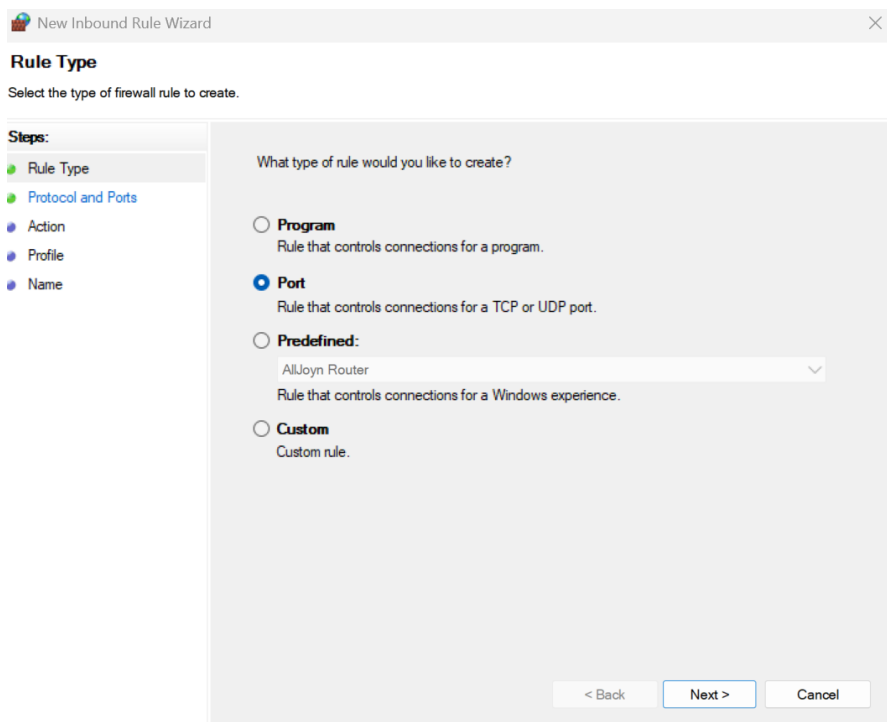
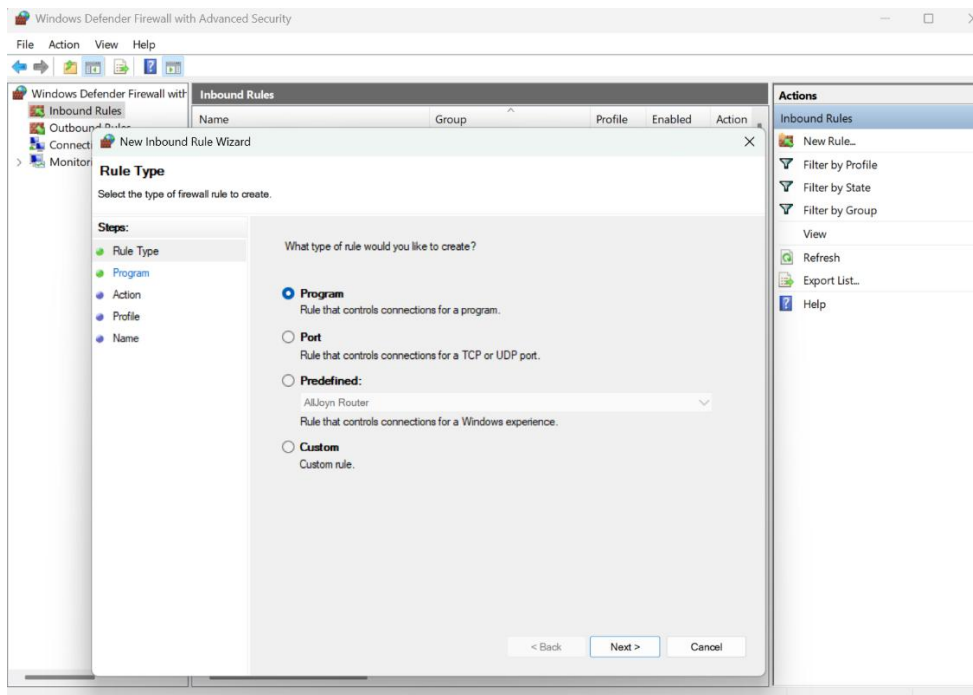


TASK 3

1. To list current firewall rules I've the following command:
`netsh advfirewall firewall show rule name=all`
2. Add a rule to block inbound traffic on a specific port.
 - I. Using the app:



New Inbound 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 local ports or specific local ports?

☐ All local ports

☒ Specific local ports:

23

Example: 80, 443, 5000-5010

< Back

Next >

Cancel

New Inbound 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.

Customize...

☒ Block the connection

< Back

Next >

Cancel

Rules

New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:

Rule Type

Protocol and Ports

Action

Profile

Name

Name:

Block Telnet

Description (optional):

< Back

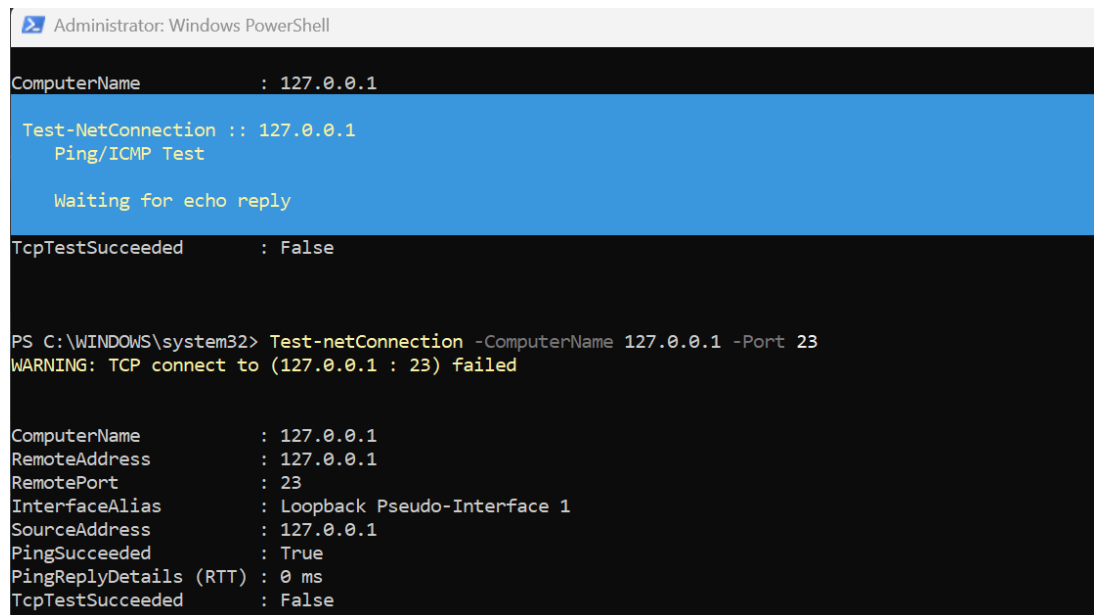
Finish

Cancel

II. Using the command prompt:

```
PS C:\WINDOWS\system32> netsh advfirewall firewall add rule name="Block Telnet" dir=in action=block protocol=TCP localport=23
Ok.
```

3. Testing the rule.



```
Administrator: Windows PowerShell

ComputerName      : 127.0.0.1

Test-NetConnection :: 127.0.0.1
  Ping/ICMP Test

  Waiting for echo reply

TcpTestSucceeded  : False

PS C:\WINDOWS\system32> Test-netConnection -ComputerName 127.0.0.1 -Port 23
WARNING: TCP connect to (127.0.0.1 : 23) failed

ComputerName      : 127.0.0.1
RemoteAddress     : 127.0.0.1
RemotePort        : 23
InterfaceAlias    : Loopback Pseudo-Interface 1
SourceAddress     : 127.0.0.1
PingSucceeded     : True
PingReplyDetails  (RTT) : 0 ms
TcpTestSucceeded  : False
```

- Chceking the rule's status:

```
PS C:\WINDOWS\system32> netsh advfirewall firewall show rule name="Block Telnet"
>>

Rule Name:                               Block Telnet
-----
Enabled:                                     Yes
Direction:                               In
Profiles:                               Domain,Private,Public
Grouping:
LocalIP:                                   Any
RemoteIP:                                 Any
Protocol:                                 TCP
LocalPort:                                23
RemotePort:                               Any
Edge traversal:                             No
Action:                                    Block
Ok.
```

4. Removing the rule.

```
PS C:\WINDOWS\system32> netsh advfirewall firewall delete rule name="Block Telnet"

Deleted 1 rule(s).
Ok.
```