NCCIC

Security Tip (ST04-004)

Understanding Firewalls for Home and Small Office Use

Original release date: June 17, 2009 | Last revised: September 10, 2018

When your computer is accessible through an internet connection or Wi-Fi network, it is susceptible to attack. However, you can restrict outside access to your computer—and the information on it—with a firewall.

> Using a firewall in conjunction with other protective measures can help strengthen your resistance to attacks.

What do firewalls do?

Firewalls provide protection against outside attackers by shielding your computer or network from malicious or unnecessary network traffic. Firewalls can also prevent malicious software from accessing a computer or network via the internet. Firewalls can be configured to block data from certain locations (i.e., computer network addresses), applications, or ports while allowing relevant and necessary data through. (See Understanding Denial-of-Service Attacks and Understanding Hidden Threats: Rootkits and Botnets for more information.)

What type of firewall is best?

Categories of firewalls include hardware and software. While both have advantages and disadvantages, the decision to use a firewall is more important than deciding which type you use.

- **Hardware** – Typically called network firewalls, these physical devices are positioned between your computer and the internet (or other network connection). Many vendors and some internet service providers (ISPs) offer integrated small office / home office routers that also include firewall features. Hardware-based firewalls are particularly useful for protecting multiple computers and controlling the network activity that attempts to pass through them. The advantage of hardware-based firewalls is that they provide an additional line of defense against attacks reaching desktop computing systems. The disadvantage is that they are separate devices that require trained professionals to support their configuration and maintenance.
- **Software** – Most OSs include a built-in firewall feature that you should enable for added protection, even if you have an external firewall. Firewall software is also available separately from your local computer store, software vendor, or ISP. If you download firewall software from the internet, make sure it is from a reputable source (i.e., an established software vendor or service provider) and offered via a secure site. (See Understanding Web Site Certificates for more information.) The advantage of software firewalls is their ability to control the specific network behavior of individual applications on a system. A significant disadvantage of a software firewall is that it is typically located on the same system that is being protected. Being located on the same system can hinder the firewall's ability to detect and stop malicious activity. Another possible disadvantage of software firewalls is that—if you have a firewall for each computer on a network—you will need to update and manage each computer's firewall individually.

How do you know what configuration settings to apply?

Most commercially available firewall products, both hardware and software based, come preconfigured and ready to use. Since each firewall is different, you will need to read and understand the documentation that comes with it to determine whether the default firewall settings are sufficient for your needs. This is particularly concerning because the “default” configuration is typically less restrictive, which could make your firewall more susceptible to compromise. Alerts about current malicious activity (e.g., NCCIC’s Alerts) sometimes include information about restrictions you can implement through your firewall.

Though properly configured firewalls may effectively block some attacks, do not be lulled into a false sense of security. Firewalls do not guarantee that your computer will not be attacked. Firewalls primarily help protect against malicious traffic, not against malicious programs (i.e., malware), and may not protect you if you accidentally install or run malware on your computer. However, using a firewall in conjunction with other protective measures (e.g., anti-virus software and safe computing practices) will strengthen your resistance to attacks. (See Good Security Habits and Understanding Anti-Virus Software for more information.)

Author

NCCIC
