



Interested in learning more about security?

# SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

## Choosing The Best Firewall

Although I only briefly touched on most of the issues involved in choosing a firewall this should be a good starting point for selecting a firewall. The best firewall however is not a product although that does influence the effectiveness of it greatly. It is more a combination of factors. A firewall is only as good as the policy it implements. A firewall should justify its existence in the reduction of impact and/or probability of threats thus reducing risk. A firewall should be active managed ...

Copyright SANS Institute  
Author Retains Full Rights

AD

An advertisement banner for Watchfire. On the left, there is a blurred image of a login form with fields for "login : YZEIF 11" and "password : .....". The central part of the banner is a dark blue rectangle with the text "Others can assess Web applications for vulnerabilities." in white. On the right is the Watchfire logo, which consists of a red flame icon followed by the word "watchfire" in a lowercase, sans-serif font.

Gerhard Cronje

GIAC Level One Security Essentials Practical  
Assignment

Version 1.2b

Choosing The Best Fire wall.

© SANS Institute 2003, Author retains full rights.

## Content

	<b>PAGE</b>
1. Introduction	2
2. IP Basics	2
2.1. IP Attributes	3
2.2. TCP Attributes.	4
2.3. UDP Attributes	4
3. Firewalls – The Basic Description	4
4. Examples	4
4.1. Packet Filters	4
4.2. Application Gateways	5
4.3. Circuit-level Gateways.	5
4.4. State-Full inspection?	5
5. Selecting The Best Firewall?	5
5.1. A firewall implements a security policy.	5
5.2. Draw up your own selection criteria.	6
6. Conclusion	6
7. Sources:	6

## 1. Introduction

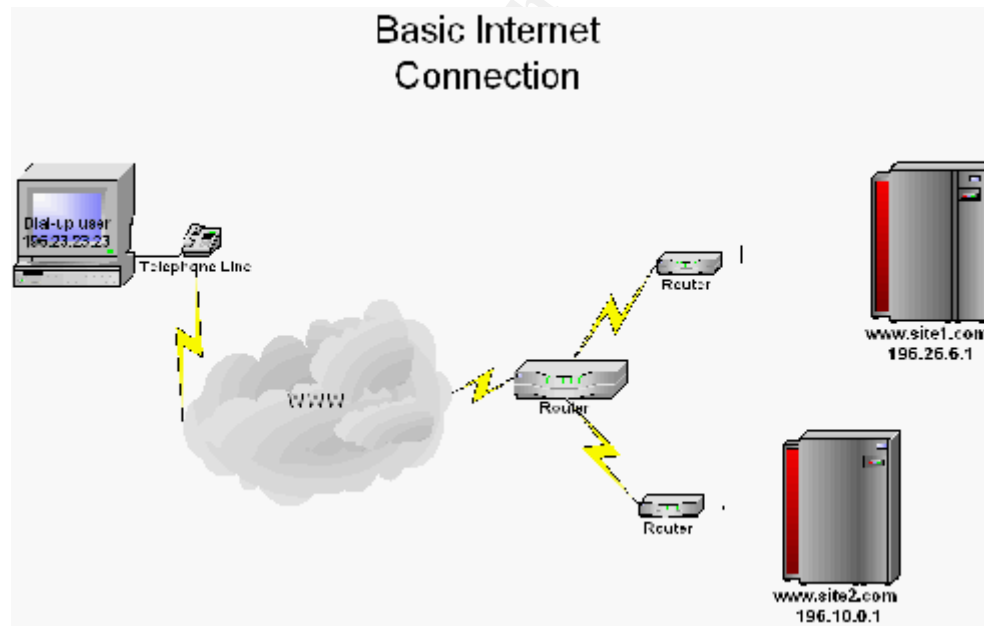
Due to the phenomenal growth of the Internet in the last couple of years companies find it hard to operate without a presence on the Internet. This means that companies are exposed to threats, which can have major business impact, even if a company is just running a web page containing advertisement data. Defacing this site will result in image loss with one's clients, which can translate into financial losses to name an example.

The fact that one needs to protect your company from unauthorized or unwanted access is considered a common fact.

In order to do this the SANS GIAC training teaches the concept of "Defence of Depth". The most common defence device on most networks is a Firewall. It can be a daunting task to pick the right firewall for any organization and this assignment focuses on exactly that issue. In order to pick the right Firewall understanding what a firewall does is crucial. Although this is considered basic knowledge I will quickly cover basic TCP/IP concepts and then move on to picking the right device.

## 2. IP Basics

We will cover a few attributes relating to UDP and TCP to discuss what a firewall does. Just to give a point of reference when briefly discussing the concepts I have included the picture 1.1.



Picture 1.1

### 2.1. IP Attributes

**IP uniquely identifies a host:** This is the main reason for an IP address but this in itself helps us to filter traffic. As Displayed [www.site1.co.za](http://www.site1.co.za) and [www.site2.co.za](http://www.site2.co.za) carries 2 distinct IP addresses.

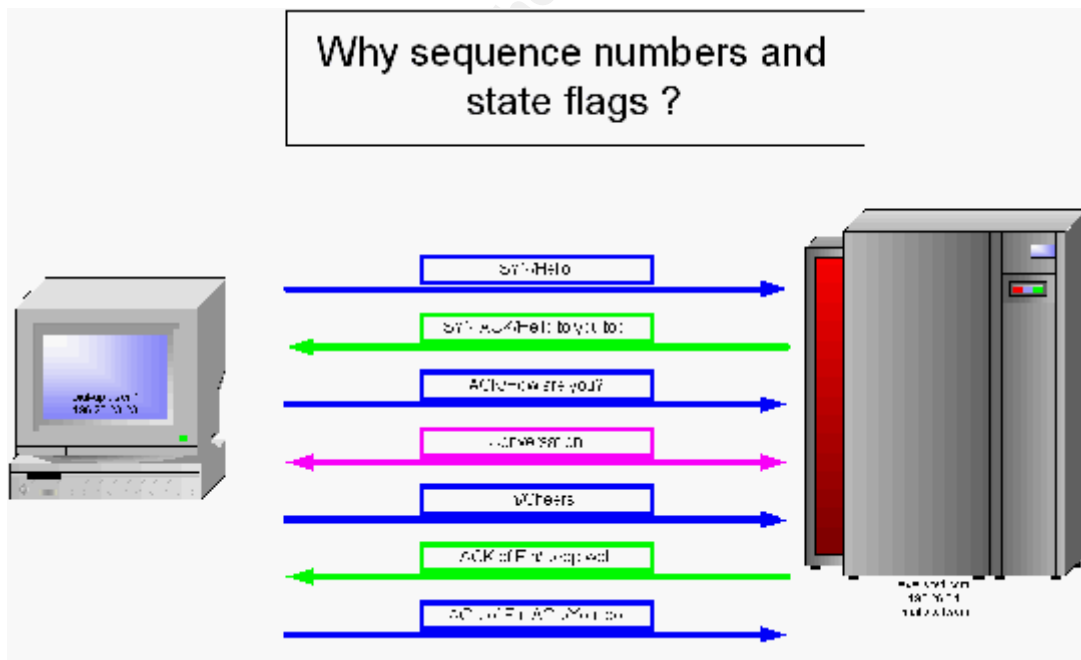
**IP is hierarchal:** This allows us to route IP traffic, which means that a single point of entry exists on most networks, which is why one machine is able to control traffic to and from a network.

22. TCPAttributes.

**TCP runs on top of IP:** Just for point of reference TCP exists on the higher level on the OSI model and deals with session concerns. The reason for nothing this common fact is that more data may be analysed in a TCP packet giving a Firewall more information to filter traffic on.

**A TCP packet contains a port number:** This is the way that a server differentiate between services required. So [www.site1.co.za](http://www.site1.co.za) may double as a mail and web server, listening on port 80 and 25 respectively for connections. A firewall will then only allow connections destined to a port. It is important to note that a source and destination port exists within a TCP packet. The source port allows a client to connect to more than one server or service and then identify which return traffic is related to a connection made. So the dial-up client in picture 1.1 may connect more than once to [www.site1.co.za](http://www.site1.co.za) with a browser and looking at the return traffic from that server based on the port that is in the TCP packet (supplied as source port when connecting) differentiate between connections. Another benefit of a service – or protocol related to a particular port is that a protocol like http on port 80 will have a set of functions or expected functions related to it. This provides a “framework” or reference by which data within a packet may be measured up against to validate the authenticity. An example of this is FTP with a limited amount of commands expected like put, get, bin, prompt and so forth. Any data that does not confirm to this standard can be considered unauthorized and hence blocked by a Firewall.

**A TCP packet contains a sequence number and a FLAG:** These 2 attributes in a TCP packet allows it to both establish and manage a connection. The FLAGS used are briefly depicted in figure 1.2 below, and drawing simple comparison with a telephone conversation one can easily understand this.



Picture 1.2

The sequence numbers in TCP connection provides a method to control and confirm data being sent across a TCP connection. Both sides of the connection will confirm the sequence number up until which data was received. The reason for just pointing out these facts is depicted in the fact that a firewall uses these attributes to monitor a session and filter traffic accordingly. It is important to note that the sequence numbers are also not easily predicted in most instances.

23. UDPAttributes

**UDP runs on top of IP:** As mentioned with TCP, UDP also provides more information by which traffic may be filtered.

**UDP contains a port number:** As with TCP again this data may be used to filter traffic and identify a protocol, providing validation information for a firewall.

**UDP is not state-full:** This means that a UDP packet does not do handshaking or confirmation of packets delivered which meant fewer overheads but also no connection verification. Making it difficult to validate an UDP connection to expected return traffic, which is done by a TCP session. Most firewalls do however try and compensate for this applying timers and expected response rules of its own.

### 3 Firewalls – The Basic Description

Although most firewall documentation presents one with a definition of a firewall. This is what they all seem to have in common.

**A firewall is a perimeter defence device:** This means that any firewall splits a network into a trusted or protected, and un-trusted or unprotected side.

**A firewall filters traffic on a pre-defined set of rules:** Any firewall is only as good as its configuration.

These 2 factors limits the effectiveness of a firewall dramatically and it is important to note that a firewall does not:

- Protect you from internal networks.
- Protect you from authorized malicious access. This entails using granted privileges or access for unintended operations.
- Protect you from all harmful attacks. Exploits found on the Internet can use service ports, which will be allowed through the firewall to an internal server.

### 4. Examples

In most firewall documentation one will find firewalls categorized in the following major groups:

- Packet Filters
- Application Gateways
- Circuit-level Gateways
- State-full inspection?

#### 4.1. Packet Filters

A packet filter monitors the source and destination IP of any connection. It then verifies the destination port of the same connection and then matches it against its configuration to allow or deny a connection. A packet filter does no content checking. This means that no connection is monitored or protocol validated to a set of rules. Can a packet filter be fooled? By spoofing an IP address one can already send unwanted packets into a network but routing remains an obstacle seeing return traffic from such an attack. This may be overcome but requires further factors or access. Port re-writing is another popular method to fool packet filters.

#### 4.2. Application Gateways

An application Gateway allows a connection to be made to the firewall and then initiates a connection on behalf of the user to the server. This means that inherently connection state is maintained and that content can be filtered if the application on the firewall (referred to as a proxy in Gauntlet) is configured to expect only certain traffic. Because an application gateway

connects on behalf of the user this kind of firewall is inherently strong on logging and recording traffic and authentication. As one can gather from the fact that a process is ran for each expected service this type of firewall puts a great amount of load on machine. The performance however of established products like the Gauntlet firewall remains very good. The other downfall of a product is that it is not seamless to the user at all. Applications, routing, browsing and mail needs to point at the firewall or an aliased IP address on the firewall for connections. UDP connections are not handled with ease.

#### 4.3. Circuit-level Gateways.

A circuit-level gateway is a firewall that runs an application that allows connections through it and copies the bytes across for any connection flowing through it, thus creating a circuit. This type of firewall has got it's own strengths in that it does not proxy a connection but rather just monitors a connection through it. This kind of firewall is a lot less seamless. The content checking is limited however for this kind of firewall. This means that a protocol could be further scrutinised and parsed (for instance http commands) to verify validity.

#### 4.4. State-Full inspection?

A couple of manufacturers have combined the concept of proxy-based firewalls and circuit-level gateways with a state-full-firewall. This means that this kind of firewall is seamless to the user if you want it to be.

- It does content checking passing protocols through a validation exercise.
- It keeps a state-table of connections whereby it monitors the state of a TCP connection and allows traffic accordingly.
- It does address translation.
- It can authenticate connections.
- Parses UDP through a set of rules and expected responses.

Examples of these kinds of firewalls include Cisco Pix and Checkpoint Firewall 1. The two examples used can also allow you to configure VPNs (Virtual Private Networks) where data across and un-trusted network can be encrypted.

## 5. Selecting The Best Firewall?

As stated in the document above each kind of firewall has got it's own strong and weak points. The concept of choosing a firewall is unfortunately not only evaluating what the best product is. A couple of principles to consider:

#### 5.1. A firewall implements a security policy.

If you do not have a security policy choosing a firewall is a very hard exercise. If you are doing an emergency implementation where there were no protection previously and the risk needs to be addressed immediately make sure to prioritise the development of such a policy. This does include change control, which is key to firewall management. There should be clear guidelines as to what is allowed and what is not on policy level.

#### 5.2. Draw up your own selection criteria.

Although a firewall implementation should be the last step in a risk-analysis process this is not always the case. What this does imply however is that a selection criteria approved by the appropriate people should be compiled. Depending on the maturity of the organization's security

function this can range from a checklist to developing an architecture including policies and standards.

In any company a major concern is cost. This needs to be balanced with benefit. What this does mean is that the features and protection required should reflect the cost involved. Another criteria will be training. This is a big factor if the firewall will be managed internally. The other option is outsourcing. Support for the product is a big factor in selecting a firewall.

## 6 Conclusion

Although I only briefly touched on most of the issues involved in choosing a firewall this should be a good starting point for selecting a firewall. The best firewall however is not a product although that does influence the effectiveness of it greatly. It is more a combination of factors. A firewall is only as good as the policy it implements. A firewall should justify its existence in the reduction of impact and/or probability of threats thus reducing risk. A firewall should be actively managed and reviewed. A combination of firewalls can also be implemented.

So, to try and put that in one sentence.

The best firewall balances functionality, risk reduction and cost in a well-managed fashion as a tool that implements a security policy along with other devices applying the concept of "Defence in Depth".

## 7 Sources:

1. SOS Corporation. "An Introduction to Firewalls" 1995 URL: [http://www.soscorp.com/products/BS\\_FireIntro.html#Firewall\\_types](http://www.soscorp.com/products/BS_FireIntro.html#Firewall_types)
2. Curtin, Matt and Ranum, Marcus J. "Internet Firewalls: Frequently Asked Questions" December 1, 2000 URL: <http://www.interhack.net/pubs/fwfaq/>
3. Goncalves, Marcus. Firewalls Complete : The McGraw-Hill Companies, 1998.
4. Roble Systems Consulting. "Firewall Comparison: Checkpoint Firewall -1 and Cisco PIX" 1999. URL: [http://www.robles.com/docs/fw1\\_or\\_pix.html](http://www.robles.com/docs/fw1_or_pix.html)
5. Grennan, Mark. "Firewall and Proxy Server HOWTO" August 21, 2000 URL: <http://www.grennan.com/Firewall-HOWTO.html>
6. Pullin, Adrian J. "Internet Security and Firewalls" Date unknown. URL: <http://www.newi.ac.uk/pullina/firewall/index.htm>



# Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS SOS London 2009	London, United Kingdom	Jul 13, 2009 - Jul 18, 2009	Live Event
SANS Future Visions 2009 Tokyo	Tokyo, Japan	Jul 15, 2009 - Jul 17, 2009	Live Event
SANS IMPACT 2009	Kuala Lumpur, Malaysia	Jul 27, 2009 - Aug 01, 2009	Live Event
SANS SEC563: Mobile Device Forensics Debut	Baltimore, MD	Jul 27, 2009 - Jul 31, 2009	Live Event
SANS Boston 2009	Boston, MA	Aug 02, 2009 - Aug 09, 2009	Live Event
SANS WhatWorks in Virtualization and Cloud Computing Security Summit 2009	Washington, DC	Aug 17, 2009 - Aug 21, 2009	Live Event
SANS Atlanta 2009	Atlanta, GA	Aug 17, 2009 - Aug 28, 2009	Live Event
SANS Virginia Beach 2009	Virginia Beach, VA	Aug 28, 2009 - Sep 04, 2009	Live Event
SANS SCDP SEC556: Comprehensive Packet Analysis - Sept. 2009	Ottawa, ON	Sep 09, 2009 - Sep 10, 2009	Live Event
SANS Critical Infrastructure Protection at Oceania CACS2009	Canberra, Australia	Sep 10, 2009 - Sep 11, 2009	Live Event
SANS Network Security 2009	San Diego, CA	Sep 14, 2009 - Sep 22, 2009	Live Event
SANS SCDP Cutting Edge Hacking Techniques - June 2009	Ottawa, ON	Sep 15, 2009 - Sep 15, 2009	Live Event
SANS Rocky Mountain 2009	OnlineCO	Jul 07, 2009 - Jul 13, 2009	Live Event
SANS OnDemand	Books & MP3s Only	Anytime	Self Paced