



VAASAN AMMATTIKORKEAKOULU  
VASA YRKESHÖGSKOLA  
UNIVERSITY OF APPLIED SCIENCES

Odunmbaku Sulaimon Abiola

Olusanya Foluseke Adurasanmi

**NETWORK ADMINISTRATION -  
INSTALLATION AND CONFIGURATION OF  
eBOX PLATFORM**

Technology and Communication  
2010

## **ACKNOWLEDGEMENTS**

Our sincere gratitude goes to God Almighty and to the Finnish government for given us the privilege to study in Vaasa, Finland. They have enriched us with sufficient knowledge to make our live meaningful. Many thanks.

Thanks goes to the teachers that have given us support in one form or the other throughout our academy years in VAMK. Although it has been a long way with them but we appreciate their impact in our life.

We will not forget to thank our supervisors, Rainer Lytz (technical) and Johan Dams (administrative) for their support and encouragement during this project.

To our friends and colleagues who have shown support one way or the other towards the successful completion of this project.

Thanks also to the eBox administrative members and eBox forum members for their support and assistance during this project.

Also, big thanks to our parents, the Odunmbaku family and Olusanya family for their total support financially, morally and other aspects.

We will not but thank Almighty God for given us good health throughout our study time in VAMK. He has been of help to us in every aspect of our lives. Although the journey was rough and tough, He has been a guiding light to our paths. Glory to His name.

*Thank you!*

Odunmbaku Sulaimon  
Olusanya Foluseke

May 2010

**ABSTRACT**

Author	Odunmbaku Sulaimon Abiola Olusanya Foluseke Adurasanmi
Title	Network Administration – Installation and Configuration of eBox Platform
Year	2010
Language	English
Pages	93
Name of Supervisor	Johan Dams

---

This thesis is centered to investigate the functionality of eBox platform for Vcross OpenSource Information Technology laboratory at Vaasa University of Applied Sciences in Vaasa, Finland. The purpose of this research is to evaluate the functionality of eBox platform and subsequently recommend the technology to Small Enterprises in Africa with maximum of 500 users.

In the course of the investigation, eBox platform will be installed and configured. The configuration will be made for a modeled small educational institution with about thirty network users. All necessary network services suited for educational purpose would be installed and configured.

# CONTENTS

ACKNOWLEDGEMENTS .....	1
LIST OF TABLES .....	8
ABBREVIATIONS .....	9
1 INTRODUCTION.....	11
1.1 BACKGROUND .....	11
1.1.1 TCP/IP Networks .....	11
1.1.2 UUCP Networks .....	12
1.1.3 Linux Networking.....	13
1.1.4 System Maintenance.....	13
2 COMPUTER NETWORK ADMINISTRATION .....	15
2.1 TYPES OF COMPUTER NETWORK .....	15
2.2 NETWORK TOPOLOGY .....	17
2.2.1 Mesh Topology.....	17
2.2.2 Star Topology .....	18
2.2.3 Bus Topology .....	19
2.2.4 Ring Topology.....	20
2.3 COMPUTER NETWORK PLANNING .....	21
3 SMALL AND MEDIUM ENTERPRISES NETWORK MODELLING.....	25
3.1 ENTERPRISE ORGANIZATION ARCHITECTURE.....	25
3.2 ENTERPRISE NETWORK REQUIREMENT .....	26
4. EBOX TECHNOLOGIES SL.....	28
4.1 eBOX PLATFORM, VERSION 4.....	28
4.2 eBOX CONTROL CENTER.....	36
5. INSTALLATION AND CONFIGURATION OF EBOX PLATFORM FOR ENTERPRISE.....	38
5.1 eBox CORE .....	38
5.1.1 Logs .....	38
5.1.2 Monitoring.....	40
5.1.3 Events and Alerts.....	43

5.1.4	Backup.....	44
5.1.5	Software Managements .....	44
5.2	eBox GATEWAY .....	46
5.2.1	High Level eBox Network Abstraction.....	46
5.2.2	Firewall.....	51
5.2.3	Routing .....	54
5.2.4	Traffic Shaping.....	55
5.2.5	HTTP Proxy Setting .....	55
5.3	eBox INFRASTRUCTURE.....	55
5.3.1	Network Configuration Service (DHCP) .....	56
5.3.2	Name Resolution Service (DNS) .....	58
5.3.4	Time Synchronization Service (NTP) .....	65
5.4	eBox OFFICE .....	65
5.4.1	Directory Service (LDAP).....	66
5.4.2	File Sharing Service and Remote Authentication .....	72
5.4.3	Printer Sharing Service.....	76
5.4.4	eGroupware Service .....	76
5.5	eBOX UNIFIED COMMUNICATIONS .....	79
5.5.1	Electronic Mail Service .....	79
5.5.2	Instant Messaging (IM) Service .....	82
5.5.3	Voice over IP Service.....	87
5.6	eBOX UNIFIED THREAT MANAGER .....	87
5.6.1	Mail Filter.....	87
5.6.2	HTTP Proxy Advanced Configuration.....	88
5.6.3	Secure Interconnection between Local Networks .....	94
5.6.4	Intrusion Detection System (IDS) .....	99
6.	CONCLUSION, CHALLENGES AND RECOMMENDATION .....	101
6.1	Conclusion .....	101
6.2	Challenges.....	101
6.3	Recommendations.....	102
	REFERENCES .....	103

## LIST OF FIGURES

Figure 3.1 – Modelled Network Architecture Diagram	25
Figure 5.1 – <i>Logs</i> full report of IDS service	40
Figure 5.2 – System load monitored by the <i>Monitor</i> module	41
Figure 5.3 – eBox component latest available version	45
Figure 5.4 – System Update	46
Figure 5.5 – Network Objects created	47
Figure 5.6 – Network Objects created	47
Figure 5.7 – Management network object configuration	48
Figure 5.8 – Non-Teachers network object configuration	48
Figure 5.9 – Teachers network object configuration	48
Figure 5.10 – Student network object configuration	49
Figure 5.11 – Network Services created and configured	50
Figure 5.12 – Asterik Service configuration	50
Figure 5.13 – HTTP Service configuration	51
Figure 5.14 – Packet filtering rules from <i>Internal network to eBox</i>	52
Figure 5.15 – Log of <i>ssh</i> connection denial by firewall traffic from <i>external network to eBox</i>	53
Figure 5.16 – Configured eBox gateway	54
Figure 5.17 – eBox Infrastructure modules activation	56
Figure 5.18 – eth0 Interface configuration	57
Figure 5.19 – eth1 Interface configuration	57
Figure 5.20 – DHCP configuration on eth1	58
Figure 5.21 – Domain Name Server list	59
Figure 5.22 – <i>sulazhy.com</i> domain name	59
Figure 5.23 – Hostname in <i>sulazhy.com</i> domain	60
Figure 5.24 – Firewall configuration to allow http in Internal Network	60
Figure 5.25 – <i>ping</i> result to <i>www.google.com</i>	61
Figure 5.26 – <i>traceroute</i> result to <i>www.google.com</i>	61
Figure 5.27 – <i>nslookup</i> result to <i>www.google.com</i>	62
Figure 5.28 – <i>nslookup</i> result of <i>www.google.com</i> from user <i>aa@sulazhy.com</i> computer	62
Figure 5.29 – Default listening port of HTTP (Port 80)	63
Figure 5.30 – Test of Apache Web Server in eBox on default port 80	64
Figure 5.31 – Listening port of HTTP changed to Port 1600	64
Figure 5.32 – Test of Apache Web Server in eBox on Port 1600	64

Figure 5.34 – Created Groups on sulazhy.com domain	67
Figure 5.35 – Created Users on sulazhy.com domain	68
Figure 5.36 – Management group configuration	69
Figure 5.37 – User (Alan Gate) Configuration	70
Figure 5.38 – User Corner address link	71
Figure 5.39 – User Corner available services	71
Figure 5.40 – File Sharing Configuration	72
Figure 5.41 – Shared Directory for each group	73
Figure 5.42 – Management Group Shared Directory Access Control	73
Figure 5.43 – Teachers Group Shared Directory Access Control	74
Figure 5.44 – Non Teacher Group Shared Directory Access Control	74
Figure 5.45 – Student Group Shared Directory Access Control	74
Figure 5.46 – Mounted personal directory and Shared Directories	75
Figure 5.47 – List of installed printers	76
Figure 5.48 – Virtual domain ( <i>sulazhy.com</i> ) selected	77
Figure 5.49 – Allowed application in eGroupware default template	78
Figure 5.50 – eGroupware login page	78
Figure 5.51 – Configuration of eBox as a mail server	80
Figure 5.52 – Network object relay policy	81
Figure 5.53 – Virtual domain <i>sulazhy.com</i> created	81
Figure 5.54 – Mail service tested	82
Figure 5.55 – IM Jabber configuration	83
Figure 5.56 – <i>Basic</i> tab configuration of Jabber/XMPP IM client	83
Figure 5.57 – <i>Advanced</i> tab configuration of Jabber/XMPP IM client	84
Figure 5.58 – <i>Proxy</i> tab configuration of Jabber/XMPP IM client	85
Figure 5.59 – Account <i>ba@sulazhy.com</i> created on pidgin installed on the computer	85
Figure - 5.60 – Group and friend list	86
Figure 5.62 – Sample instance messaging chat with <i>sg@sulazhy.com</i>	87
Figure 5.65 – <i>File extension filtering</i> tab of the <i>Default filter profile</i>	90
Figure 5.66 – <i>MIME types filtering</i> tab of the <i>Default filter profile</i>	91
Figure 5.67 – <i>Domain filtering</i> tab of the <i>Default filter profile</i>	92
Figure 5.68 – <i>File extension filtering</i> tab of the <i>Teachers filter profile</i>	93
Figure 5.69 – <i>MIME types filtering</i> tab of the <i>Teachers filter profile</i>	93
Figure 5.70 – <i>Domain filtering</i> tab of the <i>Teachers filter profile</i>	94
Figure 5.71 – <i>Certificate Authority</i> certificate and Client certificates	95

Figure 5.72 – Created and enabled eBox OpenVPN Server	96
Figure 5.73 – eBox OpenVPN Server Configuration	96
Figure 5.74 1 – Advertised Network of eBox OpenVPN	97
Figure 5.75 – eBox OpenVPN Clientt Bundle Download	98
Figure 5.77 – eBox OpenVPN Client Connection	99
Figure 5.78 – nmap to eth0 (external interface)	100
Figure 5.79 – IDS Query log report of nmap connection	100



## LIST OF TABLES

Table 5. 1 .....	66
Table 5. 2 .....	66
Table 5. 3 .....	66
Table 5. 4 .....	67

## ABBREVIATIONS

OS	Operating System
TCP/IP	Transmission Control Protocol/Internet Protocol
UUCP	Unit-to-unit Copy Protocol
IPX	Internet Packages Exchange
WAN	Wide Area Network
LAN	Local Area Network
MAN	Metropolitan Area Network
MAC	Media Access Control Address
CSMA/CD	Carrier Sense Multiple Access with Collision Avoidance
DSL	Digital Subscriber Line
CAN	Controller Area Network
HAN	Home Area Network
ATM	Asynchronous Transfer Mode
ISP	Internet Service Provider
FDDI	Fiber Distributed Data Interface
SMDS	Switched Multimegabit Data Service
PPPoE	Point-to-point Protocol over Ethernet
VLAN	Virtual Local Area Network
NAT	Network Address Translation
DMI	Desktop Management Interface.
QoS	Quality of Service
HTTP	Hypertext Transfer Protocol
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol.
LDAP	Lightweight Directory Access Protocol
I/O	Input and Output
FTP	File Transfer Protocol
UTM	Unified Threat Management
IMAP	Internet Message Access Protocol
XMPP	Extensible Messaging and Presence Protocol
ERM	Enterprise Resource Management
IM	Instant Messaging

DMZ	Demilitarized Zone
SSL	Secure Socket Layer
VoIP	Voice-over Internet Protocol
NTP	Network Time Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network
IDS	Intrusion Detection System
CPU	Central Processing Unit
RAID	Redundant Array of Independent Disks.
ACPI	Advanced Configuration and Power Interface.
SSH	Secure Shell
HTTPS	HyperText Transfer Protocol Secure
TLS	Transport Layer Security
SMB/CIFS	Server Message Block (Common Internet File System)
PDC	Primary Domain Controller
MIME	Multipurpose Internet Mail Extensions
CA	Certificate Authority
UDP	User Datagram Protocol
NIDS	Network Intrusion Detection Systems

# 1 INTRODUCTION

Networking is a concept with history probably as far as twenty five decades ago when people communicate using smoke signals and talking drums. For instance, consider two people, John and Janet in the olden days living far from each other. If John wishes to invite Janet, he could bang his drum to call the attention of Janet. But if they live too far apart, a possibility is to get a bigger drum, walk down to Janet or ask another person who lives between them to forward the message to Janet. Forwarding the message through a third party is called *networking*.

However, it was not until 1830s that electrical telecommunication systems were invented (Kirch, O. & Dawson, T. 2000). Nowadays, we have electronics devices such as the computers sends messages to each other over large assembly of wires, optics, microwaves, and fibres to form a network. Achieving this requires some underlying protocols like TCP/IP, UUCP and IPX. Transmission Control Protocol/Internet Protocol is the most commonly used protocol suite because of its popularity in Local Area Networks (LANs) and Wide Area Network (WANs), such as the Internet. Implementing a computer network requires installation of several software modules, and configuring same based on the network requirement. During the inception of computer networking, Computers running *Windows* operating systems were used. But nowadays, Linux operating systems has been widely accepted mainly because it is an open source, and entertain modifications in order to suit individual's need.

## 1.1 BACKGROUND

### 1.1.1 TCP/IP Networks

Networking applications needs high intelligent approach transmitting data from one computer to another. Many systems have adopted the TCP/IP to ensure data are transferred between machines without interference. TCP/IP protocol is a set of protocols independent of the physical medium used to transmit data, but most data transmission for Internet communication begins and ends with Ethernet frames (Rabbit Semiconductors 2000, 4). In a LAN, the Ethernet is the most common hardware with a speed of 10, 100 or 1000 Megabits per second. Ethernet can either use a star or bus topology, and uses the

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method in order to ensure proper sharing of network resources without collision. All Ethernet cards have a unique 48-bit identification number which is called the MAC (Media Access Control) address. All systems in a TCP/IP network require at least an Ethernet card, and many Ethernet cards can be connected using hubs and routers to form a network.

However, local networks can be connected to the internet through a gateway, which is always a computer connected to both the local network and the Internet. The gateway receives data whose destination is one of the computers in the LAN, and then sends it to the actual destination. It also receives data whose destination is outside the LAN, and then passes it on for routing to the outside world. Computers and devices in an Ethernet are connected together using the Ethernet cables. There are two types of cables – crossover and straight – through. Crossover cable is used to connect network devices together but in a case where two computers are to be directly connected together, a crossover cable must be used. Messages passing across the Ethernet are grouped together and are called *frames*. An Ethernet frame is a structure with size between 46 and 1500 bytes, and has four different sections – *Preamble, Header, Data and Trailer*.

### **1.1.2 UUCP Networks**

UUCP means Unix – to – Unix Copy. It consists of bunch of software programs which were designed to transfer files over serial lines, schedule those transfers, and initialize execution of commands on remote sites (Kirch, O. & Dawson, T. 2000, 30). UUCP is mostly used in Wide Area Network and its application is mainly based on dial-up connections. When UUCP was developed, it was used to connect different Unix environments together. But today, it is been used with several other platforms, including DOS and Mac OS. Computers in a UUCP network have modems, which makes them suitable to be used remotely from character-mode terminals via dial-up lines.

In the network, the modems dial to establish a temporary peer-to-peer link between two clients. During this connection, the transfer of all emails and files queued occurs. Due to the queuing character of UUCP, several applications cannot be used with it. UUCP has continued to grow tremendously and has connected thousands of sites across the world.

### 1.1.3 Linux Networking

The development of networking capabilities in Linux started from the early stage of Linux OS itself. Several programmers across the globe have immensely contributed towards Linux and its connectivity as well. UUCP started running on Linux almost at the beginning of Linux, but TCP/IP network implementation started later when Net-1(the first Linux network module) was created. Several versions of Linux Network code have been released and the Net-4 version offers a wide variety of device drivers and more advanced features. Net-4 remains the standard official module and possesses some advanced features which include IP accounting, IP forwarding, IP masquerade and NAT and IP tunnelling.

Great changes have occurred and still continue in the Linux kernel networking implementation. Nowadays, Net-4 network implementation is in use in many sites and is increasingly gaining popularity among Internet Service Providers because of its cheapness and reliability to build servers for small and large enterprises.

### 1.1.4 System Maintenance

Network administration is not only installation and configuration; it also extends to the maintenance of the system after set up. System maintenance is basically checking overall performance and log files regularly for errors and unusual events. To carry out a routine check, couples of written administrative shell scripts must be run from *cron*. The *cron* result usually consists of replies from each application running on the system. *Cron* replies can include error reports, log files summaries and the application usage statistics. Frequent maintenance of the servers and the workstations are highly important due to the following reasons;

- Critical security updates need to be applied at least once in four weeks.
- Frequent review and management of firewall, virus and spyware protection is important.
- Regular use of the system by the users can cause network issues.
- Regular observation and analyzing of the server event logs can prevent future problems.

- Proper management of hard drives would prevent damaged drive and data lost.
- Frequent optimization of workstations and servers would increase speed and efficiency.

In order for proper network and systems maintenance, the administrator must be available to answer complaints either by phone, email or in person.

## 2 COMPUTER NETWORK ADMINISTRATION

Administering a computer network involves the installation, configuration and supporting a network and internet system or a segment of a network system. However, a network administrator must perform network hardware and software maintenance, ensure network availability to all system users, and implement and ensure network security measures.

### 2.1 TYPES OF COMPUTER NETWORK

Computers can be connected locally, nationally and globally depending on the use of the network. The main types of computer network are emphasized below.

**a) Local Area Network (LAN):** LAN is a type of computer networks that covers a small physical area like home, office or small group of buildings, such as a school, campus, or a building. It is usually privately owned by individuals and links the network devices together in order for communication to occur. Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two personal computers (PCs) and a printer in someone's home office. It can also be extended throughout a company which includes audio and video peripherals. LAN can go as far as few kilometres within the region designed for.

LANs are designed to allow resources to be shared between PCs and workstations. The share resources can be hardware (such as, a printer, scanner, etc.), software (e.g., an application program), or data.

Over recent years, LAN has been developed with many technologies such as Token Ring, FDDI, ARCNET, Ethernet and Wi-Fi but among all these technologies, Ethernet and Wi-Fi have been in common in usage.

There are categories of networks which are interconnected by LAN;

- Campus Area Network (CAN) which is limited within a geographical area, such as a university campus, a corporate campus or military base.
- Home Area Network (HAN) is a residential LAN. It is used for communication between digital devices typically deployed in the home,



usually a small number of personal computers and accessories, such as printers and mobile computing devices. The important aspect of it is that, it is always a shared network of internet access, often broadband service through a cable TV or Digital Subscriber Line (DSL) provider.

**b) Wide Area Network (WAN):** WAN is a computer network that covers a broad area, that is, many network whose communication links cross metropolitan, regional, or national boundaries. It provides long distance transmission of data, image, audio, and video information over large geography areas that may comprise a country, a continent, or even the whole world. Many WANs are built for one particular organization and are private while others built by internet service providers (ISPs), provide connections from organization's LAN to the internet. As been studied, a WAN can be as complex as the backbones that connect the internet or as simple as a dial-up line that connects a home computer to the internet. The backbone connection is referred as switched WAN that connects to the end system, which normally comprise a router (internet-working connecting device) that connects to another LAN or WAN and the dial-up connection as a point-to-point WAN which is normally a connection from line leased of a telephone or cable TV provider to home computer or a small LAN to an Internet service provider (ISP).

**c) Metropolitan Area Network (MAN):** A MAN is a network with a size between a LAN and a WAN. It is a large computer network that usually spans a town or a large city. A MAN usually interconnects a number of LANs using a high-capacity backbone technology, such as fibre-optical links, and provides up-link service to WAN and internet. It is designed for customers who need a high-speed connectivity, normally to internet, and have endpoints spread over a city or part of city. An example of MAN can be implemented in an organization that needs to use MAN to connect the LANs in all of its offices throughout a city. Usually a MAN can be operated and owned by a private company, or it may be a service provided by a public company, like a local telephone company. Some technologies used for implementing MAN are Asynchronous Transfer Mode (ATM), Fibre Distributed Data Interface (FDDI). The most popular MAN service telephone companies provide is called Switched Multi-megabit Dada service (SMDS).

## 2.2 NETWORK TOPOLOGY

Network topology can be categorized into two i.e. the physical and the logical network topology. The physical topology is the physical design of a network putting into consideration the devices to be installed, the installation cables and the location. On the other hand, logical topology refers to management and sharing of available bandwidth by the network devices. The various types of physical topology are discussed below.

### 2.2.1 Mesh Topology

This topology is part of the most reliable topologies used in computer networking. All the network devices are directly connected to each other. Therefore, the connection link carries traffic only between the two devices it connects. It allows a continuous connections and reconfiguration around broken or blocked paths by hopping from node to node until the destination is reached. Due to the way it was designed, a mesh topology is a bit different from other topologies because of its complexity in build-up. To find the number of physical links in a fully connected mesh network with  $n$  nodes, one need to consider first that each node must be connected to all other nodes. A mathematical equation to get the number of connections in mesh topology is  $n(n-1)/2$  (Forouzan, B. 2007, 9).

Note that a mesh offers several advantages over other network topologies.

- i. The dedicated link can carry its own data load, thus reducing or eliminating the traffic problems that can occur when links has to be shared by multiple network devices.
- ii. It is highly robust and efficient. The failure of a link does not affect other links or put a stop to the entire system.
- iii. It has a great advantage on privacy or security state. Since data travels in a dedicated link and does not have to be routed through other devices, only the recipient sees it. Thus, the security becomes assured and privacy is adequately enforced.

Just as mesh advantages, it does have disadvantages too. The main disadvantages of mesh topology are the large amount of I/O ports and the cabling required. Other disadvantages of mesh topology are

- i. Installation and reconnection are difficult in mesh topology because of its connectivity where all devices are connected to each other.
- ii. Large amount of cables are required during installation, therefore space to accommodate the cables might be limited.
- iii. Installation of Mesh topology can be expensive.

### **2.2.2 Star Topology**

Star topology is quite different from mesh topology. Here, every network device has its dedicated point-to-point link only to a hub, which serves as a central controller. The connection in star topology is done in a way that the devices are not linked to one another. The central node is passive somehow and the passiveness allow the original node to be able to tolerate the reception of an echo of its own transmission, delayed by the two-way transmission time-the transmission from to and fro central node with additional delay generated in the central node. This makes the controller to acts as an exchange device communication. If one device wants to send data to another, it will need to send the data to the controller, which then relays the data to the other connected devices.

Star topology has great advantages over the other previous topology in term of their expenses. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor of one link and I/O makes it easy to install and reconfigure. This therefore, will require less cabling to be used when installing through the building walls. There is only one connection for the additions, moves and deletions between the device and the hub.

Other advantages include robustness. The robustness includes it confidentiality. If one link fails, only that link is affected and does not affect the remaining link whatsoever. This makes it easy to identify and isolate faults when there is any. If the controller is still functioning, link monitoring would still be possible and traffic can bypass the defective links.

Although star topology is reliable because of its robustness, but it has a major problem which includes the dependency of the whole topology on one single point, the hub. If the hub fails, it will make the whole system become inactive.

### **2.2.3 Bus Topology**

A bus topology uses multipoint connection, where its architecture is made to set all clients via a shared communication line, called a bus. This means that one long cable acts as a backbone to link all the devices in a network. (Forouzan, B. 2007, 11)

The connection includes the node connecting to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. In a *bus topology*, a sharp edge connector pierces into the main cable to create a contact with metallic core. This connector is known as a *tap*. During installation, limited taps are required because signal tends to lose its energy to become heat as it travels farther along the backbone. Some advantages of bus topology are;

i. Bus topology is relatively easy to install. Backbone cable can be laid along the most efficient path, and then connected to the nodes by drop lines of various lengths (Forouzan, B. 2007, 12). In this case, it can be noticed that less cable will be required for installation and that suggests that bus topology uses less cable compare to mesh or star topologies.

The computers in the bus topology also listen directly for a signal; they are not responsible for moving the signal along.

ii. They are also well-suited for temporary or small networks not requiring high speeds (quick setup).

iii. It is much less expensive compared to previous network topologies (mesh and star topologies) and easy to implement because only a single cable is needed.

iv. It also reduces weight due to fewer wires.

v. If there is any fault in the cable, it will be easier to identify where the fault(s) comes from since it involves few cables.

Disadvantages of bus topology include;

- i. Part of the difficulties bus topology has is difficult reconnections and fault isolation: A bus normally is designed to be optimally efficient at installation; therefore it can be very difficult to add new devices (Forouzan, B. 2007, 12).
- ii. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable (Forouzan, B. 2007, 12).
- iii. If there are many computers on a single signal then privilege will be given first to those that are closer to the sending signals. Therefore, it works best with limited number of nodes.
- iv. If there is a problem with the backbone cable, the entire network goes down.

#### **2.2.4 Ring Topology**

A ring topology is network topology that connects node to node forming a continuous pathway for signals through each node. It's therefore is a point-to-point connection with only the two devices on either side of it. Data travels from node to node, with each node along the way handling every packet. Signal is being passed in a unidirectional manner, i.e., from nodes to nodes, until it reaches its destination. Each device in the ring incorporates a repeater. This process shows that when a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

Just as the previous topologies, ring topology also has its usefulness and setbacks. The benefits of bus topology are;

- i. Every device on bus topology has a good accessibility to the token and the opportunity to transmit due to its orderliness.
- ii. It can create much larger network using Token Ring.
- iii. It requires only two connections changing when adding or deleting device(s).
- iv. Because of continuous circulation of a signal in the ring shaped manner, if a device is broken in the network, it won't affect the other devices. When a device

is down or not receiving a signal within a specified period, it generates a signal alarm which will prompt the network operator for alert.

- v. Under heavy network load, a ring topology will perform better than the star topology.
- vi. It is easy to install and reconfigure.

Disadvantages include;

- i. Since it is a unidirectional traffic, it can cause some problems for the whole networks. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network (Forouzan, B. 2007, 12).
- ii. Under normal load, it will be slower than Ethernet network.

## 2.3 COMPUTER NETWORK PLANNING

Before decisions are made when preparing to configure computer network, several things need be put in place. Plans are needed to strategize the way for the easy installation, accessibility, massiveness, capability, etc. Therefore in order to make a good network design, one need makes good plans.

The following are the steps needed to plan and design a network:

**a) Identification:** In a computer network, applications are seriously needed which helps to build a successful network. A computer network can be very diverse, i.e. requiring several large applications such as Enterprise Resource Management (ERM), Internet telephony, Instant Messaging (IM), email and others. All these are so important to pay attention to because they are the basis of estimation of what software, hardware, the capacity and the traffic requirement the network would need.

**b) Traffic Requirements:** Just like day-to-day business activities where monitoring of some projects or activities is been done, it is also necessary in computer network to monitor the network traffic regularly. Before a computer network is designed, several

factors must be considered about the traffic requirement. Some of the factors to be considered are;

- i. Identification and documentation of major sources.
- ii. Estimation of bandwidth requirements for each application.
- iii. Requirements for reliability. Reliability in network configuration is much appreciated by the end users.
- iv. Categorization of traffic as local, client/server, peer-to-peer, distributed, terminal/host or server/server.
- v. Quality of Service (QoS) requirements for each other. (Anand Software and Training Private Limited 2010)

**c) Scalability Requirements:** When planning a network, scalability should be seriously considered. The extent of network growth that should be supported by network is called *Scalability* (Anand Software and Training Private Limited 2010). A good scalable network must have provisions for additional users, applications, additional sites, and external network connections.

**d) Geographical Requirements:** This aspect is also much important to be considered because the network that is in progress or intends to build will be determined by its region. The area, size and users involved should be visible enough for whomever in charge of configuring, so that one will know the area network to use.

For the consideration to be fully made, one should consider if the link(s) needs for the project should be LAN, WAN or MAN. For example, offices with large separated distance can be linked together by WAN. Similarly, building complexes within a compound can be linked by LAN. Notice, the LANs fall within the premises of a company whereas WANs are typically leased and maintained by the telecom companies or Internet Service Provider (ISP). Hence, WANs are costly and need to be planned and designed with utmost care to minimize resource consumption.

**e) Availability:** To design a network, availability of network is highly recommended to be considered carefully. It is the amount of time a network is available to users over a period of time and many times a delicate design parameter (Anand Software and Training Private Limited 2010). There is a great tier between availability and amount of redundancy required. If network is not properly planned, unavailability of the network at some times could result to a great business loss to the company. For profitability to be maintained, a right balance should be consider first to arrive.

**f) Security and Accessibility:** The security for a network should be well planned and needs to be properly implemented to meet the required security specifications. In order to achieve a full security requirement, the following must be certainly considered;

- i.** A list of network services that will be provided such as FTP, web, email, etc.
- ii.** The person to be in charge of administrating the security of these services must be put to plans.
- iii.** How the people would be trained on security policies and procedures, should be on the agenda.
- iv.** Recovery plan should also be put to practice, should a security breach does take place. (Anand Software and Training Private Limited 2010)

**g) Cost Consideration:** When planning to configure and install a network, another very important factor to be considered is the cost of the whole setup. For examples, to minimize the equipment cost, LANs has the full tendency since all the configuration will be within the locality or small region. These goes to cable cost minimization, minimization of port cost, and labour cost. For WANs, the primary goal is to maximize the usage of bandwidth because the cost of bandwidth increases tremendously. This cost is usually much higher than other cost.



Some factors to be considered about cost are:

- i.** Improvement of WAN circuits efficiency is important using features such as compression, voice Activity Detection and so on.
- ii.** Use technologies such as ATM that dynamically allocate WAN bandwidth.
- iii.** Integrate both voice and data circuits.
- iv.** Optimize or eliminate underutilized circuit. (Anand Software and Training Private Limited 2010)

### 3 SMALL AND MEDIUM ENTERPRISES NETWORK MODELLING

#### 3.1 ENTERPRISE ORGANIZATION ARCHITECTURE

In this project, an education institution consisting of one (1) server, eight (8) work stations and one printer was modelled. eBox was used as a gateway and several other network services were configured on the eBox machine. The network consisted of four (4) groups (departments) with twenty-seven (27) users. The workstations were distributed into groups as shown in Figure 3.1.

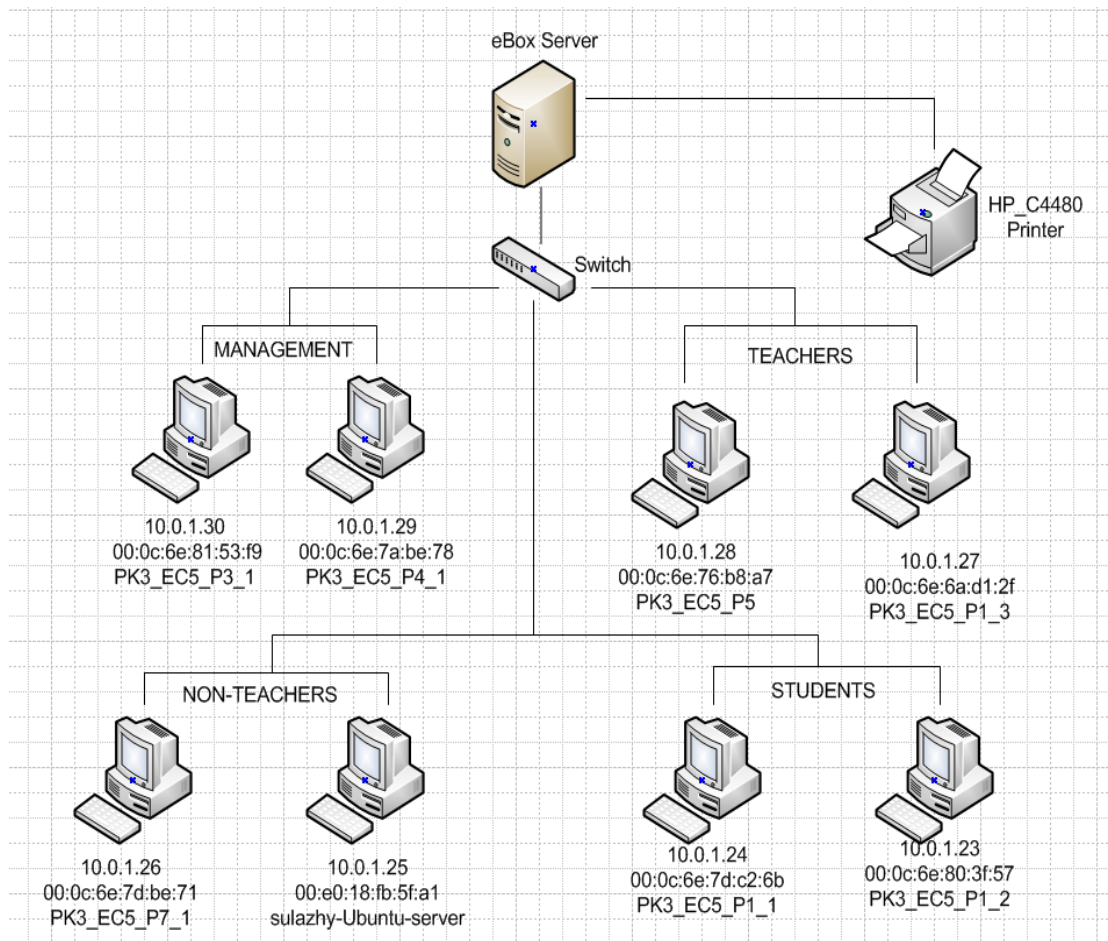


Figure 3.1 – Modelled Network Architecture Diagram

As shown in Figure 3.1 above, each workstation is labelled with its IP address, MAC address and the host name. The four groups created in this project are;

- i) **Management Department:** The management department consists of the institution authorities; the Rector, Deputy Rector, Dean e.t.c. In this project, two client computers were provided in this department but additional clients can be added.
- ii) **Teaching Staff Department:** The teaching department consists of the academic staff. Academic staff department consists of two client computers.
- iii) **Non – Teaching Staff Department:** The non-teaching staff department consists of non-academic staff. The bursar, student counsellors, student office staff are examples of non-teaching staff.
- iv) **Students Department:** The students department consists of all the students in the institution.

### **3.2 ENTERPRISE NETWORK REQUIREMENT**

The network requirement of the enterprise is the most important to be considered when planning a network. All network services to be implemented will solely depend on what is required of the network. The network requirement and architecture can only be determined by identifying the enterprise business requirements and the technical requirements. In this project, the network requirement is to satisfy a full operating educational institution. The network services implemented in this project are;

1. Internet Gateway / Proxy Server
2. Email Server
3. Web Server
4. NTP Server
5. DHCP and DNS
6. File and Printer Sharing

7. Firewall/Security
8. Intrusion Detection / Prevention
9. Virus Protection
10. Spam Filtering
11. Network Awareness / Monitoring
12. Data Back-up, Failover, and Recovery
13. Usage Report
14. Instant Messaging
15. User and Groups
16. SSH
17. VPN
18. Web and Email Filtering

## 4. EBOX TECHNOLOGIES SL

*eBox technologies S.L* is the company responsible for *eBox Platform*, *eBox Control Center* and all technologies and services under eBox. *eBox Technologies SL* is incorporated in Spain and the company's goal is to make *eBox platform* the best unified network server for small and medium businesses, thereby making it the number one choice for computer network management.

### 4.1 eBOX PLATFORM, VERSION 4

The eBox platform v4 is the Linux small business server that can act as a gateway, Unified Threat Manager (UTM), Office Server, Infrastructure Manager, Unified Communication Server or a combination of them. Each network service from eBox platform are based on the same technology and fully integrated, allowing the network engineer to manage the network easily as one single unit (eBox Technologies SL 2010, 1). eBox platform packages and their features are fully explained below.

**a) eBox Gateway:** *eBox Gateway* is the eBox package whose function is to enable eBox server act as the gateway to a network. The *eBox Gateway* can make a perfect reliable network, optimize the allocated bandwidth and helps control all traffic coming into the network. The eBox gateway consists of several eBox modules which serves different purpose in order to make eBox an efficient and reliable gateway.

The eBox gateway has the following features;

- **Transparent caching:** This transparent caching helps in making internet connection faster. When users visit a website very often, eBox recognizes the website and make very connection to that website easy and faster. This reduces traffic congestion and allows other users and important application to make use of the bandwidth.
- **Traffic Control:** The traffic control in eBox platform is made in order to ensure a good process of managing, prioritizing, controlling or reducing the network. Enabling traffic control allows most important traffics to be served, regardless of the network load.

- **Load Balancing and Availability:** The effectiveness of load balancing and availability in eBox gateway is to give assurance of continuous connections. The guarantee of the internet connection is highly appreciated in eBox platform. For example, if one has more than one connection to the internet, it will distribute transparently the clients that are in the network and make sure each user are connected even if one of the connections is down.
- **Content Filter:** Content filter is used to filter the accessibility of internet properties. In this eBox platform, restriction can be made to certain sites by the administrator using the content filtering module. From the packages in the eBox platform, options can be made to filter which type of sites or type of files one can access, so implementing this from the platform is part of the function one can utilize in this whole configurations.

The full features in the eBox gateway are listed below;

- Configuration network interfaces (Ethernet, Wi-Fi, PPPoE and VLAN)
- Advanced firewall (NAT, redirections, DMZ, etc.)
- The quality of service (QoS) through traffic shaping (application layer L7) and load balance
- Multi-gateway with WAN fail-over
- Advance routing
- HTTP proxy with cache, content filtering and anti-virus
- RADIUS authentication server.
- Policies suite for users, groups and sub-networks. (eBox Technologies SL 2010)

**b) eBox Infrastructure:** In this section, several things will be explained about the services that is in used to manage and optimize internal traffic and in the infrastructure of designated local network, including domain management, automatic network

configuration in network clients, publication of internal Web sites and time synchronization using internet.

In the eBox infrastructure, there are few things that are needed to be enabled, these includes;

- The DHCP which is widely used to configure different network parameters automatically, such as the IP address of a host or the gateway to be used for internet access.
- The DNS service which provides access to services and hosts using names instead of IP addresses, which are more difficult to memorize.

In this project, the eBox infrastructure has been used to manage and optimize internal traffic which also includes the configuration of domain server and the management of machines and digital certificates.

The features of eBox infrastructure are;

i. **Network Objects:** The network objects are methods of giving a network element or a group of element a common name. They are used in order to facilitate network configuration management in a simple and subsequent form by being able to select behaviour for these objects.

In the network objects, one or many can be managed. Here, a single setting can be made on the whole network, segment of the network or a single computer.

ii. **Web Server:** The *eBox Gateway* consist of the HTTP module used to configure the *Box Web Server*. *EBox Web Server* is powered by *Apache*. Users can be able to deploy their web application using the *eBox Web Server*.

iii. **DNS Server:** *eBox Gateway* houses the *eBox DNS Server*. With *eBox DNS Server*, one can assign every computer in the network a fixed address and name. It is relatively easier to remember names *mycompany.com* than *195.168.173.100*.

iv. **Enterprises-grade SSL:** This helps to create personal certificate either for users in the network or administrator on the network. When one is in need of external certificate to create for end users who is on the network, the enterprises-grade SSL will give chance to

normalize way to allocate the certificate authority in order to build trust between network administrator and the users. But internally, it is not advisable to spend much to have a good security with eBox, so one can create an own SSL certificate and use them for internal email or websites.

The full features of eBox infrastructure are listed below;

- Network interfaces on several VLANs.
- DHCP server
- DNS server
- Certification Authority and Virtual Private Network (VPN)
- Web server
- Network Time Protocol (NTP) server. (eBox Technologies SL 2010)

**c) eBox Office:** eBox platform is very flexible and part of its flexibility is the feature of using various resources which is coupled in the office package. One of the primary aims for the creation of computer networks was due to the sharing of resources and data. The office package is very essential for daily operations of many local area networks in offices or at home. In the eBox office, the administrator can add or delete users to the network as well as bulk of groups. The users also have access or advantage to use some important materials needed for their daily tasks. Example of those materials include, sharing of files and printers, email package using groupware services, which also have features like calendar, contacts and address book, etc. In summary, the eBox office package allow office resource to be managed and shared, which includes user profiles and group accounts, files, printers, calendars, contacts and tasks, and backup of data (eBox Technologies SL 2010).

Features present in eBox office are listed below.

**i. Open Directory:** This is one of the features of eBox office. It manages all users and resources from a central point. In the package, one can decide who should get access and



to what network resource. It is based on the open standards like LDAP, for easier integration of application and services on current hold. In open directory in eBox office, users can be implemented in one place.

**ii. File and Printer Sharing:** File and printer sharing in the networks helps to get easy access of communication in transferring files between users of the network. It might take much time sending files via email, or using hardware transferring (USB or flash disk transfer of data) but with the eBox sharing, it can be done in shorter time using the file transfer coupled in the office package. This therefore makes sharing easy to carry out. User can easily share folders by creating shared directories for group of workers in the same work area or department. File and printer sharing within eBox is independent on any OS. Windows, Linux or Mac user can participate in the file and printer share.

**iii. Calendars, Contacts and Tasks:** This gives an easy collaboration tools. The calendars and contacts tools can be configured in the groupware module. The administrators in his/her capability can enable any feature(s) he/she wants each network users to use in the groupware service. So the groupware helps to solve the sharing of calendar, contacts and tasks with the rest of the team or users in the same network.

**iv. Data Backup:** Backing up files in computer world has been a good thing that many network users have appreciated. Data can get corrupted, lost or get deleted by mistake but when copies has been backed up, it give great sense of safety. In *eBox Office*, data is saved in centralized document storage.

The full features in the eBox Office are listed below;

- LDAP server
- Centralized authentication including Primary Domain Controller (PDC) and Active Directory (AD)
- Calendar, contacts and task sharing
- Files and folder sharing
- Printers sharing
- Roaming profiles

- Data backup. (eBox Technologies SL 2010)

**d) eBox Unified Communication:** *eBox Unified Communication Server (UCS)* manages all the communications between users by email, instant messaging and VoIP switchboard.

*eBox Unified Communication* handles the different communication methods for sharing information that are centralized in eBox and how they are accessible when we use the same username and password.

The unified communication on eBox platform technology handles the mail service of eBox. The mail service in eBox platform allows a quick and easy integration with the preferred mail client of the users of the network, which also includes the latest techniques available to prevent spam.

However, the configuration of instant messaging (IM) service will be mentioned. The instant messaging service uses Jabber/XMPP protocol which has feature to add user from the same or outside network to the owned IM account. The protocol mentioned earlier is a self reliable real-time service which provides internal IM service without relying on external service or internal connection. The service also offers conference when using and can be used with any of the many available.

Finally, the service package of unified communications is very important for voice over IP (VoIP) implementation. This part of service enables each person to have an extension to make calls or participate in conferences easily. Before implementing, one needs an external provider to provide the service because eBox itself cannot host the users on the network.

The feature that eBox unified communications posses are;

**i. User Management:** In the network where there are many end users, it will not be possible if all the users just sign in to the network without having identity which will authenticate to the service. But with the user management service, the administrator can create user, give the user identity on the network which will be registered and the identity includes password. The administrator can therefore, manage all the users and groups in the

network with the resources available to them from a central point. With the given username and password, users will have access to all services they are authorised to use.

**ii. Instant Messaging:** This application is used to supplement the work of emailing. Sometimes one need to make an instant communication with other users on the same network for a quick reply, so the eBox instant messaging service will be used instead of email service. eBox provides its IM services based on the Jabber/XMPP protocol, so it will be easy to use an existing clients on any platform even on cell phones if there are agreement made between the two parties.

**iii. Email:** eBox provides an integrated email solution, with anti-spam and antivirus technologies. The usual standards of emailing is been supported by normal email client using Linux kernel system.

**iv. VoIP:** With eBox, VoIP can be easily installed and implemented for users or employees with their own extension within the internal network to make easy and convenient internal calls and conferences. It is also possible to get a real phone numbers and route them to eBox account to make and receive calls at very low cost.

The full features in the eBox Unified Communication are listed below;

- E-mail: SMTP and POP3/IMAP4 with SSL/TLS. Antispam, antivirus and relay policies. Webmail. SIEVE server-side filters.
- Instant Messaging (IM)
- VoIP: Internet based calls to mobile phones and landline, call transfers, call parking, voicemail, conference rooms, e.t.c. (eBox Technologies SL 2010)

**e) eBox Unified Threat Manager (UTM):** The UTM is used to protect network beyond a simple firewall, external attacks and also used to detect possible intrusion into network service (eBox Technologies SL 2010, 123). It helps to filter email spamming, avoid virus that might attack the email service provided by eBox, filter *HTTP* proxy with an antivirus and integrate several advanced configurations in order to provide greater security to the internet browsing of the users in the network.

The features that eBox UTM posses are;

**i. Content Filtering:** There are various important and useful things of using internet. The internet has been a wonderful discovery, and it is filled with lots of useful and amazing content when using but there are still lots of threats on the internet. Threats like spam, viruses and phishing. In eBox platform, the content filtering has been developed to prevent such threat. In summary, the content filtering filters out the harmful content coming into a network or already in the network.

**ii. Firewall:** In a network, security is very essential for several purposes. eBox firewall is responsible for security, threats and the blockage of unwanted access to some part of the network or some resources in the network. If firewall is not enabled, it can create difficulties for accessing internet and not allowing other service packages to function.

Security has different layers, but all starts with good firewall. It only allows the needed traffic from network and sieve against unwanted attackers. (eBox Technologies SL 2010, 48)

**iii. Virtual Private Networks (VPN):** VPN gives flexibility on mobility. Same standard security can be guaranteed by VPN for data, communications or files wherever the user moves to. The importance of implementing VPN in network is to allow network users to connect to the internal network from other locations through the internet. e.g., a user can use connect to the office network from home and have access to the office network resources. It helps in connecting computers from various sections or department together with full security on each system and one virtual office. eBox uses OpenVPN for its VPN implementation.

**iv. Intruder Detection:** This intruder detection in eBox was made to give full assurance of securing unwanted spies to the internal network. The implementation of eBox IDS has been made to give information for any suspicious attempts, and it allows the analysis and evaluation of the attempts afterwards. It gives one step ahead of any intrusion.

The full features in the eBox Unified Threat Manager are listed below

- Advanced firewall
- Mailfilter (antivirus, antispam, greylisting)

- Web filtering (content analysis, white lists and black lists, antivirus)
- Virtual Private Networks (VPN)
- Intrusion Detection System (IDS). (eBox Technologies SL 2010)

## 4.2 eBOX CONTROL CENTER

After installing eBox platforms for several clients, there is a need for monitoring of the network servers installed. eBox has developed *eBox Control Center* in order to remotely monitor and troubleshoot multiple eBox servers. In other word, eBox control center allows centralized real-time monitoring and administration of several eBox servers. It has features such as remote, centralized and secure administration of groups of eBox servers, network monitoring, customized reports and automatic remote configuration backup. The eBox control center is very easy to use and have great performance efficiency. eBox Control Center packages and features are explained below.

**a) Remote, Centralized and Secure Administration:** This feature gives allowance to control several eBox platform installations on the administrator server by ensuring remote, centralization and secured administration of groups of eBox platform with a massive security updates and tasks automation through a single web-based interface (eBox Technologies SL 2010).

**b) Network Monitoring:** It is use to control network activities on each eBox platforms installation made. After an installation has been done for several clients, the administrator might want to monitor each client's eBox server, and with many servers on the network, the administrator needs to be kept notified often. To keep the eBox servers alive regularly, the network monitoring will alerts events in each eBox platform installation if there is any defect on the network server. The alerts on the event in platform installation provide graphic storage where it displays the information of all the activities that's running, load, CPU, memory use, etc., of each eBox platform and groups of eBox platform installations (eBox Technologies SL 2010).

c) **Automatic Remote Configuration Backup:** This feature provides the chance to make automatic remote backups of the configuration of each eBox platform installation, and allowing recovering of lost data easily. It can be configured remotely.

d) **Customized Reports:** This feature offers reports on the state of the usage of the server; use of the network service installed in each eBox platform installation. It helps the administrator to keep update of what has happened on each installed eBox platform server.

## 5 INSTALLATION AND CONFIGURATION OF EBOX PLATFORM FOR ENTERPRISE

The installation of eBox platform was done on a standalone desktop computer using the eBox platform installation CD. During the installation, some pre – configuration were made. Since eBox is an open source project, it was packaged on Linux operating system. Therefore, the base system; Linux was installed and the computer underwent a reboot. After the reboot, eBox was ready to be installed. There comes an option of the package selection method to use for the installation of eBox packages. The *simple* method was chosen because the server would be dedicated to all the services eBox can offer. The option of the eBox profiles to be installed was made and all the profiles (Gateway, Security, Infrastructure, Office and Communication) were selected and installed. After the installation, all eBox modules were ready to be configured. It was mandatory to know that the entire module to be configured on eBox must be activated in the *Module Status* option on the administrative webpage. Since all modules were to be configured in the project, all the modules were activated.

### 5.1 eBox CORE

*eBox Core* is a section of *eBox Platform* that facilitates the administration of all other eBox platform modules. *eBox Core* function as a backup to restore state, logs of services to find out what has happened and what time it has happened. It also notifies about specific events and incidents, monitors the machine or secures update of the software that is issued. Some features of eBox Core are emphasized in this section while others have more connectivity with other modules and they will be adequately explained with regard to the configurations in this project.

#### 5.1.1 Logs

Modules in eBox have an infrastructure which allows them to log their activities whenever they operate. The logged data will be available to the administrator and can be used for important analysis of the system. These *logs* are found through the eBox web interface. The logs are also found in the system database for making queries, reports and updates in an easier and more efficient way. In eBox *Logs*, the PostgreSQL database is used.

It is also possible to configure different dispatchers for various events. The administrator can be notified by different means either by email, RSS or Jabber.

The activities or events of the following eBox module can be logged by the *log* module:

- OpenVPN (*Virtual Private Network*)
- SMTP Filter (*Simple Mail Transfer Protocol, mail filter*)
- Firewall
- Printers
- DHCP (*Dynamic Host Configuration Protocol*, network configuration service)
- Mail
- Proxy (*HTTP Proxy Service*)
- IDS (*Intrusion Detection System*)

One can likewise receive notifications of the following events:

- eBox health status
- Service status
- Free disk space
- Problems with internet routers
- Specific values inside the logs
- Events from the software RAID subsystem.
- Problems with internet routers

To make use of the *Logs* module, it has to be enabled in the *Module Status*. To enable the *Logs* service, go to *Module Status* and select *Logs*. One can either query the *Log* module for *Summarized Report* or *Full report* of the activities or events that has happened for a



period of time in one of the listed eBox modules above. And From the query logs menu, there are also two options that can provide administrator to get report or feed back of the system information. Figure 5.1 below shows the log of IDS when a user tries to connect using *ssh*.

The screenshot shows the eBox Logs interface. On the left is a sidebar with navigation options: Core, Gateway, and Office. The main area is titled 'Logs' and includes a 'Custom query' section with filters for date, priority, description, source, and destination. Below the filters is a table of log entries.

Date	Priority	Description	Source	Destination	Protocol	Event
2010-03-16 17:18:29	2	BAD TRAFFIC Non-Standard IP protocol (De...	10.0.1.27:123	192.168.1.2:123	UDP	Alert
2010-03-16 17:18:29	2	BAD TRAFFIC Non-Standard IP protocol (De...	10.0.1.27:123	192.168.1.1:123	UDP	Alert
2010-03-16 17:18:13	2	BAD TRAFFIC Non-Standard IP protocol (De...	10.0.1.27:123	192.168.1.2:123	UDP	Alert
2010-03-16 17:18:13	2	BAD TRAFFIC Non-Standard IP protocol (De...	10.0.1.27:123	192.168.1.1:123	UDP	Alert
2010-03-16 17:17:57	2	BAD TRAFFIC Non-Standard IP protocol (De...	10.0.1.27:123	192.168.1.2:123	UDP	Alert
2010-03-16 17:17:57	2	BAD TRAFFIC Non-Standard IP protocol (De...	10.0.1.27:123	192.168.1.1:123	UDP	Alert
2010-03-16 17:17:40	2	BAD TRAFFIC Non-Standard IP protocol (De...	10.0.1.27:123	192.168.1.2:123	UDP	Alert
2010-03-16 17:17:40	2	BAD TRAFFIC Non-Standard IP protocol (De...	10.0.1.27:123	192.168.1.1:123	UDP	Alert
2010-03-16 17:17:24	2	BAD TRAFFIC Non-Standard IP protocol (De...	10.0.1.27:123	192.168.1.2:123	UDP	Alert
2010-03-16 17:17:24	2	BAD TRAFFIC Non-Standard IP protocol (De...	10.0.1.27:123	192.168.1.1:123	UDP	Alert
2010-03-16 17:17:08	2	BAD TRAFFIC Non-Standard IP protocol (De...	10.0.1.27:123	192.168.1.2:123	UDP	Alert

Figure 5.1 – Logs full report of IDS service

### 5.1.2 Monitoring

When a machine is set up for an important purpose such as a server, the administrator needs to keep full monitoring of the system to avoid malfunction and unexpected failure. In eBox, this has been made easy with the help of the *Monitor* module. In other words, *eBox Monitor* is used to monitor the condition and state level the resources of the eBox

machine is, at different moments. This is very important to troubleshoot and plans in advance for necessary resources.

Monitoring gives vital information for the eBox administrator to know and interpret the values of the systems in the eBox machine in order to decide if those values falls within an expected range or not. In eBox, different systems have their expecting usage values and checks have to be carried out occasionally if the values are within the safe range. One thing should also be seriously considered; fetching values that are useless for monitoring scenario. This reason is why eBox monitors only have few system metrics. These are; *CPU usage, system load, memory usage, and file system usage.*

The fetched data are displayed graphically, as in Figure 5.2. This monitor module helps user to easily visualize the evolution of the resources during time.

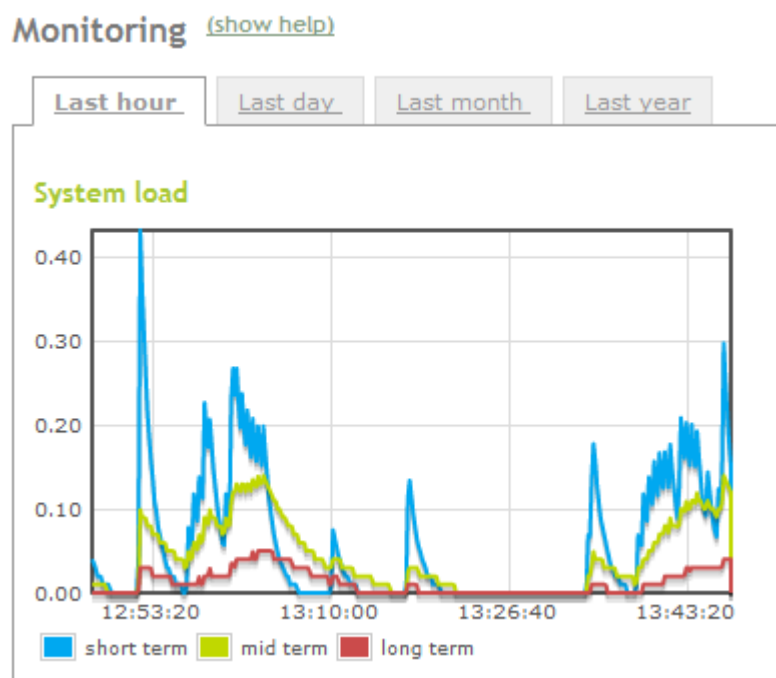


Figure 5.2 – System load monitored by the *Monitor* module

## Metric

The metric in eBox is used to determine the performance of the system. In network, there can be several systems that multitask, so in order to stable their performances and regulate their work rate, the administrator make sure it checks the eBox metric. The

metrics consist of several measurement tools to measure the hardware performance of the eBox server.

**i. System Load:** In the eBox server, several processes occur simultaneously. The system load metrics measures and shows the rate of pending work over the completed work (eBox Technologies SL 2010, 162). Different tasks come in at the different time, which means data cannot be send at almost the same time. For the data to be delivered, the load on the system must have priorities for incoming and outgoing tasks. The number of active process in the CPU is the computed value in the system loading.

The capacity of the used CPU over a given time is called the *Metric*. The computed value of the metric means to have a full working capacity, the CPU must work at one load of task. A load of one-half can make the CPU work as twice as normal. Oppositely, a load of two means that, an additional required CPU will be needed to fulfil the requirements of the current work load. (eBox Technologies SL 2010, 162)

**ii. CPU Usage:** The CPU works as a backbone for the system. In the eBox system, the CPU shows how client systems are used. The administrator tries to get report of the CPU performance in order to analyze the system performance. There can also be multi-task or multi-core usage in process which needs to analyze for a report, so the operator tries to get all necessary information for the CPU performances.

To show update reports, the graph shows the full detailed of the CPU usage and in case of having multi-core or multi-task, there will be one graph needed for each of the cores. Therefore, the graphs represent the amount of time that CPU spends in each of its states: which runs the user code, system code, inactive, input/output (I/O) wait, and so on. The measurement is therefore not in measured in percentage, but in scheduling units called *jiffies*.

**iii. Memory Usage:** The memory aids the performance of system. The higher the memory used, the higher the performance. The system needs to have storage for its data and how system characters need to work. To get the full report on the memory usage, the administrator needs to get the daily or timely event of the graph. The following variables are monitored for memory usage:

- **Free Memory:** Amount of memory used.

- **Page cache:** Amount of memory the disk swap has cached.
- **Buffer cache:** Amount of memory I/O operations has cached.
- **Memory used:** Amount of memory that is not included in any of the above.

**iv. File System Usage:** The file system usage is used to know the free space of every mounting point.

**v. Temperature:** It is good to know how systems are controlled in temperature wise. If the temperature is too high for system, there can be failure in the network traffic and can cause delay for data sharing or operations of network. The temperature is measured in degree Celsius using the ACPI system.

## Alerts

The alert helps to give some notice on time if there is an unexpected error or failure in the system. Configuring the *eBox Alerts* informs when the system is reaching its maximum load capacity.

*Note:* The graphs are not efficient enough to give notification in case of unexpected behaviour so alert is a good option here.

To configure the monitor alerts, access the Event → Configure Events, there the full necessary configuration information would be requested.

### 5.1.3 Events and Alerts

Through events module, users will easily receive notification of certain events and alerts that happens in the eBox machine.

The services which eBox allow user to receive for alerts and event are listed below;

- Mail
- Jabber

- Logs
- RSS

Before any events watcher is enabled, the event module should be enabled first. In the *Event and Alerts* section, the events must be enabled before they can be used. In this project, no *Event and Alerts* event was configured. Detailed instruction on the configuration of *Event and Alerts* can be found in the eBox 1.2 for Network Administration Handbook.

#### **5.1.4 Backup**

The backup performs the recovery lost data for each system in the eBox machine. If there are crashes in the system connected to a specific network server and the users or clients loss some data in network, the backup will go to its cache memory to fetch out recent works done on it. It also backup any failure for network connectivity. If a network is down, the backup gives some support to the clients that are on the network, so that the queue from client to the network will not be much.

The eBox backup was not configured in this project. Further details on eBox backup can be found in the eBox 1.2 for Network Administration Handbook.

#### **5.1.5 Software Managements**

eBox platform requires periodic updates just like any other software system. It can either be to add new features or to fix defects or system failures. eBox distributes its software as packages and it uses Ubuntu standard tool called APT. To ease this task, eBox provides a web interface to simplify the process.

The web interface gives new feeds for either the administrator or the user using eBox platform for any available versions of eBox components and installing them in a simple way. It also helps to update the software supporting eBox, mainly to rectify any potential security assault.

## eBox components management

The management of eBox components lets one to install, update and remove eBox modules. The component management module must be enabled before any configuration can be done. Figure 5.3 shows some available latest components.

















Component	Installed version	Latest version	Actions
eBox - Monitoring module	1.2.3-0ubuntu1~ppa1~hardy1	1.2.3-0ubuntu1~ppa1~hardy1	
eBox - OpenVPN server module	1.2.2-0ubuntu1~ppa1~hardy1	1.2.2-0ubuntu1~ppa1~hardy1	
eBox - client for remote services	1.2.4-0ubuntu1~ppa1~hardy1	1.2.4-0ubuntu1~ppa1~hardy1	
eBox - Certificate Authority Manager for eBox	1.2-0ubuntu1~ppa1~hardy1	1.2-0ubuntu1~ppa1~hardy1	
eBox - Network configuration module	1.2.7-0ubuntu1~ppa1~hardy1	1.2.7-0ubuntu1~ppa1~hardy1	
eBox - DHCP server module	1.2.1-0ubuntu1~ppa1~hardy1	1.2.1-0ubuntu1~ppa1~hardy1	
eBox - Mail filter module	1.2.2-0ubuntu1~ppa1~hardy1	1.2.2-0ubuntu1~ppa1~hardy1	
eBox common library for server and client	1.2.3-0ubuntu1~ppa1~hardy1	1.2.3-0ubuntu1~ppa1~hardy1	
eBox - layer 7 protocols	1.2-0ubuntu1~ppa1~hardy1	1.2-0ubuntu1~ppa1~hardy1	
eBox platform - communication server suite	1.1.30-2	1.1.30-2	
eBox - Instant messaging (Jabber)	1.2.1-0ubuntu1~ppa1~hardy1	1.2.1-0ubuntu1~ppa1~hardy1	
eBox - Web Server	1.2.1-0ubuntu1~ppa1~hardy1	1.2.1-0ubuntu1~ppa1~hardy1	
the eBox platform - Base framework	1.2.9.2-0ubuntu1~ppa1~hardy1	1.2.9.2-0ubuntu1~ppa1~hardy1	
eBox - eGroupware	1.2.1-0ubuntu1~ppa1~hardy1	1.2.1-0ubuntu1~ppa1~hardy1	
eBox - Mail server	1.2.3-0ubuntu1~ppa1~hardy1	1.2.3-0ubuntu1~ppa1~hardy1	
eBox - DNS server	1.2.2-0ubuntu1~ppa1~hardy1	1.2.2-0ubuntu1~ppa1~hardy1	
eBox - Backup	1.2.2-0ubuntu1~ppa1~hardy1	1.2.2-0ubuntu1~ppa1~hardy1	
eBox - Antivirus module	1.2.2-0ubuntu1~ppa1~hard1	1.2.2-0ubuntu1~ppa1~hard1	

Figure 5.3 – eBox component latest available version

If an eBox component is not installed or up to date, it can be installed by clicking the “*Update all packages*” button through the *Actions* column. It is also possible to uninstall components that are no longer needed, but must be carefully done.

## System Updates

The programs used in eBox are being updated by the system updates, and for one to carry out this function, eBox Platform integrates different system programs with eBox components packages. The program is called dependencies which ensure that eBox

installation should be up-to-date. The update status of our eBox server was checked and this can be seen in Figure 5.4.

### System updates

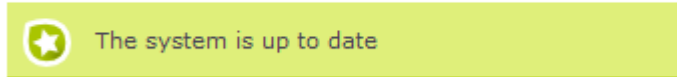


Figure 5.4 – System Update

## **Automatic Updates**

This application helps eBox Platform to perform available automatic installation in real time service.

## **5.2 eBox GATEWAY**

### **5.2.1 High Level eBox Network Abstraction**

#### **Network Objects**

Network objects in eBox are objects that are created to represent groups of devices present in a network. Network objects are used to make easy the configuration of a group of network devices located in the same working area. Each network object can be given an IP address so that a single configuration could be done on the several network devices present in the network object. For example, a computer classroom can be configured to be a network object. In this project, eight computers were used, and four network objects were created. As shown in Figure 5.5 below.

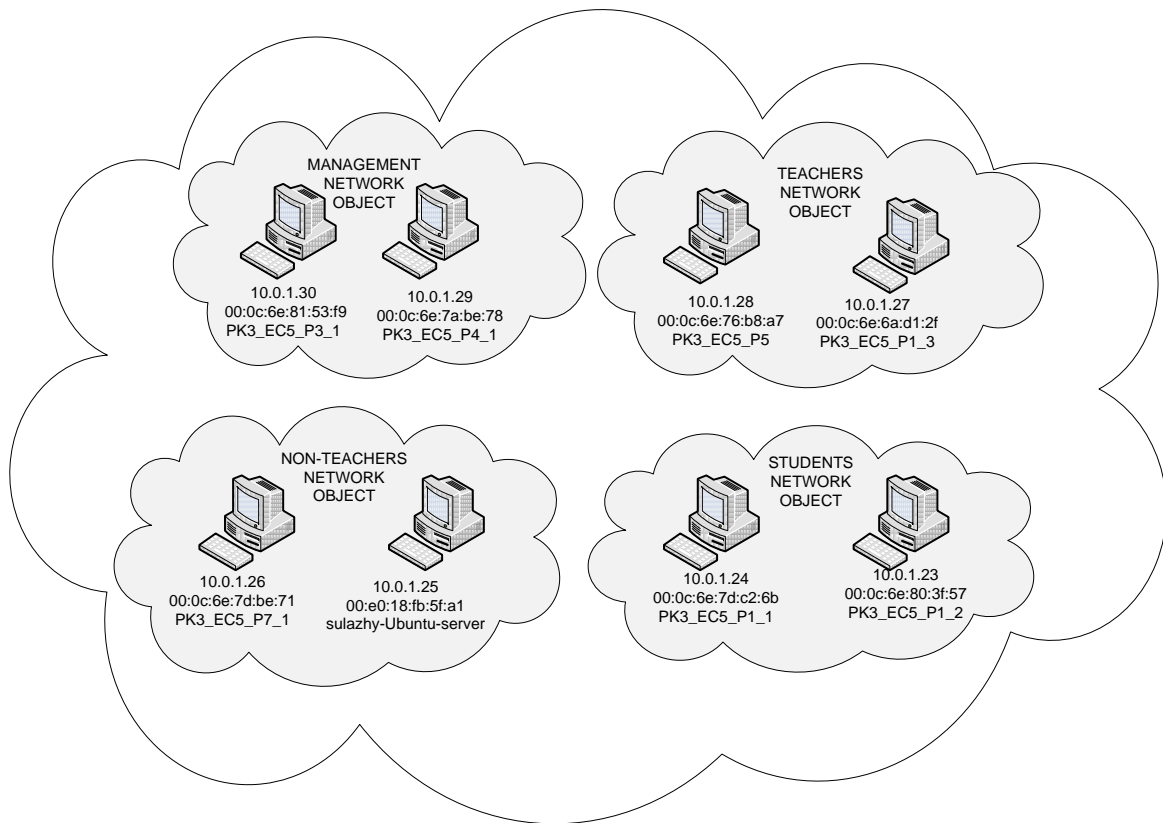


Figure 5.5 – Network Objects created

From Figure 5.5 above, it can be seen that there are two members in each network object created and they can be identified by their hostname, physical address and their logical address. They can be deleted or edited. These objects will be used in other eBox modules like file sharing, http proxy, and firewall e.t.c. The configuration of our network objects can be seen in Figure 5.6, 5.7, 5.8, 5.9 and 5.10.

The screenshot shows the eBox management interface. The top navigation bar includes 'Logout' and 'Save changes'. The left sidebar lists various modules, with 'Network' and 'Objects' highlighted. The main content area displays the 'Objects' section, which includes a search bar and a table of created network objects.

Name	Members	Action
Management	2	[Delete] [Edit]
Non-Teachers	2	[Delete] [Edit]
Students	2	[Delete] [Edit]
Teachers	2	[Delete] [Edit]

At the bottom right of the table, there is a pagination control showing '10' items per page and 'Page 1'.

Figure 5.6 – Network Objects created



Objects > Management [\(show help\)](#)

Members

[Add new](#)

Search

Name	IP address	MAC address	Action
PK3_EC5_P3_1	10.0.1.30/32	00:0c:6e:81:53:f9	
PK3_EC5_P4_1	10.0.1.29/32	00:0c:6e:7a:be:78	

10 Page 1

Figure 5.7 – Management network object configuration

Objects > Non-Teachers [\(show help\)](#)

Members

[Add new](#)

Search

Name	IP address	MAC address	Action
PK3_EC5_P7_1	10.0.1.26/32	00:0c:6e:7d:be:71	
sulazhy-Ubuntu-server	10.0.1.25/32	00:e0:18:fb:5f:a1	

10 Page 1

Figure 5.8 – Non-Teachers network object configuration

Objects > Teachers [\(show help\)](#)

Members

[Add new](#)

Search

Name	IP address	MAC address	Action
PK3_EC5_P1_3	10.0.1.27/32	00:0c:6e:6a:d1:2f	
PK3_EC5_P5	10.0.1.28/32	00:0c:6e:76:b8:a7	

10 Page 1

Figure 5.9 – Teachers network object configuration




Figure 5.10 – Student network object configuration

## Network Services

Network service is the abstraction of one or more applicable protocols that can be used in other eBox modules (eBox Technologies SL 2010, 45). The *network service* is very similar to network object, but here, we will be dealing with protocols, applications and ports.

In eBox, the management of network services requires the name of the service, protocol, source port and the destination port allocated to the application. Also, network administrators have to indicate if the service is internal or external. A *service* is internal if it is running in the eBox machine. Usually, it is always advisable to allow any source port because a client uses any source port to connect to a known destination port. The eBox network services created will be used in other eBox modules such as traffic shaping, firewall e.t.c. Figure 5.11 shows the list of services created and enabled in this project while Figure 5.12 and Figure 5.13 shows the service configuration for Asterik (used for VOIP) and HTTP service.


Logout Save changes


**Core**  
 Dashboard  
 Module Status  
 System  
 Network  
 Objects  
 Services  
 Monitor  
 Logs  
 Events  
 Backup  
 Software Management  
**Gateway**  
 HTTP Proxy  
 Traffic Shaping  
**UTM**  
 Firewall  
 IDS  
 VPN  
 Antivirus  
 Mail Filter  
**Infrastructure**  
 DHCP  
 DNS  
 Web Server  
 Certification Authority  
**Office**  
 Users  
 Groups

**Services** [\(show help\)](#)  
 List of services  
[Add new](#)

Service name	Description	Internal	Configuration	Action
Asterisk	eBox VoIP system	✓		
HTTP software	software service to update packages via apt	✗		
Mail system	eBox Mail System	✓		
POP Transparent proxy	POP transparent proxy	✓		
POP3	POP3 protocol	✓		
any	any protocol and port	✗		
any TCP	any TCP port	✗		
any UDP	any UDP port	✗		
dhcp	--	✓		
dns	--	✓		
eBox administration	eBox Administration port	✓		
http	--	✓		
ipp	--	✓		
ldap	--	✓		
ntp	--	✓		
samba	File sharing (Samba) protocol	✓		
ssh	ssh	✗		
tftp	--	✓		
usercorner	--	✓		

Page 1

Figure 5.11 – Network Services created and configured


Logout Save changes

**Core**  
 Dashboard  
 Module Status  
 System  
 Network  
 Objects  
 Services  
 Monitor  
 Logs  
 Events

**Service configuration**  
[Add new](#)

Protocol	Source port	Destination port	Action
UDP	any	5036	
UDP	any	10000:20000	
UDP	any	5060	
UDP	any	4569	

Page 1

Figure 5.12 – Asterik Service configuration

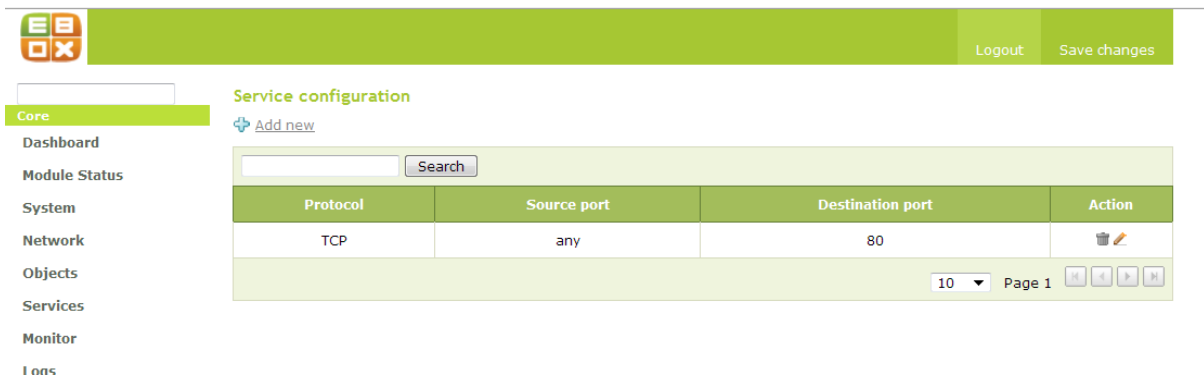


Figure 5.13 – HTTP Service configuration

### 5.2.2 Firewall

A Firewall is an application which ensures the security policies between networks connected to one another. In firewall configuration, the network administrator must define series of security/access policies by using traffic filtering rules based on the ports, protocols, source and destination IP address and physical address. For *Firewall* implementation, eBox uses *Netfilter*. Netfilter is a security tool that offers *packet filtering* and *Network Address Translation* (NAT).

In this project, eBox was made to act as firewall and the gateway to WAN. The external interface must be specified in order for the *Firewall* module to establish the filtering policies created. By default, eBox has established a policy for external interfaces to deny all connection attempts to eBox and denies all connection attempts to internal interface excepts when the internal service has been created in the *Services* module.

Configuring the eBox *Firewall* module requires creating filtering rules to control and check the traffic from a local or remote service if they can be accepted or not. In eBox *Firewall* configuration, network administrators can control traffic using five types of network traffic control options. These options are;

- Traffic from an internal network to eBox.
- Traffic among internal networks and from internal networks to the Internet.

- Traffic from eBox to external networks.
- Traffic from external network to eBox.
- Traffic from external networks to internal networks.

Configuring the *Firewall* module was relatively easy, as it is network object – configured. Any network traffic rule can be enabled on any network object. For example, the *Management* object can be restricted from accessing the internet or using some services on eBox. The *Firewall* access rule has a *source* and *destination* which would depend on the type of filtering used.

When eBox finally filters a traffic, it makes a decision which can either be to accept the connection or deny the connection and inform the source that connection cannot be established.

The Figure 5.14 below shows the packet filtering from *Internal networks to eBox* in this project.

The screenshot shows the 'Packet Filter' configuration page for 'Internal networks to eBox'. A table lists various rules with columns for Decision, Source, Service, Description, and Action. The rule for 'ssh' under the 'VPN' category is highlighted with a red border.

Decision	Source	Service	Description	Action
↑	Any	ipp	--	🗑️✏️⬆️⬇️⬆️
↑	Any	samba	--	🗑️✏️⬆️⬇️⬆️
↑	Any	ntp	--	🗑️✏️⬆️⬇️⬆️
↑	Any	RADIUS	--	🗑️✏️⬆️⬇️⬆️
↑	Any	dns	--	🗑️✏️⬆️⬇️⬆️
↑	Any	dhcp	--	🗑️✏️⬆️⬇️⬆️
↑	Any	tftp	--	🗑️✏️⬆️⬇️⬆️
↑	Any	http	--	🗑️✏️⬆️⬇️⬆️
↑	Any	POP Transparent proxy	--	🗑️✏️⬆️⬇️⬆️
↑	Any	ManageSieve	--	🗑️✏️⬆️⬇️⬆️
↑	Any	Mail system	--	🗑️✏️⬆️⬇️⬆️
↑	Any	Asterisk	--	🗑️✏️⬆️⬇️⬆️
↑	Any	usercorner	--	🗑️✏️⬆️⬇️⬆️
✖️	Any	ldap	--	🗑️✏️⬆️⬇️⬆️
↑	Any	ssh	--	🗑️✏️⬆️⬇️⬆️
↑	Any	eBox administration	--	🗑️✏️⬆️⬇️⬆️

Figure 5.14 – Packet filtering rules from *Internal network to eBox*

*ssh* was highlighted because a simple test was carried out using *ssh*. The *ssh* service was created but not added to the traffic rule in packet filtering from *internal network to eBox*. When user tried to connect to *ssh* from the local network, the connection was unsuccessful. When the *ssh* rule was added, the connection was successful. The logs of the connection denial can be checked in *eBox Logs* module. A subsequent test was equally done denying *ssh* connection in the packet filtering from *external network to eBox*. And the result of the logs can be seen in Figure 5.15.

The screenshot shows the 'Logs' section of the eBox interface. On the left is a navigation menu with categories like Core, Gateway, UTM, and Office. The main area is titled 'Logs (show help)' and includes a dropdown for 'Select available full reports: Firewall' and a 'View' button. Below this is a 'Custom query' section with date pickers for 'From date' (11 / March / 2010 - 15 : 17) and 'To date' (13 / March / 2010 - 15 : 17), a 'Refresh logs' checkbox, and input fields for 'Input interface', 'Output interface', 'Source', 'Destination', 'Protocol', 'Source port', and 'Destination port'. An 'Event' dropdown is set to 'Any'. 'Search' and 'Save as event' buttons are at the bottom of the query section.

Date	Input interface	Output interface	Source	Destination	Protocol	Source port	Destination port	Decision
2010-03-12 15:17:23	eth0		192.168.69.148	192.168.69.255	UDP	138	138	DROP
2010-03-12 15:17:23	eth0		192.168.69.148	192.168.69.255	UDP	138	138	DROP
2010-03-12 15:17:23	eth0		192.168.69.148	192.168.69.255	UDP	138	138	DROP
2010-03-12 15:17:23	eth0		192.168.69.148	192.168.69.255	UDP	138	138	DROP
2010-03-12 15:17:22	eth0		192.168.69.95	192.168.69.255	UDP	138	138	DROP
2010-03-12 15:17:22	eth0		192.168.69.95	192.168.69.255	UDP	138	138	DROP
2010-03-12 15:17:22	eth0		192.168.69.95	192.168.69.255	UDP	138	138	DROP
2010-03-12 15:17:19	eth0		192.168.69.49	192.168.69.255	UDP	138	138	DROP

Figure 5.15 – Log of *ssh* connection denial by firewall traffic from *external network to eBox*

## Port Redirection

Port redirection in eBox means *Network Address Translation* (NAT). This service checks the destination port address of an incoming packet and routes it to a host listening on a certain port that has been translated to the incoming packet port address. In this project, port redirection was not implemented.

### 5.2.3 Routing

Routing is the transfer/distribution of packets from a host to a network interface specified in an earlier made routing rule in the routing table. In a routing rule, the most important parameters to make a decision is the *router*, *interface* and the *destination address*. Routers must be accessible through interfaces in order for packets to be routed according to the rules set in the routing table.

In eBox, it is possible to manually set the routing table, but in this project, no routing rule was made, because *DHCP* was used.

## Gateway

In eBox, a gateway must be configured and enabled as the default gateway with the *eth0* (external interface) IP address if the *eth0* is statically configured. If eBox *eth0* is served by a DHCP server, no gateway should be configured.

In this project, eBox was made the gateway and statically configured as shown in Figure 5.16.

Enabled	Name	IP address	Interface	Weight	Default	Action
<input checked="" type="checkbox"/>	Gateway to LAN	195.148.173.62	eth0	1	<input checked="" type="checkbox"/>	

Figure 5.16 – Configured eBox gateway

#### **5.2.4 Traffic Shaping**

Traffic shaping is the control of network traffic in order to give priority to more important packets and guarantee performance and efficient bandwidth usage. Traffic shaping is a set of rule imposed on a set of packet to reduce or eliminate constraints such as delivery delay, low bit rate, packet loss, e.t.c. This is especially important when bandwidth is used by bandwidth demanding applications like multimedia data stream applications such as voice over IP and video over IP.

Quality of service (QoS) is the measure of the traffic shaping. eBox uses Linux kernel shaping using *token bucket* mechanism that allow to assign a limited rate, a guaranteed rate and a priority to certain types of data flows. To configure the eBox traffic shaping, an internal and external network interface and a configure gateway with a download and upload rate not equal to zero is needed.

In this project, traffic shaping was not needed because there was not congestion in the network.

#### **5.2.5 HTTP Proxy Setting**

HTTP Proxy is used to manage the bandwidth usage, control access and ensure security and surfing speed. HTTP proxy is an application between two connections using the HTTP protocol.

In eBox, the HTTP proxy service uses the *squid* as proxy and *Dansguardian* for content control. In this project, the configured HTTP proxy can be seen in “*HTTP advanced configuration*” section.

### **5.3 eBox INFRASTRUCTURE**

Before any module can be configured in eBox infrastructure, all eBox infrastructure modules and other supporting modules must be activated in the *Module Status* menu. In this package, four modules were activated and can be seen in Figure 5.17 below.



Module	Depends	Status
Network		<input checked="" type="checkbox"/>
Firewall	Network	<input checked="" type="checkbox"/>
Antivirus		<input checked="" type="checkbox"/>
DHCP	Network	<input checked="" type="checkbox"/>
DNS		<input checked="" type="checkbox"/>
Backup		<input checked="" type="checkbox"/>
Events		<input checked="" type="checkbox"/>
IDS	Network	<input checked="" type="checkbox"/>
Logs		<input checked="" type="checkbox"/>
Mail Filter	Network, Antivirus, Firewall	<input checked="" type="checkbox"/>
Monitor		<input checked="" type="checkbox"/>
Web Server		<input checked="" type="checkbox"/>
NTP		<input checked="" type="checkbox"/>

Figure 5.17 – eBox Infrastructure modules activation

### 5.3.1 Network Configuration Service (DHCP)

Network configuration is done by static method or dynamically by DHCP. DHCP means *Dynamic Host Configuration Protocol* and it's the protocols that allow network devices to request and obtain network parameters i.e. IP address, default gateway, network mask and the IP of the name servers. When network configuration is done statically, the entire network parameters are entered manually by the network administrator.

In eBox configuration, both interfaces (eth0 and eth1) and the DNS (Domain Name Service) have to be configured before DHCP configuration can be done. In this project, eth0 and eth1 were configured statically. The configuration of eth0 can be seen in Figure 5.18 and eth1 in Figure 5.19. Note that eth0 was marked as *external (WAN)*, with IP address – 195.148.173.50 in order to serve as the gateway to the LAN.

**Network Interfaces** (show help)

eth0 eth1

**!** You are connecting to eBox through this interface. If you set it as external the firewall will lock you out unless you add firewall rules to [Filtering rules from external networks to eBox](#) to allow access to the eBox administration port, SSH, ...

Name:

Method:

External (WAN):  Check this if you are using eBox as a gateway and this interface is connected to your Internet router.

IP address:

Netmask:

**Virtual Interfaces**

Name	IP address	Netmask	Action
<input type="text"/>	<input type="text"/>	255.255.255.0	<input type="button" value="⊕"/>

Figure 5.18 – eth0 Interface configuration

**Network Interfaces** (show help)

eth0 eth1

Name:

Method:

External (WAN):  Check this if you are using eBox as a gateway and this interface is connected to your Internet router.

IP address:

Netmask:

**Virtual Interfaces**

Name	IP address	Netmask	Action
<input type="text"/>	<input type="text"/>	255.255.255.0	<input type="button" value="⊕"/>

Figure 5.19 – eth1 Interface configuration

After the interfaces configuration, the DHCP was configured in the Common options tab of the DHCP menu, on eth1 with an IP range of 10.0.0.1 – 10.0.1.254. This can be seen in Figure 5.20. In the Dynamic DNS Option, dynamic DNS can be enabled and domain names can be allocated to clients based on their method of network configuration. The

Advanced Option was left un-configured because there was no lightweight server present in this project and the lease time was adequate.

Figure 5.20 – DHCP configuration on eth1

### 5.3.2 Name Resolution Service (DNS)

Domain Name System is a service which converts readable hostnames into IP address and vice versa (eBox Technologies SL 2010, 28). In eBox, DNS can be created in the DNS submenu under Network menu. Configuration of the created domain can be done in the DNS menu of the eBox Infrastructure. Many DNS domains can be configured but in this project, only one domain was configured with the name; sulazhy.com and IP address; 10.0.1.1. The created domain name can be seen in Figure 5.21 and the configuration of the domain can be seen in Figure 5.22.

Domain Name Server Resolver [\(show help\)](#)

Domain Name Server Resolver List

[Add new](#)

Search

Domain Name Server	Action
10.0.1.1	
193.166.140.200	
193.166.140.100	

10 Page 1

Search Domain

Domain:  Optional

Figure 5.21 – Domain Name Server list

DNS

List of Domains

[Add new](#)

Search

Domain	Hostnames	Mail Exchangers	Name Servers	IP Address	Dynamic	Action
sulazhy.com				10.0.1.1		

10 Page 1

Figure 5.22 – sulazhy.com domain name

In the configuration of the *sulazhy.com* domain, the hostnames were added to the domain as shown in Figure 5.23.



Figure 5.23 – Hostname in *sulazhy.com* domain

After the configuration of the eBox DHCP and DNS service, the *firewall* module must be configured to allow packets sent by eBox. For example, to ping, the firewall must be configured to allow *icmp* protocol. In our configuration, the *packet filter* submenu of the firewall module was configured to allow *http Service* in “*Packet Filtering from Internal Network*” in order to allow clients in the LAN to access the internet. This can be seen in Figure 5.24.

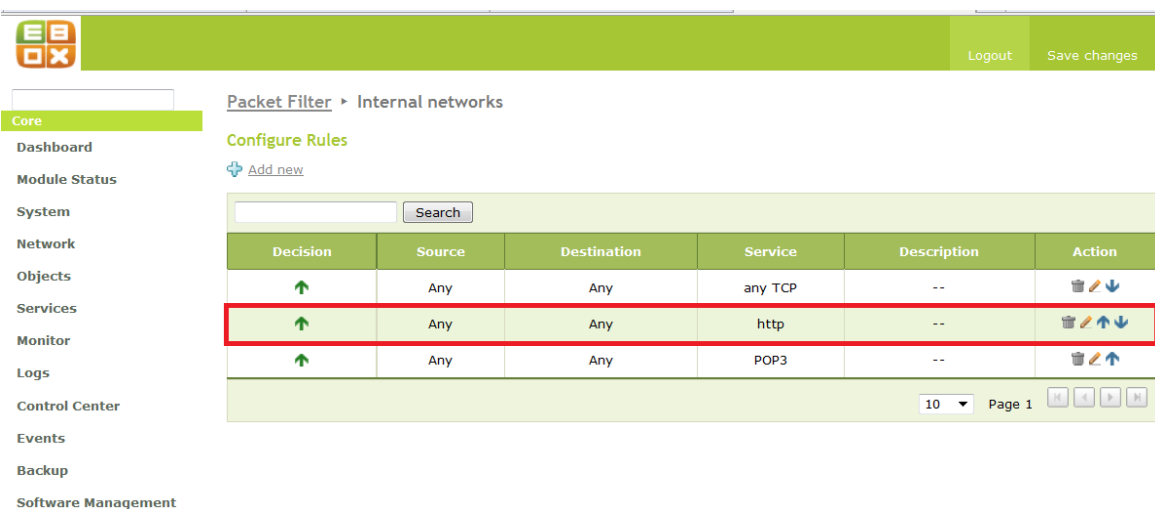


Figure 5.24 – Firewall configuration to allow http in Internal Network

However, the *Diagnostic Tools* submenu in the *Network Menu* was used to test the network configurations and the results are as shown in Figure 5.25, 5.26 and 5.27. Also an nslookup result from user aa@sulazhy.com computer can be seen in Figure 5.28.

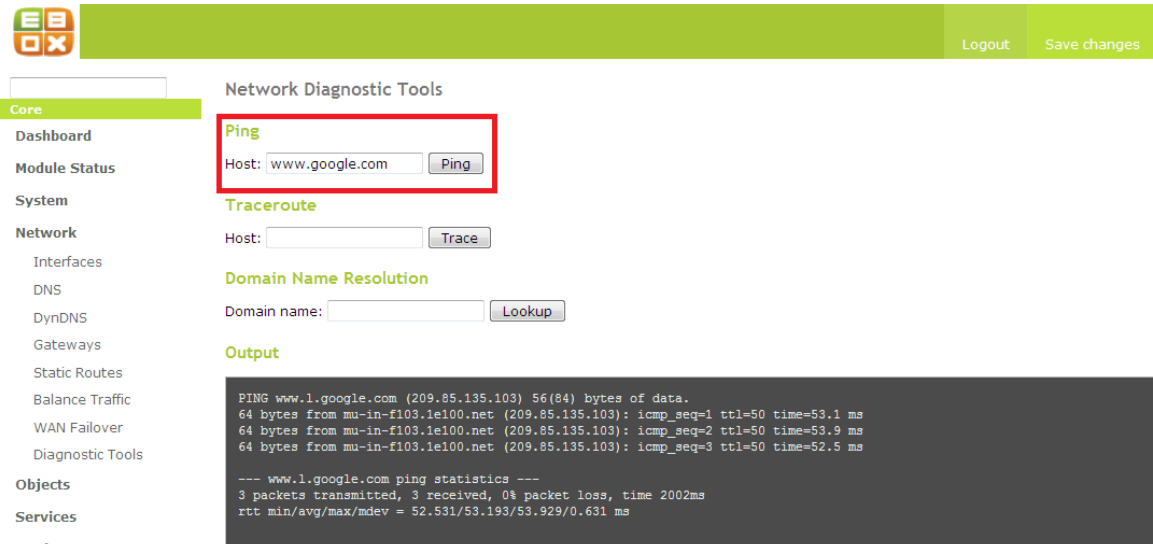


Figure 5.25 – ping result to www.google.com

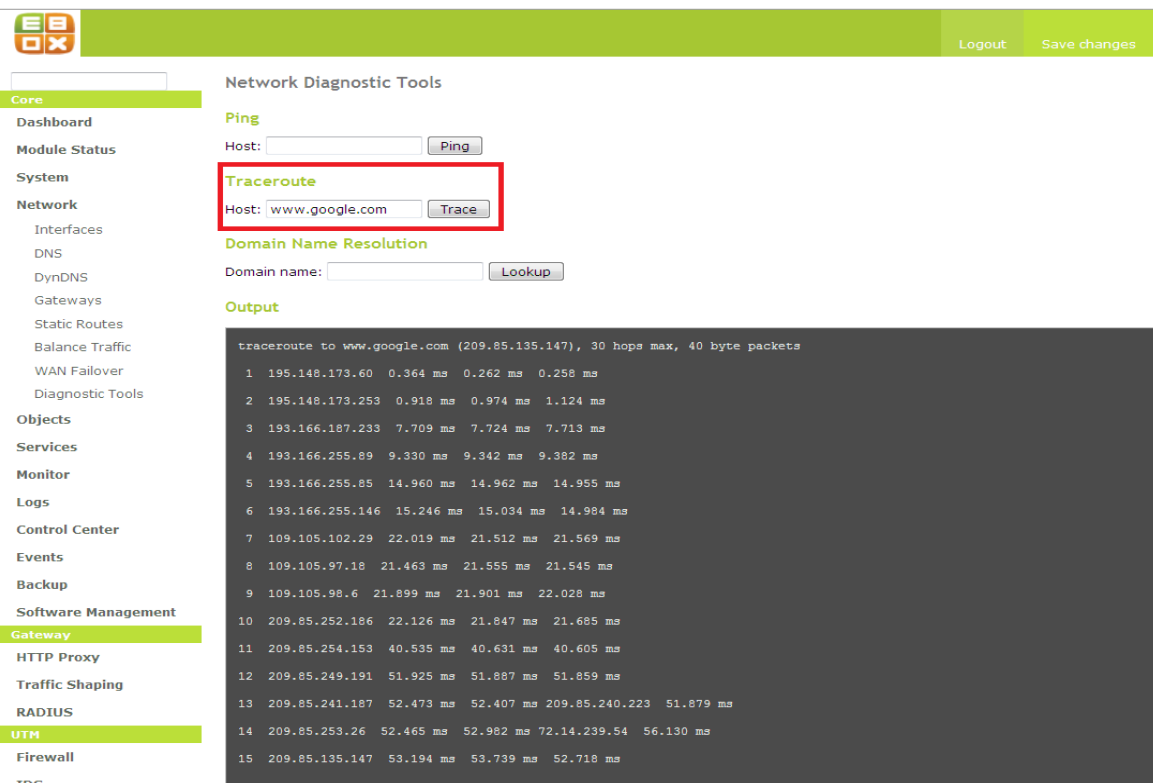


Figure 5.26 – traceroute result to www.google.com

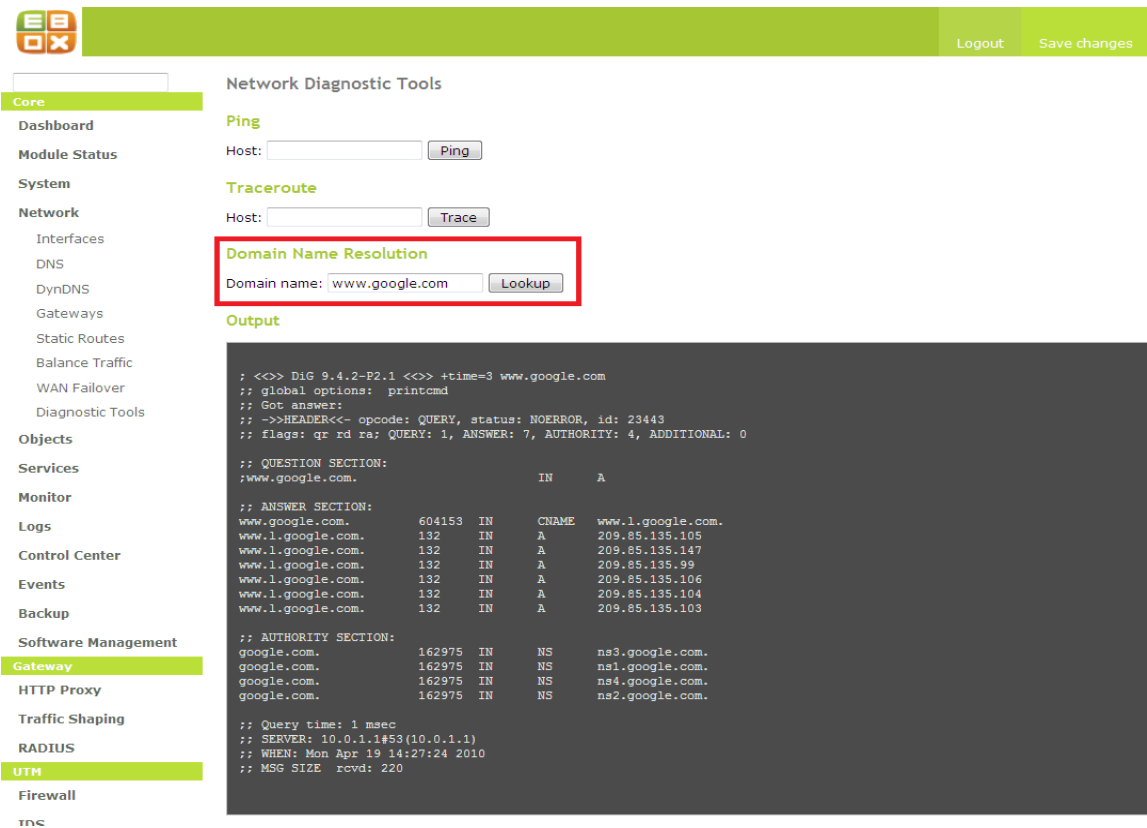


Figure 5.27 – nslookup result to www.google.com

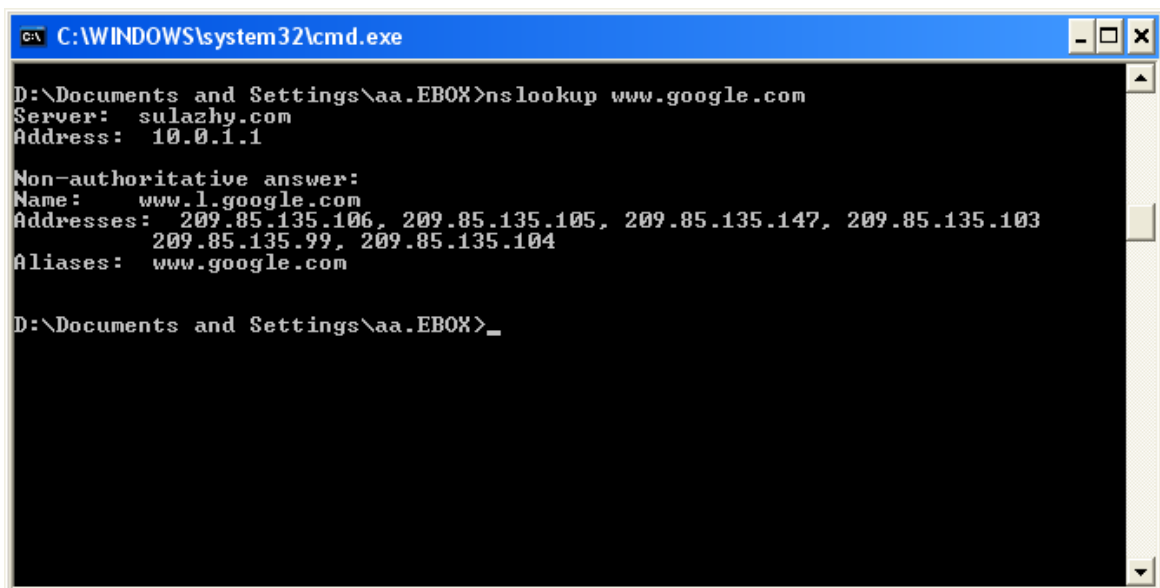


Figure 5.28 – nslookup result of www.google.com from user aa@sulazhy.com computer

### 5.3.3 Web Data Publication Service (HTTP)

Web data application service is available in eBox through the *Web Server* module. Web application operates using HTTP (HyperText Transfer Protocol). HTTP is a request and response protocol that uses TCP (Transport Control Protocol) default port 80 for unencrypted connections, and port 443 for encrypted connections (HTTPS) using TLS (Transport Layer Security) technology (eBox Technologies SL 2010, 35). Using HTTP, the client request for information from the server located within the same network or in a different network. The server processes the request and gives a response. eBox uses *Apache* web server for both its web interface and the web server module. In this project, the HTTP listening port was port 80 (Figure 5.29 and Figure 5.30) and was also tested with port 1600. This is illustrated in Figure 5.31 and Figure 5.32. In addition, eBox was used as a file server and our eBox users can publish web content by creating a subdirectory named *public\_html* in their private directory. To enable the *public\_html* per user, the “*Enable per user public\_html*” box must be ticked.

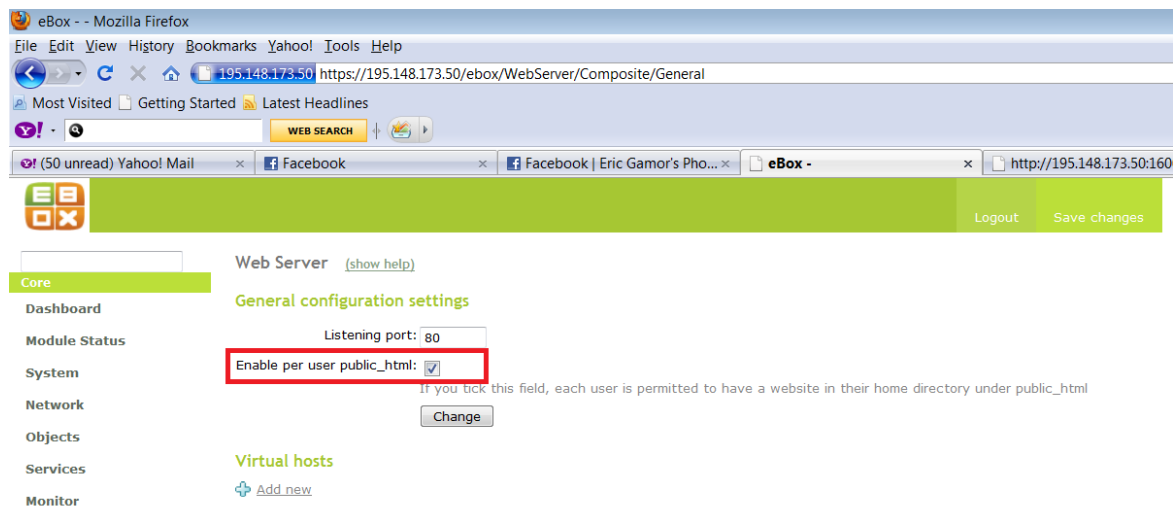
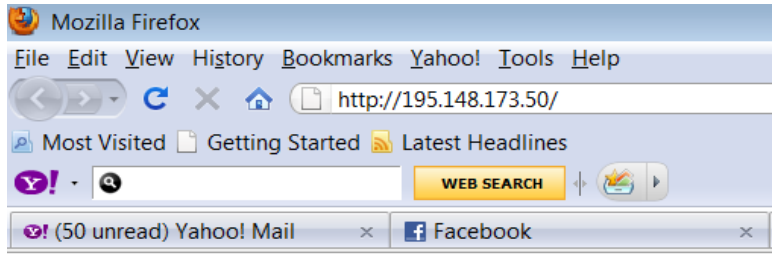


Figure 5.29 – Default listening port of HTTP (Port 80)





**It works!**

Figure 5.30 – Test of Apache Web Server in eBox on default port 80

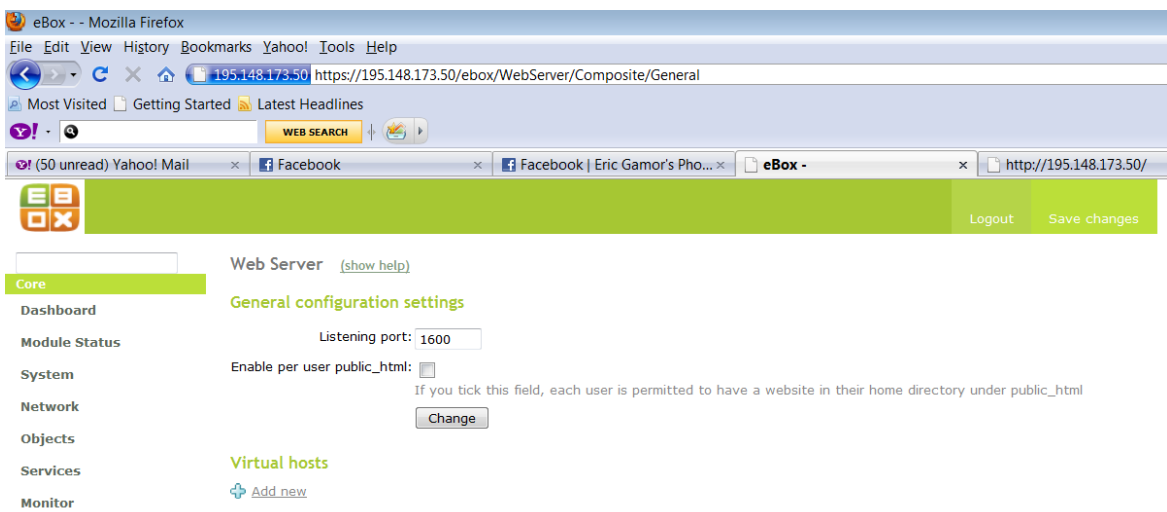
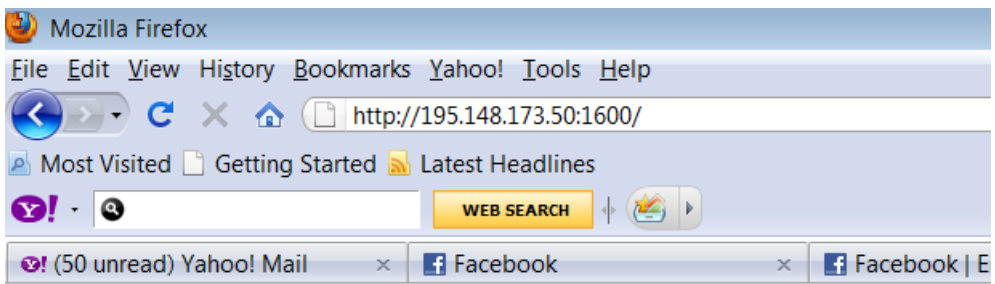


Figure 5.31 – Listening port of HTTP changed to Port 1600



**It works!**

Figure 5.32 – Test of Apache Web Server in eBox on Port 1600

Before testing the HTTP configuration, the firewall was configured to allow “any TCP” and “HTTP Software” services in the “External networks to eBox” option. eBox can also be used to create Virtual Domain in order to host websites for several domain names in the same eBox server.

### 5.3.4 Time Synchronization Service (NTP)

eBox can be configured as an NTP server using the Network Time Protocol. As seen in Figure 5.33, our eBox server was configured as an NTP server by first synchronizing it with “pool.ntp.org” as an NTP client.

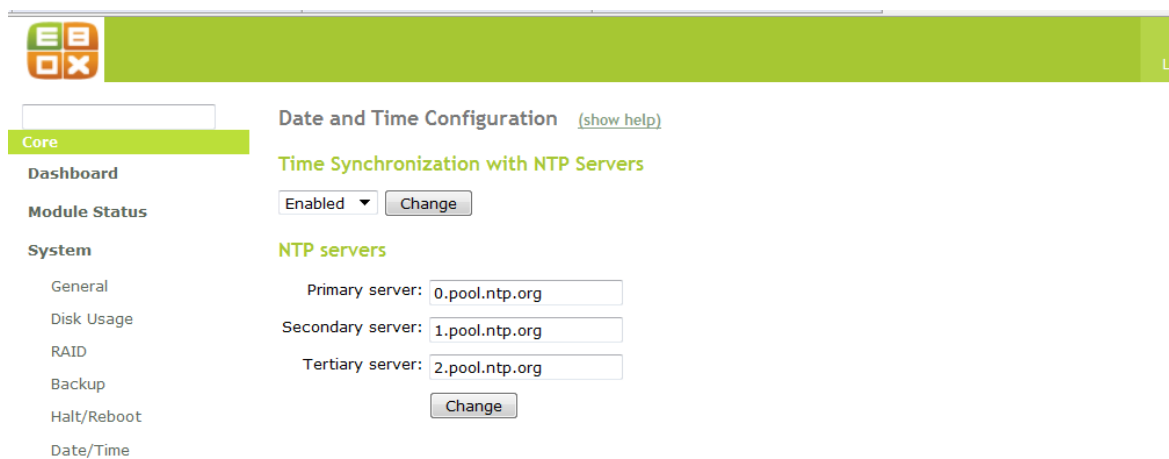


Figure 5.33 – eBox synchronized as an NTP client

## 5.4 eBox OFFICE

eBox office deals with the sharing of data and resources on the network. In this section, directory service, file sharing and remote authentication, printer sharing and groupware service were implemented. Before any module was configured in eBox Office, the eBox Office module and related module i.e. *Users and groups*, *Jabber*, *Mail*, *RADIUS*, *File sharing*, *Users Corner* and *Printer Sharing* were activated in the *Module Status Configuration* menu.

### 5.4.1 Directory Service (LDAP)

With eBox directory service, users and groups are created, and their data are sorted and stored in the organization network. This service allows share access to network users and gives a data access interface in order to handle the authentication process of each user when making attempt to use available network resources (eBox Technologies SL 2010, 73).

#### Users and Groups

In this project, users and groups were created as shown table 5.1, table 5.2, table 5.3 and table 5.4.

Table 5. 1

S/No	Last Name	First Name	Username/E-Mail	Password
1	Smith	Johnson	js@sulazhy.com	johnson
2	Gate	Alan	al@sulazhy.com	alan
3	Administrator	Admin	aa@sulazhy.com	admin

Table 5.1 – Management Group Members

Table 5. 2

S/No	Last Name	First Name	Username/E-Mail	Password
1	Liu	Gao	gl@sulazhy.com	liu
2	Chao	Yang	yc@sulazhy.com	chao
3	Makela	Naomi	nm@sulazhy.com	makela
4	Ghodrat	Menani	mg@sulazhy.com	ghodrat
5	Smail	Ghampour	gs@sulazhy.com	smail
6	Adebayo	Emmanuel	ea@sulazhy.com	adebayo
7	Ndzibah	Agbejule	an@sulazhy.com	ndzibah
8	Carl	Seppo	sc@sulazhy.com	carl

Table 5.2 – Teachers Group Members

Table 5. 3

S/No	Last Name	First Name	Username/E-Mail	Password
1	Makinen	Monika	mm@sulazhy.com	monika
2	Aalto	Borje	ba@sulazhy.com	borje
3	Lam	Joseph	jl@sulazhy.com	joseph
4	Mukaila	Adebayo	am@sulazhy.com	adebayo

Table 5.3 – Non-Teachers Group Members

Table 5. 4

S/No	Last Name	First Name	Username/E-Mail	Password
1	Odun	Abiola	s0600100@sulazhy.com	abiola
2	Makela	Johnson	s0600101@sulazhy.com	johnson
3	Mirka	Halonen	s0600102@sulazhy.com	halonen
4	Olusanya	Adura	s0600103@sulazhy.com	adura
5	Salam	Adeola	s0600104@sulazhy.com	adeola
6	Taofeek	Fillin	s0600105@sulazhy.com	fillin
7	Joke	Jacob	s0600106@sulazhy.com	jacob
8	Emmanuel	Anderson	s0600107@sulazhy.com	anderson
9	Mattison	Lumberg	s0600108@sulazhy.com	lumberg
10	Soikilla	Evra	s0600109@sulazhy.com	evra
11	Koskiniemi	Marti	s0600110@sulazhy.com	marti
12	Malmi	Nurmi	s0600111@sulazhy.com	nurmi

Table 5.4 – Students Group Members

In Figure 5.34 and Figure 5.35 the created groups and the created users can be seen.

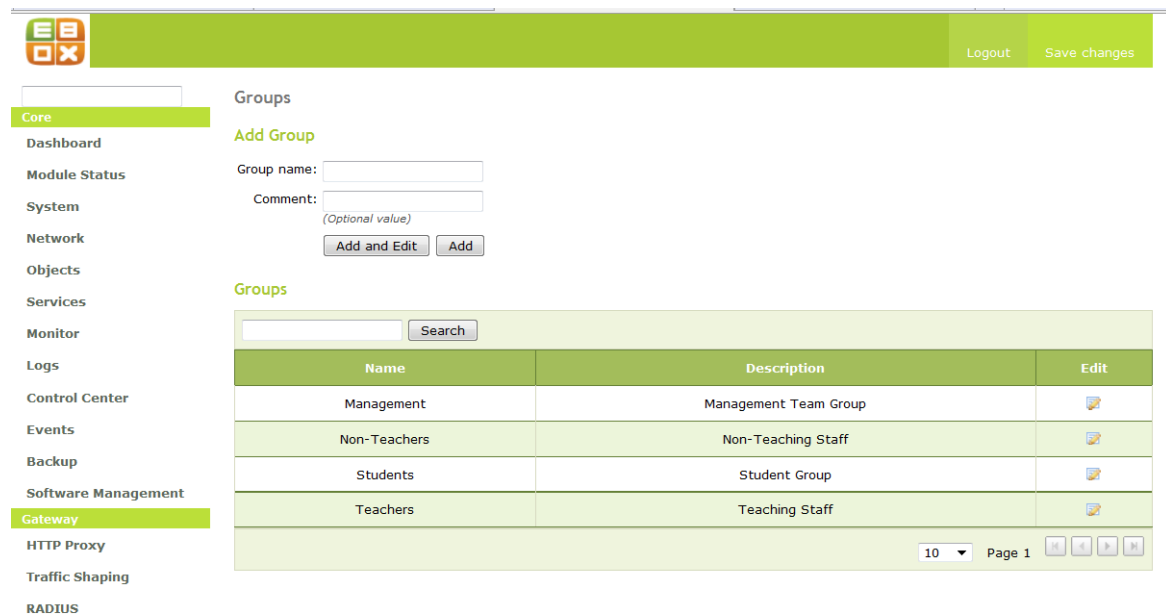


Figure 5.34 – Created Groups on sulazhy.com domain

The screenshot displays a web-based user management interface. On the left, a sidebar lists various system modules: Core, Gateway, UTM, and Infrastructure. The main content area is titled 'Users' and features an 'Add User' form with fields for User name, First name, Last name, Comment, Password, Retype password, and Group. Below the form are 'Add' and 'Add and Edit' buttons. A table below the form lists existing users with columns for Name, Full name, and Edit. The table contains 10 rows of user data. At the bottom right, there is a search bar, a dropdown menu showing '10', and pagination controls indicating 'Page 1 of 3'.

Name	Full name	Edit
aa	Admin Administrator	
ag	Alan Gate	
am	Adebayo Mukaila	
an	Agbejule Ndzbah	
ba	Borje Aalto	
ea	Emmanuel Adebayo	
gl	Gao Liu	
gs	Ghampour Smail	
jl	Joseph Lam	
js	Johnson Smith	

Figure 5.35 – Created Users on sulazhy.com domain

After creating the groups, the groups were configured to use *Asterik* group queue, *eGroupware*, *e-mail*, *shared directory* for the users in same group and *printer*. *Management* group configuration can be seen in Figure 5.36.

Also, all users created in this project was be configured to have and use;

- Jabber server account (for Instant Messaging).
- PDC and File sharing with a customized quota of 100MB.
- HP\_C4480 printer access and permission.
- E-mail account and aliases for the e-mail.
- eGroupware applications like webmail, calendar, address book, translation tools e.t.c.
- Asterik service. i.e. telephone extension.

The configuration of a user (*Alan gate*) can be seen in Figure 5.37. Only users in the *Management* group were given administrative right so they could carry out administrative task.

Groups > Management [\(show help\)](#)

**Administration of group Management**

Comment: Management Team Gr

**Users in group**      **Users not in group**

js	am
ag	an
aa	ba
	ea
	el
	gs
	jl
	mg

**Asterisk group queue**

Group queue:

Extension:

**eGroupware group**

Permissions template:

**Mail alias settings**

Mail alias	Action
<input type="text" value=""/> sulazhy.com	<input type="button" value="+"/>
management@sulazhy.com	<input type="button" value="🗑"/>

**Sharing directory for this group**

Directory name:

**Printers**

Select the printers this user will have access to.

Printer	Allow
HP_C4480	<input checked="" type="checkbox"/>
<b>Allow all printers</b>	<input checked="" type="checkbox"/>

Figure 5.36 – Management group configuration



[Logout](#)   [Save changes](#)

Core

- Dashboard
- Module Status
- System
- Network
- Objects
- Services
- Monitor
- Logs
- Control Center
- Events
- Backup
- Software Management

Gateway

- HTTP Proxy
- Traffic Shaping
- RADIUS

UTM

- Firewall
- IDS
- VPN
- Antivirus
- Mail Filter

Infrastructure

- DHCP
- DNS
- Web Server
- Certification Authority

Office

- Users and Groups
  - Users
  - Groups
  - Default User Template
  - LDAP Info
  - Slave Status
- User Corner
- File Sharing
- Printer Sharing

Groupware

Communications

- Mail
- Jabber
- VoIP
- Webmail

[Users](#) > [ag](#) [\(show help\)](#)

### Administration of user **ag**

First name:   
Last name:   
Comment:   
Password:   
Retype password:

#### User groups

Management

#### Other groups

Teachers  
Non-Teachers  
Students

### Asterisk account

User account:   
Extension:

### eGroupware account

Permissions template:

### Jabber Account

User account:   
Administration rights:

### Mail account settings

Mail address:    
Quota type:   
Maximum mailbox size in MB:

### Create mail aliases

Mail alias	Action
<input type="text" value=""/> @ <input type="text" value="sulazhy.com"/>	<input type="button" value="⊕"/>
alan.gate@sulazhy.com	<input type="button" value="🗑"/>

### PDC/File sharing account

User account:   
Administration rights:   
Disk quota limit (MB):

### Printers

Select the printers this user will have access to.

Printer	Allow
HP_C4480	<input checked="" type="checkbox"/>
<b>Allow all printers</b>	<input checked="" type="checkbox"/>

### Delete user

★ This operation will cause the removal of the user and all dependent data such as mail accounts, user files, etc.

eBox created by [eBox Technologies S.L.](#)

Figure 5.37 – User (Alan Gate) Configuration

In eBox Office, all *Samba* users are privileged to change their own data. Changing of data by a user can only be done in the *User Corner*. *User Corner* is a module that must first be enabled in the *Module Status*, and listens on port 8888. Users can be able to change their current password, set mail retrieval from external e-mail account and activate their voicemail configuration. In this project, all users were enabled to use user corner. User corner address and available services can be seen in Figure 5.38 and Figure 5.39.



Figure 5.38 – User Corner address link



Figure 5.39 – User Corner available services



## 5.4.2 File Sharing Service and Remote Authentication

### File Sharing

File sharing in eBox is done using SMB (Server Message Block)/CIFS (Common Internet File System) implementation for Linux. These are used to share access to files, printers, serial port and all other series of communication between nodes in a LAN. eBox uses Samba SMB/CIFS implementation for Linux as a file server, thus allow the allocation to each created user a personal directory and each group a shared directory for its users. In this project, eBox was made a file server, and shared directory was created for each group in our installation. The file sharing configuration can be seen in Figure 5.40.

The screenshot displays the eBox File Sharing configuration page. On the left is a sidebar menu with categories like Core, Dashboard, Module Status, System, Network, Objects, Services, Monitor, Logs, Control Center, Events, Backup, and Software Management. The main area is titled 'File Sharing' with a '(show help)' link. Below the title are tabs for 'General settings', 'PDC', 'Shares', 'Recycle Bin', and 'Antivirus'. The 'General settings' tab is selected, showing the following configuration options:

- Enable PDC:
- Domain name: EBOX
- Netbios name: Sulazhy-Ebox
- Description: EBox Samba Server
- Quota limit: Limited to 100 Mb
- Enable roaming profiles:
- Drive letter: U:
- Samba group: All users

A note below the Samba group dropdown states: 'Only users belonging to this group will have a samba account. Sync happens every hour'. A 'Change' button is positioned at the bottom of the configuration area.

Figure 5.40 – File Sharing Configuration

Figure 5.41 below shows how the shared directory for each group was created and configured. Shared directories can be created either by editing the group profile or through the *shares* in the *file sharing* menu. After the shared directories were created, access control was given to each group's directory. In each group, only members of the group can read and write files in the shared directory except members in the *Management* group which have administrator right. The allocation of the access control can be seen in Figure 5.42, 5.43, 5.44 and 5.45.

**File Sharing** [\(show help\)](#)

General settings | PDC | **Shares** | Recycle Bin | Antivirus

**Adding a new share**

Enabled:

Share name:

Share path: **Directory under eBox**   
Directory under eBox will automatically create the share.directory in /home/samba/shares  
 File system path will allow you to share an existing directory within your file system

Comment:

**Shares**

Enabled	Share name	Share path	Comment	Access control	Action
<input checked="" type="checkbox"/>	Teachers Public Share	Teachers_Public_Share	All users public share		
<input checked="" type="checkbox"/>	Student Public Share	Students_Public_Share	All users public share		
<input checked="" type="checkbox"/>	Non Teacher Public Share	Non_Teachers_Public_Share	All users public share		
<input checked="" type="checkbox"/>	Management Public Share	Management_Public_Share	All users public share		

10 Page 1

Figure 5.41 – Shared Directory for each group

**Shares** > Management Public Share

**Access Control**

[Add new](#)

User / Group	Permissions	Action
Management	Administrator	

10 Page 1

Figure 5.42 – Management Group Shared Directory Access Control

Shares > Teachers Public Share

Access Control

[Add new](#)

Search

User/Group	Permissions	Action
Teachers	Read and write	
Management	Administrator	
Students	Read only	
Non-Teachers	Read only	

10 Page 1

Figure 5.43 – Teachers Group Shared Directory Access Control

Shares > Non Teacher Public Share

Access Control

[Add new](#)

Search

User/Group	Permissions	Action
Students	Read only	
Management	Administrator	
Non-Teachers	Read and write	
Teachers	Read only	

10 Page 1

Figure 5.44 – Non Teacher Group Shared Directory Access Control

Shares > Student Public Share

Access Control

[Add new](#)

Search

User/Group	Permissions	Action
Non-Teachers	Read only	
Management	Administrator	
Teachers	Read and write	
Students	Read and write	

10 Page 1

Figure 5.45 – Student Group Shared Directory Access Control

## Remote Authentication and Primary Domain Controller (PDC)

PDC in eBox is a Linux implementation used to log into the system through remote access control using username and password. eBox as a PDC server was enabled in this project, as seen in Figure 5.40 and users were able to login into *sulazhy.com* domain from the clients in the LAN. After login, the personal directory and shared directories are mounted and mapped to the drive letter selected, on the domain registered computer the user is using if the “*roaming profiles*” is enabled. Figure 5.46 shows a user’s personal directory and the created group shares. However, eBox contains an antivirus and a recycle bin service. The recycle bin service creates a recycle bin folder in the personal directory of users if enabled in the file sharing submenu.

To register a PDC client computer to a domain, a user account with administrative rights is needed to configure the PDC client. All members of the *Management* group have administrative rights, so one of them was used to configure the PDC client.

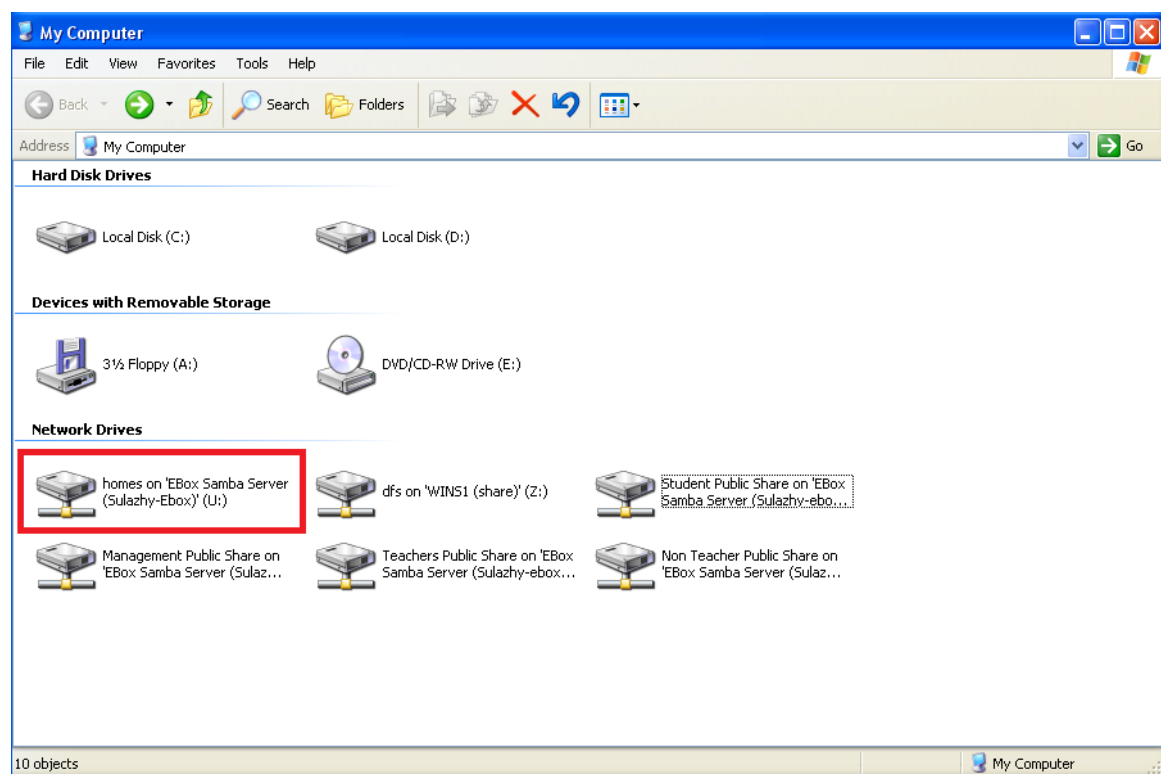


Figure 5.46 – Mounted personal directory and Shared Directories

### 5.4.3 Printer Sharing Service

Printer sharing service in eBox makes it possible to install and configure printers, and to allow or deny access to users and groups. Printers can be connected to eBox through several ways, but in this project, our HP printer named *HP\_C4480* was installed using USB connection. Figure 5.47 shows the list of installed printers.

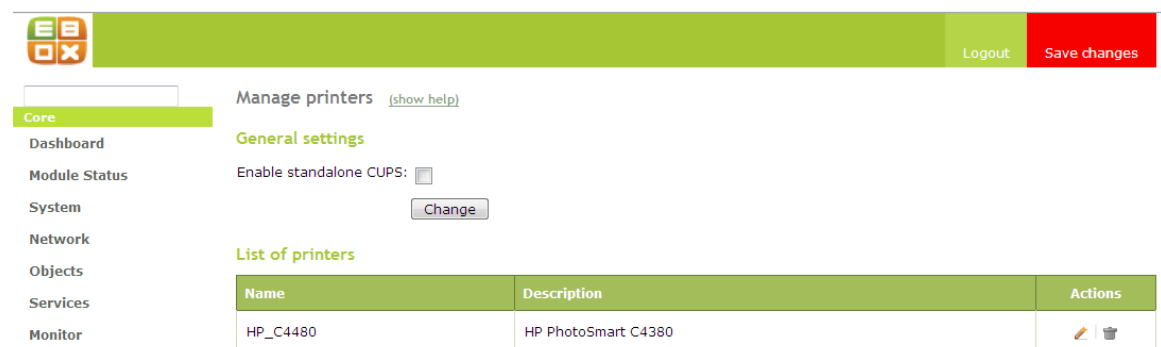


Figure 5.47 – List of installed printers

### 5.4.4 eGroupware Service

eGroupware is a software package comprising of different applications, and integrating the work of different users in a common project (eBox Technologies SL 2010, 92). In eBox, eGroupware works with the LDAP service (directory service) and have the following services available to users;

- Information Sharing: File sharing, calendar sharing, news, task lists, address books e.t.c
- Communication: Users communicates by e-mail, instant messenger e.t.c.
- Resource management, project management and time management e.t.c.

In this project, eGroupware was configured by selecting the created virtual domain (*sulazhy.com*) as seen in Figure 5.48, and configuring the IMAP service in the *eBox Unified Communication Package*.

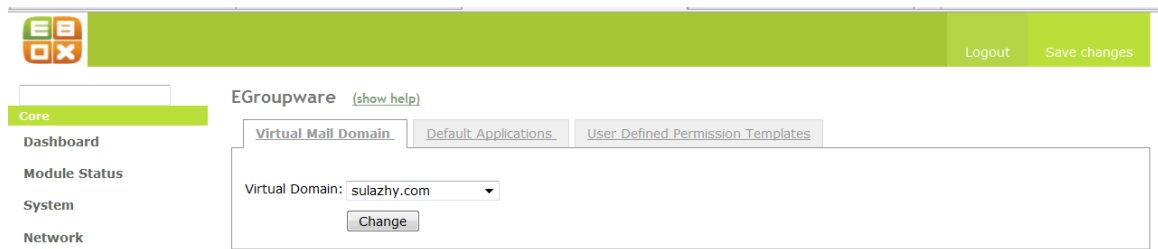
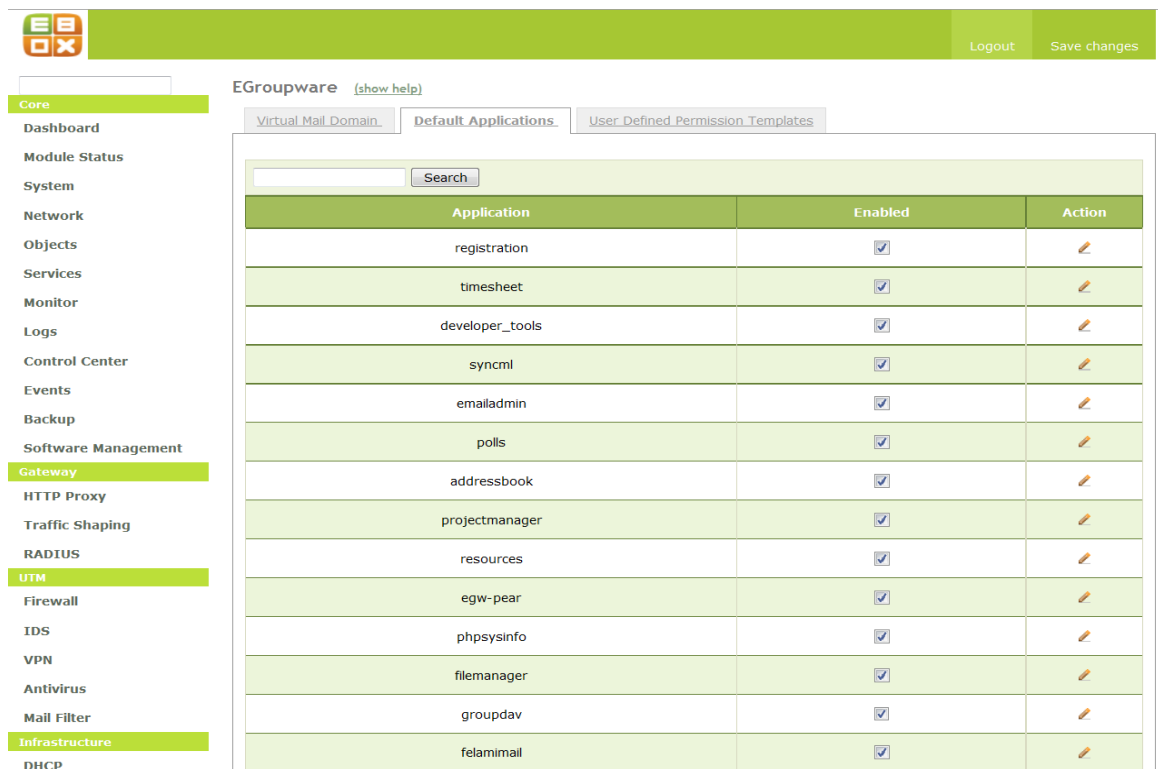


Figure 5.48 – Virtual domain (*sulazhy.com*) selected

In the *Default Application* tab of the eGroupware menu, the applications to be available to the users were selected. And the *user Defined Permission Template* tab can be used to define a permission template which would allow selected application to be available to the specified group, or user(s). This was left un-configured as we wanted all the users to have access to all the eGroupware applications. Figure 5.49 shows all eGroupware applications enabled.



DNS	preferences	<input checked="" type="checkbox"/>	
Web Server	tracker	<input checked="" type="checkbox"/>	
Certification Authority	notifywindow	<input checked="" type="checkbox"/>	
Office	phpbrain	<input checked="" type="checkbox"/>	
Users and Groups	notifications	<input checked="" type="checkbox"/>	
User Corner	news_admin	<input checked="" type="checkbox"/>	
File Sharing	calendar	<input checked="" type="checkbox"/>	
Printer Sharing	bookmarks	<input checked="" type="checkbox"/>	
Groupware	infolog	<input checked="" type="checkbox"/>	
Communications	admin	<input type="checkbox"/>	
Mail	workflow	<input checked="" type="checkbox"/>	
Jabber	phpgwapi	<input checked="" type="checkbox"/>	
VoIP	home	<input checked="" type="checkbox"/>	
Webmail	manual	<input checked="" type="checkbox"/>	
	etemplate	<input checked="" type="checkbox"/>	
	wiki	<input checked="" type="checkbox"/>	
		30	Page 1

eBox created by eBox Technologies S.L.

Figure 5.49 – Allowed application in eGroupware default template

After eGroupware configuration, eGroupware was tested as shown in Figure 5.50.

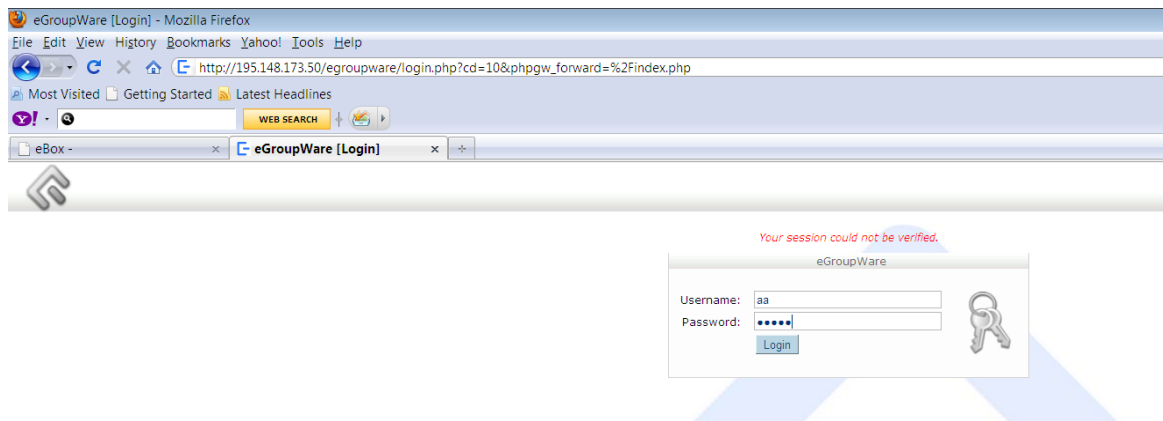


Figure 5.50 – eGroupware login page

## 5.5 eBOX UNIFIED COMMUNICATIONS

eBox Unified Communication package consists of modules responsible for communication in eBox. The package contains electronics mail service, instant messaging and voice over IP.

### 5.5.1 Electronic Mail Service

eBox electronic mail service, like other mail service is a store and forward method, using SMTP (Simple Mail Transfer Protocol) and IMAP(Internet Access Message Protocol)/POP3 (Pop Office Protocol).

Configuring the eBox electronic mail service, the *Mail Server Options* tab was configured as shown in Figure 5.51 below. It can be seen in Figure 5.51 that in our configuration, users are required to authenticate in order to send email through the server. In the *Relay policy for network objects* tab, we created relay policy for the four network object we have. This will allow the mail server to recognise all network hosts thereby preventing spam messages. Figure 5.52 shows the network object relay policy.



- Core
- Dashboard
- Module Status
- System
- Network
- Objects
- Services
- Monitor
- Logs
- Control Center
- Events
- Backup
- Software Management
- Gateway
- HTTP Proxy
- Traffic Shaping
- RADIUS
- UTM
- Firewall
- IDS
- VPN
- Antivirus
- Mail Filter
- Infrastructure
- DHCP
- DNS
- Web Server
- Certification Authority
- Office
- Users and Groups
- User Corner
- IDS
- VPN
- Antivirus
- Mail Filter
- Infrastructure
- DHCP
- DNS
- Web Server
- Certification Authority
- Office
- Users and Groups
- User Corner

### Mail server

Mail server options
Relay policy for network objects
Mail filter options

**Authentication**

TLS for SMTP server:

Require authentication:   
Users will have to authenticate to be able to send mails through this server

[Change](#)

**Options**

Smarthost to send mail:   
*Optional* The format is host[:port] being port set to 25 if none is supplied

Smarthost authentication:

Server mailname:

Postmaster address:   
Address used to report mail problems

Maximum mailbox size allowed:   
When a mailbox reaches this size further messages will be rejected. This can be overridden by account

Maximum message size accepted:

Expiration period for deleted mails:   days

Expiration period for spam mails:   days

[Change](#)

**Mail retrieval services**

POP3 service enabled:

Secure POP3S service enabled:

IMAP service enabled:

Secure IMAPS service enabled:

Retrieve mail for external accounts:   
This allow users to retrieve mail for external accounts, the mail would be delivered to their local account. External account can be configured in the user's corner.

Manage Sieve scripts:   
This service allows to a user to manage his Sieve mail filtering scripts from a local client which speaks the ManageSieve protocol

[Change](#)

**Mail retrieval services**

POP3 service enabled:

Secure POP3S service enabled:

IMAP service enabled:

Secure IMAPS service enabled:

Retrieve mail for external accounts:   
This allow users to retrieve mail for external accounts, the mail would be delivered to their local account. External account can be configured in the user's corner.

Manage Sieve scripts:   
This service allows to a user to manage his Sieve mail filtering scripts from a local client which speaks the ManageSieve protocol

[Change](#)

Figure 5.51 – Configuration of eBox as a mail server

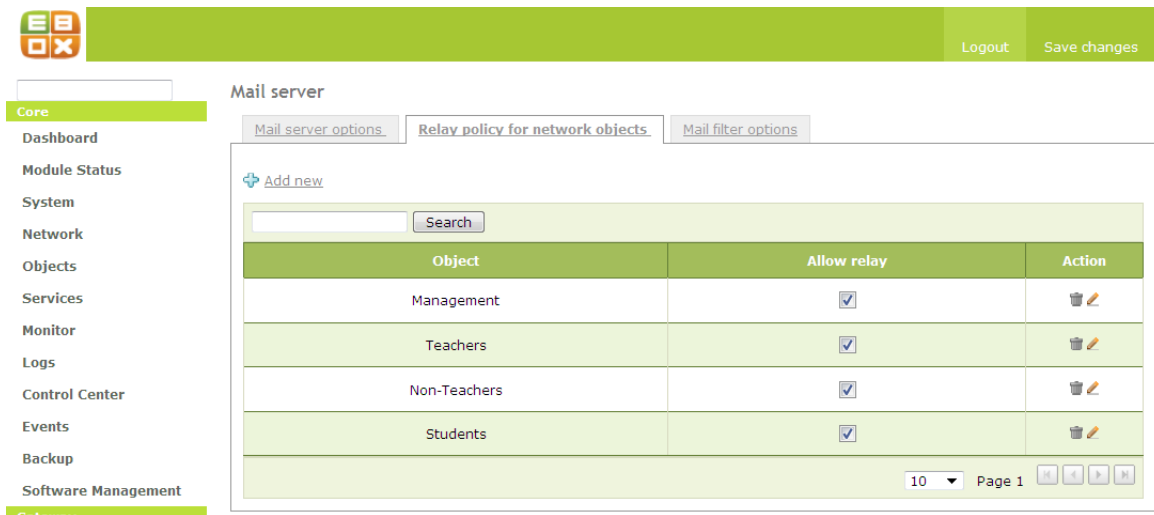


Figure 5.52 – Network object relay policy

Furthermore, in order to setup an email account for the eBox users, a virtual domain must be created. A virtual domain serves as the domain name for users email. Here, *sulazhy.com* virtual domain name was created and can be seen in Figure 5.53.

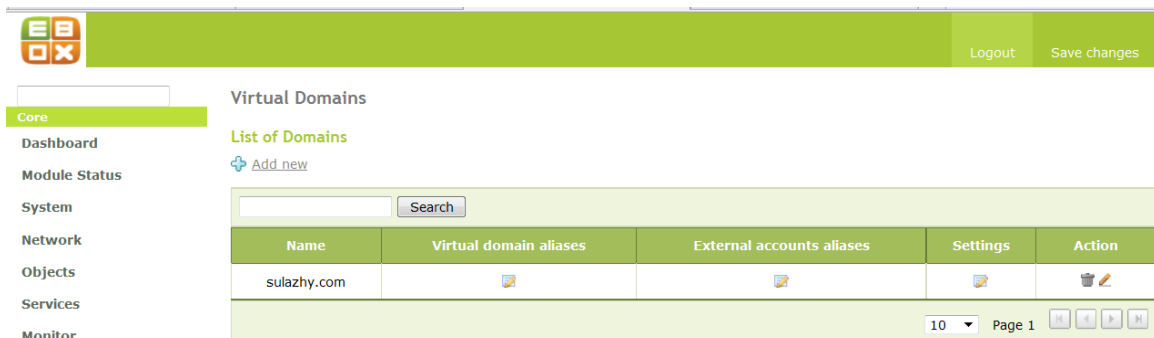


Figure 5.53 – Virtual domain *sulazhy.com* created

After all mail configurations were done, the testing was done and can be seen in Figure 5.54.

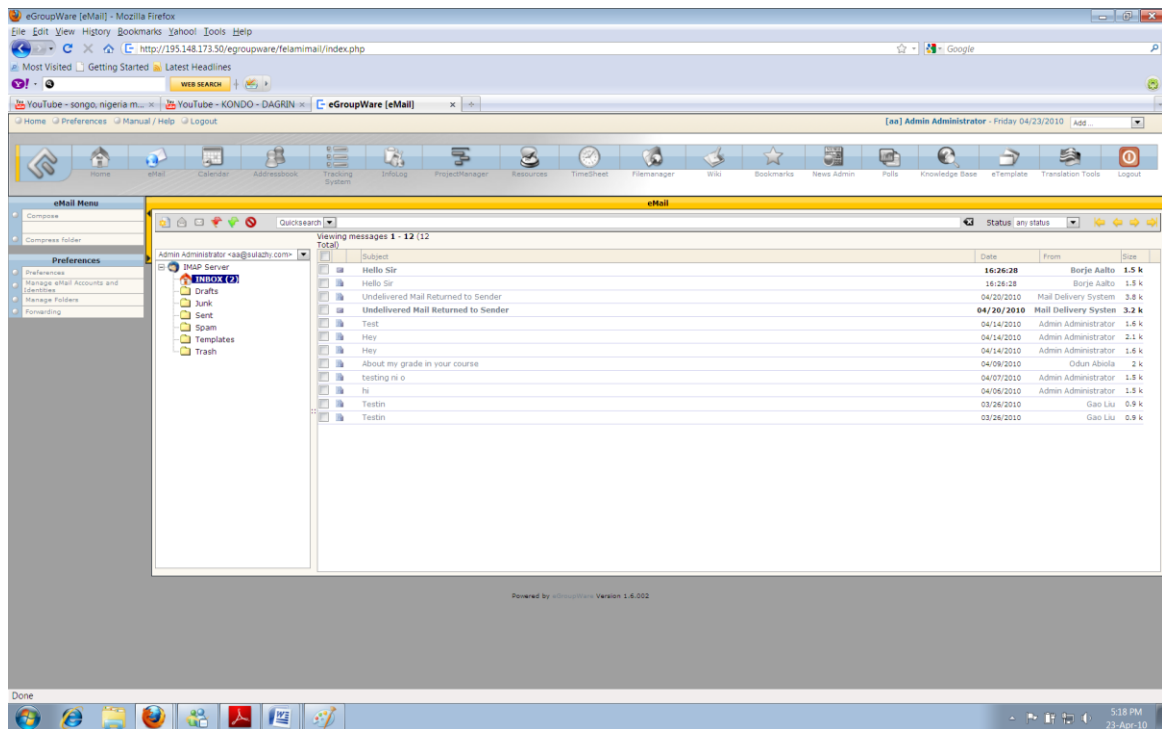


Figure 5.54 – Mail service tested

## 5.5.2 Instant Messaging (IM) Service

Instant messaging applications are used to manage list of people with which they exchange messages. IMs convert the asynchronous communication provided by email in a synchronous communication in which users can communicate in real time (eBox Technologies SL 2010, 107). IMs also have more features such as file transfer, video chat, real time voice exchange e.t.c.

However, eBox instant messaging service uses Jabber/XMPP as its protocol. In order for the IM to work, the Jabber/XMPP must be integrated with eBox user management. In our configuration of the IM, the *Jabber* general configuration was done as seen in Figure 5.55. When the jabber server has been configured, it is mandatory to configure the jabber client on each of the machines in the network.

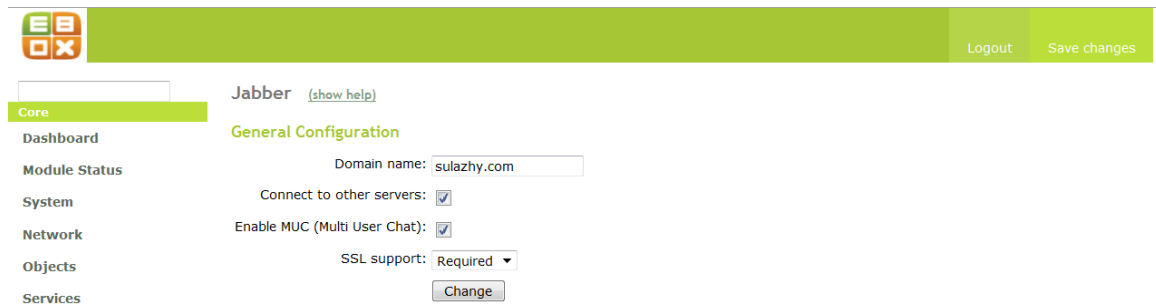


Figure 5.55 – IM Jabber configuration

### Instant Messaging Service Client Configuration

In our jabber client configuration, **Pidgin** was used. Pidgin is an instant messaging program which allows multiple accounts login on multiple chat networks simultaneously. In other words, users can chat with friends on other networks like yahoo, msn, goggle talk, e.t.c simultaneously. Pidgin supports multiple protocols including Jabber/XMPP.

Figure 5.56, 5.57 and 5.58 shows the configuration of *pidgin* client.

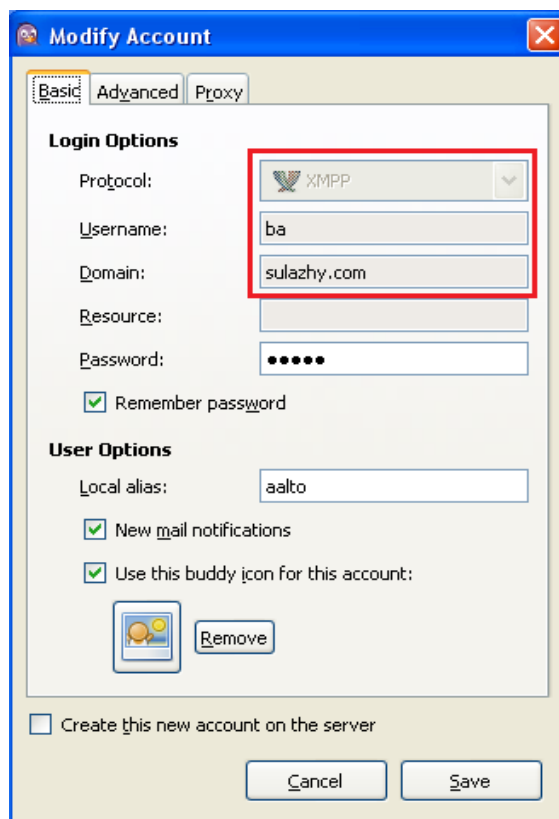


Figure 5.56 – Basic tab configuration of Jabber/XMPP IM client

Figure 5.56 above shows that *XMPP* jabber protocol was used to configure the client. And the user *ba* (*ba@sulazhy.com*) in the domain *sulazhy.com* was registered on the *pidgin*.

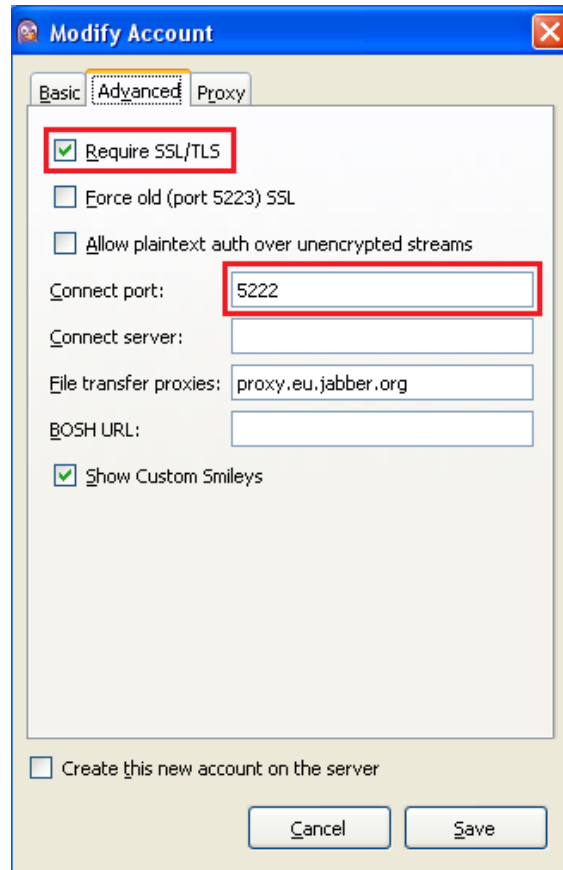


Figure 5.57 – *Advanced* tab configuration of Jabber/XMPP IM client

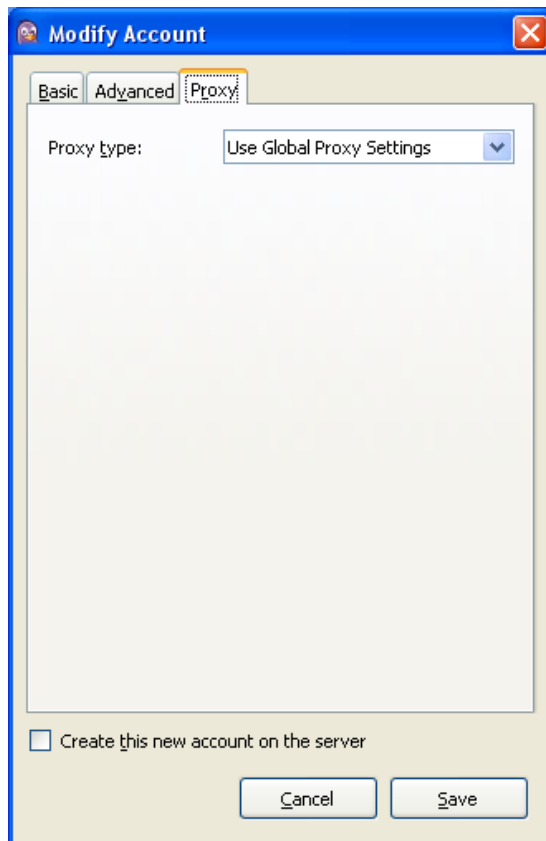


Figure 5.58 – Proxy tab configuration of Jabber/XMPP IM client

After the configuration, the account for *ba@suazhy.com* was registered on the client on the machine the *pidgin* was installed. After the client IM configuration, the user account must be enabled as in Figure 5.59.

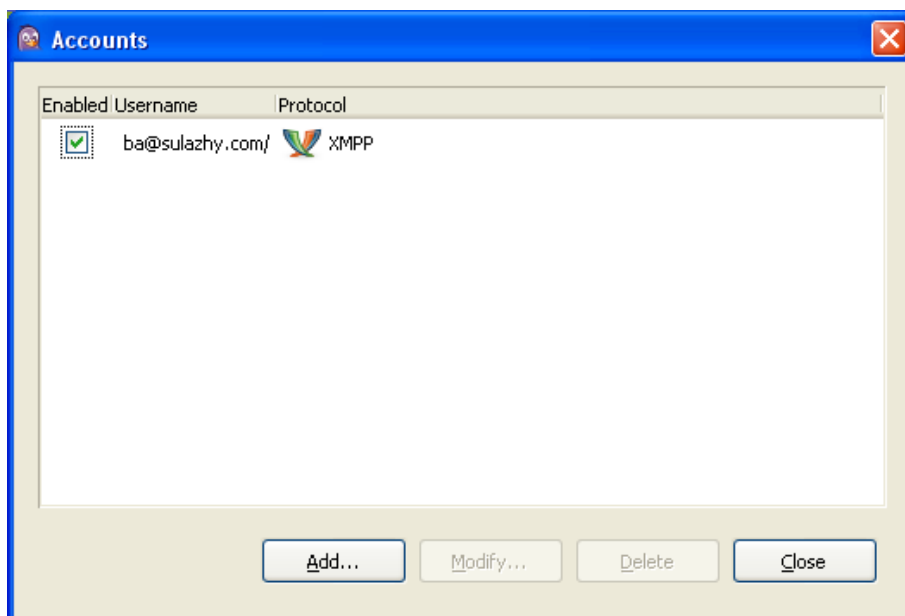


Figure 5.59 – Account *ba@sulazhy.com* created on pidgin installed on the computer

After all configurations and account creation, groups were added and friends were added as seen in Figure 5.60. Figure 5.61 and Figure 5.62 shows some IM sample chat.

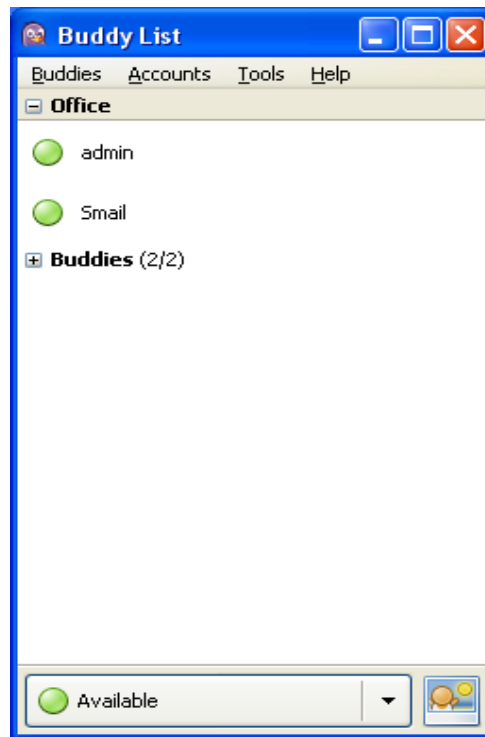


Figure 5.60 – Group and friend list

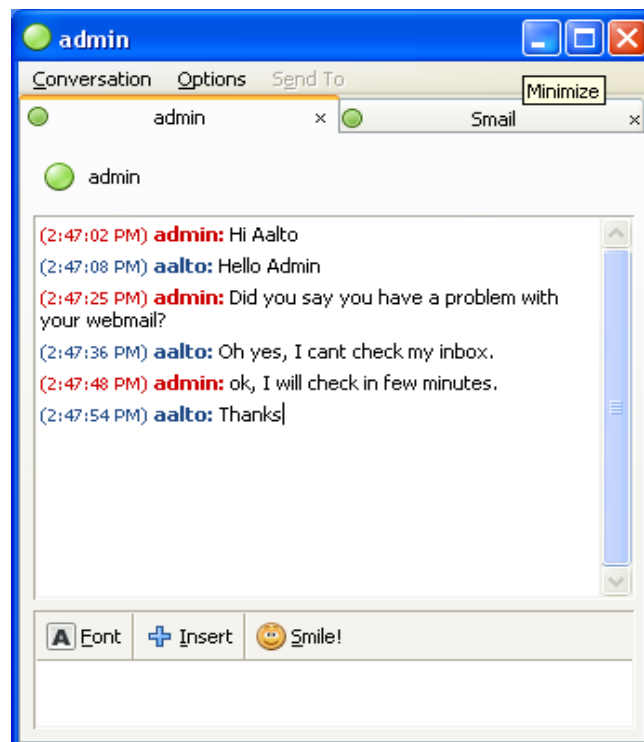


Figure 5.61 – Sample instance messaging chat with *aa@sulazhy.com*

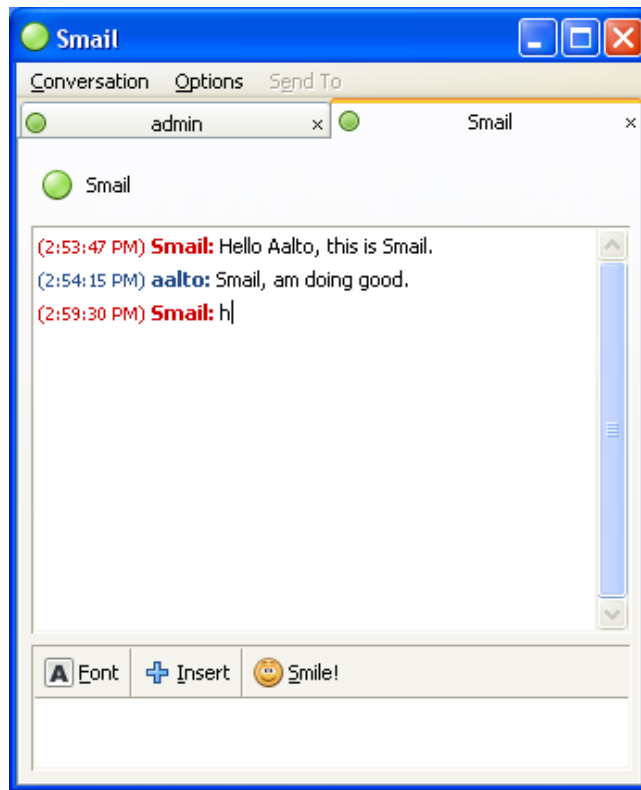


Figure 5.62 – Sample instance messaging chat with [sg@sulazhy.com](mailto:sg@sulazhy.com)

### 5.5.3 Voice over IP Service

In this project, the Voice over IP Service was not configured.

## 5.6 eBOX UNIFIED THREAT MANAGER

eBox Unified Threat Manager is the package responsible for preventing the network against external attacks, detecting possible intrusions into the network services, prevent spam mails and viruses, and secure connection to the local network using virtual private networks (eBox Technologies SL 2010, 123).

### 5.6.1 Mail Filter

Mail Filter is used to enhance security by filtering mails for spam and viruses. Spam use up some bandwidth and thereby affects the network and email services.

In this project, eBox default mail filter configuration was used.



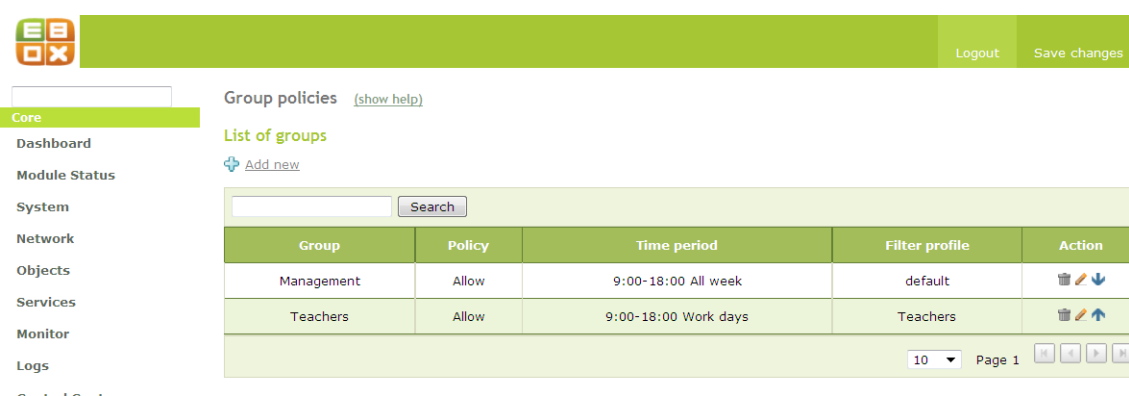
## 5.6.2 HTTP Proxy Advanced Configuration

In eBox HTTP advanced configuration, more advanced proxy settings are available. The advance setting involves group based filtering, group-based filtering for objects and filter profiles configuration. As compared to HTTP proxy service in *eBox Gateway* where the only filter profile is the *default filter profile*.

### Group Based Filtering

In the group based filtering, group were created by grouping computers in the same work area such as a department, a subnet or a class. Two groups were created and control access (*Authorize and allow all*) was set for both groups so that they could surf the internet. Also the use of content filtering solely depends on if there is a default policy or group policy that is set to filter. In our configuration, the two created groups were *Management group* and *Teachers group*. The *Management group* was set to use the *Default Filter Profile* and the *Teachers group* was set to use the created *Teachers Filter profile* (Figure 5.64). This can be seen in Figure 5.63 below.

The time period indicates the time they can surf the internet and while they do, the filtering policies will apply to the members of the groups.



The screenshot shows the 'Group policies' section of the eBox configuration interface. It features a search bar and a table with the following data:

Group	Policy	Time period	Filter profile	Action
Management	Allow	9:00-18:00 All week	default	[Delete] [Edit] [Down Arrow]
Teachers	Allow	9:00-18:00 Work days	Teachers	[Delete] [Edit] [Up Arrow]

At the bottom of the table, there is a pagination control showing '10' items per page and 'Page 1'.

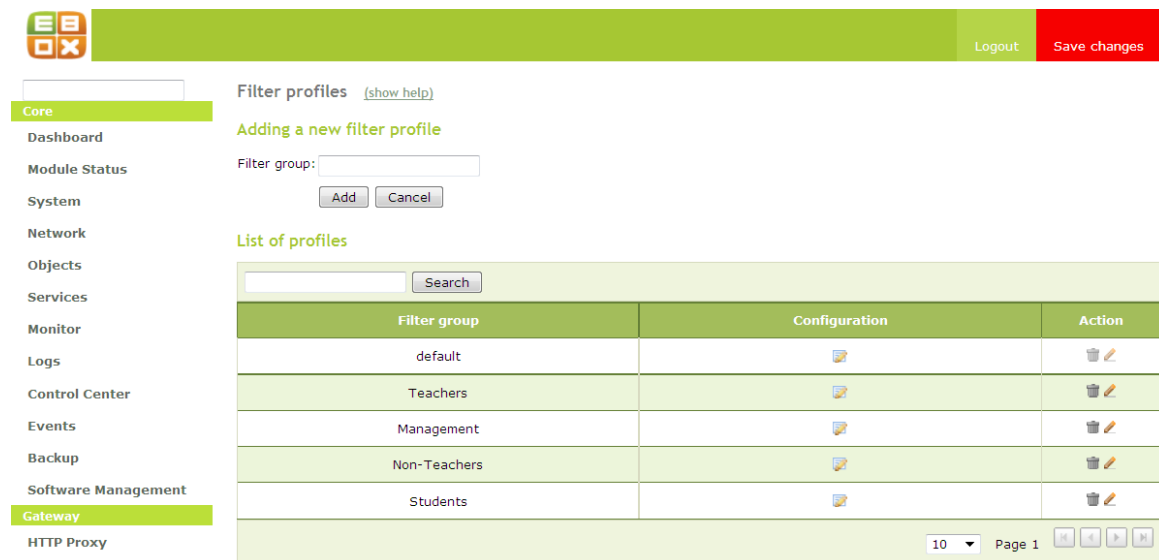
Figure 5.63 – List of created groups and their policies

## Group Based Filtering for Objects

Here, custom policies can be configured for network objects that always override the global policy. Here, created custom policies affects the filtering content of the groups concerned while group policies only affect to the permission for browsing only.

## Filter Profiles Configuration

In this section, filter profiles can be created and configured. Four new profiles were created for each of the created objects. The created filter profiles can be seen alongside the *default profile* in Figure 5.64.




The screenshot displays the 'Filter profiles' configuration page. At the top, there is a navigation bar with 'Logout' and 'Save changes' buttons. A sidebar on the left lists various system components, with 'Gateway' currently selected. The main content area is titled 'Filter profiles' and includes a 'show help' link. Below this, there is a section for 'Adding a new filter profile' with a 'Filter group:' input field and 'Add' and 'Cancel' buttons. The 'List of profiles' section features a search bar and a table with the following data:

Filter group	Configuration	Action
default		
Teachers		
Management		
Non-Teachers		
Students		

At the bottom right of the table, there is a pagination control showing '10' items per page and 'Page 1'.

Figure 5.64 – New filter profiles created

The configuration of the *default filter profile* is shown in Figure 5.65, 5.66 and 5.67. According to Figure 5.65, administrator can choice which file can be sent through the server. In this project, all file extensions were allowed.


Logout Save changes

Filter Profiles > default [\(show help\)](#)

**Core**  
 Dashboard  
 Module Status  
 System  
 Network  
 Objects  
 Services  
 Monitor  
 Logs  
 Control Center  
 Events  
 Backup  
 Software Management  
**Gateway**  
 HTTP Proxy  
   General  
   Objects' Policy  
   Groups' Policy  
   Filter Profiles  
 Traffic Shaping  
 RADIUS  
**UTM**  
 Firewall  
 IDS  
 VPN  
 Antivirus  
 Mail Filter  
**Infrastructure**  
 DHCP  
 DNS  
 Web Server  
 Certification Authority  
**Office**  
 Users and Groups  
 User Corner  
 File Sharing

**Filter virus**  
 Use antivirus:  Change

**Content filter threshold**  
 Threshold: Disabled ▼  
This specifies how strict the content filter is.  
Change

File extensions filtering
MIME types filtering
Domains filtering

**Configure allowed file extensions**  
[+ Add new](#)

Search

Extension	Allow	Action
ade	<input checked="" type="checkbox"/>	
adp	<input checked="" type="checkbox"/>	
asf	<input checked="" type="checkbox"/>	
asx	<input checked="" type="checkbox"/>	
avi	<input checked="" type="checkbox"/>	
bas	<input checked="" type="checkbox"/>	
bat	<input checked="" type="checkbox"/>	
be	<input checked="" type="checkbox"/>	
bin	<input checked="" type="checkbox"/>	
bz2	<input checked="" type="checkbox"/>	

10 Page 1 of 10

**Set policy for all extensions**  
 Allow all extensions:   
Use this field to change the value of all the above rows at once  
Change

Figure 5.65 – File extension filtering tab of the Default filter profile

Filter Profiles > default (show help)

Filter virus

Use antivirus:  [Change](#)

Content filter threshold

Threshold: Disabled  [Change](#)  
This specifies how strict the content filter is.

File extensions filtering | **MIME types filtering** | Domains filtering

Configure allowed MIME types

[Add new](#)

[Search](#)

MIME Type	Allow	Action
application/compress	<input checked="" type="checkbox"/>	
application/gzip	<input checked="" type="checkbox"/>	
application/java-vm	<input checked="" type="checkbox"/>	
application/x-compress	<input checked="" type="checkbox"/>	
application/x-gzip	<input checked="" type="checkbox"/>	
application/zip	<input checked="" type="checkbox"/>	
audio/mpeg	<input checked="" type="checkbox"/>	
audio/x-mpeg	<input checked="" type="checkbox"/>	
audio/x-mpeg	<input checked="" type="checkbox"/>	
audio/x-pn-realaudio	<input checked="" type="checkbox"/>	
audio/x-wav	<input checked="" type="checkbox"/>	

10 Page 1 of 2

Set policy for all MIME types

Allow all MIME types:  Use this field to change the value of all the above rows at once

[Change](#)

Figure 5.66 – MIME types filtering tab of the Default filter profile

The second tab of the *default filter profile* is the *MIME types filtering*. MIME means “Multipurpose Internet Mail Extensions”. All the MIME’s were allowed.

HTTP advanced proxy configuration also contain the domain filtering and as can be seen in Figure 5.67, a test was done by filtering *www.youtube.com*.

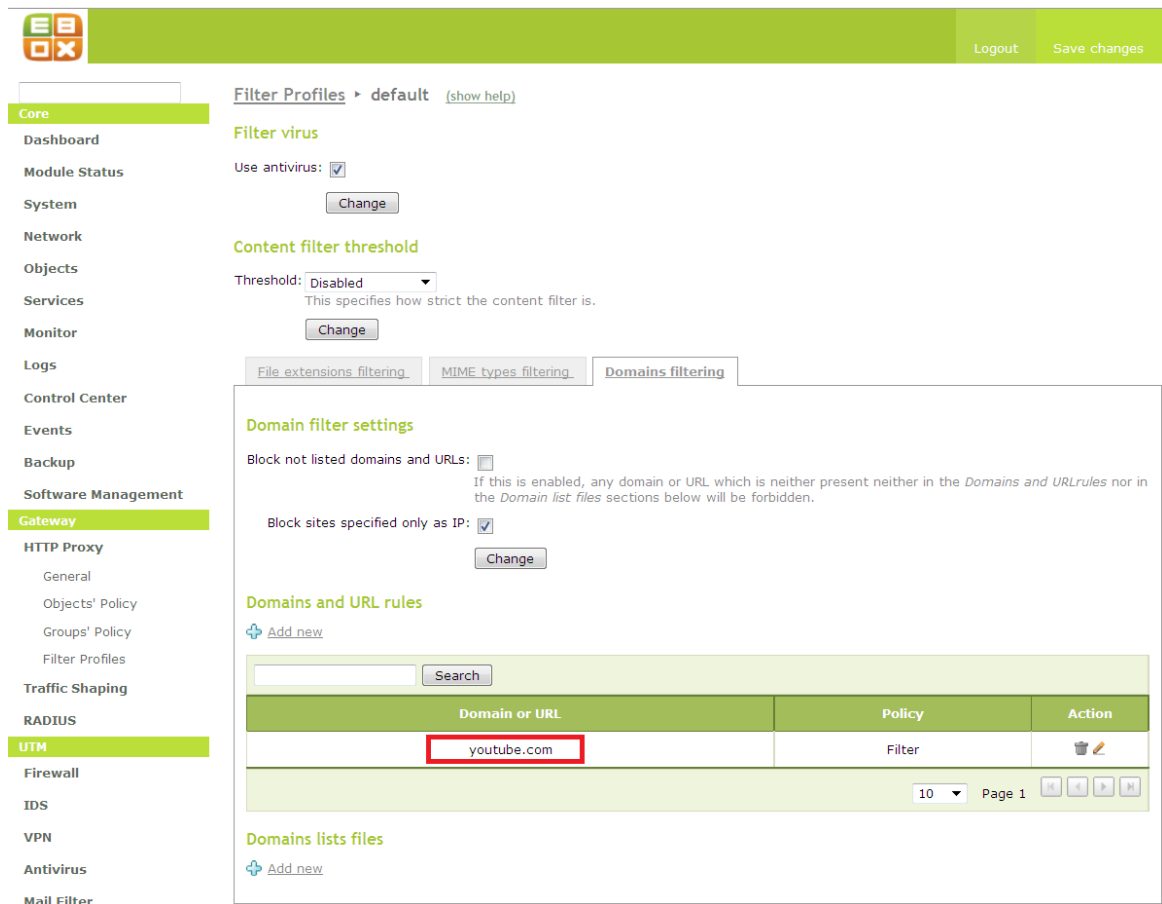


Figure 5.67 – Domain filtering tab of the Default filter profile

As said earlier, four (4) filter profiles were created, each for each network objects created. The configuration of one of the created filter profiles are as shown below. Some part of the created filter profiles can be configured to use the configuration of the *default filtering profile*. Therefore, in this project, the considered *Teachers filter profile* was configured to use the *File extensions filtering* and the *Domain filtering for filter group* of the *default filtering policy*. Figure 5.68, 5.69 and 5.70 shows the full configuration of the *Teachers Filter Profiles*.

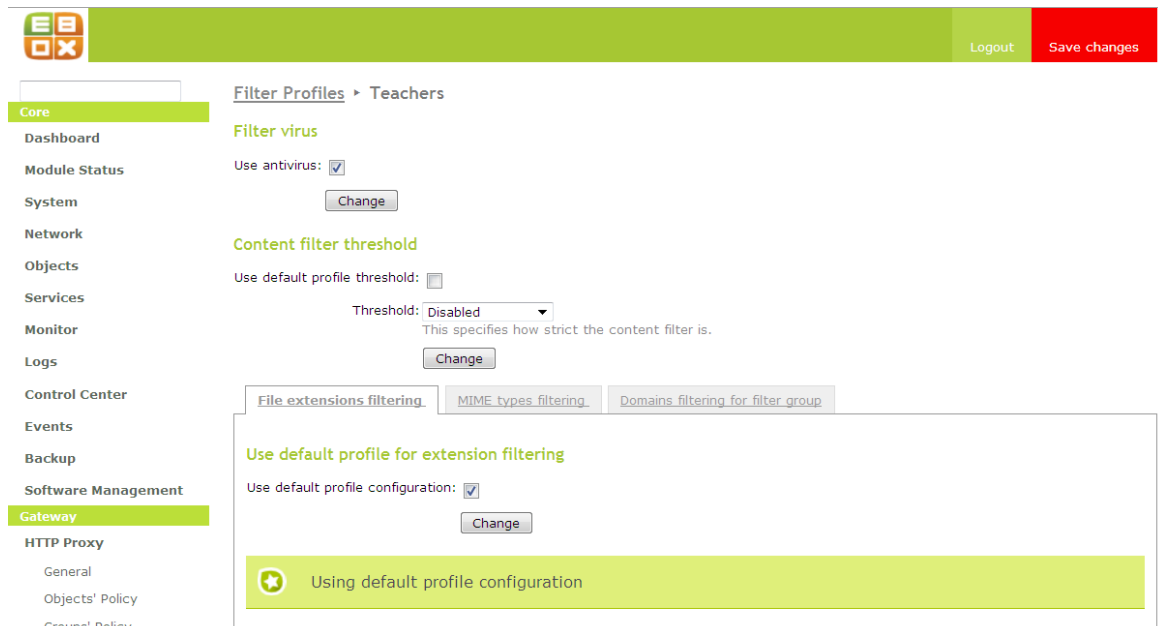


Figure 5.68 – File extension filtering tab of the Teachers filter profile

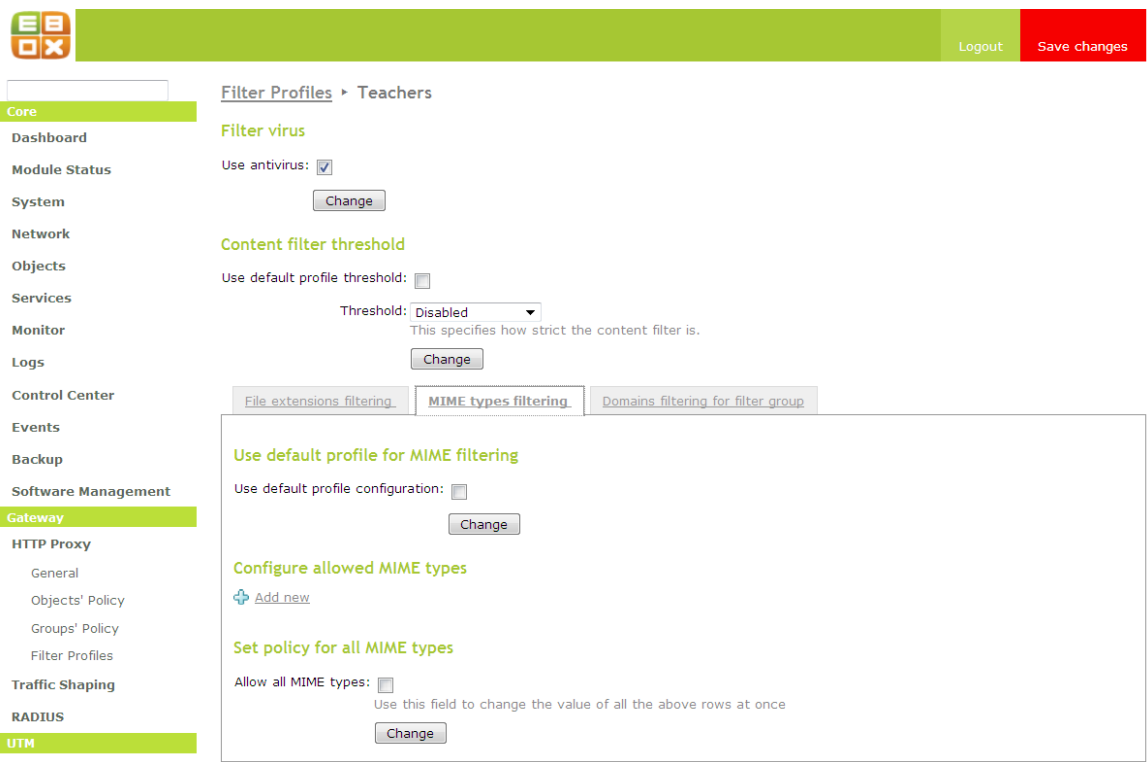


Figure 5.69 – MIME types filtering tab of the Teachers filter profile

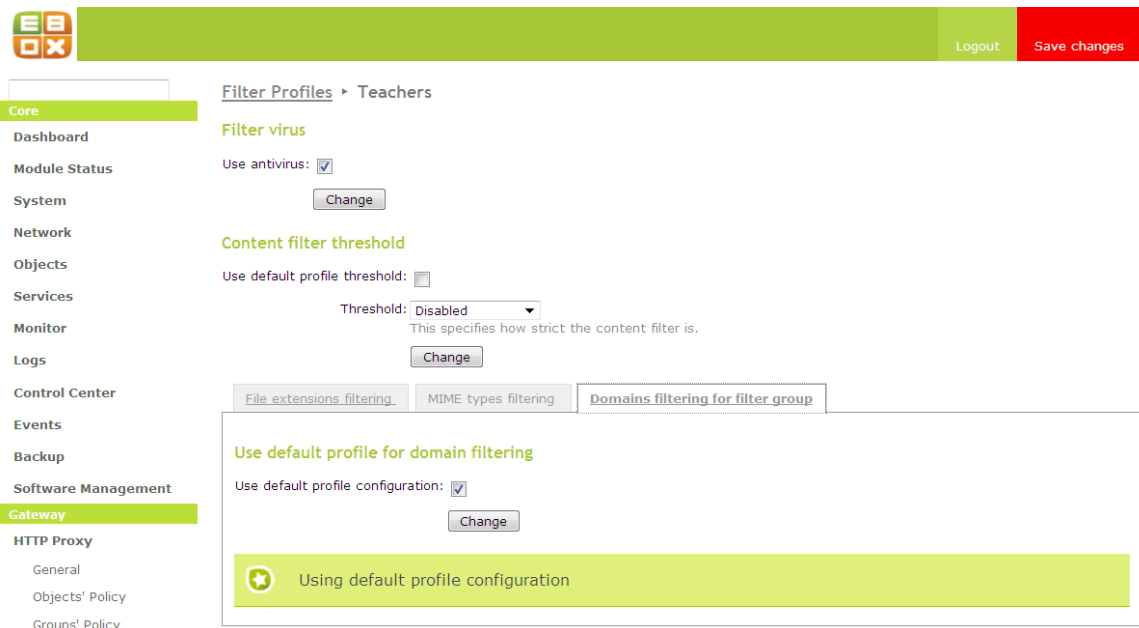


Figure 5.70 – Domain filtering tab of the Teachers filter profile

### 5.6.3 Secure Interconnection between Local Networks

Virtual Private Network (VPN) is a computer network which gives secure connection between Local Area Networks linked together by the internet. VPN allows remote computers to access resources available on a local network and thus act as though they are on this local network.

#### Certificate Authority with eBox Platform

eBox platform has its integrated management Certification Authority using the OpenSSL technology. To use this certificate authority in eBox, one has to issue a CA (Certificate Authority) certificate before clients or user certificate can be issued.

In this project, the CA certificate was issued to the eBox and named *Sulazhy Enterprise*. And certificates to client was issued and signed by *Sulazhy Enterprise*. The certificate issued to the clients by *Sulazhy Enterprise* can be seen in Figure 5.71.

The screenshot shows the eBox web interface. On the left is a navigation menu with categories like Core, Gateway, and UTM. The main content area is titled 'Certification Authority (show help)' and includes a form to 'Issue a New Certificate' with fields for 'Common Name', 'Days to expire', and 'Subject Alternative Names'. Below the form is a table titled 'Current Certificate List' with columns for Name, State, Date, and Actions. The table contains several entries, including a 'Certification Authority Certificate from Sulazhy Enterprise' and several EC5 certificates. A red box highlights the first row of the table.

Name	State	Date	Actions
Certification Authority Certificate from Sulazhy Enterprise	Valid	2011-03-26 12:16:39	✘   ↓   ↻
EC5-P3-1	Valid	2011-03-26 12:16:39	✘   ↓   ↻
EC5-P4-1	Valid	2011-03-26 12:16:39	✘   ↓   ↻
EC5-P5-1	Valid	2011-03-26 12:16:39	✘   ↓   ↻
EC5-P7	Valid	2011-03-26 12:16:39	✘   ↓   ↻
sulazhy-Ubuntu-server	Valid	2011-03-26 12:16:39	✘   ↓   ↻

✘ Revoke   ↓ Download Key(s) and Certificate   ↻ Renew

Figure 5.71 – Certificate Authority certificate and Client certificates

## Configuring a VPN with eBox

eBox uses OpenVPN for its VPN implementation. eBox choose OpenVPN because of the following benefits;

- Based on Secure Socket Layer (SSL) for its encryption.
- Authentication using public key infrastructure.
- Client application for Windows, MacOS and Linux available.
- No need to modify network stack as code runs in user space.
- Network applications can also work transparently. (eBox Technologies SL 2010, 142 – 143)

Configuring the eBox VPN requires that a Certificate Authority be present and issue certificates to all the eBox users to use VPN, all OpenVPN clients and the OpenVPN server. After the issuance of the certificate, the clients and the server can then be created and configured.



In this project, the eBox machine was made the OpenVPN server. The server was named “eBox” and was enabled. The creation and configuration of the server is as shown in Figure 5.72, 5.73 and 5.74.

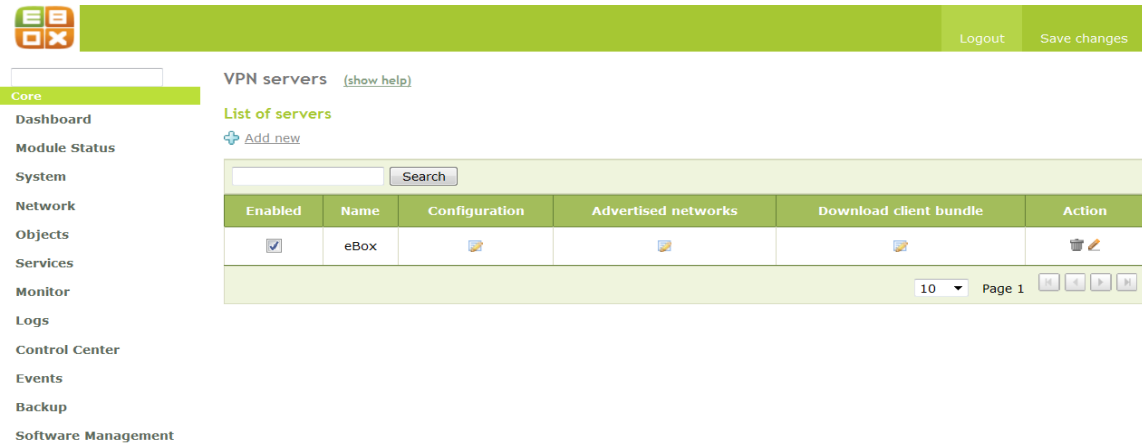


Figure 5.72 – Created and enabled eBox OpenVPN Server

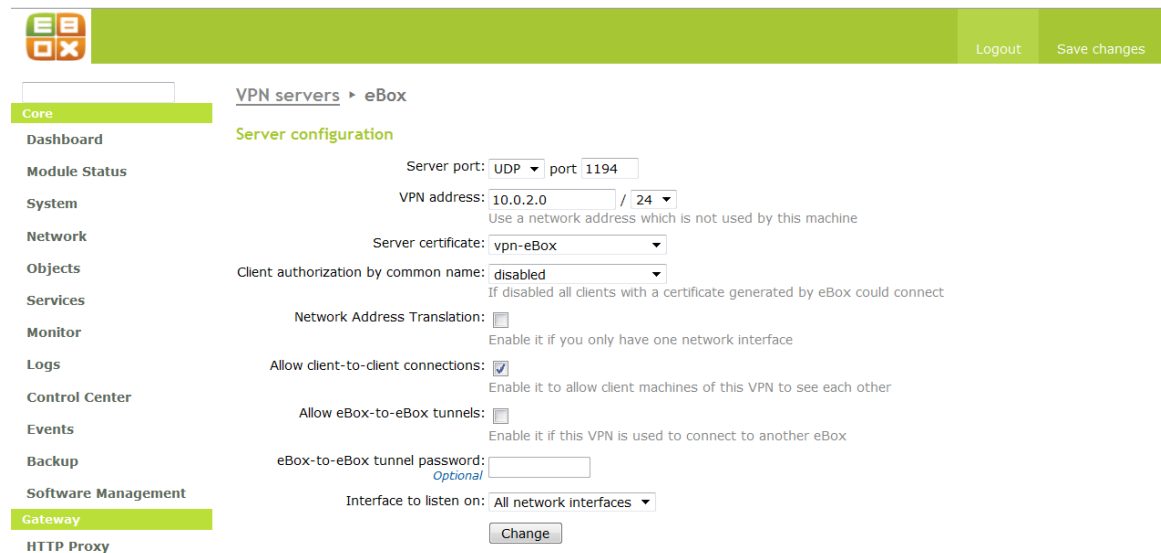


Figure 5.73 – eBox OpenVPN Server Configuration

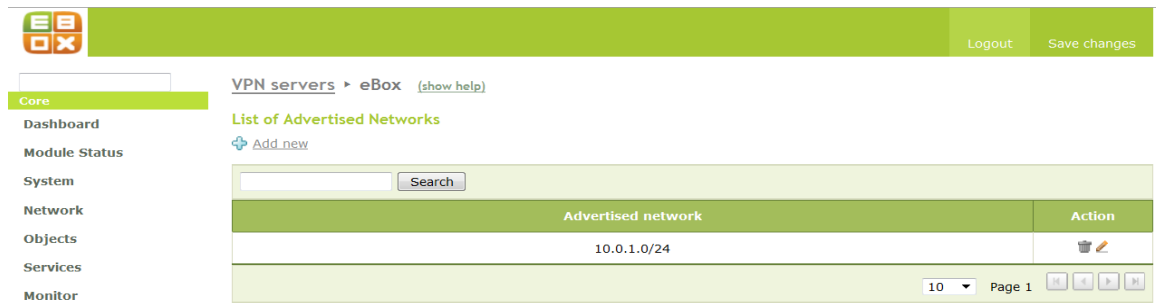


Figure 5.74 – Advertised Network of eBox OpenVPN

The server uses UDP and was configured on port 1194 with an IP address of 10.0.2.0. During the configuration, the server certificate created was chosen for authentication to the server. Also, the client-to-client connection was enabled so that client can connect to one another. The eBox OpenVPN listens on an external port which must be statically configured. Our eBox VPN server listens on the *eth0* (external) interface which was configured statically with the IP address 195.148.173.50. Although, eBox OpenVPN server can be inside the network, but NAT (Network Address Translation) must be done. Also, the server must be configured to listen on all internal interfaces.

After the server configuration, a network advertisement must be done. All local networks that would be accessible by OpenVPN must be advertised. In our implementation, the LAN (10.0.1.0/24) was advertised as shown in Figure 5.74. Therefore, all authorized clients connecting to the OpenVPN server would be able to access all network resources in the 10.0.1.0 LAN.

Configuring eBox OpenVPN client is relatively easy. Installation and configuration of the client involves the download of OpenVPN client installer on [www.openvpn.net](http://www.openvpn.net) and installing it on the client machine. Alternatively, eBox provides OpenVPN installer and can be used instead. To get the installer with the bundle, the “*Add OpenVPN installer to bundle*” button must be clicked (Figure 5.75). After the installation, the client bundle can then be downloaded from the eBox server as shown in Figure 5.75.

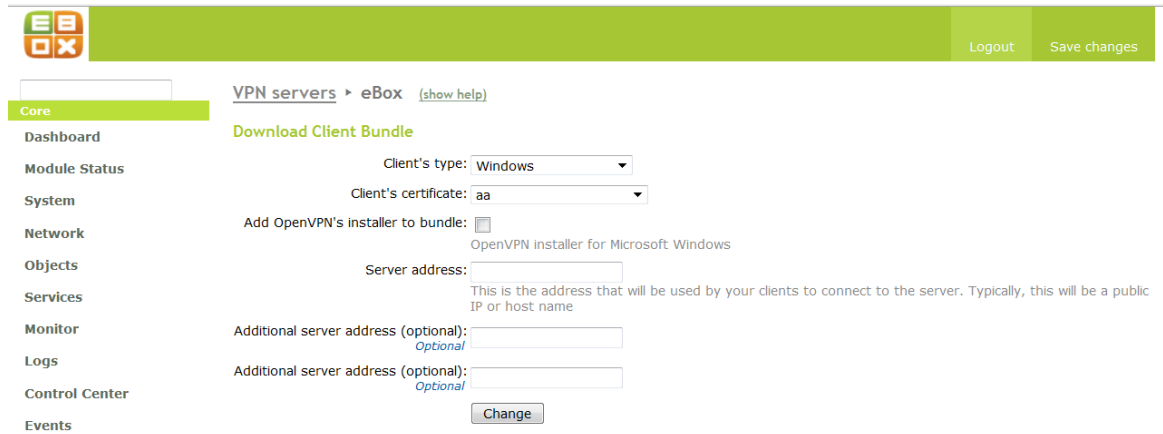


Figure 5.75 – eBox OpenVPN Clientt Bundle Download

To download the client’s bundle, the operating system of the client was chosen and the certificate of eBox username was also chosen. eBox client bundle is available for Windows OS, MacOS and GNU/Linux. The downloaded client bundle was copied to the “*config folder*” of the OpenVPN program. In Figure 5.76, it can be seen that the *OpenVPN daemons* was running in eBox. The configuration was tested and connection result is as shown in Figure 5.77.

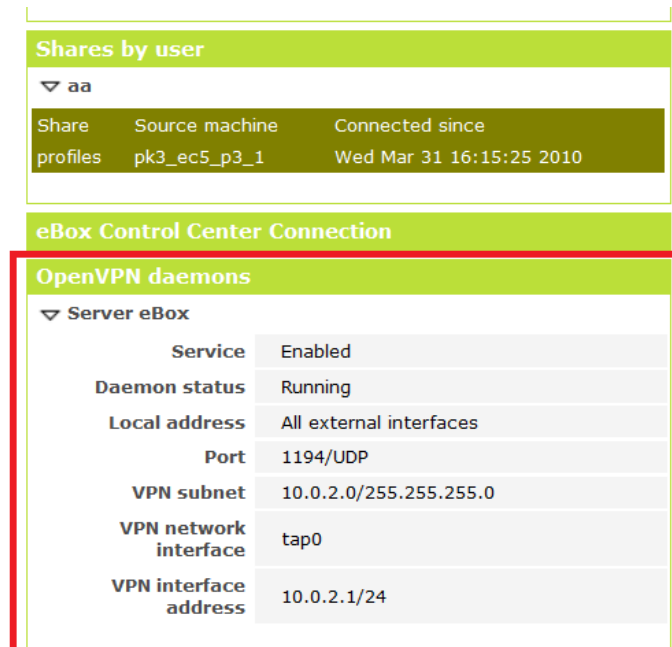


Figure 5.76 – eBox OpenVPN Server Running

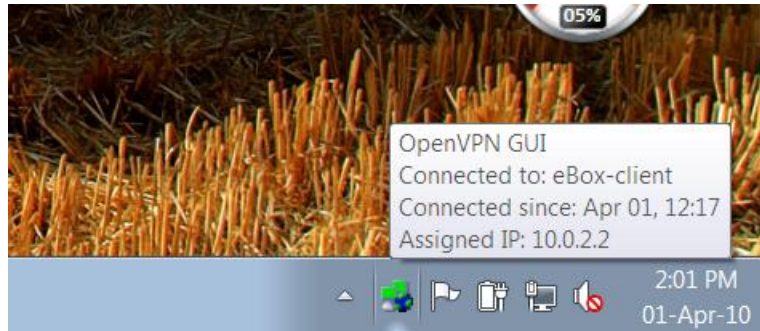


Figure 5.77 – eBox OpenVPN Client Connection

#### 5.6.4 Intrusion Detection System (IDS)

Intrusion Detection System helps prevent unauthorized access to the network and the network devices. This system functions by detecting a potential attack, prevent the attack and record the details of the attack by storing the information in a database. This information contains the IP address of the attacker. eBox uses *Snort* to implement its Intrusion Detection System. Snort is a type of Network Intrusion Detection System (NIDS) which monitors the overall traffic of a local area network.

To configure IDS in eBox, we enabled the *eth0* (external) interface to monitor. After the interface has been enabled, all connections to the enabled rules of the services will be monitored. In eBox, all monitoring/alerts on the IDS enabled interface can be seen using the *eBox logs*.

We tested the configuration by running *nmap* on a Linux client with the IP address of the monitored interface (Figure 5.78). The full report query log of the IDS is as shown in Figure 5.79.

```

sulazhy@sulazhy-Ubuntu-server: ~
File Edit View Terminal Help
sulazhy@sulazhy-Ubuntu-server:~$ nmap 195.148.173.50

Starting Nmap 5.00 ( http://nmap.org ) at 2010-04-26 16:57 EEST
Interesting ports on a18-ope.bet1.puv.fi (195.148.173.50):
Not shown: 983 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    filtered smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
143/tcp   open  imap
389/tcp   open  ldap
443/tcp   open  https
465/tcp   open  smtps
636/tcp   open  ldaps
993/tcp   open  imaps
995/tcp   open  pop3s
3128/tcp  open  squid-http
5222/tcp  open  unknown
5269/tcp  open  unknown
8888/tcp  open  sun-answerbook

Nmap done: 1 IP address (1 host up) scanned in 1.43 seconds
sulazhy@sulazhy-Ubuntu-server:~$

```

Figure 5.78 – nmap to eth0 (external interface)

The screenshot shows a web-based interface for managing an Intrusion Detection System (IDS). The top navigation bar includes 'Logout' and 'Save changes'. The main content area is titled 'Query Logs > Full Reports (show help)'. Under 'Log Domain', there is a dropdown menu for 'Select available full reports:' set to 'IDS' and a 'View' button. The 'Custom query' section includes filters for 'From date:' (25 / April / 2010 - 16 : 59) and 'To date:' (27 / April / 2010 - 16 : 59), along with fields for 'Priority:', 'Description:', 'Source:', and 'Destination:', and an 'Event:' dropdown set to 'Any'. There are 'Search' and 'Save as event' buttons. Below the filters is a table of log entries:

Date	Priority	Description	Source	Destination	Protocol	Event
2010-04-26 16:57:55	3	TCP Portscan	195.148.174.197	195.148.173.50	PROTO:255	Alert
2010-04-26 16:53:49	3	BARE BYTE UNICODE ENCODING	195.148.173.50:1240	193.66.251.210:80	TCP	Alert
2010-04-26 16:43:24	3	BARE BYTE UNICODE ENCODING	195.148.173.50:1236	193.66.251.210:80	TCP	Alert
2010-04-26 16:41:19	3	BARE BYTE UNICODE ENCODING	195.148.173.50:1235	193.66.251.210:80	TCP	Alert
2010-04-26 16:32:59	3	BARE BYTE UNICODE ENCODING	195.148.173.50:1233	193.66.251.210:80	TCP	Alert
2010-04-26 16:22:35	3	BARE BYTE UNICODE ENCODING	195.148.173.50:1229	193.66.251.210:80	TCP	Alert
2010-04-26 16:12:09	3	BARE BYTE UNICODE ENCODING	195.148.173.50:1223	193.66.251.210:80	TCP	Alert
2010-04-26 16:01:44	3	BARE BYTE UNICODE ENCODING	195.148.173.50:1221	193.66.251.210:80	TCP	Alert
2010-04-26 15:52:53	3	BARE BYTE UNICODE ENCODING	195.148.173.50:1195	193.66.251.210:80	TCP	Alert

Figure 5.79 – IDS Query log report of nmap connection

## 6. CONCLUSION, CHALLENGES AND RECOMMENDATION

### 6.1 Conclusion

In this work, the functionality of eBox platform was investigated. It involved the installation of Ubuntu, Linux OS as the base system, and afterwards the installation of the eBox packages according to the network requirement. A small educational institution was modelled and network services was installed and configured according to the requirement of the network. eBox network services were tested and were seen to be magnificent. However, eBox proof to have a promising future when the development gets to an adequate point.

### 6.2 Challenges

eBox covers several aspects of computer networking and it requires a full understanding of telecommunication, networking and Linux OS before it can be handled. We had to revise our knowledge of telecommunication. More also, since eBox is a new technology and the development still continues some of the configuration files contain bugs and thereby prevents some modules from functioning adequately. Also, there was no material addressing several problems administrators' face during the installation and configuration of eBox platform. We joined the eBox user's forum where users share ideas and assist one another to solve problems. On several occasion, we had to add patches to the configuration files to solve some problems we faced. However, part of the problems we were faced with are;

- Users could not access the server using *ssh*.
- Deployment of webpage in the eBox Apache web server.
- Configuring the LAN to access the internet.
- Accessing the eBox web interface when the external network interface was ticked as external.
- Configuring the firewall module.
- OpenVPN connected but could not ping or connect to clients in the LAN.

- Domain and URL filtering not functioning.
- PDC sometimes fails to mount directories.

### **6.3 Recommendations**

eBox technologies appear to be a very efficient solution to network services. It makes installation and configuration of network services very easy for network administrators. Since eBox is an open source server mounted on Linux operating system, it is free to use and can be afforded by all. eBox is still undergoing major development and not very efficient to be used for serious and sensitive organizations. eBox is gradually becoming popularly known and its future is surely promising.

Existing eBox installation should be updated frequently and future installation should be the latest version because several errors and bugs in present version are always addressed in future versions. Also end users often request for additional functionalities which are not present in previous versions.

## REFERENCES

- [1] Rabbit Semiconductors 2006, Dynamic C<sup>®</sup> - An Introduction to TCP/IP, "*For Embedded System Designers*".
- [2] Kirch, O. and Dawson, T. 2000, *Linux Network Administrator's Guide*.
- [3] eBox Technologies SL 2010, *eBox 1.2 for Network Administrators*, Revision 1.2, [www.eboxplatform.com](http://www.eboxplatform.com). Accessed 20th November 2009.
- [4] Forouzan, B. 2007, *Data Communication and Networking*, 4th Edition.
- [5] Anand Software and Training Private Limited 2010, *Network Planning and Design*, <http://networking.anandsoft.com/network-planning-design.html> . Accessed 18th Febraury 2010.