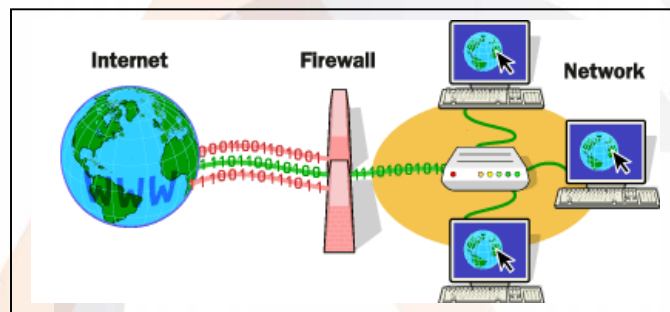


Firewall, Proxy, DMZ

If you have been using the Internet for any length of time, and especially if you work at a larger company and browse the Web while you are at work, you have probably heard the term **firewall** used. For example, you often hear people in companies say things like, "I can't use that site because they won't let it through the firewall."

If you have a fast Internet connection into your home or SME (either a DSL or a Cable Modem), you may have found yourself hearing about firewalls for your home network as well. It turns out that a small home / SME network has many of the same security issues that a large corporate network does. You can use a firewall to protect your home / SME network from offensive Web sites and potential hackers.



Basically, a firewall is a barrier to keep destructive forces away from your property. In fact, that's why its called a firewall. Its job is similar to a physical firewall that keeps a fire from spreading from one area to the next. As you read through this article, you will learn more about firewalls, how they work and what kinds of threats they can protect you from.

What Firewall Does

A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network. If an incoming packet of information is flagged by the filters, it is not allowed through.

Let's say that you work at a company with 500 employees. The company will therefore have hundreds of computers that all have network cards connecting them together. In addition, the company will have one or more connections to the Internet through something like T1 or T3 lines. Without a firewall in place, all of those hundreds of computers are directly accessible to anyone on the Internet. A person who knows what he or she is doing can probe those computers, try to make FTP connections to them, try to make telnet connections to them and so on. If one employee makes a mistake and leaves a security hole, hackers can get to the machine and exploit the hole.

With a firewall in place, the landscape is much different. A company will place a firewall at every connection to the Internet (for example, at every T1 line coming into the company). The firewall can implement security rules. For example, one of the security rules inside the company might be:

Out of the 500 computers inside this company, only one of them is permitted to receive public FTP traffic. Allow FTP connections only to that one computer and prevent them on all others.

A company can set up rules like this for FTP servers, Web servers, Telnet servers and so on. In addition, the company can control how employees connect to Web sites, whether files are allowed to leave the company over the network and so on. A firewall gives a company tremendous control over how people use the network.

Firewalls use one or more of three methods to control traffic flowing in and out of the network:

- **Packet filtering** - Packets (small chunks of data) are analyzed against a set of **filters**. Packets that make it through the filters are sent to the requesting system and all others are discarded.
- **Proxy service** - Information from the Internet is retrieved by the firewall and then sent to the requesting system and vice versa.
- **Stateful inspection** - A newer method that doesn't examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information. Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics. If the comparison yields a reasonable match, the information is allowed through. Otherwise it is discarded.

Customizing Firewall

Firewalls are customizable. This means that you can add or remove filters based on several conditions. Some of these are:

- **IP Addresses** - Each machine on the Internet is assigned a unique address called an **IP address**. IP addresses are 32-bit numbers, normally expressed as four "octets" in a "dotted decimal number." A typical IP address looks like this:
216.27.61.137. For example, if a certain IP address outside the company is reading too many files from a server, the firewall can block all traffic to or from that IP address.
- **Domain Names** - Because it is hard to remember the string of numbers that make up an IP address, and because IP addresses sometimes need to change, all servers on the Internet also have human-readable names, called **domain names**. For example, it is easier for most of us to remember www.howstuffworks.com than it is to remember 216.27.61.137. A company might block all access to certain domain names, or allow access only to specific domain names.
- **Protocols** - The **protocol** is the pre-defined way that someone who wants to use a service talks with that service. The "someone" could be a person, but more often it is a computer program like a Web browser. Protocols are often text, and simply describe how the client and server will have their conversation. The **http** in the Web's protocol. Some common protocols that you can set firewall filters for include:
 - **IP** (Internet Protocol) - the main delivery system for information over the Internet
 - **TCP** (Transport Control Protocol) - used to break apart and rebuild information that travels over the Internet
 - **HTTP** (Hyper Text Transfer Protocol) - used for Web pages
 - **FTP** (File Transfer Protocol) - used to download and upload files
 - **UDP** (User Datagram Protocol) - used for information that requires no response, such as streaming audio and video
 - **ICMP** (Internet Control Message Protocol) - used by a router to exchange the information with other routers
 - **SMTP** (Simple Mail Transport Protocol) - used to send text-based information (e-mail)
 - **SNMP** (Simple Network Management Protocol) - used to collect system information from a remote computer
 - **Telnet** - used to perform commands on a remote computer

A company might set up only one or two machines to handle a specific protocol and ban that protocol on all other machines.

- **Ports** - Any server machine makes its services available to the Internet using numbered **ports**, one for each service that is available on the server. For example, if a server machine is running a Web (HTTP) server and an FTP server, the Web server would typically be available on port 80, and the FTP server would be available on port 21. A company might block port 21 access on all machines but one inside the company.
- **Specific words and phrases** - This can be anything. The firewall will **sniff** (search through) each packet of information for an exact match of the text listed in the filter. For example, you could instruct the firewall to block any packet with the word "X-rated" in it. The key here is that it has to be an exact match. The "X- rated" filter would not catch "X rated" (no hyphen). But you can include as many words, phrases and variations of them as you need.

What Does Firewall Protect

There are many creative ways that unscrupulous people use to access or abuse unprotected 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** - You have probably heard this phrase used in news reports on the attacks on major Web sites. This type of attack is nearly impossible to counter. What happens is that 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** - Probably the most well-known threat is computer viruses. A virus is a small program that 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.

Some of the items in the list above are hard, if not impossible, to filter using a firewall. While some firewalls offer virus protection, it is worth the investment to install anti-virus software on each computer. And, even though it is annoying, some spam is going to get through your firewall as long as you accept e-mail.

The level of security you establish will determine how many of these threats can be stopped by your firewall. The highest level of security would be to simply block everything. Obviously that defeats the purpose of having an Internet connection. But a common rule of thumb is to block everything, then begin to select what types of traffic you will allow. You can also restrict traffic that travels through the firewall so that only certain types of information, such as e-mail, can get through. This is a good rule for businesses that have an experienced network administrator that understands what the needs are and knows exactly what traffic to allow through. For most of us, it is probably better to work with the defaults provided by the firewall developer unless there is a specific reason to change it. One of the best things about a firewall from a security standpoint is that it stops anyone on the outside from logging onto a computer in your private network. While this is a big deal for businesses, most home networks will probably not be threatened in this manner. Still, putting a firewall in place provides some peace of mind.

Proxy Server, DMZ

A function that is often combined with a firewall is a **proxy server**. The proxy server is used to access web pages by the other computers. When another computer requests a Web page, it is retrieved by the proxy server and then sent to the requesting computer. The net effect of this action is that the remote computer hosting the Web page never comes into direct contact with anything on your home network, other than the proxy server. Proxy servers can also make your Internet access work more efficiently. If you access a page on a Web site, it is **cached** (stored) on the proxy server. This means that the next time you go back to that page, it normally doesn't have to load again from the Web site. Instead it loads instantaneously from the proxy server.

There are times that you may want remote users to have access to items on your network. Some examples are:

- Web site
- Online business
- FTP download and upload area

In cases like this, you may want to create a **DMZ** (Demilitarized Zone). Although this sounds pretty serious, it really is just an area that is outside the firewall. Think of DMZ as the front yard of your house. It belongs to you and you may put some things there, but you would put anything valuable inside the house where it can be properly secured. Setting up a DMZ is very easy. If you have multiple computers, you can choose to simply place one of the computers between the Internet connection and the firewall. Most of the software firewalls available will allow you to designate a directory on the gateway computer as a DMZ.

