Information Security 2IF30
Essay: Firewalls and intrusion detection

Christian Luijten, 0496505

October 25, 2004

Firewalls and intrusion detections measures have become a necessity on today's networks. Virtually every company in the western world "does something with Internet", often ignorant of the risks they expose themselves to.

1 History

When the Internet was developed, the only users online were the developers of it themselves. They were universities and the U.S. military and since they were not out to destroy their own creation, there was no need for firewalls or intrusion detection.

As the Internet opened up for any user, the network became a virtual playing ground for users who were technically advanced. Previously they were cracking corporate phone systems (called 'phreaking' or 'wardialing'), now they were on new and unexplored grounds. It created many new oppurtunities to get all sorts of information from the technically challenged users of the Internet.

The need for securing information was born.

2 Early firewalls

Before firewalls came into being, computers usually were directly addressible from the Internet. They could be reached from the outside. The securing of these machines had to be done individually, a task that is infeasible if your network consists of tens or even hundreds of machines. Firewalls were introduced as a gatekeeper between the big bad Internet and the trusted local network. They let outgoing connections go through without problems, but incoming connections were blocked, with little exceptions made.

They work, but lay big restrictions on the usage of the network. For instance, if incoming packets are blocked, then noone can reach the webserver of the network from outside. A safe passage has to be created from the firewall to the webserver, without the packets being able to go another way if they are past the firewall.

Since early networks were shared mediums, and packets destined for one machine are received by all other machines on the network, this can be a problem if for instance a known vulnerability for a buffer overflow in one of the IP stacks of the machines in the network is found.

A solution to this problem is placing the machines which receive request from the Internet in another network and connecting the two networks with a switch or bridge. This way, packets destined for the webserver don't reach the internal machines with lowered security measures.

3 The Internet boom

Around 1993, together with the introduction of the first World Wide Web browser Mosaic and the first webservers, the Internet really became a network for everyone. Every person with a computer and a modem could subscribe to an Internet Service Provider (ISP) and 'surf the web'. Before that time, the Internet was mostly FTP, Usenet, Gopher and of course E-Mail.

People with standard IBM PC's running a defacto standard operating system using a defacto standard browser were connecting to the Internet which was before that a varied mixture of many different systems.

Just like in nature, monocultures tend to be vulnerable to infections by viruses and illnesses and that is exactly what happened. Already in 1988 an Internet worm was released which propagated through BSD Unix machines, but the first really successful worm came in 1999 and was called Melissa.

Melissa infected Microsoft Word files and sent out considerable amounts of E-Mails using Microsoft Outlook, clogging many Microsoft Exchange mailservers. It was the first time that an attack came from the presumedly safe internal network and there were no measures against such an attack. Many networks went down on the load the mails put on them and E-Mail on the Internet itself came almost to a halt.

4 Current firewalls

Today, firewalls are far more than the packet manglers they used to be. On systems running Microsoft Windows, they are often integrated with anti-virus

and privacy software. A good firewall also keeps logfiles in order to detect and deal with intrusion attempts.

Examples of firewalls include iptables for Linux 2.6 and ZoneAlarm for Windows.

4.1 Keeping packets out

One of the key features of a firewall is of course keeping packets that don't belong on the network out. By default, if a port isn't opened by a program on the machine, it is closed and no connections can be made there. If no ports are opened, there is no need for an inbound firewall at all.

But, malicious software might open a port without the user knowing. A trojan horse could announce itself to someone on the internet who can then connect to the system and take it over. A firewall that blocks everything solves this and does not restrict the usage of the machine, which should not have any open ports in the first place, at all.

It is however still possible for a trojan to make an outbound connection to some server and then hand over control over the system.

4.2 Keeping packets in

In order to prevent data caused by viruses or illegal activities to get out of the network, a firewall also can provide some services.

The owner of a system is also responsible for the use of it, including misuse. If a system is used in a denial of service attack (DoS), the owner is responsible for finding out who abused his system.

A firewall can make sure no packets go out of the system. Of course, that is not what a normal user wants, so there have to be exceptions.

For example, many ISPs nowadays block outbound SMTP connections, except for the connection to their own, well-administrated, SMTP server. They do this to be able to control the mailflow coming from infected systems to make sure their IP addresses don't get on blacklists used by other ISPs to filter out garbage, thereby also discarding perfectly legitimate mail.

4.3 Detecting and reporting intrusions

One of the purposes of logging everything which passes a firewall is detecting intrusions. In the past decennium, much effort has been put in detecting intrusions by using statistics and other artificial intelligence techniques like neural networks to detect patterns in traffic.

As attackers become smarter, they choose more non-obvious ways of getting in a system or a network. Also, they tend to be more cautious and prefer a very slow and low profile attack in order to slip past human logfile analysers. An automated system could detect such an attack and stop it before it succeeds.

4.4 Other tasks integrated in firewalls

Firewalls often do various other tasks besides blocking packets. Popular are web proxies and mail scanners. Both are preferably transparent to the end users, thus they don't have to configure anything on their own computers.

4.4.1 Web proxy

Web proxies can for instance cache pages that are requested for later reuse and block advertisements (banners) on web pages. Both are perfectly benign uses of web proxies. It is however also possible to track users and to block certain websites.

In a company, this can put the relation between employer and employee under pressure. Mutual distrust is no basis for a healthy relation. There are various examples of people who got fired because they were surfing the web for private goals during working time and also of people leaving companies who don't trust their employees.

At home, if the filtering is done by the internet service provider or the government this can lead to serious privacy interventions and even censorship. In China, the national Internet connection is controlled by the government and web pages like Google are censored.

In order to configure a web proxy, all outgoing packets destined for a HTTP port (80 or 443) should be rerouted through a process on the firewall machine itself or on another machine handling the requests.

The author uses a Linux iptables firewall with the Squid web proxy running on port 3128. The command to direct HTTP requests to Squid is

```
/sbin/iptables -t nat -A PREROUTING -p tcp -i eth0 --dport 80 \
  -j REDIRECT -d ! 192.168.0.0/16 -s 192.168.0.0/16 --to-ports 3128
```

Meaning: Every TCP connection (-p) with destination port 80 (–dport) and the destination is not on the local intranet (-d) is being redirected (-j) to port 3128 (–to-ports) on the firewall, but only if the packet came in via the intranet interface (-i).

4.4.2 Mail scanner

Sending one E-Mail message costs about the same as sending one million E-Mail messages.

Secondly, the mail system is not an authorized system, so anyone can state to be anyone they like.

This is interesting for a company who wants to sell something; instead of having to pay for one million flyers and distribute them, it can send out one million E-Mails at a fraction of the cost. This is called junk mail and clogs the mail system and almost any Internet user will say he hates this misuse.

Junk mail on itself puts no threat to the security of a network, but the bandwidth it takes, and thus the cost, is considerable. Of greater risk are E-Mail viruses which spread using broken mail clients and infecting other users via E-Mail. Those who don't use the vulnerable mail clients are still overwhelmed by the enormous amounts of mails they get from others who are infected.

Junk mail and virus protection can be integrated into a firewall, by rerouting all packets to the SMTP ports (25 and 465) to a scanner process. However, since mail is a routed application layer protocol, it can also be done in a nicer fashion, by using MX DNS records and blocking SMTP from the outside to anything else but the mailserver.

The mailserver can read the messages and decide upon if they are spam or contain viruses, deal with them appropriately and send them on on their journey to the receiver. There are various applications which filter out the garbage by using Bayesian statistics and pattern matching. Mail filters include SpamAssassin[1] (used by the TU Eindhoven) and Bogofilter[2]. Some mail clients offer filters themselves, like Mozilla Thunderbird[3] and Novell Evolution[4].

4.5 Annoyances by firewalls

The author has experiences with clients (home users) removing their firewall because of annoyance about the user interaction of the software. They knowingly expose themselves to the dangers of the Internet, but there is no decent way for them to configure a firewall properly.

While firewalls should be unobtrusive to the end user doing its normal job, Windows firewalls tend to present the user with all sorts of questions they don't know the answer to. When they are configured after a while, they almost always are in a sort of paranoid mode, feeling the need to inform the user about every

[1] http://spamassassin.apache.org/
[2] http://bogofilter.sourceforge.net/
[3] http://www.mozilla.org/products/thunderbird/
[4] http://www.novell.com/products/evolution/

single incoming packet. In the end that annoys the users so much they decide to completely remove the firewall and remain unprotected.

A firewall should do its job quietly and correctly. It should have sane defaults and protect the user from the moment it is started. Firewalls are created to protect the ignorant, but for their configuration a crash course in computer networks is often necessary.

4.6 The quiet and sensible firewall

The new Windows Firewall which is integrated in Windows XP Service Pack 2 does a better job on ease of use, giving the user basically only the choice of being protected or not (see Figure 1). If this firewall works, it is great, if it doesn't it gives the user a false sense of security, which is even worse than to know you have no security. It does however nothing about outgoing traffic.

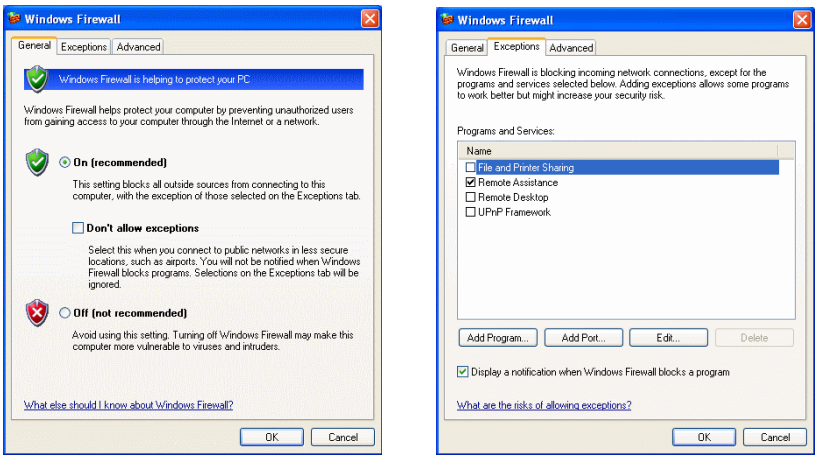

Figure 1: Windows Firewall

Linux firewalls aren't much better when it comes to ease of configuration, but they don't display dangerous looking warnings on the screen of the user. Besides that, Linux (and most Unices) are secure by default by not opening ports that are not strictly needed, so a firewall to keep packets out is often unnecessary.

5 Future

In the future, more illicit activities will occur. Companies are becoming more dependent on the Internet for their businesses and where is money, there will

always be crime.

Attempts to prevent attacks like distribute denial of service attacks will result in broken networks if no security model for the Internet as a whole will be implemented. TCP and IP were both developed in the early 1980s when the Internet was not a place like it is today and actually never was thought to be like today.