Firewall

Himadri Barman

A firewall is a set of related programs or hardware device, located at a network gateway server that protects the resources of a private network from users from other networks (The term also implies the security policy that is used with the programs). Computer security borrows this term from firefighting, where it originated. In firefighting, a firewall is a barrier established to prevent the spread of fire. Firewall technology emerged in the late 1980s when the Internet was a fairly new technology in terms of its global use and connectivity. The predecessors to firewalls for network security were the routers used in the late 1980s.

Basically, a firewall, working closely with a router program, examines each network packet to determine whether to forward it toward its destination or not. A firewall filters the information coming through the Internet connection into your private network or computer system. If an incoming packet of information is flagged by the filters, it is not allowed through. A firewall also includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources.

There are a number of firewall screening methods. A simple one is to screen requests to make sure they come from acceptable (previously identified) domain name and Internet Protocol addresses. For mobile users, firewalls allow remote access in to the private network by the use of secure logon procedures and authentication certificates.

An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to. We can see how a firewall helps protect computers inside a large company. 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. 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. 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.

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, TCP, HTTP, FTP, UDP, ICMP, SMTP, Telnet, etc. 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 (see How Web Servers Work for details). 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.

Some operating systems come with a firewall built in. Otherwise, a software firewall can be installed on the computer in your home that has an Internet connection. This computer is considered a gateway because it provides the only point of access between your home network and the Internet.

With a hardware firewall, the firewall unit itself is normally the gateway. A good example is the Linksys Cable/DSL router. It has a built-in Ethernet card and hub. Computers in your home network connect to the router, which in turn is connected to either a cable or DSL modem. You configure the router via a Web-based interface that you reach through the browser on your computer. You can then set any filters or additional information.

Why Firewall Security? 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** - 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.

References:

- http://en.wikipedia.org/wiki/Firewall_(computing) , accessed on 11.04.2012 @ 1145 Hrs
- http://searchsecurity.techtarget.com/definition/firewall, accessed on 11.04.2012 @ 1150 Hrs
- http://computer.howstuffworks.com/firewall.htm, accessed on 11.04.2012 @ 1155 Hrs