

WHITEPAPER

Choosing firewalls

Author: MH
October 2002
V1.1

Table of Contents

1	FIREWALLS	2
2	TYPES OF FIREWALL	2
2.1.1	Software.....	2
2.1.2	Appliance.....	2
2.2	STATEFUL INSPECTION FIREWALLS	4
2.2.1	What is Stateful Inspection	4
2.2.2	How it Works	4
2.2.3	Rule processing	4
2.2.4	Advantages.....	4
2.2.5	Disadvantages.....	5
2.3	APPLICATION PROXY FIREWALL	6
2.3.1	What is Application Proxy	6
2.3.2	How it works.....	6
2.3.3	Rule Processing	6
2.3.4	Advantages.....	7
2.3.5	Disadvantages.....	7
2.4	WHICH FIREWALL DO I USE?.....	8
2.4.1	Proxy vs. Stateful.....	8
2.4.2	Software vs. appliance	8
2.4.3	Priorities	9

1 Firewalls

In today's world most organisations are conducting some type of business activity on the Internet. This may be as simple as sending emails or browsing some web pages, to earning revenue of internet activities through e-commerce. In all cases Firewalls are the first line of defence for anyone connected to the internet. The firewall may range from a simple piece of software on a laptop (personal firewall) to fully redundant, load balancing behemoths that have to function at high speed to cope with the demands placed on them.

There are different types of firewalls and there are a number of them on the market. So which one is appropriate to your needs? This document aims to answer some of those questions and allow you to select a firewall which is appropriate to your requirements.

2 Types of firewall

Traditionally firewalls were defined in generations.

- **Generation 1 Packet filtering firewall** – This type of firewall determines if access is permitted based on the source and destination. Today this is most commonly implemented in routers using Access Control Lists.
- **Generation 2 Application Level Firewalls** – An application firewall inspects the traffic at the highest level. It inspects each piece of traffic by taking it apart, examining the source, destination and contents before putting it back together again and passing it on if it is allowed.
- **Generation 3 Stateful inspection firewalls** – These types of firewalls inspected the source, destination, and some content as well as the state. Ie. Did it originate from our environment?

Most firewalls today combine the above "generations" to provide a more comprehensive solution, these are generally called hybrids. They however tend to be categorised by their main feature, either stateful or application (proxy) firewalls. Packet filters provide some protection, but are generally considered to be insufficient for most firewall requirements.

2.1.1 Software

Software firewalls are those that are installed on a particular operating system such as Windows, Unix (Linux, Solaris, AIX, HP, Tru64) and even proprietary platforms. Many harden the operating system by removing unnecessary functionality and by adding processes that maintain security at a certain level.

The advantage of these types of firewalls is that they are upgradeable and the hardware can be changed according to your requirements without impacting licensing.

The disadvantage is that you have to purchase the hardware and you have to maintain the skills to manage the underlying operating system.

2.1.2 Appliance

A firewall appliance is a piece of purpose built hardware which has a firewall installed on it. Typically these types of appliances are purpose built "PC's" that run a cut down operating system such as Linux and have the firewall software preinstalled. A second type of appliance uses an application specific integrated circuit (ASIC) chip. Many

Choosing Firewalls

firewall functions are performed on the chip and some software is provided to manage the firewall and extend its capabilities.

The advantage of appliances is that you do not have to purchase nor manage an operating system.

The disadvantage is that once you have purchased it there is limited scope to upgrade the firewall. While software can be upgraded the hardware often cannot be. You therefore have to make sure that the firewall is sized correctly as generally the only hardware upgrade path is to purchase a new one.

2.2 Stateful Inspection Firewalls

Some stateful inspection firewalls are:

- Firewall-1,
- Netscreen,
- PIX,
- Netfilter,
- Watchguard.

2.2.1 What is Stateful Inspection

Stateful inspection is a technique used to determine if traffic should be permitted or not. The traffic is inspected so not only are the source and destination determined, to some extent the contents are examined. Details of the traffic are placed in a state table and this table is used to make decisions on future traffic from the same source and destination.

2.2.2 How it Works

When a stateful inspection firewall receives traffic (packets) it collects information on the packet such as described above. This information is placed in a state table.

When another packet is intercepted by the firewall, its characteristics are compared to the details in the state table. If they match, then it is allowed through. If they do not match then rules are processed in order to determine if it should be allowed through.

2.2.3 Rule processing

Firewalls control traffic through rules. Stateful inspection firewalls process rules in order. In other words they start with rule number one. If it does not match they go on to rule number two, etc until they have a match. Once they have a match no further rules are processed.

This type of processing means that you have to make sure that a rule you implement does not invalidate a rule further down or vice versa.

2.2.4 Advantages

- Stateful Inspection firewalls may offer much higher performance than proxies.
- Stateful Inspection ensures that all packets must be part of an authorized communication session. Therefore, a high level of protection is provided to users communicating with systems external to the "Trusted" network.
- Stateful Inspection provides a greater level of security control by enforcing security policies at the "application socket" or port layer as well as the protocol and address level.

2.2.5 Disadvantages

- State Tables may provide more complexity, because of the need to keep dynamic state tables and remember connections. This opens the door to a variety of Denial of Service Attacks (DOS)
- There are several types of attacks that are aimed at flooding the state table with bogus information. When the state table is saturated, it can either freeze the device or cause it to reboot. As a result of this the device loses the information on all connections and will start denying legitimate packets.
- It may not be stateful for all protocols used. Those not statefully inspected may be passed through with minimal controls.

2.3 Application Proxy Firewall

Some application proxy firewalls are:

- Symantec Enterprise Firewall (previously known as Raptor)
- Cyberguard
- Gauntlet

2.3.1 What is Application Proxy

An Application Proxy is a software program or device that makes software requests on behalf of another device on the network. An application proxy firewall evaluates network packets for valid data at the application layer before allowing a connection. In an application level firewall, a set of application-specific security proxies evaluates all attempts to pass data into or out of the protected network.

2.3.2 How it works

This type of firewall examines the data in all network packets at the application layer and maintains complete connection state and sequencing information (which packet arrived when).

A proxy stands between a trusted and untrusted source and actually makes the connection, each way, on behalf of the source. They make a copy of each accepted packet before transmitting it. They also repackage the packet to hide the packets true origin. The firewall receives an incoming connection, determines whether it is allowed, and creates a corresponding connection with the intended computer. It rewrites the source and destination information of the connection to keep information about your network secret. Therefore, for application level traffic, there are always two TCP or UDP connections, one between the firewall and the source, and another between the firewall and the destination.

2.3.3 Rule Processing

Application proxy firewalls generally process rules differently to other firewalls. They create a unique identifier for each rule. When a packet arrives at the firewall certain information is taken from the packet, a unique identifier is created and this is compared against the list of identifiers created for the rules. If the traffic is permitted it is handed on to the proxy who then performs more checks on the actual content of the traffic.

This type of processing means that the most appropriate rule for a particular piece of traffic will be applied and it is more difficult to mis-configure rules.

2.3.4 Advantages

- Looks at the information within the packet all the way up to the application layer.
- Is aware of protocols, services and commands being used.
- Can provide a high level of protection against "Denial of Service" attacks against the firewall.
- Can allow or deny traffic based on the content of the payload (for example, deny bad http requests, only allow certain commands to be used when using FTP)

2.3.5 Disadvantages

- Proxies must be written for specific application programs, and not all applications have proxies available.
- May degrade traffic performance.
- Breaks client server model which is good for security but at times bad for functionality.

2.4 Which firewall do I use?

The choice of which firewall to use may not be straight forward. There are a few things that you should keep in mind:

- What am I protecting?
- What is the value of what I'm protecting?
- What level of protection will I need?
- What services will be provided by the vendor organisation?
- What functionality is required on the firewall
- What is the cost of:
 - Purchase,
 - Annual maintenance
 - Hardware
 - Management costs

These are just some of the factors to keep in mind when deciding on a firewall to purchase.

2.4.1 Proxy vs. Stateful

A proxy firewall is generally accepted as providing a marginally higher level of security as it has more control over traffic. It takes it apart, examines it, recreates it and then passes it on. At no stage does it pass the traffic directly without intervention. For those protocols it has proxies for, it will be able to allow/deny certain commands, look for strings in the traffic, etc.

However proxies do apply the letter of the law as specified in the RFC's¹. This means that traffic which violates the RFC will be denied. This could impact propriety applications.

For those protocols that the firewall does not have a specific proxy, it will use a generic proxy or plug. This plug applies some controls but not at the same level as a protocol specific proxy.

Stateful inspection firewalls will be slightly faster and provide a high level of security for the statefully protected protocols. Like the application proxy firewall it will use different techniques for those protocols that are not statefully protected.

2.4.2 Software vs. appliance

When you purchase an appliance you pay one price for the software and the hardware (both proxy and stateful inspection firewalls are available as an appliance). This can mean that the initial capital outlay will be less than when purchasing a software firewall. However keep in mind that you are usually not able to increase the capacity of the firewall without purchasing a new firewall. It is therefore essential that you allow for growth when making the initial purchase.

The system is usually a "black box" and the operating system is locked away from the administrator, no operating system maintenance is possible and generally not needed.

¹ RFC – Request For Comment. These documents are publications on the internet that specify how protocols should handle events. In other words when an error occurs what happens, when to a connection is made what happens.

Choosing Firewalls

Software firewalls run on various hardware platforms and operating systems. This allows you to change the underlying hardware to meet your requirements. For example more capacity is needed, add memory, disk space etc. One disadvantage is that operating systems inherently have vulnerabilities and the machine needs to be hardened and maintained. This requires some operating skills, for this reason many site choose as their underlying firewall operating system the one in which they possess the most skills.

2.4.3 Priorities

With all of the above in mind what should you select? The following tables may give you further ideas.

Do you need a VPN?	All commercial firewalls on the market will have IPSEC VPN capabilities. Some features to look out for: <ul style="list-style-type: none">• Are remote clients included?• Does the remote client provide personal firewall capabilities?• Can the remote clients be managed centrally?• Are DES, 3DES and AES supported?
Speed/Throughput	From fastest to slowest: <ul style="list-style-type: none">• ASIC based firewall• Stateful Inspection firewall• Proxy Firewall
Level of protection	<ul style="list-style-type: none">• Most Secure – Proxy firewalls• Very Secure – Stateful firewalls <p>NOTE: it is important to remember that this applies for those protocols that have specific proxies or full stateful inspection. Other mechanisms will be used for remaining protocols.</p>
Features The features provided by the firewall may be a deciding factor. Does it integrate with Authentication product? How is logging provided? How easy or difficult is it to add functionality? What functionality can be added?	<ul style="list-style-type: none">• Software firewalls are generally more feature rich than application firewalls. However some of the leading firewalls provide the same functionality on both platforms.• ASIC Firewalls can only extend features in software and may therefore be limited somewhat.• Appliances can be as feature rich as software firewalls, but features may not be upgradeable.
Environment?	<ul style="list-style-type: none">• Static environment – ASIC/Appliances• Complex – Software Firewall may provide more options