Jestr

Journal of Engineering Science and Technology Review 12 (1) (2019) 80 - 86

JOURNAL OF
Engineering Science and Technology Review

Research Article

www.jestr.org

Design and Implementation of Firewall Security Policies using Linux Iptables

M. G. Mihalos[1,*], S. I. Nalmpantis[2] and K. Ovaliadis[2]

[1]*School of Social Sciences, Hellenic Open Unoversity*
[2]*Dpt of Electrical Engineering, Eastern Macedonia and Thrace Institute of Technology, Kavala, Greece*

Received 30 September 2018; Accepted 20 March 2019

Abstract

It is generally accepted today that security implementations on networking infrastructures are highly necessary. Specifically, when organization and corporal networks interconnect to the internet for financial transactions and valuable data administration, counter measures for unwanted attacks must be installed. This paper examines the network security threats, policies and mechanisms and analyses the firewall as a network concealing technology by elaborating the Netfilter/Iptables as an implementation mechanism. Consequently, the virtualization of a test-bed network takes place along with the respective development of the network security policy relying on the company's services and other significant requirements. Finally, this network security policy enlivens through iptables technology which is also evaluated using penetration tests.

Keywords: Network Security, Firewall, Netfilter, Iptables.

1. Introduction

Information security has become indispensable because of the distinctive value that data has gained in our days. Undoubtedly, operations of organizations have thoroughly changed over the last twenty years changing from large rooms with shelves full of paper dossiers to high technology computing systems. At the same time, the world started interconnecting along with the rapid development and spread of the Internet. Today, personal, business, military, academic and government information systems are interconnected through network infrastructures around the world [1].

Along with this enormous spread of networks, came the issue of security. Apart from securing a personal computer, as a stand-alone machine, a new security concept should be invented and developed in order to conceal a whole network. Communications through network terminals have become very easy making interactions quite vulnerable since one could have access to networks from a laptop and a dial up modem wired with a telephone cable. Network security has become even more susceptible with the presence of the internet where users have gained access not only to enormous volumes of information but to opportunities for mean use of computer interconnectivity.

The network, as an operational infrastructure is based on the foundations of the ISO/OSI seven-layered reference model. According to this model, many attacks as well as threats have been invented and constantly developed in order to cause functional problems on a network or infiltrate to gain administration or nab data.

By taking into consideration these potential attacks as well as the organization's services and requirements the network security is being defined by a policy which finds implementation on the network [2]. Although elaborating a security policy doesn't sound as a pleasant procedure it is the most critical part of a network's security development. A network security policy can define whether an expensive, highly secure steel door is being customized to fit a tent's entrance or a respective door casing.

The last step of network security development is to define the appropriate mechanisms that implement the aforementioned policy. One of the most well-known network security mechanisms of concealing a network is the firewall.

Firewalls are network security tools that operate between the connection of an organization's internal and the external network. Firewalls philosophy is basically to build a barrier at this choke point where all incoming and outgoing traffic passes. This barrier uses specific rules in order to decide which packets to let through or, if some packets don't meet the firewalls regulations, they are being blocked before even entering the internal network. As a result, firewall could be defined as a software, device or arrangement or equipment that is designed to filter a network's traffic and limit network access [3]. Besides the barrier operation, firewall meets a list of additional criteria such as resistance to security compromise, resource monitoring and auditing of capabilities, direct user access forbidding and fail safety operation which even if part of infrastructure fails, traffic won't be allowed to pass through the wall.

2. Firewalls

Firewalls are security mechanisms that are intended to meet specific goals [4]. Firstly, the network topology of the organization should be configured in order for the traffic to pass only through the firewall. Secondly, this choke point conceals the network by implementing security policies, thus determining which packets to allow or drop. Lastly, the

*E-mail address: mmihalos@gmail.com
ISSN: 1791-2377
doi:10.25103/jestr.121.09

firewall is able to conceal an entire network, and build a barrier for attackers and infiltration attempts.

Moving forward, firewall's operation leans on specific controls which implements on the network's infrastructure in order to carry out all the aforementioned characteristics. These services include Service Control, Direction Control, User control and Behavior control [5].

Service Control is a firewall's feature which decides which types of services are allowed to be accessed from the outside of the network to the outside and vice versa. Direction Control which deals with the inbound or outbound traffic course. This type of control examines the threshold of a packet, which service this packet administers, the terminal that attempts to reach and decides to allow or decline the packet flow. User control is a firewall's feature that basically controls access to the users that operate inside an organization's network or, on some occasions on users that access a network's internal infrastructure from outside of it. Last, but not least, Behavior control is the last control a firewall operates and determines how services can be used.

A. Firewall Limitations

Although firewalls are able to strengthen a local network security policy, they also introduce some flaws. The first issue that rises when installing a firewall, is that a significant amount of time must be invested in order to properly configure the security policy of the local network [6]. Another critical issue that firewalls must deal is the increasing and protocol complicated traffic. Although the choke point of a firewall can thoroughly examine all incoming and outgoing traffic it is a fact that firewall's operation could turn to be slow on a large amount of traffic [7]. Furthermore, another problem that arises is the wireless infrastructure of a local network. In this case, there are vulnerabilities which come up since the points of connection can't be as enforced as the wired network.

Some other vulnerabilities of firewalls include encryption issues. Encrypted packets include non-transparent headers but firewalls show difficulties in recognizing and trafficking packets. Last, but not least firewalls don't seem to fully collaborate with protocols that include sophisticated handshake mechanisms. FTP for example works by initiating connections from client to server and vice versa. Firewalls are familiar with handling these protocols but some operations remain vulnerable and unsafe.

B. Classification of Firewalls

Firewalls can be classified regarding the ISO/OSI network layer model into two main categories: network layer and application layer operating firewalls. A more detailed description of network and application layer firewalls follows.

Network layer firewalls

In network layer firewalls traffic is routed directly through the network layer. Packet filters have a simple philosophy of operation that lies on the IP packet characteristics [43]. If the packet complies with the rules defined by the local security policy, its trespassing is being allowed. In any other case the packet is being discarded and its entrance on the local network is being blocked.

IP packet headers inspection includes the examination of the following characteristics: Source IP Address, Destination IP Address, Protocol inspection, TCP and UDP port enforcement and last but not least, TCP flag examination.

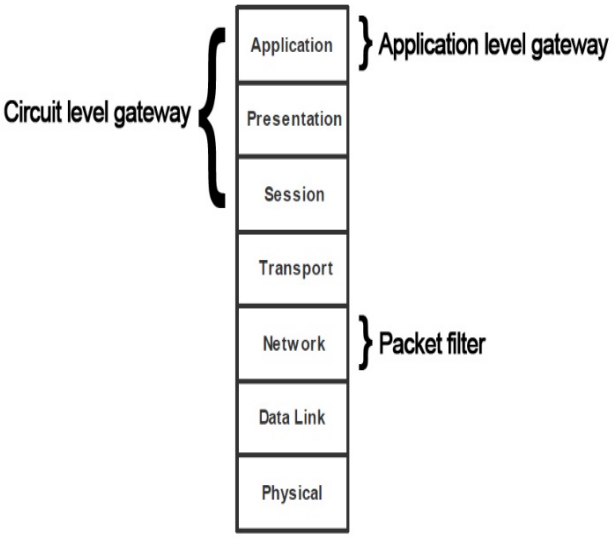

Fig. 1.. Classification of firewalls on the OSI/ISO network layer model.

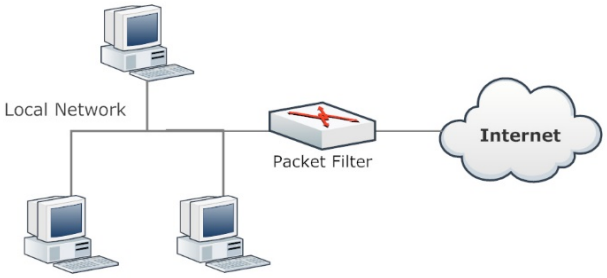

Fig. 2. Packet filter firewall topology.

Packet filters although, are also divided into two categories of filtering, stateless and stateful.

In stateless packet filtering the firewall decides whether to allow or discard a packet by examining all the aforementioned packet characteristics [8]. Stateful packet filtering on the other hand is an enhanced version of the stateless filtering mechanism. The main difference is that it maintains specific characteristics of the TCP/IP protocol [9] as sessions, thus, storing packet's active connections while any other packet which doesn't belong to any of these connections is being blocked. Stateful packet filtering also comes with dynamic packet filtering, a service where the firewall has the ability to ping the source IP of the packet that is under examination and examine its integrity.

Higher-layer Firewalls

In this category firewalls are able to control network traffic on the OSI/ISO network layers up to the Application Layer. Circuit Level Gateways and Application Level Gateways find implementation in this category of Firewalls.

Circuit Level Gateways may be of the same operating philosophy as the Packet Filter firewalls but they are a bit more sophisticated as they include TCP handshakes reviews. Specifically, packet filtering in this type of firewall has an additional operation on the Session layer of the OSI/ISO network model which includes handshaking observation between packets in order to examine and decide whether the request is legitimate or fraud [10].

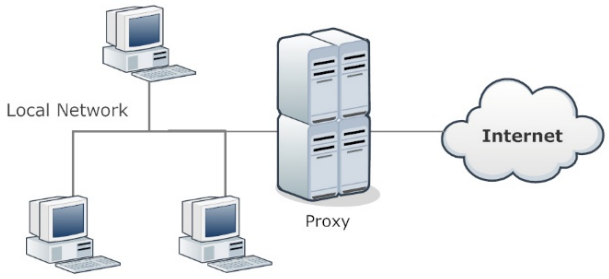

Fig. 3. Application level gateway topology.

Application level gateways are software application firewalls that operate through proxy servers and proxy clients [11]. When a user from the local network requests to initiate a connection to the internet, this request is redirected to the proxy server where the firewall is established. The proxy server then examines the specific request through the local security policy's rules and decided if the request is granted to move to the next hop or not.

C. Firewall Basing

Depending on the security level as well as the purpose of operation and the size of the network to be protected, there are three different types of firewalls basing: bastion host, host based firewalls and personal firewalls.

Bastion host is considered to be the critical strong point of a network which is responsible for the overall security as it is installed at the choke point and audits incoming and outgoing traffic [12]. Host-based firewalls are firewalls installed on a host that usually is a server, thus enforcing security additionally to the normal network firewall [13]. Personal firewalls are installed locally on a user's host. This type of firewall has been introduced in order to fill the gap of mobility [14].

D. Firewall Topologies

When it comes to infrastructure there are different topologies which can be used to install a firewall. Some of them, the most important, are the DMZ, Virtual Private Networks and NAT.

Demilitarized Zone (DMZ) is a firewall topology where a separate network is being added between the internal and the external network in order to provide safe and seamless outbound access [15]. Through this architecture the DMZ manages to provide with external visitors any inbound services such as a web server and SMTP but with isolate connection without giving the opportunity to the visitor to access the rest of the internal network.

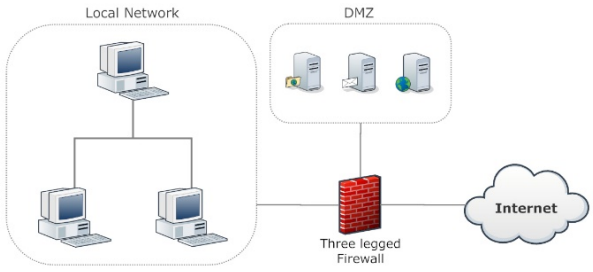

Fig. 4. DMZ networking topology.

VPNs are virtual shared networks which operate on a public network. In VPNs machines manage to exchange encrypted packets through the public network while they are decrypted only when the packet reaches its destination [16].

Last, but not least, NAT isn't much of a firewall by itself but it definitely helps enforce security along with the deployment of a firewall since it translates addresses from public to private and vice versa thus, hiding the addresses them from each other while only the router knows where traffic is addressed to [17].

3. Network security implementation

This paper deals with a small translation agency situated in the Center of Athens, Greece. The nature of this business doesn't require a large-scale network since it is compiled from a few but quite specific scope-oriented departments. In this case, the company is composed from the general manager and three departments, sales, production and accountant.

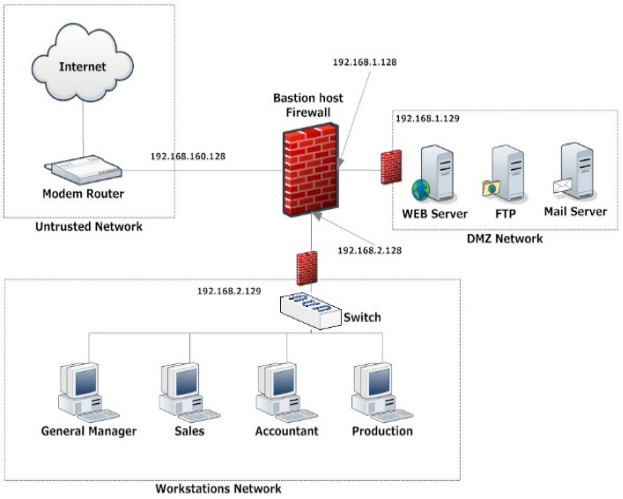

Fig. 5. Test-bed corporate network.

Although this company's network exists, it isn't possible to recruit it for the purposes of this paper. This is why it has been virtualized using the sophisticated software of VMware in order to work and configure each machine virtually.

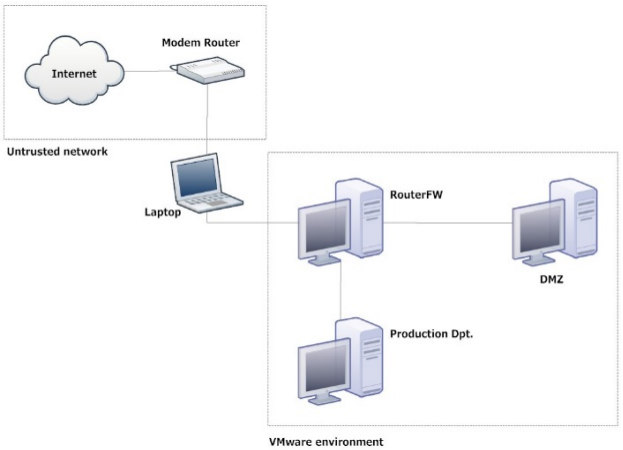

Fig. 6. Test-bet network in virtual environment.

Figure 6 depicts the exact configuration of the real infrastructure as well as the virtual machines installed. A personal computer hosts a VMware installation in which three virtual machines are being hosted, RouterFW, DMZ

and Production Dpt. RouterFW is responsible for routing traffic through the local network and will host the company's basic firewall. DMZ is a virtual machine which hosts the web, mail and FTP server applications which corresponds to company's requirements. Last but not least, Production Dpt. corresponds to the employees' workstations which have been cut down to one, since the security policy which refers to the local network machines is the same for all.

For the purposes of the specific test bed environment, Ubuntu 12.10 installations have been used for every Virtual Machine while for the virtualization environment VMware was installed at the host machine. As for the networking scheme the following configuration has been implemented.

Table 1. Virtual Machines IP addressing scheme

VM	Int	Interface IP	VMnet
RouterFW	eth0	192.168.160.128	VMnet8
(DMZ conn.)	eth1	192.168.1.128	VMnet2
(Prod conn.)	eth2	192.168.2.128	VMnet3
DMZ	eth0	192.168.1.129	VMnet2
Production Dpt	eth0	192.168.2.129	VMnet3

A. Evaluation of network security requirements and business services

The translation agency's scope is to receive documents, send them to freelancers, receive them back translated and deliver them to the customers.

Due to this file trafficking deployment, a sophisticated system of file management is being implemented as shown in figure 5, where there are two operating zones behind the firewall, the DMZ Network and the Workstations Network.

The DMZ Network provides specific services to the untrusted network but can be accessed by the Workstations Network as well.

The Workstations network includes a group of personal computers used by the corresponding departments. This is where all the operations of the company are taking place.

The overall concept of this network's security policy is to protect what's inside, while allowing access and communication for some services from inside to outside and vice versa.

B. Network security policy composition process

The security policy is being built by taking into consideration two main principles, the defense-in-depth and the compartmentalization of information [18].

The main firewall implementation is situated at the choke point of the network's communication with the untrusted network. The defense-in-depth principle implements a specific idea of what the basic firewall might miss from an incoming attack the other firewall deployment may prevent from further trafficking inside the network.

The concept of the compartmentalization principle is to make information and services available to different network users, trusted and untrusted thus, retaining security and confidentiality amongst all users [19]. In the specific network security this takes place due to the DMZ installation.

Before composing the security policy, it is important to comprehend that the main goal of the security policy is to come up with a top down approach of the network requirements and business operation security regulations [20].

Some of the topics that helped composing the security policy are how will the services be provided under secure networking communication, if users are authorized to access the internal network from outside through remote access and if collaborating persons must have access to the company's files through the internet.

C.Network security policy

Following, with the rigorous combination of all the aforementioned facts and factors, the emanating depiction of the security policy takes place.

Main Firewall zone

- Implement the use of a packet filter mechanism at the network's choke point, as well as the all the rest hub conjunctions with additional packet filtering mechanisms.
- Firewall should provide limited and controlled incoming access from the untrusted network to the company's system.
- Firewall should provide service oriented limited outgoing access from the users of the internal LAN to the external network.
- Block any incoming well known attacks that could damage the network or gain access to any potential intruders.
- DMZ deployment is necessary due to the server based applications that business services require.
- Logging of incoming and outgoing traffic will take place in order to monitor any suspicious packet movement.

DMZ zone

- Visitors from the untrusted network can have access to the web server in order to view the company's website.
- FTP server is available for clients and freelancers coming from the untrusted network, as well as from the Workstations zone from where employees traffic files.
- No other communication is allowed regarding the DMZ zone.

Workstations zone

- Users can have access to the internet due to the agency's operation since they may need to translate websites or transcribe video and audio.
- Users are not allowed to access any social media websites such as Facebook and Twitter.
- Email communication is regularly taking place due to the client and freelancer constant communication.
- Attachment of outgoing files is prohibited, files are being sent to clients and collaborators only through the FTP server.
- The above results into constraining the whole outgoing email size into a small volume, to avoid attachments.
- Web-based email accounts such as Gmail, Yahoo and Hotmail are forbidden.

C. Network security policy implementation and testing

Having implemented iptables rules that depict the aforementioned security policy, a series of tests takes place in order to examine the validity of the iptables implementation.

Common attacks simulation

A series of test are being performed locally on the RouterFW as attack simulations. NMAP can simulate specific attacks regarding the policy rules that have been written for this project as well. For example, regarding the NULL attack, the firewall managed to block the specific attack as nmap returned "Operation not permitted" message as shown in Figure 7.

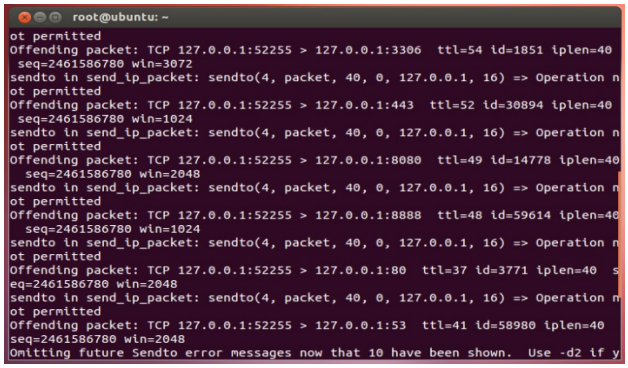

Fig. 7. NULL attacked blocked by the firewall.

What's most important, the specific attack has been logged, Figure 8 represents the log file where one can see the corresponding prefix for NULL recognized attacks.

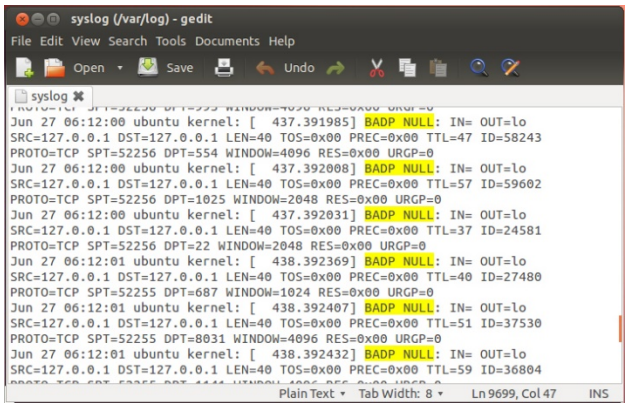

Fig. 8. NULL attack logging.

Following, the results from the attacks of an XMAS attack, a SYN flag, ACK flag and SYN flood attack.

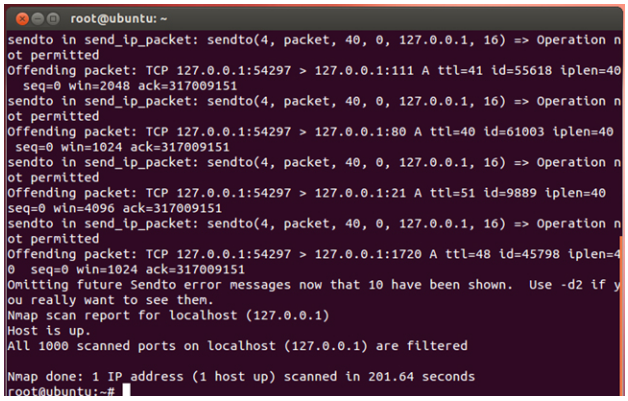

Fig. 9. XMAS attack blocked by the firewall.

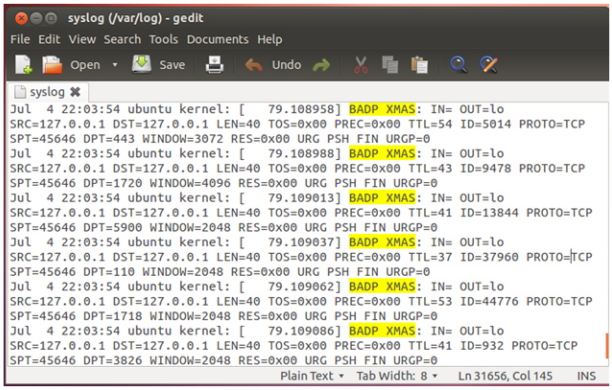

Fig. 10. XMAS attack logging.

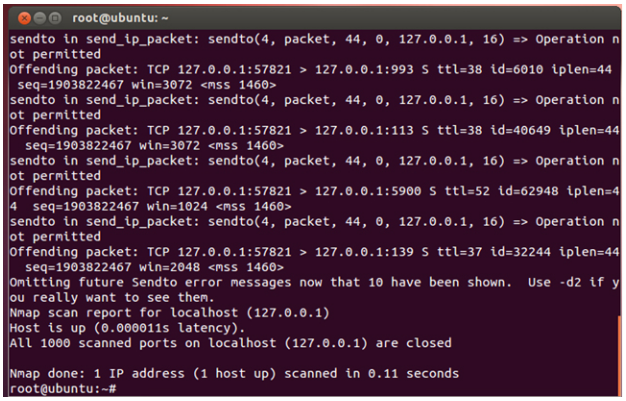

Fig. 11. SYN flag attack blocked by the firewall.

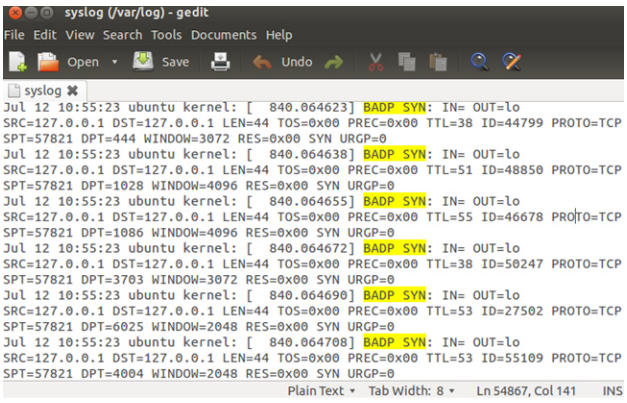

Fig. 12. SYN flag attack logging.

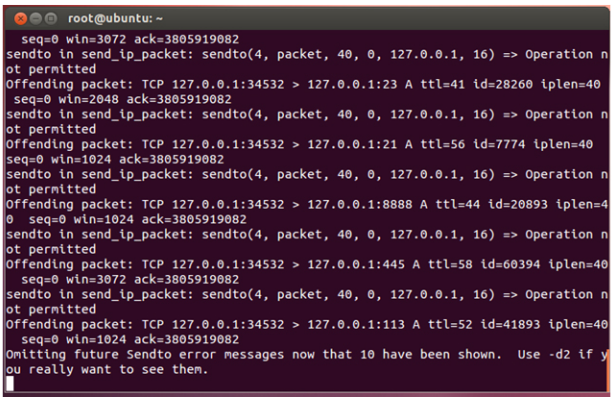

Fig. 13. ACK flag attack blocked by the firewall.

This type of attack isn't being logged due to the rule that corresponds to every non SYN set packet. This means that every packet that isn't SYN set when arriving the RouterFW is being dropped and not logged.

Fig. 14. SYN flood attack block by the firewall.

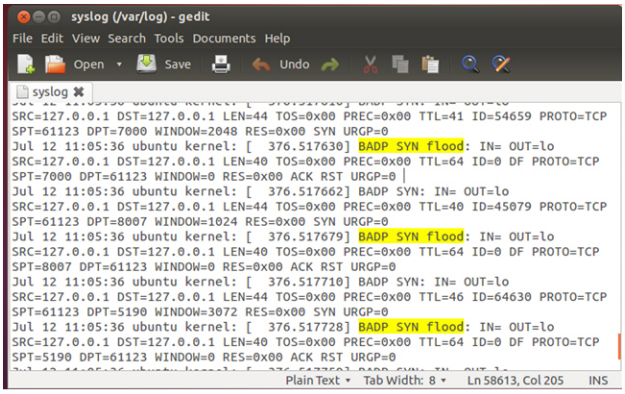

Fig. 15. SYN flood attack logging.

All attacks have been prohibited and have been logged as well.

Interconnection Penetrating test

Following, some test have been performed depicting the interconnection through the VMs.

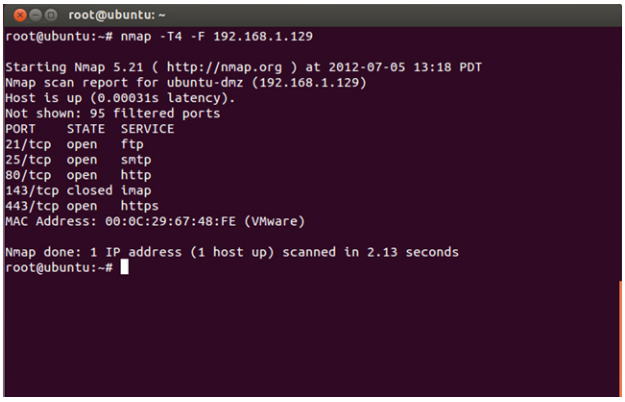

Fig. 16. RouterFW to DMZ quick scan test.

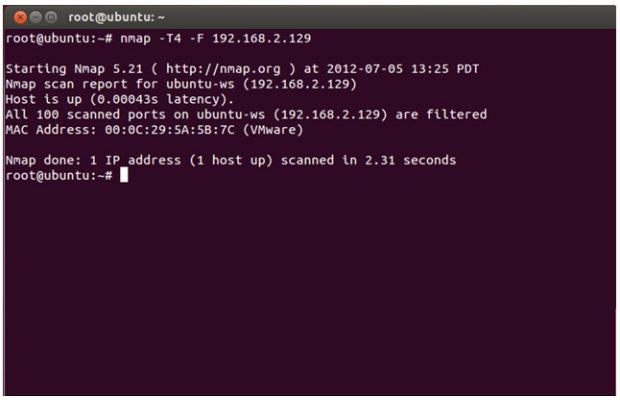

Fig. 17. RouterFW to ProductionDpt quick scan test.

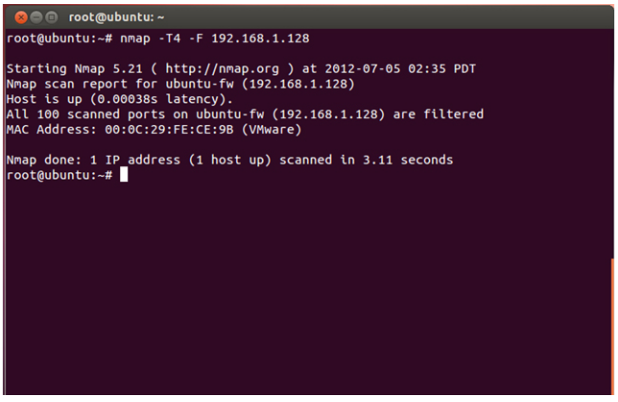

Fig. 18. DMZ to RouterFW quick scan test.

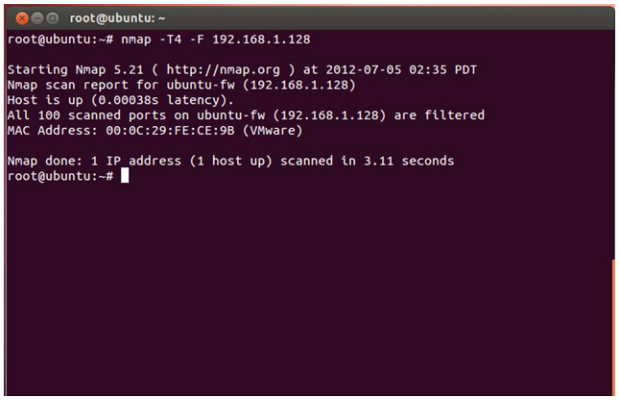

Fig. 19. ProductionDpt to RouterFW quick scan test.

All virtual machines are totally secured as from the interconnection scanning between the VMs, all ports are being filtered through the firewall. Nmap defines the filtered ports as blocked ports that don't allow the definition of the port if it is opened or closed. The only ports that are open, are the ports that define the services of the DMZ and redirects traffic from the untrusted zone through the RouterFW to the DMZ.

4. Conclusions

This paper initially relied on a research of a more general view regarding network security and firewalls, but soon took shape using a specific case study through Linux Netfilter and more specifically, the iptables firewall technology.

Despite its complexity, iptables has proved to be solid and trustworthy. Complexity includes a deliberate translation of the business network security policy requirements into multi-VM-layered combined rules.

Two aspects have been evaluated in this simulation, the routing and the security one. Without proper Linux and iptables configuration none of the VMs would have access to the internet and none of the untrusted originated visitors would have had access to the network's services. On the other hand, and having excellent performance of routing traffic throughout the virtual network, iptables has been configured to define if this traffic is legitimate to flow around the routing source and destinations. Nmap examination on each VM has proved that the current iptables implementation is as defined through the security policy, allowing only specific services and filtering all incoming traffic through RouterFW VM. Both aspects though could be crumpled though if only one rule is set wrong.

Another security aspect that improves the security environment of the test bed network, is the LOG configuration. Through the Kernell's logging system, iptables in this case study was proven quite efficient as it managed to monitor incoming and outgoing traffic by identifying the source and the destination of the packets and most importantly, it drastically represented all malicious attacks simulation that was performed at the RouterFW.

Some drawbacks can be found on policies that lie on application oriented requirements. The unwanted websites that Production Dpt. users must not have access to, are being defined through specific keyword hashes. Although this defines unwanted website it could end up as an unwanted policy eventually. This lies to the fact that the rules block any connection initiating, for Facebook for example. But, if

the user wishes to visit the website http://www.facebookfacts.com then the same implies to this web address as well.

Iptables are capable of coping with even more demanding requirements such as load balancing traffic throughout any VM connected to the router and traffic flow prioritization through packet regulations. On the latest Netfilter editions there are even patches which amplify the effectiveness and customization options of iptables.

Commercial applications and hardware solutions can be compared to the iptables' technology configuration, efficiency and rules imperialism. The most important aspect regarding iptables though is its free, open source and simple environment of constant research, development and growth.

References

1. A brief [1] The CIA triad: Have you thought about Integrity? (2007). Kinamik. [Internet]. <http://www.kinamik.com/download/>. [Accessed 12th March 2018].
2. How to develop a Network Security Policy. (2002). WindowSecurity. [Internet]. <http://www.windowsecurity.com/>. [Accessed 16th March 2018].
3. IATAC. (2011). Information Assurance Tools Report – Firewalls. [White Paper]. Retrieved from <http://iac.dtic.mil/>.
4. Dr. Weis. (2003). Types of Firewalls. Security in Computer Networks, University of Duisburg-Essen, unpublished.
5. Brijendra Singh. (2009). Network Security and Management. PHI Learning Pvt. Ltd.
6. Firewall Limitations. (2008). San Diego PC Help. [Internet]. <http://www. sandiegopchelp.com/>. [Accessed 23rd May 2018].
7. David W Chadwick. (2004). Network Firewall Technologies. Proceedings of the NATO Advanced Networking Workshop on Advanced Security Technologies in Networking, September 15 – September 18, Bled, Slovenia.
8. Chris May, Marie Baker, Derek Gabbard, Travis Good, Galen Grimes, Mark Holmgren, Richard Nolan, Robert Nowak and Sean Pennline. (2004). Advanced Information Assurance Handbook. Carnegie Mellon University.
9. Avishai Wool. (2012). Packet Filtering and Stateful Firewalls. School of Electrical Engineering, Tel Aviv University, unpublished.
10. Matt Warnock. (2005). An Evaluation of Firewall Technologies. Coursework paper, University of Virginia, USA.
21. enterasys.com/>.
11. Packet Filtering Firewall: An Introduction. (2010). World of Security. [Internet]. < http://www.tech-faq.com />. [Accessed 23rd May 2018].
12. Todd Jenkins. (2001). Hardening Bastion Hosts. [White Paper]. Retrieved from <http://www.sans.org/>.
13. Martin Englund. (2001). Securing Systems with HostBased Firewalls . [White Paper]. Retrieved from <http://www.oracle.com/>.
14. Almut Herzogl and Nahid Shahmehri. (2007). Usability and Security of Personal Firewalls. Proceedings of the IFIP SEC 2007. May 14 - May 16 May, Sandton, South Africa.
15. William Atkins. (2007). Design and Implementation of a Hardened Distributed Network Endpoint Security System for Improving the Security of Internet Protocol-based Networks. Thesis dissertation, University of Missuri-Rolla, USA.
16. Virtual Private Networking Basics. (2005). Netgear, Inc. [Internet]. <http://ciscosecurity.org.ua/>. [Accessed 28th May 2018].
17. Aaron Balchunas. (2007). Introduction to Firewalls. [White Paper]. Retrieved from <http://www.routeralley.com/>.
18. Chenghua Tang and Shunzheng Yu. (2008). Assessment of Network Security Policy Based on Security Capability. Proceedings of the 2008 International Conference on Computer Science and Software Engineering. December 12 – December 14, Wuhan, China.
19. [Daniel Oxenhandler. (2003). Designing a Secure Local Area Network. [White Paper]. Retrieved from <http://www.sans.org/>.
20. Entersys. (2010). Enabling Compliance – A Network Approach. [White paper]. Retrieved from <http://www.