

Firewall Frequently Asked Questions

What is a firewall?

An Internet firewall is a piece of software or hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. If you are a home user or small-business user, having a properly configured firewall is the most effective and important first step you can take to help protect your computer. It is important to always remember, have your firewall and antivirus software turned on before you connect to the Internet.

Why do I need a firewall?

If your computer is not protected when you connect to the Internet, hackers can gain access to personal information (credit card, social security number, personal documents, etc.) on your computer. They can install code on your computer that destroys files or causes malfunctions. They can also use your computer to cause problems on other home and business computers connected to the Internet. A firewall helps to screen out many kinds of malicious Internet traffic before it reaches your system. Some firewalls can also help to prevent others from using your computer to attack other computers without your knowledge. Using a firewall is important no matter how you connect to the Internet — dial-up modem, cable modem, or digital subscriber line (DSL or ADSL) or your business network.

If you have a version of Windows other than Windows XP, such as Windows 2000, Windows Millennium Edition, or Windows 98, you should obtain a hardware or software firewall and install it. If you already have a network, you can check the manuals of your networking devices, such as wireless access points or broadband routers, to determine if they include built-in hardware firewalls.

How does the Windows Firewall work?

The Windows Firewall monitors all network traffic on the connections for which it is enabled. For example, the firewall can monitor all traffic on your dial-up connection to the Internet. The firewall keeps track of all communications that have originated from your computer, and it prevents unsolicited traffic from reaching your computer. If necessary, the firewall dynamically opens ports and allows your computer to receive traffic that you have specifically requested, such as a Web page for which you have clicked the address.

A "port" is a networking term that identifies the point at which a type of network traffic reaches your computer. The exact ports that you open depend on the type of traffic you want to send and receive.

If you have not requested the incoming traffic, Internet Connection Firewall helps block it before it can reach your computer. For special uses, such as networking, hosting online games, or hosting your own Web server, you can select ports that you want to leave open. This allows others to make connections to your computer, but it can also reduce security. Internet Connection Firewall is part of Windows XP Home Edition and Windows XP Professional.

What else do I need besides a firewall?

A firewall will not make your computer 100 percent safe. However, a firewall provides an effective line of defense. You should install a firewall and antivirus software first and then check every two weeks for critical software updates from Windows Update.

What can a firewall protect me against?

A firewall helps to protect your computer by hiding it from external users and preventing unauthorized connections to your computer. The firewall can also protect against a variety of computer worms that can be transmitted over the network. A computer worm is similar to a virus, but is self-contained and can spread without the help of other programs.

What doesn't a firewall protect me against?

A Firewall cannot protect against viruses that spread through e-mail, such as Trojan horses, which masquerade as helpful or benign software and trick you into opening or downloading them. The firewall cannot prevent spam or pop-up ads. A firewall will not prevent access to an otherwise unsecured wireless network. However, the firewall helps to protect the computers on your network, so if an intruder were to gain access to your network, he or she could not access your personal computer.

Will the Internet Connection Firewall protect my wireless network?

The Internet Connection Firewall will help protect a computer on a wireless network, but will not restrict access to the network itself. You should configure your wireless network to use a network key using either Wi-Fi Protected Access (WPA) or wired equivalent privacy (WEP). For more information, consult the manual for your wireless networking devices.

Should I enable the Windows Firewall on all computers on my home network?

Yes. If you have multiple network connections on any of your computers, you should turn on the firewall for each connection. In some cases the Internet Connection Firewall can interfere with file and print sharing and prevent your computer from finding other network devices. To allow these types of uses, you can manually open network ports. When network ports are left open, the protection provided by Internet Connection Firewall for your computer is reduced.

Can I use both a software firewall from another company and the built-in firewall in my Windows XP computer?

No. Running multiple software firewalls is unnecessary for typical home computers, home networking, and small-business networking scenarios. Using two firewalls on the same connection could cause issues with connectivity to the Internet or other unexpected behavior. One firewall, whether it is the Windows XP Internet Connection Firewall or a different software firewall, can provide substantial protection for your computer.

I use a laptop in home and business networks that are protected by firewalls. What should I do when I'm traveling?

You should always enable the Internet Connection Firewall when connecting to the Internet using a dial-up modem or any broadband connection when you are traveling.

I use a Virtual Private Networking connection to access a large network from home or while traveling. Should I turn on the firewall in Windows XP?

You should ask the network administrator for the large network to which you are connecting. You should follow the administrator's guidance on whether to turn on Internet Connection Firewall for the VPN connection.

My computer is part of a large business, school, or organizational network should I enable the firewall?

You should follow the policy established by the network administrator for your business, school, or organizational network. In some cases, network administrators may configure all computers on the network so that you cannot turn on the firewall while your computer is connected to the network. The check box to turn on the firewall in the Windows Security Center or in the Network Connection Properties dialog box will be dimmed. In any case, you should ask your network administrator for guidance on whether you need a firewall on your computer.