

WINDOWS FIREWALL LAB

Windows Defender Firewall (Windows 10)

[Firewall and Network Protection Settings](#)

Microsoft Windows Firewall formerly known as Internet Connection Firewall

Windows Firewall Lab.

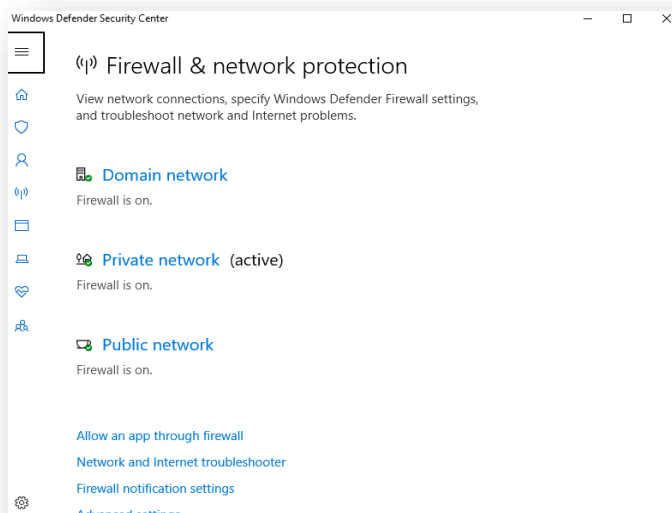
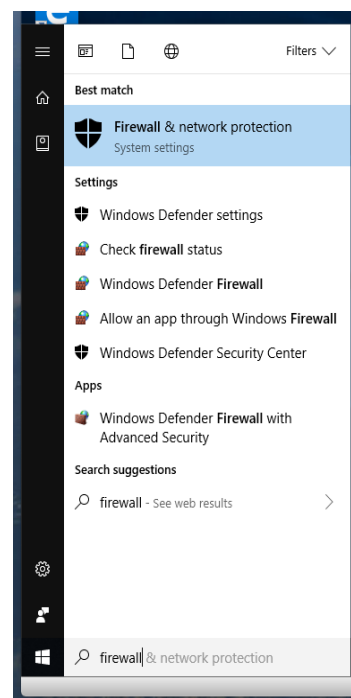
Lab information:

Windows Firewall (officially called Windows Defender Firewall in Windows 10), is a firewall component of Microsoft Windows. It was first included in Windows XP and Windows Server 2003. Prior to the release of Windows XP Service Pack 2 in 2004, it was known as Internet Connection Firewall. With the release of Windows 10 version 1709, in September 2017, it was renamed Windows Defender Firewall as part of the "Windows Defender" branding campaign.

In this lab, you will change a number of firewall settings to stop certain traffic from being used on a Windows 10 machine.

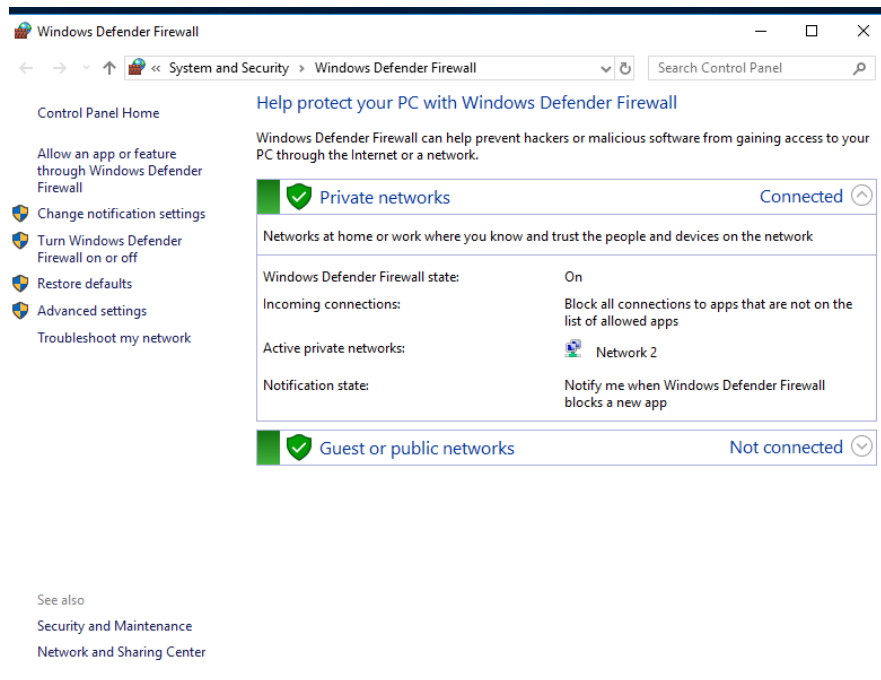
Step 1:

Search for firewall within the Windows search bar.

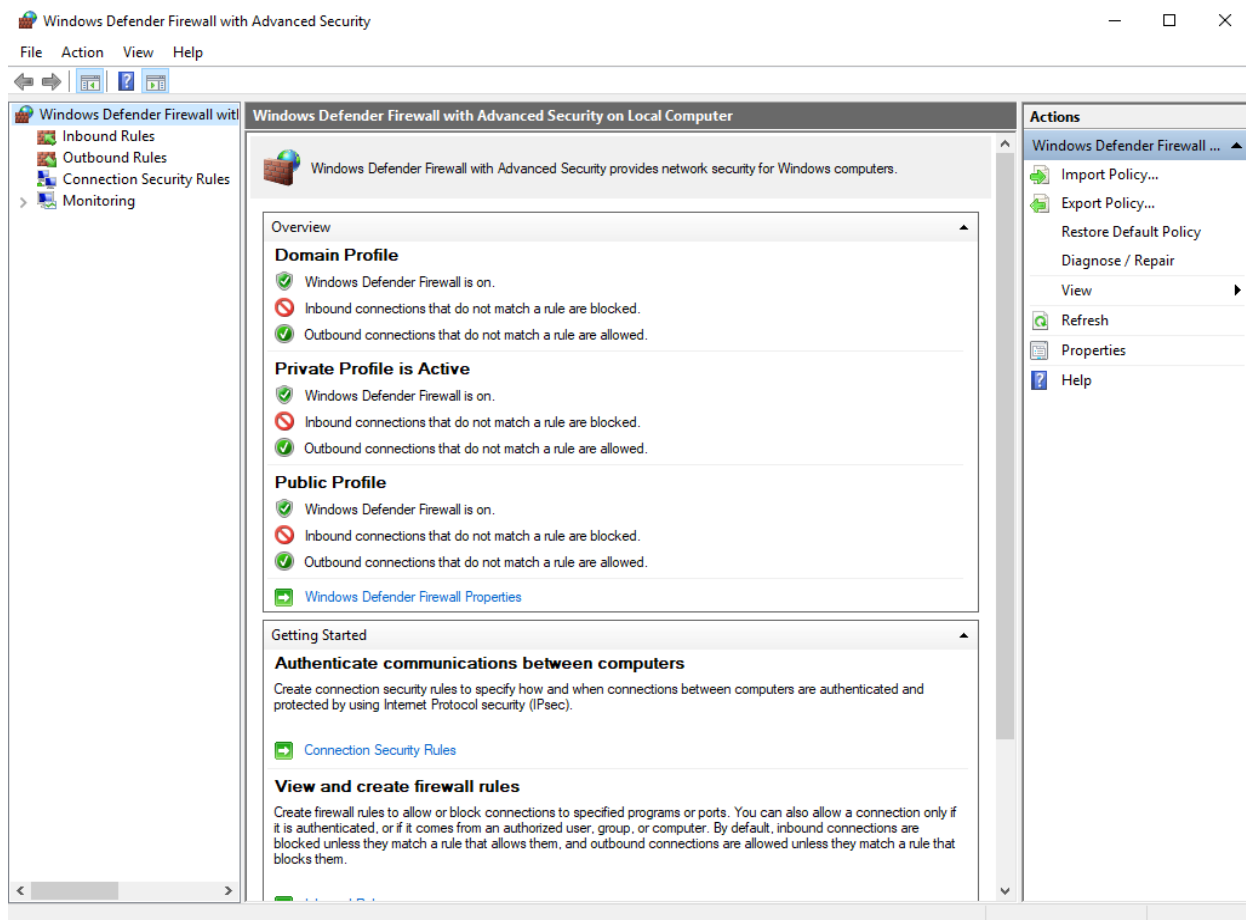


The firewall and network protection area shows us the firewall status with a basic view.

We are required to open the Windows Defender Firewall. This is a more advanced version of the above option.

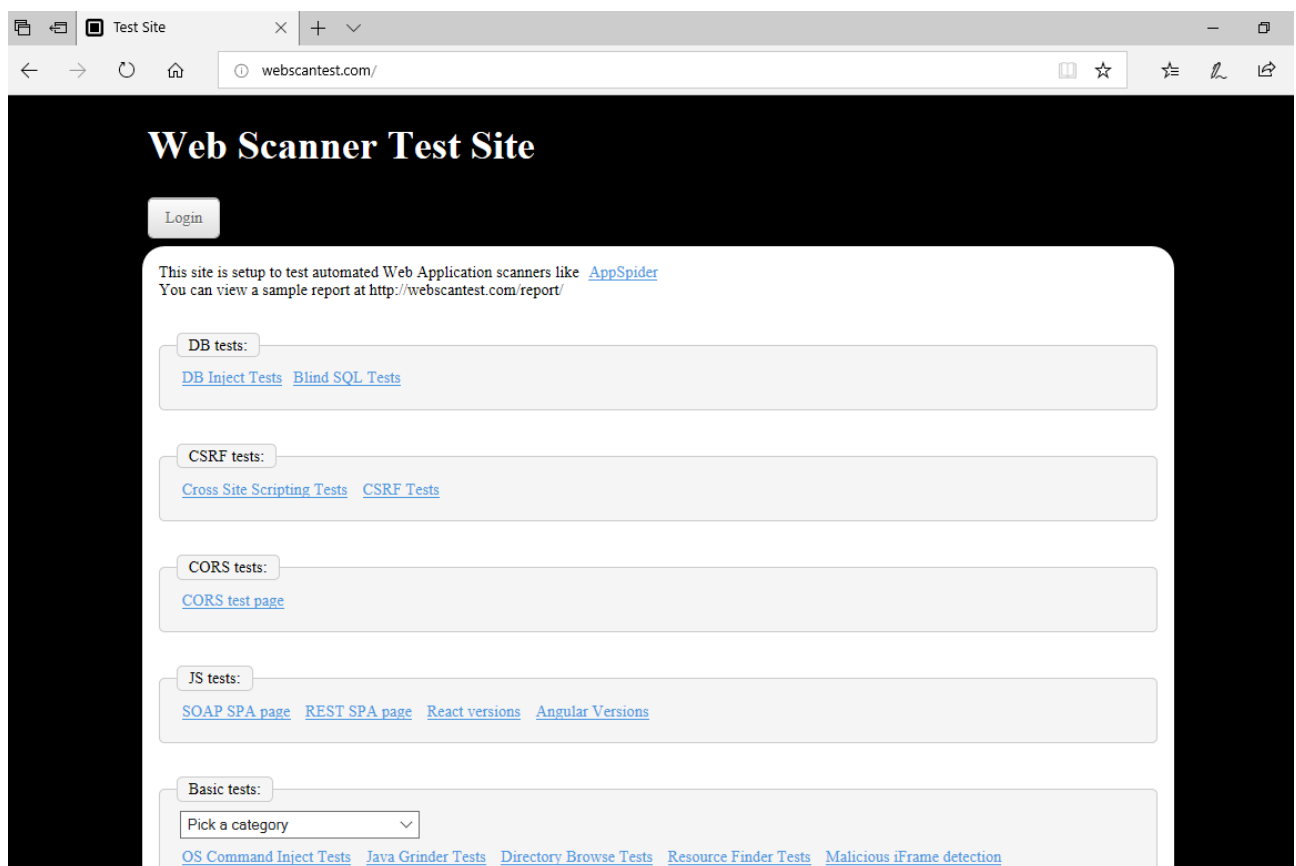
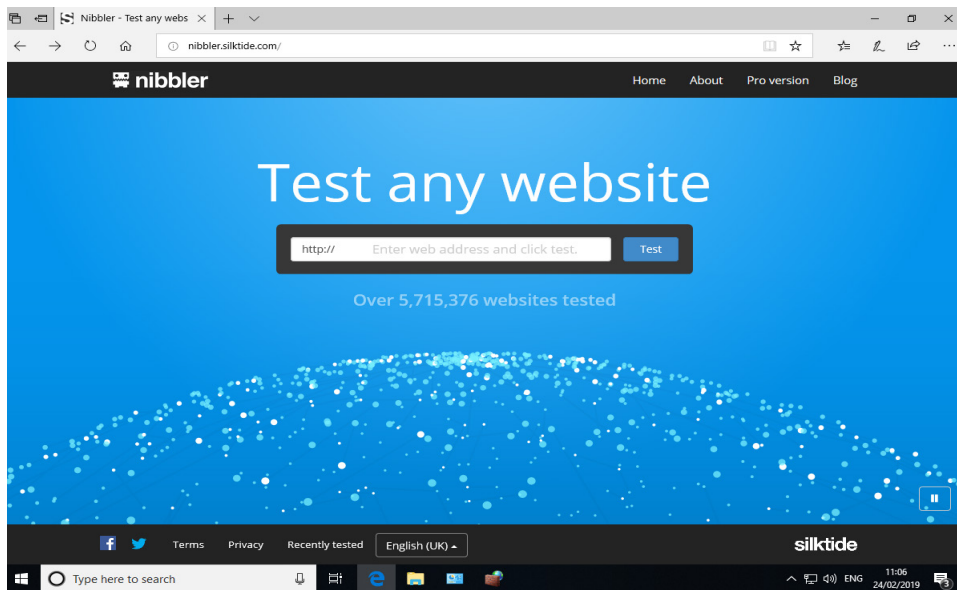


Let's open the advanced settings from the left-hand sidebar.



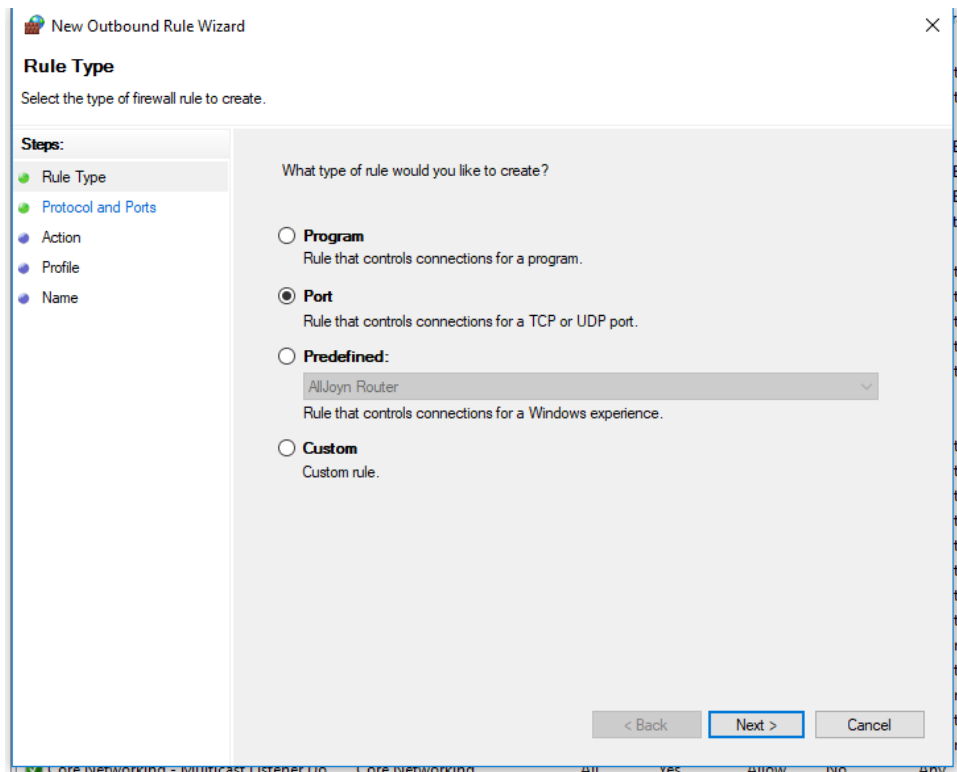
Step 2:

Now, we will create an outbound FW rule that blocks HTTP traffic on the PC. Firstly, let's browse to a few HTTP websites to prove that HTTP is currently working.



Now, let's open the Windows FW and create a new outbound rule...

We will choose the port option.



The screenshot shows the 'New Outbound Rule Wizard' window at the 'Rule Type' step. The left sidebar lists the steps: Rule Type (selected), Protocol and Ports, Action, Profile, and Name. The main area asks 'What type of rule would you like to create?' with four options: Program, Port (selected), Predefined (with a dropdown menu showing 'AllJoyn Router'), and Custom. The 'Next >' button is highlighted.

New Outbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

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

What type of rule would you like to create?

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

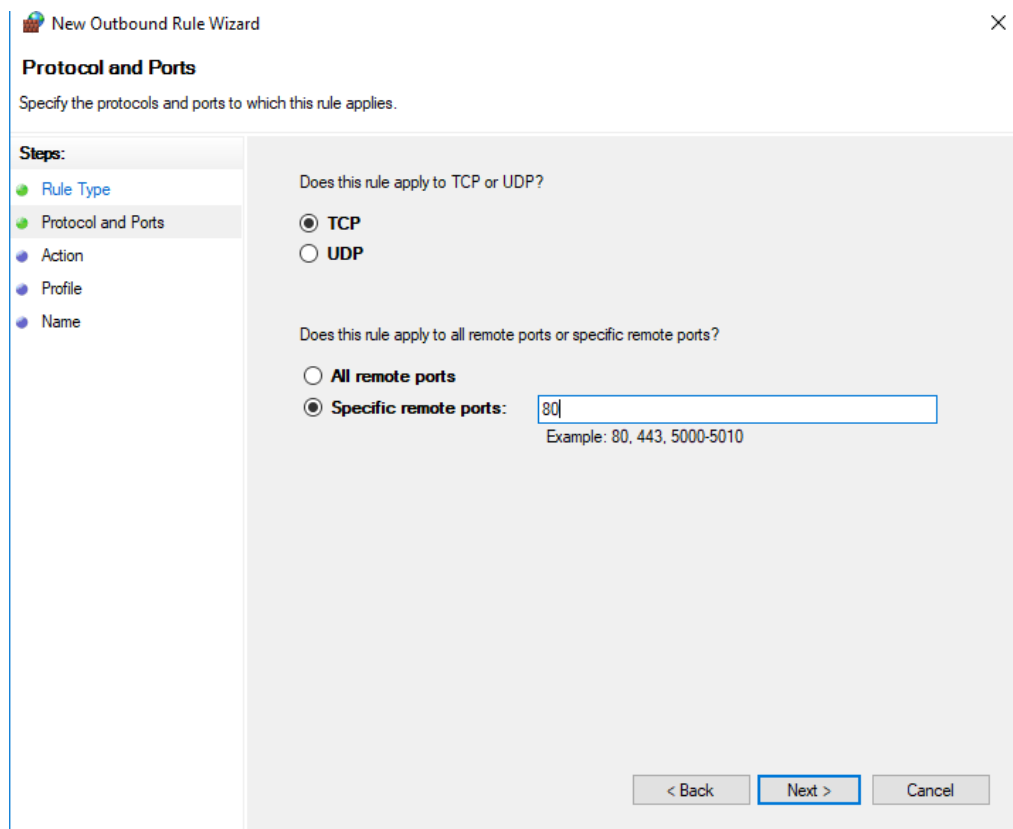
☒ **Port**
Rule that controls connections for a TCP or UDP port.

☐ **Predefined:**
AllJoyn Router
Rule that controls connections for a Windows experience.

☐ **Custom**
Custom rule.

< Back Next > Cancel

When asked at the next stage, we will type port 80.



The screenshot shows the 'New Outbound Rule Wizard' window at the 'Protocol and Ports' step. The left sidebar lists the steps: Rule Type, Protocol and Ports (selected), Action, Profile, and Name. The main area asks 'Does this rule apply to TCP or UDP?' with TCP selected. It then asks 'Does this rule apply to all remote ports or specific remote ports?' with 'Specific remote ports' selected and a text box containing '80'. The 'Next >' button is highlighted.

New Outbound 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**

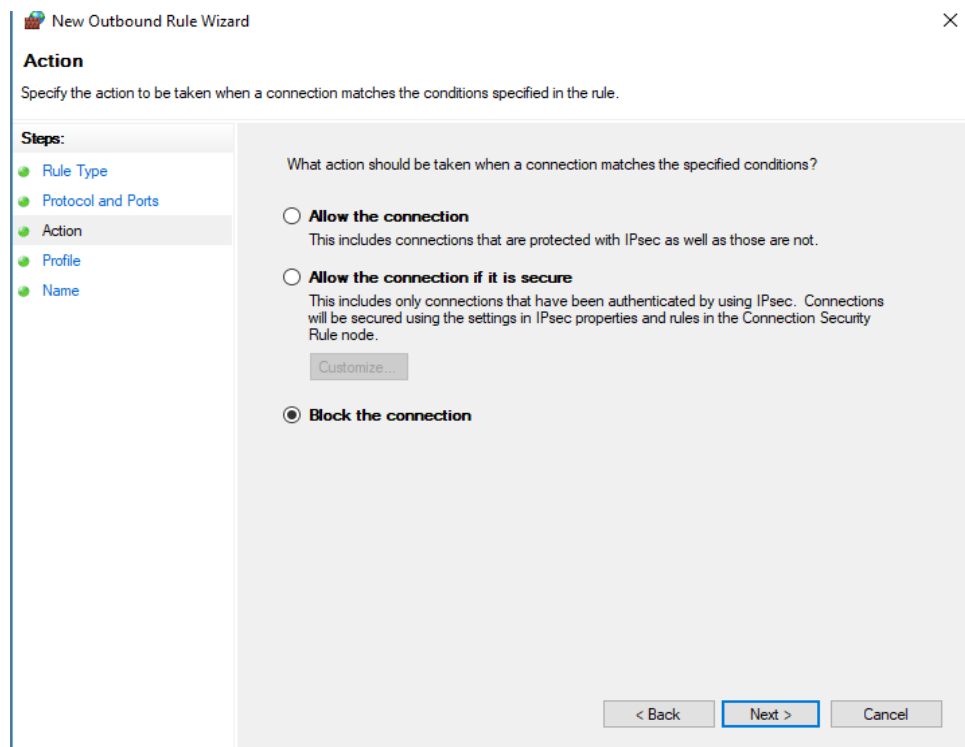
Does this rule apply to all remote ports or specific remote ports?

☐ **All remote ports**

☒ **Specific remote ports:** 80
Example: 80, 443, 5000-5010

< Back Next > Cancel

We will block the connection.



The screenshot shows the 'Action' step of the 'New Outbound Rule Wizard'. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action (selected), Profile, and Name. The main area asks 'What action should be taken when a connection matches the specified conditions?'. There are three radio button options: 'Allow the connection' (unselected), 'Allow the connection if it is secure' (unselected), and 'Block the connection' (selected). Below the 'Allow the connection if it is secure' option is a 'Customize...' button. At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

New Outbound 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?

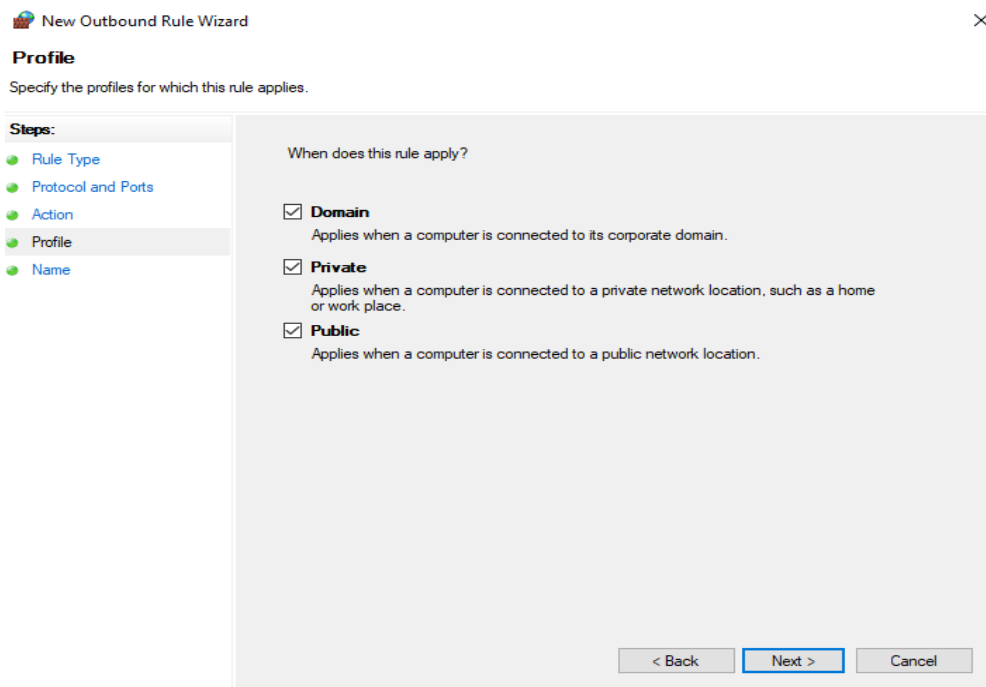
☐ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

☐ **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

Leave all three applied as per the default option.



The screenshot shows the 'Profile' step of the 'New Outbound Rule Wizard'. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action, Profile (selected), and Name. The main area asks 'When does this rule apply?'. There are three checked checkbox options: 'Domain', 'Private', and 'Public'. Each option has a description of when the rule applies. At the bottom right are '< Back', 'Next >', and 'Cancel' buttons.

New Outbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

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

When does this rule apply?

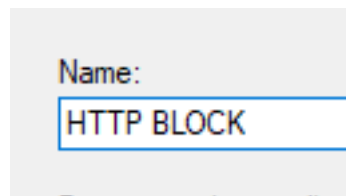
☒ **Domain**
Applies when a computer is connected to its corporate domain.

☒ **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

Give it a name.

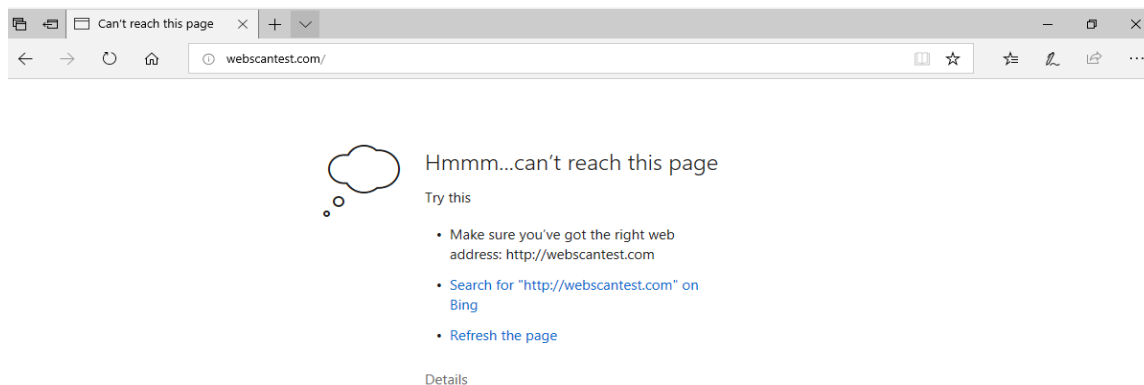


The FW rule will now be applied.

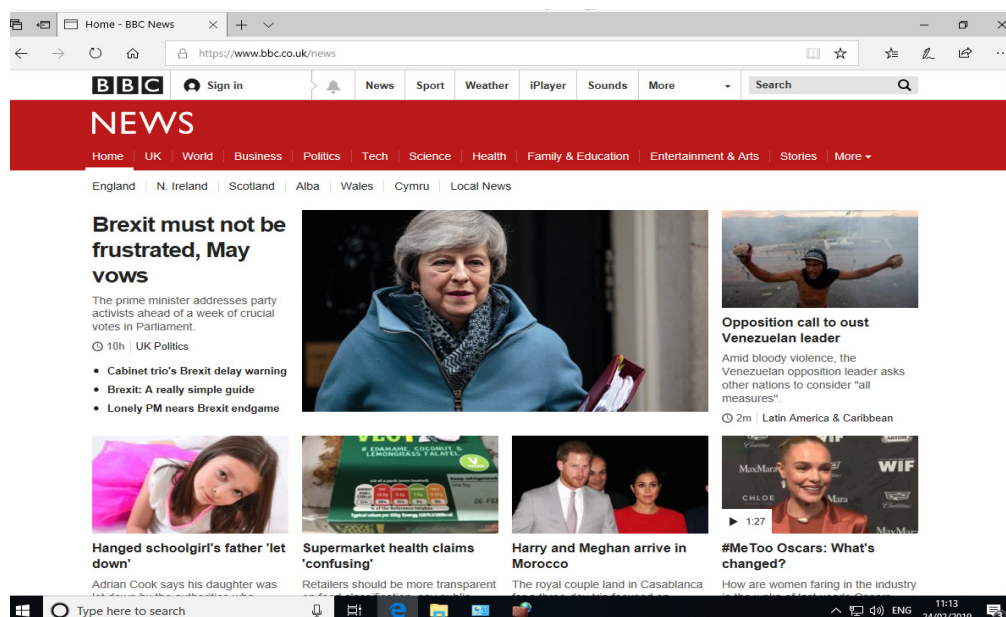
Next, browse to the same websites as before and you will see that our rule actually blocks this from happening as they are using port 80 which is for HTTP traffic.

Please browse to HTTPs websites. These will still work as they aren't using port 80, they are using port 443.

The below screenshot shows that the same website as before does not work.



However, the below HTTPS website test does work, as expected.



Much more can be done with the Windows FW. The rule that we have applied here is applied only to this PC. Companies will most likely use a Windows Server and issue group policies, whereby the administrator can set company-wide firewall settings from one panel, rather than having to go to every PC and change the FW manually.