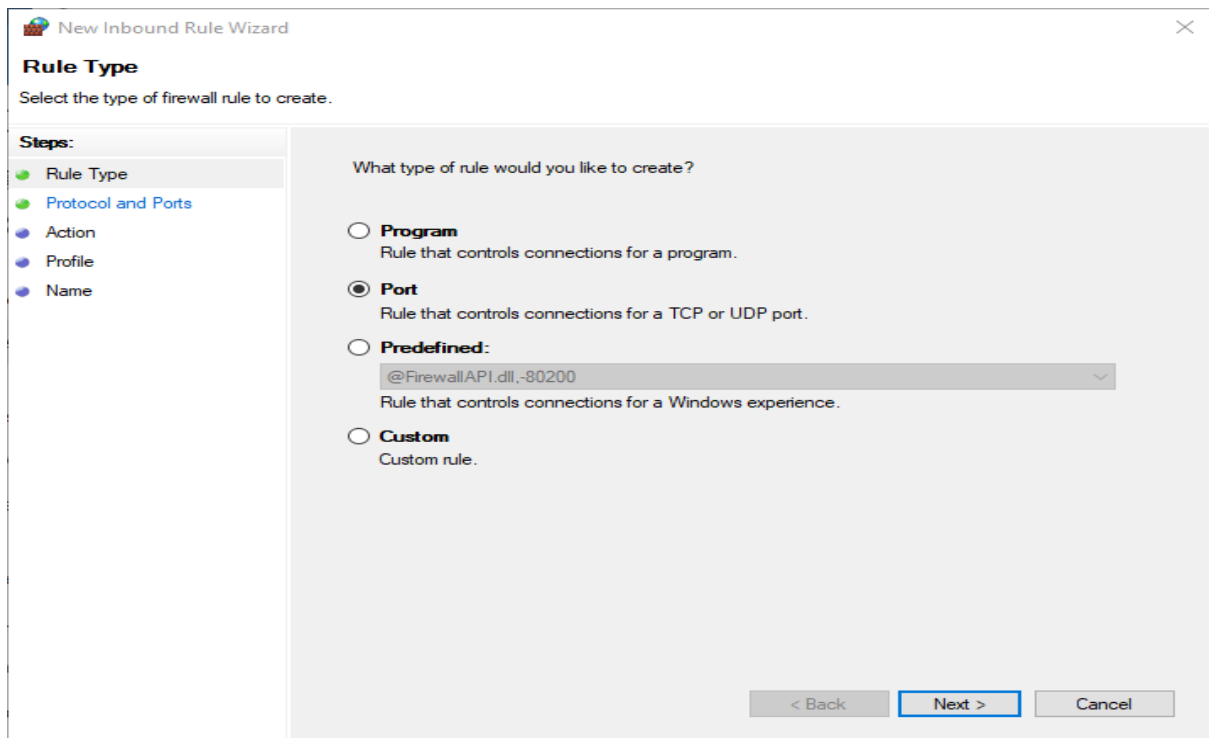
Step 2: Create a Rule to Allow HTTPS Traffic

Windows Firewall:

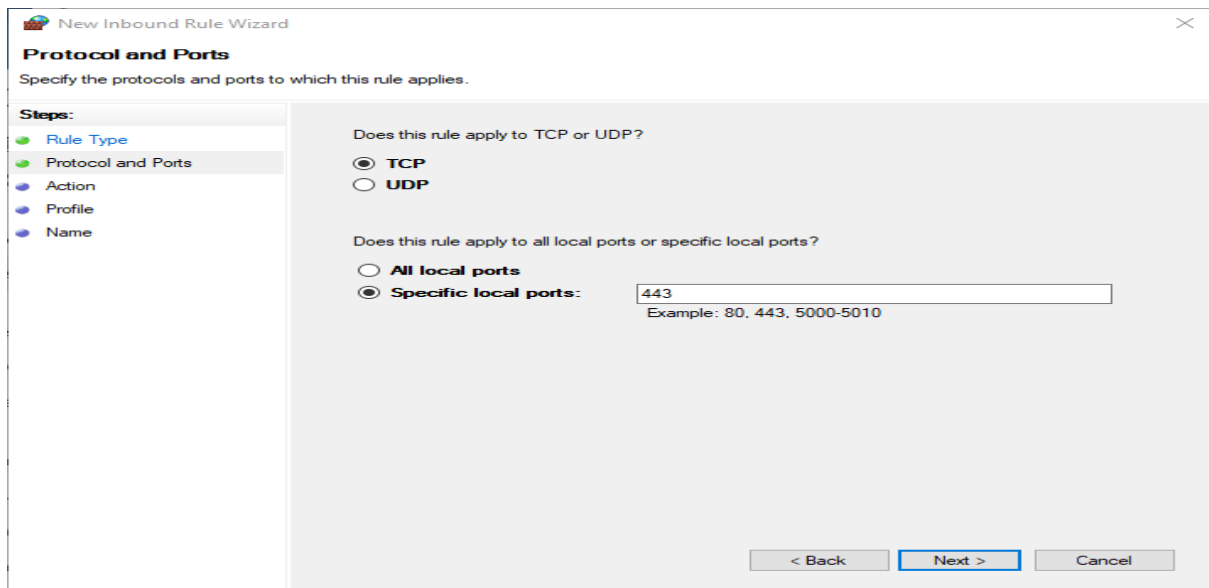
1. Click on New Rule in the right-hand panel.



2. Select Port as the rule type and click Next.

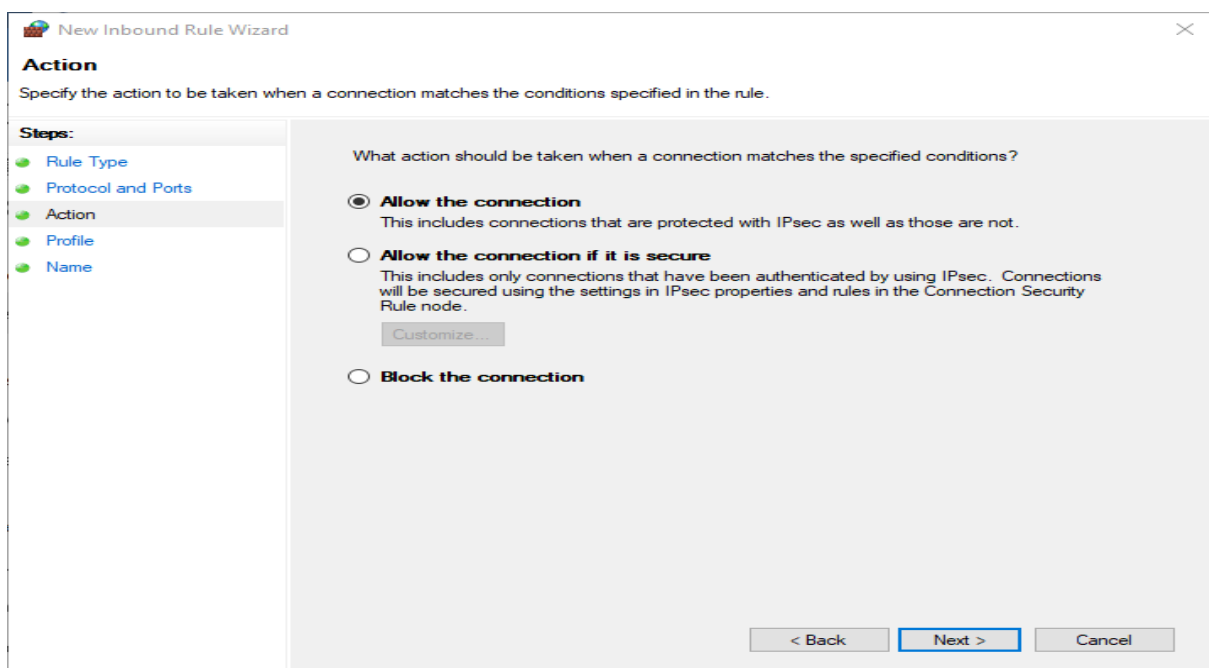


3. Choose TCP and specify port `443` (the default port for HTTPS).



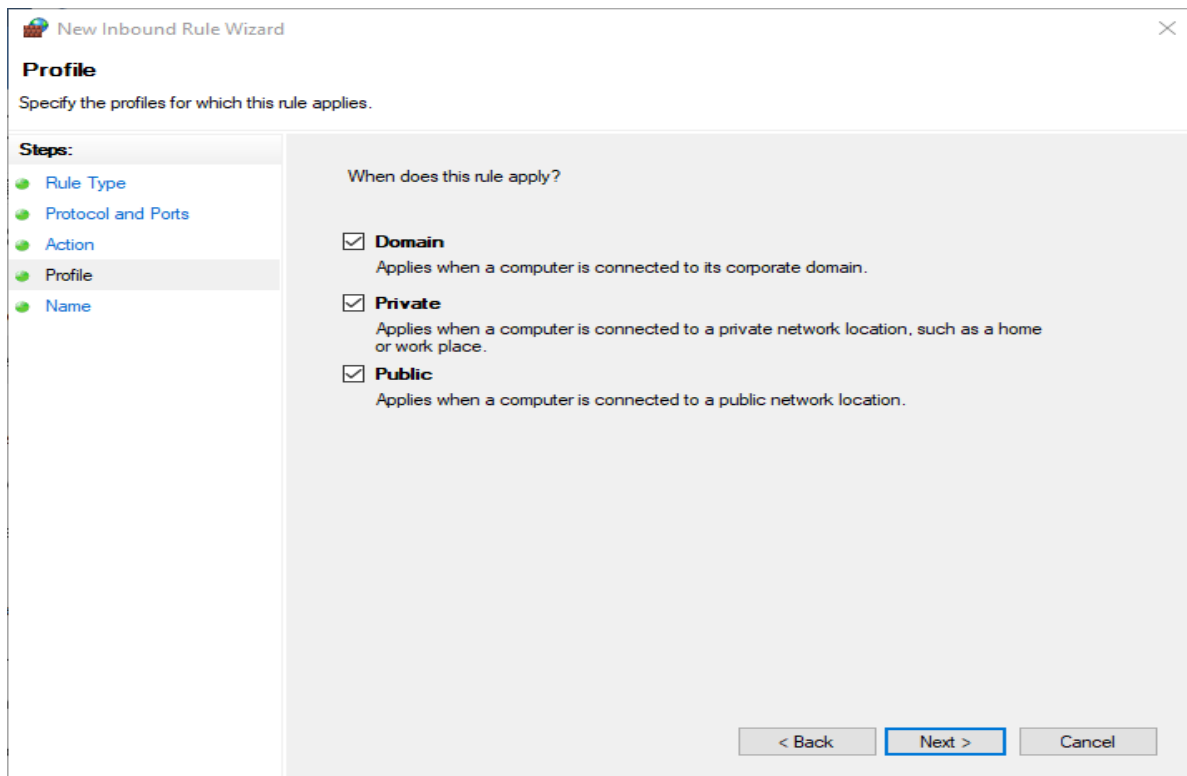
The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The left sidebar lists the steps: Rule Type, Protocol and Ports (selected), Action, Profile, and Name. The main area contains two questions. The first question is 'Does this rule apply to TCP or UDP?' with radio buttons for TCP (selected) and UDP. The second question is 'Does this rule apply to all local ports or specific local ports?' with radio buttons for All local ports and Specific local ports (selected). A text box next to 'Specific local ports' contains the value '443', with an example 'Example: 80, 443, 5000-5010' below it. At the bottom right are buttons for '< Back', 'Next >' (highlighted), and 'Cancel'.

4. Select Allow the connection and click Next.



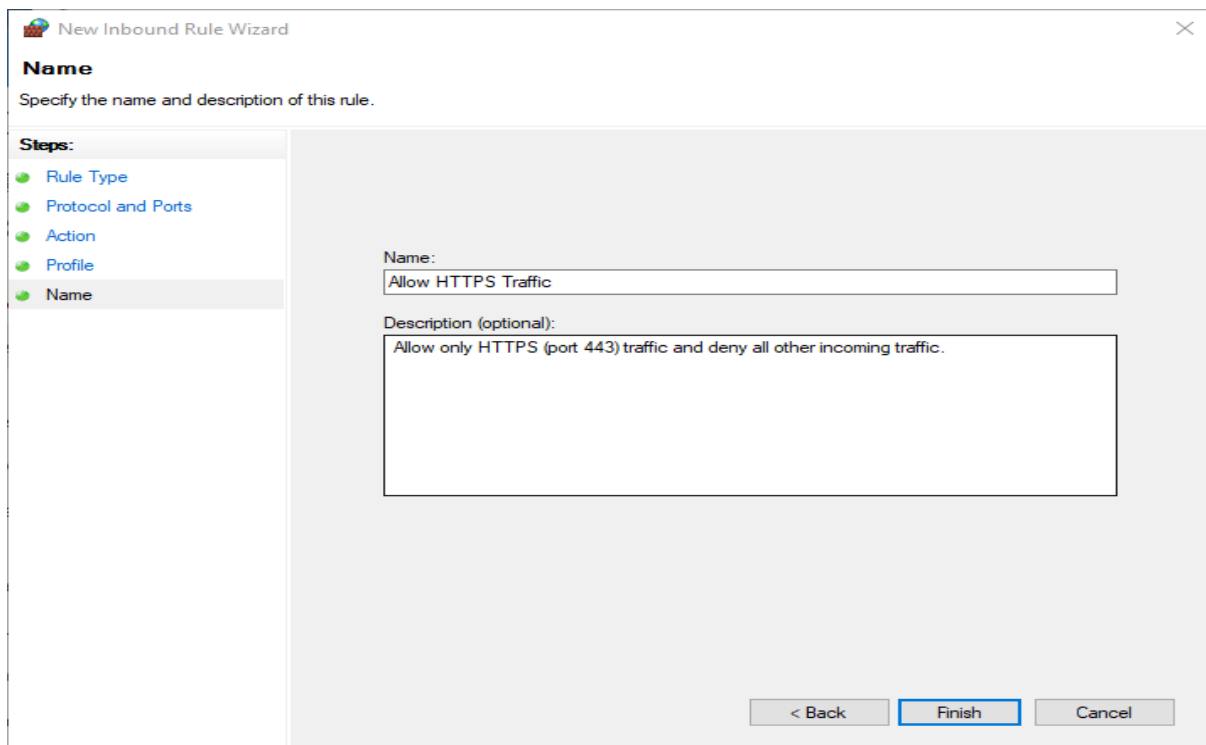
The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Action' step. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action (selected), Profile, and Name. The main area contains the question 'What action should be taken when a connection matches the specified conditions?'. There are three radio button options: 'Allow the connection' (selected), 'Allow the connection if it is secure', and 'Block the connection'. The 'Allow the connection' option has a description: 'This includes connections that are protected with IPsec as well as those are not.' The 'Allow the connection if it is secure' option has a description: '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.' and a 'Customize...' button. At the bottom right are buttons for '< Back', 'Next >' (highlighted), and 'Cancel'.

5. Apply the rule to Domain, Private, and Public networks.



The screenshot shows the 'New Inbound Rule Wizard' window at the 'Profile' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Profile' with the instruction 'Specify the profiles for which this rule applies.' On the left, a 'Steps:' pane lists 'Rule Type', 'Protocol and Ports', 'Action', 'Profile' (highlighted), and 'Name'. The main area is titled 'When does this rule apply?' and contains three checked options: '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.), and 'Public' (Applies when a computer is connected to a public network location.). At the bottom right are buttons for '< Back', 'Next >' (highlighted), and 'Cancel'.

6. Name the rule (e.g., "Allow HTTPS Traffic") and click Finish.



The screenshot shows the 'New Inbound Rule Wizard' window at the 'Name' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Name' with the instruction 'Specify the name and description of this rule.' On the left, a 'Steps:' pane lists 'Rule Type', 'Protocol and Ports', 'Action', 'Profile', and 'Name' (highlighted). The main area has a 'Name:' label followed by a text box containing 'Allow HTTPS Traffic'. Below it is a 'Description (optional):' label followed by a text box containing 'Allow only HTTPS (port 443) traffic and deny all other incoming traffic.'. At the bottom right are buttons for '< Back', 'Finish' (highlighted), and 'Cancel'.

For Linux (IPTables):

Run the following command to allow HTTPS traffic to your server:

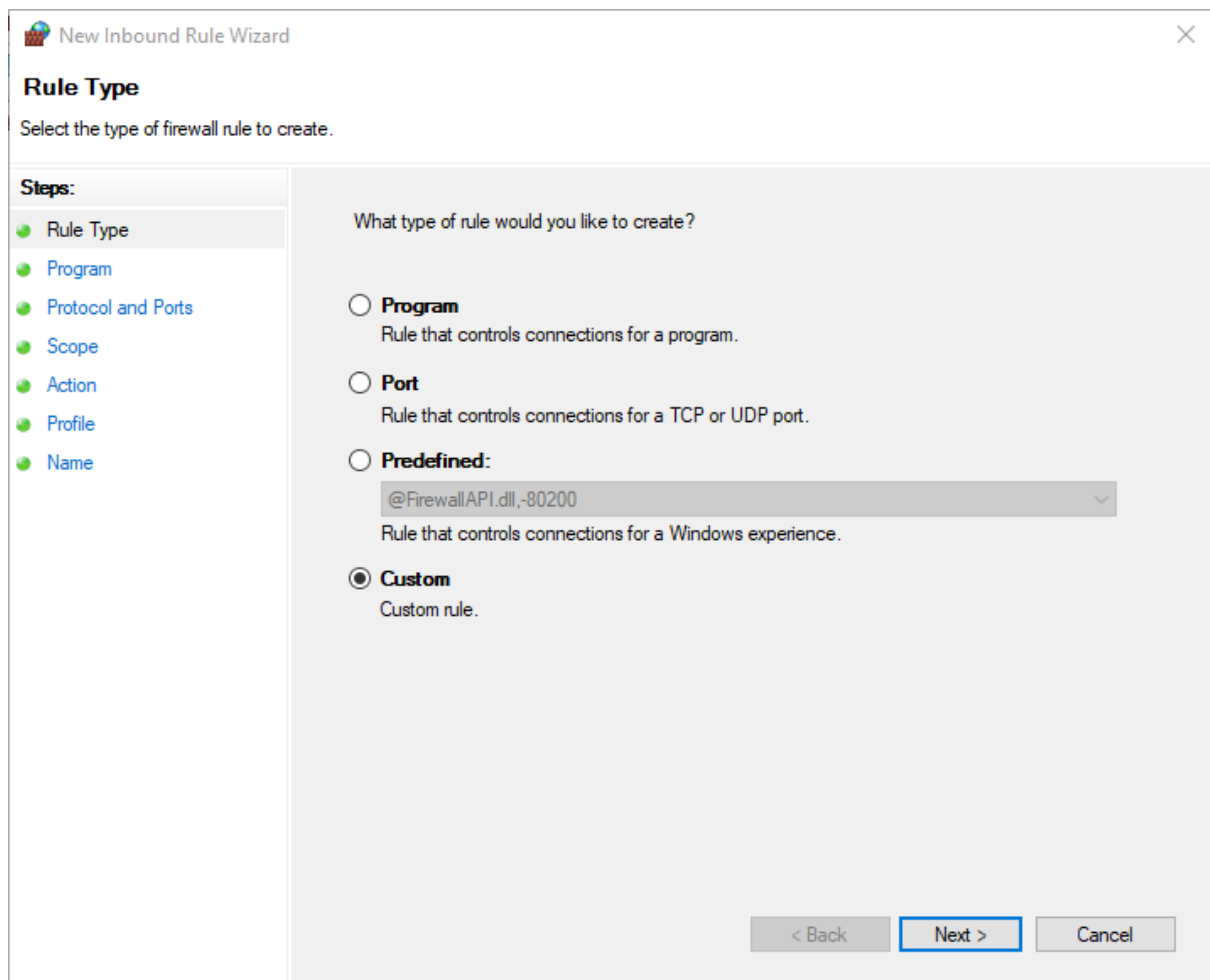
```
sudo iptables -A INPUT -p tcp --dport 443 -d 192.168.1.100 -j ACCEPT
```

Replace `192.168.1.100` with your server's IP address.

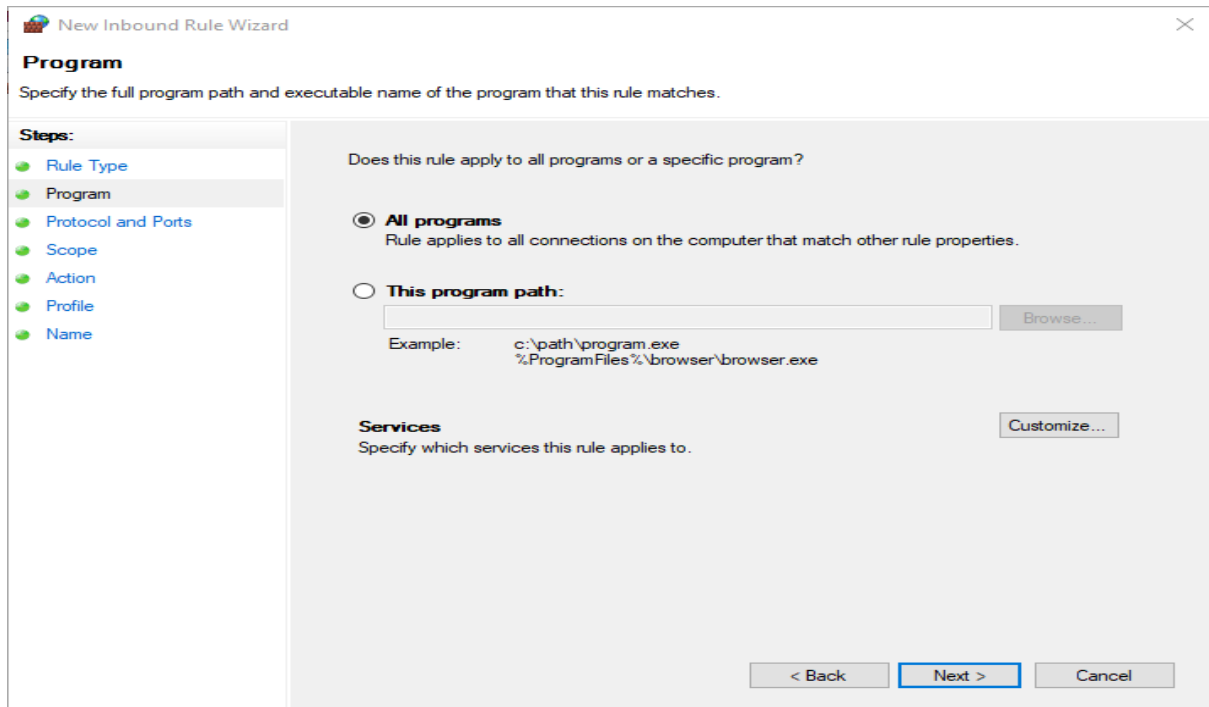
Step 3: Deny All Other Incoming Traffic

For Windows Firewall:

1. Create a new rule:
2. Rule Type: Select Custom and click Next

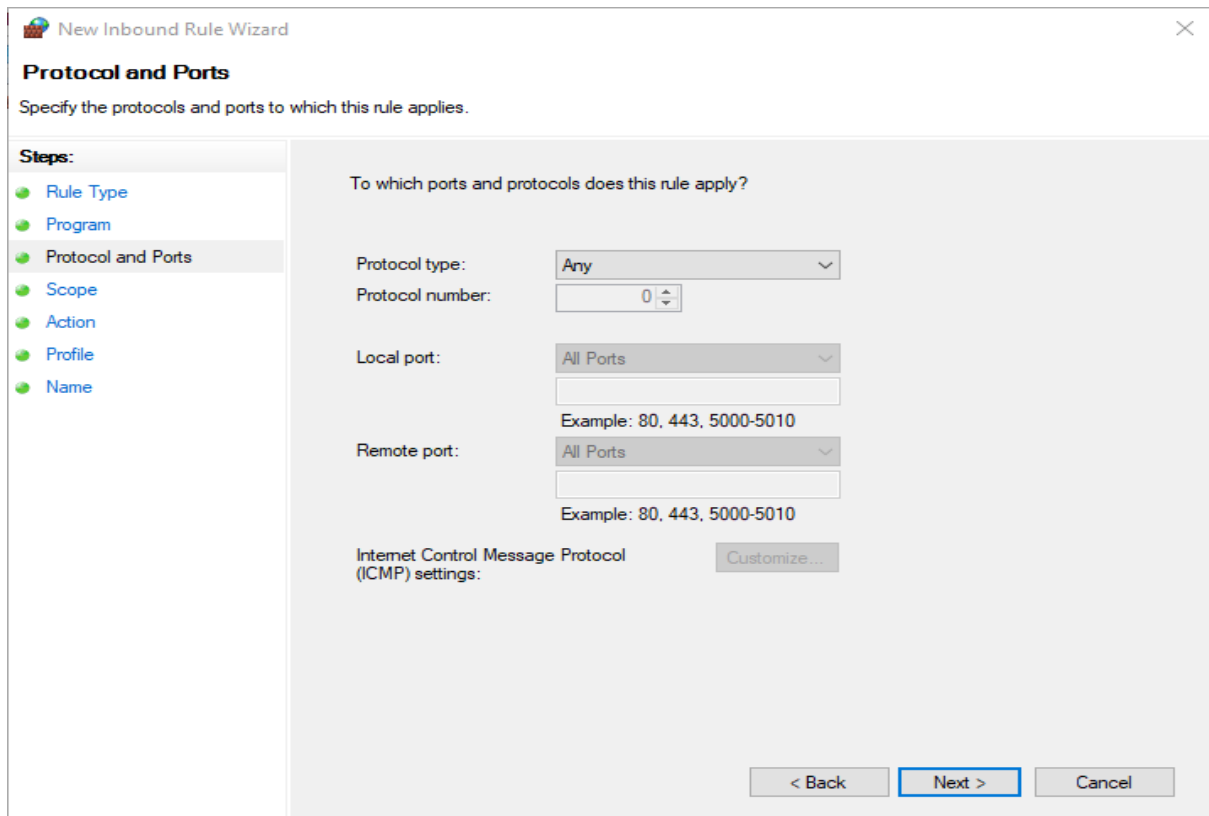


3. Program: Choose All Programs and click Next.



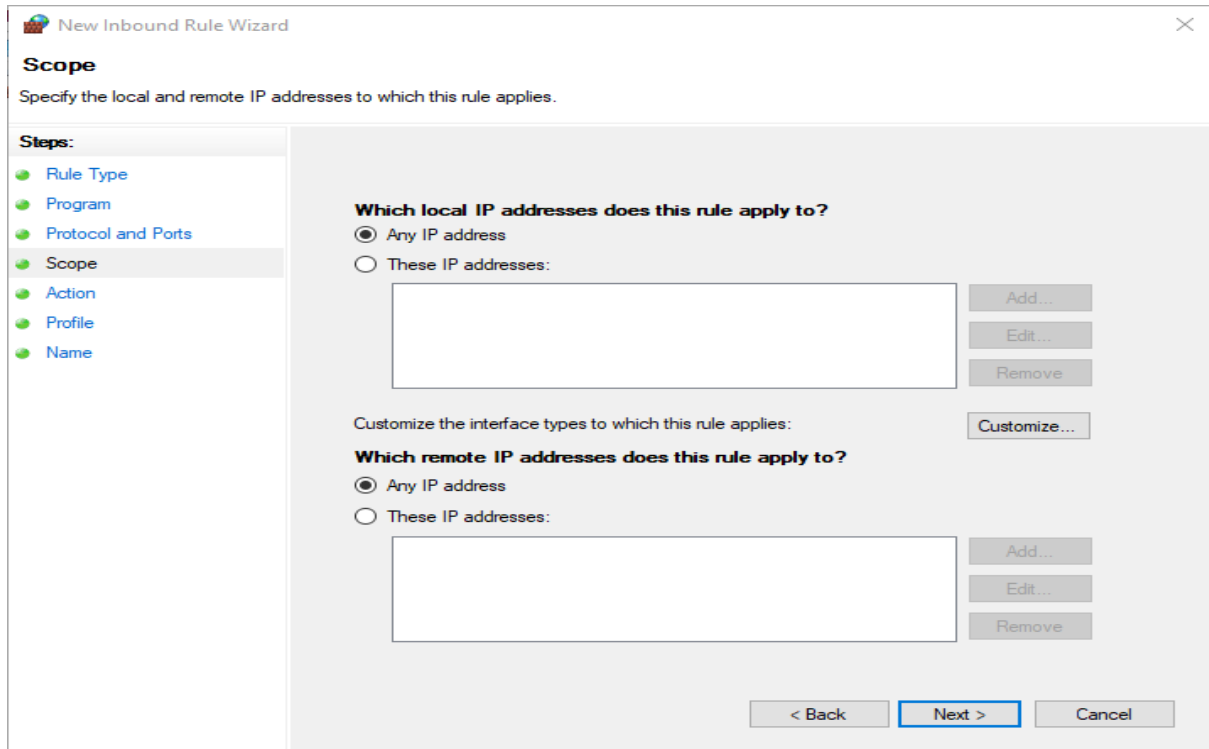
The screenshot shows the 'New Inbound Rule Wizard' window at the 'Program' step. The title bar reads 'New Inbound Rule Wizard'. The left sidebar lists the steps: Rule Type, Program (selected), Protocol and Ports, Scope, Action, Profile, and Name. The main area is titled 'Program' and contains the instruction 'Specify the full program path and executable name of the program that this rule matches.' Below this, it asks 'Does this rule apply to all programs or a specific program?'. There are two radio button options: 'All programs' (selected) and 'This program path:'. The 'All programs' option has a sub-instruction 'Rule applies to all connections on the computer that match other rule properties.' The 'This program path:' option has a text input field and a 'Browse...' button. Below the input field, it shows an example: 'Example: c:\path\program.exe' and '%ProgramFiles%\browser\browser.exe'. At the bottom of the main area, there is a 'Services' section with the instruction 'Specify which services this rule applies to.' and a 'Customize...' button. At the bottom right of the window are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

4. Protocol and Ports: Leave as Any and click Next.



The screenshot shows the 'New Inbound Rule Wizard' window at the 'Protocol and Ports' step. The title bar reads 'New Inbound Rule Wizard'. The left sidebar lists the steps: Rule Type, Program, Protocol and Ports (selected), Scope, Action, Profile, and Name. The main area is titled 'Protocol and Ports' and contains the instruction 'Specify the protocols and ports to which this rule applies.' Below this, it asks 'To which ports and protocols does this rule apply?'. There are four input fields: 'Protocol type:' with a dropdown menu set to 'Any'; 'Protocol number:' with a spinner box set to '0'; 'Local port:' with a dropdown menu set to 'All Ports' and a text input field below it; and 'Remote port:' with a dropdown menu set to 'All Ports' and a text input field below it. Below the text input fields, it shows an example: 'Example: 80, 443, 5000-5010'. At the bottom of the main area, there is an 'Internet Control Message Protocol (ICMP) settings:' section with a 'Customize...' button. At the bottom right of the window are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

5. Scope: Keep the default settings (applies to all IP addresses) and click Next.



The screenshot shows the 'New Inbound Rule Wizard' window at the 'Scope' step. The left sidebar lists the steps: Rule Type, Program, Protocol and Ports, Scope (selected), Action, Profile, and Name. The main area is titled 'Specify the local and remote IP addresses to which this rule applies.' It contains two sections: 'Which local IP addresses does this rule apply to?' and 'Which remote IP addresses does this rule apply to?'. Both sections have a radio button for 'Any IP address' (which is selected) and a radio button for 'These IP addresses:' followed by a text box and 'Add...', 'Edit...', and 'Remove' buttons. There is also a 'Customize...' button for interface types. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

New Inbound 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?

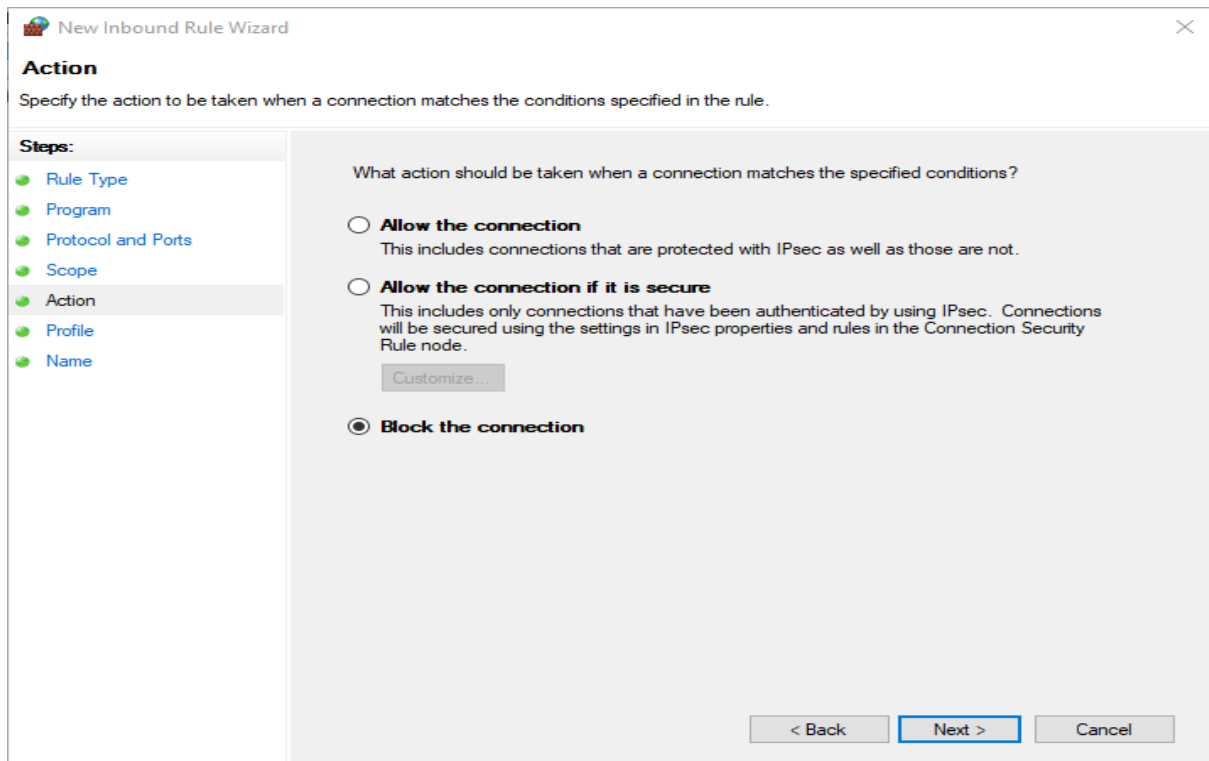
☒ Any IP address

☐ These IP addresses:

Add... Edit... Remove

< Back Next > Cancel

6. Action: Select Block the connection and click Next.



The screenshot shows the 'New Inbound Rule Wizard' window at the 'Action' step. The left sidebar lists the steps: Rule Type, Program, Protocol and Ports, Scope, Action (selected), Profile, and Name. The main area is titled 'Specify the action to be taken when a connection matches the conditions specified in the rule.' It contains a section 'What action should be taken when a connection matches the specified conditions?' with three radio button options: 'Allow the connection' (with a description), 'Allow the connection if it is secure' (with a description and a 'Customize...' button), and 'Block the connection' (which is selected). At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

New Inbound 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?

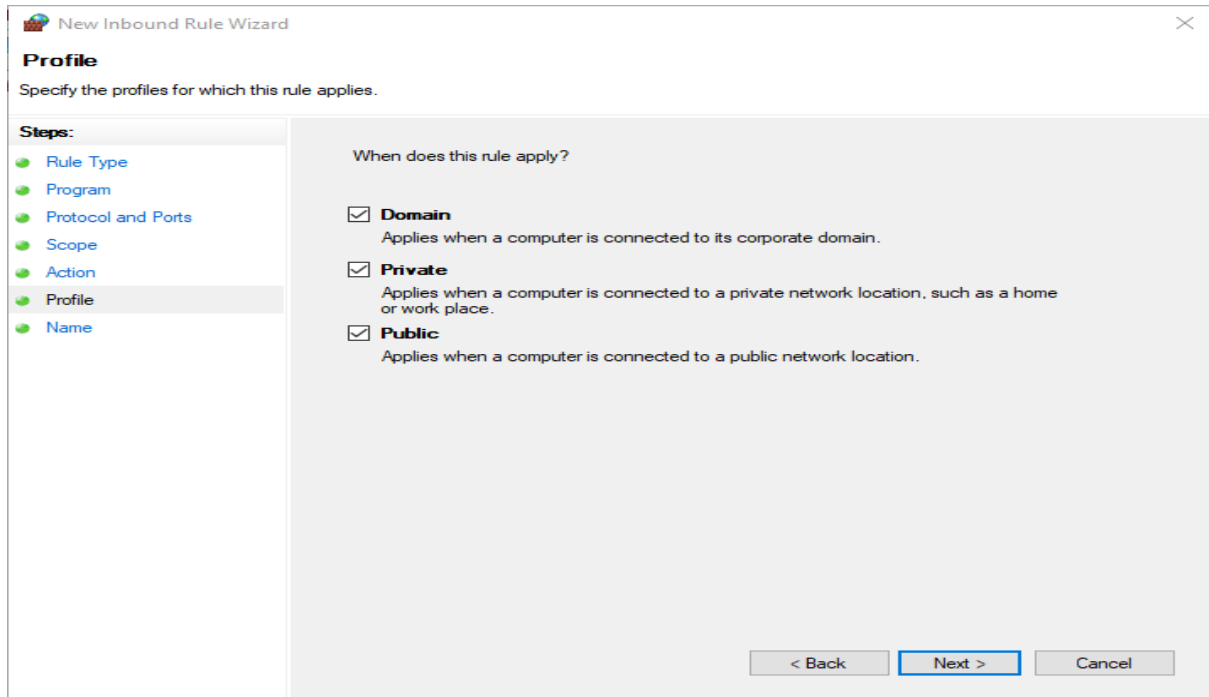
☐ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

☐ **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**

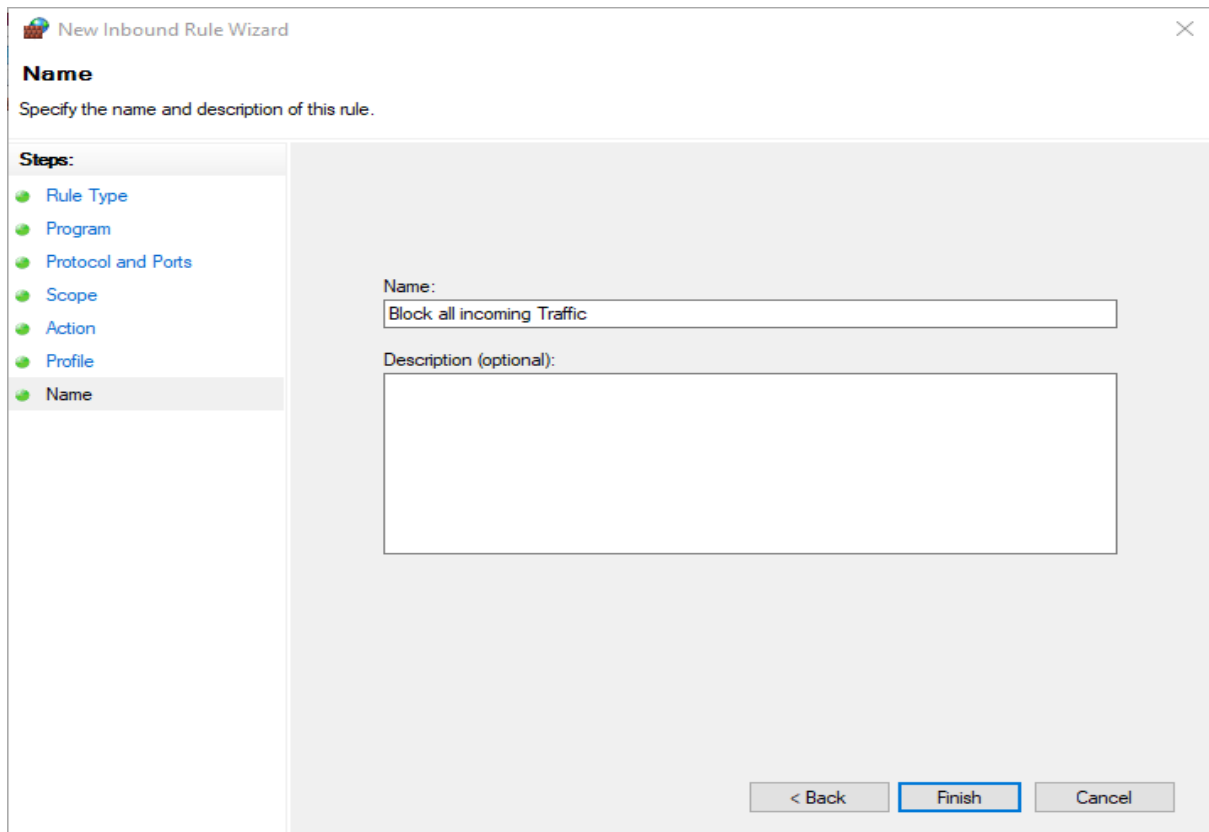
< Back Next > Cancel

7. Ensure Domain, Private, and Public are all checked.



The screenshot shows the 'New Inbound Rule Wizard' window at the 'Profile' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Profile', followed by the instruction 'Specify the profiles for which this rule applies.' On the left, a 'Steps:' list includes 'Rule Type', 'Program', 'Protocol and Ports', 'Scope', 'Action', 'Profile' (which is highlighted), and 'Name'. The main area is titled 'When does this rule apply?' and contains three checked options: '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.), and 'Public' (Applies when a computer is connected to a public network location.). At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

8. Name the rule (e.g., “Block All Incoming Traffic”) and click Finish.



The screenshot shows the 'New Inbound Rule Wizard' window at the 'Name' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Name', followed by the instruction 'Specify the name and description of this rule.' On the left, a 'Steps:' list includes 'Rule Type', 'Program', 'Protocol and Ports', 'Scope', 'Action', 'Profile', and 'Name' (which is highlighted). The main area has a 'Name:' label above a text box containing 'Block all incoming Traffic'. Below this is a 'Description (optional):' label above a larger text box. At the bottom right are buttons for '< Back', 'Finish', and 'Cancel'.

For Linux:

Run the following command to block all other incoming traffic:

```
sudo iptables -A INPUT -d 10.0.2.11 -j DROP
```

Replace `10.0.2.11` with your server's IP address.

Step 4: Save and Apply the Rules

For Windows:

No additional steps are required. Windows automatically saves and applies the rules once created.

For Linux:

Save the IPTables rules to ensure they persist after a reboot:

```
sudo iptables-save > /etc/iptables/rules.v4
```

The below are all Linux steps:



```
(rachael@ray)-[~]  
$ sudo su  
[sudo] password for rachael:  
(root@ray)-[/home/rachael]  
# sudo iptables -A INPUT -p tcp --dport 443 -d 10.0.2.11 -j ACCEPT  
  
(root@ray)-[/home/rachael]  
# sudo iptables -A INPUT -d 10.0.2.11 -j DROP  
  
(root@ray)-[/home/rachael]  
# sudo iptables-save > /etc/iptables/rules.v4
```

✓ You're Done!

Your firewall is now configured to allow only HTTPS traffic to your server, blocking all other incoming connections. This setup ensures that your server remains secure while enabling encrypted communication for legitimate users.

