FIREWALLS: THE PRESENT SECURITY PARADIGM

Dr. Ashok Vasistha*

Aaruni Goel**

Abstract

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. A network firewall performs exactly the same role, protecting an asset inside the firewall from a hazard on the outside. Firewalls are often used to protect an organization from hazards on the Internet but they can, and probably should, also be used within an organization to separate different departments, working areas or networks. Locked offices and buildings cannot protect information if the computers holding it are open to everyone on the network. The importance of securing an organization's internal network has always been high. In today's world of technology hackers, viruses, mal-ware, and identity theft, companies both large and small have found that properly securing their networks is a never-ending challenge. An essential component of achieving effective security is the network firewall. There are many different types of firewalls available, all varying greatly in configuration, capability, and complexity. This document discusses not

only the different firewall types, but also provides some best-practice suggestions for configuration and administration

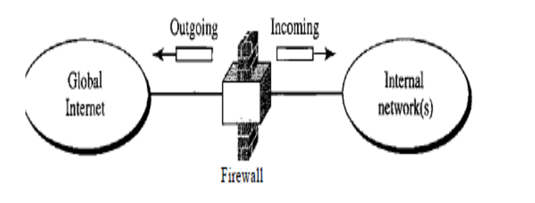
Keywords: Hyper Text Transfer Protocol(HTTP), IP Security(IPSEC), Gateways, Virus, Choke Points, Spams, Botnets, Zombies

* Research Supervisor, Mewar University, Chittorgarh, India.

** Research Scholar , Mewar University, Chittorgarh, India

Introduction

To control access to a system, we need firewalls. A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet. It is designed to forward some packets and filter (not forward) others. In principle, the firewall can be thought of as a pair of mechanisms: one which exists to block traffic, and the other which exists to permit traffic. Some firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic.



Some firewalls permit only email traffic through them, thereby protecting the network against any attacks other than attacks against the email service. Other firewalls provide less strict protections, and block services that are known to be problems. Generally, firewalls are configured to protect against unauthenticated interactive logins from the ``outside" world [1]. More elaborate firewalls block traffic from the outside to the inside, but permit users on the inside to communicate freely with the outside.

For example, a firewall may filter all incoming packets destined for a specific host or a specific server such as HTTP. A firewall can be used to deny access to a specific host or a specific service in the organization. Firewalls provide an important logging and auditing function; often they provide summaries to the administrator about what kinds and amount of traffic passed through it, how many attempts there were to break into it, etc. This is an important point: providing this ``choke point" can serve the same purpose on the network as a guarded gate can for the site's physical premises [2] [3]

IPSEC vs. Firewalls

IPSEC (IP SECurity) refers to a set of standards developed by the Internet Engineering Task Force (IETF). IPSEC solves two problems which have plagued the IP protocol suite for years:

- Host-to-Host authentication (which will let hosts know that they're talking to the hosts they think they are) and
- Encryption (which will prevent attackers from being able to watch the traffic going between machines).

Note that neither of these problems is what firewalls were created to solve. Firewall here is to refer another two classes of problems:

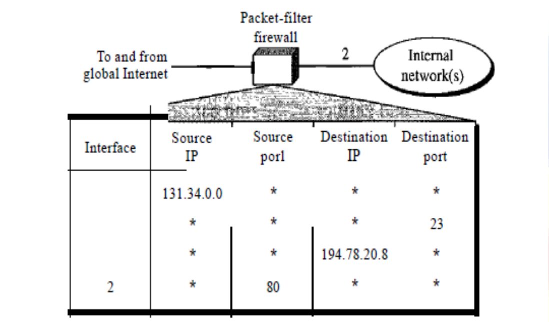
- Integrity and Privacy of the information flowing between hosts and
- The limits placed on what kinds of connectivity is allowed between different networks [2][4].

A firewall is usually classified as a packet-filter firewall or a proxy-based firewall.

1. Packet-Filter Firewall

A firewall can be used as a packet filter. It can forward or block packets based on the information in the network layer and transport layer headers: source and destination IP addresses, source and destination port addresses, and type of protocol (TCP or UDP).

A packet-filter firewall is a **router** that uses a filtering table to decide which packets must be discarded (not forwarded). See Figure 1.



Interface	Source IP	Source porl	Destination IP	Destination port
	131.34.0.0	*	*	*
	*	*	*	23
	*	*	194.78.20.8	*
2	*	80	*	*

Figure 1

1. Incoming packets from network 131.34.0.0 are blocked (security precaution). Note that the * (asterisk) means "any."

2. Incoming packets destined for any internal TELNET server (port 23) are blocked.

3. Incoming packets destined for internal host 194.78.20.8 are blocked. The organization wants this host for internal use only.

4. Outgoing packets destined for an HTTP server (port 80) are blocked. The organization does not want employees to browse the Internet.

It should be noted that a packet filter firewall filters at the network or transport layer.

2. Proxy Firewall

The packet-filter firewall is based on the information available in the network layer and transport layer headers (IP and TCPIUDP). However, sometimes we need to filter a message based on the information available in the message itself (at the application layer). As an example, assume that an organization wants to implement the following policies regarding its Web pages: Only those Internet users who have previously established business relations with the company can have access; access to other users must be blocked. In this case, a packet-filter firewall is not feasible because it cannot distinguish between different packets arriving at TCP port 80 (HTTP). Testing must be done at the application level (using URLs).

One solution is to install a proxy computer (sometimes called an application gateway), which stands between the customer (user client) computer and the corporation computer.

See Figure 2.

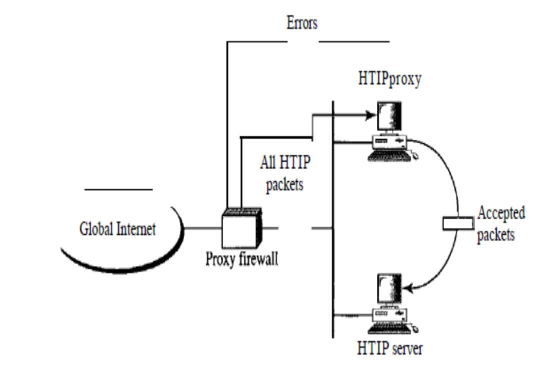


Figure 2

When the user client process sends a message, the proxy firewall runs a server process to receive the request. The server opens the packet at the application level and finds out if the request is legitimate. If it is, the server acts as a client process and sends the message to the real server in the corporation. If it is not, the message is dropped and an error message is sent to the external user. In this way, the requests of the external users are filtered based on the contents at the application layer [5].

This is to be remembered that the proxy firewall filters at the application layer.

Firewall Configuration

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 to remember www.google.co.in 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.

- **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 i.e. fragmentation & reassembly at source & destination.
  - **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 "bomb-purchase" in it. The key here is that it has to be an exact match. The " bomb-purchase ed" filter would not catch "bomb purchase" (no hyphen). But you can include as many words, phrases and variations of them as you need.

SOFTWARE FIREWALLS:

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.

Software firewalls are not much secured, but they are quiet cheap.

HARDWARE FIREWALLS:

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 home network connect to the router, which in turn is connected to either a cable or DSL modem. One can configure the router via a Web-based interface that reach through the browser on computer by setting any filters or additional information.

Hardware firewalls are incredibly secure but are very expensive. Further they are replaced and not reinstalled like software firewalls [6].

Impacts of Firewalls

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 [5][7][8].

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 firewall as long as one accept e-mail. The level of security you establish will determine how many of these threats can be stopped by 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 one will allow. 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.

Firewall Disability

Firewalls can't protect against attacks that don't go through the firewall. Many corporations that connect to the Internet are very concerned about proprietary data leaking out of the company through that route. Unfortunately for those concerned, a magnetic tape can just as effectively be used to export data.

Firewall policies must be realistic and reflect the level of security in the entire network. For example, a site with top secret or classified data doesn't need a firewall at all: it should be placed isolated from the rest of the corporate network & Internet.

Another thing a firewall can't really protect against is traitors or fools inside the network.

Firewalls can't protect very well against things like viruses. There are too many ways of encoding binary files for transfer over networks, and too many different architectures and viruses to try to search for them all. In general, a firewall cannot protect against a data-driven attacks in which something is mailed or copied to an internal host where it is then executed. So blanketing your network with virus scanning software(a antivirus) will protect against viruses that come in via pen drives, modems, and Internet [9] [10].

Conclusion

As one can see having a firewall and thereby protecting the computer is a necessity from hackers or viruses. With the proper monitoring and rules one will be able to use applications on the Internet safely. It is quite obvious that when one leaves house, he locks doors to prevent robbery, then why not use a firewall to put a lock on computer. Firewalls can no longer stay isolated from the rest of the world. Rather than closed systems, today's firewalls are enforcers in a global intelligence network that collects, shares and updates information about applications, attack signatures, attacker addresses and reputations. The firewall is just one part of this global "conversation" about attacks and is only as good as the latest update. Because of zero-day attacks and rapidly propagating malware, firewalls must be able to respond the latest threats with great speed. Firewall administrators need to be able to manage firewalls as a "fleet" deploying new access control restrictions, patterns, signatures and policies across a global infrastructure. The firewalls must also be able to receive updates automatically, to counter distributed threats like botnets. Botnets evolve very rapidly and can attack from multiple directions at the same time. In order to defend against such threats, firewalls need to be able to receive automatic reputation updates that can identify and counter the latest botnets as they are discovered.

References

[1] Tesink, S. (2007). Improving Intrusion Detection Systems through Machine Learning. Group, (07). www.bughunt.org/thesis_lai.pdf

[2] Cramer, M. L. , Cannady, J. , & Harrell, J. (1996). New Methods of Intrusion Detection using Control-Loop Measurement. Information SystemsSecurity. http://w.w.w.scis.nova.edu/~cannady/ids_newm.pdf

[3] Abad, C. , Taylor, J. , & Rowe, K. (n. d.). Log Correlation for Intrusion Detection?: A Proof of Concept Systems Research. www.cs.scranton.edu/~dag2/blog/10_19/intrusion.pdf

[4] Paper, W. (n. d.). Firewalls – Overview and Best Practices. www.decipherinfosys.com/Firewall.pdf

[5] Kerkhofs, J. , &Pannemans, D. (2001). Web Usage Mining on Proxy Servers?: A Case Study. www.citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.116.

[6] Ning, P. , & Carolina, N. (n. d.). Intrusion Detection Techniques. Bernoulli. https://alexids.googlecode.com/files/IDTechniques.pdf

[7] Booth, D. , & Jansen, B. J. A Review of Methodologies for Analyzing Websites. faculty.ist.psu.edu/jjansen/academic/jansen_website_analysis.pdf

[8] Zhang, C. , Zhang, G. , & Sun, S. (2009). A Mixed Unsupervised Clustering-Based Intrusion Detection Model. 2009 Third International Conference on Genetic and Evolutionary Computing, 426-428. Ieee. doi:10. 1109/WGEC. 2009. 72 www.ieeexplore.ieee.org/xpl/articleDetails.jsp?reload...Conference...

[9] Salama, S. E. , I. Marie, M. , El-Fangary, L. M. , & K. Helmy, Y. (2011). Web Server Logs Preprocessing for Web Intrusion Detection. Computer and Information Science, 4(4), 123-133. doi:10. 5539/cis. v4n4p123 www.journal.ccsenet.org/index.php/cis/article/download/10909/7966

[10] Brugger, S. T. (n. d.). Data Mining Methods for Network Intrusion Detection, V, 1-35. www.minds.cs.umn.edu/papers/nsf_ngdm_2002.pdf