Evaluation of Firewall Open Source Software

Diogo Sampaio[1] and Jorge Bernardino[1,2]
[1]*Polytechnic of Coimbra, ISEC, Coimbra Institute of Engineering, Rua Pedro Nunes, 3030-199, Coimbra, Portugal*
[2]*CISUC, Centre for Informatics and Systems of University Coimbra, Pinhal de Marrocos 3030-290, Coimbra, Portugal*

Keywords: Computers Systems Security, Open Source Software, Free Software, Firewall, Web Applications Firewall.

Abstract: Computers systems are virtually in every area of our life, but their use has several risks. This is particularly relevant for small business that are beginning to resort in informatics systems for all their activities, and where a breach of security can have catastrophic consequences. Most risks or security vulnerabilities, besides inadverted errors, originates from criminal activity, which anonymously thrives on the Web and can outbreak any organization, mainly for profit but sometimes just for the challenge of doing it. Consequently, creating and managing a security system is often the main form of precaution and it is the solution that guarantees better success rates. In this paper, we are interested in software with a lower financial cost, therefore our focus is in Free and Open Source Software. To this end, the following types of security tools are analyzed: Firewall and Web Applications Firewall (WAF).

1 INTRODUCTION

Securing computers and cyberspace is one of today's grand challenges for science and engineering. However, the use of the Web entails a high number of risks and security threats, and to ensure their feasibility, companies must be able to protect themselves and avoid criminal attacks from hackers with the primary purpose of undermining their business (Osmanbegovic and Zahirovic, 2013). Computers are under continuous threat from attackers who want to steal credit card numbers, intellectual property, and other sensitive information.

Computer security refers to the protection of all components of a computer system that includes hardware, software, firmware and all stored information and data, in order to provide Confidentiality, Integrity and Availability (Razzaq et al., 2013).

It is a great concern that a large proportion of SMEs – Small and Medium Enterprises do not associate computer security as one of their main worries, particularly in the current time of global economic crises. One of the main reasons for the insufficiency or nonexistence of security policy by SMEs is the tight budget that they have, that is often spent on other expenses, mistakenly thought by managers as more important (Tawileh et al., 2007).

This reality takes truly an alarming dimension when a significant percentage of companies, around 45.6%, have already experienced some form of data corruption by cybercrime, with capital losses associated with it (Computer Crime and Security Survey, 2012). Our paper aims not only to draw attention to this problem, but also to offer viable solutions to solve it.

In our work we assume that a first line of defense can be achieved through two types of software: Firewall and Web Applications Firewall. Opting only for free and open source software is, as we will demonstrate, an option with many advantages (Bernardino, 2011), such as the lack of financial costs or the access to the source code, that for example, allows a better integration with complementary software and minor changes that will bring the application to the business needs.

The remainder of this paper is structured as follows. In section 2 we present some computer security background, discussing the importance of a security policy. In section 3, we describe the firewall software systems (Host-based and Web applications). Next, in section 4 we evaluate the software solutions. Finally, the concluding remarks and future work are presented in section 5.

Sampaio, D. and Bernardino, J.
Evaluation of Firewall Open Source Software.
DOI: 10.5220/0006361203560362
In *Proceedings of the 13th International Conference on Web Information Systems and Technologies (WEBIST 2017)*, pages 356-362
ISBN: 978-989-758-246-2

2 COMPUTER SECURITY BACKGROUND

Still a few years ago, companies enclosing their documents in drawers, put padlocks on the doors and installed an alarm on its premises, and that was enough to ensure effective protection of the most important information. But, today most of the company's information resides in computers and with the increasing importance of the Web and the Cloud the security measures mentioned above are completely obsolete and ineffective.

Cybercrimes are now one of the major threats to business endurance. Given this new and growing wave of crime, a new kind of security necessarily had to arise to ensure the protection of digital information and computer systems, usually designated as computer security or IT security.

We assume the definition of computer security as protection of computers, to ensure the ultimate goal of preserving the confidentiality, integrity and availability of information resources, which includes hardware, software, firmware, information and data (Razzaq et al., 2013).

It is important not to confuse computer security with data security. Being data security all the process to ensure confidentiality of information when transmission of this same information between two terminals in a network. Usually cryptography is the most common method.

The volume and sophistication of cybercrimes are increasing and include: scams, data theft, virus, etc. Thousands of infections are being launched and discovered every day, as new attack methods. Hundreds of millions of records have been involved in data breaches. Huge financial losses have been recorded in recent years (Ponemon Institute, 2013). A company unprotected or that does not have the resources to create an efficient security in a few moments may be in bankruptcy (Dowd and McHenry, 1998). The risk of cyber crimes is increasing, and all signs indicate that this growth does not have a tendency to slowdown (Kessel and Allan, 2013).

Users, as is well known, are the weakest link in the computer security layout. Often they assume an inadequate and relaxed attitude, ignoring safety guidelines and taking risk approaches that increase immensely the danger of damage. Moreover the security system is in most cases only based on software, which is not able to anticipate or eliminate every threat. The inability of regular users to understand the various IT terms and notions specifically related to computer security, whether they are related to prevention, as the firewall or threats such as virus, is perhaps the major difficulty. The lack of concern with the risks has also to do with the lack of knowledge of the real hazard (Adele et al., 2012). In this sense, (Liang, 2010) reached to the following conclusions: "…to motivate computer users to avoid IT threats, they need to be convinced that the threats exist and are avoidable. If users fail to see a threat, they will not act to avoid it. If they see the threat but believe it is unavoidable, they will not act to avoid it, either. Thus, both the threat appraisal and the coping appraisal are necessary to motivate security behaviors".

3 FIREWALL

A firewall is a software or hardware-based network security system that controls the incoming and outgoing network traffic based on an applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not secure (Oppliger, 1997). In other words, a firewall is a system designed to prevent unauthorized access to a computer as well as unauthorized outflow of data. Another notion that is important to mention is that firewalls don't decrease the processing speed of computers but optimize it (Garantla and Gemikonakli, 2009), which is against common sense.

There are two basic types of firewalls: hardware-based and software-based. Each has its own advantages and disadvantages. In next sections we analyze firewalls based on software, and focusing on the host-based and Web applications firewalls.

3.1 Host-based Firewall

Firewalls are the cornerstone of computer security and the primarily line to security defenses. However, most types of firewalls requires a detailed understanding of data networking elements, such as routers or switches, as well as a detailed understanding of network protocols.

Host-based firewalls or personal firewalls eliminate most of technical difficulties, since these types of applications are simple and able to ran by any user. These applications are designed to support just a few protocols in order to function. Simplicity makes verification of the rule set simpler as well. The effectiveness of host-based firewall comes for defining a security policy responsible for a single host or machine, like computers or similar, having

the ability to protect the machine even if it is moved from network to network.

Another advantage is the specificity, as host-based firewall can be adjusted to support a unique set of applications and to block everything else. Host-based firewall is also well defined for each machine type, which can be an improvement, since every machine may have different needs, as well the network in which the machine operates.

To select the host-based firewalls to test we used the work of (Meredith, 2010) and (Schroder, 2012). Based on this study we choose the following three systems: IPcorp, pfSense and Zentyal Community.

In next sections, we describe the key features of the firewall applications listed above. The list of features to be compared is based on the work of (Sulaman, 2011).

3.1.1 IPCop

IPCop (www.ipcop.org) is an open source host-based firewall software system, developed by IPCorp Team for operating systems based on Unix, like Linux (IPCorp, 2016). Its last stable version is IPCorp 2.1.9 and it is distributed under the license GNU GPL.

IPCop is a secure software system, highly configurable and easily maintained with several features, such as Caching DNS proxy (to help speed up Domain Name queries), Web caching proxy (to speed up Web access), Intrusion Detection systems, Traffic Shaping, Web Antivirus, Web Content Filtering, OpenVPN, and more. IPCorp also has the ability to partition the network into a green, safe network protected from Internet, a blue network for the wireless LAN and a DMZ or orange network containing publicity accessible servers, partially protected from the Internet.

IPCop uses a Web based interface, that once been installed, the dialup setting are added via browser based from a client on the LAN. Although not officially part of IPCop, there is many add-ons, that include extra features to IPCop, such as QOS, virus check email, traffic control, extended interfaces to control proxy, etc.

IPCop is available for multiple languages: Bulgarian, Czech, Dutch, English, French, Greek, Italian, Polish, Portuguese, Swedish, Romanian, etc. IPCop also has a system of monitoring and performance charts that quickly warns if there are trouble spots. IPCop can be downloaded at: http://ipcop.org/download.php.

3.1.2 pfSense

pfSense (www.pfsense.org) is a open source host-based firewall/rooter software system for FreeBSD operating systems. Distributed under the license BSD License, pfSense is developed by Electric Sheep Fencing, LLC and started in 2004 as a fork on the Monowall project. From beginning it is focused on full PC installations, as opposed to Monowall that is on embedded hardware (pfSense, 2016). Its last stable version is pfsense 2.3.2.

pfSense is a software tool known by is reliability, with several features such as: Network Address Translation, Filtering by: source/destination ip, protocol, os/network fingerprinting; Flexible Routing; Packet Scrubbing; Web Content Filtering; OpenVPN; Traffic Shaping, etc. pfSense uses a Web interface that allows the configuration of all their components. There are several companies that already use this software, some examples are: Check Point, Cisco PIX, Cisco ASA, Juniper, Sonicwall, Netgear, Watchguard, and Astaro.

As happens with IPCop, there are many add-ons available for pfSense, including language packs, dashboards, etc, which not only significantly improve the use of the tool, but also increase the range of functionality, like add-ons directly connected with the detection of threats. pfSense can be downloaded at: http://www.pfsense.org/download/index.html.

3.1.3 Zentyal Community

Zentyal Community version (www.zentyal.com) formerly known as eBox Platform cannot be considered a typical firewall, but as its creators claim to, a server for SMEs. However, its features and functionalities meets what is expected from a firewall and because of that it is relevant to our analysis (Zentyal, 2016). Zentyal is an open source system available for operating systems based on Linux, distributed by GPL and its last stable version is Zentyal server 4.2.

Zentyal is a very robust software tool with many features: Intrusion Preventing System, IPSec, OpenVPN, Firewall failover capability, Traffic Shaping, and more. Zentyal is composed of several open source software packages: Apache Web server, mod_perl CGI engine, OpenLDAP, OpenSSL cryptography, BIND DNS server, Web cache, APT, CUPS, APT and more. Zentyal Community can be downloaded at: http://www.zentyal.org/server/#server-feature

3.2 Web Application Firewall

The growing development of web applications and its massive usage has increased exponentially attacks on web application layer, which is a trend that shows no tendency of decreasing (Beechey, 2009). This fact becomes even more critical when the collected data indicates that 71% of all attacks could have been mitigated or totally eliminated using firewall solutions for Web applications (Security Statistics Report, 2012). Therefore, there was the necessity to use tools and solutions, designated as Web application firewall (WAF), which will minimize the risks for users and businesses.

One of the main advantages of Web applications firewalls, is its greater capacity when compared with network firewalls, to prevent attacks like Script injections, parameter tampering, Forceful browsing or buffer overflows (Pałka and Zachara, 2011).

The selection of systems to analyze was based on the work of Abdul Razzaq and colleagues, (Razzaq et al., 2013). In the next sections we study the following tools: ModSecurity, WebCastellum and Ironbee.

Defining a security policy responsible for a single host or machine, like computers or similar, having the ability to protect the machine even if it is moved from network to network.

3.2.1 ModSecurity

ModSecurity (www.modsecurity.org) is an open source Web applications firewall that works on Apache system supported by Trustwave's SpiderLabs Team, released under the Apache license 2.0 (ModSecurity, 2016).

The main features of ModSecurity are: Simple filtering, regular expression based filtering, URL encoding validation, Unicode encoding validation, Auditing, null byte attack prevention, upload memory limits and server identity masking. ModSecurity is also a well-documented application, essential for users with less computer expertise. ModSecurity uses four different security models: Negative Security, Positive Security, Virtual Patching, and Extrusion Detection.

ModSecurity can be downloaded at: http://www.modsecurity.org/download, and it is available for Microsoft Windows, Ubuntu/Desbian and Fedora/CentOS.

3.2.2 WebCastellum

WebCastellum (www.webcastellum.org) is an open source Web applications firewall developed in Java. It is able to protect the system against some threats like SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Parameter Manipulation, etc (WebCastellum, 2016). Its last stable version is 1.8.3 and it is release under Eclipse Public License.

WebCastellum is a very robust software tool with many features: URL Encryption, CSRF Protection, Form Protection, Stateful Attack Detection, etc. WebCastellum, also enables a monitoring of response and request. The handling and processing of responses which can be switched on as required makes possible, for example, the automatic filtering out of confidential information so that these are not transferred to the client. WebCastellum uses a Rule-based defense: a category of defensive function based on a complex recognition of patterns related to e.g. request parameters, form values, cookies, IP addresses or protocols. The patterns to be used when scanning are defined based on regular expressions. WebCastellum can be downloaded at: https://sourceforge.net/ projects/webcastellum/.

3.2.3 Ironbee

Ironbee (www.ironbee.com) is an open source Web applications firewall, distributed under the BSD License and Apache 2.0 (Ironbee, 2016)

Ironbee is a very reliable and scalable software tool, with many features: implementing custom security logic, User agent profiling, inbound and outbound traffic analysis, Behavioral monitoring (IP addresses, sessions and users), Passive vulnerabilty scanning, Cookie encryption and signing, Policy decisions, Tailored defense, etc.

Ironbee also allows a perfect interaction with external security systems (e.g., firewalls) and data exchange. Ironbee is still a relatively recent application and seeks to become the most complete application of the WAF in the market, with strong community support. Ironbee can be downloaded at: www.github.com/ironbee/ironbee.

4 COMPARISON OF OPEN SOURCE SOFTWARE TOOLS

In this section, we compared the free and open source software tools described in the previous sections. This analysis will be done by categories, which distinguishes the different types of software presented. We begin by comparing the firewall tools.

In Table 1 are compared the key features to firewall applications. The choice of features to be compared is based on the work of Sardar Sulaman (Sulaman, 2011), and the feature list of each application on theirs official websites.

According to our comparison, pfSense demonstrates to be the most complete host-based firewall open source system. It reveals a clear superiority in terms of available features when compared with the other systems studied in this work. The union of 10 of the 12 features compared, allows to apply a security policy more efficient and with a greater number of options.

Table 1: Host-based firewall tools comparison.

	IPCop	PFSense	Zentyal
Stateful firewall	Yes	Yes	Yes
Web antivirus (http,ftp)	Yes		Yes
Web url blacklist	Yes		Yes
Web content filtering	Yes	Yes	
IPSec	Yes	Yes	Yes
OpenVPN	Yes	Yes	Yes
Firewall failover capability		Yes	Yes
Load balancing		Yes	Yes
Traffic Shaping	Yes	Yes	Yes
Network IDS system	Yes	Yes	Yes
Policy routing		Yes	
RRD Graphs Reporting		Yes	

pfSense besides being the most featured full firewall distribution has also the ability to generate simple and intuitive reports witch is a huge advantage over other solutions. Furthermore, pfSense is a solution that has less power consumption, needs less space and generates less heat. It also has a simple installation process and a clear and easy learning interface.

Figure 1: 1pfSense Dashboard.

Now we will focus our study on Web Applications Firewall (WAF). Table 2 shows the comparison of the most important features, according to the work of Abdul Razzaq (Abdul et al., 2013).

Table 2: Web Applications Firewall (WAF comparison).

	ModSecurity	Web Castellum	Ironbee
Simple filtering	Yes	Yes	Yes
Regular expression based filtering	Yes		
Auditing	Yes		Yes
Null byte attack prevention	Yes		
URL Encryption	Yes	Yes	
Stateful Attack Detection		Yes	Yes

ModSecurity, as illustrated in Table 2, is the best open source system of WAF. It has a superior number of features in comparison with the other two tools systems. Additionally, the requirement of authentication is also a positive argument.

The main disadvantage of ModSecurity (see Figure 2) is the need to be configured manually, which can hinder the inclusion of users with lower computer literacy. However, we do not consider this disadvantage represents an insurmountable difficulty, since can be circumvented using its large community as its manual user. The setup and installation can also be a negative point for less experienced users, but once again, the community and user's guide are useful.

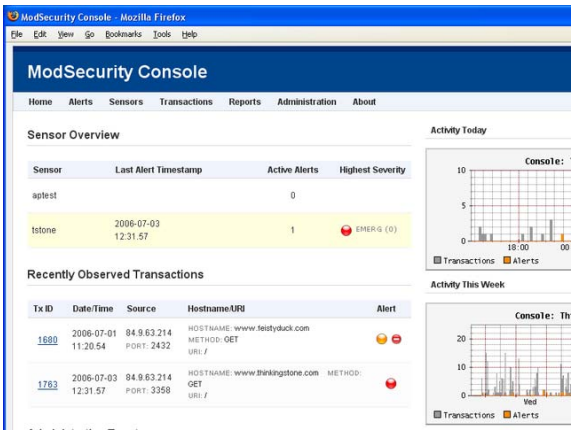

Figure 2: Console of ModSecurity.

5 CONCLUSIONS

In this paper, we proposed to design a security plan based only in free and open source software that could eliminate or at least mitigate the damage for the most common threats, such as: Trojan, antivirus, spyware, phishing, cookies and spam. Following this, we consider that the first approach to computer security will be Firewall host-based and web application firewall systems.

We analyze firewall systems that aim to apply a security policy to a particular point in the network, to control the traffic denying access to any malicious program. Firewall host-based has two great advantages: offering maximum flexibility and high configurability on a per-machine basis. According to our evaluation, pfSense is the most complete open source firewall available in the market. Web applications firewall use the same technology as firewall host-based but directly for the protection of web applications, increasingly more used. ModSecurity is clearly the best open source system of WAF available with its superior number of features and capacities.

These tools are intended to be the first line of defense, and each company must have the knowledge to understand their security needs, and add more security-related IT tools if necessary. We consider that is necessary to study the tools in a real environment and test its effectiveness.

As future work, we also pretend to evaluate and present a data security management evaluation, respecting the limitation of reduced costs, which means a investigation mainly focused in free and open source software systems.

REFERENCES

Abdul, R., Hur, H. and Shahbaz, S., 2013. Critical analysis on Web applications firewall solutions. IEEE Autonomous Decentralized Systems - ISADS.

Adele Howe, I. Ray, M. Roberts, M. Urbanska, 2012.The Psychology of Security for the Home Computer User. IEEE Symp. on Security and Privacy, pp. 209-223.

Beechey, J., 2009. Web Application Firewalls: Defense in Depth for Your Web Infrastructure.SANS Institute.

Bernardino, J., 2011. Open source business intelligence platforms for engineering education. WEE2011, Lisbon, Portugal, pp. 693-698.

Computer Crime and Security Survey, 2012. 15th Annual Computer Crime and Security Survey 2011/2012. CSI Computer Security Institute.

Dowd, P. W.; McHenry, J. T., 1998. Network security: it's time to take it seriously. Computer, vol.31, no.9, pp.28.

Garantla and Gemikonakli, O., 2009. Evaluation of Firewall Effects on Network Performance. 3rd IT Conf. for next generation, Univ. of East London, UK.

IPCorp, 2016. Official website from www.ipcop.org.

Ironbee, 2016. Official website from www.ironbee.com.

Liang, H., 2010. Understanding Security Behavior. Journal of the Association for Information Systems Vol. 11 Issue 7 pp. 394-413 July 2010.

Meredith, M., 2010. 7 of the best Linux firewalls.Available on techradar.com.

ModSecurity, 2016. Official Website from www.modsecurity.org/

Oppliger, R., 1997. Internet security: firewalls and beyond. Communications of ACM 40, 5 (May 1997), 92-102. DOI=10.1145/253769.253802.

Osmanbegovic and Zahirovic, 2013. Perception of Information Security of Management of Banking and Insurance Companies in Countries of Western Balkans. Research in Applied Economics, Vol. 5 (2).

Pałka, D., and Zachara, M., 2011. Learning Web Application Firewall - Benefits and Caveats. Computer Science Volume 6908, 2011, pp 295-308.

Paul van Kessel and Ken Allan, Under cyber attack EY's Global Information, 2013.

Pfsense, 2016. Official website from www.pfsense.org/

Ponemon Institute, 2013 2013 Cost of Cyber Crime Study: United States. Sponsored by HP Enterprise Security Independently conducted by Ponemon Institute, available http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf.

Razzaq, A. Hur, A., Sidra Shahbaz, Muddassar Masood, Farooq Ahmad, H., 2013. Critical Analysis on Web Application Firewall Solutions. 013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS).

Razzaq, Ahmad, H., Muddassar, M., 2013. Cyber Security: Threats, Reasons, Challenges, Methodologies and State of the Art Solutions for Industrial Applications. Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh International Symposium, pp 1-6.

Schroder, C., 2012. 5 best open Source firewalls.Available on smallbusinesscomputing.com.
Security Statistics Report, 2012. 12th addition- Industry Benchmarks. official Website.
Sulaman, S., 2011. An Analysis and Comparison of The Security Features of Firewalls and IDSs. Master thesis Performed in ISY (Information Coding).
Tawileh, A., Hilton J. and McIntosh S., 2007. Managing information in smes: a hollistic approach. Highlights of the Information Security Solutions Europe/ SECURE 2007 Conference, UK, pp 331-339.
V. Liggans 2006. The importance of firewall technology. Article conducted for the purpose of applying for a full scholarship for a bachelor's degree in Jonhson C. Smith University.
WebCastellum, 2016. Official Website from www. webcastellum.org/
Zentyal, 2016. Official website from www.zentyal.com.