Internet Security

Jason Lingohr & Rick Harris
The Fulcrum Consulting Group

15 April, 1997*

Abstract

As we all know, the Internet can be a wonderful thing. Along with its wonders though, come risks, forcing us to protect our valuable networks. The Internet is so large and varied though that protection can be quite a complex and sometimes costly venture. This document describes some aspects of a successful corporate-strength firewall, including monitoring, management, architecture, tools and design approaches.

1 Introduction

Corporate networks connected to the Internet are becoming more popular. The fundamental design of the Internet allows for unimaginable business possibilities, and this realisation itself is gaining popularity.

Along with this comes a higher awareness from would-be intruders of this same fact – there is a lot of valuable information available on the Internet. Much of this is without protection and is fully exposed to these would-be intruders. What's more, every day more businesses connect.

In light of this reality, Internet firewalls are also becoming popular. Their structure and function can differ depending on the requirements of the organisation, but essentially they all share the same goal to protect and serve.

2 Problem space

Problem: there exists a need to connect your networks to "the outside world", but you do not want your network and its information exposed and freely available to the rest of the world. Solution: a firewall.

The fundamental idea behind a firewall is to connect two (or more) networks together, but to give the ability to restrict both who and what goes between those networks. Consider the idea behind a castle, its moat, doors, bastion and so on, as this is effectively the same concept.

Successfully employing a firewall is a challenge; mostly requiring something more "intelligent" than just a router, or set of routers. Unix, TCP/IP and other open systems technologies have been the basis for building firewalls for some time, but the design concept of open systems is functionality, not security. This problem is slowly diminishing as these systems are made more robust and secure, but still has some way to go. The idea of firewalls is not to be open, as openness tends to give users more power, not less.

An important point to be made clear is that a network administrator, or management, might consider their networks contents to be useless information to any knowledgable would-be attacker. Conversely, the people who would find this private information useful would not have the required skills to access it.

This may be true, but user friendly "exploit" code is available on the Internet that takes advantage of inherent weaknesses in open systems, and is often cookbook style. This gives the average user the ability to intrude; including competitors, disgruntled customers or people just out for some fun.

It is a difficult task to secure all of your systems against attack from the outside, so the firewall allows you to concentrate much of your attention on the point at which the network is most at risk: the Internet gateway.

*Presented at the CMGA conference, 1997

3 Firewall Architecture & Technology

3.1 Security Policy

The design of a good firewall begins with a security policy. The importance of a policy cannot be stressed enough. If you don't know what you are trying to achieve, how will you know when you have done it?

Many organisations already have an unwritten policy being used. In these cases, writing the policy is a case of determining what that policy is and making sure that everyone agrees. It may be reasonable to add to an existing "building security" policy or, perhaps more appropriately, an existing "sensitive document management" policy.

A strong policy allows the development of a good case for properly protecting your computing assets. It should have the input and backing of management and technical staff. Once in place, a security policy acts as a guideline for the operation and use of the computing facilities.

The role of a firewall is then merely to enforce the agreed-upon security policy.

3.2 Simplicity

One of the key elements in a firewall and its design is simplicity. A simple system is one that is easy to understand. The more complex a firewall becomes, the more likely a mistake will be made in designing, implementing, installing, configuring or operating the firewall.

Mistakes can vary between a simple typing mistake in a rules database, through to a complete lack of understanding of the firewalls structure leading to fundamental configuration errors.

3.3 Education

An understanding of the network technology and protocols being used is important in building or configuring a firewall. Using an off-the-shelf product without completely understanding what it does may lead to serious defects in its security. One example would be the installation of a commodity firewall "backwards", where the Internet was protected from the internal network while allowing any system on the Internet to connect to the internal network. This is an extreme example, but it can happen without proper education.

More commonly, allowing a protocol to pass through the firewall may open an internal system to attack. Only by understanding the protocols and applications can an intelligent decision be made about the risks.

3.4 Established Technology

This is fairly straightforward logic; why re-invent the wheel? A firewall, obviously, has to consist of trusted parts; introducing new and untested components only makes the whole task of installing a firewall that much more unnecessarily complex.

Established technology can include things such as brand-name routers, operating systems and software that has been in development for the purpose of a firewall for a substantial time. Using known and tested components is a given in the installation of a corporate-strength firewall.

3.5 Defence in Depth

When designing a firewall, it is useful to keep in mind the possibility that a particular component of that firewall will fail to do its job. Tomorrow, someone may discover a magical bug in the system software that will completely drop the defences of some part of your firewall. If redundancy is built into the firewall system, there is at least a chance that the internal network will be safe. This is commonly described as "defence in depth".

It is important not to rely on unusual configurations to protect your system. A good exercise is to reconsider the security of a firewall in the event of an attacker having complete documentation available to them. Good security is based on solid doors, locks and keys, not just a twisted maze. Today's contractor may turn into tomorrow's attacker, so do not assume that no one knows how the firewall works.

3.6 Packet Filtering

Packet filtering is a technique where data packets are selectively passed or ignored when attempting to pass through a network device, like a router. The decision to pass or ignore a packet is based on the lower-level protocol, so a packet filter can examine the source and destination addresses, protocols and some other special options. The actual data being transferred, however, is not taken into account when deciding whether to forward a packet. Advantages of using packet filters include:

- Requires little computer power to examine the low-level protocol layer information.
- Existing network equipment will often already support packet filtering.
- Users do not need to change the way they work.

Disadvantages of using packet filtering include:

- The low-level packet examination makes its applications limited to implementing policies like “do not allow any user to connect to system A” and not for policies like “do not allow user Z to connect to system A”.
- Some protocols cannot be effectively controlled with packet filters.
- Packet filters can be difficult to correctly configure.

4 Proxies

A proxy is a mini-application that relays data from one network to another. A connection is made through the firewall by first connecting to the firewall itself. The firewall then opens a connection to the desired destination. This may happen in a completely transparent way, so the user does not know it is happening. Advantages include:

- Proxies are designed and implemented with knowledge of the protocols being used. This allows much more intelligent control over the connection. For example, a proxy can accept or deny a connection based on the user attempting the connection. A proxy for a file transfer protocol can allow only certain files to be available.
- Proxy services can provide more detailed logging (due to the fact that it understands the data it is forwarding).

Nothing comes for free, though:

- Proxies are often slower, as they are examining more data.
- A proxy must be available for every protocol being used.
- Effective use of proxies may require modification to the client or server software.
- Some protocols are too difficult to effectively control, due to their complexity or flexibility.

5 Stateful Filtering

Stateful filtering is a combination of packet filtering and proxy use. It combines knowledge of the protocols being used with the speed of packet filtering. For example, if a service is a request-reply type service, a stateful filter can reject a reply for which it has not seen a corresponding request.

6 Combinations

Most commercial firewalls are a combination of several of the above technologies in order to produce a secure, but functional, system. This is in line with the “defence in depth” philosophy of avoiding reliance on any single technology.

7 After Installation

Once a firewall is installed, it is important to properly maintain it, for several reasons:

- Changes in security policy need to be reflected by the firewall.
- Newly discovered weaknesses in existing technology can leave the firewall vulnerable to attack.
- Routine problems, like a logging disk filling, need to be noticed and rectified.

8 Monitoring

Once installed, the firewall should be closely watched to ensure any attempted attacks are properly thwarted. Even a heavily fortified castle will have guards posted to make sure no one is climbing the walls.

Some guidelines may help in determining a monitoring regime:

- Log as much as possible – it is easier to ignore unwanted information than it is to find more information after the fact.
- Flag possible events that you know about that are important. This includes attempts to log into the firewall or configuration updates. If an event of this sort is received unexpectedly, there is a problem to worry about.
- Use an automated filter to remove log messages that are generated with normal operation. If all of the logs are examined, important messages will often be lost in the noise of routine messages.
- Messages that are left over after filtering should be examined to determine why they occurred. Update your log filters to appropriately deal with these messages in the future.

Most importantly, if the firewall is not being watched closely, an intruder may never be noticed.

9 Maintenance

An important part of any firewall administrators job is keeping up to date with new security problems. Keeping track of problems and updates to solve those problems is a trying and time-consuming occupation, but is an excellent weapon against attackers who are continually finding new ways to break into your systems.

Common ways of achieving this continuing education are mailing lists, security bulletins and newsgroups. There are organisations that exist solely for the purpose of tracking and publishing security information. These are often the first to know of any problems that surface in the security of computing. Organisations such as CERT, and the Australian equivalent AUSCERT, are examples of this.

The vendors of the various components also provide updates and information about their products. Maintaining contact with these vendors is an important way to keep educated about the the firewall and computer security in general.

10 Conclusion

This paper has described some aspects of building and maintaining an effective Internet firewall. A firewall needs to perform a complex job but when properly implemented provides an effective and efficient means to protect your network.

Important issues to consider when building a firewall include:

- Keep it simple
- Avoid reliance on any single technology. Do not ignore internal security just because you have a firewall.
- Fail-safe not fail-open. The firewall is there to protect your network. If a component fails, it is better to deny access to everyone rather than let the Internet hoards in.
- Pay close attention to the proper configuration of the system. Buying an off-the-shelf solution will not help if it is not properly set up to implement the organisation's security policy.
- Watch the firewall closely to make sure it is performing its job.
- Treat your firewall like a virus scanner keep it up to date on a regular basis.

Opportunities that are offered by the Internet can be safely pursued if appropriate precautions are taken. The decision to connect to the Internet should be an informed and measured one, not one taken lightly.