



Enterprise Security Office Monthly Security Tips NEWSLETTER

AUGUST 2008

Volume 3, Issue 8

Firewalls

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall information security posture.

What is a firewall and why should I use one?

A firewall is a software program or hardware device that filters the inbound and outbound traffic between your network or computer and the Internet. Firewalls add a layer of protection by blocking unauthorized and potentially dangerous data from entering your computer or network. Firewalls are especially critical for users who have an "always on" connection to the Internet.

All state computing systems are protected by firewalls and are managed by your information technology section. You should consider, however, utilizing a firewall for your home computer as well. Some users may think that data residing on their computer is not valuable and therefore a firewall is not necessary. Even small pieces of information, however, can be obtained by a hacker and used to steal identities and other personal data. In addition, hackers may be interested in taking over your computer to store illegal materials or launch other attacks that can leave a trail back to your computer. Once a hacker gets access to your computer, the intruder may have access to resources and data stored on your machine.

What does a firewall protect me from?

Firewalls can help protect your data and computer by blocking:

- unsolicited traffic/malware from coming into your computer or network
- traffic from known malicious computers
- specific traffic you don't want leaving your computer or network
- programs, protocols and ports that you specify
- attempts to access or attack your computer

Firewalls can also log activity, and these logs should be reviewed periodically to identify any anomalous or unexpected activity.

What type of firewall should I use?

There are two types of firewalls: hardware and software. A hardware firewall is usually an external device that sits between your computer and your connection to the Internet. Routers with built-in firewalls are often used this way. A software firewall (also known as a personal firewall) runs directly on your computer. This firewall is the most common type for home users and may come pre-installed on newer computers.

The selection of a firewall is dependent on what is being protected. The value of the assets, the complexity of the computers or networks, and their usage of the Internet will dictate the type and size of firewall that should be used.

Make sure you have a firewall – selected based on your business or personal needs -- and that it is enabled.

Before enabling a firewall, read the documentation carefully to ensure proper configuration. A properly configured firewall can save you hours of recovery or rebuilding of data.

Below are some areas for consideration when installing a firewall.

- Purchase a wireless (or wired) router with a built-in firewall. Most routers on the market today have this extra feature. Change the "admin" password on the device, make sure the firewall feature is turned on, then leave the

default settings alone. Simply having this device between your computer and your “always on” Internet connection provides a layer of protection. This is the best and easiest option for most home users.

- Many anti-virus packages and later versions of Windows have a basic software firewall built in. As with hardware firewalls, simply make sure the firewall feature is turned on and leave it at default settings. If you do not already have a software firewall as part of your Windows operating system or built in to your anti-virus software, consider such third party software firewalls as ZoneAlarm, Comodo or PCTools Firewall. When installing, accept the recommended options and keep the default settings.
- Enable the “automatic update” feature if one exists and also periodically check the firewall vendor’s Web site for the latest software updates.
- If you use the Windows operating system, you can easily check to see if your firewall is working. From the Windows desktop, open the Control Panel and look for the Security (Center or Status) tab to check the setting. Do not install more than one firewall product as they may conflict and impact the performance of your system.

A firewall is a very valuable tool to protect your data and your computers, but it must be selected, installed, configured, monitored, and maintained effectively to do its job. Remember that a firewall is just one layer of multi-layer protection. While firewalls can block intruders, viruses or unwanted traffic from getting into your computer, using a firewall is not a complete solution to security. Firewalls should be used along with anti-virus, anti-spyware, and anti-spam software as part of a defense-in-depth strategy for protecting your computer from various forms of malware (viruses, worms, Trojans, etc.), hackers, and others who want your data or your computer for illegal or malicious purposes. Keep your system updated with the latest patches and keep your anti-virus software up to date.

Remember: Cyber security is your responsibility. Always apply safe cyber security practices to protect the data on your computer or network.

References

To learn more about firewalls, please visit the following sites:

MS-ISAC - Beginners Guide to Firewalls

<http://www.cscic.state.ny.us/localgov/#download>

US-CERT

<http://www.us-cert.gov/cas/tips/ST04-004.html>

How Stuff Works - Firewalls

<http://computer.howstuffworks.com/firewall.htm>

Firewalls for Dummies

<http://www.dummies.com/WileyCDA/DummiesTitle/Firewalls-For-Dummies-2nd-Edition.productCd-0764540483.html>

Brought to you by:



www.msisac.org

