by Jen Sharp

Using a firewall: closing the front door to the computer

It is certain that a concept has become mainstream in society's consciousness when a movie is named after it. In the 2006 film titled "FIREWALL," Harrison Ford plays a bank executive whose family is held hostage until he can break through the computer system and pay off some bad guys:

Jack Stanfield: "I just hacked into your accounts."

Bill Cox: "That's impossible."

Jack Stanfield: "You just lost $20 million."

A firewall is considered the first line of defense against electronic attacks on our sensitive, private information. For most of us, the lives of our families or $20 million may not be at stake, but the difficulty of recovering from a breach is daunting. The best preventative solution is to make the firewall a piece of a comprehensive approach to securing your system.

Jen Sharp
JenSharp.com

What is it?

The traditional definition of a physical firewall is provided by *www.dictionary.com*. It is "a partition made of fireproof material to prevent the spread of a fire from one part of a building or ship to another or to isolate an engine compartment, as on a plane, automobile, etc."

Much in the same way, the electronic version of a firewall prevents damage to a computer system. Wikipedia.com describes it as "an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system. It is also a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteria."

History of the firewall

In 1988, a curious university student wrote a simple program intended to measure the use and size of the Internet. However, due to a mistake in his programming, Robert Morris instead wrote the first virus, and his widely propagated code bogged down what was estimated to be more than 10 percent of machines using the Internet at that time. The entire online community was taken aback, unprepared for anything like this large scale attack on its resources. Despite being convicted on computer abuse charges, Morris now works for MIT.

This 'Morris Worm' was one of a few incidents that year that provided the impetus for the creation of firewalls. Today, worms and viruses and attacks on systems are usually designed to intend intrusion and harm. Fortunately, although some large companies might suffer targeted attacks, for most users firewalls do a satisfactory job when used correctly.

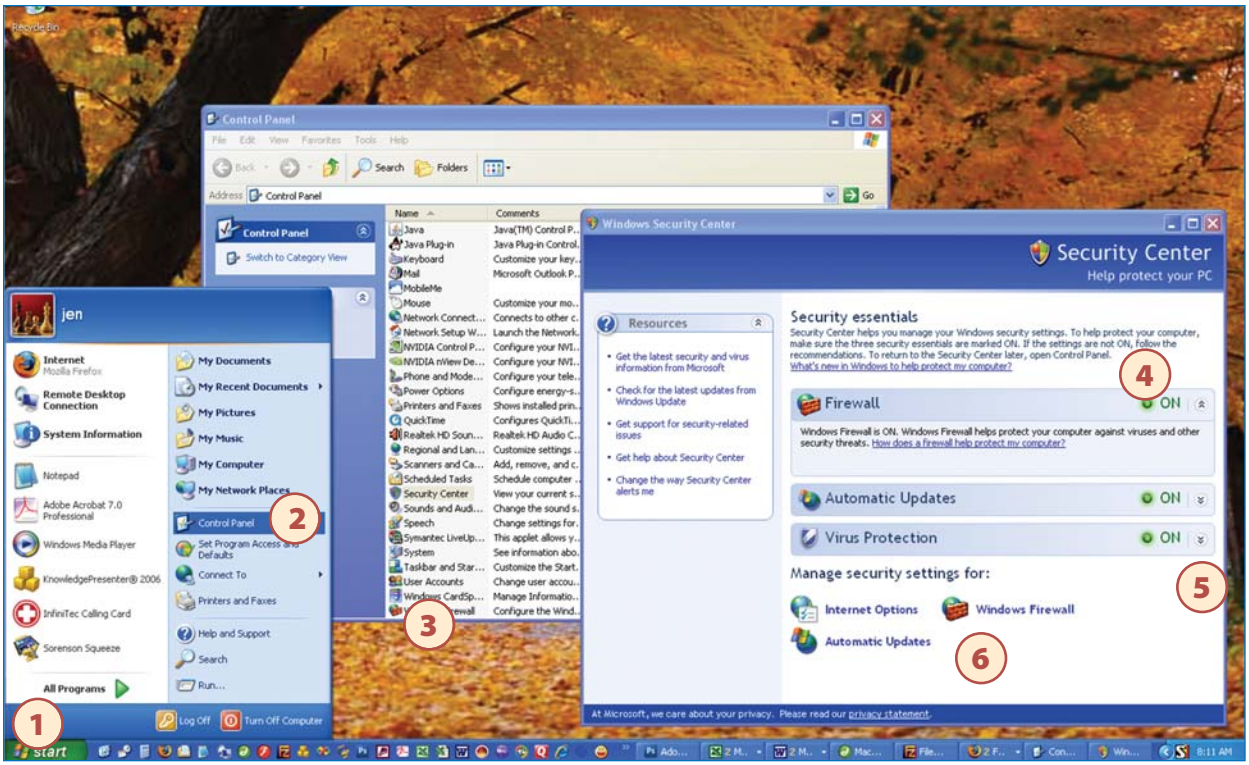
Choosing a firewall and its settings

So, how does a firewall handle these risks? The job of a firewall is to apply rules for allowing data in or out of a given system. If the rules are not clear or effective, then breaches can occur. There are two approaches to assigning rules for firewalls:

1. Allow everything in, and just block obvious attacks – *blacklisting*.
2. Allow nothing in, and then make exceptions based on trusted access – *whitelisting*.

The *whitelist* approach is a much more effective way to control unwanted access to your computer. This allows for configuration based on your usage. For example, if all you do with your computer is send e-mail, then all other ports and exceptions should be disallowed, and you could apply the strictest settings. For other uses, such as file sharing or remote login, allow specific exceptions only per application or particular user. For more complicated usage, hiring an IT tech to set up a good working system would pay for itself in peace of mind.

Firewalls come in two types: hardware and software. Hardware takes the form of routers, wireless routers, or an Ethernet hub to connect to your Internet Service Provider (ISP). A physical firewall



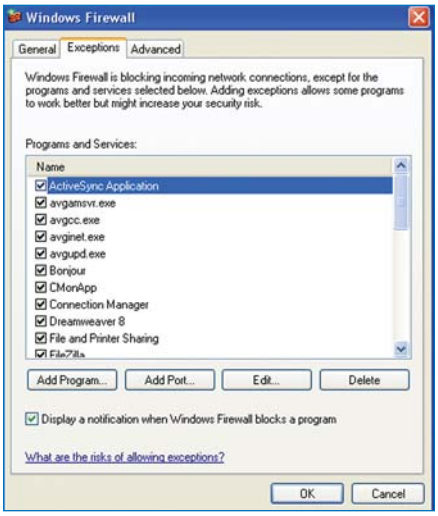
The screen shot above shows how to check or activate a computer's Windows XP Firewall component. ① Click start, then ② click on the Control Panel button. ③ In the Control Panel list, choose and click Security Center. At the Security Center box ④ make sure the three buttons are clicked 'on.' By toggling the switch at the right of each on button, ⑤ a drop box explains what each function performs for the computer. By clicking on the Windows Firewall button, ⑥ the 'Exceptions' box with three tabs allows selections for connection exceptions. See the three images of Windows XP Firewall Settings on the next page.

is one of the most effective, simple, inexpensive ways to implement this security. The only necessary item for a user to check is to make sure the ISP uses a proxy server, a common security practice which hides your true IP address.

Firewall software is more customizable, though possibly more complicated to choose from and use. Windows operating systems have their own firewalls automatically installed. Most experts have called Windows XP Service Pack 2 firewall ineffective, as it only monitors incoming data. *Forbes* writer Stephen Manes explains, "If malware somehow gets into your machine, Windows Firewall will not stop it from making outbound Internet connections to do its evil deeds." Windows Vista upgraded to monitor both outgoing and

Windows XP Firewall Settings

The 'General Tab' above allows three settings for Windows Firewall. One for activation, the second for exceptions and a third for deactivation of Windows Firewall.



The second or 'Exceptions' tab lets programs and services to be selected in the list allowing some programs to work better even though doing so might increase a security risk.

The third 'Advanced' tab allows exceptions for individual connections and to affect individual settings for these.

incoming requests, however, its firewall has been called 'inadequate at best.' Mac users don't fair much better. Microsoft answered these claims by offering a product called Windows Live OneCare that costs approximately $50 per year. However, there are several third-party products available free of charge that do a great job of protecting. (see links in sidebar on the next page)

Most experts agree that a router or other hardware with firewall used in tandem with firewall software installed on each machine offers the best protection.

Other ways to protect a system

Whether the computer problem is loss of data or unwanted access, the most common problem I see comes internally. Statistics show that most divulging of sensitive information comes from an inside source, such as a disgruntled employee, or an employee with good intentions but misinformed. Employees might be unaware of installing that CD they received in the mail, or how copying a CD or revealing information over the telephone harms the integrity of a system's security. A firewall cannot protect against this common breach.

While most firewalls have minimal virus protection capabilities, they can only work on viruses coming in directly from the Internet. Installing a heavy duty virus protection software on every machine individually that runs scans regularly and updates automatically is a must towards building an effective overall security structure.

Spam is virtually unaffected by firewall protection. If you plan to have e-mail, you will have spam. Implementing a spam filter is a must to not only make your workload lighter, but to protect from accidental installation of unwanted code.

Having a comprehensive plan

Firewalls are a necessary and effective tool to protect access and data. However, they need to be only one part of a security plan. It makes no sense to build a thick steel door to a shabby wooden house with broken windows!

Links

For more info:

- HowStuffWorks explains "How Firewalls Work" http://computer.howstuffworks.com/firewall.htm
- Firewall Knowledge Network www.cubma.com/index.php
- PCStats.com
- AnswersThatWork.com

To test a system:

- Shields Up www.grc.com/x/ne.dll?bh0bkyd2
- Security Space.com
- HackerWhacker.com

Free & subscription software:

- AVG (www.avg.com)
- Comodo Firewall Pro 3.0 www.personalfirewall.comodo.com/
- Agnitum Outpost www.agnitum.com/
- IPNetSentry www.sustworks.com/site/prod_ipns_overview.html
- Jetico www.jetico.com/
- Lavasoft Personal Firewall www.lavasoft.com/products/lavasoft_personal_firewall.php
- Norton www.symantec.com/
- Sunbelt Personal Firewall www.sunbelt-software.com/Home-Home-office/Sunbelt-Personal-Firewall/
- ZoneAlarm www.zonelabs.com/

2009 Conference technology topics

The 2009 KRWA Conference & Exhibition will feature numerous topics regarding computer and software technology. Mark calendars now for March 24 - 26, Century II Convention Center, Wichita, Kansas.

Risks

Although most people have a general idea of what a firewall does, they may not understand its capabilities and limitations. Here is a list condensed from HowStuffWorks.com that gives an overview of the ways hackers try to access others' computers:

Remote login - When someone is able to connect to your computer and control it in some form. This can range from being able to view or access your files to actually running programs on your computer.

Application backdoors - Some programs have special features that allow for remote access. Others contain bugs that provide a backdoor, or hidden access, that provides some level of control of the program.

SMTP session hijacking - SMTP is the most common method of sending e-mail over the Internet. By gaining access to a list of e-mail addresses, a person can send unsolicited junk e-mail (spam) to thousands of users. This is done quite often by redirecting the e-mail through the SMTP server of an unsuspecting host, making the actual sender of the spam difficult to trace.

Operating system bugs - Like applications, some operating systems have backdoors. Others provide remote access with insufficient security controls or have bugs that an experienced hacker can take advantage of.

Denial of service - The hacker sends a request to the server to connect to it. When the server responds with an acknowledgement and tries to establish a session, it cannot find the system that made the request. By inundating a server with these unanswerable session requests, a hacker causes the server to slow to a crawl or eventually crash.

E-mail bombs - An e-mail bomb is usually a personal attack. Someone sends you the same e-mail hundreds or thousands of times until your e-mail system cannot accept any more messages.

Macros - To simplify complicated procedures, many applications allow you to create a script of commands that the application can run. This script is known as a macro. Hackers have taken advantage of this to create their own macros that, depending on the application, can destroy your data or crash your computer.

Viruses – This small program can copy itself to other computers. This way it can spread quickly from one system to the next. Viruses range from harmless messages to erasing all of your data.

Spam - Typically harmless but always annoying, spam is the electronic equivalent of junk mail. Spam can be dangerous though. Quite often it contains links to Web sites. Be careful of clicking on these because you may accidentally accept a cookie that provides a backdoor to your computer.

Redirect bombs - Hackers can use ICMP to change (redirect) the path information takes by sending it to a different router. This is one of the ways that a denial of service attack is set up.

Source routing - In most cases, the path a packet travels over the Internet (or any other network) is determined by the routers along that path. But the source providing the packet can arbitrarily specify the route that the packet should travel. Hackers sometimes take advantage of this to make information appear to come from a trusted source or even from inside the network! Most firewall products disable source routing by default.