Firewalls

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 (either a DSL connection 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 network has many of the same security issues that a large corporate network does. You can use a firewall to protect your home network and family from offensive Web sites and potential hackers.

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.

Making the Firewall Fit

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 (Transmission 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 (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.

What It Protects You From

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.

Where can I get more information on firewalls on the Internet?

Site Security Handbook

http://www.rfc-editor.org/rfc/rfc2196.txt The Site Security Handbook is an information IETF document that describes the basic issues that must be addressed for building good site security. Firewalls are one part of a larger security strategy, as the Site Security Handbook shows.

Firewalls Mailing List

http://www.isc.org/index.pl?/ops/lists/firewalls/ The internet firewalls mailing list is a forum for firewall administrators and implementors.

Firewall-Wizards Mailing List

http://honor.icsalabs.com/mailman/listinfo/firewall-wizards The Firewall Wizards Mailing List is a moderated firewall and security related list that is more like a journal than a public soapbox.

Firewall HOWTO

http://www.linuxdoc.org/HOWTO/Firewall-HOWTO.html Describes exactly what is needed to build a firewall, particularly using Linux.

Firewall Toolkit (FWTK) and Firewall Papers

ftp://ftp.tis.com/pub/firewalls/

Marcus Ranum's firewall related publications

http://www.ranum.com/pubs/

Texas A&M University security tools

http://www.net.tamu.edu/ftp/security/TAMU/

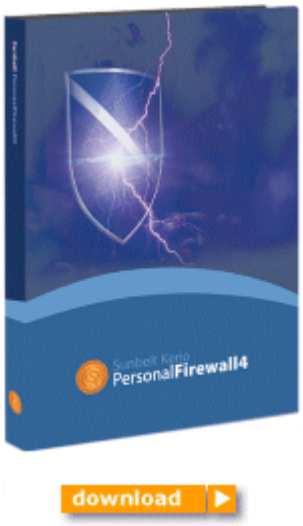
COAST Project Internet Firewalls page

http://www.cerias.purdue.edu/coast/firewalls/

FIREWALLS 2 DOWNLOAD

http://download.zonelabs.com/bin/free/1001_cnet_zdnet/zlsSetup_65_737_000_en.exe

Sunbelt Kerio Personal Firewall™



http://www.sunbelt-software.com/evaluation/440/kerio.exe

Sygate Personal Firewall 5.6

http://link.tucows.com/files3/spf.exe

This firewall automatically protects your PC from hackers and other malicious attacks. It includes full-ICS support, protocol driver-level protection and enhanced logging.

Outpost Firewall

Outpost Firewall Pro provides a superior arsenal of defense against PC infiltration. Outpost ensures your online security with solid protection against all Internet-borne threats.

http://www.agnitum.com/download/trial/7ff9613052f1e3f9d248a1076573bc83/OutpostInstall.exe

(NOTE: download link will be expired after 5 days.)

crack/serial number:

Zone alarm pro 5.1.025.000
S/N: ck5vn3x3fcwsr8vf087bvhw8080
Zone Alarm Pro 5.1.025
d18e4-79gus-crnx1-g1usji-g1rg00
Zone Alarm Pro 5.0.590.015
cmfeu-p72qd-7hbp7-c3cptm-hwq500
Zone Alarm Internet Security Suite 6.0.667.000
dr2wr-3v31k-3707p-3bb52k-psws80
Zone Alarm internet security 6.5.700.000
b9bss-grivu-e50ji-2s65vw-v91bg0

Agnitum Outpost Firewall Pro2.1 Build.303.4009.314
003UsGY+J0WEt8+qi99bGojJRgHlVMFonq6sBf6lJ1ueCpME5undhiejZmxPloQJI/U4u8ACm
Okg78JTVTPm6ia9Z0bA7jOUl0NzYUCct3RqPGmBPivPmqET6BQbnDxTTWrpBiFMxvQye
SBw/RwBYUmLXOsTVeMXWXOC5dwkYarw
Agnitum Outpost Firewall Pro Ver. 3.51.748.6419 (462)
0CpnKPKTRBweUN3TU21h8E5NwtI6D9gLwBCRTXQz7UeFLBUrNgaq+JTKGh
TToGWrLlYyp2nXPrHAFmS89rvtVRIppWQP6v4OIOe4yancSrLqvwDCSv
D9oJ/fgprt1g0E58rbw2pNNT232yYpVF1KC4lDspGcIEExRSK3VKfdzjs71zbkp+pccFqFBYhepaFBWQQ==
Sygate Personal Firewall Pro v5.5 build 2637
G4455565-903176B5 REG CODE: 9WQ7IR9V or G4015540-794106NB
Registration Code : UAU0QAYB or G4275563-912174D4 Registration Code: 3V5BC5TD
Sygate personal firewall pro v 5.5 buil2516
serial:G4505588-935121X7 registration code:5X64D48W
Sygate Personal Firewall Pro 5.5.2577
Serial Number : G4445545-833101NR Registration Code : 60O39E08
Serial Number : G4135547-835113TQ Registration Code : 0F5G0RU8