



# ***Firewalls – Overview and Best Practices***

---

White Paper

**© Copyright Decipher Information Systems, 2005. All rights reserved.**

The information in this publication is furnished for information use only, does not constitute a commitment from Decipher Information Systems of any features or functions discussed and is subject to change without notice. Decipher Information Systems assumes no responsibility or liability for any errors or inaccuracies that may appear in this publication.

Last revised: June 2006

## Table of Contents

Table of Contents.....	3
Firewalls – Overview and Best Practices.....	4
Abstract.....	4
Hardware vs. Software Firewalls.....	4
Implementation – Things to Consider.....	7
Configuring Access Rules.....	9
Firewall Logs and Auditing.....	10
Summary.....	12

# Firewalls – Overview and Best Practices

## Abstract

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.

## Hardware vs. Software Firewalls

There are two basic types of firewalls: hardware and software. Each has its own advantages and disadvantages. Hardware firewalls are exactly what the name implies; a hardware device that is placed somewhere in the traffic flow of an organization's network. Once in place, the device receives and analyzes packets traveling into and out of the network. The device then checks a list of previously specified access rules to see if it should allow the packet to continue to its destination, or if the packet should be discarded. There are a number of advantages to using hardware firewalls. The devices do not depend on common operating systems, such as Microsoft Windows or Linux, so they are immune to the seemingly infinite number of bugs, viruses, and other malicious attacks that those operating systems suffer from. Hardware firewalls also perform much

better (faster) than a software based solution, and are much more scalable – additional devices can be added as needed with relative ease. Performance should be one of the main considerations when selecting a firewall solution due to the fact that all network traffic traveling into and out of the organization’s network will pass through the device and it takes time and processing overhead to analyze each packet to determine what needs to be done with it. Another advantage is that hardware firewalls only perform firewall-related duties and are not burdened with other tasks. This type of single-purpose functionality allows these hardware devices to perform their designed tasks much more effectively than a multi-function software based solution. Counter to the advantages, hardware firewalls also suffer from a number of disadvantages. For example, if the device goes down, all inbound and outbound network traffic stops, which can be operationally unacceptable to an organization. Also, because of their proprietary nature, hardware firewalls require specialized knowledge to install, configure, and administer effectively. Finally, the financial costs of hardware based solutions are fairly high due to initial acquisition as well as the previously mentioned specialized administrative resources required to operate them.

Software based firewalls are installed on an existing device, such as a workstation or server. These applications perform the same tasks as hardware based solutions, namely analyzing network packets to determine whether or not they should be allowed to continue to their intended destination. Software based solutions are usually less expensive to acquire, and there are actually a number of free firewall applications available to download. However, the principle of you get what you pay for certainly applies here. Free solutions do not offer the comprehensive features of more expensive applications.

Additionally, technical support is not readily available, and the overall effectiveness of free firewalls is suspect enough to where they should not even be considered except for personal use or protecting marginally important resources. One major problem with software based firewalls is that, since they are installed on an existing operating system, they are susceptible to the same viruses and malicious attacks as their host machine, thereby increasing the likelihood that the firewall can be disabled or otherwise rendered useless in the event of an attack. Also, one must ensure that the host system has enough hardware resources (CPU and memory) available for the firewall to operate effectively. If those resources are insufficient, the firewall will perform poorly, and network throughput will suffer. Finally, another disadvantage of software firewalls is that not only do the network administrators have to worry about keeping the firewall software updated and properly patched, but the operating system the solution is installed on must be diligently ‘hardened’ and patched as well. Table 1-1 summarizes the hardware and software firewall comparison:

Table 1-1

	<b>Advantages</b>	<b>Disadvantages</b>
<b>Hardware Firewall</b>	<ul style="list-style-type: none"> <li>Operating system independent</li> <li>Not vulnerable to malicious attacks</li> <li>Better performance</li> <li>Focuses on only firewall-related duties</li> </ul>	<ul style="list-style-type: none"> <li>Can be single point of failure</li> <li>Higher administrative overhead</li> <li>Higher cost to implement and maintain</li> </ul>
<b>Software Firewall</b>	<ul style="list-style-type: none"> <li>Less expensive to implement and maintain</li> <li>Lower administrative overhead</li> </ul>	<ul style="list-style-type: none"> <li>Dependent upon host operating system</li> <li>Requires additional host hardware</li> <li>Vulnerable to malicious attacks</li> <li>Lower performance</li> </ul>

It is recommended to implement a firewall solution that actually combines hardware and software based firewalls. The hardware devices can be placed at strategic locations throughout the network, and would be the primary defense against malicious attacks from outside the organization's network. To compliment the security of the hardware devices, software based solutions should be installed on important systems, or on all systems if budget permits, as a last line of defense in the event that the hardware firewalls either failed to detect the attack, or if an attack is accidentally launched from within the organization.

## **Implementation – Things to Consider**

In addition to choosing what type of firewall to implement, there are a number of other things to consider when implementing a solution. One must first consider where to physically place the firewall or firewalls. If only one firewall is being considered, it should ideally be placed between the Internet and the organization's DMZ. However, a more secure solution is to have one firewall between the Internet and DMZ, and a second firewall between the DMZ and the internal network. If necessary, additional firewalls can be placed at strategic locations within the organization's LAN. These additional devices should be considered if malicious attacks from within the organization are a concern. Another consideration is whether to use stateless or stateful packet filtering. Stateless packet filtering uses information in the protocol header of a packet to determine if it should allow or block that packet from continuing to its destination. This type of filtering is usually done via IP header, ports and socket numbers, or the number of ACK (acknowledge) bits contained within the packet. The main advantage to stateless filtering is cost; most firewalls using this filtering are relatively inexpensive or free. There are,

however, major disadvantages to stateless packet filtering. They are unable to filter attacks from a computer that has not already have a connection in place, which means that a firewall using stateless filtering is susceptible to IP spoofing attacks and denial of service attacks. Also, stateless filtering means that each packet is examined individually, which results in poorer performance versus a firewall using stateful filtering. Firewalls that use stateful packet filtering are more intelligent than those using stateless filtering. They maintain a state table that keeps a record of connections that devices have made with each other. When a connection is first initiated, stateless filtering is used; the firewall analyzes all packets traveling between the devices. This information is added to the state table, and any subsequent packets with the same configuration are no longer scrutinized. This allows for more a more efficient flow of network traffic.

The implementation and configuration of the firewall solution should be closely based upon an organization's security policy, which ultimately determines what internal users should and should not have access to. A section dedicated to the firewall should be added to the security policy. Adhering to these pre-defined policies will help ensure that the desired Quality of Service (QoS) is maintained for the organization. If the firewall is configured in a manner that is counter to the specifications of the security policy, the danger exists that the organization will not be able to function effectively once the firewall(s) have been activated.

As important as it is to know what a firewall does, it is just as important to understand what a firewall *does not* do. Firewalls are not a single solution for an organization's security needs. They cannot protect an organization from malicious attacks originating from inside the organization. Also, without an effective security policy and an

overall dedication to security, the benefits from even the best firewall solution will unfortunately be minimal. To maximize network security, it is recommended that a firewall should be combined with antivirus software, intrusion detection systems (IDS), and end-user education.

## Configuring Access Rules

Once the firewall has been installed and basic configuration is complete, a set of access rules will need to be configured. These rules will determine what network traffic the firewall will allow either into or out of the organization's network, and what traffic will not be allowed. The rules should adhere to the following six guidelines:

<b>Firewall Access Rules to Live By</b>
1. The network administrator should be able to communicate directly with the firewall.
2. The firewall should not be able to communicate directly with any other device.
3. No other device should be able to communicate directly with the firewall.
4. Other network traffic should be routed directly to the appropriate servers.
5. All outbound communications should be allowed - unless corporate policy dictates otherwise.
6. The last rule should deny entry to any packet that does not match any other rule.

In addition to these basic guidelines there are other points to consider. Each rule that a firewall has to analyze results in additional processing overhead. This means that the more rules a firewall has, the longer it will take for the firewall to determine whether or not the packet in question may pass through. Therefore, it is best to limit the number of rules to no more than 30-50. However, for best performance, less than 25 rules are recommended. Also, firewalls process their rule base from the top down. As soon as the

firewall finds a rule that applies to a particular packet, the rule is applied and the packet is processed (either allowed to continue or dropped). It is recommended that the most important and most utilized rules should be at the top of the rule list. This prevents the firewall from having to process through a number of rarely used rules to finally get to rules that apply to the majority of the network traffic. Determining the correct order of rules for a particular implementation is an ongoing process. Initially, there is a significant amount of testing and trial-and-error involved in determining the correct order that the rules should be in. Also, the rule base should be reviewed periodically to see if the organization's requirements or network usage has changed that would require the reordering of existing rules as well as adding or removing rules. Finally, one should make sure to keep the number of domain objects in the rule base to a minimum, and also make sure that these objects are kept towards the bottom of the rule base list.

## **Firewall Logs and Auditing**

The initial implementation of a firewall is only the beginning of continuous monitoring and maintenance process. Two major tasks that need to be conducted on an ongoing basis are logging and auditing of the firewall. One of the first considerations should be what should be logged. As with too many rules in the rule base, enabling too much logging can significantly degrade firewall performance. Many firewalls by default limit logging events to those affected by Deny actions, which is recommended for most implementations. Log files should be reviewed regularly for unusual activity and to determine the effectiveness of the existing rule base. Since these log files need to be screened manually, it is best to present them in the most user-friendly form as possible. Less sophisticated firewalls their log file in plain text formats, which should be imported

into a separate reporting application for ease of use. More expensive and sophisticated firewalls come with integrated reporting capabilities that allow for logging information to be displayed in a multitude of formats and search criteria. There are many different approaches that can be taken when working with log files, but there are five main steps for working with log files that should be applied regardless of what firewall solution is in place:

### **5 Steps of Firewall Logging**

1. Activate logging on the firewall and review the summary of recent events.
2. Generate reports from the raw data.
3. Analyze the report and identify any potential issues.
4. Modify the firewall's access rules to address the issues identified in Step 3.
5. After any changes have been made, review the log files again to ensure that the changes achieved the desired results.

One final aspect of logging that one should keep in mind is the storage of the log files. Log files can, even when in plain text format, grow to be quite large in a very short period of time. Making sure sufficient disk space is available and limiting the amount of logging will aid in preventing the log file sizes from becoming unmanageable.

Another important item to include in the ongoing management of a firewall is auditing, which is beneficial in determine the actual strength and effectiveness of the security measures implemented at an organization. One method of auditing is using internal or external in an attempt to penetrate and compromise the network's defenses. Another method of auditing is keeping track of certain key events that take place on the network, such as user login activity, file access and deletions, and ensuring that old user

accounts are disabled or deleted. External auditors should also be employed to review the effectiveness of the security measures from a perspective independent from the organization. Additionally, security procedures and the associated security policy should also be reviewed at regular intervals. External auditors can prove to be extremely helpful in locating potential vulnerabilities that would otherwise have remained undetected.

## **Summary**

This white paper provided an overview of the different firewall types, their recommended usage, as well as best practices both the initial installation and ongoing administration of a firewall infrastructure. We hope this information will help you in your organization's firewall selection, or if you have already implemented firewalls, has proven helpful in effectively configuring them.