Binh Nguyen

Network Security and Firewall

ClearOS – A Linux Open Source Firewall

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Bachelor’sThesis

Date 29 April 2016

Author Title Number of Pages Date	Binh Nguyen Network Security and Firewall 39 pages 29 April 2016
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Supervisor	Erik Pätynen, Senior Lecturer

The purpose of this final year project was to learn how to use a firewall - the outermost layer of protection - for network security. The aim was to learn the basic concepts of a firewall and threats against security system and to find methods to defend against the detected problems.

The first part of the study describes the overall concepts, functions and types of a firewall. Also some network security threats and attacks are mentioned. Details of a firewall basic architectures are presented and explained, how the architectures work, what the biggest advantages are and why use them. The second part of the study focuses on studying and testing ClearOS - a Linux open source a firewall- which can be effectively deployed for small and medium organizations. The method used in this project is combining theories with practical testing on an open source firewall product.

The result in the testing phase shows that the overall security of the system was raised to the satisfied level. Some suggestions for improvement for this project such as VPN, LDAP authentication and Snort intrusion detection which can be further studied and applied are mentioned in the conclusion.

Keywords	firewall ,network security, attack, threats

Contents

Abbreviations

DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DPI	Deep Packet Inspection
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
NFS	Network File System
OSI	Open Systems Interconnection
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network

1. Introduction

Information security is a critical need for individuals as well as society and all countries around the world. Since invented, computer network has brought along tremendous effectiveness in every aspect of life. Besides that users also have to face threats from all kinds of attack from hackers. Network security includes protection methods for all information that is stored and transferred through a system network. This is also a special field of interest and a difficult and complex work at the same time. Reality has proved that attack methods are more advanced and sophisticated than before and hackers aim to attack information during the storing, processing and transferring phases. Since the Internet era, more and more computers are attacked by viruses, Trojans and also by various kinds of TCP/IP protocol injections. [13, 5]

In the information outburst age, hackers develop at a faster rate than ever on all scales. A firewall is not only software (like a firewall on Windows OS) but also can be a dedicated hardware in network security. A firewall as dedicated hardware helps computers in network to analyse data ensuring that malware cannot penetrate into the system. It also allows network administrators to control activities on users' computers, filter and restrict data access and transfer data from inside out and vice versa. [13, 6-11]

Due to the importance of network security, I chose the topic "Network Security and Firewall" as my final year project to study solutions enhancing computer security. There is no absolute safety solution so in order to secure the information on a network, we need to construct many layers of protection. A firewall is the outermost layer of that system. The goal of this project is to study the basic concepts of a firewall, threats to computer network security, a firewall topologies, how they work and deployment of open source firewall products. The firewall product used for testing phase is ClearOS which runs on the basis of open source Linux.

2. A firewall

2.1. Network Security Methods

Due to a lack of absolute security solutions a network should be contemporarily constructed with multilayers to form a barrier against violating activities. The act of information security in the network focuses on protecting data stored on computers, especially on servers.

Figure 1 below describes commonly used security layers in network servers.

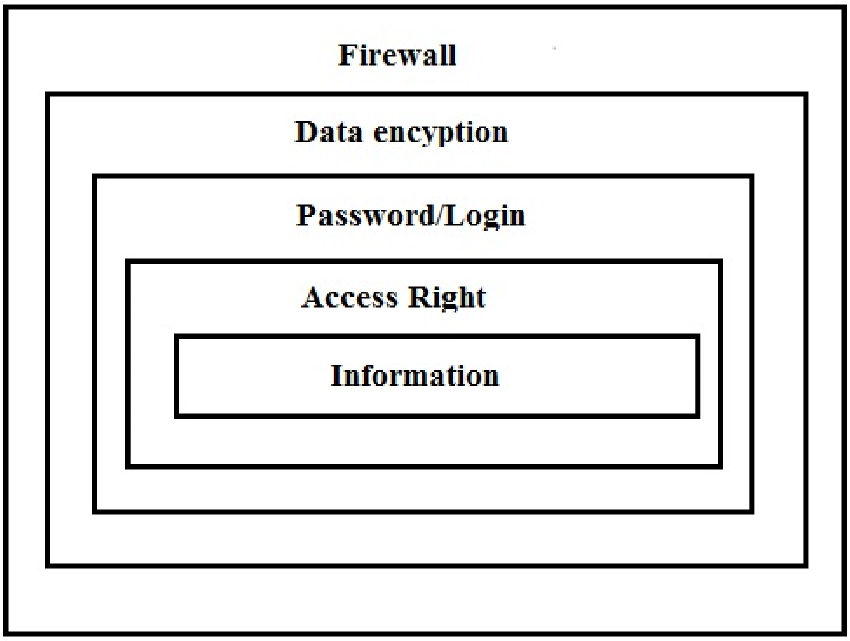


Figure 1. Network security layers

Network servers commonly have many security layers in order to enhance the ability to protect data and information. The innermost layer of protection is **Access Right**. This layer controls network resources (information) and rights (what users can do with those resources). This control applies to partitions, folders and files. The next layer restricts account access including usernames and passwords (**Password/Login**). This is a commonly used method of protection due to its simplicity, economical and highly effective. The administrator has full responsibility to control and manage the activities of other users. The third layer uses a data encryption method (**Data Encryption**). Data is encrypted with a certain algorithm so that even in case of data loss, hackers will not be able to read it without an encryption key. The outermost layer (**Firewall**) prevents intrusions, filters unwanted outgoing or incoming information packets. [3, 48]

2.2. Describing a Firewall

A firewall can be either hardware-based or host-based. A hardware-based firewall usually means specialized network boxes, such as routers or switches, containing customized hardware and software. This kind of firewall is often expensive, complicated and difficult to configure. In contrast to a hardware-based firewall, a host-based firewall is easier to use for individuals or small organizations. A host-based firewalls can be understood as a piece of software running on an individual’s PC, notebook or host. It is designed to allow or restrict data transferred on a network based on a set of rules. A firewall is used to protect a network from intrusions and concurrently allow legitimate data pass through. Usually a firewall should have at least two network traffics, one for private network and one for public network activities such as the Internet. At that time it acts as a gate controlling outgoing/incoming data streams of an intranet. Figure 2 illustrates a simple a firewall concept.

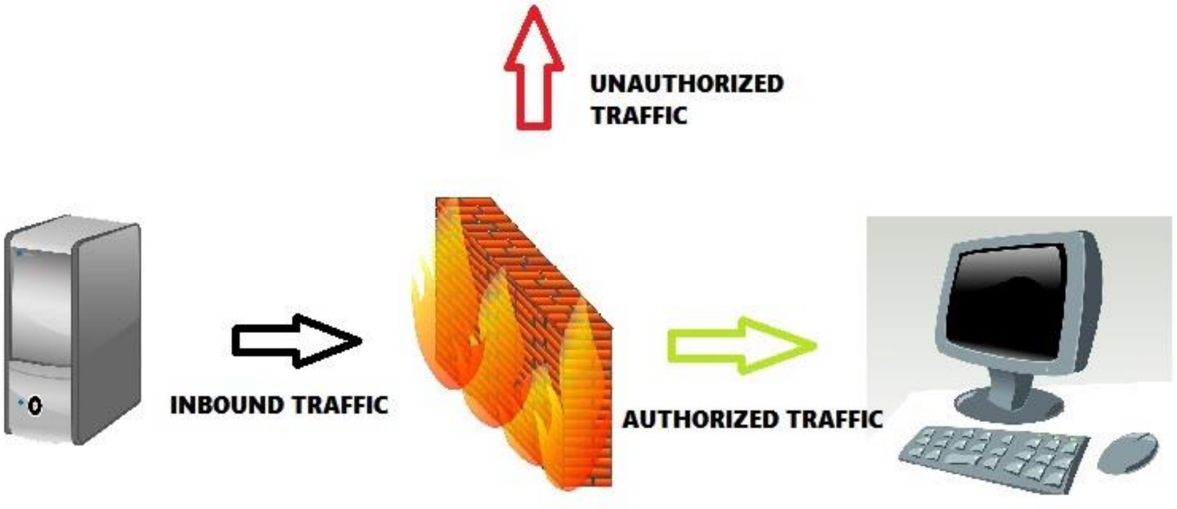


Figure 2. A firewall

Note: There are different concepts of a firewall on the Internet and in the books. “The thing to note here is that there is no fixed terminology for the description of a firewalls.” [2, 20]

2.3. Key Functions of a Firewall

Before study about how a firewall works, we need to know what a firewall can and cannot do. All kinds of a firewalls share some general features and functions to identify what a firewall can do. Technically a firewall should have these basic functions:

- Manage and control network traffic
- Authentic access
- Protect resources
- Record and report on events
- Act as an intermediary
- Record and report on events [5, 73-76]

Obviously a traditional a firewall is just an outermost layer of protection so it cannot perform everything. A firewall is just an artificial machine so it cannot classify information as good or bad. It can only block traffic with clearly defined parameters. Moreover, a firewall cannot prevent an attack if that attack does not pass through it. Basically it cannot prevent an information leak when data is physically copied. Last but not least, a firewall cannot concurrently act as a virus scanner due to the processing speed, the continuously appearance of viruses and also data encryption to conceal a virus. However it is still one of the most commonly used protection methods nowadays. [7, 25]

2.3.1. Managing and Controlling Network Traffic

The first and most basic function of a firewall is to control and manage traffic through a network. This means it should be able to identify which data packets are coming through, which connection is established and also be able to control those traffics in the system. A firewall can do this by inspecting data packets and manage connection traffics. Base on the result of this inspection, it will allow or deny access. Packet inspection is the process of handling data in a packet to determine whether to permit or deny that packet based on access rules and it should be executed on both incoming and outgoing traffics. The elements considered in the inspection include IP addresses, ports, IP Protocol and packet header. [3, 380-381]

2.3.2. Authentication Access

The usage of packet filtering helps to restrict resource access from unexpected sources. This can partly limit threats to the valuable resources. However, an intruder can fake an IP address in a trustworthy network and then can have full access to the files and data, at that moment one need an extra mechanism to improve the security. A firewall provides access authentication to eliminate those mentioned threats.

The simplest mechanism for verification is asking users for a username and password whenever they want to access the system. Information about a username and password must be created first by an administrator on that required server. When users want to access a certain server, that server will request user to input username and password, then it will check whether users input is correct or not. If it is correct server allows connection and vice versa false input will be rejected. This mechanism is not only for verification but also for applying privacy policy on separate users (for example giving a user a read-only right in a Data directory but full rights in a Shared directory). [4, 69-75]

The second authentication mechanism is using Certificate and Public Key. The benefit of this mechanism compared to using a username and password is that it does not require user's intervention. Users are no longer needed to insert username and password anymore. After that a system will create a Private/Public key pair. This method can be useful when deployed on a large scale. By using access authentication, a firewall provides an extra method for ensuring a legitimate connection. Even when that packet can bypass the packet inspection and filtering but it cannot be verified, it will also be denied. [3, 249-250]

2.3.3. Acting as an Intermediary

An Internet connection is a practical need and indispensable for individuals and organizations. However when allowing local stations in the network connecting directly to the Internet is a risk. Users can accidentally or intentionally download malicious content which cause dangerous to the network system.

The solution for this problem is that instead of allowing local computers connect directly to the Internet, we modify a firewall into an intermediate device to the Internet. At that time a firewall operates as a Proxy Server. The workflow of a Proxy Server can be described as follow: When a client wants to access Internet, for example access a website http://www.abc.com, that client will send a request to the Proxy Server instead of the web server. The Proxy Server will accept that request and if it is eligible the request will be processed. After that the Proxy Server collects information about the website http://www.abc.com. Collected information will be checked and then returned to client.

Local stations hardly recognize when there is a Proxy Server because it is almost transparent. The gain of the Proxy Server includes the usage efficiency of the network will be increased. Moreover all the requests are sent to the Internet through IP address of the Proxy Server and all responses from the Internet are checked for virus, malware, and Trojans before being transferred back to the client. [8, 295-298]

2.3.4. Resource Protection

The most important task of a firewall is to protect the network resources from outside threats. Network resources can be local stations in the intranet, or mail servers and web servers and uttermost important is business sensitive data. An administrator can apply packet filtering, access authentication, using a Proxy Server or any extra methods to protect the network. However an administrator should remember that a firewall is not an absolute safety solution for network securities. [6, 12]

2.3.5. Recording and Reporting on Events

Reality proves that no matter how many security layers you have, it is not 100% sure that the network system is safe. You cannot block every attack on the system. Due to that reason it is reasonable to have a precaution against what a firewall cannot defend. Recording and reporting events feature records all information about policy violated activities and reports it to administrator. Administrator will base on this report to evaluate and analyse problems and provide specific solutions. This information will be used regularly to analyse problems and its cause in the network system. [8, 350]

3. Firewall Technology

In this part we focus on components using in different a firewalls and how it works. A standard a firewall includes one or many of following components: packet filtering, application level gateway (or proxy server) and packet inspection. [5, 73]

3.1. Packer Filtering

A firewall operates closely with a TCP/IP protocol and works with an algorithm to split data received from applications on the network, or more clearly from services run on protocols (Telnet, SMTP, DNS, SMNP, NFS, etc.) into data packets. After that it assigns addresses for these data packets for identification and re-establishing packets at the destination. That is the reason why a firewall involves with data packets and their addresses. [5, 103-105]

A simple packet filtering is described in Figure 3.

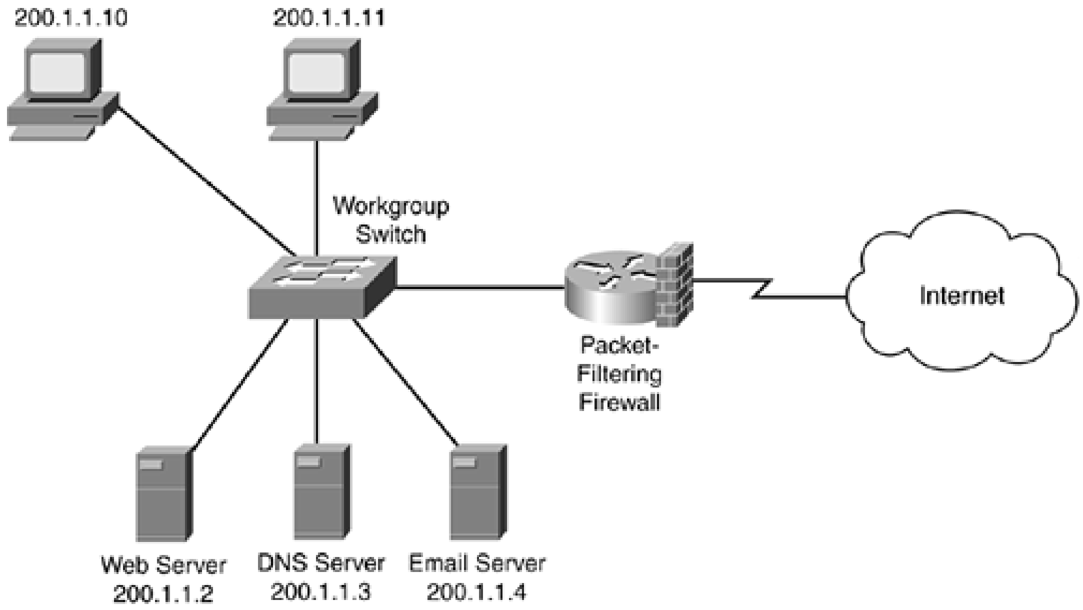


Figure 3. Packet filtering a firewall Copied from Kizza 2005 [8]

Packet filtering can receive or deny each packet. It checks the whole data packet in order to decide whether that packet meets the requirements or not. The rules for this packet filtering are based on information in a packet header allowing packets to be transferred in that network. These rules include:

- IP source address
- IP destination address
- Transfer protocols (TCP, UDP, ICMP, etc.)
- TCP/UDP source port
- TCP/UDP destination port
- ICMP message type
- Interface of incoming/outgoing packet [8, 289]

If packet filtering rules are satisfied, a packet can be transferred through a firewall. If not, that packet will be removed. These rules allow a firewall to block a connection to certain hosts or servers, or block the illegal connection to a local network from an invalid IP address. Moreover, port controlling provides the firewall the ability to allow certain types of connection to certain hosts, or only these protocols (Telnet, SMTP, FTP, etc.) are granted to be transferred in a local network. [8, 290-291]

A firewall system using packet filtering has many benefits. Packet filtering is a low cost and easy to manage method and that is why this method is included in almost every router. Besides that, packet filtering is invisible to users and applications, so it does not require any special training. On the other hand, this method also has some drawbacks. Identification of a packet filtering mode is complex, it requires administrator to have sufficient knowledge about Internet services, packet header types and specific values they will get in each situation. When the need for filtering expands, filtering rules will be longer and more complex, which is difficult to control and manage. Besides that, due to packet filtering working on a packet header, it obviously cannot control the packet content. A packet transferred still can carry bad intentions to steal or destruct system information. [11, 204]

3.2. Application Level Gateway

An application level gateway is designed to enhance the ability to control services and protocols on the network. Its operating principle is based on a proxy service method. Proxy service is a set of special code installed on a gateway for each application. If an administrator does not install a proxy code for a certain application, the corresponding service will not be provided therefore it cannot be transferred through a firewall. Besides, a proxy code can be configured to support only a few features in an application that an administrator considers acceptable while rejecting other features. [3, 414]

An application level gateway is often considered a bastion host because it is designed to protect against outside attacks. There are some solutions to secure a bastion host. The first method is always using secure versions of operating systems on a bastion host. These secure versions are designed specifically to protect against operating system attacks, as well as ensure a firewall integration. Moreover, an administrator installs only necessary services on a bastion host, simply because a service cannot be attacked if it is not installed. Usually, only limited applications for Telnet, DNS, FTP, SMTP and user authentication are installed on bastion host. Besides that, an administrator can also deploy different levels of authentication, such as username/password or smart card to enhance the security of a bastion host. [3, 415]

Figure 4 below shows how an application level gateway works.

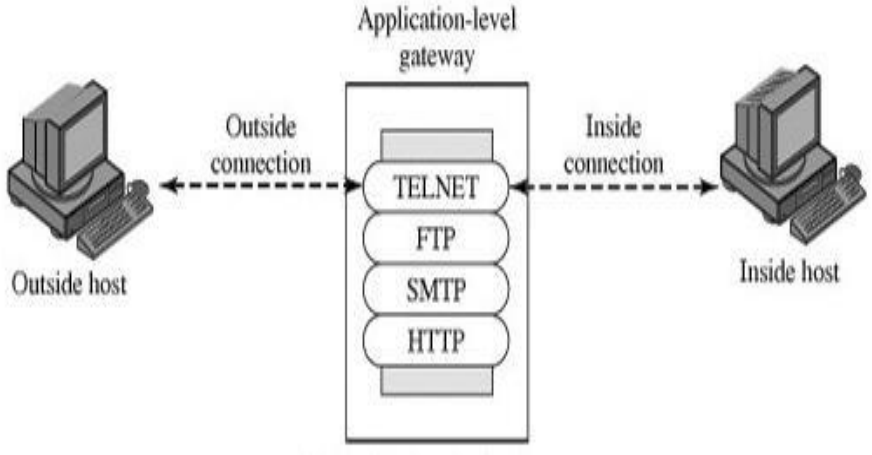


Figure 4. Application level gateway copied from Kizza 2005 [8]

Each proxy is configured to allow accessing only certain hosts. This means a command set and configured characteristics for each proxy only work on certain hosts in the whole system. A proxy maintains a diary to record details of traffic, connection events and connection length. This diary is useful for tracking and finding intruders. Every proxy is independent of each other and this simplifies installation process of a new proxy or removes a malfunctioning proxy. An administrator can fully control every service on the network, because a proxy restricts command set and decides which service can access which host. Moreover, filtering rules for gateway are easier to configure and control compare to packet filtering. [4, 213-216]

3.3. Stateful Inspection firewalls

Section 3.3 will focus on a stateful inspection firewall, which is a firewall that attempts to keep track of the state of every network connection passing through the interfaces until that particular connection is closed. So keeping track of the state of connections means to keep a scoreboard of all various protocol header values while packets go back and forth in the system. These values must be correct and in the right sequence. Typically, a stateful firewall tracks the states of the connection and maintains a table with Layer 3 and Layer 4 information [14, 10]. If a packet matches an existing a firewall rule, it can go through the firewall and all information about that specific entry is stored in a dynamic state table (source and destination IP address, source and destination ports, protocol types, header flags, sequence numbers, etc.). [7, 632]

This method increases the overall performance of a firewall because only initiating packets need to be decapsulated. Once the initial packets go through this in-depth inspection, from that point forward, the firewall just inspects the network and transport header. The reason for this scaling down from the full packet inspection to just the headers is to increase the system performance. Some of the common stateful firewall products on the market are Cisco PIX A firewalls, Checkpoint A firewall-1 and Cisco Reflexive ACLs. [7, 632-633]

Figure 5 illustrates a simple stateful packet inspection firewall.

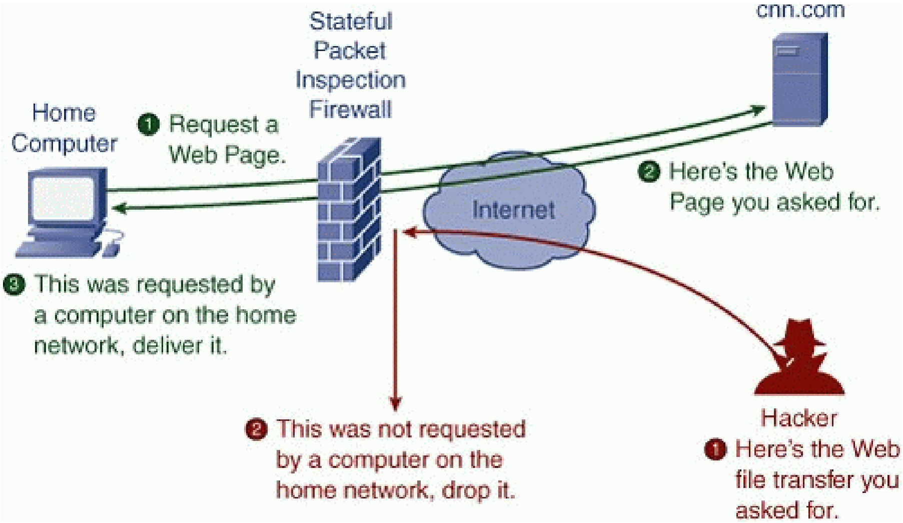

Stateful Packet Inspection Firewall
cnn.com
Home Computer
❶ Request a Web Page.
❷ Here's the Web Page you asked for.
Internet
❸ This was requested by a computer on the home network, deliver it.
❷ This was not requested by a computer on the home network, drop it.
Hacker
❶ Here's the Web file transfer you asked for.

Figure 5. Stateful packet inspection firewall Copied from Best Security Tips. [15]

Some characteristics of a stateful firewall include that it maintains a state table to keep track of the state of each and every communication session and provides more control over which packets are allowed to go through and which are rejected. Besides that, a stateful packet inspection firewall is transparent to users, scalable up to demand and it is hard to spoof packets through the firewall. Many stateful a firewall products also contain content filtering or Deep Packet Inspection (DPI) – an advanced method of packet filtering that operates at application layer (Layer 7) of the OSI model. DPI examines the content of a packet, searching for viruses, spam, Trojans, malicious packets and drop these packets at the ingress point of the network. [7, 633-636]

3.4. Demilitarized Zone (DMZ)

A common way to enhance network security is the DMZ (Demilitarized Zone), also known as a perimeter network. SI Security defines it as a network added between a protected network and an external network in order to provide an additional layer of security. A DMZ is used to separate an internal network from an external network by isolating the machine that is being accessed directly from other machines. An internal network in this case is normally the one which has more valuable information and is needed to be protected from the external one. The purpose of a DMZ is to provide insulation and extra protection for a server that provide services for protocols such as HTTP, FTP, DNS and SMTP to the general public. [6, 30-32]

Remember that all the machines in the DMZ area still have a great degree of exposure from both internal and external networks. Therefore these machines must be protected from both internal and external users by using a firewalls on each side of the DMZ. The positioning of DMZ servers are illustrated in Figure 8. DMZ can also include IDS (Intrusion Detection System) to filter out malicious contents. [7, 628-629]

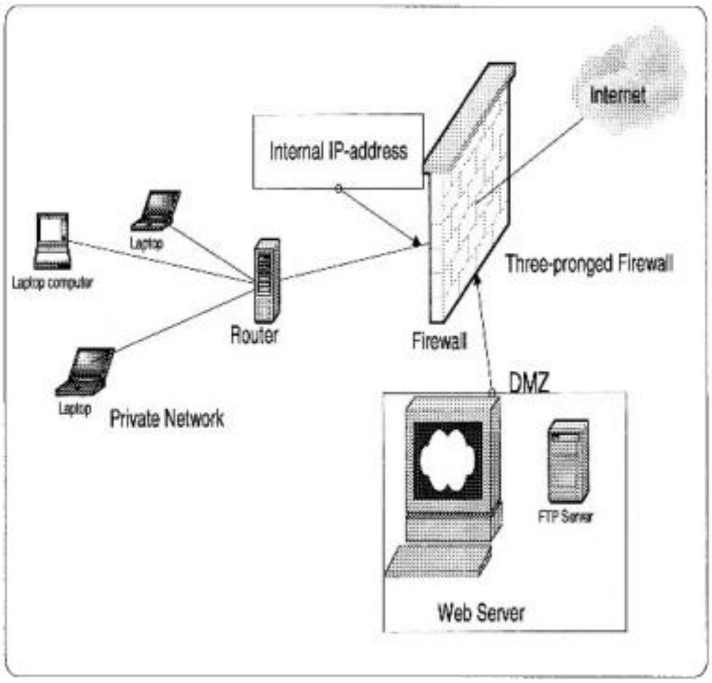


Figure 8. Placing of Web, DNS, FTP, SMTP servers in the DMZ Copied from Kizza 2005 [8]

The main advantage of a DMZ is the creation of three layers of protection that separate the protected network. So if a hacker wants to penetrate that protected network, he/she must crack three routers: the outside a firewall router, the bastion a firewall and the inside a firewall routers. This can increase the security for the network system significantly. [8, 306]

4. Network Security Policy

4.1. Definition

Network security is a security assurance of an entire network system from all vandalism activities initiating from both inside and outside. Vandalism activities include: intrusion, illegal resource usage, information stealing, deceitful activity aimed at sabotaging network resource and system database. Network security has always been considered a significant and serious undertaking. The more a network system grows, the more network security should be focused on. In order to control and manage network efficiently, following levels of security are considered:

- Network level: prevent intrusion to the network.
- Server level: control access right, security policy, users' identification.
- Database level: who can access to which host or server.
- Encryption level: encrypt all data with a certain algorithm, only users with a right key can access and use that data [9, 204].

When analysing network security, there are certain factors needed to be considered. First of all is the human factor. In network security, a human has an important influence on the whole system. When analysing a security plan, we need to concern about who will join the system, their rights and responsibilities. For example, a person who has no authority to access network premises can perform sabotage activity at a physical level. Second important factor in a network security plan is network architecture. It is a foundation of the whole network. We need to examine, plan and construct architecture carefully and suitable for the system based on the infrastructure. Finally, an administrator needs to understand and know the required hardware and software and their functions in order to be able to construct a compatible network system. [4, 203]

4.2. Threats

A threat can be understood as any event or circumstance with the potential to cause harm to an IT system. Threats can be non-malicious, hardware/software failures, natural or human error. When the network environment was still a closed and limited-access system, threats mostly come from inside and are called internal threats. These threats usually start from discontent employees with privileged access wanting to sabotage the system. Since the outburst of the Internet, external threats have grown accordingly. External threats mostly come from human sources. Motivation and curiosity – the human nature – make a human become one the most dangerous threat sources [11, 170].

4.2.1. Unstructured and Structured Threats

Threats can be classified as unstructured and structured. Unstructured threats are often from people with limited network system knowledge and little to no programming skills. They obtain tools on the Internet, from the forums for amateur hackers and try to exploit the vulnerability in random and multiple targets. If their attempts fail, they will likely try somewhere else. Although attackers do not have enough knowledge of hacking, they still can cause significant damage due to the fact that they can unintentionally obstruct the system by messing with the target environment. [9, 78-82]

Structured attacks, on the other hand are more troublesome because they are conducted by professional hackers with excellent level of hacking and computer science knowledge. Usually they write their own tools for attacking, or they can modify and improve tools from others. Professional hackers have a profound knowledge about computer, so they can study and discover new vulnerabilities in systems by experimenting complex actions against the security policy of the system. One of the biggest problems of structured attacks is that professional hackers often have stronger motivations than just simple mischief. A structured attack might not be blocked by traditional tools and methods such as Firewall or IDS (Intrusion Detection System). Even non-computer methods like social engineering, which means tricking people to obtain security information, can be used. [9, 78-82]

4.2.2. Virus, Worm and Trojans

A virus is a program or a set of code designed to self-clone and copy itself to other infected targets like files, folders or directories. In the beginning, it was written in order to prove the programming ability with certain features such as erasing data, freezing and crashing computers or other annoying pranks. Nowadays it is used for stealing sensitive information or hijacking computing systems. The important feature of a virus is that it cannot automatic spread but first requires a human touch to enable its' activity. [5, 322]

A worm likes a virus, it can replicate itself and rapidly spread in the system. A special feature which make a worm far more dangerous than a virus is that it can spread through a network system but a virus cannot. The primary task of a worm is to obstruct a network or even shut down the whole network. The worm is designed to spread rapidly in the network without a need to be activated by human. That is the reason why a worm is far more dangerous compared to other traditional viruses because it can be spread to thousands of computers. [5, 322]

A Trojan is a malicious program like a virus. The only different is that it cannot replicate itself. A Trojan will hide itself behind a trusted application and when one executes that application, a Trojan will be activated. Modern Trojans act as a backdoor, allowing hackers to install zombies in the computer, which then can have unauthorized access to the affected system. One of the simplest ways to prevent Trojans from infecting the system is to never open any email, software or message from an unknown sender. Hackers usually use intrigued messages to take advantage of users' curiosity, so it is best to delete those unknown messages. Anti-virus software is also an option for preventing Trojans but it can only recognize a portion of all known Trojans and does not recognize unknown ones. [13, 99-100]

4.2.3. Malicious Content

Malicious content can mean many things, but in general it means documents or programs that are infected with viruses, websites that attempt to infect a computer with a virus, or websites that attempt to solicit sensitive personal information. It usually asks users to execute a simple action which will allow hackers to approach the system, such as click on a link to open a website or read an email. These actions seem harmless but are actually very dangerous since one unintentionally gives permission to hackers to attack the system. [5, 323]

4.3. Attacks

4.3.1. Social Engineering

Social Engineering is a technique which takes advantage of what has been considered the weakest link in the security chain – the human factor. It is the process of obtaining confidential information by manipulation of legitimate users, and can also be known as hackers who use their brains instead of hacking tools. People usually ignore threats thinking that this won't happen to them. They also consider security problems as administrators' job and they do not need to know about that. Moreover, human are usually lazy and do not pay attention to what they do not have an interest in. Good security policy and protocols will not be effective if they are not followed. [10, 49-50]

Figure 9 describes the cycle of social engineering, which consist of four phases: Information gathering, developing relationship, exploitation and execution.

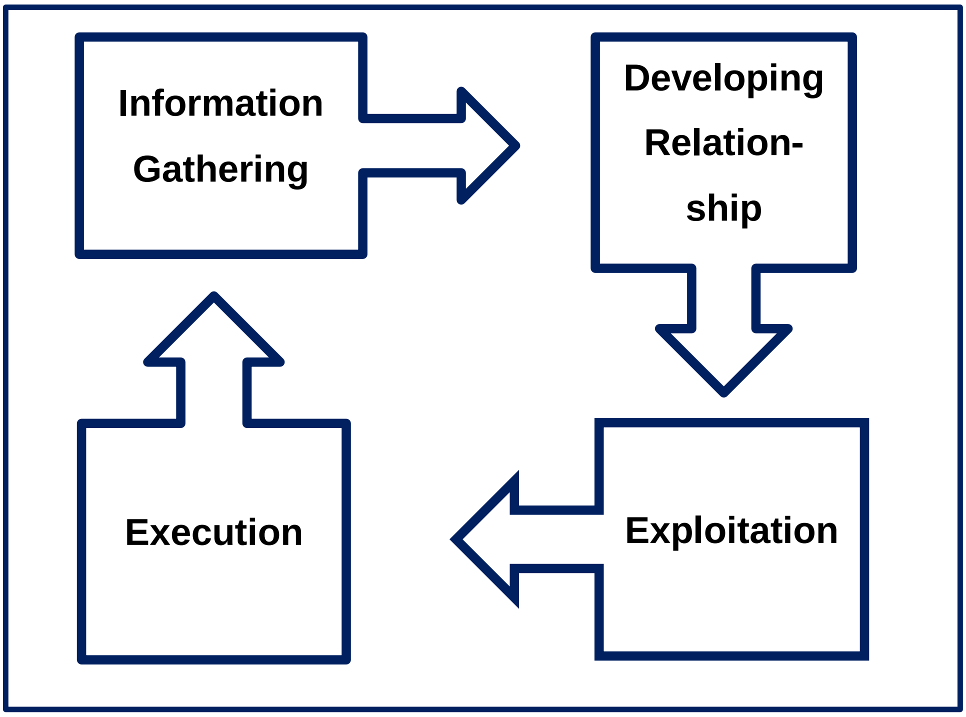


Figure 9. Social Engineering Cycle.

The best way to defend against social engineering is training the employees. Help desk staff, receptionist and call center employees should receive addition training because they are far more likely to be the target of this kind of attack than others. You should also inform employees about the importance of personal identity security and ask them to follow it strictly. [10, 71]

4.3.2. Host Reconnaissance

Malicious hackers value host reconnaissance as their first step to gather information for a successful attack. It is wise to invest time to see what is on the other side of the hill before launching attacks. The goal of host reconnaissance is to know the IP addresses, UDP/TCP ports and operating sytem of targeted network hosts. Reconnaissance can be divided into passive and active. While passive reconnaissance focuses on sniffing regular traffic as illustrated in Figure 10 to gain information from user groups, website, business partners and social engineering, active reconnaissance involves in port scanning and OS scanning. [10, 104-105]

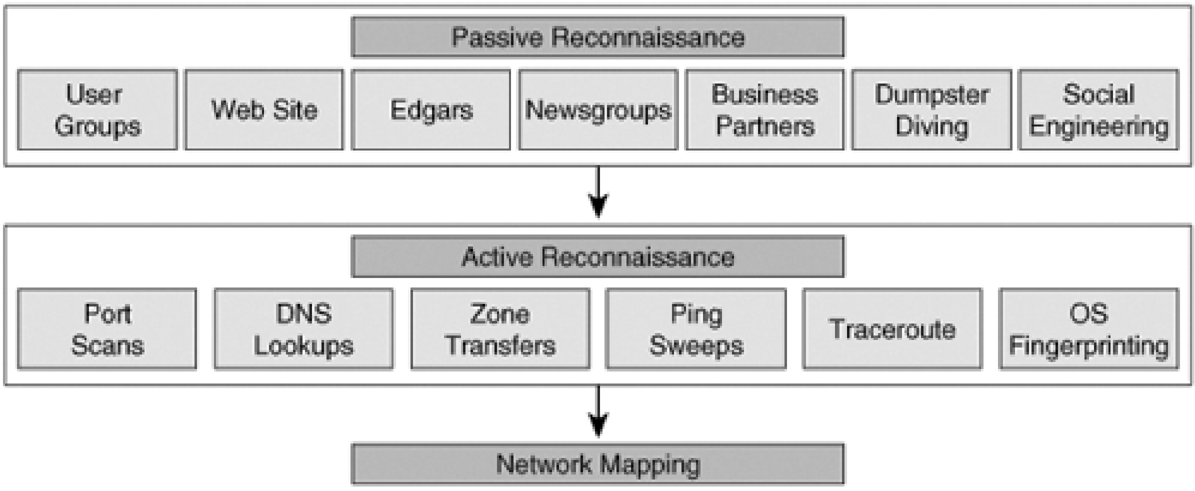


Figure 10. Passive and Active Reconnaissance Copied from Whitaker 2006 [10]

Passive reconnaissance can be time consuming but hard to be detected. The starting point to perform this kind of reconnaissance is the target's website. On the other hand, active reconnaissance can be far more revealing which means it is easier to be detected. After identifying the host within the target network, one can use port scanning techniques like TCP connect scan, SYN, FIN, ACK or NULL scan to identify potential vulnerabilities. These scanning techniques are usually done with NMap, one of the most common and powerful tool to carry out port scanning. [10, 122-123]

4.3.3. Network Traffic Flood

The principle of network traffic flood, so-called Denial of service (DoS) attacks, is that it attacka a network by flooding a host or server with dozens to hundreds of thousands of phony requests. This action will result in overwhelming the host/server's capacity to respond causing denial of service for valid users. Another variation is a distributed DoS (DDoS), also known as a zombie attack or zombie net [5, 321-322]. DDoS attacks do not change, alter, modify or destroy the system resources but instead they affect the system through diminishing the system’s ability to function. These attacks include flooding the network, disrupting network connections and services and preventing legitimate network traffic from going through the network. [8, 134]

DoS attack occurs when one computer and one Internet connection are used to attack another targeted server, whereas a DDoS attack uses multiple computers and connections to attack the targeted server. The computers using for DDoS attacks are often scattered around the whole world and are known as botnets and DDoS is much more difficult to withstand as the targeted server will be overloaded by a massive number of different connections.

A common venue of an attack is from network bandwidth and connectivity and the goal of attack is to disrupt services on a network and prevent legitimate traffic from being transmitted. A typical example of this type of attack is the SYN flood attack. In the SYN flood, an attacker starts the SYN/ACK process with the server in such a way that the connection is never completed. Almost all DoS and DDoS attacks focus on Web servers as a target, but any computer attached to the Internet can be a victim of this attack. Targets can be data servers, email servers and even workstations in the system. [8, 80-82]

4.3.4. IP Spoofing

IP spoofing is used when hackers spoof an IP address in the network to conceal their real identity by changing the packet headers of a message. The spoofed address is normally a trusted port in the network, which permits hackers to go through a firewall. Sometimes hackers insert illegal data packets into network sessions or change the routing table to collect the desired packets. IP spoofing is normally combined with other types of attacks such as SYN flood attack to create a half-open connection, which means that connection is never completed. [9, 281]

IP spoofing can be prevented by implementing a firewall that filter out the input to the external interface (known as input filter or ingress filter) by not allowing a packet through if it starts from the internal network address. Another way to protect a network from IP spoofing is using an IP verify method, so-called reverse path forwarding (RPF). When using RPF, it will check the source IP address of a packet to see if it is available in the routing table. If there is no route in the routing table, then that packet will be likely sent from a spoofed IP and the router will drop it. [9, 282]

5.3.5. Password Cracking

Password cracking is the process of recovering passwords from data that have been stored and transmitted in the system. There are three main methods to perform password cracking:

- Dictionary attack: a dictionary file which contains all the possible regular passwords is used. Hackers can create their own dictionary or download it form the Internet. A dictionary attack is usually attempted before using a brute force attack.
- Brute force attack: every possible combination to crack a password is used. This type of attack consumes the biggest amount of time but it will eventually find out the passwords.
- Hybrid attack: a combination of a brute force and dictionary attack. This type of attack will crack password by combining common dictionary words with common numbers. Therefore passwords such as mycomputer123 and 123mycomputer are checked twice. [10, 285].

Those who are familiar with using command-line, John the Ripper (http://www.openwall.com/john) is a popular password cracking tool for both Windows and UNIX platforms. Besides that L0phtcrack is one of the most popular Windows cracking tools. L0pthcrack can perform all three main methods of attack: dictionary, brute force and hybrid attacks. Moreover it can grade the passwords level, which is useful for evaluation of the password difficulty.

The best way to secure against password cracking is to apply a strong password policy. The password combination should have at least eight characters, with both lowercase and uppercase letters, numbers and even special characters. A small tip for creating a secure password is to combine a personally memorable sentence, some personal memorable tricks to modify that sentence into a password, and create a long-length password. Something like “My name is Nguyen Thai Binh and my birthday is 18 March” might become “mnisNtbinh183”. That password will not be in any dictionary for sure. Remember to change the password regularly and lock out accounts when failing three attempts to input a password. [10, 286]

5. ClearOS

5.1. Introduction

Nowadays there are many open source Linux a firewalls, such as Monowall, Endian, IPCop, SmoothWall Express, etc. Basically, they all run on a netfilter framework provided by the Linux kernel. Some distributions of Linux even implement functions such as Proxy, IDS, and VPN in order to provide a more perfect security solution.

ClearOS is developed by a prestigious organization ClearFoundation with a big user community and is a famous distribution according to http://distrowatch.com (ranked 40). ClearOS (formerly known as ClarkConnect) is a Linux distribution based on CentOS and Red Hat Enterprise and is designed as a Server, Network and Gateway system with an elegant user management interface that is completely web-based. Like other Free and Open Source Software (FOSS), ClearOS is released under GNU General Public License v2, which can easily download and install the open source community version for free from the server. ClearOS is a promising alternative solution for Windows Small Business Server of Microsoft which was terminated in 2012. The development progress of ClearOS is illustrated in Figure 11.

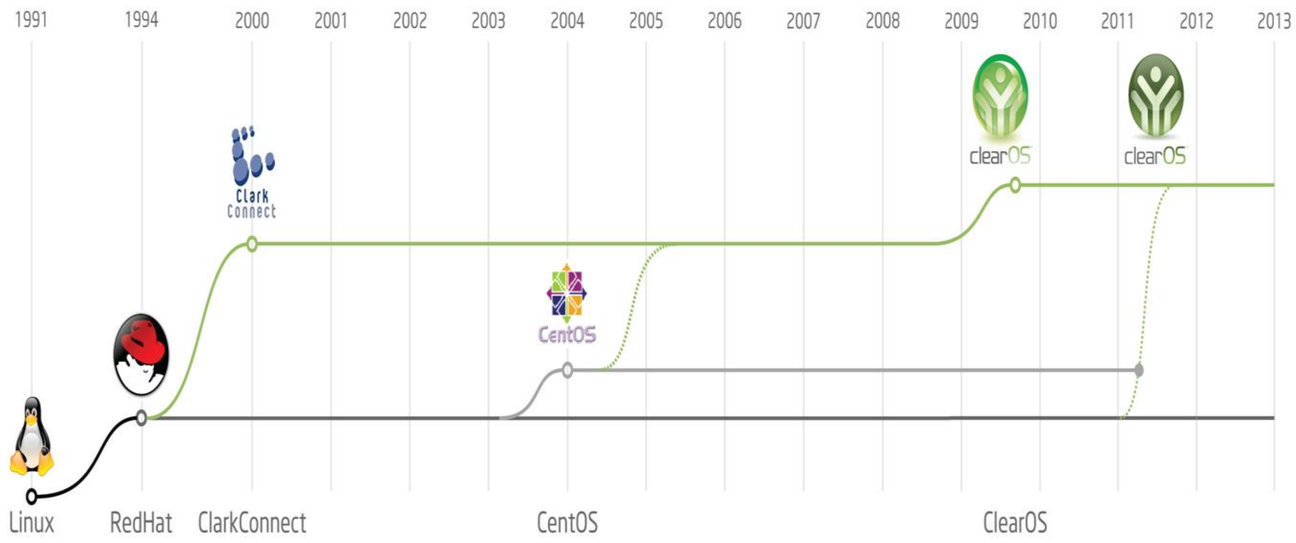


Figure 11. ClearOS development progress Copied from ClearOS Community Dashboad [14]

Some outstanding features of ClearOS include the following:

- Stateful a firewall (with iptables)
- Clean, simple and easy to use browser-based interface.

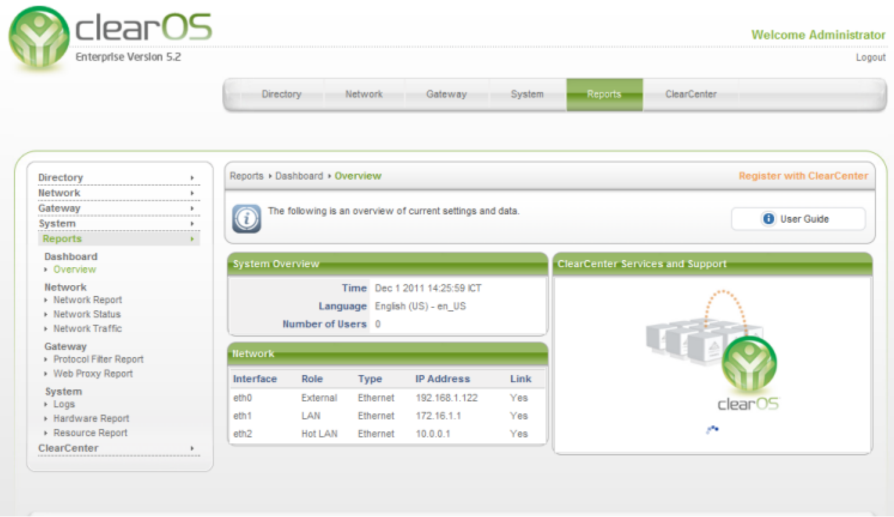
- Web proxy, content filtering and antivirus.
- Intrusion Detection and prevention System (IDS, IPS)
- Virtual Private Networking (PPTP, IPSec, OpenVPN).
- Get more control of the bandwidth.

5.2. System Requirements

Similar to other Linux distributions, ClearOS Enterprise can be installed with both a graphic user interface (GUI) and a console interface. Administrators can install with a console interface and administer it easily through a web-based interface. With console interface, the requirements for the server are just 512 MB RAM and 2GB hard disk. If installing with a Standalone mode, just one network card is required. If installing with Gateway mode, two network cards are needed.

5.3. Web-based Interface

After ClearOS has been installed, an administrator can configure all other ClearOS features from the web browser from any desktop or laptop computer. Figure 12 below is a screen shot of the main web-based interface.



The following is an overview of current settings and data.

Time: Dec 1 2011 14:25:59 ICT
Language: English (US) - en_US
Number of Users: 0

Network

Interface	Role	Type	IP Address	Link
eth0	External	Ethernet	192.168.1.122	Yes
eth1	LAN	Ethernet	172.16.1.1	Yes
eth2	Hot LAN	Ethernet	10.0.0.1	Yes

Figure 12. Main web-based interface

In the main web-based interface, there are five main menus. Menu **Directory** contains the most basic system configurations and information such as basic setup for account and user’s group, basic configurations of Domain, LDAP and other information about the organization and password rules. Menu **Network** is the main configure menu for the network system. An administrators can custom parameters for IP addresses such as IP address of the internal zone, external zone, DMZ, settings for DNS, DHCP, Multi-Wan. Moreover, an administrator can establish rules for a firewall, DMZ, incoming and outgoing connections.

Menu **Gateway** provides settings for Antimalware, bandwidth, Protocol filter and Proxy and menu **System** provides settings for server running ClearOS, resources of that server such as hard disk, running services and processes, backup settings for the server. Finally, menu **Reports** contains reports about network traffic, web proxy and protocol filter as well as system logs. This menu provides statistic values of the system.

6. Case Study and Experiment

6.1. Case Study

In this case study, ClearOS was used as a server for a small business organization with 3 different zones: Internet, Local and DMZ. The case study used two topologies: one is the consumption topology (Figure 13), which describes the actual organization infrastructure and one is the demo topology (Figure14) which is used in the experiment.

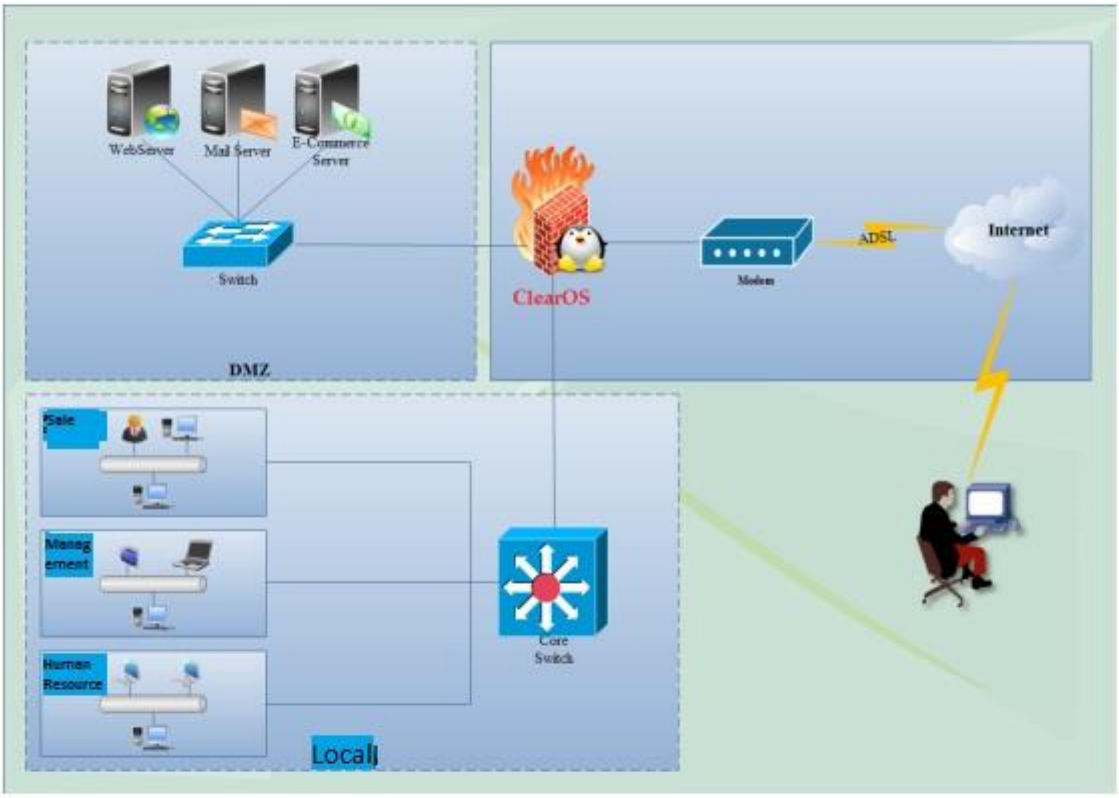


Figure 13.ConsumptionTopology

The consumption topology consists of:

- ClearOS as a server and a firewall with three interfaces connected to three network zones: Local, Internet and DMZ
- Modem: a device for connect to the Internet
- Switch: a network division device for servers in DMZ: Web server, Mail Server, E-Commerce Server.
- Core Switch: switch layer 3 device for segregating departments: Sale, Human Resource and Management.
- Workstations of each department.

6.2. Experiment

6.2.1. Demo topology

The demo topology in this experiment consisted of following characters:

- ClearOS as a server installed on a virtual machine using Virtualbox, includes three interfaces: etho0 (connect with the Internet), eth1 (connect with DMZ) and eth2 (connect with Local network).
- Client: local workstation with Windows 7 operating system installed on Virtualbox.
- Web server: CentOS operation system and httpd services installed on Virtualbox.
- User: Ubuntu operating system.
- Attacker: Kali Linux Operating system.

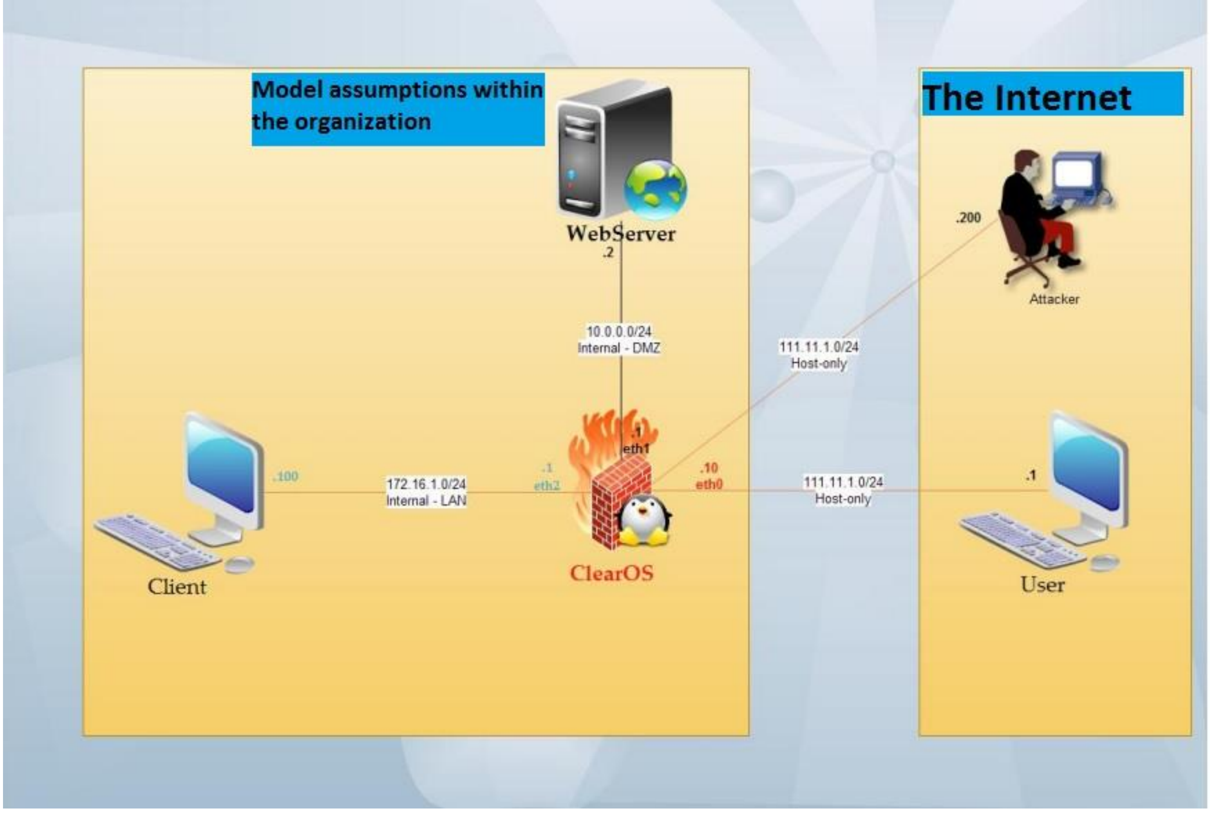


Figure 14. Demo topology

A list of experiments are tested in this project, the details about what to do and why will be explained in the Description, Task and Deploy of each experiment:

- Block bad website, malicious content with Web Proxy and Content Filter.
- Publish Web server on the Internet.

- Establish security protocols for Web Server.
- Allow only one IP address from the Internet and only one address from the local network SSH to a firewall.
- Prevent using Nmap to scan port.
- Prevent Dos and DDoS.

Table 1 describes all the interfaces and IP addresses used in the demo topology.

Table 1. IP addresses in demo topology

Name	Zone	IP
Client	Local	172.16.1.100/24
Web Server	DMZ	10.0.0.2/24
External interface (eth0)	A firewall	111.11.1.10/24
DMZ interface (eth1)	A firewall	10.0.0.1/24
Internal interface (eth2)	A firewall	172.16.1.1/24
Attacker	Internet	111.11.1.200/24
User	Internet	111.11.1.1/24

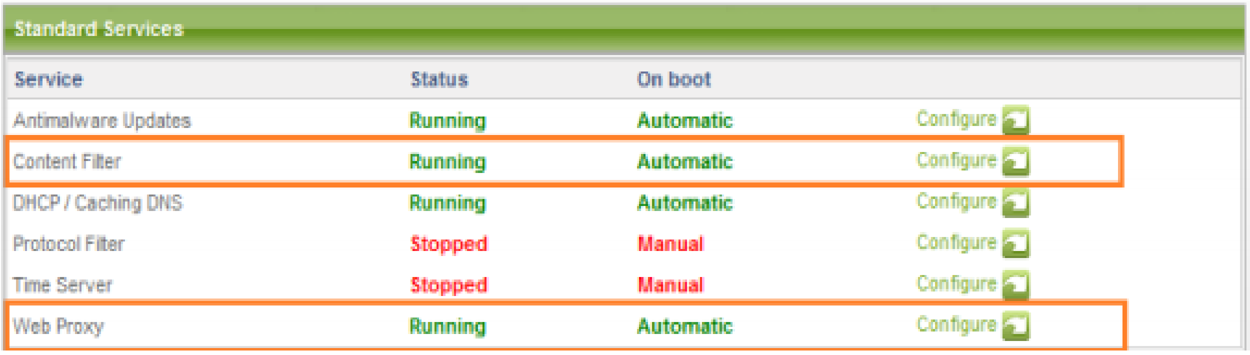
In the demo topology, ClearOS A firewall will have three interfaces eth0, eth1 and eth2. Eth0 will be the external interface connects to the Internet zone; eth1 will be the internal interface connects to the DMZ and eth2 will be the internal interface connects to the Local zone. The client will represent all the Local workstations of the Consumption topology, the Web server will represent all servers in DMZ and Attacker and User will be in the Internet zone.

6.2.2. Web Proxy and Content Filter

The organization provides employee Internet connection to support daily work tasks. However employees usually use Internet for their private needs, such as reading news, surfing Facebook, chatting, listening music, watching movies, and sometimes downloading malicious files that can harm the network system. The task for an administrator is to block users from accessing certain web pages during working hours. In this experiment, the task is to block two famous Vietnamese pages; the first one is an entertainment sites http://zing.vn and the other one is online news http://vnexpress.net

The following steps describe a process how to establish block rules

- Step 1: Start Web Proxy and Content Filter services in System/Service menu

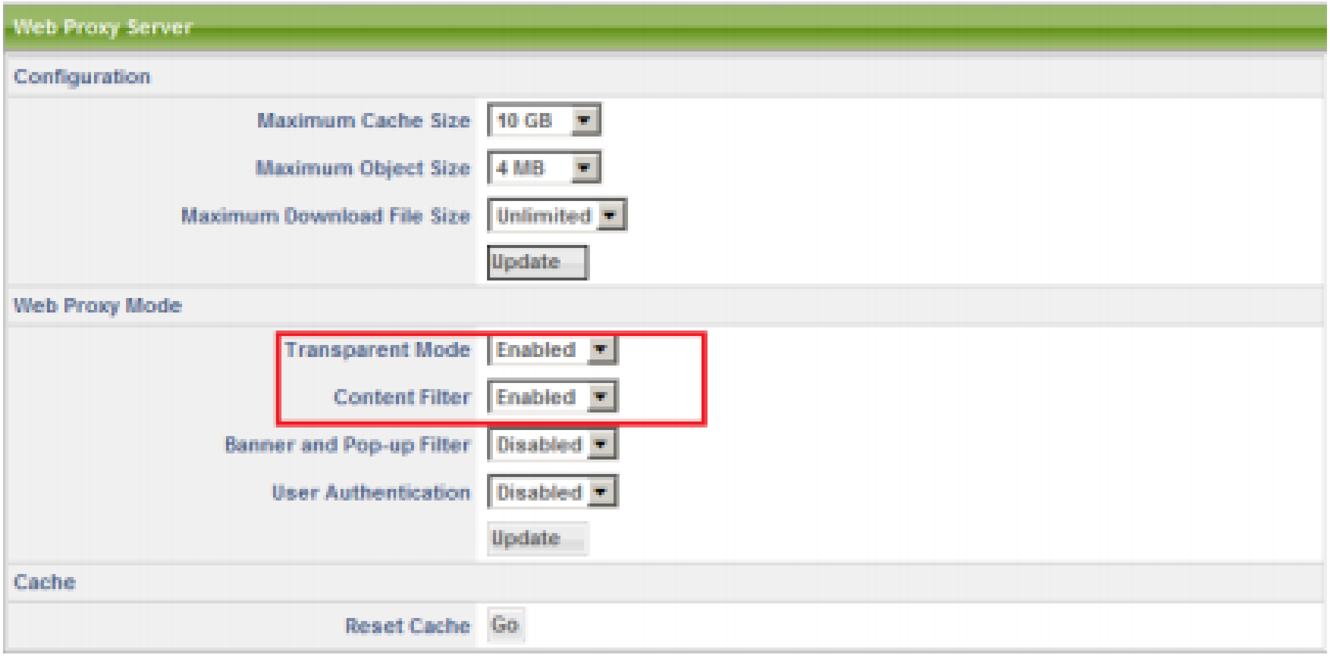


Standard Services

Service	Status	On boot	
Antimalware Updates	Running	Automatic	Configure
Content Filter	Running	Automatic	Configure
DHCP / Caching DNS	Running	Automatic	Configure
Protocol Filter	Stopped	Manual	Configure
Time Server	Stopped	Manual	Configure
Web Proxy	Running	Automatic	Configure

Figure 15. Web Proxy and Content Filter

- Step 2: Configure Web Proxy at Transparent Mode and enable Content Filter. In this mode all requests from local traffics will go through Proxy Server and local users will not have to configure anything, it is invisible to them.



Web Proxy Server

Configuration

Maximum Cache Size	10 GB
Maximum Object Size	4 MB
Maximum Download File Size	Unlimited

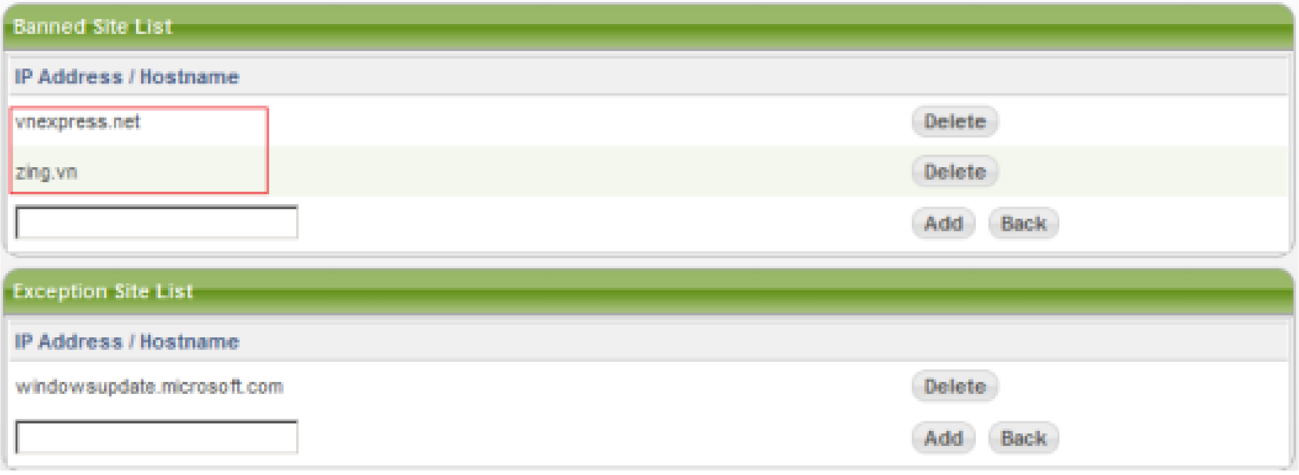
Web Proxy Mode

Transparent Mode	Enabled
Content Filter	Enabled
Banner and Pop-up Filter	Disabled
User Authentication	Disabled

Cache

Figure 16. Web Proxy Transparent Mode

- Step 3: Create rules in a Content filter module to block sites http://zing.vn and http://vnexpress.net by adding these two websites to the banned site list.



Banned Site List

IP Address / Hostname

vnexpress.net

zing.vn

Exception Site List

IP Address / Hostname

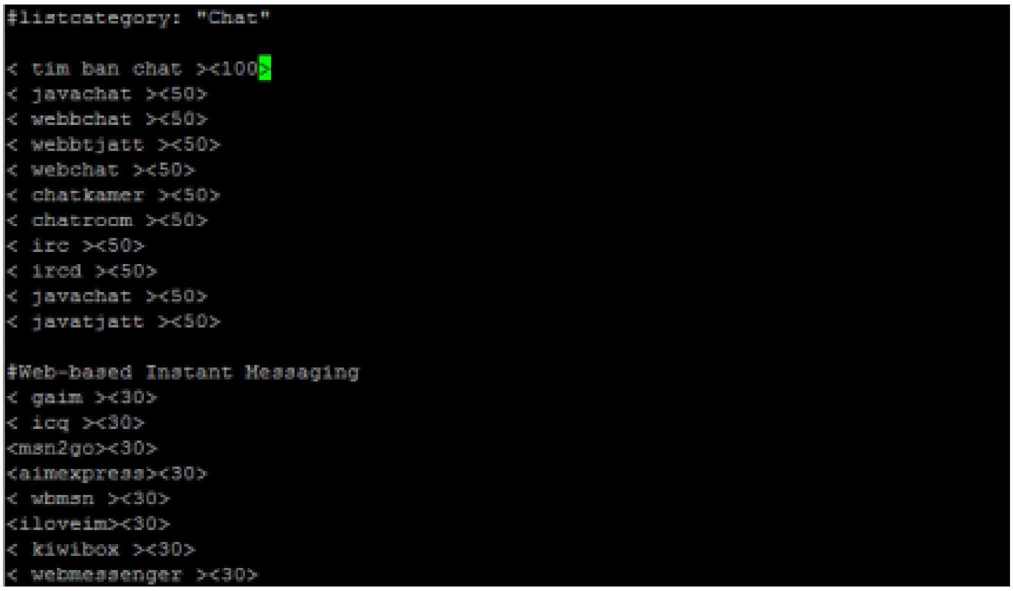
windowsupdate.microsoft.com

Figure 17. Adding Domain Block

- Step 4: Content Filter prevent users from accessing websites with certain phrases (by default ClearOS has already defined some common words and phrases like chat, games, news, pornographic contents).

We can also add new phrases to the list by SSH to ClearOS and modify weighted files with root privileges as illustrated in Figure 18.

```
vi /etc/dansguardian-av/lists/phraselists/chat/weighted
```



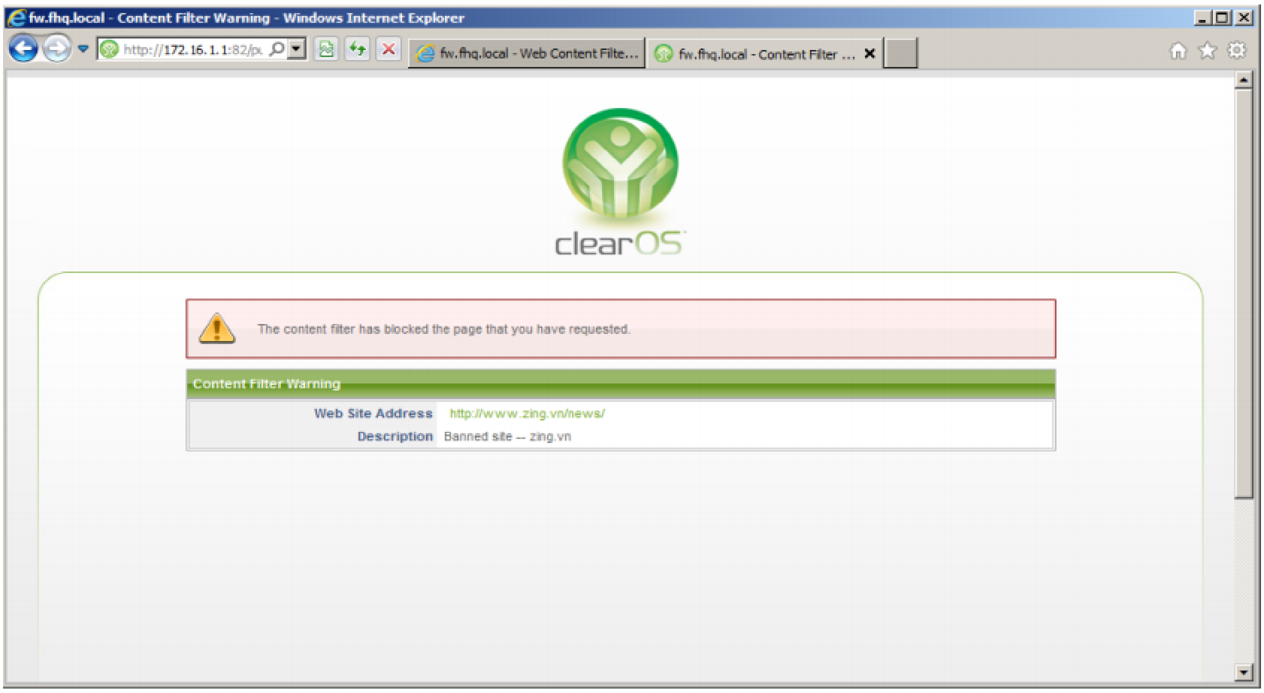
```
#listcategory: "Chat"

< tim ban chat ><100>
< javachat ><50>
< webbchat ><50>
< webbtjatt ><50>
< webchat ><50>
< chatkamer ><50>
< chatroom ><50>
< irc ><50>
< ircd ><50>
< javachat ><50>
< javatjatt ><50>

#Web-based Instant Messaging
< gaim ><30>
< icq ><30>
<msn2go><30>
<aimexpress><30>
< wbmsn ><30>
<iloveim><30>
< kiwibox ><30>
< webmessenger ><30>
```

Figure 18. Modify weighted files

An administrator can increase the filter level to 100 for a higher level of restriction. After modifying, it is required to restart the corresponding service, which is the dansguardian-av service with the following command:

```
    ./etc/init.d/dansguardian-av restart
```

All the commands to modify the weighted files and restart the dansguardian-av service must be executed in root privileges. After all the commands had been launched and the service restarted, the administrator can test for the result. Figure 20 shows that Local users cannot access two domains http://zing.vn and http://vnexpress.net .


fw.fhq.local - Content Filter Warning - Windows Internet Explorer
http://172.16.1.1:82/p
fw.fhq.local - Web Content Filte...
fw.fhq.local - Content Filter ...
clearOS

The content filter has blocked the page that you have requested.

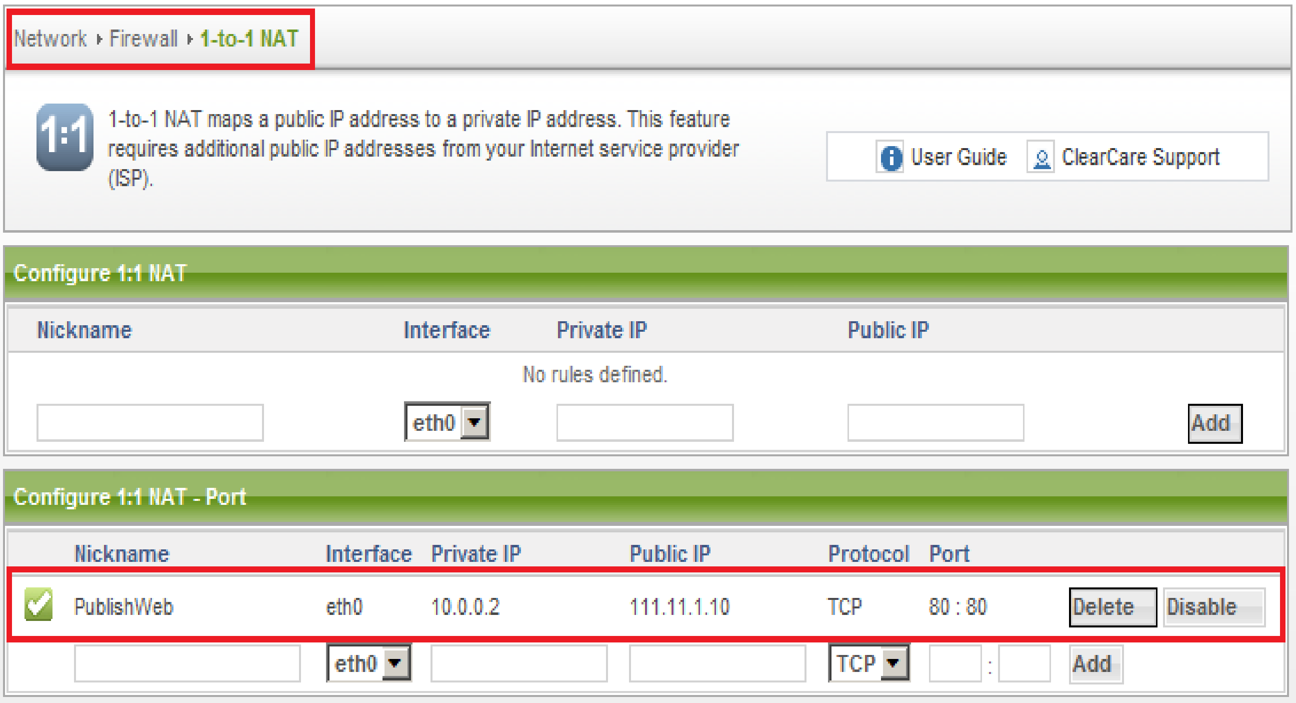
Content Filter Warning

Web Site Address	http://www.zing.vn/news/
Description	Banned site -- zing.vn

Figure 20. Test domain http://http.zing.vn

6.2.3. Publishing Web Server on the Internet

In the demo topology, the organization has a Web Server located in the DMZ. In order to allow customers and partners accessing the Web Server, the administrator needs to configure one public address to reach the Web Server in the DMZ. The administrator can perform this task by initiating the 1-to-1 NAT service in Firewall menu as show in Figure 22.



Network › Firewall › 1-to-1 NAT

1-to-1 NAT maps a public IP address to a private IP address. This feature requires additional public IP addresses from your Internet service provider (ISP).

Configure 1:1 NAT

Nickname	Interface	Private IP	Public IP	
		No rules defined.		
	eth0			Add

Configure 1:1 NAT - Port

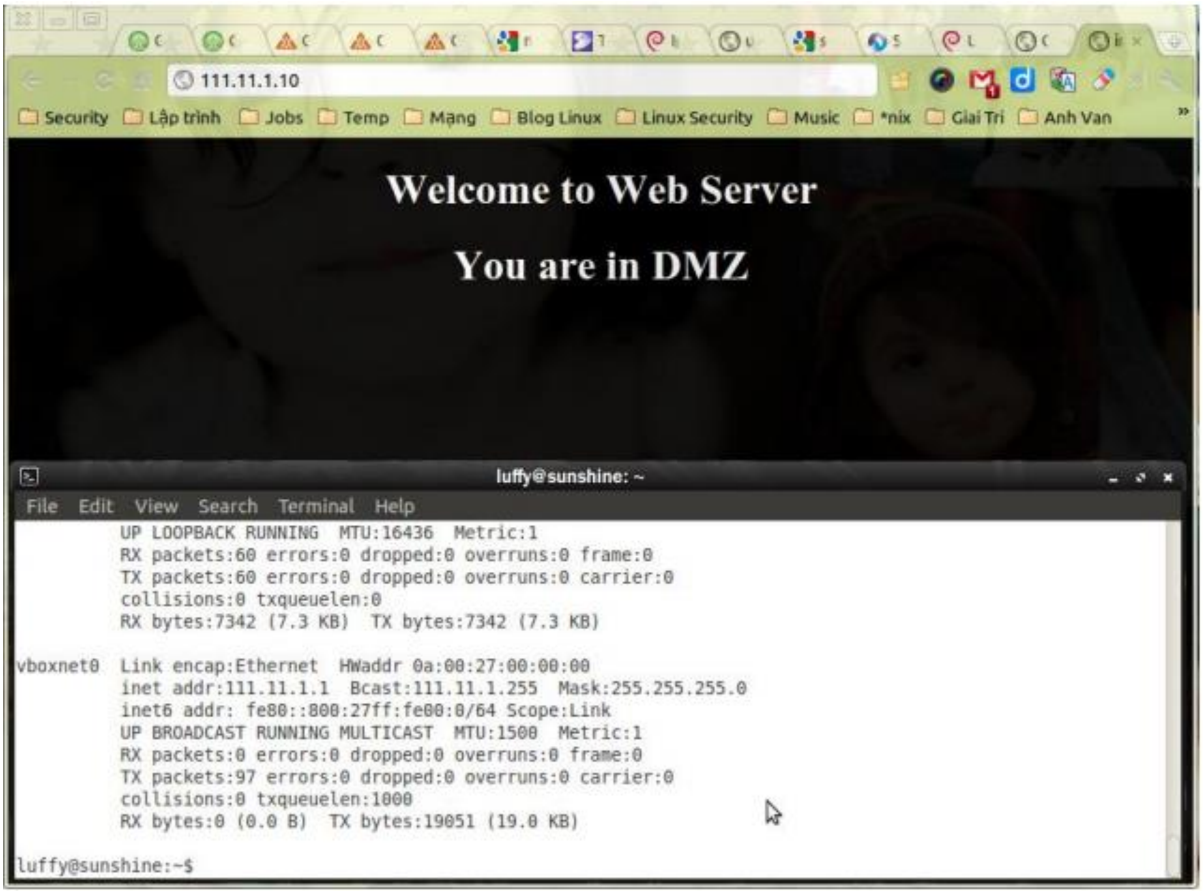
	Nickname	Interface	Private IP	Public IP	Protocol	Port	
✓	PublishWeb	eth0	10.0.0.2	111.11.1.10	TCP	80 : 80	Delete Disable
		eth0			TCP	:	Add

Figure 22. 1-to-1 NAT Configuration

Parameters for establishing a 1-to-1 NAT service includes following:

- Nickname: optional
- Interface: external a firewall interface, the one connect with the Internet (according to the demo topology it will be eth0).
- Private IP: the IP address of Web Server in DMZ.
- Public IP: IP address of external a firewall interface.
- Protocol: TCP
- Port: 80:80 (HTTP)

Once all the parameters had been filled in, the administrator can test whether Users can access Web Server from an User workstation with IP address 111.11.1.1 (according to Demo Topology). As shown in Figure 23, an User workstation with IP address 111.11.1.1 can access Web Server in DMZ through the external a firewall interface with IP address 111.11.1.10



Welcome to Web Server

You are in DMZ

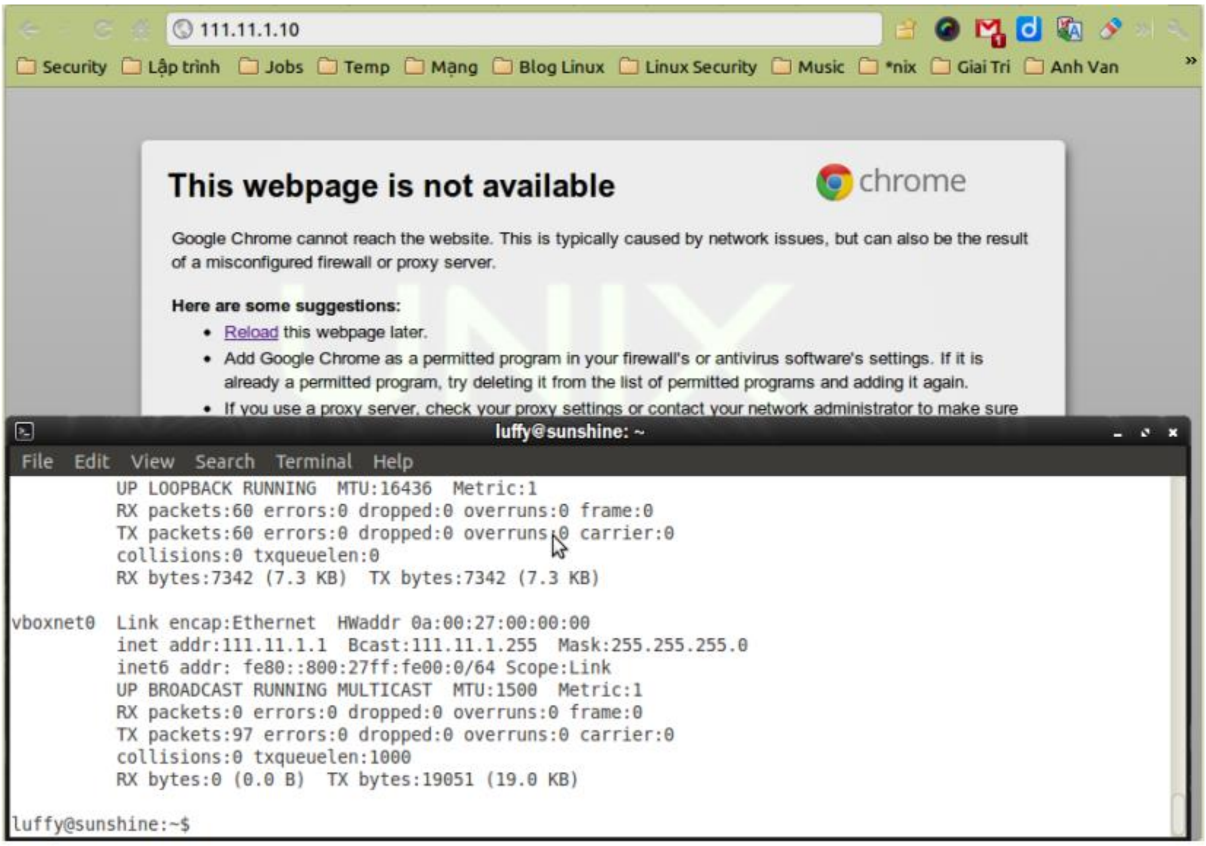
```
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:60 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:7342 (7.3 KB)  TX bytes:7342 (7.3 KB)

vboxnet0  Link encap:Ethernet  HWaddr 0a:00:27:00:00:00
          inet addr:111.11.1.1  Bcast:111.11.1.255  Mask:255.255.255.0
          inet6 addr: fe80::800:27ff:fe00:0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:19051 (19.0 KB)

luffy@sunshine:~$
```

Figure 23. Testing Web Server access

6.2.4. Rule Sets for Web Server

In this case study, the administrator noticed a couple of Public IP addresses from the Internet usually access the website and forum for spamming, vandalism and malicious mischief. It is important to block these Public IP addresses from accessing organization’s website and forum, while other users can normally access them. In this experiment User (a role in demo topology with IP address 111.11.1.1) will be blocked.

Firstly, the administrator choose Firewall from menu Network, then choose option Incoming. From this option there is a section called Blocked External Hosts which will be used to block an IP address of the User. The administrator can also block the whole subnet by replacing IP address 111.11.1.1 with the subnet, for example: 111.11.1.0/24. After finishing, the administrator can test whether a connection from User workstation can access the external firewall interface (eth0). Figure 25 shows the result of testing phase.



This webpage is not available

Google Chrome cannot reach the website. This is typically caused by network issues, but can also be the result of a misconfigured firewall or proxy server.

Here are some suggestions:

- Reload this webpage later.
- Add Google Chrome as a permitted program in your firewall's or antivirus software's settings. If it is already a permitted program, try deleting it from the list of permitted programs and adding it again.
- If you use a proxy server, check your proxy settings or contact your network administrator to make sure

```
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:60 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:7342 (7.3 KB)  TX bytes:7342 (7.3 KB)

vboxnet0  Link encap:Ethernet  HWaddr 0a:00:27:00:00:00
          inet addr:111.11.1.1  Bcast:111.11.1.255  Mask:255.255.255.0
          inet6 addr: fe80::800:27ff:fe00:0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:19051 (19.0 KB)

luffy@sunshine:~$
```

Figure 24. Blocking Public IP address result

As we can see in Figure 24, after configuring to block the User's IP address, User can no longer be able to access Web Server. This blocking setting can be easily undone and added through a web interface.

6.2.5. SSH to A firewall from the Internet

In practical, the administrator cannot always be present at the company to access the network system. The administrator need to use SSH from the Internet to the network. Besides that at the company, only the administrator workstation can SSH to the a firewall, other workstations are prohibited. To ensure the security for the system, the administrator establish a rule which only allows a certain IP address to access the firewall through SSH protocol from the Internet.

In this instance, only IP address 111.11.1.101 from the Internet and IP address 172.16.1.100 of Administrator are allowed to SSH to the A firewall, all others are blocked

The administrator needs to add rules to the iptables script as follow :

- Step 1: Block all IP from SSH to the A firewall with the following rule

```
iptables - | INPUT -p tcp --dport 22 -j DROP
```

- Step 2: Allow IP 111.11.1.101 SSH to the A firewall with the following rule

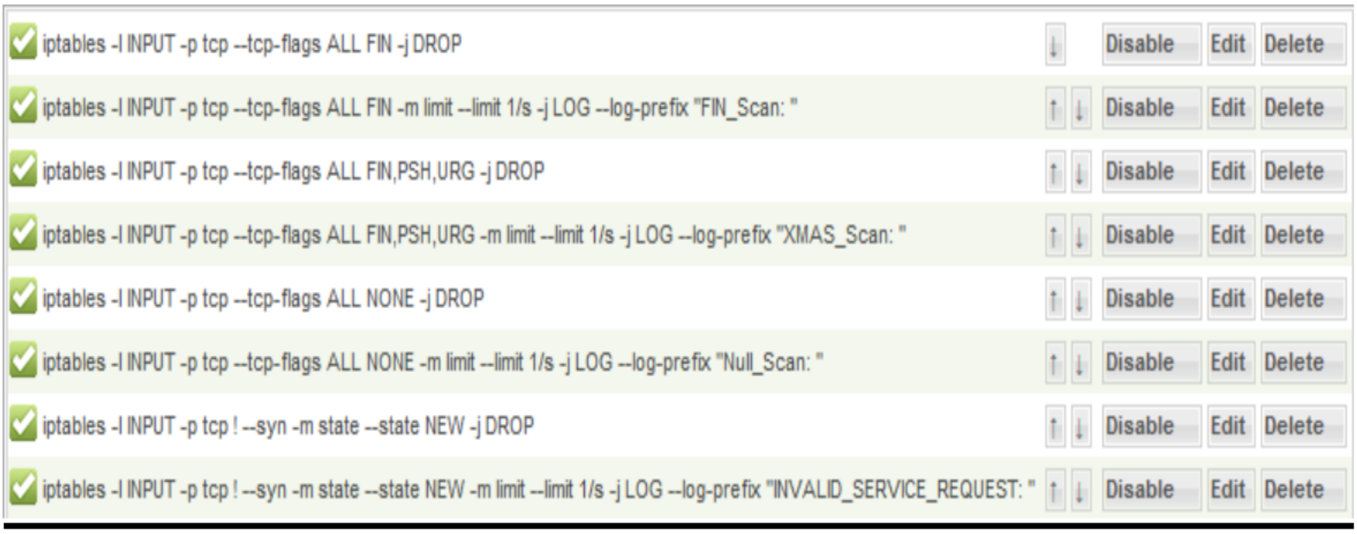
```
iptables - | INPUT -p tcp -source 111.11.1.101 --dport 22 -j ACCEPT
```

- Step 3: Allow Administrator’s IP 172.16.1.100 SSH to the A firewall with the following rule

```
iptables - | INPUT -p tcp -source 172.16.1.100 --dport 22 -j ACCEPT
```

6.2.6. Blocking Scan Port using Nmap

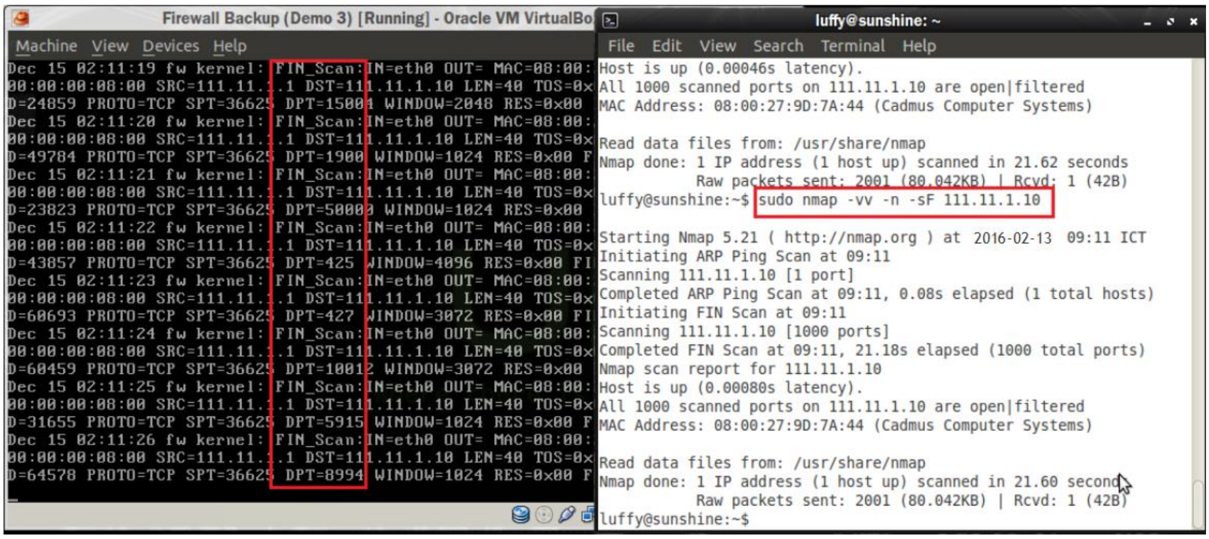
Hackers usually use tool like NMap to scan ports on public servers like Web server or Mail server to find out the excess open ports to exploit. There are several scan types such as FIN Scan (-sF), Xmas Scan (-sX), Null Scan (-sN), Ack Scan (-sA). In order to block those scans, the administrator needs to know the characteristics of each scan port types. After recognized the scan port types, the administrator can set rules for the firewall in the Custom section. Figure 26 below shows all the rules configured for blocking the scan port using NMap.



```
iptables -I INPUT -p tcp --tcp-flags ALL FIN -j DROP
iptables -I INPUT -p tcp --tcp-flags ALL FIN -m limit --limit 1/s -j LOG --log-prefix "FIN_Scan: "
iptables -I INPUT -p tcp --tcp-flags ALL FIN,PSH,URG -j DROP
iptables -I INPUT -p tcp --tcp-flags ALL FIN,PSH,URG -m limit --limit 1/s -j LOG --log-prefix "XMAS_Scan: "
iptables -I INPUT -p tcp --tcp-flags ALL NONE -j DROP
iptables -I INPUT -p tcp --tcp-flags ALL NONE -m limit --limit 1/s -j LOG --log-prefix "Null_Scan: "
iptables -I INPUT -p tcp ! --syn -m state --state NEW -j DROP
iptables -I INPUT -p tcp ! --syn -m state --state NEW -m limit --limit 1/s -j LOG --log-prefix "INVALID_SERVICE_REQUEST: "
```

Figure 26. Rules for blocking scan port using NMap

After all the rules have been established, the administrator tests how the firewall respond to the scan port by using NMap to perform a FIN Scan on Web Server (111.11.1.10) as shown in Figure 27 below.


Firewall Backup (Demo 3) [Running] - Oracle VM VirtualBo
Machine View Devices Help
luffy@sunshine: ~
File Edit View Search Terminal Help

```
Dec 15 02:11:19 fw kernel: FIN_Scan:IN=eth0 OUT= MAC=08:00:
00:00:00:08:00 SRC=111.11.1.1 DST=111.11.1.10 LEN=40 TOS=0x
D=24859 PROTO=TCP SPT=36625 DPT=15004 WINDOW=2048 RES=0x00
Dec 15 02:11:20 fw kernel: FIN_Scan:IN=eth0 OUT= MAC=08:00:
00:00:00:08:00 SRC=111.11.1.1 DST=111.11.1.10 LEN=40 TOS=0x
D=49784 PROTO=TCP SPT=36625 DPT=1900 WINDOW=1024 RES=0x00 F
Dec 15 02:11:21 fw kernel: FIN_Scan:IN=eth0 OUT= MAC=08:00:
00:00:00:08:00 SRC=111.11.1.1 DST=111.11.1.10 LEN=40 TOS=0x
D=23823 PROTO=TCP SPT=36625 DPT=50000 WINDOW=1024 RES=0x00
Dec 15 02:11:22 fw kernel: FIN_Scan:IN=eth0 OUT= MAC=08:00:
00:00:00:08:00 SRC=111.11.1.1 DST=111.11.1.10 LEN=40 TOS=0x
D=43857 PROTO=TCP SPT=36625 DPT=425 WINDOW=4096 RES=0x00 FI
Dec 15 02:11:23 fw kernel: FIN_Scan:IN=eth0 OUT= MAC=08:00:
00:00:00:08:00 SRC=111.11.1.1 DST=111.11.1.10 LEN=40 TOS=0x
D=60693 PROTO=TCP SPT=36625 DPT=427 WINDOW=3072 RES=0x00 FI
Dec 15 02:11:24 fw kernel: FIN_Scan:IN=eth0 OUT= MAC=08:00:
00:00:00:08:00 SRC=111.11.1.1 DST=111.11.1.10 LEN=40 TOS=0x
D=60459 PROTO=TCP SPT=36625 DPT=10012 WINDOW=3072 RES=0x00
Dec 15 02:11:25 fw kernel: FIN_Scan:IN=eth0 OUT= MAC=08:00:
00:00:00:08:00 SRC=111.11.1.1 DST=111.11.1.10 LEN=40 TOS=0x
D=31655 PROTO=TCP SPT=36625 DPT=5915 WINDOW=1024 RES=0x00 F
Dec 15 02:11:26 fw kernel: FIN_Scan:IN=eth0 OUT= MAC=08:00:
00:00:00:08:00 SRC=111.11.1.1 DST=111.11.1.10 LEN=40 TOS=0x
D=64578 PROTO=TCP SPT=36625 DPT=8994 WINDOW=1024 RES=0x00 F
```

```
Host is up (0.00046s latency).
All 1000 scanned ports on 111.11.1.10 are open|filtered
MAC Address: 08:00:27:9D:7A:44 (Cadmus Computer Systems)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.62 seconds
           Raw packets sent: 2001 (80.042KB) | Rcvd: 1 (42B)
luffy@sunshine:~$ sudo nmap -vv -n -sF 111.11.1.10

Starting Nmap 5.21 ( http://nmap.org ) at 2016-02-13 09:11 ICT
Initiating ARP Ping Scan at 09:11
Scanning 111.11.1.10 [1 port]
Completed ARP Ping Scan at 09:11, 0.08s elapsed (1 total hosts)
Initiating FIN Scan at 09:11
Scanning 111.11.1.10 [1000 ports]
Completed FIN Scan at 09:11, 21.18s elapsed (1000 total ports)
Nmap scan report for 111.11.1.10
Host is up (0.00080s latency).
All 1000 scanned ports on 111.11.1.10 are open|filtered
MAC Address: 08:00:27:9D:7A:44 (Cadmus Computer Systems)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.60 seconds
           Raw packets sent: 2001 (80.042KB) | Rcvd: 1 (42B)
luffy@sunshine:~$
```

Figure 27. FIN Scan testing

The command to perform FIN Scan using NMap is:

```
Sudo nmap -vv -n -sF 111.11.1.10
```

As shown in Figure 27, when hackers use a scan port tool like NMap and scan the Web Server, the firewall will detect, inform and block those scans. Other scan port testing with XMAS Scan, NULL Scan and ACK Scan are all blocked by the firewall.

6.2.7. Counteract DoS and DDoS

Nowadays, DoS and DDoS are commonly used to sabotage a server. Attackers flood a massive number of packets to the Web server freezing the system and make it unable to provide normal service for users. There are some common attack forms like SYN Flood, ICMP Flood. The administrator can prevent DoS and DDoS attacks by limit the amount of request per second, filter out those IPs flooding the server.

In this experiment, I chose to establish rules against SYN Flood by adding rules to the iptables script as follow:

```
iptables –N syn_flood
iptables –A INPUT –p tcp –syn –j syn_flood
iptables –A syn_flood –m limit –limit 1/s –limit-burst 3 –j RETURN
iptables –A syn_flood –j DROP
```

With the above rules, all incoming connections are allowed until the limit is reached:

- --limit 1/s: Maximum average matching rate is 1 second.
- --limit-burst 3: maximum initial number of packets to match is 3.

The administrator can test for result by using Attacker workstation (Kali Linux OS) to perform following command:

```
# hping3 –flood –S –p 80 111.11.1.10
```

hping3: a tool to send packet with difference options
--flood: send packet with flooding speed
-S: packet with SYN flag
-p 80: send to port 80 of the A firewall, where A firewall will use NAT inbound to connect to Web server in DMZ.
111.11.1.10: A firewall external interface’s IP address (eth0).
On the Web server we can use tcpdump (command) or Wireshark (graphic) to catch packets and analyse.

`# tcpdump –ni eth0 port 80`: catch packets going to eth0 at port 80.

7. Conclusion

The goal of this project was to gain knowledge about a firewall as well as threats to the computer network security and deployment of ClearOS an open source Linux firewall. This thesis includes theoretical background of a firewall and network security as well as a study case about real life situations which administrators have to deal with. Those practical situations consisted of blocking certain IPs accessing the Web servers, only allowing one local and one external IP to access and administer a firewall, preventing a scan port with Nmap, establishing rules for countering DoS.

In general, setting rules on a web interface enables the administrator to easily create rules and administer them visually. But an experienced administrator should not be constrained in setting rules on a web interface. The experiments in the Chapter 6 are just only the most frequent, common and the most needed ones to be established. Depending on the specific situation, such as data, services needed to be protected and network architecture of the organization the administrator can create new rules that meet those requirements.

However, due to the limitation of the time to study and implement the project, as well as the deployment on virtual machines, other sophisticated and complex attacks could not be tested. DoS attacks mentioned in Chapter 6 are just the basic types which hackers execute at the IP layer of the TCP/IP model. Very likely hackers will use more complex and sophisticated attacking methods and unfortunately I do not have the resources and time to deploy and test them. Some other useful features of ClearOS which were not implemented in this study are Antivirus, Antiphising with integrated modules like ClamAV, Bandwidth management and QoS. All the mentioned problems above can be studied further. In addition, it is also possible to study and deploy the ClearOS in practical situations with other features like VPN, LDAP authentication, and Snort intrusion detection.

References

1. Contegix. A firewall and VPN services.

   URL: http://www.contegix.com/products/a firewall-vpn-services/
   Accessed 12 January 2016

2. B. Fraser Networking Group. RFC 2196. Site security handbook.
   URL: https://www.ietf.org/rfc/rfc2196.txt.Accessed 12 January 2016

3. Vacca JR. Practical Internet security. USA: Springer; 2007.

4. Whitman ME, Mattord HJ, Green A. Guide to A firewalls and VPNS, 3rd edition. Boston, MA: Course Technology, Cengage learning; 2012

5. Henmi A, Lucas M, Singh A, Cantrell C. A firewall Policies and VPN Configurations. Rockland, MA: Syngress Publishing, Inc; 2006

6. Whitman ME, Mattord HJ, Mackey D, Green A. Guide to network security. Boston, MA: Course Technology, Cengage learning; 2013

7. Harris S. CISSP All in One Exam Guide, 6th edition. US: McGraw-Hill Companies; 2013

8. Kizza JM. Computer Network Security. New York: Springer Science+Business Media Inc; 2005

9. Bastien G, Degu CA. CCSP Cisco Secure PIX A firewall Advanced Exam Certification Guide. Indianapolis: Cisco Press; 2003

10. Whitaker A, Newman D. Penetration Testing and Network Defense. Indianapolis: Cisco Press; 2006

11. Isaac DS, Isaac ML. SSCP Prep Guide: Mastering the Seven Key Areas of System Security. Indianapolis: Wiley Publishing; 2003

12. Nothcutt S, Zeltser L, Winters S, Kent K, Ritchey RW. Inside Network Perimeter Security, 2nd edition. US: Sams Publishing, 2005

13. Santos O. End-to-End Network Security Defense-in-Depth. Indianapolis: Cisco Preess; 2008

14. ClearOS Community Dashboad. Going back to Our Red Hat Roots.

    URL: https://www.clearos.com/clearfoundation/social/community-dashboard/entry/going-back-to-our-red-hat-roots

    Accessed 03 February 2016

15. Best Security tips. Stateful Packet Inspection A firewalls.
    URL: http://www.bestsecuritytips.com/xfsection+article.articleid+2.htm
    Accessed 28 January 2016