There's your problem. You need a little more than just the web browser to have a working Internet connection. Specifically, all of the Core Networking rules are important, especially DNS. (It's rather difficult to visit web sites if you can't resolve their IPs.)

You can restore the standard rules - both outbound and inbound - by right-clicking the root node in the firewall management window and choosing Restore Default Policy. That will roll back the firewall state to what it was when Windows was first installed. You'll lose all custom entries, so some programs might need to have their rules re-added. (Alternatively, you could attempt to restore them by creating "predefined" rules.) After you do that, you can try disabling some outbound rules until stuff breaks, at which point you've discovered which ones are critical. Be aware that the network icon in the notification area isn't necessarily right about whether you can access the Internet; its checks may differ from what you're interested in.

My experimentation indicates that only the Core Networking ones are super important. You'll need to allow your browser too, of course. Note: Some browsers (Microsoft Edge, for instance) have one executable that is the UI and one that makes the actual requests; you need to unblock the latter.

I recommend also allowing the Windows Update service; you can create a service rule by creating a "custom rule", leaving the Program screen setting at All programs, and choosing a service with the Customize button at the bottom.

If you want pinging to work, you'll need to create a rule that allows certain types of ICMP traffic, which will also be a "custom rule." Let it apply to all programs, but on the Protocols and Ports screen, click the Customize button after choosing ICMPv4 as the protocol. Select the specific types that you're interested in; I recommend Echo Request (ping) and Destination Unreachable.

Windows’ built-in firewall hides the ability to create powerful firewall rules. Block programs from accessing the Internet, use a whitelist to control network access, restrict traffic to specific ports and IP addresses, and more – all without installing another firewall.

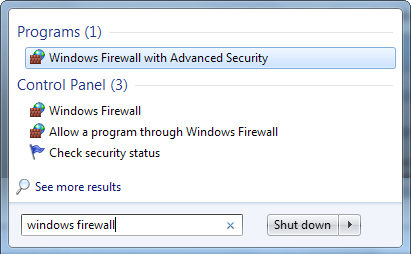
The firewall includes three different profiles, so you can apply different rules to private and public networks. These options are included in the Windows Firewall with Advanced Security snap-in, which first appeared in Windows Vista.

**Accessing the Interface**

There are a variety of ways to pull up the Windows Firewall with Advanced Security window. One of the most obvious is from the Windows Firewall control panel – click the Advanced settings link in the sidebar.



You can also type “Windows Firewall” into the search box in the Start menu and select the Windows Firewall with Advanced Security application.



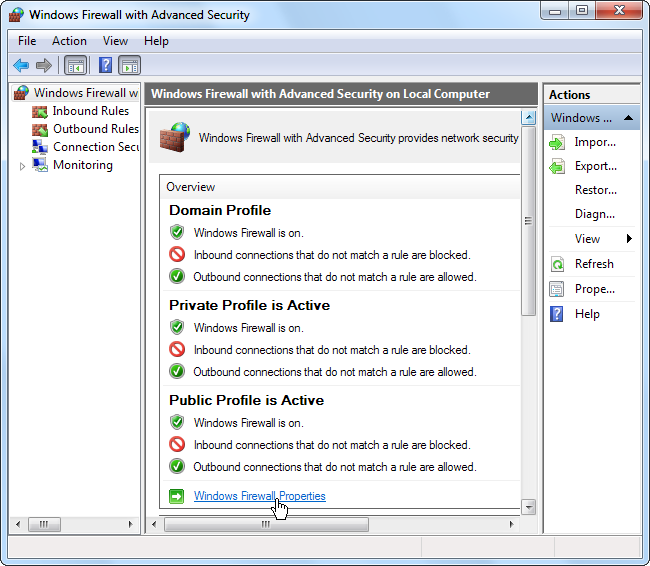
**Configuring Network Profiles**

The Windows firewall uses three different profiles:

* **Domain Profile**: Used when your computer is connected to a domain.
* **Private**: Used when connected to a private network, such as a work or home network.
* **Public**: Used when connected to a public network, such as a public Wi-Fi access point or a direct connection to the Internet.

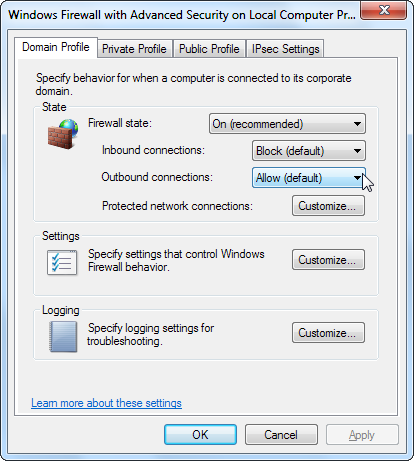
Windows asks whether a network is public or private when you first connect to it.

A computer may use multiple profiles, depending on the situation. For example, a business laptop may use the domain profile when connected to a domain at work, the private profile when connected to a home network, and the public profile when connected to a public Wi-Fi network – all in the same day.



Click the Windows Firewall Properties link to configure the firewall profiles.

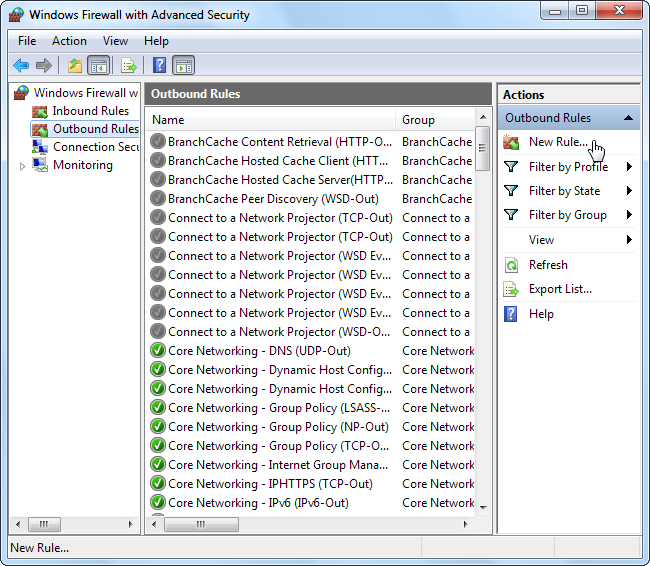
The firewall properties window contains a separate tab for each profile. Windows blocks inbound connections and allows outbound connections for all profiles by default, but you can block all outbound connections and create rules that allow specific types of connections. This setting is profile-specific, so you can use a whitelist only on specific networks.



If you block outbound connections, you won’t receive a notification when a program is blocked – the network connection will fail silently.

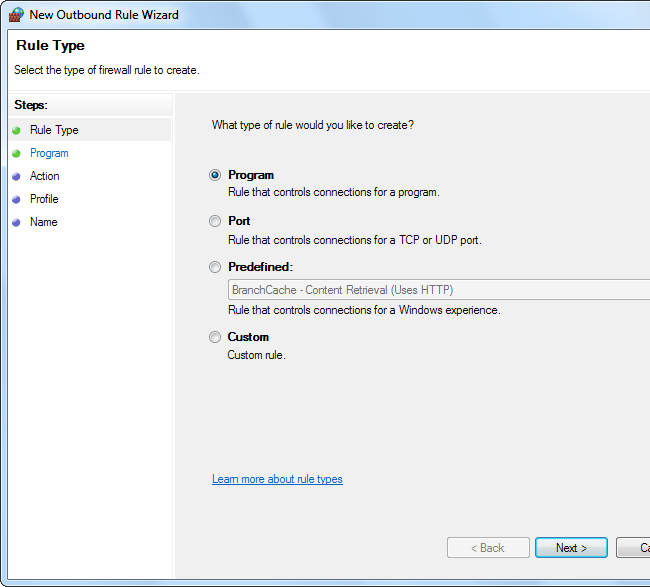
**Creating a Rule**

To create a rule, select the Inbound Rules or Outbound Rules category at the left side of the window and click the Create Rule link at the right side.



The Windows firewall offers four types of rules:

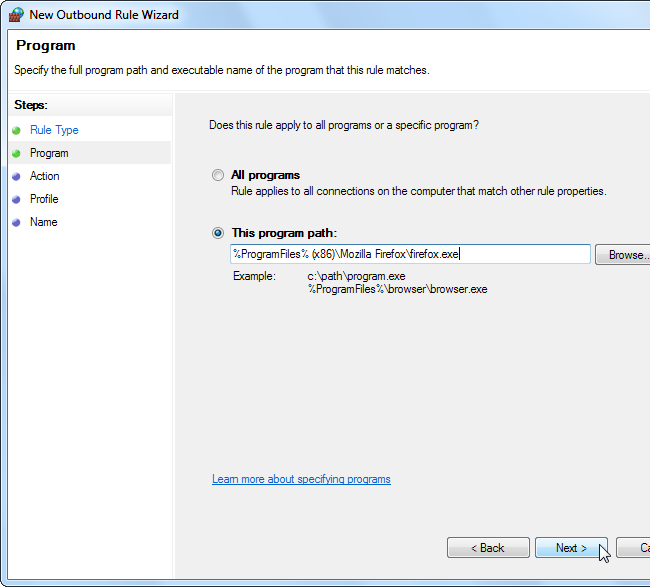
* **Program** – Block or allow a program.
* **Port** – Block or a allow a port, port range, or protocol.
* **Predefined** – Use a predefined firewall rule included with Windows.
* **Custom** – Specify a combination of program, port, and IP address to block or allow.



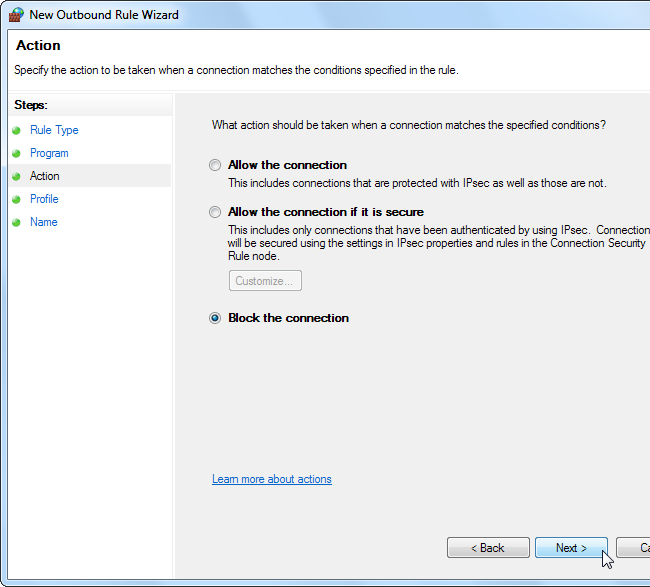
**Example Rule: Blocking a Program**

Let’s say we want to block a specific program from communicating with the Internet — we don’t have to install a third-party firewall to do that.

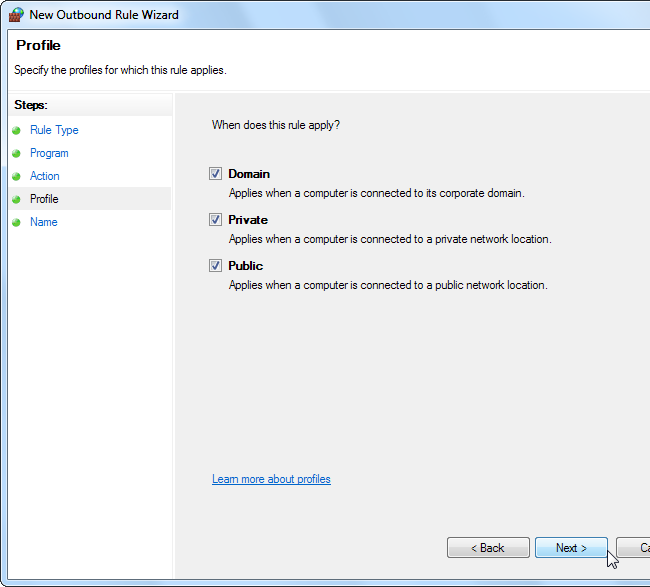
First, select the Program rule type. On the next screen, use the Browse button and select the program’s .exe file.



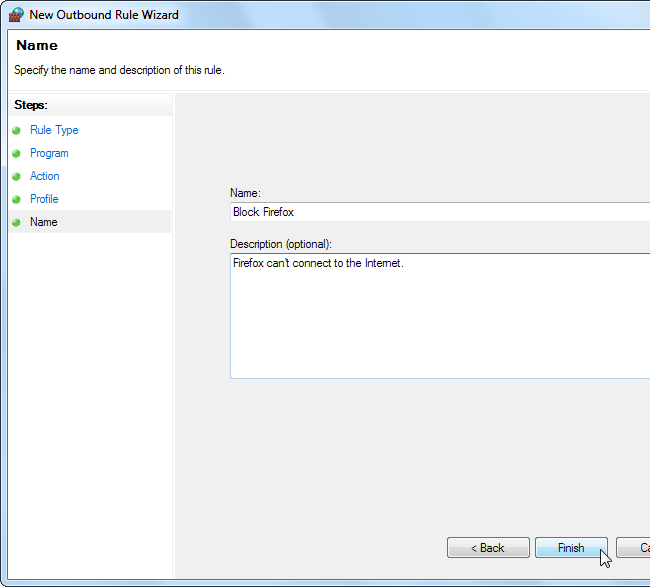
On the Action screen, select “Block the connection.” If you were setting up a whitelist after blocking all applications by default, you’d select “Allow the connection” to whitelist the application instead.



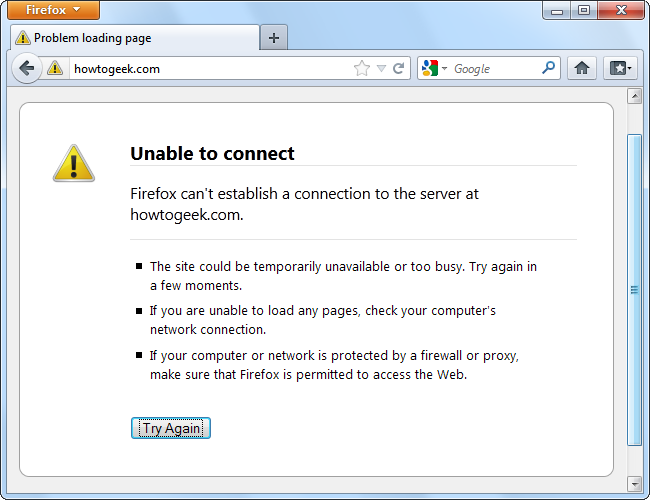
On the Profile screen, you can apply the rule to a specific profile – for example, if you only want a program blocked when you’re connected to public Wi-Fi and other insecure networks, leave the “Public” box checked. By default, Windows applies the rule to all profiles.



On the Name screen, you can name the rule and enter an optional description. This will help you identify the rule later.



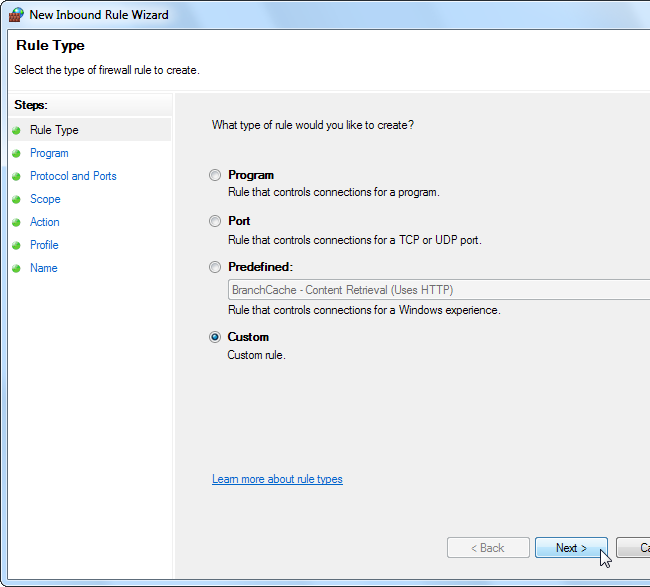
Firewall rules you create take effect immediately. Rules you create will appear in the list, so you can easily disable or delete them.



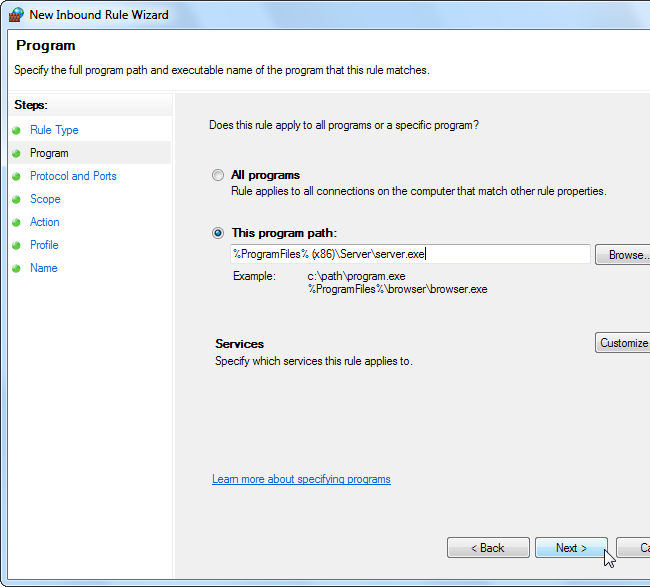
**Example Rule: Restricting Access**

If you really want to lock down a program, you can restrict the ports and IP addresses it connects to. For example, let’s say you have a server application that you only want accessed from a specific IP address.

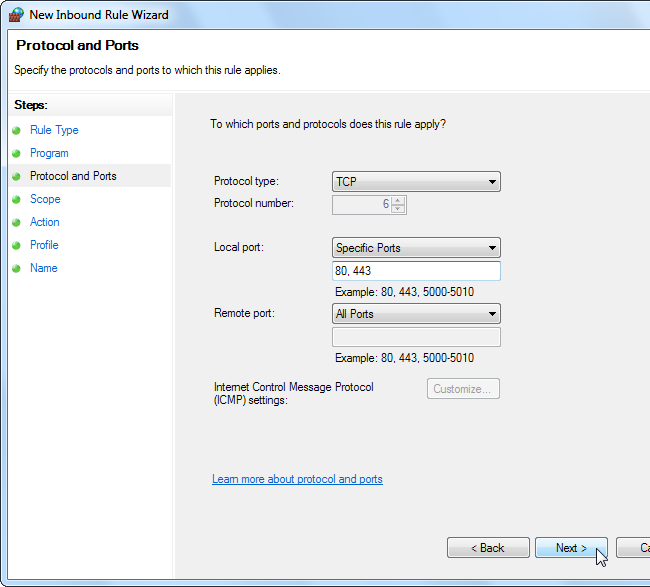
From the Inbound Rule list, click New Rule and select the Custom rule type.



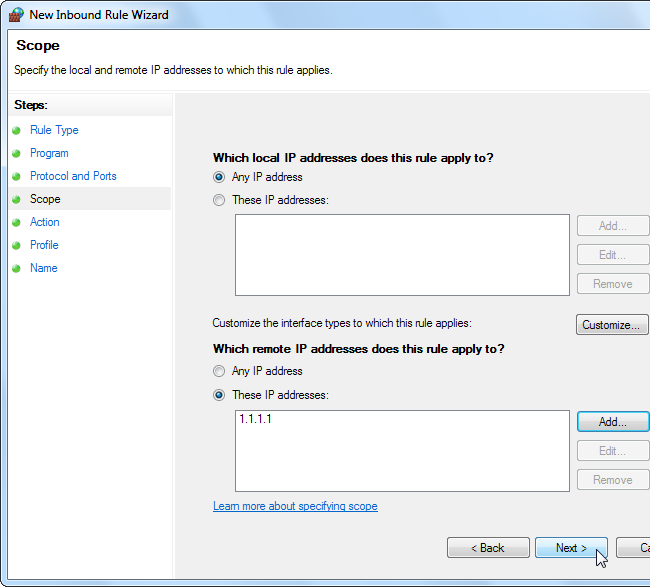
On the Program pane, select the program you want to restrict. If the program is running as a Windows service, use the Customize button to select the service from a list. To restrict all network traffic on the computer to communicating with a specific IP address or port range, select “All programs” instead of specifying a specific program.



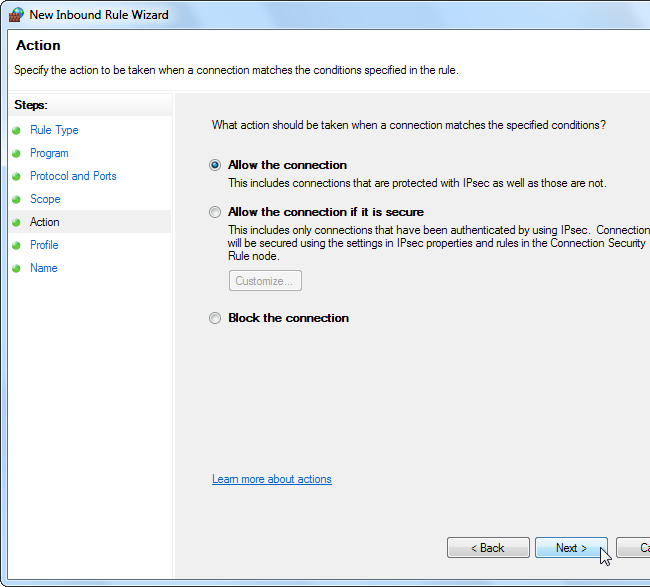
On the Protocol and Ports pane, select a protocol type and specify ports. For example, if you’re running a web server application, you can restrict the web server application to TCP connections on ports 80 and 443 by entering these ports in the Local port box.



The Scope tab allows you to restrict IP addresses. For example, if you only want the server communicating with a specific IP address, enter that IP address in the remote IP addresses box.



Select the “Allow the connection” option to allow the connection from the IP address and ports you specified. Be sure to check that no other firewall rules apply to the program – for example, if you have a firewall rule that allows all inbound traffic to the server application, this rule won’t do anything.



The rule takes effect after you specify the profiles it will apply to and name it.

The Windows firewall isn’t as easy-to-use as third-party firewalls, but it offers a surprising amount of power. If you want more control and ease of use, you may be better off with a third-party firewall.