Firewall

Research · October 2015

DOI: 10.13140/RG.2.1.1622.7289

Ahmed Elnaggar
Information Technology Institute

معهد الدراسات العليا والبحوث
جامعة الاسكندرية

Firewall

2nd Assignmen Web Technology.

Department of Information Technology,
Institute of Graduate Studies and Research,
University of Alexandria,Egypt.

Presented by:

Ahmed Atef Elnaggar

Supervisor:

Prof . Ahmed M. Elfatatry

Abstract

If you have been using the Internet for any length of time, and especially if you work at a larger company and browse the Web while you are at work, you have probably heard the term firewall used. You can use a firewall to protect your home network, computers and personal information from offensive Web sites and potential hackers.

Contents:

Kindly find the attached softcopy of report.

1- Introduction

Basically, a firewall is a barrier to keep destructive forces away from your property. In fact, that's why its called a firewall. Its job is similar to a physical firewall that keeps a fire from spreading from one area to the next.

In this report, we will cover the main points about :

What are firewalls and its types?

How do firewalls work?

What techniques do firewalls use?

What is a proxy?

Figure 1

2- History

Firewall technology emerged in the late 1980s when the Internet was a fairly new technology in terms of its global use and connectivity. A network's firewall builds a bridge between an internal network that is assumed to be secure and trusted, and another network, usually an external network, such as the Internet, that is not assumed to be secure and trusted.

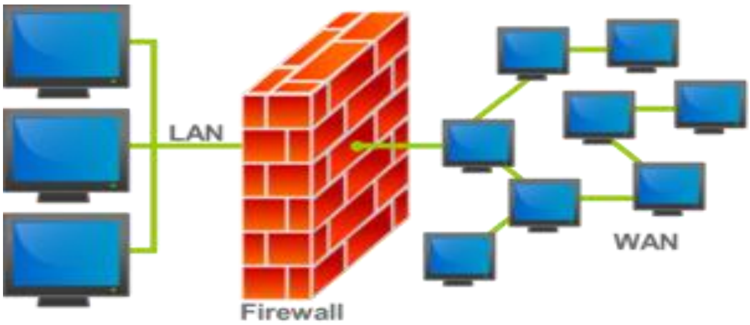


Figure 2

3- Types of firewall

A firewall can either be software-based (ex: AVG-Zone Alert- ISA –TMG) or hardware-based (ex: Cisco-JUNIPER) and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set.

Many personal computer operating systems include software-based firewalls to protect against threats from the public Internet.

4- Techniques of firewall

There are different Techniques of firewalls depending on where the communication is taking place, where the communication is intercepted and the state that is being traced.

4. A- Network layer: Network layer firewalls generally fall into two sub-categories, stateful and stateless.

♦ *First generation packet filters "stateless".*

Packet filters act by inspecting the "packets" which transfer between computers on the Internet. If a packet matches the packet filter's set of rules, the packet filter will drop (silently discard) the packet, or reject it (discard it, and send "error responses" to the source).Packet filtering firewalls work mainly on the first three layers of the OSI reference model, which means most of the work is done between the network and physical layers, with a little bit of peeking into the transport layer to figure out source and destination port numbers.

For example, if a rule in the firewall exists to block telnet access, then the firewall will block the TCP protocol for port number 23.

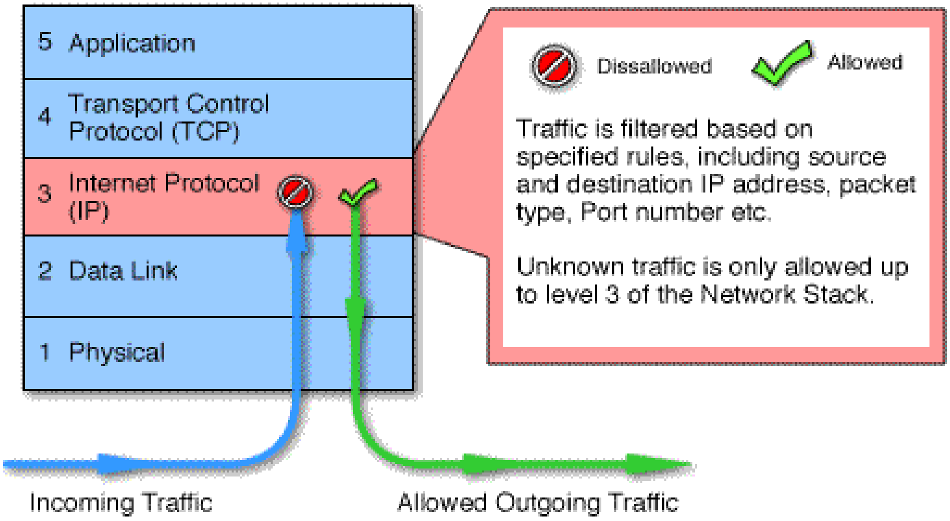

5 Application
4 Transport Control Protocol (TCP)
3 Internet Protocol (IP)
2 Data Link
1 Physical
Dissallowed
Allowed
Traffic is filtered based on specified rules, including source and destination IP address, packet type, Port number etc.
Unknown traffic is only allowed up to level 3 of the Network Stack.
Incoming Traffic
Allowed Outgoing Traffic

Figure 3

♦ *Second generation: filters circuit level "stateful".*

Second-generation firewalls perform the work of their first-generation predecessors but operate up to layer 4 (transport layer) of the OSI model. This is achieved by retaining packets until enough are available to make a judgment about its state. Known as stateful packet inspection, it records all connections passing through it and determines whether a packet is the start of a new connection, a part of an existing connection, or not part of any connection. Though static rules are still used, these rules can now contain connection state as one of their test criteria.

Certain denial-of-service attacks bombard the firewall with thousands of fake connection packets in an attempt to overwhelm it by filling its connection state memory.

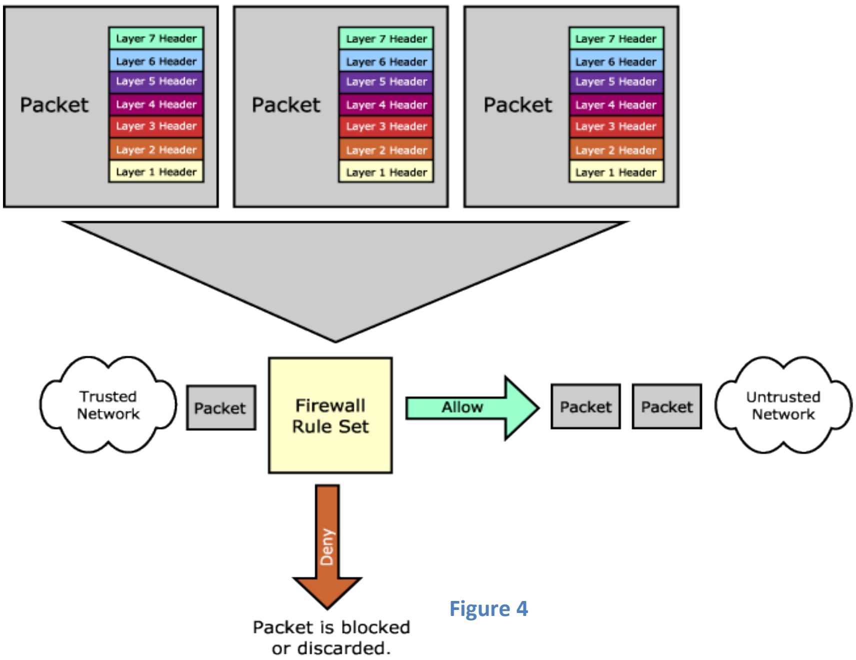


Figure 4

4. B- Application layer firewall (Third generation)

The key benefit of application layer filtering is that it can "understand" certain applications and protocols (such as File Transfer Protocol (FTP), Domain Name System (DNS), or Hypertext Transfer Protocol (HTTP)). This is useful as it is able to detect if an unwanted protocol is attempting to bypass the firewall on an allowed port, or detect if a protocol is being abused in any harmful way. (Usually dropping them without acknowledgment to the sender).

Firewalls can restrict or prevent outright the spread of networked computer worms and Trojans.The additional inspection criteria can add extra latency to the forwarding of packets to their destination.

Another axis of development is about integrating identity of users into Firewall rules. Many firewalls provide such features by binding user identities to IP or MAC addresses, which is very approximate and can be easily turned around.

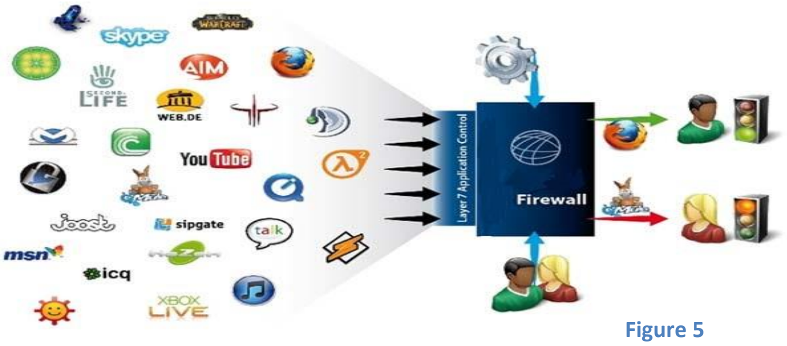
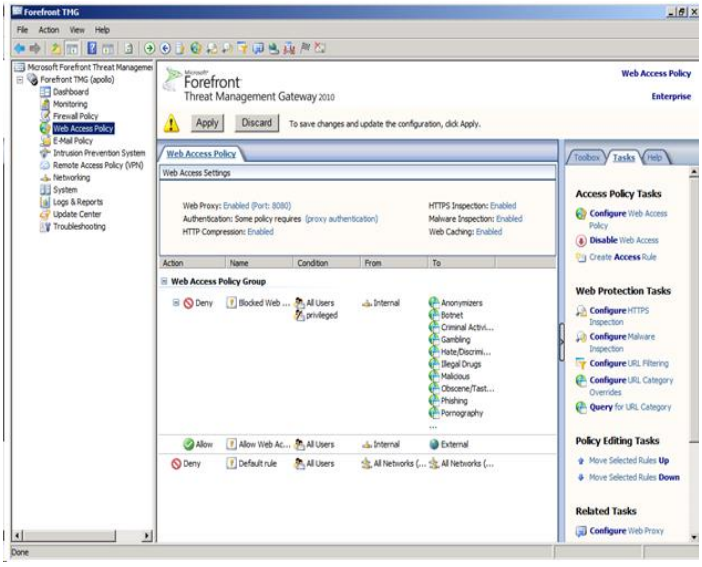


Figure 5

5- *Proxies as a firewall*

A proxy server (running either on dedicated hardware or as software ex: ISA or TMG) may act as a firewall by responding to input packets in the manner of an application, while blocking other packets. A proxy server is a gateway from one network to another for a specific network application.



To save changes and update the configuration, click Apply.

Web Access Settings

Web Proxy: Enabled (Port: 8080)
Authentication: Some policy requires (proxy authentication)
HTTP Compression: Enabled
HTTPS Inspection: Enabled
Malware Inspection: Enabled
Web Caching: Enabled

Action	Name	Condition	From	To
Web Access Policy Group				
Deny	Blocked Web ...	All Users privileged	Internal	Anonymizers Botnet Criminal Activi... Gambling Hate/Discrimi... Illegal Drugs Malicious Obscene/Tast... Phishing Pornography ...
Allow	Allow Web Ac...	All Users	Internal	External
Deny	Default rule	All Users	All Networks (...	All Networks (...

Access Policy Tasks
- Configure Web Access Policy
- Disable Web Access
- Create Access Rule

Web Protection Tasks
- Configure HTTPS Inspection
- Configure Malware Inspection
- Configure URL Filtering
- Configure URL Category Overrides
- Query for URL Category

Policy Editing Tasks
- Move Selected Rules Up
- Move Selected Rules Down

Related Tasks
- Configure Web Proxy

Figure 6

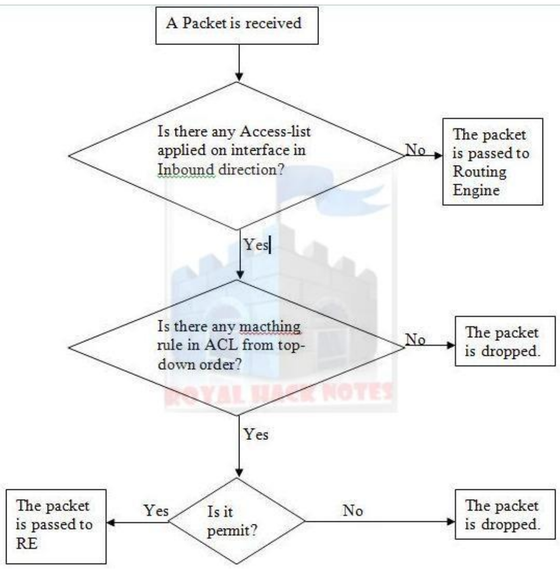

A Packet is received
Is there any Access-list applied on interface in Inbound direction?
No
The packet is passed to Routing Engine
Yes
Is there any macthing rule in ACL from top-down order?
No
The packet is dropped.
Yes
Is it permit?
Yes
The packet is passed to RE
No
The packet is dropped.
ROYAL HACK NOTES

Figure 7

6- Choosing a firewall

What are the most important points to focus on when choosing a firewall?

- A good firewall will ensure the security of ports that can be used to access your system.
- Your system should not just be protected from incoming communications; your firewall should also make sure personal information is not leaving your system unauthorized.
- Your firewall should be monitoring your system for any suspicious behavior.
- A firewall should not be slowing you down. It should not send you any unnecessary notices.

7- Check your firewall

How can I check if my firewall is working?

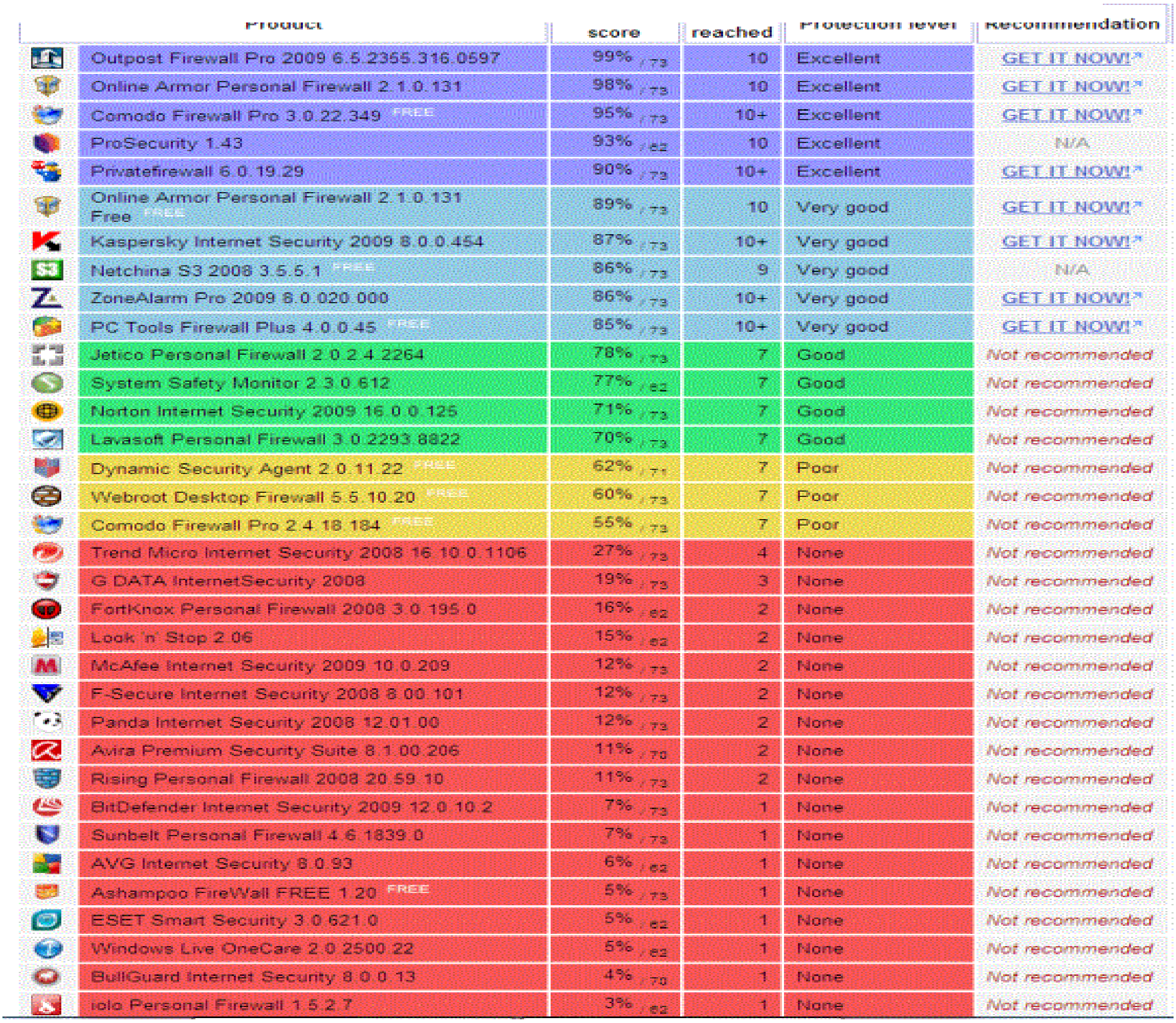
If you would like to check if your firewall is functioning properly you can run what is called a port scan which will check if a connection to any of your system's ports can be established. If so your firewall is not doing what it should be.

8- Conclusion

Stateless firewalls require less memory, and can be faster for simple filters that require less time to filter than to look up a session. They may also be necessary for filtering stateless network protocols that have no concept of a session. However, they cannot make more complex decisions based on what stage communications between hosts have reached.

Modern firewalls can filter traffic based on many packet attributes like source IP address, source port, destination IP address or port, destination service like WWW or FTP. They can filter based on protocols, TTL values, netblock of originator, of the source, and many other attributes. Commonly used packet filters on various versions of UNIX.

Figure 8 Comparison between most common Firewalls



Product	score	reached	Protection level	Recommendation
Outpost Firewall Pro 2009 6.5.2355.316.0597	99% / 73	10	Excellent	GET IT NOW!
Online Armor Personal Firewall 2.1.0.131	98% / 73	10	Excellent	GET IT NOW!
Comodo Firewall Pro 3.0.22.349 FREE	95% / 73	10+	Excellent	GET IT NOW!
ProSecurity 1.43	93% / 62	10	Excellent	N/A
Privatefirewall 6.0.19.29	90% / 73	10+	Excellent	GET IT NOW!
Online Armor Personal Firewall 2.1.0.131 Free FREE	89% / 73	10	Very good	GET IT NOW!
Kaspersky Internet Security 2009 8.0.0.454	87% / 73	10+	Very good	GET IT NOW!
Netchina S3 2008 3.5.5.1 FREE	86% / 73	9	Very good	N/A
ZoneAlarm Pro 2009 8.0.020.000	86% / 73	10+	Very good	GET IT NOW!
PC Tools Firewall Plus 4.0.0.45 FREE	85% / 73	10+	Very good	GET IT NOW!
Jetico Personal Firewall 2.0.2.4.2264	78% / 73	7	Good	Not recommended
System Safety Monitor 2.3.0.612	77% / 62	7	Good	Not recommended
Norton Internet Security 2009 16.0.0.125	71% / 73	7	Good	Not recommended
Lavasoft Personal Firewall 3.0.2293.8822	70% / 73	7	Good	Not recommended
Dynamic Security Agent 2.0.11.22 FREE	62% / 71	7	Poor	Not recommended
Webroot Desktop Firewall 5.5.10.20 FREE	60% / 73	7	Poor	Not recommended
Comodo Firewall Pro 2.4.18.184 FREE	55% / 73	7	Poor	Not recommended
Trend Micro Internet Security 2008 16.10.0.1106	27% / 73	4	None	Not recommended
G DATA InternetSecurity 2008	19% / 73	3	None	Not recommended
FortKnox Personal Firewall 2008 3.0.195.0	16% / 62	2	None	Not recommended
Look 'n' Stop 2.06	15% / 62	2	None	Not recommended
McAfee Internet Security 2009 10.0.209	12% / 73	2	None	Not recommended
F-Secure Internet Security 2008 8.00.101	12% / 73	2	None	Not recommended
Panda Internet Security 2008 12.01.00	12% / 73	2	None	Not recommended
Avira Premium Security Suite 8.1.00.206	11% / 70	2	None	Not recommended
Rising Personal Firewall 2008 20.59.10	11% / 73	2	None	Not recommended
BitDefender Internet Security 2009 12.0.10.2	7% / 73	1	None	Not recommended
Sunbelt Personal Firewall 4.6.1839.0	7% / 73	1	None	Not recommended
AVG Internet Security 8.0.93	6% / 62	1	None	Not recommended
Ashampoo FireWall FREE 1.20 FREE	5% / 73	1	None	Not recommended
ESET Smart Security 3.0.621.0	5% / 62	1	None	Not recommended
Windows Live OneCare 2.0.2500.22	5% / 62	1	None	Not recommended
BullGuard Internet Security 8.0.0.13	4% / 70	1	None	Not recommended
iolo Personal Firewall 1.5.2.7	3% / 62	1	None	Not recommended

9-References

1- Oppliger, Rolf (May 1997). "Internet Security: FIREWALLS and BEYOND". Communications of the ACM 40 (5): 94.

2- http://www.wanredundancy.org/resources/firewall/network-layer-firewall Network Layer Firewall

3- Firewall http://www.tech-faq.com/firewall.html

4- http://en.wikipedia.org/wiki/Firewall_%28computing%29