An Overview of Firewall Technologies[1]

Habtamu Abie
Norwegian Computing Center
P. O. Box 114 Blindern, 0314 Oslo, Norway
abie@nr.no, http://www.nr.no/~abie
January 2000

Abstract

The increasing complexity of networks, and the need to make them more open due to the growing emphasis on and attractiveness of the Internet as a medium for business transactions, mean that networks are becoming more and more exposed to attacks, both from without and from within. The search is on for mechanisms and techniques for the protection of internal networks from such attacks. One of the protective mechanisms under serious consideration is the firewall. A firewall protects a network by guarding the points of entry to it. Firewalls are becoming more sophisticated by the day, and new features are constantly being added, so that, in spite of the criticisms made of them and developmental trends threatening them, they are still a powerful protective mechanism. This article provides an overview of firewall technologies.

Keywords: Firewall Technologies, Network Security, Access Control, Security Policy, Protective Mechanisms.

1 Introduction

Today's networks change and develop on a regular basis to adapt to new business situations, such as reorganisations, acquisitions, outsourcing, mergers, joint ventures, and strategic partnerships, and the increasing degree to which internal networks are connected to the Internet. The increased complexity and openness of the network thus caused makes the question of security more complicated than hitherto, and necessitates the development of sophisticated security technologies at the interface between networks of different security domains, such as between Intranet and Internet or Extranet. The best way of ensuring interface security is the use of a firewall.

A Firewall is a computer, router or other communication device that filters access to the protected network [18]. Cheswick and Bellovin [6] define a firewall as a collection of components or a system that is placed between two networks and possesses the following properties:

- All traffic from inside to outside, and vice-versa, must pass through it.
- Only authorised traffic, as defined by the local security policy, is allowed to pass through it.
- The firewall itself is immune to penetration.

[1] Telektronikk Volume 96 No. 3-2000, pp.47-52

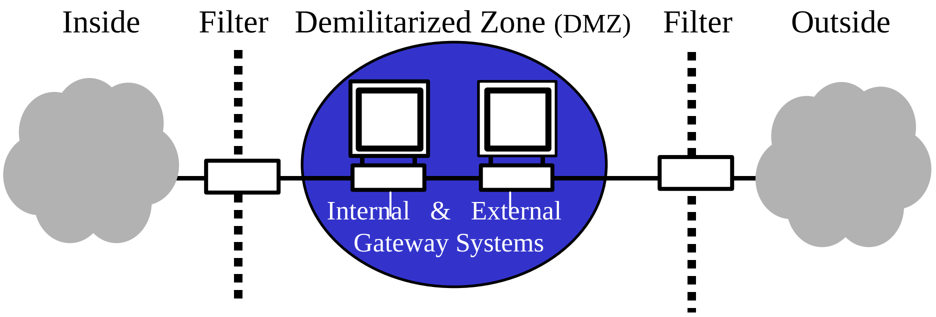

Figure 1: Firewall Schematics

Such traditional network firewalls prevent unauthorised access and attacks by protecting the points of entry into the network. As Figure 1 shows, a firewall may consist of a variety of components including host (called bastion host), router filters (or screens), and services. A gateway is a machine or set of machines that provides relay services complementing the filters. Another term illustrated in the figure is "demilitarised zone or DMZ"[6]. This is an area or sub-network between the inside and outside networks that is partially protected. One or more gateway machines may be located in the DMZ. Exemplifying a traditional security concept, defence-in-depth, the outside filter protects the gateway from attack, while the inside gateway guards against the consequences of a compromised gateway [6, 10]. Depending on the situation of the network concerned, there may be multiple firewalls, multiple internal networks, VPNs, Extranets and perimeter networks. There may also be a variety of connection types, such as TCP and UDP, audio or video streaming, and downloading of applets. Different types of firewall configuration with extensive practical guides can be found in [6, 4]. There are also many firewall products on the market from different vendors. See [9] for an updated list of products and vendors.

This article surveys the basic concept of firewall technology by introducing the various kinds of approach, their applications, limitations and threats against them.

2 Firewalls: Basic Approaches and Limitations

Firewall technology can be used to protect networks, by installing it strategically at a single security screen station where the private network or the Intranet connects to the public Internet, making it easier to ensure security, audit and monitor traffic, and trace break-in attempts. It can also be used to isolate sub-networks, in order to provide additional layers of security (defence-in-depth) within the organisation. There are three basic approaches or services that a firewall uses to protect a network: packet filtering, circuit proxy, and application proxy [6, 11]. Some authors [13, 10] broadly classify these into two kinds of approach: transport level and application level (by including circuit proxy in this category).

2.1 Packet filtering

Firewalls having this function perform only very basic operations, such as examining the packet header, verifying the IP address, the port or both, and granting and denying access without making any changes. Due to this simplicity of operation, they have the advantage of both speed and efficiency. The filtered packets may be incoming, outgoing or both, depending on the type of router. An additional advantage is that they do their job quiet independently of the user's knowledge or assistance, i.e., they have good transparency. Packets can be filtered on the basis of some or all of the following criteria: source IP address, destination IP address, TCP/UDP source port, and TCP/UDP destination port. A firewall of this type can block connections to and from specific hosts, networks and ports. They are cheap since they use software already resident in the router, and provide a good level of security since they are placed strategically at the choke point.

2.2 Circuit Proxy

The second approach is the use of what is called a circuit proxy. The main difference between the circuit proxy and the packet filtering firewall is that the former is the addressee to which all communicators must address their packets. Assuming access has been granted, the circuit proxy replaces the original address (its own) with the address of the intended destination. It has the disadvantage of laying claim to the processing resources required to make changes to the header, and the advantage of concealing the IP address of the target system.

2.3 Application Proxy

The third approach involves the use of what is known as an application proxy. An application proxy is more complicated in operation than a packet filtering firewall or a circuit proxy. The application proxy understands the application protocol and data, and intercepts any information intended for that application. On the basis of the amount of information available to make decisions, the application proxy can authenticate users and judge whether any of the data could pose a threat. The price to be paid for this more comprehensive function is that users or clients often have to be reconfigured to them, sometimes a complicated process, with a consequent loss of transparency. Application proxies are referred to as proxy services, and the host machines running them as application gateways.

2.4 Packet Inspection Approach

This approach, in contrast to the technologies so far described, involves inspecting the contents of packets as wells as their headers. An inspection firewall carries out its inspection by using an inspection module, which understands, and can therefore inspect, data destined for all layers (from network layer to application layer). It carries out its inspection by integrating all information gathered from all layers into a single inspection point, and then examining it. A state-full inspection firewall is one which also registers the state of any connection it is handling, and acts on this information. An example of a state-full inspection firewall is the state-full packet-filtering mode in Checkpoint's “Firewall-1”[5] or Network Associates' Gauntlet.

Inspection firewalls can provide address translation and hiding, virus scanning, Web site filtering, screening for key words (typically in e-mail), and context-sensitive security for complex applications.

2.5 Firewall Limitations

As pointed out in [10], "Information security professionals often find themselves working against misconception and popular opinions formed from incomplete data. Some of these opinions spring more from hope than fact, such as the idea that internal network security can be solved simply by deploying a firewall". While it is true that firewalls play an important and central role in the maintenance of network security and any organisation that ignores them, does so at its peril, they are neither the panacea of every security aspect of a network, nor the sole sufficient bulwark against intrusion. Knowing what firewalls can't do is as important as knowing what they can. The following are limitations one should be aware of.

- A firewall is by its nature perimeter defence, and not geared to combating the enemy within, and consequently no useful counter measure against a user who abuses authorised access to the domain.
- A firewall is no real defence against malicious code problems like viruses and Trojan horses, although some are capable of scanning the code for telltale signs.
- Configuring packet-filtering rules tends to be complicated process in the course of which errors can easily occur, leading to holes in the defence. In addition, testing the configured rules tends to be a lengthy and difficult process due to the shortcomings of current testing tools. Normal packet-filtering routers cannot enforce some security policies simply because the necessary information is not available to them.

3 Additional Important Features

Firewalls are becoming more complex and sophisticated by the day, and thus more efficient at identifying intrusions and logging them, and automatically notifying the right people. They provide multiple layers of protection and some cache data to improve performance, and support Virtual Private Network (VPNs), Web-based administration, authentication, etc. There is also a tendency to add non-security-related functions to the firewall such as built-in Web servers, FTP servers, and e-mail systems, and even proxy servers for streaming audio and video.

We agree with those who feel that some additions to firewalls make sense and are useful when they enhance security, while others don't make sense and may even be dangerous, especially over time, when they represent a decrease in security and an increase in vulnerability. For example, to add services that increase the administration load adds another potential avenue of attack.

3.1 Content Caching

While caching is not traditionally a function of firewalls, it is becoming an increasingly frequent and important feature. An increase in performance is achieved by caching the contents of an accessed location with the result that subsequent requests for access will lead to already cached contents being used, without it being necessary to access the location again (except when it is necessary to refresh).

3.2 Logging and Alerts

It is important for a firewall to log events, determine their legitimacy or otherwise, and notify the network administrator. It should be noted that it is essential to protect the integrity of the log, since unauthorised access to, and editing of, the log will, of course, neutralise its raison d’être. Whether the function of protecting the log is fulfilled by the firewall itself or not, is a matter of implementation.

3.3 Management

Management ranges from command line to sophisticated GUI-based and secured remote access. Security management and administration, particularly as it applies to different firewalls using different technologies and provided by different vendors, is a critical problem. As more and more security services are introduced and applied to different firewall components, properly configuring and maintaining the services consistently becomes increasingly difficult. An error by an administrator in maintaining a consistent configuration of security services can easily lead to security vulnerability. A firewall should thus provide a security management interface that enables it to be locally or remotely managed in a coherent and comprehensible fashion.

3.4 Virtual Private Networks (VPNs)

A VPN is an encrypted tunnel over the Internet or another untrusted network providing confidentiality and integrity of transmissions, and logically all hosts in a VPN are in one Intranet [18]. Some firewalls include VPN capabilities (reasonable extension) to secure networks, so that they can safely communicate in private over the public network. They achieve this by strong authentication and encryption of all traffic between them.

3.5 Adaptive Firewalls

The new trend is towards adaptive firewalls that tie filters, circuit gateways and proxies together in series [2]. This gives the firewall administrator greater control over the level of security used for different services or at different points in the use of those services. He may, for example, configure the firewall to give priority to speed of transfer at the expense of security when this is appropriate. The firewall will then on such occasions reduce security to a lower level, thus allowing for greater speed of transfer, and return it to its original level on completion of the transfer.

Phoenix [17] states that Adaptive Firewall Technology provides fluid, self-adapting control of network access, a key to establishing an effective network security policy by examining every packet (and adapting rules "on-the-fly" based on information in the packet) passing through the network interface.

3.6 Quality of Service (QoS)

Some firewalls include QoS features that allow administrators to control what proportion of a given network connection is to be dedicated to a given service. There are those who feel that QoS should be handled by Internet routers, while others insist that this is a matter of access control, and thus should be included in the firewall. Quoting [2]: "Moreover, some vendors, notably Check Point, have built their QoS engine using the same technology that is in their firewall. The philosophy here seems to be, access control is access control."

3.7 Policy and Firewalls

There are two levels of network policy that directly influence the design, installation and use of a firewall system: higher-level policy and lower-level policy [10]. The former is the network service access policy, which lays down which services are to be accessible to whom, and how they are to be used. The latter is the firewall design policy, which describes how the firewall will implement the network service access policy, and precisely how it will take access decisions in accordance with it. Firewalls typically implement one of two design policies. The firewall may permit any service not expressly denied, or it may deny any service not expressly permitted.

Service access policy may, for example, decree that there shall be no access to a site from the Internet, but allow access from the site to the Internet. Alternatively, it may decree that access from the Internet shall be restricted to certain selected services in the site. The latter is the more widespread of the two.

Today’s business environments are, however, dynamic. Organisations are continually changing to adapt to new circumstances brought about by reorganisations, mergers, acquisitions etc. Therefore there are regularly new policies to be enforced, and, to remain effective, today’s firewalls must be able to adapt to them.

4 Trends Threatening Firewalls – and Counter Trends

4.1 Trends Threatening Firewalls

Common network denial of service attacks include mail bombs, ping floods, and attacks using known software bugs, all of which are reported to be on the increase. This fact alone means that traditional firewalls performing packet analysis using rules and patterns are no longer adequate protection against network-based attacks, in addition to which, according to recent risk surveys [20, 19, 16, 7], more than half of all breaches today are perpetrated by some legitimate user already behind the firewall.

The traditional assumption that all inside the firewall are friendly and all outside it potentially hostile, is now becoming somewhat outdated. Internet connectivity has expanded, Extranets can allow outsiders access to areas protected by firewalls, and some machines require greater access to the outside than others, which often involves a change in the internal IP address. Another threat is the use of end-to-end encryption since the firewall is unable to peer through the encryption.

In the literature [3], some people have gone so far as to suggest that a more adaptive approach would be to drop firewalls altogether on the basis that they are obsolete, or that the use of cryptography obviates the need for them. Bellovin [3] disagrees with this view, and so do we.

4.2 Counter Trends and Arguments

Bellovin [3] argues that firewalls are still powerful protective mechanisms for the following reasons:

- Most security problems are due to buggy code - in 1998, 9 of 13 CERT advisories concerned buffer overflows and two of the rest were cryptographic bugs - and cannot be prevented by encryption or authentication. A firewall shields most such applications from hostile connections.
- Firewalls are also useful at protecting legacy systems. While applications that require strong authentication should provide their own, there are too many older protocols and implementations that do not. Saying that strong cryptography

should be used is true but irrelevant. In the context of such applications, it is simply unavailable.

- More subtly, firewalls are a mechanism for policy control. That is, they permit a site's administrator to set a policy on external access. Just as file permissions enforce an internal security policy, a firewall can enforce an external security policy.

As already stated, we concur with the above, and cite the following additional arguments.

Cryptography notwithstanding, the use of firewalls is deeply entrenched in a number of organisations and is part and parcel of their security set up, and will continue to be so for some years yet. While it is true that cryptography is the heir apparent to the firewall, the number of as yet unresolved issues prevents the assembling of a comprehensive solution for securing distributed computing resources around Public Key Infrastructure (PKI) and encryption. In addition, the process of standardisation within the area of PKI is not proceeding particularly rapidly. Thus, even those organisations favouring technologies other than firewalls will just have to bite the bullet and live with them for the moment.

Another factor is the ongoing development of new features and services at present being continually added to firewalls. These reduce a number of the limitations listed above and increase the firewall's flexibility while allowing it to retain its original function unimpaired. Examples, to mention but a few, that illustrate this point are:

- The proposal of a distributed firewall [3], using IPSEC (IP Security), a policy language, and system management tools, that preserves central control of access policy while reducing or eliminating any dependency on topology.
- Phoenix's Adaptive Firewall Technology [17], as noted above, provides self-adapting control of network access, thus establishing an effective network security policy by examining every packet and adapting rules "on-the-fly" based on information in the packet passing through the network interface.
- FORE Systems' Firewall Switching Agent [8], in combination with Check Point's Firewall-1 [5], provides 20 Gbps of firewall switching bandwidth while delivering wire-speed routing, switching, and class-of-service delivery.
- OMG's [15] CORBA Firewall Security [13], which brings firewalls to distributed object technology and provides a standard approach by which a firewall identifies and controls the flow of IIOP (Internet Inter-ORB Protocol), which has become the defacto standard interoperability protocol for Internet, providing "out-of-the-box" interoperation with ORBs (Object Request Brokers), thereby increasing the security of CORBA-based applications [1].

These trends in the development of firewalls make them important mechanisms to ease the transition to flexible and truly distributed security solutions, such as CORBA Security Services [14], thus sparing traditionally-minded network/firewall administrators much discomfort. After all, the laboratory test results described in "Super firewalls" [12] show that today's high-end firewalls are tougher, faster, and easier to use.

5 Conclusions

Notwithstanding the limitations of firewalls and the fact that they are neither the panacea of every security aspect of a network, nor the sole sufficient bulwark against network intrusion, and despite development trends that threaten them, they are still a powerful protective mechanism, and will continue to play an important and central role in the maintenance of network security for some years yet, and any organisation that ignores them does so at its peril.

They continue to change and develop, and new features are regularly added as the need arises. If developments follow the present trend, they will continue to combine configurable access control and authentication mechanisms with their traditional functions, thus providing more powerful and flexible protection for networks to make them secure.

References

1. H. Abie, CORBA Firewall Security: Increasing the Security of CORBA Applications, Telektronikk Volume 96 No. 3-2000, pp. 53-64, January 2000
2. F. M. Avolio, Firewalls: Are We Asking Too Much?, http://www.crossnodes.com/icsa/perimeter.html
3. S. M. Bellovin, Distributed Firewalls, ";login:" November 1999, Special Issue on Security, ISSN 1044-6397, Also at: http://www.usenix.org/
4. D. B. Chapman and E. D. Zwicky, Building Internet Firewalls, O'Reilly & Associates, Inc., November 1995.
5. Check Point Firewall-1, version 3.0 White Paper, June 1997. http://www.checkpoint.com/products/whitepapers/wp30.pdf
6. W. R. Cheswick and S. M. Bellovin, Firewalls and Internet Security, Repelling the Wily Hacker, Addison-Wesley Publishing Company, 1994
7. G. Dalton, Acceptable Risks, a survey by PricewaterhouseCoopers and InformationWeek, August 31, 1998, http://www.informationweek.com/698/98iursk.htm
8. FORE Systems, Firewall Switching Agent White Paper, October 1998.
9. C. Fulmer, Firewall Product Overview, December 30, 1999, http://www.waterw.com/~manowar/vendor.html
10. ICSA, ICSA Firewall Policy Guide V2.00, Security White Paper series, http://www.icsa.net/services/consortia/firewalls/fwpg.shtml
11. T. Moran, Fight Fire with Firewalls, Microsoft Corporation, July 27, 1998, http://msdn.microsoft.com/workshop/server/proxy/server072798.asp
12. D. Newman, Super Firewalls, Data Communications, Lab Tests, May 21, 1999, http://www.data.com/
13. OMG, Joint Revised Submission, CORBA/Firewall Security+Errata, OMG Document, ftp://ftp.omg.org/pub/docs/orbos/98-07-03.pdf, July 6, 1998
14. OMG, The CORBA Security Service Specification (Revision 1.2), ftp://ftp.omg.org/pub/docs/ptc/98-01-02.pdf, January 1998
15. OMG, The Object Management Group, http://www.omg.org/
16. J. L. Phipps, Hackers: Can You Stop Them?, PricewaterhouseCoopers and Information Week, http://www.mediainfo.com:81/ephome/news/newshtm/minfocom/1198a.htm

17. Phonex Adaptive Firewall Technology, Multi-Layer Stateful Inspection White Paper, Progressive Systems, Inc., http://www.progressive-systems.com

18. R. Schreiner, CORBA Firewall White Papers, TechnoSec Ltd., 1998 http://www.technosec.com/whitepapers/corba/fw/main.html

19. M. J. Thompson, Corporate Network Security, September 21, 1998, http://www.thestandard.com.au/metrics/display/0,1283,750,00.html

20. Warroom Study: 1996, Security in Cyberspace Hearings before the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs, United States Senate, 104th Congress, 2nd Session. ISBN 0-16-053913-7, http://www.warroomresearch.com/researchcollabor/infosecuritysurvey.htm