KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY

COLLEGE OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE

AN IMPROVED COMPUTER NETWORK ACCESS CONTROL USING FREE BSD PFSENSE

A CASE STUDY OF UMaT LOCAL AREA NETWORK

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

BY

AKPAH SYLVESTER (BSc. INFORMATION TECHNOLOGY)

AUGUST 2015

TABLE OF CONTENTS PAGE

DECLARATION

I hereby declare that this submission is my own work towards the MSc and that, to the best of my knowledge, it contains no material previously published by another person nor material which has been accepted for the award of any other degree of the University, except where due acknowledgement has been made in the text.

SYLVESTER AKPAH ………..……………… …………………….....

(PG8957913) Signature Date

Certified by:

Dr. Michael Asante ………..……………… …………………….....

(SUPERVISOR) Signature Date

Certified by:

Dr. J. B. Hayfron-Acquah ……....……………… …………………….....

(HEAD OF DEPT.) Signature Date

DEDICATION

I dedicate this thesis to my dear parents, Mr. Philip A. Akpah and Mrs. Ruth Ankudze Akpah who have been the source of inspiration throughout my education. My sister, Mrs. Bridget Hover is highly appreciated for her support.

ACKNOWLEDGEMENTS

My foremost appreciation is to the Almighty God for his undefined grace and strength throughout this project. I salute the immeasurable guidance and contribution of my supervisor, Dr. Michael Asante. It has undeniably been a true privilege to be mentored by him, his indepth knowledge, unfaltering standards of excellence and ingenuity has inspired me throughout my study at the Kwame Nkrumah University of Science and Technology (KNUST).

Further, I express my profound gratitude to Prof. Daniel Mireku-Gyimah (Foundation Vice Chancellor) of UMaT for his strict guidelines, eye for perfection, tutoring and unfailing support in the completion of this thesis.

I am also grateful to Prof. Richard K. Amankwah (Dean, Faculty of Mineral Resources Technology), Dr. Grace Ofori Sarpong (Head, Petroleum Engineering Department), Dr. Ishmael Quaicoe (Lecturer, Safety & Environment Department) and Dr. Mrs. P. B. Mireku-Gyimah for their incessant encouragement, direction and support.

Generous appreciation goes to colleagues at the UMaT Network Operation Centre (NOC), notably Mr. Emmanuel K. Eshun and Felix Larbi Aryeh for their valuable discussions. Not forgetting Emmanuel Ahene, Michael O. Mensah and Jacob Tawiah for their support.

My final and heartfelt appreciation goes to the most special person in my life, Epilogue Annku who aided me in proofreading as well as prayed tirelessly for me throughout my study.

ABSTRACT

The University of Mines and Technology (UMaT) has a Local Area Network (LAN) whose primary purpose was to facilitate research; teaching and learning; and information sharing. Unfortunately, the LAN had some challenges attributable to high demand by over 2500 users on the limited bandwidth of 45 MB, misuse of the bandwidth on low priority bandwidth hungry applications, insecurity from virus attacks, phishing and lack of effective user access control. This thesis sought to study the behaviour patterns of the network users and deploy an enhanced network access control using pfSense open source software as the dedicated perimeter firewall. Prior to the installation of the firewall, a test was conducted using wireshark protocol analyzer to identify completely the vulnerabilities of the LAN and their causes. The results showed that the network was slow due to the limited bandwidth, and phishing out user credentials and other vital information was easy since illegitimate users could gain unauthorised access to the LAN. To resolve this problem, the LAN was upgraded by installing additional software packages which included Squid, squidGuard, Squid Analyses Report Generator (SARG) and setting up of an Active Directory server with user access protocols and policies on the firewall to effectively improve user access control and insulate the LAN from misuse and virus attacks. A test was then conducted using freeBSD pfsense software to assess any improvement in the upgraded LAN. The results showed that in spite of the limited bandwidth, the speed of the upgraded LAN had improved significantly and become more secure. It is recommended that the bandwidth of the LAN at UMaT is increased from 45 MB to at least 80 MB especially as the student enrolment is expected to increase. The installed software packages should also be upgraded periodically.

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

LAN – Local Area Network

NOC – Network Operating Center

SARG – Squid Analysis Report Generator

AD – Active Directory

NAC – Network Access Control

CSMA/CD - Collision Sense Multiple Access/Collision Detection

IEEE - Institute of Electrical and Electronics Engineers

AIEE - American Institute of Electrical Engineers

IRE - Institute of Radio Engineers

WLAN - Wide Local Area Network

UTP - Unshielded Twisted Pair

CAT-3 - Category-3

CAT-5 - Category-5

UMaT – University of Mines & Technology

NIC - Network Interface Card

MAC - Media Access Control

MiTM - Man-in-the-Middle

SSL - Secure Socket Layer

DHCP - Dynamic Host Configuration Protocol

IDS - Intrusion Detection Systems

NAT - Network Address Translators

VPNs - Virtual Private Networks

ACLs - Access Control Lists

AAA - Authentication, Authorization and Accounting

RADIUS - Remote Authentication Dial-In User Service

MAC - Mandatory Access Control

DAC - Discretionary Access Control

RBAC - Role-Based Access Control

EAP - Extended Authentication Protocol

ARP - Address Resolution Protocol

PPP - Point-to-Point protocol (PPP)

TLS/SSL - Transport Layer Security/Secure Socket Layer

HTTPS - Secure HTTP

VLAN – Virtual LAN

AS – Authentication Server

PAE - Port Access Entity

EAP over LAN (Extensible Authentication Protocol over LAN

NAS – Network Access Server

UBas – University Basic School

SPS – School of Postgraduate Studies

CENCES - Center for Communication and Entrepreneurship Skills

FOE – Faculty of Engineering

FMRT – Faculty of Mineral Resource Technology

HTTP - Hypertext Transfer Protocol

CHAPTER ONE

INTRODUCTION

1.0 Statement of the Problem

The University of Mines & Technology (UMaT) is a relatively young university established by Act 2004 (Act 677). The vision of the university is to become a Centre of Excellence in Ghana and Africa for producing world-class professionals in the fields of mining, technology and related disciplines. UMaT's mission is to provide higher education with special reference to mining and related fields, to promote knowledge through active research and to offer professional services to the national and international communities.

In line with one of its major action plans, in its strategic plan, to effectively fulfil its mission, UMaT has put in place a Local Area Network (LAN) infrastructure that interconnects the administration block, the faculties, the library, the halls of residence and the University Basic School with high speed ethernet links operating over a dedicated fiber optic backbone with a download and upload speed of 45 MB connected through a dedicated server located at the Network Operation Centre (NOC).

The primary purpose of the LAN was to facilitate active research; teaching and learning; information sharing; online course registration; examination results checking; staff and student workgroup collaborations; and many others. Unfortunately, while the network was replete with the stated benefits, it had some problems attributable to limited bandwidth and lack of effective user access control.

The problem of limited bandwidth arises because the demand for bandwidth on UMaT campus is on a constant rise. This was attributed to the annual increase in student enrolment, increasing use of electronic devices/gadgets and the shifting patterns of internet access and usage. Thus, the available bandwidth was generally not enough to meet and support the core purpose for which the LAN was put in place. A plausible approach to address the problem of limited bandwidth is to increase the current internet capacity by purchasing additional bandwidth. However, this proved to be very expensive due to the high cost associated with acquiring dedicated bandwidth. Indeed, even if additional bandwidth could be purchased, the problem cannot be solved since the demand for more bandwidth will grow to exceed whatever becomes available.

The problem arising out of limited bandwidth was further exacerbated by the lack of an effective user access control, which enabled the unwarranted use of the LAN by users, especially students, who used the network to access and download bandwidth-hungry applications/software such as peer-to-peer file sharing and media streaming software, pornographic materials, audio and video streaming applications embedded in multimedia websites and other social media platforms. Worst of all, due to the uncontrolled access and unwarranted use of the network, users knowingly or unknowingly introduced viruses, trojans and other malware infections which worsen the efficiency of the LAN, leading to a reduction in speed and sometimes destruction of vital or confidential information thus making the network on UMaT campus very insecure.

Currently, the network administrators control the usage, and manage the security of the LAN with per user authentication to prevent eavesdropping and phishing of confidential information such as departmental repository files, examination records and many others. However, this proved to be ineffective since illegitimate users were able to masquerade as trustworthy users to phish out user credentials of legitimate users which enabled them to gain unauthorized access to the LAN.

A logical way to control the use of the LAN is by limiting user access to the available bandwidth and preventing authorized users from accessing unwarranted websites. It is only when the use of the LAN is effectively controlled that it will become secure. This thesis therefore aims at designing an effective network access control system to assist the network administrators to efficiently control access and manage the security of the LAN.

1.1 Objectives of the Thesis

The objectives of the thesis are to:

1. Study the existing LAN infrastructure;
2. Setup a comprehensive user access group policy using Active Directory; and
3. Design an effective computer network access control system using freeBSD pfsense as the dedicated perimeter firewall with the introduction of squid, squidGuard and Squid Analysis Report Generator (SARG).

1.2 Research Questions

1. What are the various types of network software firewalls available, and how will the identified firewall software enhance network security?
2. How can the identified network firewall software be effectively integrated into the existing network infrastructure?

3. How effective is an open source network software firewall as compared to a proprietary network software firewall in improving network security?

1.3 Importance of study

1. The research brings to light the efficient usefulness of freeBSD pfSense open source network software firewall in network security management.
2. The research opens opportunities for more research to be done in the area of open source network software firewalls.
3. The findings will also serve as a reference material for interested individuals who want to acquire knowledge in open source network software firewalls.

1.4 Scope of the Thesis

The thesis is focused on the LAN of UMaT and is concerned with the deployment of a secured network access control architecture, using FreeBSD pfSense tools only.

1.5 Thesis Organization

The thesis is structured into five (5) main chapters. Chapter 1 gives details of the problem statement, objectives of the thesis, research methodology and scope of the research work. The chapter ends with the organization of the thesis. Chapter 2 gives a detailed overview of related works in the research area. Chapter 3 gives details of the research methodology. It explains fully the various methods employed to carry out the research work. Chapter 4 presents the analysis and discussion of results. Chapter 5 presents the conclusions of the study and provides recommendations.

CHAPTER TWO

REVIEW OF RELATED LITERATURE

This chapter reviews the current literature on the relevant areas of this research. The areas reviewed include Local Area Network (LAN), LAN standards, LAN security, Network Access Control (NAC), access control models, policy based management strategies and previous related works.

2.1 Local Area Network (LAN)

According to Abhimanyu (2012), a Local Area Network (LAN) is a high-speed data network that covers a relatively small geographic area and interconnects workstations, personal computers, printers, servers, and other devices. A LAN offers users many benefits, including shared access to devices and applications, file exchange between connected users, and communication between users via electronic mail and other applications. It typically relies on traditional wired structures as its main transmission medium.

The range of transmission for a LAN is within a specified geographic area, such as an office, a building, or a university campus. The most widespread of LAN technology is the ethernet, which enables the transmission of data frames across baseband cables using Collision Sense Multiple Access/Collision Detection via the network interface card of a computer workstation.

LAN technologies have become more popular in organizations and personal life than it were in the past. This popularity can be attributed with the ease of setup, central management, possibility to upgrade or expand with little difficulty, improved security, better performance and many others. The LAN has indeed eliminated a lot of paperwork and speeded the flow of information. Most LANs are based on the Institute of Electrical and Electronics Engineers (IEEE) 802 standards.

In spite of its lasting existence, security issues such as porous network perimeters, failure to properly configure firewalls, failure to authenticate network users and unauditable networks proves to be major drawbacks to LAN technologies. These exposes the network environment to eavesdropping and jamming. As a result, strategies need to be developed to mitigate these security risks in any computing environment.

2.2 Overview of Firewalls

Firewalls are usually the first component of network security. They separate networks in different security levels, by utilizing network access control policies. The major function of the firewall is to protect the private network from non-legitimate traffic.

Firewalls are primarily located between the Internet and private network. They monitor all traffic leaving or coming into a network; also they can prevent the harmful traffic and attacks from Internet. If a computer from the local network is attacked by an intruder and generates non-legitimate traffic, the firewall can prevent and detect that computer. Firewall can detect such succeeded attack, so it can be recovered.

According to Chapman and Zwicky (1995), a firewall is the most effective way to connect a network to the Internet and still protect that network Firewalls create a separation between public networks (Internet) and private networks by examining the traffic according to the predefined policy, and allowing only legitimate traffic to pass between the public and private network. They help implementing a larger security policy that defines the services and access to be permitted. It is an implementation of that policy in terms of a network configuration, one or more host systems and routers, and other security measures such as advanced authentication in place of static passwords.

A firewall system can be a router, a personal computer, a host, or a collection of hosts and/or routers, set up specifically to shield a site or subnet from protocols and services that can be abused from hosts outside the subnet (Wack and Carnahan 1995). Firewalls must be installed at the choke points to control network traffic and implement network security policy of the organization. Firewalls achieve this by examining the all incoming and outgoing network traffic according to the predefined firewall policy. All network traffic must pass through the firewall, which ensures that only permitted traffic are allowed through.

2.3 Types of Network Firewalls

2.3.1 Wireshark

Wireshark also known as Ethereal is a network protocol analyzer which captures network packets in real time and display them in human-readable format. Wireshark includes filters, color-coding and other features that let you dig deep into network traffic and inspect individual packets. It can be used to inspect suspicious program’s network traffic, analyze traffic flows on your network and/or troubleshoot network problems. It runs on most computing platforms including Windows, OS X, Linux, and UNIX. Network professionals, security experts, developers, and educators around the world use it regularly. It is freely available as open source, and is released under the GNU General Public License version 2. It has a rich and powerful feature set and is the world's most popular tool of its kind.

Wireshark has a rich feature set which includes the following:

- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis
- Standard three-pane packet browser
- Multi-platform: Runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many others
- Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
- The most powerful display filters in the industry
- Rich VoIP analysis
- Capture files compressed with gzip can be decompressed on the fly
- Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)

2.3.2 IPFire

IPFire is an open source network linux distribution software which acts as a router and/or a firewall. It can be maintained via the Graphical User Interface (GUI). The distribution furthermore offers selected server daemons and can easily be expanded to a SOHO server. IPFire is based on linux from scratch and is, like the Endian Firewall, originally a fork from IPCop. Since version 2, only IPCop's GUI is used.

IPFire caters to users not overly familiar with networking and server services. IPFire ships with an extensive package management utility (Pakfire) which allows the base system to be extended by various addons. The package manager also enables updates to address security issues.

The base system provides the following features:

- Proxy server with content filter and caching functionality for updates (i.e. Microsoft Windows updates and anti-virus)
- Intrusion detection system (Snort) with intrusion prevention guardian
- VPN via IPsec and OpenVPN
- Wake-on-LAN (WOL)
- Dynamic DNS
- Quality of Service
- Outgoing firewall
- System monitoring and log analysis

2.3.3 Smoothwall

According to Manning and Morrell (2000), smoothwall is an open source Linux distribution firewall software used for web content filtering. Created using Red Hat Linux, Smoothwall GPL originally had two simple functions: control the modem to dial and hang up, and to route TCP/IP packets from the LAN to the Internet connection, and back again. The Smoothwall Open Source Project was set up in 2000 to develop and maintain Smoothwall Express - a Free firewall that includes its own security-hardened GNU/Linux operating system and an easy-to-use web interface.

Released in September 2001, this version incorporated a web-based multi-language GUI so the firewall could be used and administered by non-Linux people. It also included the Snort Intrusion Detection System (IDS) and support for ADSL modems and PPPoE connections. December 2003 saw the release of Smoothwall Express 2.0 and an array of comprehensive written documentation. By June 2004, Express 2.0 had seen over 200,000 installations. The alpha version of Express 3 (code-named Koala) was released in September 2005. Based on the Linux 2.6 kernel, this test version featured new open architecture, designed to make it easy for developers to produce their own security components. With the benefit of software contributions from around the world, a Beta version followed in 2007. This version was code named “Degu”, in remembrance of one of our team’s pets, who sadly died during development. A current, final and stable version of Express 3.0 (code-named Sammy) is currently available on the download page.

2.3.4 Comparing Open Source and Proprietary Software Firewall

Open Source Software - This is a computer software program with its source code made available with a license in which the copyright holder provides the right to study, change and distribute the software to anyone and for any purpose. It's source code is the part of the software that most computer users don't ever see. It's that part that computer programmers can manipulate to change how a piece of software should work. It may be developed in a collaborative public manner. The open source model or collaborative competition development form multiple independent sources that generates an increasingly more diverse scope of design perspective than any one company is capable of developing and sustaining in a long term.

Proprietary Software - This is a computer software that is designed and owned by an individual or a company. It comes with major restrictions on its use and its source code is almost always kept secret. Although definitions vary in scope, any software which places restrictions on its use, analysis, modifications or distribution can be termed proprietary.

Firewall	License	Cost/Usage Limits	Operating Systems
Comodo Internet Security	Proprietary	Free	Windows 7/8, Vista, XP SP2
FirewallD	GPL	Free	Fedora, RedHat Enterprise Linux, CentOS
GlassWire	Proprietary	Free	Windows 7/8/10, Mac OS
IPFilter	GPLv2	Free	Package for multiple Unix-like OS
pfSense	BSD	Free	BSD Package
Kaspersky Internet Security	Proprietary	$59.95/yr	Windows
Norton 360	Proprietary	$59.99/yr	Windows

Table 2.1 Comparing Open Source and Proprietary Software's

2.3.4. 1 How the Ethernet Works

The ethernet architecture makes use of the Carrier Sense Multiple Access/Collision Detection (CSMA/CD) standard. This standard simply means that all workstations stations have equal access to the same transmission medium, and can either send or receive data whenever the network becomes idle. Prior to this, the station wishing to transmit listens to the network to be sure if it’s not already in use. According to Pidgeon (2001a), the primary advantage of the ethernet is its ability to sense collisions on the network. A collision occurs when two or more stations send data packets at the same time.

A station on an ethernet network wishing to transmit data frames to another station first listens to the network to be sure it is idle. If the station senses that the network is free, it will begin to send its data frames. These data frames will be transmitted to all nodes on the network. However, only the node for which the data frame is intended for will be able to view the contents (Pidgeon, 2001b). This is made possible through a sender and destination addressing which is only known to the sender and receiving workstations.

However, if more workstations become active on the network, the probability of multiple stations trying to send information at the same time increases and in so doing the tendency for collisions to occur also increases. However, according to Spurgeon (1995a), immediately a collision occurs, the sending station sends out a jam sequence alerting all other nodes that there has been a collision and that any data received should be discarded. The station then waits a period of time for the network to become idle and retransmits again.

The CSMA/CD standard can be broken down into individual parts and applied to the description above. The Carrier Sensing (CS) is the ability of the computers to listen to the network and determine if there is activity. Multiple Access (MA) refers to the fact that all nodes on the network have equal access to the transmission medium at all times, and finally, the Collision Detection (CD) process was explained above (Pidgeon, 2001c).

2.3.5 IEEE 802.3 Standard Relationship to the OSI Model

The IEEE 802.3 ethernet standards fall within the first two layers of the Open Systems Interconnection (OSI) Model. The first layer, the Physical Layer, outlines all physical and electrical specifications for devices used to interface the network, including the shape and layout of pins in connectors, voltages, cable specifications, broadcast frequencies and also handles the actual transport of the bits from the source to destination. It is solely responsible for transporting the electrical impulses across the physical medium (Kaplan and Noseworthy, 2000).

The Data Link layer which is the second layer in the OSI model is responsible for encoding bits into packets prior to transmission from the source and then decoding the packets back into bits at the destination. It provides the procedural means of data transfer from one workstation to another. It is also responsible for logical link control, media access control, hardware addressing, handling and defining physical layer standards. In addition, bits are grouped into frames and certain maintenance and timing issues are addressed (Fairhurst, 2001a; Slone, 1998). The relationship between 1EEE 802 and the OSI Model is illustrated in Figure 2.1.

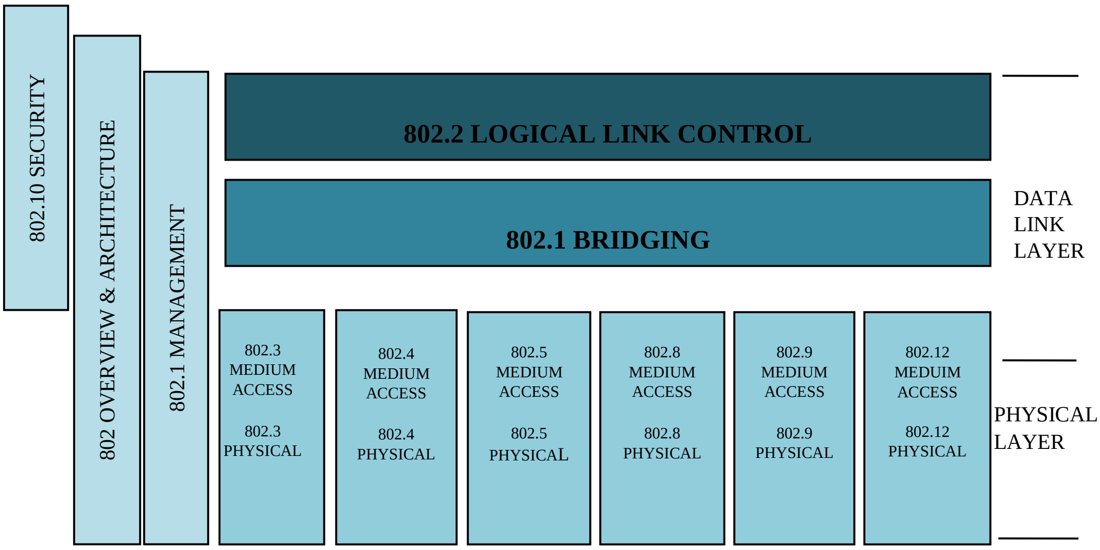


Figure 2.1 Relationship between IEEE 802 and the OSI Model.

2.3.6 IEEE 802.3 Physical Media of Ethernet Network

Anon. (1999d) describes the physical components of an ethernet network that is made up of the network cables and network interface cards which are the essential parts of the transmission medium that actually enables the encoded bit stream of data packets to flow from one client workstation to the other on the network. There exist four main types of cabling schemes used on the ethernet networks and these include thin coaxial, thick coaxial, Category 5 Unshielded Twisted Pair (UTP) and fiber optics cable. A summary of the specifications for each type of transmission medium is illustrated in Table 2.1.

IEEE 802.3 Values						
Characteristics	**Ethernet Value**	**10Base5**	**10Base2**	**10BaseT**	**10BAEFL**	**100BaseT**
Data Rate (Mbps)	10	10	10	10	10	100
Signaling Method	Baseband	Baseband	Baseband	Baseband	Baseband	Baseband
Maximum Segment Length	500	500	185	100	2,000	100
Media	50-ohm coax (thick)	50-ohm coax (thick)	50-ohm coax (thin)	Unshielded twisted-pair cable	Fiber-optic	Unshielded twisted-pair cable
Topology	Bus	Bus	Bus	Star	Point-to-point	Bus

Table 2.2 IEEE 802.3 Transmission Medium Specifications

It can be deduced from the above illustration that each transmission medium has a maximum length for a given segment. In addition, the physical layout of the network depends heavily on the type of the transport medium used (Anon., 1999e). The most common and widely used transmission medium for ethernet is 10BaseT. It uses a standard 4-pair UTP cable which carries eight wires mostly in a twisted form.

This twisting reduces the cross-talk that normally will occur within the cable and cuts down on data collisions that would be detected due to wire cross-talk (Spurgeon, 1995b). The standard IEEE 802.3 signal uses two pairs of wires, one for data transmission and one for receiving. For a client workstation to be able to communicate on a network, a network interface card (NIC) is needed. This is simply an expansion card that plugs into the motherboard of the computer. Each network card comes with a unique Media Access Control (MAC) address that distinguishes itself from every other workstation on the network.

The NIC acts as the interface between a client workstation and the transmission medium. It usually contains an internal transceiver that “listens” to the network to detect collisions. It also contains an ethernet controller protocol that enables it to support the MAC protocol used by the IEEE 802.3 standard (Fairhurst, 2001b). Additionally, an ethernet network is made up of many other hardware equipment’s namely routers, switches, bridges and hubs. Even though these topics go beyond the focus of this thesis, it’s important to recognize their involvement in ethernet networking.

2.3.7 Data Transmission

On an ethernet network domain, data packets transmitted from one workstation is sent to all workstations on the network, whether it is intended for that particular workstation or not. A workstation accepts only the data frame addressed to it (Fairhurst, 2001c). Outlined below is the series of steps followed by a workstation when it is ready to transmit data packets on an ethernet network.

i. The workstation first listens to the network to see whether any other workstation is transmitting. The workstation listens by sensing the carrier signals present on the transmission channel. When the workstation realises there is activity, it continues to wait.

ii. When the workstation does not detect any signal on the transmission channel, it starts to transmit the message frames.

iii. In the process of transmitting, the workstation continues to listen to the network. It then compares the received message with what was actually transmitted. If it realizes they are the same, the workstation continues the transmission.

iv. If the message sent was not what was actually received, the sending workstation assumes it was a collision and thus stops transmitting.

v. The sending workstation then transmits a Jam sequence which tells other workstations on the network on the occurrence of a collision.

vi. The sending workstation then waits a random amount of time and then begins again.

This is the basic process of data packet transmission from one workstation to the other. Figure 2.2 gives a detailed illustration of the transmission process. The process looks very simple, but the truth is, a lot goes on behind the scenes that enable the steps to take place. The workstation “listens” to the transmission channel by way of a transceiver. The transceiver monitors the current flow along the cable. When the transceiver picks up current flow that translates to a bit flow, it responds by saying the cable is busy and does not transmit any data (Fairhurst, 2001d). When the transceiver senses that there is no activity on the transmission channel, it then begins data transmission.

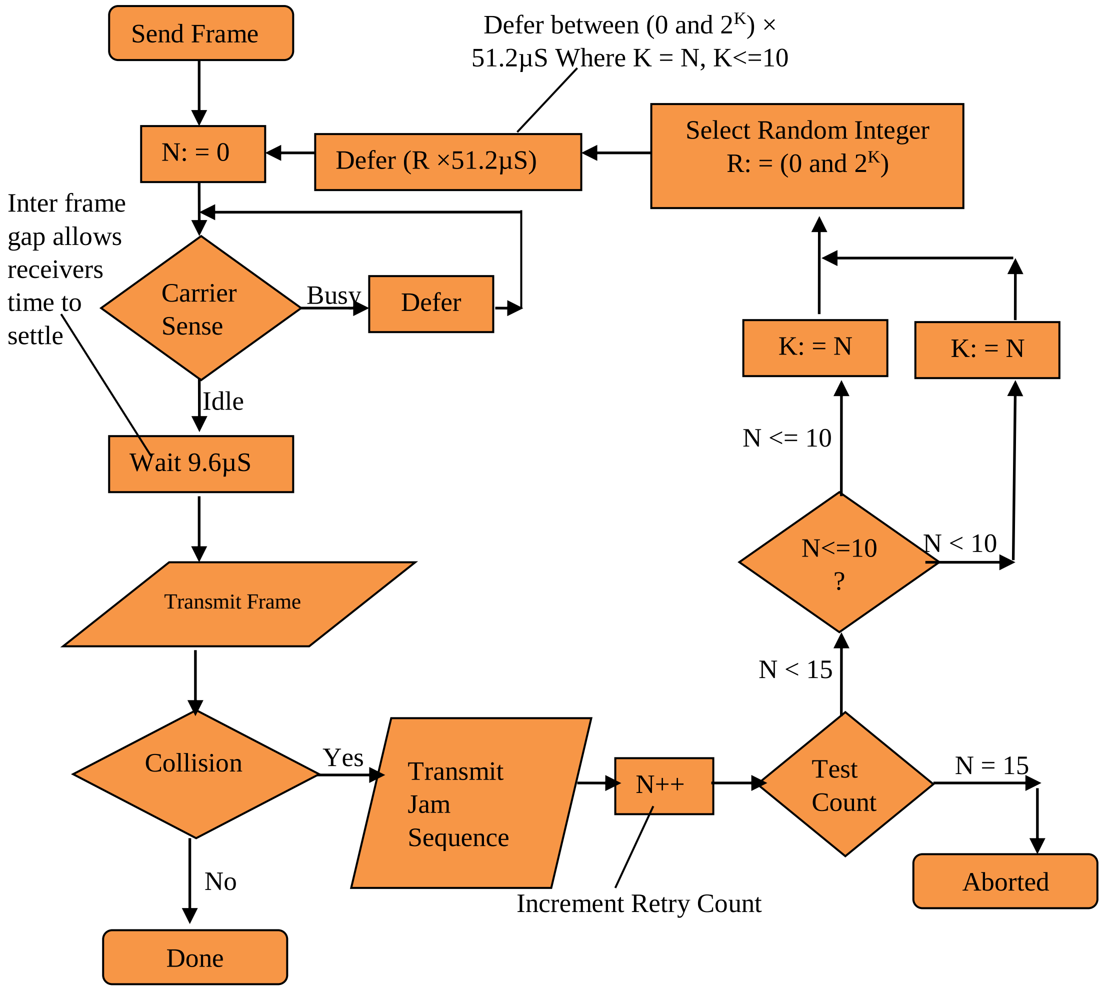


Figure 2.2 IEEE 802.3 Data Transmission Algorithm

2.3.8 Advantages and Disadvantages of the IEEE 802.3 Standard

The IEEE 802.3 ethernet standard is the most widely used networking standard in most Local Area Networks (LANs) because of its flexibility, ease of use and vendor-neutrality which is built into the ethernet system. Most computers developed today are equipped with ethernet cards that enable direct connectivity to either 10 Mb/s, 100 Mb/s or 1Gb/s networks. This makes it very easy to connect new nodes and upgrade existing ethernet networks.

The cost of a standard Category 5 (CAT5) ethernet cable as compared to that of either coaxial cabling or fiber optic cable is very cheap and this sets apart this cabling scheme from the others. An ethernet network can be easily setup by simply connecting two or more machines with CAT5 cabling terminated with Registered Jack-45 (RJ-45) connectors connecting to a and a simple hub/switch through respective wall jacks. This allows for easy expansion of the network as the organization grows. A scenario in which user A moves and plugs his/her workstation into a different wall jack; the network will still recognize the Media Access Control (MAC) address of the Network Interface Card (NIC) and automatically assigns the workstation an IP address.

However, with all of the stated benefits of the ethernet, there exist some limitations. A major drawback is the limit to the length of a particular ethernet cable segment. The maximum length of any standard 10BaseT cabling is 100m. Even though this may seem like a lot of length, it indeed becomes insufficient if a particular segment is to span several floors of an office building.

Another drawback is the number of workstations that can be connected to any single ethernet segment at a particular point in time. The maximum number of workstations that can be connected to an ethernet segment or domain is 1024 but simply put, the more workstations on a particular segment, the slower the network will become.

This drawback has however been overcome by the use of switched ethernet, which basically segments the workstations. Each segment is thus attached to a switch which actually does the routing of traffic, so the entire ethernet medium is no longer shared by all connecting workstations. The issue of Collision Detection is no longer a problem because there is no shared medium (Pidgeon, 2001c).

2.3.9 Attacks on LANs

This section focuses on the security issues encountered during the transmission of data between users on a LAN. This is mainly attributed to porous network perimeter walls and lack of effective user access control strategies. Some of the attacks are passive, meaning information on the network is monitored; others are active, meaning the information is actually altered with the intent to corrupt or destroy valuable information or the network itself.

2.3.10 Types of Attacks on LANs

According to Memon et al. (2010), attacks are always associated with systems, software and sensitive flow of data within a network. The primary goal of the hacker is to look out for loopholes in a network thus to interrupt or decrease the performance of the network in order to gain access to sensitive data. Below are lists of attacks suffered on LANs.

A. **IP Address Spoofing:** IP address spoofing is one of the most frequently used spoofing attack methods. With this attack, an attacker transmits IP packets from a "spoofed" source address in order to disguise itself that the packets are coming from a legitimate IP address source. There exists two (2) techniques of IP spoofing attacks used to overwhelm the target workstations with traffic. The first technique is to simply flood the target workstation with data packets from multiple spoofed IP addresses. This method works by directly sending the target workstation with more data packets than it can actually handle. The second technique is to spoof a target's IP address and send data packets from that address to many other workstations on the network. Since the spoofed packets appear to be sent from the target's IP address, all responses to the spoofed packets will be sent to the target's IP address. IP spoofing attacks can also be used to bypass IP address-based authentication. This enables malicious parties to use spoofing attacks to impersonate machines with access permissions and bypass trust-based network security measures.

B. **Man-in-the-Middle (MiTM) Attack:** As the name specifies, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. This form of attack is used to gain unauthorized access to sensitive information or data packets in transit. It can be classified as another form of eavesdropping in which the attacker establishes connections with many other users. The main aim of the attacker is to gain unauthorized access, read and modify data at his/her discretion during a communication session without the knowledge of the legitimate user. There are several drawbacks created by this type of attack. This includes:

i. Gaining unauthorized access to the network;

ii. Capturing sensitive information;

iii. Flooding network sessions with data packets; and

iv. Interfering and corrupting of the transmitted data.

According to Cao and Malik (2005), the use of cryptographic encryption and authentication known as secure socket layer (SSL) can be used to mitigate this type of attack.

C. **Dynamic Host Configuration Protocol Attack:** This attack occurs when an attacker deliberately sends many requests to the DHCP server. This forces the server to respond to the requests of the client (attacker) by issuing IP addresses against each request. The main goal of this type of attack is to spoof DHCP replies from the server. After receiving the IP addresses from the server, the intruder then gains control to attack the DHCP server which at this point is not able to respond to other user requests. To avoid this type of attack, it is advisable to use the static IP addressing scheme in the network (Patrick and Vargas, 2006).

D. **Spam Attack:** Spam refers to the electronic equivalent of junk, unsolicited, bulk or unwanted email. Spam attacks create a lot of problems in a network by consuming bandwidth and causing increased delays for user authentication and data transmission. The main purpose of a spam attack is to overwhelm the entire network with messages like traditional emails. The recommended solution to eliminate spam messages is to use anti-spam software (Patrick and Vargas, 2006).

E. **Conversation Sniffing Attack:** This type of attack is the process of intercepting and understanding network information that is in transition in the network medium. In a networked environment all information passes through the Network Interface Cards (NICs) across the transmission channel to all client workstations. Whenever an attacker wants to carry out this type of attack, the attacker simply configures the NIC in a promiscuous mode that is the same mode from which the centralized device transmits data packets in the network. Often, attackers can make use of conversation sniffing to steal secret/confidential information or to eavesdrop on the network medium to phish out user login credentials, **IP** address of client workstations, MAC addresses of the NICs, emails and any other information in transit (Anh and Shorey, 2005). Confidentiality is an important factor in the transmission of data and voice. However, traffic on the LAN can be sniffed if communication media traffics are not properly safeguarded. Confidentiality and integrity are two key points in LANs. Confidentiality in LAN, means to ensure the privacy of information exchange among users. Whereas integrity means ensuring that the information being exchanged is not interfered with during transmission. Internet Protocol Security (IPSec) can be used in either transport or tunnel mode to guarantee the integrity and confidentiality of information and also perform authentication operations on a LAN (Cao and Malik, 2005).

2.4 Network Security

According to Simmonds; Sandilands and Van Ekert (2004), network security is primarily focused on the provision of policies adopted by network administrators to prevent and monitor unauthorized access, misuse, modification, or denial of service to computer and network-accessible resources. Network security can be said to be the authorization to access network resources, which are controlled by the network administrator. Users are normally assigned a user ID and password which grants them access privileges to information and programs within their authority.

Several security strategies are adopted to prevent unauthorized access by intruders. Firewalls are the primary defensive strategy adopted - they serve as perimeter wall enforcement points where incoming and outgoing traffic are analyzed based on clearly defined policies. There are other technologies that take up more active roles in detecting and identifying attacks. This includes Intrusion Detection Systems (IDSs), Network Address Translators (NATs) and Virtual Private Networks (VPNs), just to mention a few but for the purposes of this thesis the focus will be on Network Access Control (NAC).

2.4.1 Network Access Control (NAC)

According to Cheswick (2003), Network Access Control is concerned with regulating access to the protected resources in a network environment that complies with pre-defined security procedures. Generally, NAC deals with two levels of protection:

i. Host-Based security protects the safety of a single client workstation that is connected to a network. Unfortunately, most commercial workstations are not bug-free, and some have serious security holes that can be exploited by an attacker. In addition, client workstations within the same administrative segment tend to trust each other such that one weak link can compromise the whole cluster of systems and the network as a whole.

ii. Perimeter-Based security protects a cluster of client workstations making up a network using two primary modules: a layer of defense built up around the cluster, called the perimeter wall, and the door that allows legitimate traffic to pass through while blocking malicious ones. This approach often assumes every host behind the wall is trusted.

Generally speaking, a NAC solution unifies a number of mechanisms which is not limited to the following techniques:

i. Endpoint security techniques whereby antivirus software prevent, detect and remove malware such as computer viruses, worms, Trojan horses, etc from client workstations. Host-based intrusion detection and prevention systems also monitor user and system activities to report malicious behavior and policy violation.

ii. User or system authentication methods such as username and password schemes (something you know), secure devices (something you own), and biometric (something you have).

iii. Network security enforcement such as firewalls to protect Local Area Networks (LANs) from network-based threat through traffic filtering to provide end-to-end or end-to-gateway encryption and authentication.

Network Access Control (NAC) allows network administrators to automate policy enforcement rather than requesting users to ensure that their devices conform to anti-malware policies. It enables network administrators to define and implement comprehensive security policies on a centralized server which then allows the network automatically enforce the policies on all network users.

NAC goes beyond just user authentication. The most practical place for a NAC to be is at the edge of the network, defusing security threats at the first point before they gain any form of access as depicted in Figure 2.3. With this network illustration, all data frames from client workstations within the network domain are required to go through the firewall before getting access to the internet. Workstations that do not meet pre-defined security policies are thus quarantined to remediation servers where they have access to certain resources such as system patch updates/antivirus update signatures. The workstations are then allowed to re-connect back to the network.

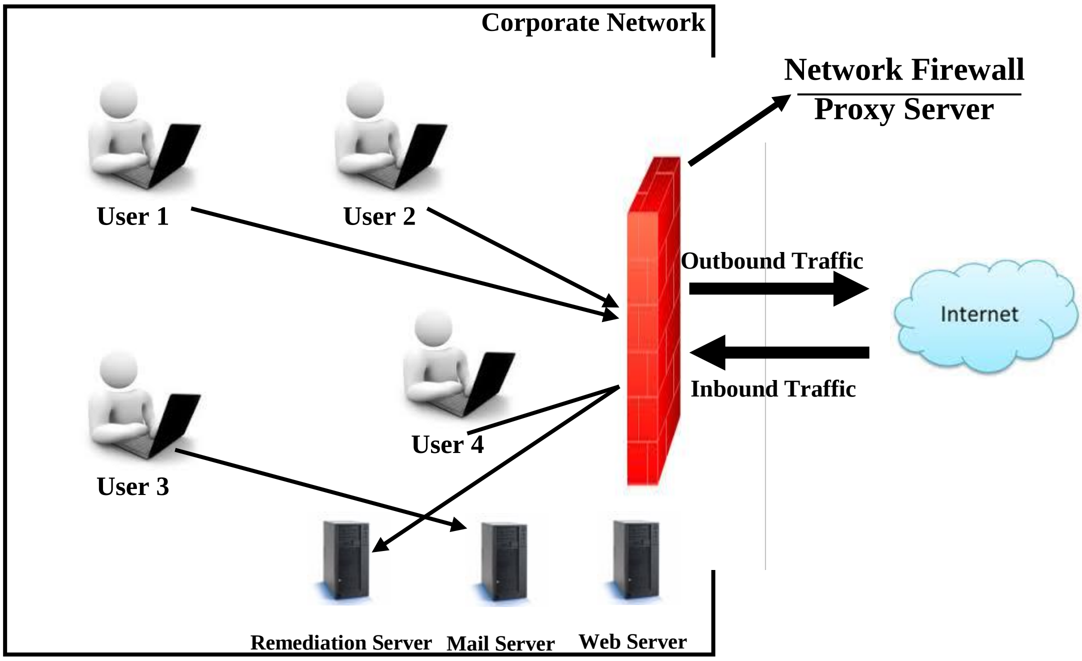


Figure 2.3 NAC implemented as a Perimeter Firewall

NAC adds additional layers of security into the LAN and to achieve this it implements three key attributes of secure networking. This includes:

i. **Access control.** Knowing who is on the network, what resources they are authorized to use, and applying access controls to their traffic.

ii. **Integrity.** Guaranteeing that the network itself is available as a critical resource and that threats can be identified and mitigated.

iii. **Privacy.** This attribute **e**nsures that all traffic on the network is not accessible to unauthorized/illegitimate users.

2.4.2 Components of NAC Architecture

The components of a NAC architecture are made up of the following: Endpoint (Agent-based Endpoint and Agentless Endpoint), Enforcement Points, Policy Servers Quarantine Server and Remediation Servers. Figure 2.4 describes the individual components that make up the NAC Framework solution.

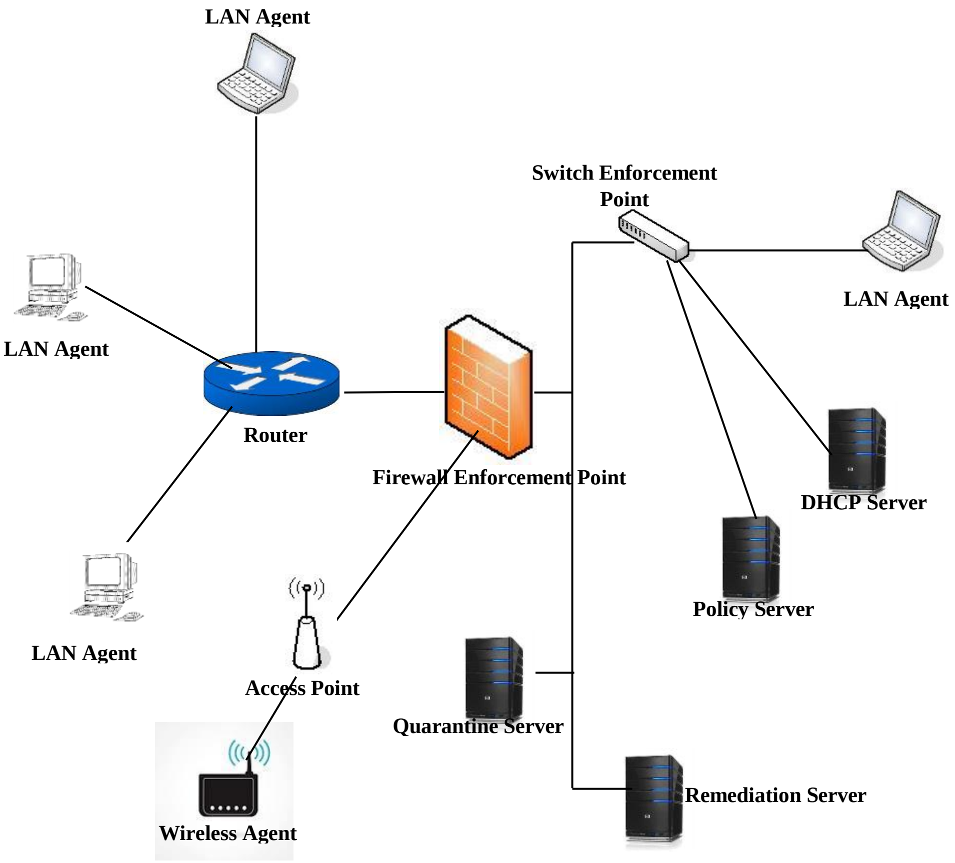


Figure 2.4 Components of the NAC Architecture

2.4.2.1 Endpoint

An endpoint is a client computer that requests access to network resources from a server computer. Two types of endpoints exists, namely; agent-based endpoint – this endpoint comes with a pre-installed application/software and agent-less endpoint – this endpoint comes without any pre-installed application/software.

Scenarios on Agent and Agentless Endpoint

When a host computer with a NAC-agent requests access to connect to a network, the agent prior to allowing access to the network will perform a posture assessment on the request for connection. The installed software is responsible for conducting posture assessment on the host.

In another instance, the NAC can sense the request for connection by a host to interact with the installed agent for posture information. The agent can then collaborate with all the other security modules to collate detailed information on the host. The observations are then forwarded to policy server(s) which are responsible for assessing the compliance status of host computers before the specified policies are enforced.

Additionally, when an agentless host connects to a protected network, the NAC is able to recognize the absence of an installed agent software on the host computer. The NAC then initiates a conversation with the host making it possible for it to download and install the required agent software. By so doing, the endpoint acts as an agent-based client.

2.4.2.2 Enforcement Points

An enforcement point is an integral part of every NAC system, in that it communicates and gains absolute control of host computers before allowing them to gain access to a protected network environment. Discussed are the enforcement points of a NAC architecture:

A. **Network Switch** - Through the IEEE's 802.1X standard for wired and WLANs, a network switch can be used to enforce access control policies at the port-level (layer-2) of the OSI model.

B. **Router** – Through the implementation of Access Control Lists (ACLs), a router is used at the IP layer (layer 3) of the OSI model to moderate network traffic and enforces policies.

C. **VPN Equipment** – A VPN device can be used to enforce policies on non-compliant hosts wanting to gain access to protected network resources and also assign access privileges to hosts on segmented networks.

D. **Firewall Technology** – This is a hardware or software security mechanism employed to monitor and control endpoint access to protected network environments by defining and enforcing defined rules as per laid down organizational network security policy.

E. **Enforcement Server** – This is a server computer that works in collaboration with a switch or a router to enforce defined policies or rules on a network. For instance, a DHCP server has the sole responsibility of leasing IP addresses to authenticated client computers on a network.

F. **Agent-Based Client** – This is a client computer that acts as an enforcement point based on the functionality of an already installed agent software. Instances where a host does not meet certain pre-defined policies, access to the network is denied. It also functions as a firewall in a network environment to enforce policies.

2.4.2.3 Policy Server

A policy server is a security component of a policy-based network which is directly involved in defining, administering and enforcing organization-wide network access control rules and regulations. In practice, the policy server can allow, deny access and control the extent to which a host can perform an action and also determine access privileges for host computers.

It accepts access control requests from host computers, matches them against pre-defined rules that define how network resources are allocated among various hosts and returns access control responses to the end users. It supports the Authentication, Authorization, and Accounting (AAA) framework and also implements the Remote Authentication Dial-In User Service (RADIUS) protocol.

2.4.2.4 Quarantine Server

A quarantine server is an isolated security-hardened server which provides a phased network access for host computers which do not meet pre-defined network policies by restricting them to a quarantine mode. It only allows non-compliant computers to communicate with a set of limited resources that mostly includes remediation servers, active directory servers, DHCP servers and policy servers. A quarantined workstation stays in quarantine mode until it passes all compliancy checks and its status configuration determined to be in compliance with the organization’s network security policy.

2.4.2.5 Remediation Server

A Remediation server contains all the resources such as patch files and antivirus signatures used to recover a quarantined workstation back to compliance status. After which, such machines are allowed to re-connect back to the protected network. A

Remediation server on its own can automatically or manually update an endpoint software, operating system software, antivirus patches and signatures.

2.5 Access Control Models

According to Samarati and Vimercati (2001), a security model presents a formal description of a security policy and its functionalities. Access Control Model is said to be the fundamental security backbone for managing network services. It serves as the foundation for regulating and managing access to network resources based on pre-defined security policies. A security policy therefore defines the high-level procedures that regulates the behavior choices of users on a network.

Access Control Models are thus classified into three main categories namely: Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role-Based Access Control (RBAC).

2.5.1 Mandatory Access Control (MAC)

Mandatory Access Control (MAC) grants access privileges to network resources based on pre-defined rules and regulations delegated by a central authority. It considers as subjects the processes operated on by users, thus controlling the indirect access of information. A multilevel security policy is the most common model of mandatory access control where each subject and object is assigned to an access class and partial order is defined among those access classes.

Views shared by Bell and LaPadula (1973) and Biba (1977), clearly state that authorization policies can be classified into secrecy-based mandatory policies and integrity-based mandatory policies. These two models could be applied in a manner to achieve the protection of both information confidentiality and user legitimacy.

2.5.2 Discretionary Access Control (DAC)

Initially proposed by Lampson (1974), and further formalized by Graham and Denning (1972) and Harrison (1975), DAC grants access privileges based on the identity of users and also enables them (users) to pass on their access privileges to other users where the permission and withdrawal of access rights are controlled by administrative policies. Typical mechanisms for enforcing DAC include: Authorization Table, Access Control List (ACL) and Capability, such that each one of them interprets and implements the access control mechanism in a different way. Discretionary access control suffers from vulnerabilities such as Torjan horses, rokbits and malwares.

2.5.3 Role-Based Access Control (RBAC)

Proposed by Baldwin (1990), RBAC supports network environments where access is granted to roles instead of individual users. A role is made up of a set of privileges granted to a user. Roles can be represented by how access control privileges are disseminated along an organization’s communication hierarchy.

With RBAC, the problem of granting access privileges to individual users is alleviated to assigning them roles. Thus the organizational responsibility of a user, rather than the user’s identity, determines the set of privileges. Defining a good role classification is not an obvious task, and there are always exceptions. Besides, organizations are dynamic in nature and the access rights associated with roles must be adjusted accordingly.

2.6 Functions of Network Access Control

The main goal of implementing Network Access Control (NAC) is to prevent the spread of malware infections and other threats in network environments. Discussed below is a set of functions provided by a NAC solution:

A. **Endpoint Detection.** The ultimate function of a NAC system is the ability to discover any device trying to gain access to a network. It is imperative for every NAC system to be aware of all devices on the internal network and those trying to connect so that other functions such as authentication, posture assessment, authorization and enforcement can be carried out. There are various ways by which a device can be detected depending on the access mediums employed such as; wired LAN, WLAN and VPN.

The following are the different means by which devices can be detected when connecting to a network:

i. A network switch can detect a device requesting access to a network in an 802.1X port-based access control architecture where the requesting device sends an Extended Authentication Protocol (EAP) request packets to the switch.

ii. Devices can also be detected when connecting to a network with a supplicant installed on the device. In an 802.1X architectures, a supplicant is required on the device for network connectivity. Whenever, the device tries to connect to the network, the supplicant will notify the NAC about its presence.

iii. A device can be detected when the Address Resolution Protocol (ARP) resolves the nodes IP address to its MAC or Ethernet address. By so doing the NAC solution discovers the device when it broadcasts an ARP request packet.

iv. A request broadcast for an IP address by a Dynamic Host Configuration Protocol (DHCP) can also lead to the element being detected.

v. Specialized hardware or software such as a firewall can also detect a node, when specific traffic is passed through them.

B. **Authentication.** A Network Access Control must be able to validate each and every workstation wanting to gain access to the network perimeter. Devices can be authentication in the following methods:

i. IEEE’s 802.1X standard for LANs and WLANs;

ii. Dynamic Host Configuration Protocol (DHCP);

iii. Point-to-Point protocol (PPP) in dial-up situations;

iv. Transport Layer Security/Secure Socket Layer (TLS/SSL); and

v. Secure HTTP (HTTPS)

C. **Posture Assessment**. One of the unique functions of a NAC system is posture assessment. It is directly responsible for accessing the compliance status of every device connecting to the network. It involves all the processes employed in gathering detailed information on devices and reporting back to policy servers to ascertain the level of compliance of each device.

D. **Authorization.** Once a device has been detected and authenticated, it must be granted permission to have access to resources on the network. When a user attempts to connect to a network environment, he/she must go through pre-defined steps of authentication and posture assessment before being considered compliant or non-compliant. If considered compliant, the NAC solution authorizes the user to access network resources and also determine the level of privileges assigned to the user.

E. **Policy Enforcement.** This is a network access control mechanism implemented by a NAC solution to define policies or rules for users and devices. The criteria determining whether a user or device is allowed or denied access to network resources is specified in a set of regulations contained in a policy. The AAA host system assesses the policy for the connecting device and forwards the decisions to the policy enforcement points where the required policies are enforced. Depending on the decisions arrived at after the posture assessment, the specified policy decision is enforced accordingly.

Below are some methodologies used to enforce access policies:

i. **Access Control List (ACL)** defines a list of permissions or access rules which are implemented to manage access privileges for devices on a particular network. It is actually used to specify which users are granted or denied access to network resources.

ii. **Virtual LAN (VLAN),** group devices with a common set of requirements regardless of their physical location. The access policies are then enforced with respect to the VLAN groups to control access to network resources. By this, a user or device is subject to a particular VLAN segment and granted access to policy-specific resources defined for that particular segment.

iii. **Firewall technology,** uses defined rule set to enforce network policies based on an existing security policy. This technology is a security control measure that enforces policies on private networks or on client machine locally. Depending on the criteria specified by the firewall, the defined policies are enforced accordingly.

F. **Quarantine.** This is an access control measure that restricts network access to devices that have failed compliancy checks. This is done to make sure the network remains safe and secure. One of the main objectives of the NAC technology is to isolate non-compliant devices to a separate network where the nodes can have access to specified network resources within a quarantine setup.

G. **Remediation.** This comprises a set of processes that a non-compliant endpoint goes through in order to recover back to a compliant state. After a device is quarantined, it is isolated to the quarantine setup where it is allowed access only to a defined set of remediation resources. The remediation resources allow the quarantined node to recover from non - compliant status to compliant status, so that the device can be re-admitted back onto the network, else quarantined again.

H. **Post-Admission Control.** This can very much be compared to threat mitigation. When a device is authenticated and authorized to access a private network, its sessions are monitored regularly for any malicious activity or policy violations. If any such activity is recorded, the user or device access is moderated by either limiting access, denying complete access or dropping the session.

2.7 Access Control with IEEE 802.1X

Over the years, the growing trend in technology has created a need to securely manage access for both users and mobile devices between the public (unprotected) and the private (protected) networks. Most organizations thus need to implement effective access control systems to detect and authenticate users and control device access to protected resources.

According to Lee (2010), IEEE 802.1X is a port-based authentication protocol used for both wired and wireless networks. It enhances the security levels of LANs by preventing unauthorized devices from gaining port-level access to the network through wired connections. It leverages an extensible architecture that supports a variety of authentication techniques, including passwords, RSA keys, token cards, and certificates. Before a client machine joins the network, the 802.1X is responsible for implementing access control and until the client is appropriately authenticated, network resources are blocked by the access control. The following key components describe the 802.1X framework:

i. **Supplicant:** This is the software installed on the client side of the 802.1X standard that seeks access to a protected network. For purposes of this thesis, a supplicant will be referred to a client machine.

ii. **Authenticator:** The authenticator serves as an intermediary between the supplicant and the external authentication server such as a switch or access point. It manages the authentication process between the supplicant and authentication server.

iii. **Authentication Server (AS):** The Authentication Server resides on the DS and provides authentication services to the authenticator. Based on the credentials provided by the supplicant, the AS controls whether the supplicant is authorized to access the services provided on the authentication server's protected network.

iv. **Port:** Typically found on a router or switch, with its state either unauthorized or authorized. An unauthenticated supplicant prior to authentication is initially connected to an unauthorized port on the public network. After successful authentication, the supplicant is then connected to an authorized port to access resources on the protected network.

v. **Extensible Authentication Protocol (EAP):** The EAP is a generic authentication architecture that supports many different types of authentication methods, including Kerberos, public-key encryption, and one-time passwords. Its communication between supplicants and authenticators is encapsulated using the EAP over LAN (EAPoL) protocol. EAP communication between authenticators and the authentication server is encapsulated using Remote Authentication Dial In User Service (RADIUS).

Executing of authentication related algorithms and mechanisms are managed by the PAE (Port Access Entity) which are present in the both the supplicant and the authenticator. Figure 2.5 illustrates the 802.1X architecture.

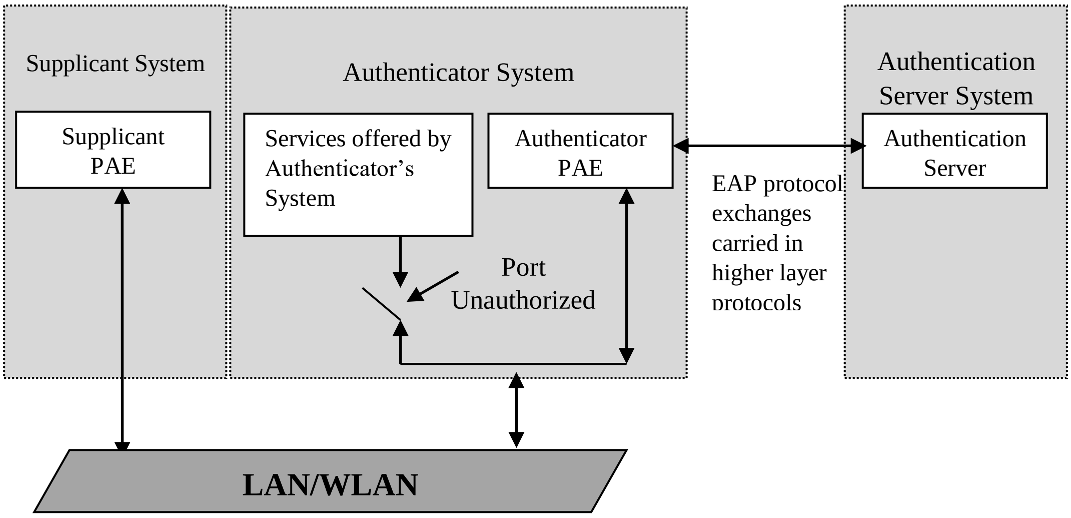

Supplicant System
Supplicant PAE
Authenticator System
Services offered by Authenticator's System
Authenticator PAE
Port Unauthorized
Authentication Server System
Authentication Server
EAP protocol exchanges carried in higher layer protocols
LAN/WLAN

Figure 2.5 IEEE 802.1X Access Control Framework (After Lee, 2010)

2.7.1 Categorization of the 802.1X Authentication Process

The IEEE 802.1X authentication process is categorized into two main stages as described below:

i. **Pre-authentication Process -** The IEEE 802.1X pre-authentication process begins with a client machine with a supplicant software installed that is used for negotiation prior to authentication. When the device connects to a communication medium, the authenticating software in the switch or access point restricts the device's connection to the protected network. Using one of the EAP methods, the authenticator establishes a security negotiation with the supplicant and creates an 802.1X session. The supplicant then provides its authentication information to the authenticator, which then proxies the information to an authentication server.

ii. **Authentication -** After the Authentication Server (AS) has authenticated the supplicant, it then initiates the authentication stage of the process, during this phase the authenticator facilitates an exchange of keys between the supplicant and the authentication server. After these keys are established, the authenticator grants the supplicant access to the protected network on an authorized port.

2.7.2 Attacks in 802.1x Protocol

The advantage of the 802.1X protocol is that it is a dual-port schema that can split network dataflow and authentication information, but its disadvantage is that it does not control access to the port after successful authentication, thus, problems, such as user name theft occur, this is described as follows.

Scenario 1: *Client* Computer 1 is connected to a port say Port A and authenticated via Switch1. After successful authentication, Computer 1 changes its IP address manually and keeps its access status to the Local Area Network (LAN) (the 802.1x protocol should therefore deny access to the client, because the client's identity is changed). An illegitimate user, Computer 2 is connected to a port say Port B and authenticated via Switch1 using the same username and password of Computer1. In this instance, Computer 2 will successfully pass the authentication because it bears the same username and password of Computer1, although it has a different IP address (the 802.1x protocol should therefore check that the same user should not be allowed from the same machine with different identity other than original). This is called *user name theft.*

Scenario 2: Hub 1 is connected to Port A in switch 1. Client 1 is a legitimate user and is connected to hub 1. Computer 2 is an illegitimate user and connected in another port of hub 1. As Computer 1 is a legitimate user, it can easily pass for authentication via switch 1. As soon as the authentication process is completed, Port A in switch1 enters into a controlled state and Port A will allow access to the supplicant from Computer 1. Once the authentication of Computer1 is successful, the authenticator will allow the illegal user of Computer 2 to freely access the Local Area Network (LAN) without any further authentication. This is very dangerous in terms of network security. This attack occurs due to absence of controlling on access port after authentication in 802.1X protocol.

Session hijacking: The Robust Security Network (RSN) provides mechanisms to deny network connectivity at the MAC layer to authorized entities via the 802.1x protocol. With IEEE 802.1X, the higher layer authentication takes place in two state machines, the RSN and the 802.1X state machine.

2.7.3 Extensible Authentication Protocol (EAP)

A lot of advantages exist in utilizing 802.1X in RSN, in that it allows various forms of upper layer authentication methods. EAP is a package that is capable of carrying out a variety of authentication mechanisms which includes digital certificates, one time passwords, etc. It also defines four primary packet types, these include; request, response, success and failure. A basic EAP message dialog is depicted in Figure 2.6.

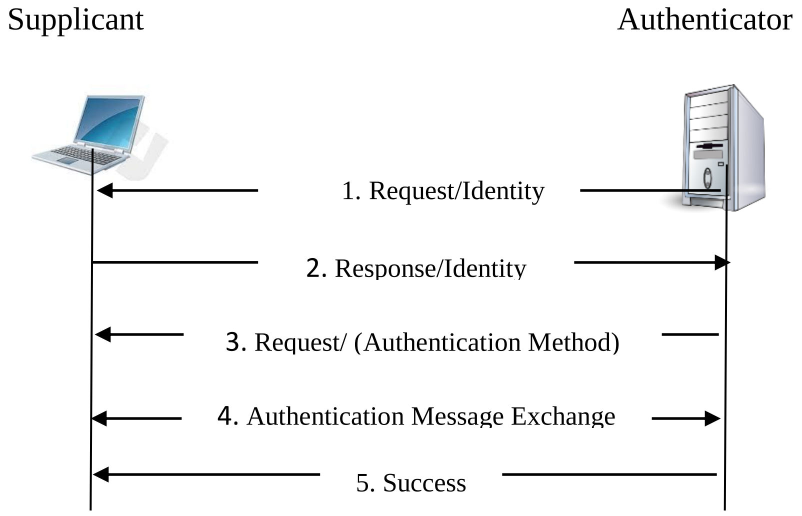


Figure 2.6 EAP Message Exchange Process (After Lee, 2010)

EAP involves a bidirectional communication approach for transmitting requests and response; this eventually produces either a success or a failure notice. With this process, a request/identity message is forwarded by the authenticator to a supplicant who replies with the message request/identity encapsulating the identifier which is to be decrypted by the authentication server. Following this process is an upper layer authentication exchange, which results in a final success or failure notification being sent to the supplicant as results.

2.7.3.1 Extensible Authentication Protocol over Local Area Network (EAPoL)

Extensible Authentication Protocol (EAP) was designed purposely to transport authentication exchange messages used by upper layer authentication models with dial-up connection via a modem. Before 802.1X became widely known as LAN authentication, EAP was mainly used to authenticate dial-up users.

In order for EAP authentication messages to be transmitted on a LAN, they need to be encapsulated. The IEEE 802.1X defined EAP over LAN (EAPoL) to encapsulate

EAP packets by adding an Ethernet header onto EAP messages so that they can be transmitted over the Ethernet. The EAPoL protocol defines the following four types of messages that are used by RSN:

EAPOL-START: This is a message sent by a supplicant of a client machine on a network to the authenticating server requesting for the authenticating process to be initiated.

EAPOL-KEY: With this type of message, the authenticator can send encryption keys to the supplicant.

EAPOL-PACKET: This structure is normally used for encapsulating actual EAP messages prior to transmission on the LAN.

EAPOL-LOGOFF: This message is used when a supplicant decides to disconnect itself from the network.

2.7.3.2 Remote Authentication Dial-In Service (RADIUS)

According to Rigney (2000), Remote Authentication Dial-In User Service (RADIUS) can be described as a networking protocol that implements the AAA framework that provides centralized authentication, authorization, and accounting (AAA) management for users and devices who connect to access services in an IP based network.

RADIUS is not explicitly a part of the IEEE 802.1X standard but most of the existing enterprise wired and WLAN implementations use it for transmitting authenticated messages between the authenticator and the authentication server. RADIUS is a client/server protocol that runs in the application layer, using UDP as the transport channel. The Remote Access Server, the Virtual Private Network Server, the Network switch with port-based authentication, and the Network Access Server (NAS), are all gateways that have a RADIUS client component that communicates with the RADIUS server. It is often the backend of choice for 802.1X authentication as well.

For this research, RADIUS was used to provide AAA services. Although Diameter (2003), a successor to RADIUS, can also be used for the same purpose, the authentication concept and operations are very similar.

2.7.3.3 802.1X Architecture in RSN

The 802.1X architecture allows for the secure exchange of client credentials and prevents unauthorized access to network resources due to the fact that authentication is done before the assignment of a network IP address.

This architecture consolidates decision making at the RADIUS server, so that passwords no longer have to be individually configured into every client machine. It also allows clients to authenticate with credentials. Supplicant credentials are securely passed to the authenticator via a secure EAP method (e.g., EAP-TLS), and then forwarded to the authentication server via EAP in RADIUS.

This is a Layer 3 transmission that allows for the secure passing of authentication messages (authentication request, authentication result) and access authorization (accept, reject) between the authenticator and authentication server. Figure 2.7 outlines the 802.1X authentication and authorization process in the RSN environment.

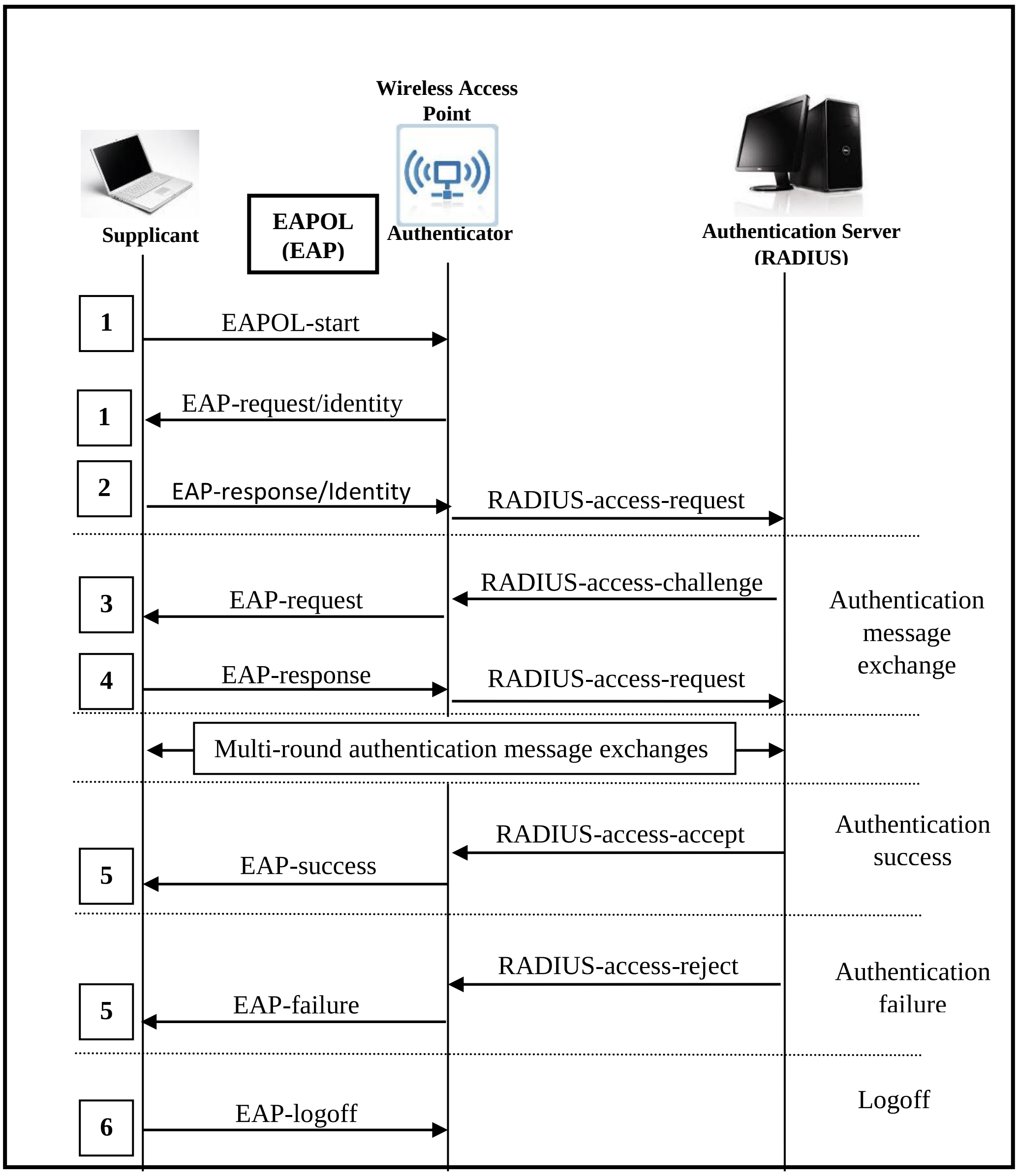


Figure 2.7 802.1X Authentication Architecture in RSN

Neither the authenticator nor the supplicant can initiate an 802.1X authentication process. The authenticator initiates a message by sending an EAP-Request/Identity frame. The supplicant initiates an authentication message by sending an EAPOL-Start frame, to which the authenticator responds with an EAP Request/Identity packet. The supplicant sends an EAP-Response/Identity message to the authentication server via the authenticator to provide its identity. The authenticator encapsulates the EAP-Response/Identity message in RADIUS-Access-Request for forwarding to the server.

The authentication server investigates the supplicant by sending a RADIUS-Access Challenge to the authenticator, which then forwards it in the form of an EAP Request frame to the supplicant.

The supplicant then provides its authentication credentials (e.g., username and password) in an EAP-Response message, which is again forwarded to the authentication server by the authenticator in the format of RADIUS-Access- Request.

After several message exchanges for the EAP authentication method (e.g., EAP-TLS), the authentication server determines the access permission and either sends a RADIUS-Access-Accept or RADIUS-Access-Reject to the authenticator. On receipt of RADIUS-Access-Accept, the authenticator changes the supplicant's state to Authenticated, unblocks the controlled port (allowing full access).

The authenticator then sends an EAP-Success message to indicate the success of authentication to the supplicant. Similarly, EAP-Failure is sent if the authentication fails.

To disconnect from the network, the supplicant sends an EAPOL-Logoff frame to the authenticator. This causes the authenticator to change the supplicant's state to unauthenticated and the controlled port to unauthorized, thus blocking the network access.

2.7.3.4 Authentication Protocols

According to Nidal *et al*., (2005), computer networks face a number of challenges, with attacks coming from within and outside of the network. Moreover, the absence of a clear line of protection at traffic concentration points also pose a challenge to implementing security solutions in networks.

The current trends in transmission media and the dynamic nature of network topologies add even more complications to network connectivity, thus, presenting other forms of security loopholes. In order to deploy a clear line of defense for any network environment, support for authentication, confidentiality, integrity, non-repudiation, and access control needs to be provided.

For every well secured network, authentication is the cornerstone service, since other services depend fully on it to further enhance the protection and security of the network and its resources. Authentication supports privacy protection by ensuring that all objects are verified and validated before disclosing any secret information amongst themselves.

Furthermore, it supports confidentiality and access control, by allowing access to network services and architecture to authorized entities only, while denying access to unauthorized entities.

2.7.3.5 Components of the Authentication Process

Authentication is a procedure that involves an authenticator initiating a communication session with a supplicant using an authentication protocol to verify access credentials presented by the supplicant in order to define the level of access privileges allowed to the supplicant.

A standard authentication process has six major sections. The first phase named Bootstrapping, is where the supplicant is securely provided with something that it should possess, say a key or a password that will prove to the authenticator that the supplicant is legible to access protected network resources.

Once the bootstrapping phase is completed, the supplicant is then ready to join the network. The pre-authentication process is where a supplicant submits its credentials to the authenticator in an attempt to substantiate its legitimacy to access the protected network resources. After the credentials of the supplicant have been verified, a procedure known as a credential establishment process is invoked to ascertain the supplicant’s new credentials, which will be used as a proof of its true identity.

After carefully going through all the steps successfully, a supplicant is then considered legitimate and authenticated, which then authorizes it to access resources protected by the authenticator. Throughout the authentication process, all communication sessions established between the supplicant and the authenticator is verified and authenticated at the source and validated at the destination using the pre-defined credentials.

Whiles a supplicant is authenticated, its behavior is regularly monitored for fear of its being compromised. Instances where a supplicant becomes compromised, its credentials are immediately revoked or its credentials re-establishment request is denied. A basic Standard Authentication Process in Networks is depicted in Figure 2.8.

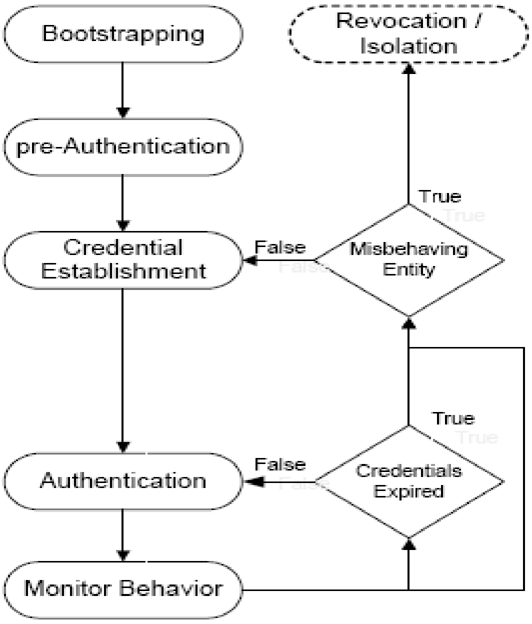


Figure 2.8 Functions in a Standard Authentication Process in Networks

CHAPTER THREE

METHODOLOGY

This Chapter focuses explicitly on the research methodology employed to achieve the objectives of the thesis. It is important to note that several open source network management software were employed to manage user access and monitor user traffic behaviors on the network. The scope of this thesis is limited to the University of Mines and Technology, UMAT campus.

3.1 Study Area

The study was conducted at the University of Mines and Technology (UMaT). UMaT is located on a 1.60 square-kilometers of undulating land at Tarkwa, 89 kilometers from Takoradi, the Western Regional capital. The campus presents a scenery of old beautiful buildings interspersed with modern ones with green lawns and tropical flora which provide a calm and refreshing atmosphere pleasant for academic work. UMaT has become a pivotal center of excellence for the training of engineers and technologists in mining, petroleum and allied disciplines not only for Ghana but also for Africa and other parts of the world within the short period of its inception.

The university's administration block, library, faculty buildings, clinic, auditorium and the halls of residence occupy the central portion of the campus. Currently, there are two Faculties, namely; the Faculty of Mineral Resource Technology (FMRT), which houses six (6) departments and the Faculty of Engineering (FOE), which houses four (4) departments. There is also the School of Postgraduate Studies (SPS) which coordinates all postgraduate education in the University and the Center for Communication and Entrepreneurship Skills (CENCES) which currently serves as the nucleus of the future Faculty of Integrated Management Sciences.

Directly opposite the university is the University Basic School (UBas). UMaT has three halls of residence namely, the Chamber of Mines hall and MT Kwoffie hall which are located at the western end of the campus while the Gold Refinery hall is situated on a highland at the northern outskirts of Tarkwa.

The University has a number of other municipal facilities. These include a Campus radio station, Maintenance Unit, Estate Unit, Transport Unit and a Security Unit.

3.2 UMaT Network Infrastructure

The Local Area Network (LAN) infrastructure implemented on UMaT campus is to provide facilities to support and enhance internal communications and also interface with external networks (i.e. the internet) to support the university’s core mandate which is active research, teaching and learning; information sharing; online course registration; examination results checking; staff and student workgroup collaborations; and many others.

Currently, the LAN infrastructure spans a maximum distance of approximately 1.39 square-kilometers and interconnects the administration block, the faculties, the clinic, the library, the halls of residence, the maintenance unit, the University radio station and the University Basic School with high speed ethernet links operating over a dedicated fiber optic backbone as shown in Figure 3.1. Below is a general overview of the UMaT LAN:

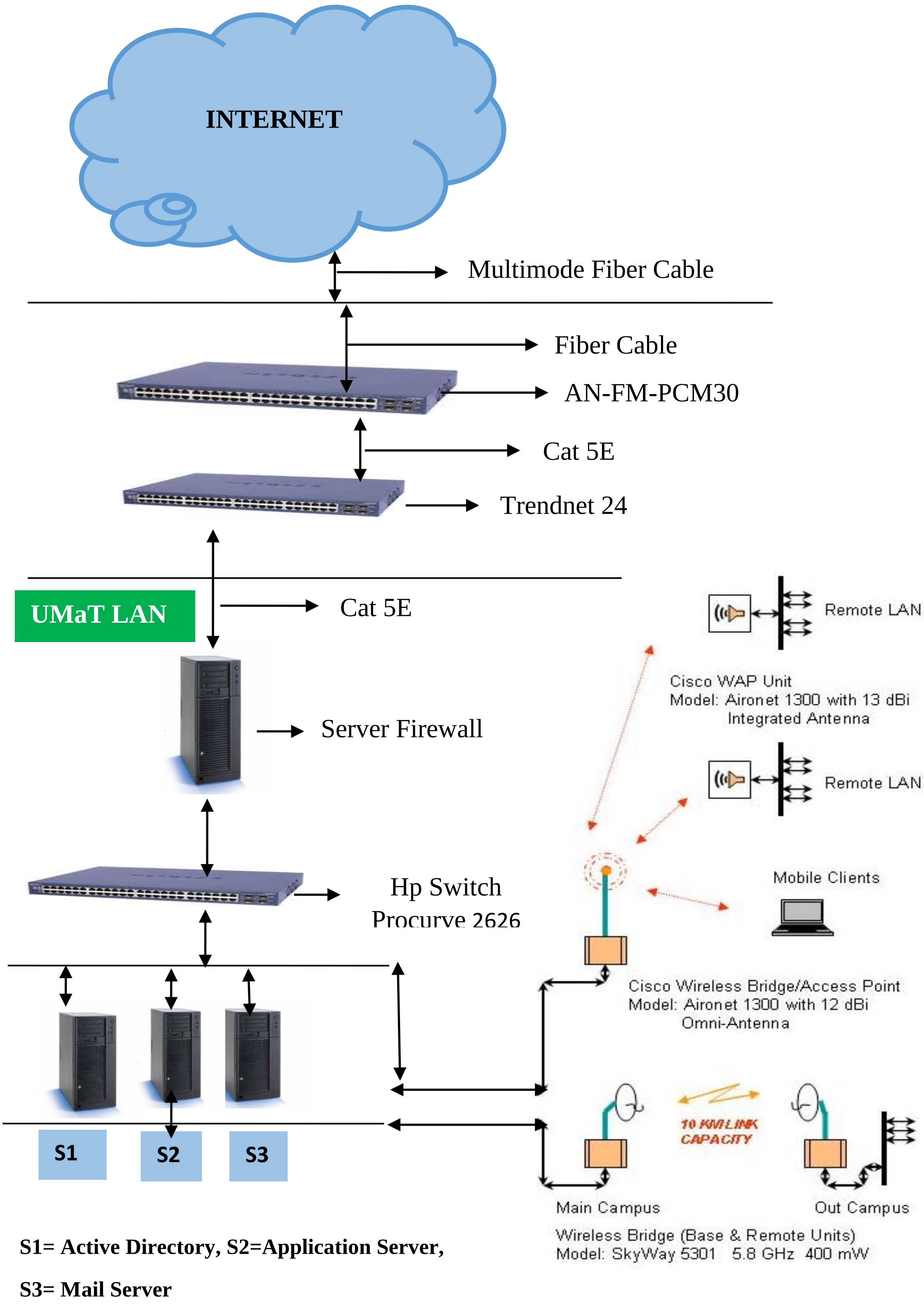
The main LAN internet backbone which is located at the Network Operation Centre (NOC) also doubles as the main base station and associates with six (6) other base stations by way of linking the respective buildings to the NOC's LAN.

The Internet Service Provider (ISP) provides a point to point internet connection with download and upload bandwidth stream of 45 MB from their main Network Operation Centre (NOC) to an HP Procurve 6108 LAN switch with fiber ports at the UMaT NOC. The LAN switch is then connected by way of Cat 5E ethernet cables through a Trendnet 24 port ethernet switch to a Linux box which serves as a firewall and doubles as a proxy server. The LAN is then connected by way of Cat 6 ethernet cables through an Hp Procurve 2626 switch to the Active Directory server, Mail server and Application server.

The LAN backbone then serves as a transmitter by receiving network signals from the main NOC and appropriately transmits it to the other base stations located at their respective points. A Cisco Aironet 1300 wireless bridge/access point with 12 dBi omni-antenna and serving as the WLAN base station is connected to the LAN switch to bridge all the other six (6) Cisco Aironet 1300 outdoor units.

At these six locations, the Cisco Aironet 1300 bridges are connected directly to one of the ethernet ports of a Dynamic Host Control Protocol (DHCP) server with two (2) network cards performing IP Address distribution and Network Address Translation (NAT).

The second Ethernet port is then connected to the switch by means of a straight cable. All offices then join the internal network through individual wall jacks directly connected to a switch.



S1= Active Directory, S2=Application Server,

S3= Mail Server

Figure 3.1 UMaT Network Infrastructure

3.2.1 NOC Association with Base Stations

The main LAN internet backbone located at the Network Operation Centre (NOC) also doubles as the main base station and associates with six (6) other base stations by way of linking the respective buildings to the NOC's LAN. Apart from the administration and the Library blocks which are connected to the NOC by way of fiber optic connectivity, the other base stations are connected by way of high speed ethernet Cat 6 cables.

There is a main base station Cisco Aironet 1300 series outdoor unit which serves as the main connection to the Local Area Network (LAN) at the Network Operation Centre (NOC). The main base station Cisco Aironet 1300 series outdoor unit then associates with the six (6) base stations Cisco Aironet 1300 series outdoor units which are located at the two faculties, administration block, basic school, library block and the Chamber of mines hall to serve as a bridge to the LAN at the NOC.

The six (6) base stations then connect through to a Proxy Server located at the NOC to distribute internet to all departments by way of Active Fiber connection, Cat 6 cable connection and Wireless connection. The six (6) base stations also connect to a Dynamic Host Configuration Protocol (DHCP) server which operates on the client-server model to perform Network Address Translation (NAT) and assignment of IP addresses to various devices on the network.

The DHCP server connects to an Active Directory server that holds usernames and passwords of all users in the University community to authenticate and authorize user credentials. The LAN is further extended using wireless network adaptors via Access Points to mobile devices such as laptops, smart phones and Personal Digital Assistants (PDAs) as depicted in Figure 3.2.

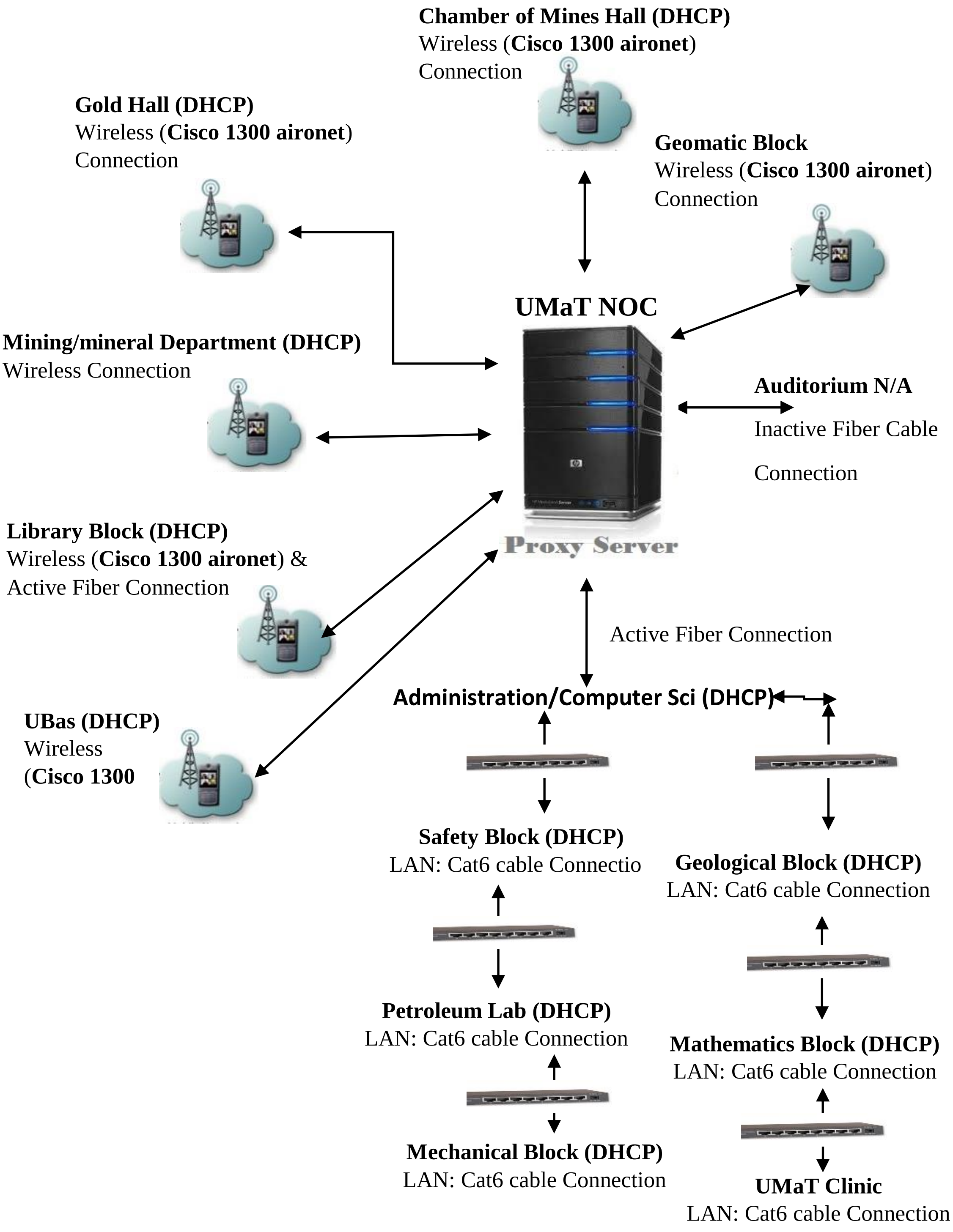

Chamber of Mines Hall (DHCP)
Wireless (Cisco 1300 aironet)
Connection
Gold Hall (DHCP)
Wireless (Cisco 1300 aironet)
Connection
Geomatic Block
Wireless (Cisco 1300 aironet)
Connection
UMaT NOC
Mining/mineral Department (DHCP)
Wireless Connection
Auditorium N/A
Inactive Fiber Cable
Connection
Proxy Server
Library Block (DHCP)
Wireless (Cisco 1300 aironet) &
Active Fiber Connection
Active Fiber Connection
Administration/Computer Sci (DHCP)
UBas (DHCP)
Wireless
(Cisco 1300
Safety Block (DHCP)
LAN: Cat6 cable Connectio
Geological Block (DHCP)
LAN: Cat6 cable Connection
Petroleum Lab (DHCP)
LAN: Cat6 cable Connection
Mathematics Block (DHCP)
LAN: Cat6 cable Connection
Mechanical Block (DHCP)
LAN: Cat6 cable Connection
UMaT Clinic
LAN: Cat6 cable Connection

Figure 3.2 Network Operating Center Association with Base Stations

The six (6) client based stations transmit network signals from the main base station located at the NOC via the DHCP server and vice versa. These signals are then transmitted to all offices for internet access by way of straight cable connection to individual wall jacks through switches in their respective locations.

This same signals are transmitted to APs to enable mobile users within the community to gain access to the network. The user enjoys Internet access after fulfilling all the requirements needed for access to the network.

3.3 Tools Used for Performing Analysis on the UMaT LAN

To attain the goal of this thesis, an analysis was performed on the UMaT LAN to identify the vulnerabilities on the network. The analysis provided insights into the behavior patterns of network users with regards to network traffic flows, protocols and individual data packets.

The analysis also provided detailed perspectives into the bandwidth utilization trends and vital views into the events taking place on the underlying network communication channel with respect to the LAN performance. The software and hardware version requirements used in this thesis are provided in respective phases.

3.4 Machine Setup to be the Main Firewall

To accomplish the objective of this thesis, the pfSense v2.1.5 open source software was installed on an Hp ProLiant GL110 server machine to make up the dedicated firewall for the network perimeter. This server machine was chosen because of its robustness, improved processor speed, memory size and performance.

3.4.1 Hard Specifications

The following hardware specifications were required:

i. Vendor: Hp

ii. Server Name: Hp ProLiant GL110

iii. Model: N5050

iv. Processor: Intel® Pentium 4

v. Hard Disk Size: 500 GB

vi. Processor Speed: 3.5GHz

vii. Installed Memory (RAM): 8GB (can be upgraded to 16 GB)

viii. Network Adaptors:

- Intel (R) Pro/1000 Legacy Network Connection 1.0.6 Server Adapter 1
- Intel (R) Pro/1000 Legacy Network Connection 1.0.6 Server Adapter 2

3.4.2 Software Requirement:

The following software was required:

i. pfSense v2.1.5 and above.

Additional Packages to be installed include:

i. Squid Proxy Server

ii. Squid Guard

iii. Squid Analysis Report Generator (SARG)

3.4.3 pfSense Software

Anon. (2004) describes pfSense as an open source network firewall/router software distribution based on the FreeBSD operating system. It is specifically installed and tailored for use as a perimeter firewall or router and can be managed or upgraded almost entirely from a Graphical User Interface (GUI). In addition to being a firewall and a routing platform, it includes a long list of other features and packages allowing its capabilities and functionalities to be further expanded. The name pfSense was arrived at because it brings out more meaning to non-technical users on the stateful packet-filtering tool (PF) which acts as a firewall, packet filter and a routing service on many BSD and Unix platforms.

pfSense provides three options for installation. The first option runs the pfSense installer directly from a Live CD or bootable USB drive. Any configuration changes made are then saved on a floppy drive or USB flash drive. The drawback to this approach is that, the setup does not allow for the installation of additional packages.

The second option deals with the installation of an embedded image of the pfSense installer on a CompactFlash (CF) card rather than on a hard drive. CF cards can handle a limited number of writes, so the embedded version runs as read only, while the file system runs as read/write from system memory.

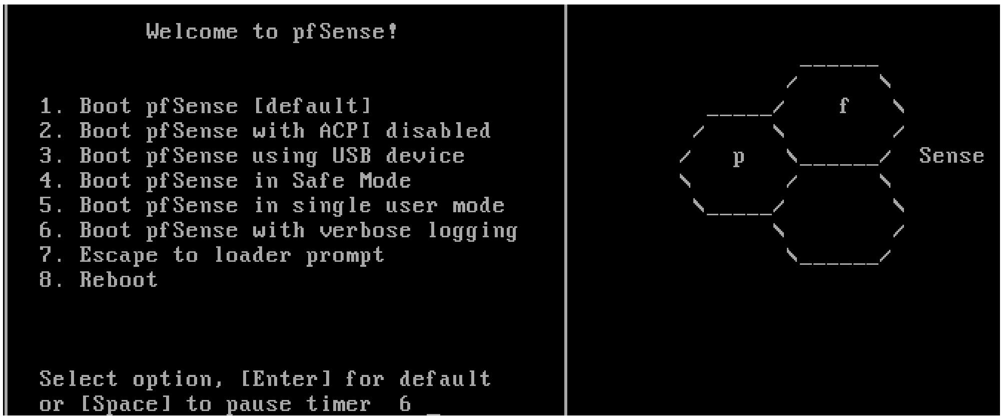
The pfSense Live CD installation is the third option which allows for a full installation onto a hard drive. Additional functional packages are fully supported using this method. Be aware though that the entire hard drive allocated will be overwritten. This installation method is the most preferred when pfSense is going to serve as the main perimeter firewall for the network.

For purposes of this thesis, the third installation option was adopted.

3.4.4 Steps involved in pfSense installation and Configuration

Step One: Getting the pfSense CD ready for Installation

The pfSense Live CD Installer was downloaded from the pfSense webpage and copied onto a blank CD/DVD as an ISO image. After successful burning, the installation CD/DVD was slotted into the CDROM of the Hp ProLiant GL110 server machine. The machine was restarted to enable booting from the pfSense installer CD/DVD. As the pfSense starts booting, a prompt was displayed with some options and a countdown timer as shown in Figure 3.3. By default, the first option was selected to install pfsense to the hard disk in the server machine.

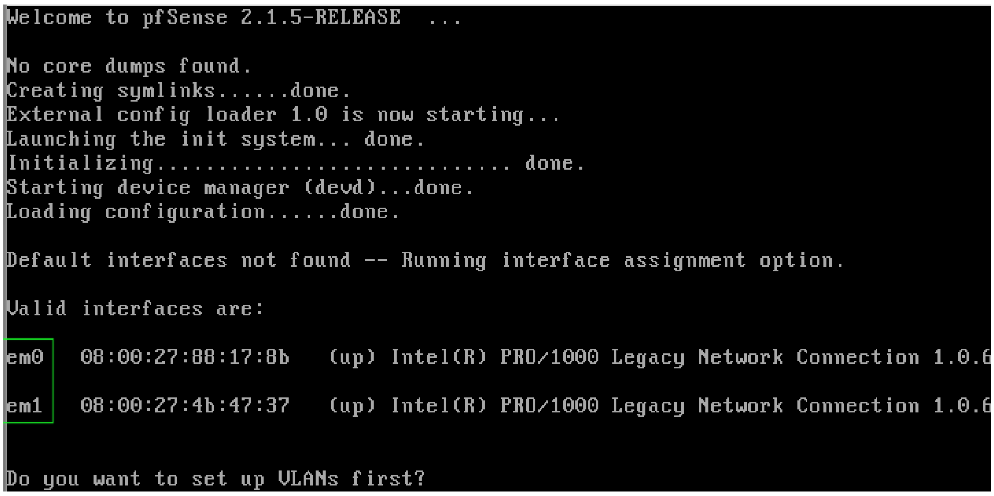


```
        Welcome to pfSense!                          ______
                                                    /      \
  1. Boot pfSense [default]                   _____/   f    \
  2. Boot pfSense with ACPI disabled         /     \        /
  3. Boot pfSense using USB device          /   p   \______/  Sense
  4. Boot pfSense in Safe Mode              \       /      \
  5. Boot pfSense in single user mode        \_____/        \
  6. Boot pfSense with verbose logging             \        /
  7. Escape to loader prompt                        \______/
  8. Reboot


  Select option, [Enter] for default
  or [Space] to pause timer  6 _
```

Figure 3.3 pfSense Software Installation Process

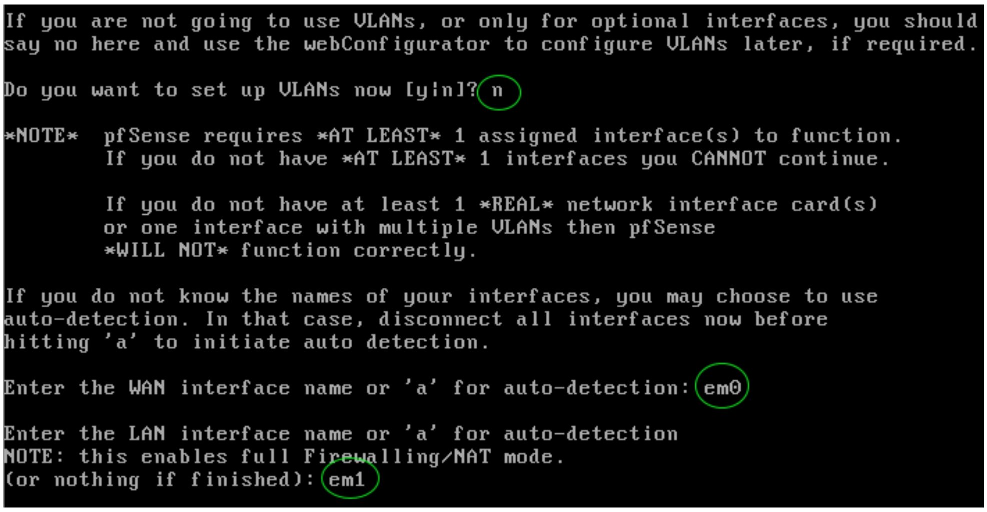
Step Two: Detect and Configure Network Interface Cards (NICs)

As started in step one, the software was made to run until a screen was presented listing the valid network interfaces with a request to setup VLANs as shown in Figure 3.4. In this instance, the VLAN setup request was declined as it would be configured later using the pfsense Graphical User Interface (GUI). By default, all the NICs in the resident machine would be detected, as in this case two cards were detected. By default the two NICs were named em0 and em1 respectively. The NIC em0 was then assigned Wide Area Network (WAN), to serve as the external interface with other networks including the internet and the NIC em1 assigned Local Area Network (LAN) to serve as an internal interface with firewall/Network Address Translation (NAT) features as shown in Figure 3.5.



```
Welcome to pfSense 2.1.5-RELEASE  ...

No core dumps found.
Creating symlinks......done.
External config loader 1.0 is now starting...
Launching the init system... done.
Initializing............................ done.
Starting device manager (devd)...done.
Loading configuration......done.

Default interfaces not found -- Running interface assignment option.

Valid interfaces are:

em0    08:00:27:88:17:8b   (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.6

em1    08:00:27:4b:47:37   (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.6


Do you want to set up VLANs first?
```

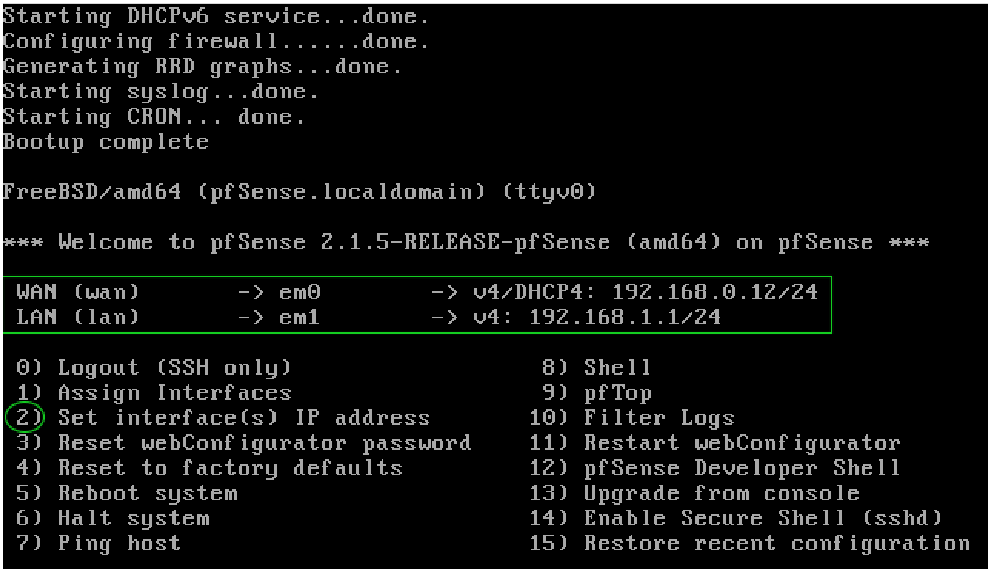
Figure. 3.4 Detecting the Network Interface Cards



```
If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y|n]? n

*NOTE*  pfSense requires *AT LEAST* 1 assigned interface(s) to function.
        If you do not have *AT LEAST* 1 interfaces you CANNOT continue.

        If you do not have at least 1 *REAL* network interface card(s)
        or one interface with multiple VLANs then pfSense
        *WILL NOT* function correctly.

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): em1
```

Figure 3.5 Labeling Network Interface Cards

The pfSense by default was configured to allow the WAN interface receive its IP address from the DHCP server whilst the LAN interface was assigned a static address of 192.168.1.1 as shown in Figure 3.6. Static IP addresses were thus assigned to both NICs after accessing the pfSense Graphical User Interface (GUI). After all the above settings were performed, a link was prompted to access the pfSense web configurator interface to configure further steps. The default username and password for the pfSense GUI is ***admin*** and ***pfsense*** respectively.



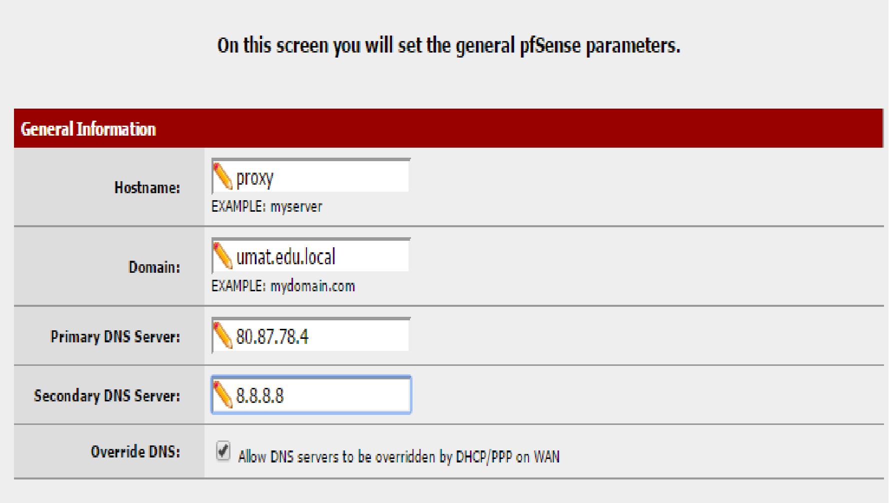
```
Starting DHCPv6 service...done.
Configuring firewall......done.
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.1.5-RELEASE-pfSense (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.0.12/24
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  8) Shell
 1) Assign Interfaces                  9) pfTop
 2) Set interface(s) IP address       10) Filter Logs
 3) Reset webConfigurator password    11) Restart webConfigurator
 4) Reset to factory defaults         12) pfSense Developer Shell
 5) Reboot system                     13) Upgrade from console
 6) Halt system                       14) Enable Secure Shell (sshd)
 7) Ping host                         15) Restore recent configuration
```

Figure 3.6 Finalizing pfSense Installation process

Step Three: Configuring pfSense Via Graphical User Interface

The pfSense WebGUI was used to configure the vast majority of items in the pfSense environment. It was accessed by connecting a client computer to the LAN and making sure it obtained an IP address via the DHCP server. The pfSense environment was accessed by navigating to https://192.168.1.1/, through a web browser and using the default username *admin* and password *pfsense* to login.

Upon successful login, the WebGUI was redirected to a setup wizard which served as a guide to complete the configuration of pfSense. The Hostname of the system was specified and the Domain Name Server (DNS) defined whilst the Primary DNS server and Secondary DNS server were configured with static IP addresses as shown in Figure 3.7. The server time zone was also configured.



On this screen you will set the general pfSense parameters.

General Information

Hostname: proxy
EXAMPLE: myserver

Domain: umat.edu.local
EXAMPLE: mydomain.com

Primary DNS Server: 80.87.78.4

Secondary DNS Server: 8.8.8.8

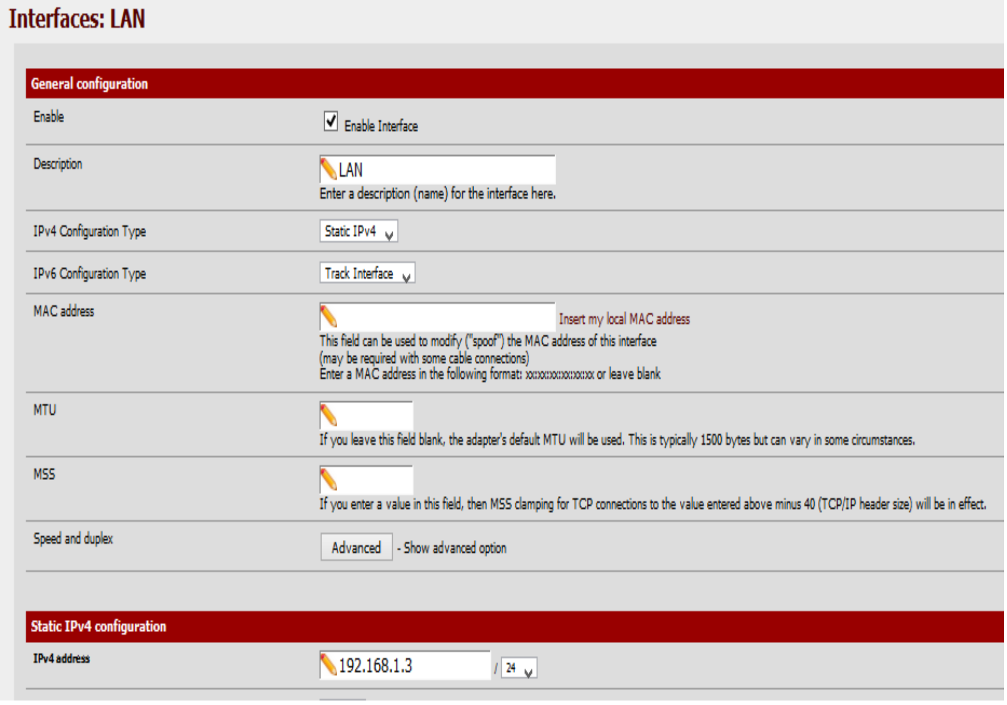
Override DNS: ☑ Allow DNS servers to be overridden by DHCP/PPP on WAN

Figure. 3.7 Configuring Domain Name Server (DNS)

Step Four: Configuring LAN and WAN Interface Cards

The LAN interface was reconfigured by assigning a static IP address of 192.169.1.3 to serve as the internal interface with the firewall and also serve as the default gateway through which web traffic from all computers plugged into the LAN will be routed before gaining access onto the internet.

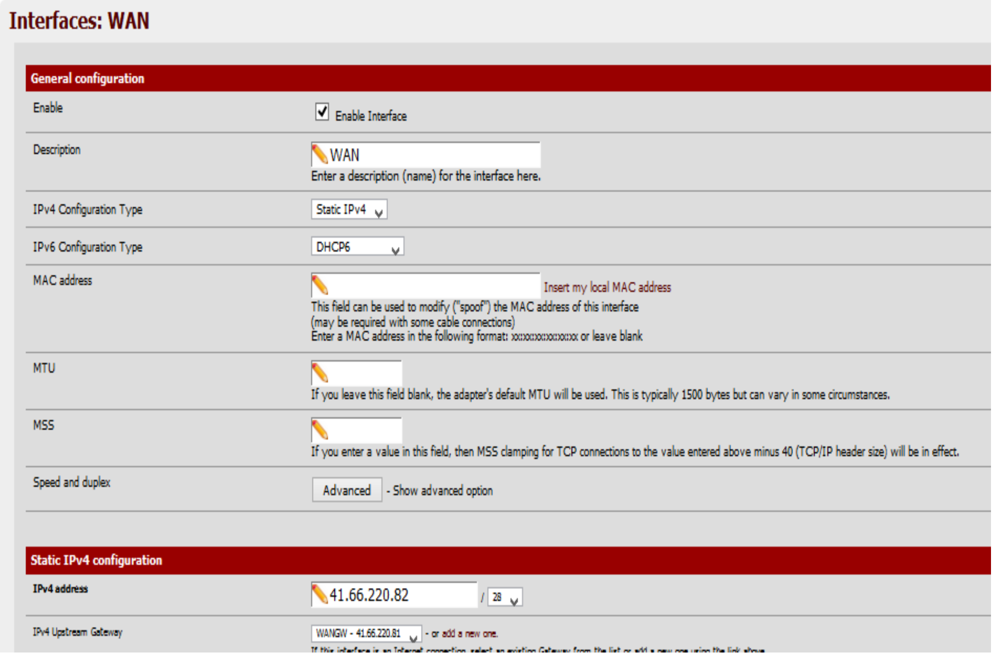
The WAN interface was used to configure all internet settings on the firewall. The WAN interface was configured by assigning a static IP address of 41.66.220.82. Figures 3.8 and 3.9 show the LAN and WAN configuration settings.



Interfaces: LAN

General configuration	
Enable	☑ Enable Interface
Description	LAN Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	Track Interface
MAC address	Insert my local MAC address This field can be used to modify ("spoof") the MAC address of this interface (may be required with some cable connections) Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank
MTU	If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.
Speed and duplex	Advanced - Show advanced option
Static IPv4 configuration	
IPv4 address	192.168.1.3 / 24

Figure 3.8 LAN Network Interface Card Configured



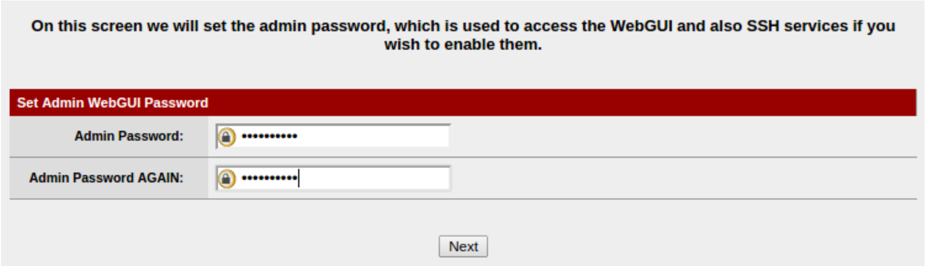
Interfaces: WAN

General configuration	
Enable	☑ Enable Interface
Description	WAN Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	DHCP6
MAC address	Insert my local MAC address This field can be used to modify ("spoof") the MAC address of this interface (may be required with some cable connections) Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank
MTU	If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.
Speed and duplex	Advanced - Show advanced option
Static IPv4 configuration	
IPv4 address	41.66.220.82 / 28
IPv4 Upstream Gateway	WANGW - 41.66.220.81 - or add a new one. If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the link above.

Figure 3.9 WAN Netwotk Interface Card Configured

Step Five: Finalizing the pfSense Configuration

In the final stages of the configuration process, the administrator username and password were changed from the default entries. The reload button was then clicked for the page to be refreshed to effect the changes. A final dialog box was presented with a link to proceed to the pfSense Dashboard.

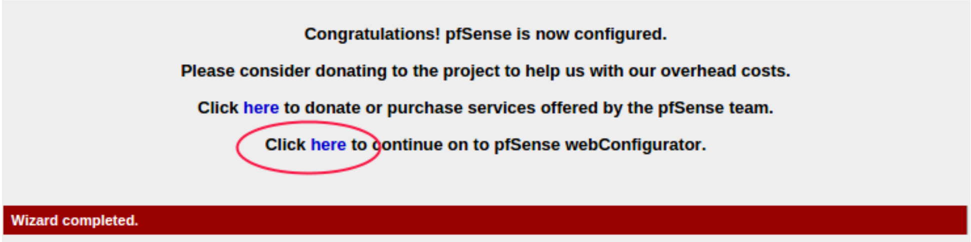


On this screen we will set the admin password, which is used to access the WebGUI and also SSH services if you wish to enable them.

Set Admin WebGUI Password

Admin Password:	••••••••••
Admin Password AGAIN:	••••••••••

Figure 3.10 Resetting pfSense Password



Congratulations! pfSense is now configured.

Please consider donating to the project to help us with our overhead costs.

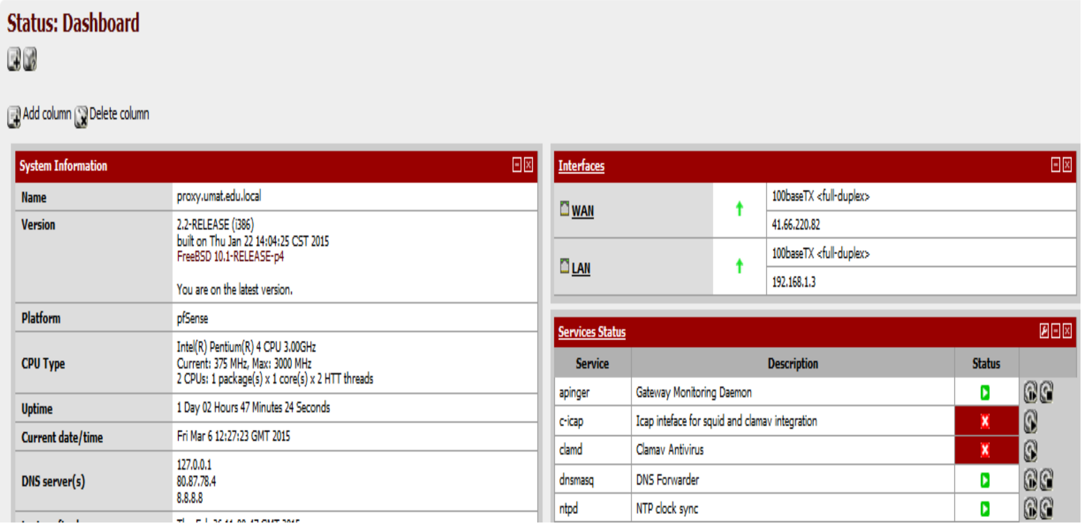
Click here to donate or purchase services offered by the pfSense team.

Click here to continue on to pfSense webConfigurator.

Wizard completed.

Figure 3.11 pfSense Final Configuration Process

The pfSense dashboard is the main page of the firewall which makes monitoring various aspects of the system easy. It is composed of various widgets with each one displaying information about different areas of the firewall. Figure 3.12 displays the dashboard that lists some of the widgets arrived at after the configuration of the pfSense firewall. The dashboard can be customized by adding and deleting columns as depicted in Figure 3.12.



Status: Dashboard

System Information

Name	proxy.umat.edu.local
Version	2.2-RELEASE (i386) built on Thu Jan 22 14:04:25 CST 2015 FreeBSD 10.1-RELEASE-p4 You are on the latest version.
Platform	pfSense
CPU Type	Intel(R) Pentium(R) 4 CPU 3.00GHz Current: 375 MHz, Max: 3000 MHz 2 CPUs: 1 package(s) x 1 core(s) x 2 HTT threads
Uptime	1 Day 02 Hours 47 Minutes 24 Seconds
Current date/time	Fri Mar 6 12:27:23 GMT 2015
DNS server(s)	127.0.0.1 80.87.78.4 8.8.8.8

Interfaces

WAN	↑	100baseTX <full-duplex> 41.66.220.82
LAN	↑	100baseTX <full-duplex> 192.168.1.3

Services Status

Service	Description	Status
apinger	Gateway Monitoring Daemon	▶
c-icap	Icap inteface for squid and clamav integration	✗
clamd	Clamav Antivirus	✗
dnsmasq	DNS Forwarder	▶
ntpd	NTP clock sync	▶

Figure 3.12 pfsense Firewall Dashboard

3.5 Squid Proxy Server

After the installation of the pfSense firewall, the squid proxy server was installed to effectively manage all incoming and outgoing web traffic. The squid proxy server is an open source web caching proxy server installed on a UNIX box through which all web traffic from client workstations connected to the LAN are routed before gaining access to the internet.

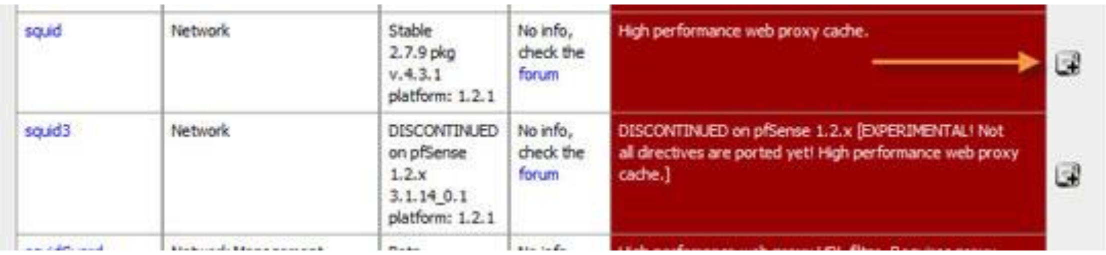
It is a fully featured web proxy cache server which provides proxy and cache services for Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS), File Transfer Protocol (FTP), and many other protocols. It also reduces bandwidth congestion and improves response times by caching and reusing frequently-requested web pages.

A squid proxy server is installed on the remote side in-front-of destination web servers to protect the servers by request filtering, speeding up web page delivery and caching frequently requested files. It acts as an intermediary by passing the client's request on to the server and saving a copy of the requested object. It was configured with a large amount of physical memory as squid maintains an in-memory cache for increased performance. It can thus be installed on most available operating systems, including Windows and is licensed under the General Public License (GPL).

3.5.1 Steps Involved in Squid Proxy Server Installation

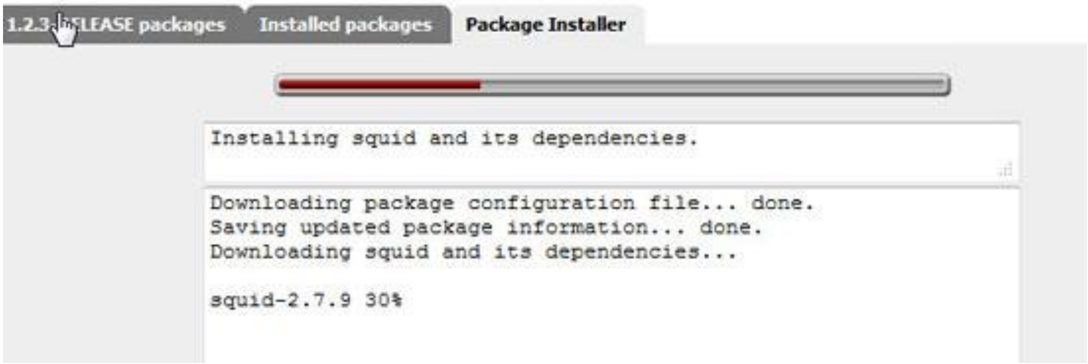
Step One: Install Squid Proxy Server Package

To install squid proxy server, the packages tab was selected under the System menu item after successful login to the pfsense Web Administrator page. Squid was located from the drop down list and the "+" button at the far right clicked to install the package as shown in Figure 3.13. The setup was allowed to run till all post-install tasks for squid, such as creating of cache directories completed, as shown in Figure 3.14.



squid	Network	Stable 2.7.9 pkg v.4.3.1 platform: 1.2.1	No info, check the forum	High performance web proxy cache.
squid3	Network	DISCONTINUED on pfSense 1.2.x 3.1.14_0.1 platform: 1.2.1	No info, check the forum	DISCONTINUED on pfSense 1.2.x [EXPERIMENTAL! Not all directives are ported yet! High performance web proxy cache.]

Figure 3.13 Initiating the Squid Proxy Installer Package



```
Installing squid and its dependencies.
```

```
Downloading package configuration file... done.
Saving updated package information... done.
Downloading squid and its dependencies...

squid-2.7.9 30%
```

Figure 3.14 Squid Proxy Installation Progress

To ascertain that the squid proxy server was installed, the interface was refreshed and the proxy server was located under the "Services" drop down menu. The arrow in Figure 3.15 shows that the proxy server has successfully installed. The pfSense Box was then restarted.

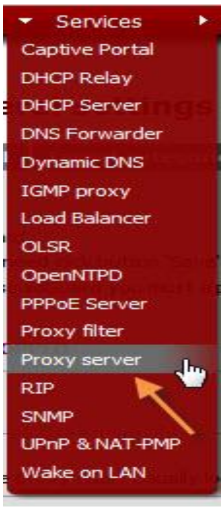
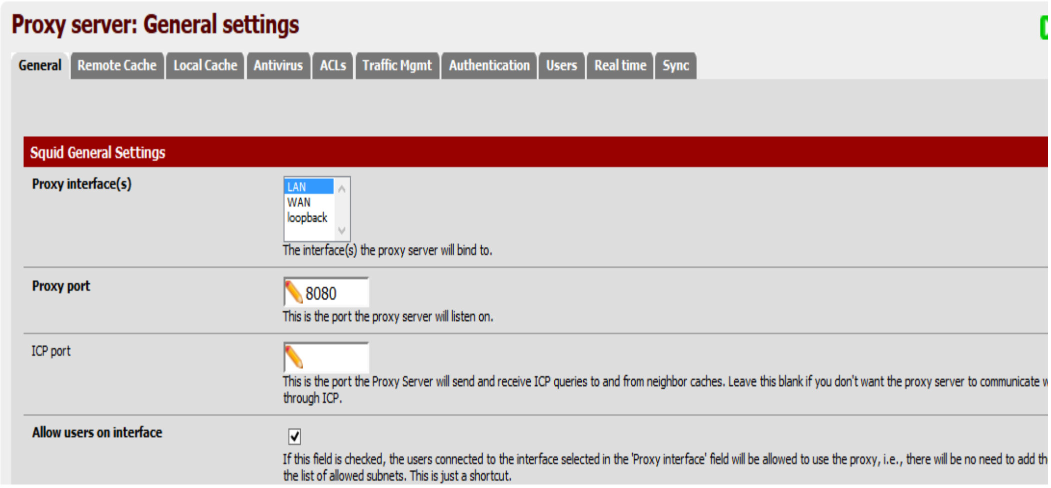


Figure 3.15 Proxy Server Successfully Installed

Step Two: Configure Squid Proxy Server

Once pfSense was restarted, the proxy setting was configured. Proxy Server was selected under the Services menu to display the general settings interface. The Proxy interface was set to "LAN" on which the squid proxy server will listen for client’s Hypertext Transfer Protocol (HTTP) requests and also interface with all firewall activities. The proxy server port was also set to 8080 to enable pfSense automatically redirect all inbound and outbound web protocols through the proxy server as shown in Figure 3.16.



Proxy server: General settings

Squid General Settings

Proxy interface(s): LAN / WAN / loopback
The interface(s) the proxy server will bind to.

Proxy port: 8080
This is the port the proxy server will listen on.

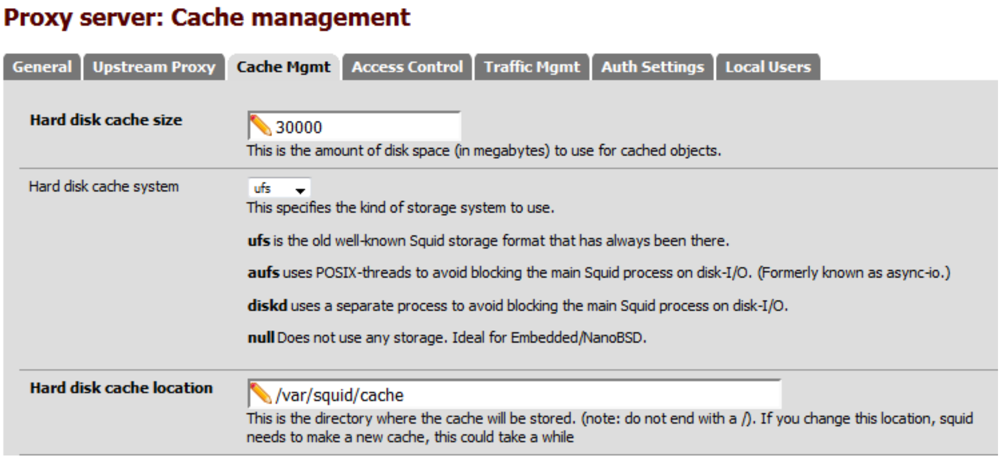
ICP port:
This is the port the Proxy Server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate w through ICP.

Allow users on interface ☑
If this field is checked, the users connected to the interface selected in the 'Proxy interface' field will be allowed to use the proxy, i.e., there will be no need to add th the list of allowed subnets. This is just a shortcut.

Figure 3.16 Proxy Server Configuration

Step Three: Hard Disk Cache Size Configuration

The hard disk cache size was configured next. By default the cache size is set to 100 MB, but considering the current university population and future growth in student enrolment, the cache size was increased to 30 000 MB. However, it is always important to consider the amount of hard disk space on the server machine before making allocations for the cache size. This is because the more web traffic going through the proxy server, the more space allocation is needed. The location where all cached transaction logs of objects will be stored was also specified as home/var/squid/cache as shown in Figure 3.17.



Proxy server: Cache management

Hard disk cache size: 30000
This is the amount of disk space (in megabytes) to use for cached objects.

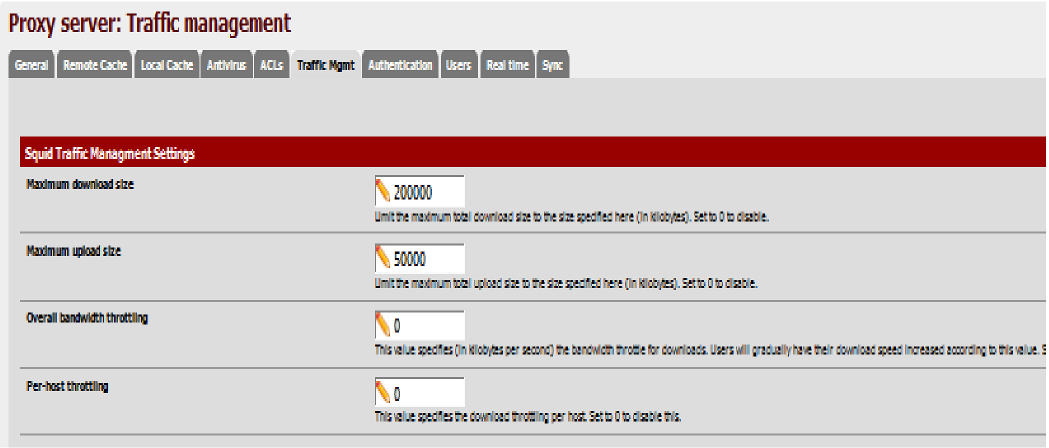
Hard disk cache system: ufs
This specifies the kind of storage system to use.
ufs is the old well-known Squid storage format that has always been there.
aufs uses POSIX-threads to avoid blocking the main Squid process on disk-I/O. (Formerly known as async-io.)
diskd uses a separate process to avoid blocking the main Squid process on disk-I/O.
null Does not use any storage. Ideal for Embedded/NanoBSD.

Hard disk cache location: /var/squid/cache
This is the directory where the cache will be stored. (note: do not end with a /). If you change this location, squid needs to make a new cache, this could take a while

Figure 3.17 Hard Disk Cache Size Configuration

Step Four: Traffic Management Configuration

It was very important to manage user activity on the network. For this, speed limits were also set with regards to how users can quickly gain access to the internet. Maximum download size was set to 200 000 kilobytes whilst maximum upload size was set to 50 000 kilobytes as displayed in Figure 3.18.



Proxy server: Traffic management

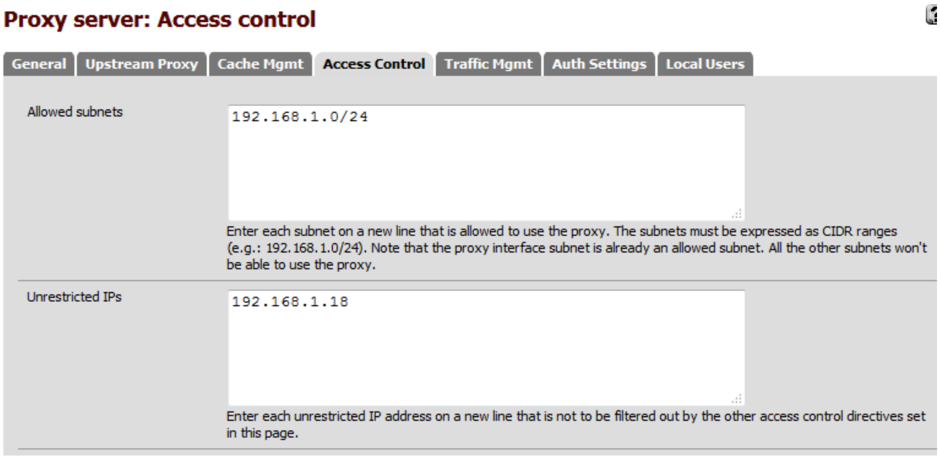
Squid Traffic Managment Settings

Maximum download size	200000 Limit the maximum total download size to the size specified here (in kilobytes). Set to 0 to disable.
Maximum upload size	50000 Limit the maximum total upload size to the size specified here (in kilobytes). Set to 0 to disable.
Overall bandwidth throttling	0 This value specifies (in kilobytes per second) the bandwidth throttle for downloads. Users will gradually have their download speed increased according to this value. S
Per-host throttling	0 This value specifies the download throttling per host. Set to 0 to disable this.

Figure 3.18 Proxy Server Taffic Management

Step Five: Access Control Lists (ACLs) Configuration

Access control rules were then defined to manage user behavior in addition to what users can or cannot do on the network. The ACLs were configured by specifying the allowed subnets on the UMaT domain 192.168.1.0/24 as shown in Figure 3.19. Each ACL describes a particular type of activity, which includes access time, source network or destination network. These activities are then matched up with the http_access statement which tells Squid whether to allow or deny the traffic that matches the defined ACL. If it finds a match, it then enforces either the allow or deny statement to the request and stops reading further.



Proxy server: Access control

Allowed subnets: 192.168.1.0/24

Enter each subnet on a new line that is allowed to use the proxy. The subnets must be expressed as CIDR ranges (e.g.: 192.168.1.0/24). Note that the proxy interface subnet is already an allowed subnet. All the other subnets won't be able to use the proxy.

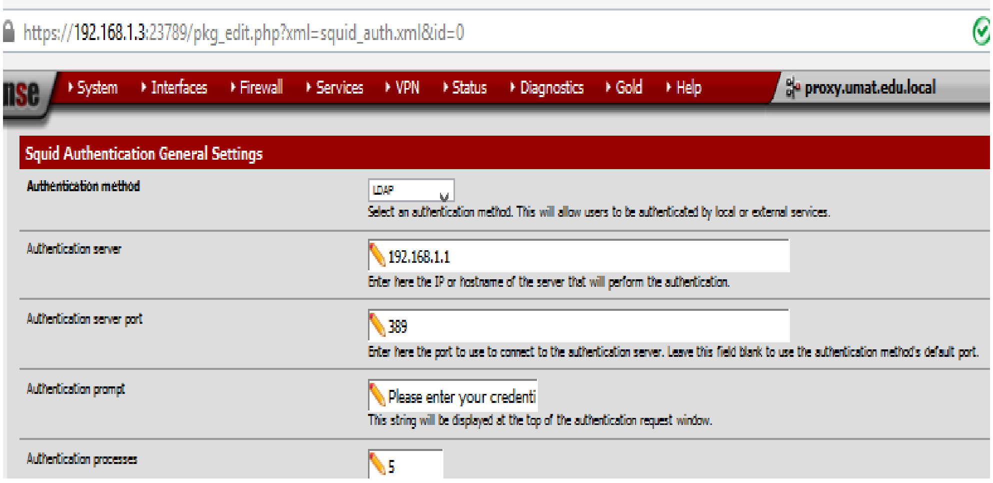
Unrestricted IPs: 192.168.1.18

Enter each unrestricted IP address on a new line that is not to be filtered out by the other access control directives set in this page.

Figure 3.19 Access Control List Configuration

Step Five: Configure Authentication

The squid authentication page was configured by defining the IP address and port number of the authentication server as 192.168.1.1 and 389 respectively as shown in Figure 3.20. In this case, the authentication server is a windows 2008 server with an active directory service that holds the full list of usernames and passwords of all users in the UMaT domain and interconnects with the DHCP server. User authentication provides a good way to manage users on the network.



https://192.168.1.3:23789/pkg_edit.php?xml=squid_auth.xml&id=0

Squid Authentication General Settings

Authentication method: LDAP

Select an authentication method. This will allow users to be authenticated by local or external services.

Authentication server: 192.168.1.1

Enter here the IP or hostname of the server that will perform the authentication.

Authentication server port: 389

Enter here the port to use to connect to the authentication server. Leave this field blank to use the authentication method's default port.

Authentication prompt: Please enter your credenti

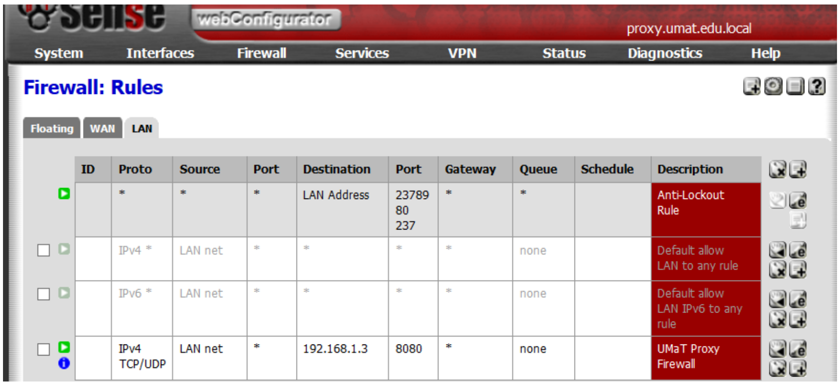
This string will be displayed at the top of the authentication request window.

Authentication processes: 5

Figure 3.20 Squid Authentication Configuration

Step Six: Firewall Rules Configuration

The final step of the Squid proxy server configuration was to define the firewall rules to force all inbound and outbound network traffic through the squid proxy server on the destination LAN interface with the static IP address 192.168.1.3 and port number 8080. The firewall rules were then managed by selecting Firewall → Rules tab, where the edit firewall rule dialog box prompted for the configuration of the firewall rules as shown in Figure 3.21. The rule was then configured on the LAN interface with the static IP address 192.168.1.3. All protocols must match the firewall rule before access can be granted on to the network.



Firewall: Rules

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		*	*	*	LAN Address	23789 80 237	*	*		Anti-Lockout Rule
□		IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule
□		IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule
□		IPv4 TCP/UDP	LAN net	*	192.168.1.3	8080	*	none		UMaT Proxy Firewall

Figure 3.21 Firewall Rule Configuration

3.6 SquidGuard

According to Haland (1998), SquidGuard is a Uniform Resource Locator (URL) redirector software used to control web contents accessed by users. It is integrated into a working squid environment to implement blacklist rules and content control over the proxy server by defining sites for which access maybe redirected or restricted. It enables the definition of multiple access rules with different levels of restrictions for different user groups on a squid cache in a particular domain. It is installed on a Unix or GNU/Linux server computer and extends its filtering capabilities to all computers in an organization, including Windows and Macintosh computers.

SquidGuard can be used for:

i. Limiting web access for some users to a list of accepted/well known web servers;

ii. Denying access to some listed or blacklisted web servers;

iii. Enforcing the use of domain names in URLs;

iv. Redirecting blocked URLs to an information page;

v. Enforcing different access rules based on time of day, day of the week, date and so on; and

vi. Classify access to the internet based on laid down user group privileges.

3.6.1 Steps involved in squidGuard Installation

Step One: Configuring Proxy Filter

The squidGuard was configured next after setting up the Squid proxy server. Proxy filter tab was located on the drop down list under the Services menu as shown in Figure 3.22. A dialog box was presented after proxy filter was clicked. The 3 boxes "Enable", "Enable GUI Log" and "Enable Log" were clicked to make sure the Squidguard service was actually STARTED as illustrated in Figure 3.23.

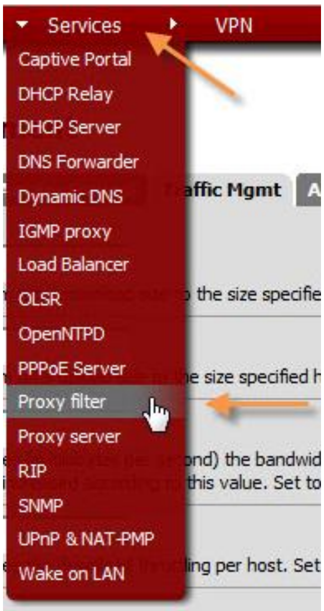
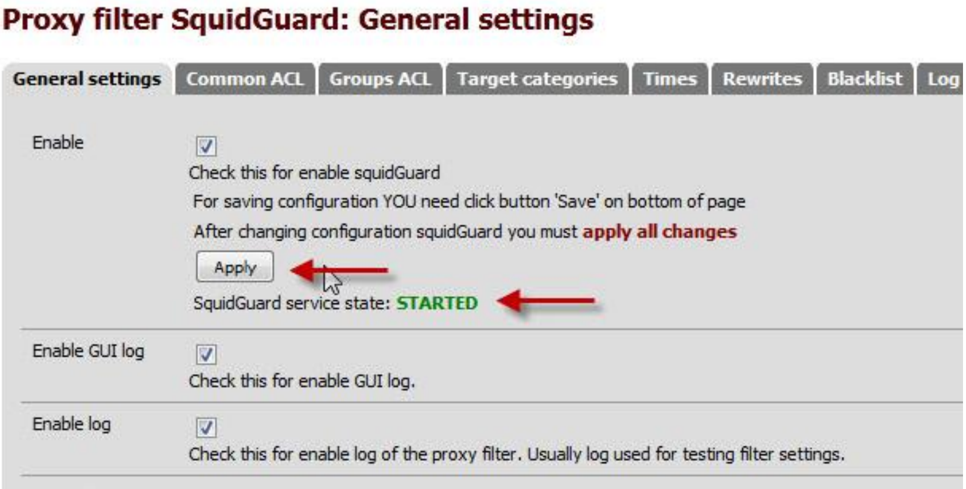


Figure 3.22 Proxy Filter



Proxy filter SquidGuard: General settings

Enable ☑
Check this for enable squidGuard
For saving configuration YOU need click button 'Save' on bottom of page
After changing configuration squidGuard you must **apply all changes**
SquidGuard service state: **STARTED**

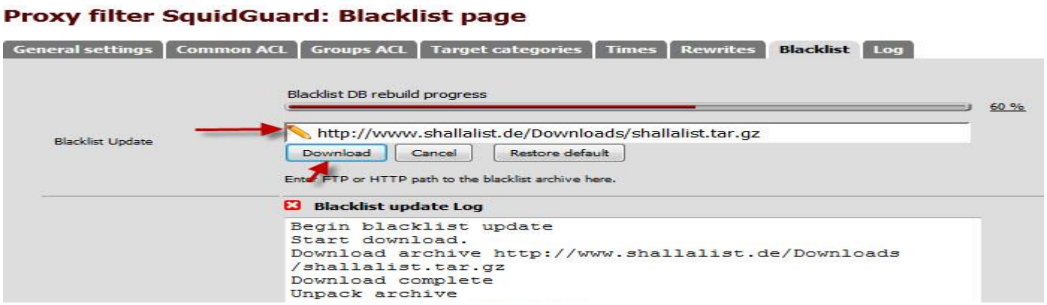
Enable GUI log ☑
Check this for enable GUI log.

Enable log ☑
Check this for enable log of the proxy filter. Usually log used for testing filter settings.

Figure 3.23 Configuring Proxy Filter

Step Two: Download Blacklist Data

The next phase of the setup was to download blacklist data as shown in Figure 3.24. The URL http://www.shallalist.de-/Downloads/shallalist.tar.gz, was typed in the blacklist URL bar. The same URL was added to the Blacklist Update Address bar to download a full list of URL’s that has to be blocked. The SquidGuard was then enabled and the changes applied. The download was then allowed to finish.



Proxy filter SquidGuard: Blacklist page

Blacklist DB rebuild progress 60 %

Blacklist Update http://www.shallalist.de/Downloads/shallalist.tar.gz

Ent FTP or HTTP path to the blacklist archive here.

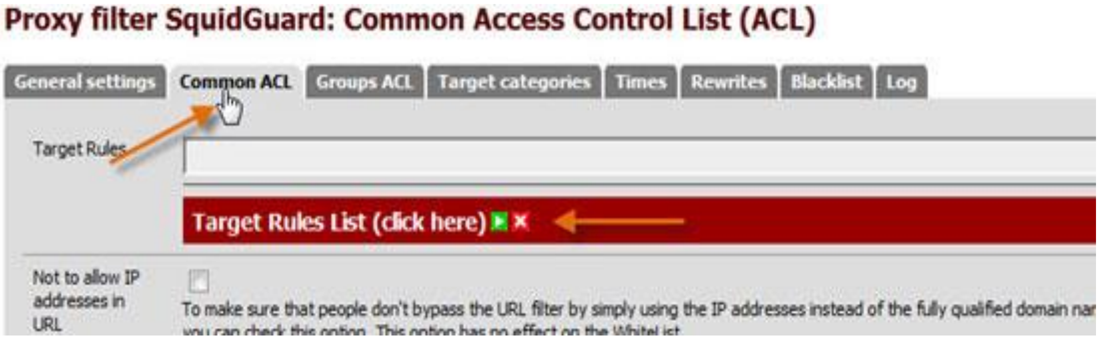
Blacklist update Log

```
Begin blacklist update
Start download.
Download archive http://www.shallalist.de/Downloads
/shallalist.tar.gz
Download complete
Unpack archive
```

Figure 3.24 Blacklist Data Download in Progress

Step Three: Configure Common ACLs

After downloading the blacklist data, the access control rules were defined. By default, all the blacklist categories were set to default. Next, the Target Rules List was selected under the common ACL tab where the appropriate rules (therefore allowed, denied or whitelisted) were defined as shown in Figures 3.25 and 3.26 respectively. Group ACLs were defined under the following categories Students, Lecturers, University Administrators and Visitors.



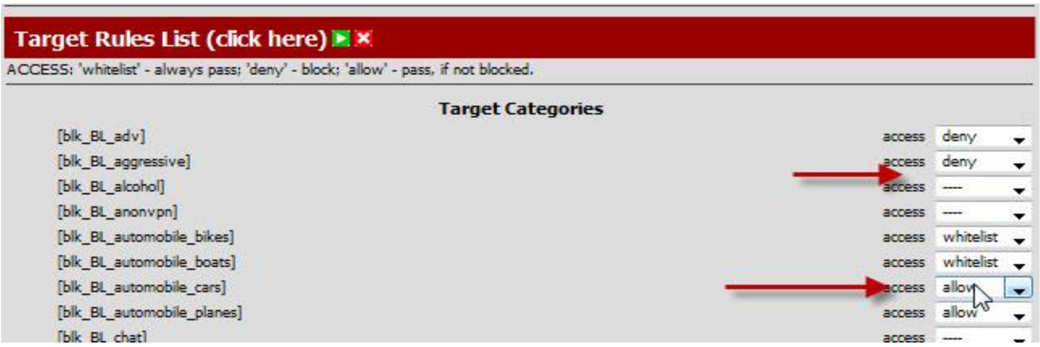
Proxy filter SquidGuard: Common Access Control List (ACL)

Target Rules

Not to allow IP addresses in URL □

To make sure that people don't bypass the URL filter by simply using the IP addresses instead of the fully qualified domain nar
you can check this option. This option has no effect on the Whitelist.

Figure 3.25 Access Control Lists Configuration



Target Rules List (click here)

ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.

Target Categories

[blk_BL_adv]	access	deny
[blk_BL_aggressive]	access	deny
[blk_BL_alcohol]	access	----
[blk_BL_anonvpn]	access	----
[blk_BL_automobile_bikes]	access	whitelist
[blk_BL_automobile_boats]	access	whitelist
[blk_BL_automobile_cars]	access	allow
[blk_BL_automobile_planes]	access	allow
[blk_BL_chat]	access	----

Figure 3.26 Target Rules List

The ***Access Control Lists*** (ACLs) were then implemented and the squidGuard service restarted and tested to ascertain that all the defined protocols were working well.

3.7 Squid Analysis Resource Generator (SARG)

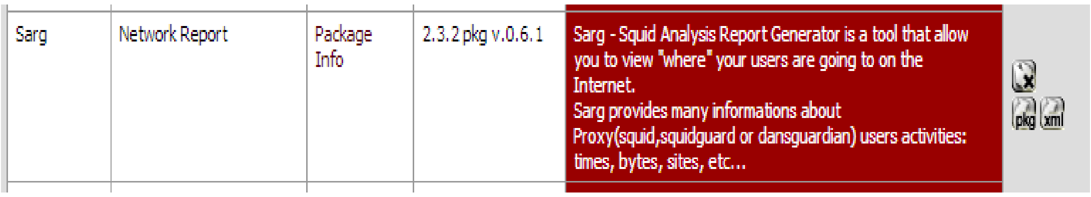
According to Ravi (2015), Squid Analysis Report Generator (SARG) is an open source squid proxy log analysis tool for linux which provides web based log file analysis and generates beautiful reports in HTML format with information about users, IP addresses, top accessed sites, total bandwidth usage, elapsed time, downloads, access denied websites, daily, weekly and monthly reports.

SARG is further described as a very handy tool used to view how much internet bandwidth is utilized by individual machines on a particular network and also provide detailed statistics on where and what network users are doing on the network. It is an additional package on the squid proxy server and can be installed on RHEL/CentOS/Fedora and Debian/Ubuntu/Linux Mint systems.

3.7.1 Steps Involved in SARG Installation

Step One: Install SARG

To begin the SARG installation, the pfsense's Web Administrator page was accessed and packages tab was clicked under System menu item. SARG was located from the drop down menu and the "+" button at the far right clicked to install the package as shown in Figure 3.27. The setup was allowed to run till the installation was completed. SARG reports was then located under the Status menu.



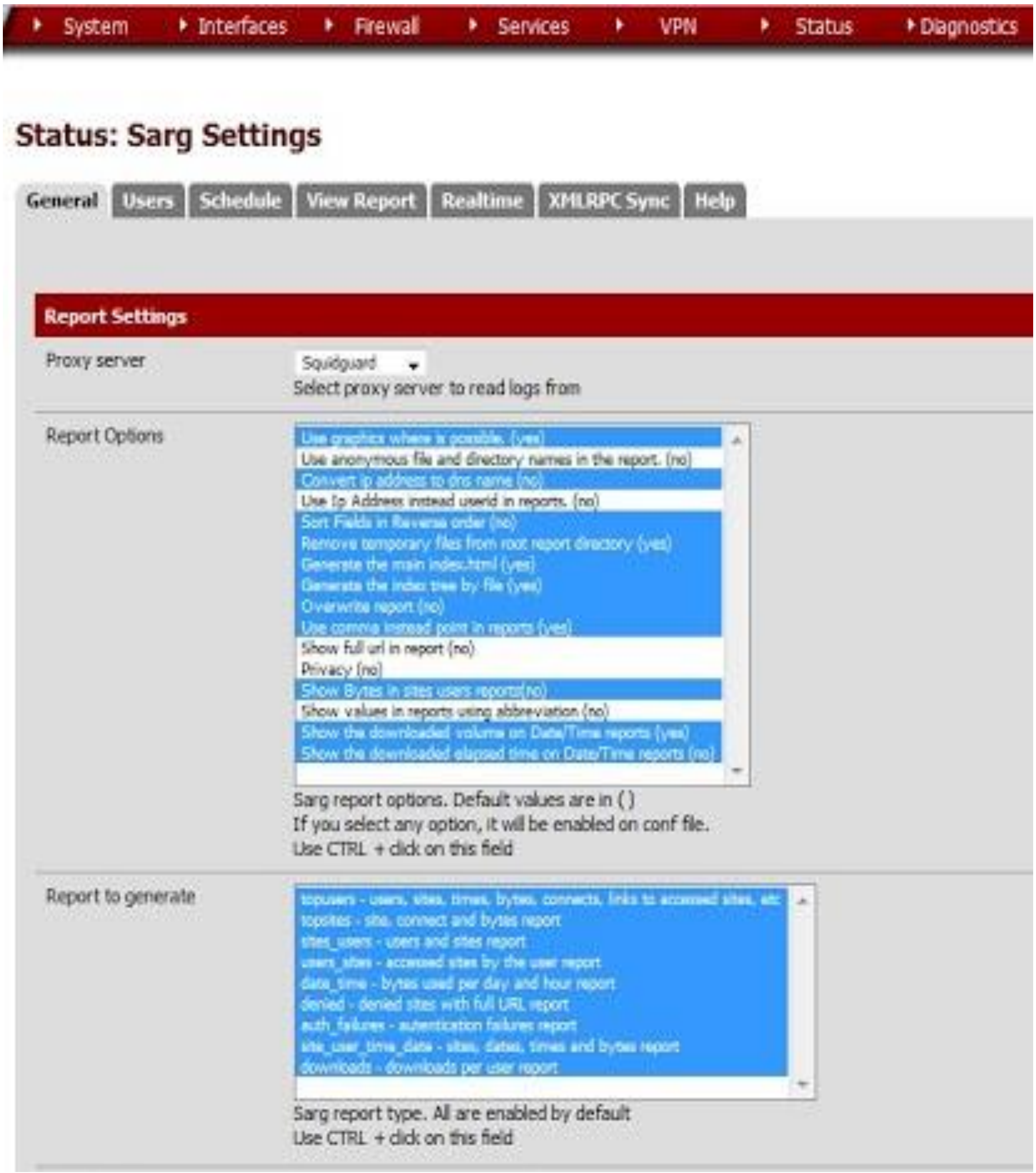
Sarg	Network Report	Package Info	2.3.2 pkg v.0.6.1	Sarg - Squid Analysis Report Generator is a tool that allow you to view "where" your users are going to on the Internet. Sarg provides many informations about Proxy(squid,squidguard or dansguardian) users activities: times, bytes, sites, etc...

Figure 3.27 Initiating the SARG Installation Process

Step Two: Configure SARG General Settings

The general SARG area was made up of other tabs that were used to configure into details the general reporting options and other report types as shown in Figure 3.28. The Users tab was the location set for user information. Since UMaT uses Squid as the main proxy server, specific usernames rather than IP addresses were used. With this, aliases were set for each username on the network under user association.

The frequency of how reports were generated was defined on the schedule tab. In this case, reports were scheduled to be generated every 4 hours as shown in Figure 3.29. The View Report Tab was configured to enable the viewing of all generated reports. The Realtime Tab reveals all active connections on the LAN at specific time intervals.



Status: Sarg Settings

Report Settings

Proxy server: Squidguard

Select proxy server to read logs from

Report Options:

- Use graphics where is possible. (yes)
- Use anonymous file and directory names in the report. (no)
- Convert ip address to dns name (no)
- Use Ip Address instead userid in reports. (no)
- Sort Fields in Reverse order (no)
- Remove temporary files from root report directory (yes)
- Generate the main index.html (yes)
- Generate the index tree by file (yes)
- Overwrite report (no)
- Use comma instead point in reports (yes)
- Show full url in report (no)
- Privacy (no)
- Show Bytes in sites users reports(no)
- Show values in reports using abbreviation (no)
- Show the downloaded volume on Date/Time reports (yes)
- Show the downloaded elapsed time on Date/Time reports (no)

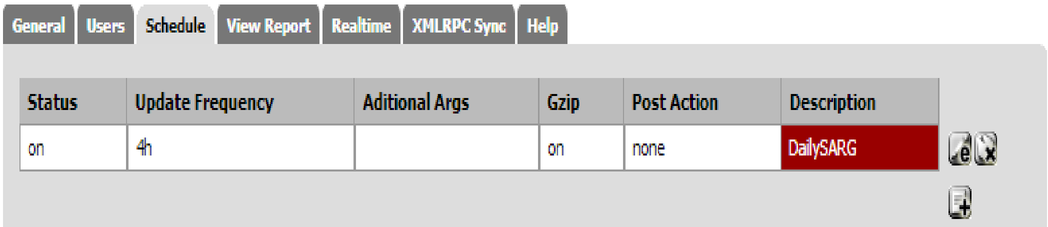
Sarg report options. Default values are in ( )
If you select any option, it will be enabled on conf file.
Use CTRL + click on this field

Report to generate:

- topusers - users, sites, times, bytes, connects, links to accessed sites, etc
- topsites - site, connect and bytes report
- sites_users - users and sites report
- users_sites - accessed sites by the user report
- date_time - bytes used per day and hour report
- denied - denied sites with full URL report
- auth_failures - autentication failures report
- site_user_time_date - sites, dates, times and bytes report
- downloads - downloads per user report

Sarg report type. All are enabled by default
Use CTRL + click on this field

Figure 3.28 SARG General Settings



Status	Update Frequency	Aditional Args	Gzip	Post Action	Description
on	4h		on	none	DailySARG

Figure 3.29 SARG Report Scheduler

3.8 Active Directory

Anon. (1990) describes Active Directory (AD) to be a special-purpose database directory service developed by Microsoft for windows domain networks to handle large amounts of read and search operations. An AD domain controller is used for authenticating and authorizing all users and computing devices in a Windows domain network by assigning and enforcing security policies for all computing devices. For example, when a user logs into a computing device which is part of a Windows domain, the AD checks the submitted credentials and matches it with what exists in its database thus to determine whether the user is indeed part of that domain. This service is included in most Windows Server operating systems.

3.8.1 Stakeholders of the UMaT Internet Community

To achieve the objectives of this thesis, there was a need to clearly define the stakeholders who make up the UMaT internet community. They include students, lecturers, administrative staff and guests. To effectively setup a comprehensive user access group policy, organizational units were created for each stakeholder to hold defined objects of interest. In this case, the objects were user credentials of users in the UMaT domain. The following are categories of users:

i. **Students.** The students make up the majority stakeholder in the UMaT community. The current population is over 2300. They consist of undergraduate and postgraduate students.

ii. **Lecturers.** The lecturers make up the academic staff within the community. They are categorized into Senior Professors, Associate Professors, Senior Lecturers, Lecturers, Assistant Lecturers and Research Fellows. This group of users connects to the university network for research and collaboration purposes. They connect to the university network through wall jacks by way of straight cables in their respective offices.

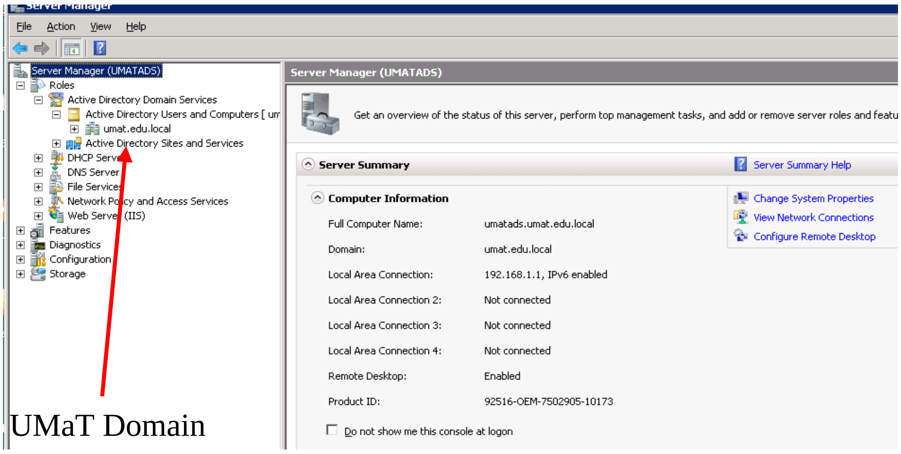
iii. **Administrative Staff.** This category is made up of the administrative staff of the University. They oversee the day to day operations within the university community. They also include national service personnel.

iv. **Guests.** This category is made up of visitors or people who work for the university and require short-term access to the university network to perform general activities.

3.8.2 Steps Involved in Creating Organizational Units

Step One: Open Server Manager Console

The first step was to open the Server Manager dialog box and expand the Roles section on the left pane of the dialog. The next was to expand the Active Directory Domain Services section to locate and click on Active Directory Users and Computers as shown in Figure 3.30. At this point, the domain umat.edu.local was located and the Organizational Units (OUs) were created for all the stakeholders.



Get an overview of the status of this server, perform top management tasks, and add or remove server roles and featu

Full Computer Name: umatads.umat.edu.local

Domain: umat.edu.local

Local Area Connection: 192.168.1.1, IPv6 enabled

Local Area Connection 2: Not connected

Local Area Connection 3: Not connected

Local Area Connection 4: Not connected

Remote Desktop: Enabled

Product ID: 92516-OEM-7502905-10173

□ Do not show me this console at logon

Figure 3.30 Server Manager Dialog Box

Step Two: Creating the OU for Student

The student OU was created by right-clicking on the domain name and pointing to the New option and selecting Organizational Unit. The name of the OU was specified and the check box Protect container from accidental deletion checked. The OU was created when the OK button was clicked as depicted in Figure 3.31 and 3.32 respectively. The same steps were repeated to create the OUs for the three remaining stakeholders as shown in Figure 3.33. Two other OUs were created in the Student OU and named Undergraduate and Postgraduate.

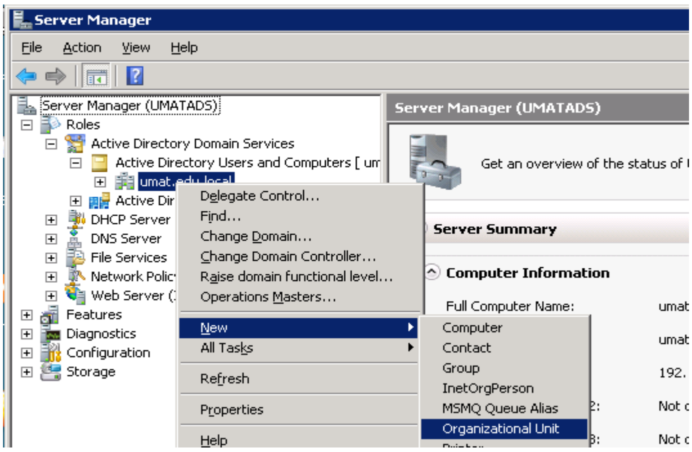
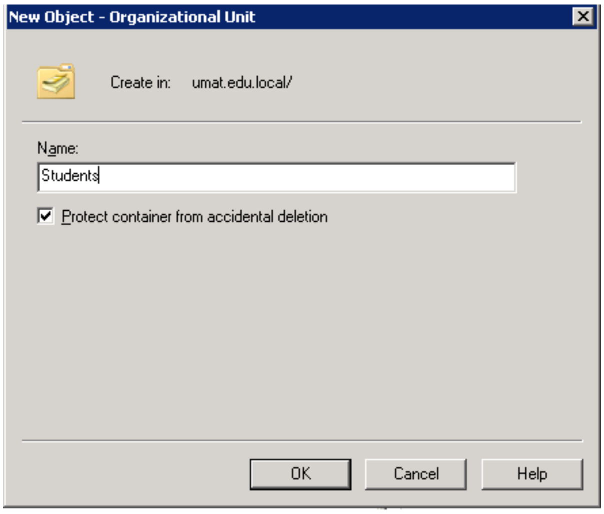


Figure 3.31 Creating the Student OU

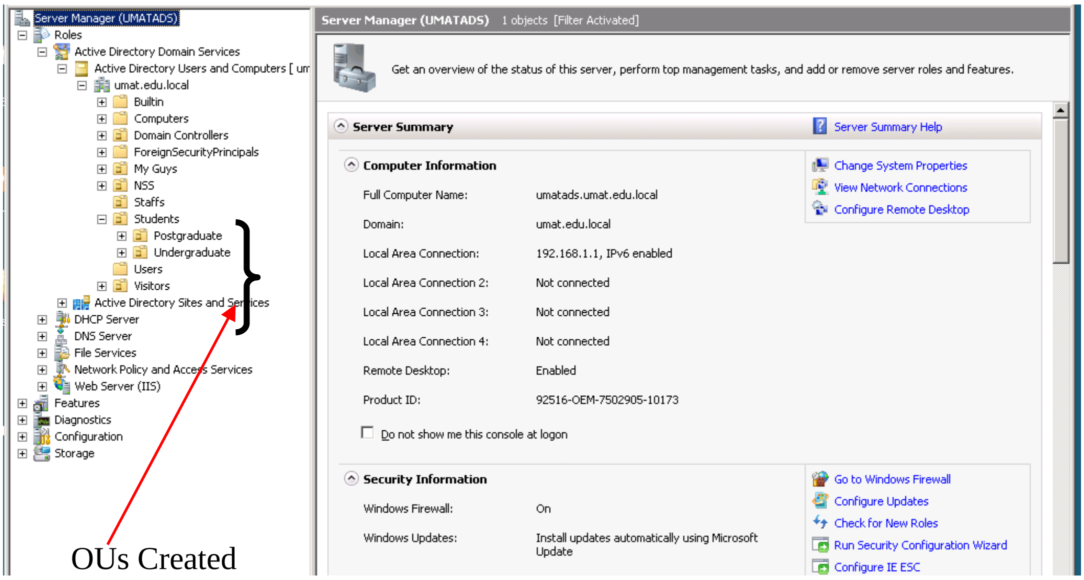

New Object - Organizational Unit

Create in: umat.edu.local/

Name:
Students

☑ Protect container from accidental deletion

Figure 3.32 Students OU Created



Server Manager (UMATADS) 1 objects [Filter Activated]

Get an overview of the status of this server, perform top management tasks, and add or remove server roles and features.

Server Summary

Computer Information

Full Computer Name: umatads.umat.edu.local

Domain: umat.edu.local

Local Area Connection: 192.168.1.1, IPv6 enabled

Local Area Connection 2: Not connected

Local Area Connection 3: Not connected

Local Area Connection 4: Not connected

Remote Desktop: Enabled

Product ID: 92516-OEM-7502905-10173

☐ Do not show me this console at logon

Security Information

Windows Firewall: On

Windows Updates: Install updates automatically using Microsoft Update

Figure 3.33 Organizational Units Created

3.8.3 Steps in Creating Staff User Credentials

After creating the OUs, the next step was to create the individuals user accounts and group them into their respective OUs.

Step One

The domain name umat.edu.local was right-clicked and the option User selected from the New drop-down menu under the Roles section as depicted in Figure 3.34. In the New Object – User dialog box, the user details, therefore, Sylvester Akpah was keyed in the fields provided as shown in Figure 3.35.

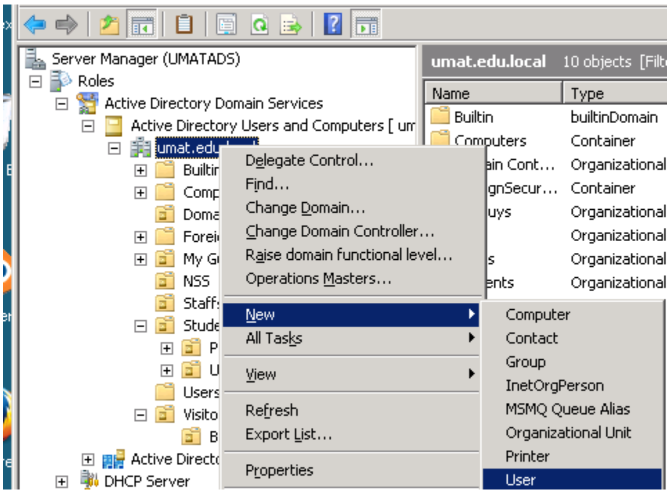
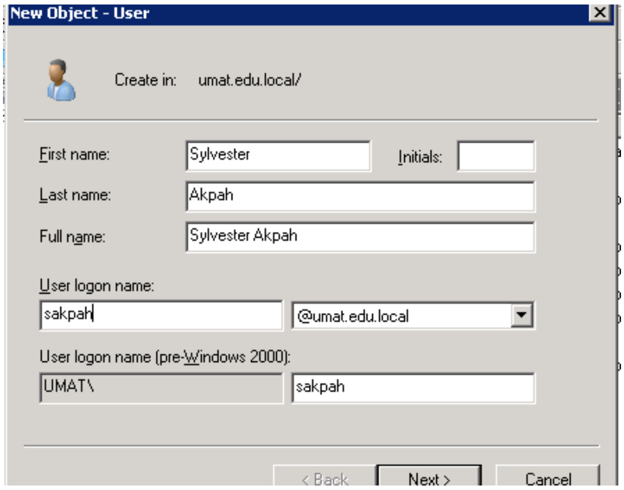


Figure 3.34 Initiating Staff User Accounts Creation Process



New Object - User

Create in: umat.edu.local/

First name: Sylvester

Initials:

Last name: Akpah

Full name: Sylvester Akpah

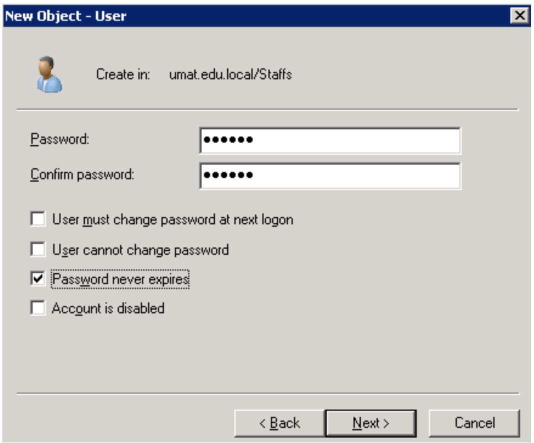
User logon name: sakpah @umat.edu.local

User logon name (pre-Windows 2000): UMAT\ sakpah

Figure 3.35 Entering User Credentials

Step Two

The user password was created next and the appropriate option selected. In this case, the third option which is Password Never Expires was selected, thus to prevent the user from been able to change the password upon logon. This option was chosen for the administrator to have absolute control over the accounts. The final step was to finish the account creation process as depicted in figure 3.36 and 3.37 respectively.



Password: ••••••

Confirm password: ••••••

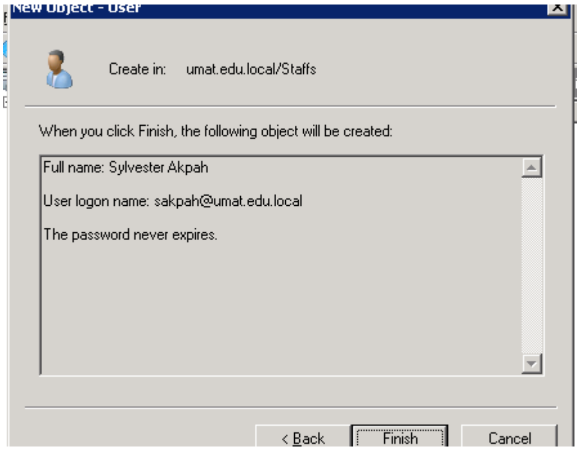
☐ User must change password at next logon

☐ User cannot change password

☑ Password never expires

☐ Account is disabled

Figure 3.36 User Password Created



When you click Finish, the following object will be created:

Full name: Sylvester Akpah

User logon name: sakpah@umat.edu.local

The password never expires.

Figure 3.37 User Account Creation Process Finished

Steps one and two were repeated to create accounts for all lecturers and staff of the University community.

3.8.4 Steps in Creating Student User Credentials

Step One

The domain name umat.edu.local was right-clicked and the option User selected from the New drop-down menu under the Roles section as depicted in Figure 3.38. In the New Object – User dialog box, the user details, therefore, Daphney Ocloo was keyed in the fields provided as shown in Figure 3.39. The student account is preceded with the department the student belongs to and ended with his/her year of entry. In this case, the student belongs to Computer Science & Engineering Department thus (ce) and ending with 14, meaning the student enrolled in the year 2014.

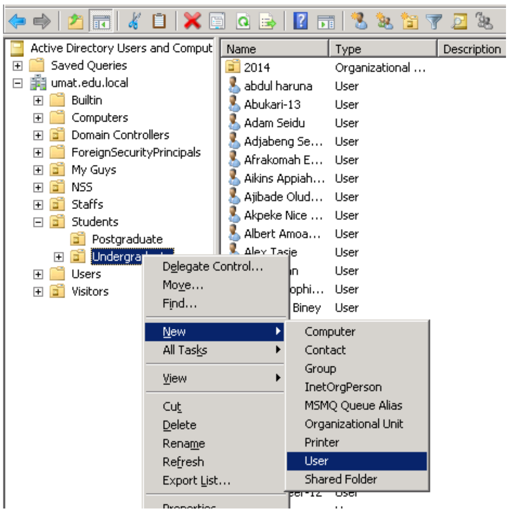
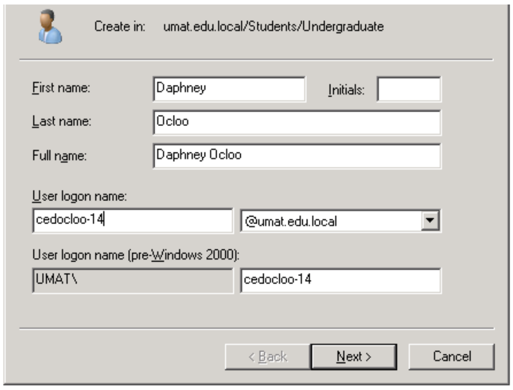


Figure 3.38 Initiating Student User Accounts Creation Process



Create in: umat.edu.local/Students/Undergraduate

First name: Daphney

Initials:

Last name: Ocloo

Full name: Daphney Ocloo

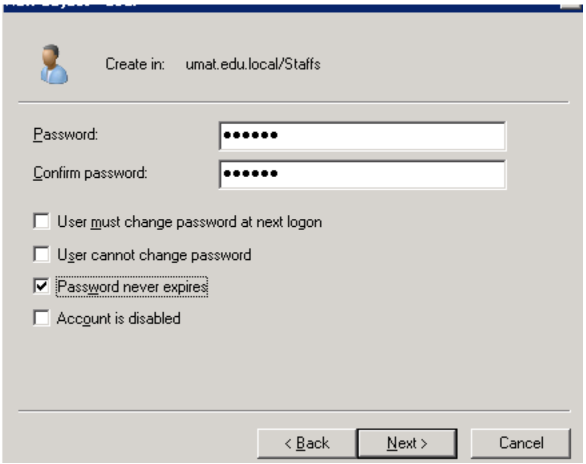
User logon name: cedocloo-14 @umat.edu.local

User logon name (pre-Windows 2000): UMAT\ cedocloo-14

Figure 3.39 Entering User Credentials

Step Two

The user password was created next and the appropriate option selected. In this case, the third option which is Password Never Expires was selected, thus to prevent the user from been able to change the password upon logon. This option was chosen for the administrator to have absolute control over the accounts. The final step was to finish the account creation process as depicted in figure 3.40 and 3.41 respectively.



Create in: umat.edu.local/Staffs

Password: ••••••

Confirm password: ••••••

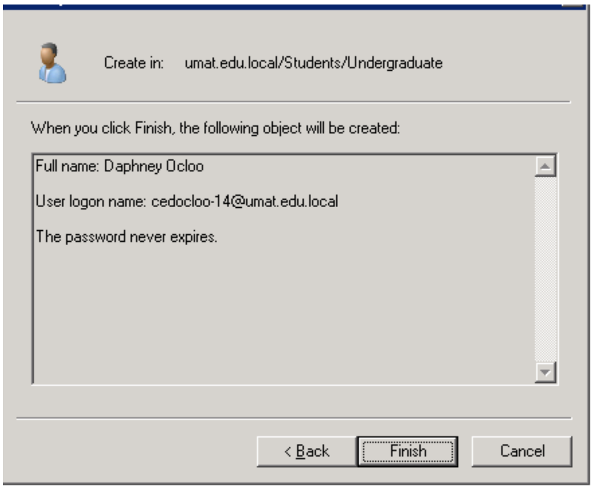
□ User must change password at next logon

□ User cannot change password

☑ Password never expires

□ Account is disabled

Figure 3.40 User Password Created



Create in: umat.edu.local/Students/Undergraduate

When you click Finish, the following object will be created:

Full name: Daphney Ocloo

User logon name: cedocloo-14@umat.edu.local

The password never expires.

Figure 3.41 User Account Creation Process Finished

Steps one and two were repeated to create accounts for all students of the University community.

CHAPTER FOUR

TESTING THE SYSTEM AND DISCUSSION OF RESULTS

This chapter presents detailed testing and evaluation of the results obtained. It further reports on the findings of the existing system as well as the new technologies employed in the current study. Finally, it presents a simulation of a secured Local Area Network architecture to palliate the security problems of the UMaT LAN.

4.1 Results of the Existing System

Prior to the installation of the squid and squidGuard on the LAN infrastructure, the existing network was managed with per user authentication. Users were assigned access credentials (username and password) that enabled them gain full access to network resources without any restrictions. Due to the relatively uncontrolled nature of the LAN, the network faced a lot of challenges that made it very insecure. Outlined are just a few of the vulnerabilities identified:

A. **Virus Attacks**

The inappropriate use of the existing bandwidth coupled with the absence of effective bandwidth management strategies promoted bandwidth wastage on unwanted traffic such as peer-to-peer file sharing and media streaming applications, uncontrolled downloads from virus infested webpages which exposed the UMaT LAN to virus attacks thereby leaving the network very insecure.

B. **Lack of Real Time Network Monitoring**

The inability to efficiently monitor in real time the behaviors patterns of users on the network caused a lot of congestion on the LAN since the activities of users couldn’t be identified and accounted for. Not being able to know who were on the network, the major consumers of the bandwidth, on what applications the bandwidth was used on created a lot of inconvenience on the network. This normally slowed down the speed of the network and also impeded the ability to use it to achieve the core purpose for which it was put in place.

C. **Higher demand compared to available bandwidth**

The annual increase in student enrolments, the increased use of electronic gadgets and the shifting trends towards the use of multimedia websites, which contain bandwidth-hungry images, video and animations posed a lot of resource and administrative challenges to the LAN on UMaT campus. The available bandwidth was generally not enough to meet the demands and support its optimal usage. This generally slowed down the speed of the LAN and places a lot of pressure on the current bandwidth.

D. **Technical Breakdowns**

The frequent breakdown of some network equipment’s hindered the transmission of network signals to users. This created a lot of inconvenience on the part of users within the University community and greatly affected communication flow between the University and the outside world.

4.2 Analysis of the Enhanced UMaT LAN

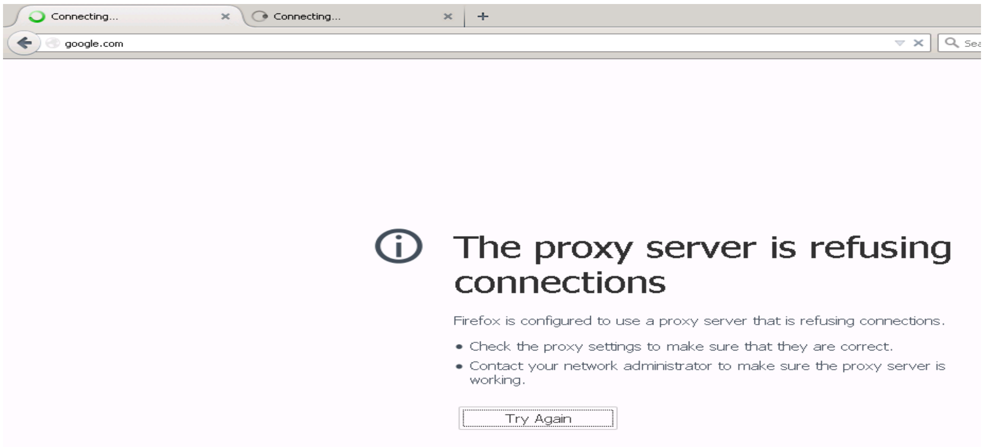
4.2.1 Results and Discussion of Squid Proxy Server

The squid proxy server is an open source web caching proxy server installed on a UNIX box through which all web traffic from client workstations connected to the

LAN are routed before gaining access to the internet. The results proved that before any client computer establishes connection with the Internet after gaining an IP address from the local DHCP server on UMaT LAN, the client machines browser software must be configured to trust the proxy server prior to authentication.

Guest User

The experiment conducted with a guest account who intended to connect to the UMaT LAN revealed that even though the client machine acquired an IP address from the local DHCP server deployed on the UMaT LAN, the user was not able to establish connection to the internet. Ideally, before a client can make any connection with the Internet after gaining IP address, the client needs to configure the Internet properties of the operating system and authenticate with the proxy server. However, in this case, with the installation of the Squid proxy server, the user failed to gain access because his/her browser software was not manually configured to point to trust the proxy server as shown in Figure 4.1.



The proxy server is refusing connections

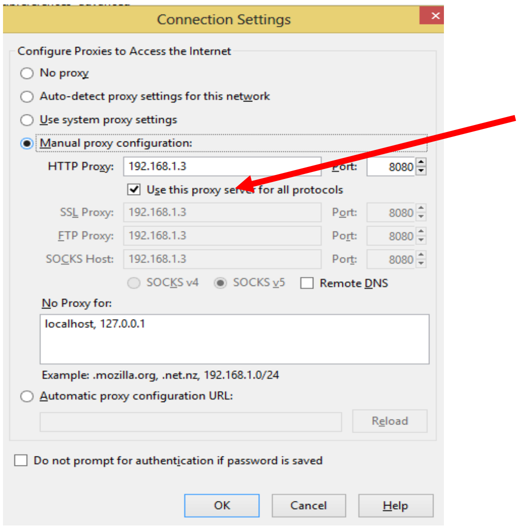
Firefox is configured to use a proxy server that is refusing connections.

- Check the proxy settings to make sure that they are correct.
- Contact your network administrator to make sure the proxy server is working.

Figure 4.1 Proxy Server Refusing Connection to the Internet

Student Account

The experiment conducted with a student account connecting to the LAN revealed that the user was able to establish connection to the internet after his/her client machine acquired an IP address from the DHCP server. The client’s browser software (i.e. Internet Explorer, Mozilla Firefox, Google chrome, etc) was manually configured to point to the proxy server deployed on the network as shown in Figure 4.2. The browser software then prompted for the credentials of the user to enable the Authentication Server (AS) cross check the submitted credentials with that contained in the Active Directory database thus to ascertain the true identity of the user prior to authentication and authorization as shown in Figure 4.3. Once the match was successful, the browser was allowed access to navigate HTTP/HTTPS requests retrieved on its behalf by the proxy server shown in Figure 4.4. All users whose browser software's were configured to explicitly configured to trust the proxy server were able to gain access to the internet. All browsers not configured to trust the proxy server were completed blocked off. Once all users are going through the proxy server, all incoming and outgoing web traffic will be efficiently managed.



Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration:

HTTP Proxy: 192.168.1.3 Port: 8080

☑ Use this proxy server for all protocols

SSL Proxy: 192.168.1.3 Port: 8080

FTP Proxy: 192.168.1.3 Port: 8080

SOCKS Host: 192.168.1.3 Port: 8080

○ SOCKS v4 ● SOCKS v5 □ Remote DNS

No Proxy for:

localhost, 127.0.0.1

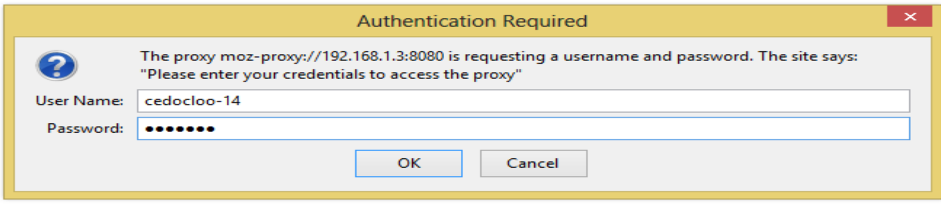
Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

□ Do not prompt for authentication if password is saved

Browser software
configured to trust
Proxy Server

Figure 4.2 Mozilla Firefox Browser Software Proxy Settings Configured

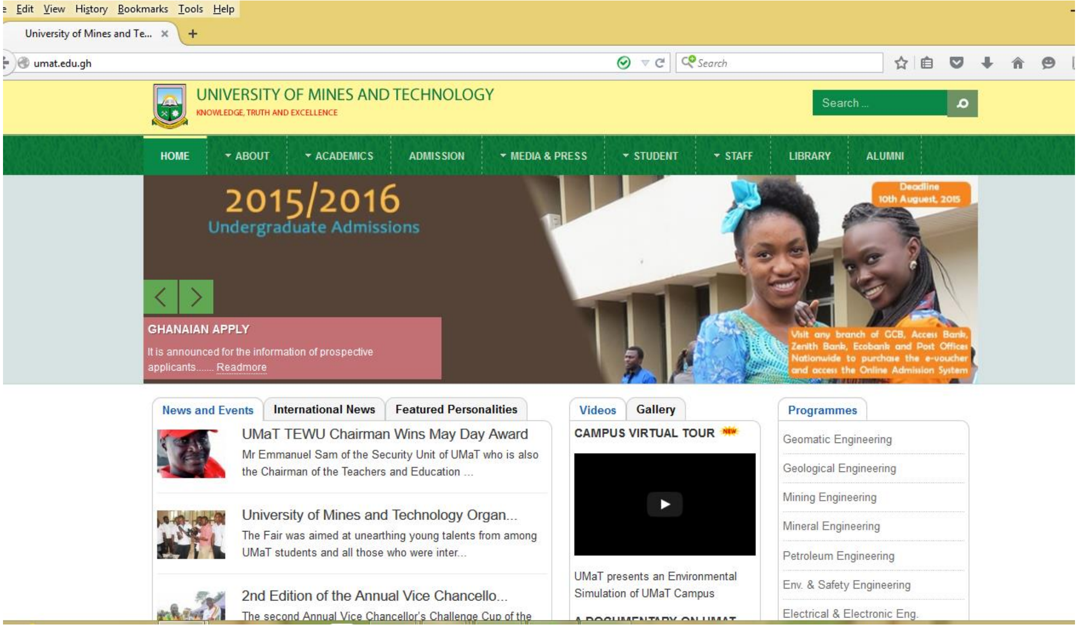


The proxy moz-proxy://192.168.1.3:8080 is requesting a username and password. The site says: "Please enter your credentials to access the proxy"

User Name: cedocloo-14

Password: ●●●●●●●

Figure 4.3 Student Credentials Entered prior to Authentication


Edit View History Bookmarks Tools Help
University of Mines and Te...
umat.edu.gh
Search
UNIVERSITY OF MINES AND TECHNOLOGY
KNOWLEDGE, TRUTH AND EXCELLENCE
Search ...
HOME
ABOUT
ACADEMICS
ADMISSION
MEDIA & PRESS
STUDENT
STAFF
LIBRARY
ALUMNI
2015/2016
Undergraduate Admissions
Deadline 10th August, 2015
Visit any branch of GCB, Access Bank, Zenith Bank, Ecobank and Post Offices Nationwide to purchase the e-voucher and access the Online Admission System
GHANAIAN APPLY
News and Events
International News
Featured Personalities
Videos
Gallery
CAMPUS VIRTUAL TOUR
Programmes
Geomatic Engineering
Geological Engineering
Mining Engineering
Mineral Engineering
Petroleum Engineering
Env. & Safety Engineering
Electrical & Electronic Eng.

It is announced for the information of prospective applicants....... Readmore

UMaT TEWU Chairman Wins May Day Award

Mr Emmanuel Sam of the Security Unit of UMaT who is also the Chairman of the Teachers and Education ...

University of Mines and Technology Organ...

The Fair was aimed at unearthing young talents from among UMaT students and all those who were inter...

2nd Edition of the Annual Vice Chancello...

The second Annual Vice Chancellor's Challenge Cup of the

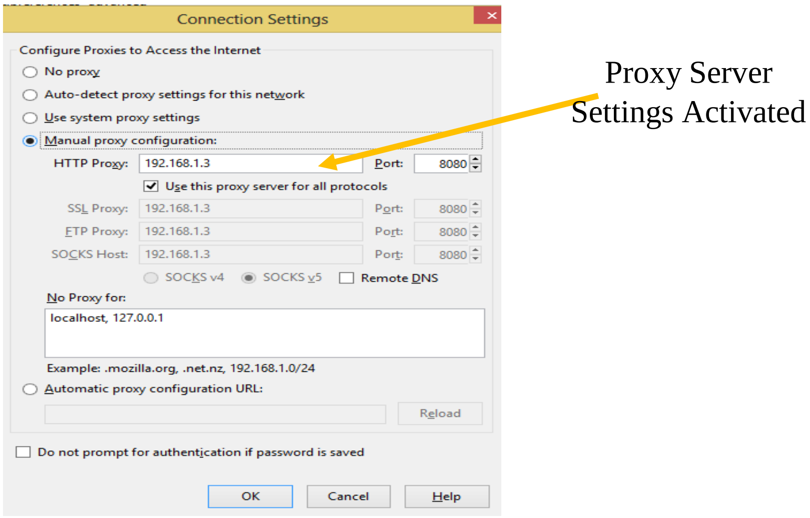
UMaT presents an Environmental Simulation of UMaT Campus

Figure 4.4 Requested HTTP Webpage Retrieved

Lecturer/Staff Account

The experiment conducted with a lecturer/staff account connected through a switch to the LAN by way of a straight cable via a wall jack revealed that the user established connection to the internet after obtaining an IP address from the DHCP server. The internet properties of the client's browser software (i.e. Internet Explorer, Mozilla Firefox, Google chrome, etc) was manually configured to point to the proxy server deployed on the network as shown in Figure 4.5. The browser software was then prompted for the credentials of the user to enable the Authentication Server (AS) cross check the submitted credentials with that contained in the Active

Directory database thus to ascertain the true identity of the user prior authentication and authorization as shown in Figure 4.6. Once the match was successful, the browser was allowed access to navigate HTTP/HTTPS requests retrieved on its behalf by the proxy server shown in Figure 4.7.



Connection Settings

Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration:

HTTP Proxy: 192.168.1.3 Port: 8080

☑ Use this proxy server for all protocols

SSL Proxy: 192.168.1.3 Port: 8080

FTP Proxy: 192.168.1.3 Port: 8080

SOCKS Host: 192.168.1.3 Port: 8080

○ SOCKS v4 ● SOCKS v5 □ Remote DNS

No Proxy for:

localhost, 127.0.0.1

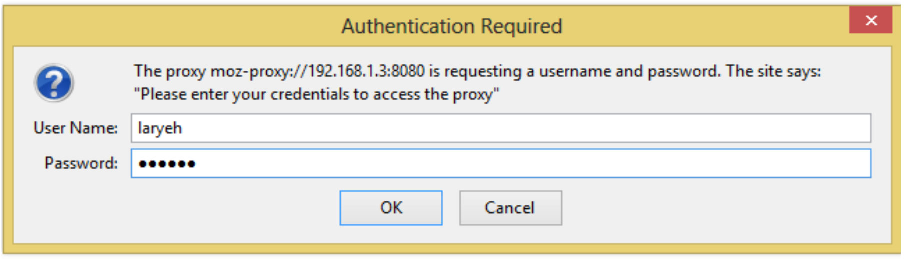
Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

□ Do not prompt for authentication if password is saved

Proxy Server Settings Activated

Figure 4.5 Mozilla Firefox Browser Proxy Settings Activated



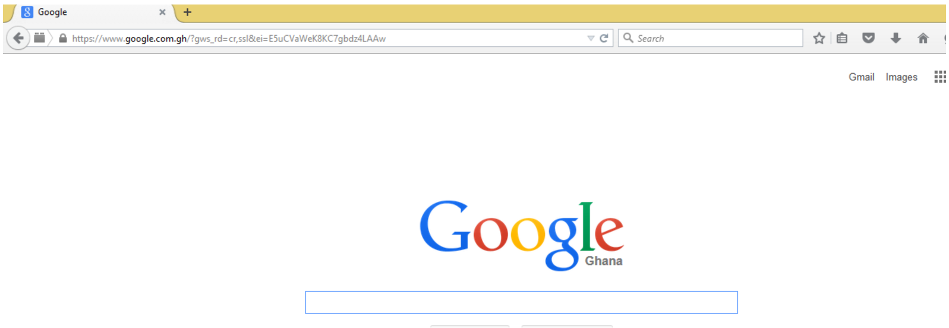
Authentication Required

The proxy moz-proxy://192.168.1.3:8080 is requesting a username and password. The site says: "Please enter your credentials to access the proxy"

User Name: laryeh

Password: ●●●●●●

Figure 4.6 Lecturer/Staff Credentials Entered prior to Authentication



https://www.google.com.gh/?gws_rd=cr,ssl&ei=E5uCVaWeK8KC7gbdz4LAAw

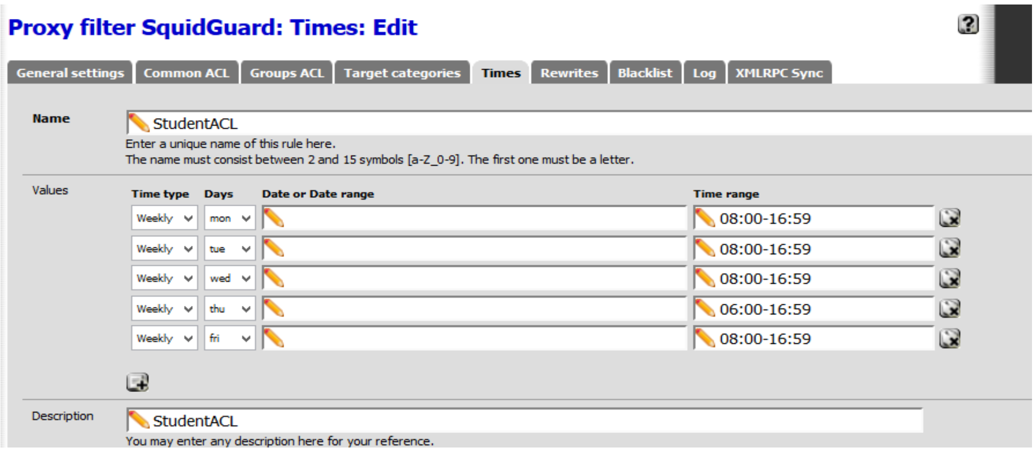
Figure 4.7 Requested HTTP Webpage Retrieved

4.2.2 Results and Discussion of SquidGuard

SquidGuard was used as a Uniform Resource Locator (URL) redirector to control web contents accessed by users. It was also used to implement blacklist rules and content control mechanisms over the proxy server to define sites for which access was deemed unworthy and thus redirected or restricted entirely.

Student/Guest Account

The experiment conducted on a student/guest account who has gained access to the LAN after acquiring an IP address from the DHCP server revealed time schedule access rules defined on the Student Access Control List Group as shown in Figure 4.8. The time schedules controlled the time periods within which students can gain access to certain websites which matches blacklisted URL addresses. Websites such as Facebook, Tumbir, Twitter, Pinterest, LinkedIn, Twoo, Google+, etc, which are deemed unworthy were redirected to the UMaT webpage during school hours from Monday to Friday between the hours of 8:00 am to 16:59 pm as shown in Figure 4.9. Students however gain full access to redirected websites from 17:00 pm to 7:59 am during week days and full access during weekends as shown in Figure 4.10. Pornographic websites, peer-to-peer file sharing software (i.e. BitTorrent, uTorrent, Tribler, Babelgum, etc), websites with aggressive and abusive contents, alcohol and drugs related contents just to mention a few were completely blacklisted. These low priority bandwidth hungry software's usually consume large portions of the bandwidth on activities which are deemed not to have much academic worth and this leaves the network hopelessly bogged down to the point where users are denied access to this valuable resource.



Name: StudentACL

Enter a unique name of this rule here.
The name must consist between 2 and 15 symbols [a-Z_0-9]. The first one must be a letter.

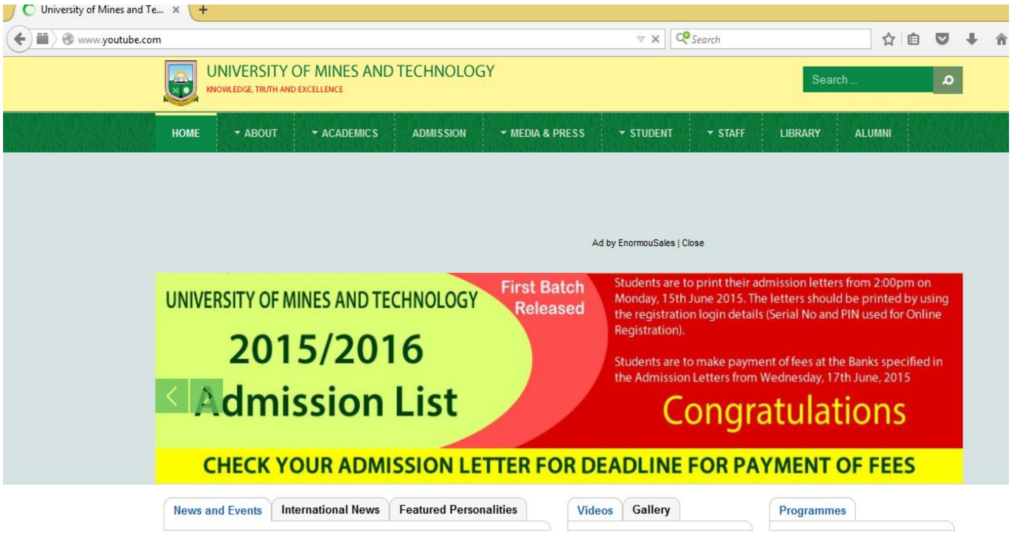
Values

Time type	Days	Date or Date range	Time range
Weekly	mon		08:00-16:59
Weekly	tue		08:00-16:59
Weekly	wed		08:00-16:59
Weekly	thu		06:00-16:59
Weekly	fri		08:00-16:59

Description: StudentACL

You may enter any description here for your reference.

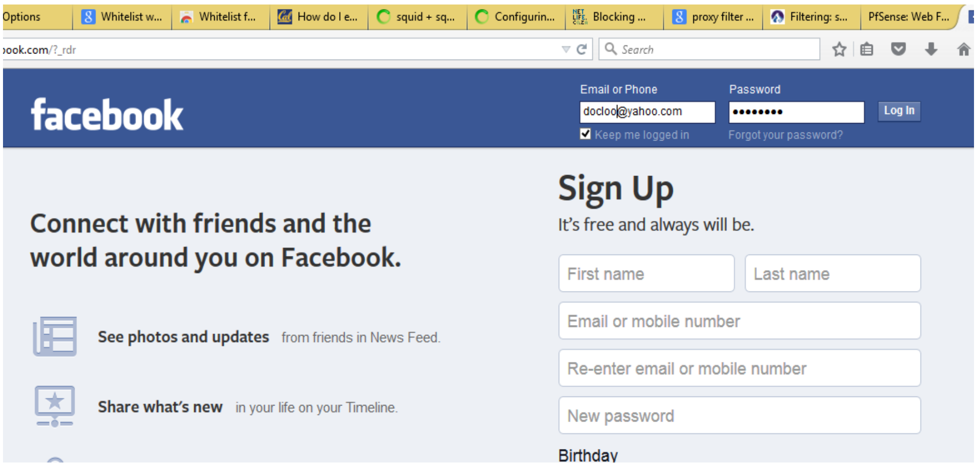
Figure 4.8 Student ACL Weekly Internet Access Time Schedule



Students are to print their admission letters from 2:00pm on Monday, 15th June 2015. The letters should be printed by using the registration login details (Serial No and PIN used for Online Registration).

Students are to make payment of fees at the Banks specified in the Admission Letters from Wednesday, 17th June, 2015

Figure 4.9 Youtube URL Redirected to the UMaT Website at 9:40am



Email or Phone: docloo@yahoo.com

Password: ••••••••

☑ Keep me logged in

Connect with friends and the world around you on Facebook.

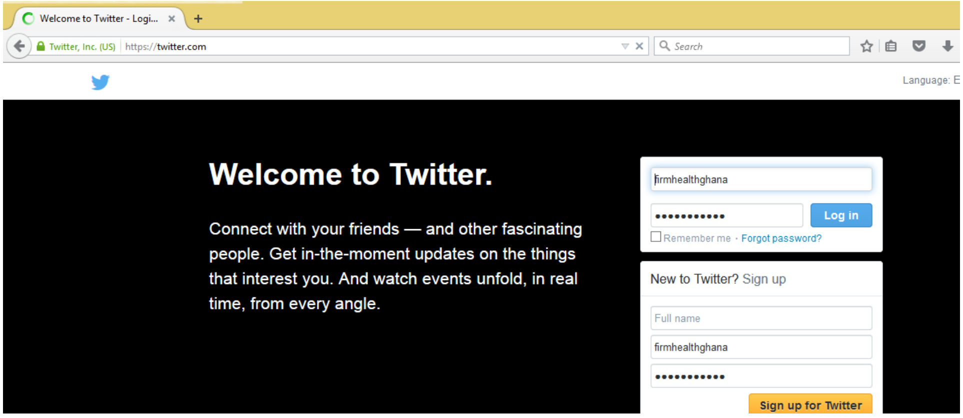
See photos and updates from friends in News Feed.

Share what's new in your life on your Timeline.

Figure 4.10 Student Gained Accessed to Facebook at 9:40pm

Lecturer/Staff Account

The experiment conducted on a lecturer/staff account which has gained access to the LAN after acquiring an IP address from the DHCP server revealed unlimited access privileges to social media webpages such as Facebook, Twitter, YouTube, Skype, Google+, Pintrest, LinkedIn, just to mention a few, whilst webpages as shown in Figure 4.11. Pornographic contents, peer-to-peer file sharing software, aggressive and abusive contents, alcohol and drugs related contents were completely redirected/ blacklisted as shown in Figure 4.12.



Welcome to Twitter.

Connect with your friends — and other fascinating people. Get in-the-moment updates on the things that interest you. And watch events unfold, in real time, from every angle.

Figure 4.11 Staff Account Gained Accessed to Twitter at 11:44am

An example of a blacklisted pornographic website redirected to the UMaT website

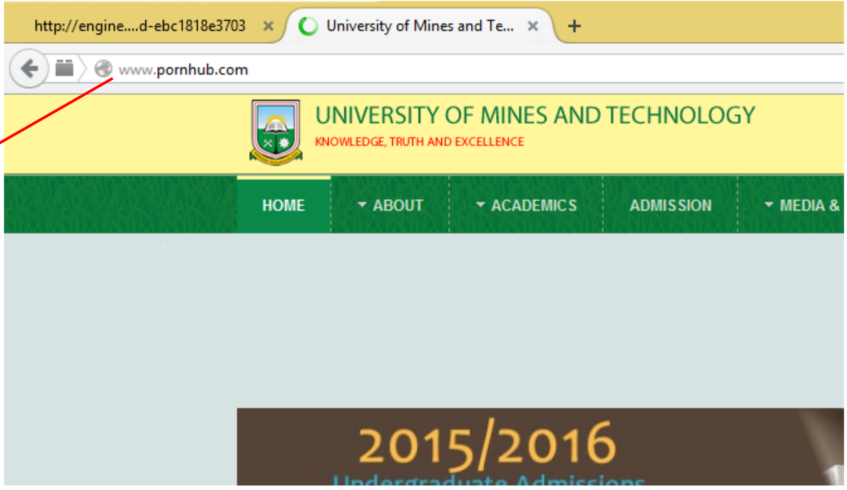
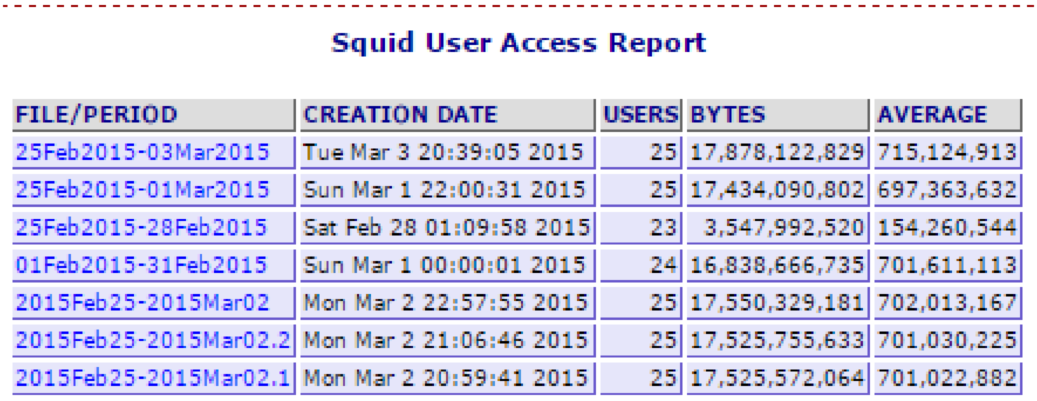

http://engine....d-ebc1818e3703
University of Mines and Te...
www.pornhub.com
UNIVERSITY OF MINES AND TECHNOLOGY
KNOWLEDGE, TRUTH AND EXCELLENCE
HOME
ABOUT
ACADEMICS
ADMISSION
MEDIA &
2015/2016
Undergraduate Admissions

Figure 4.12 Pornographic URL Redirected to the UMaT Webpage

4.2.3 Results and Discussion of Squid Analysis Report Generator (SARG)

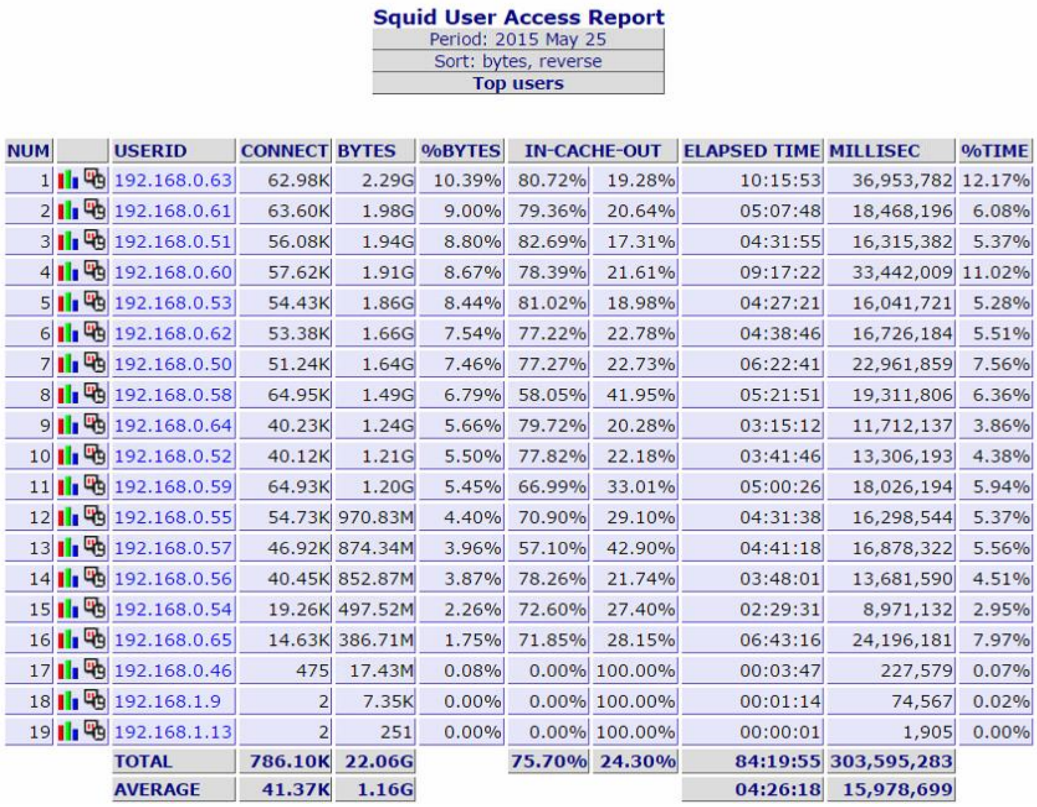
Squid Analysis Report Generator (SARG) is an open source squid proxy log analysis tool which provided web based log file analysis and report generating in HTML format based on information about users, IP addresses, top accessed sites, total bandwidth usage, elapsed time, downloads, access denied websites, etc. With the case of UMaT, SARG was implemented to track internet behavior patterns of users. Figure 4.13 depicts results of the total amount of bandwidth consumed by the top 25 users of the LAN between 25th February and 3rd March, 2015. It also shows web access logs creation dates and the periods the logs were created. Figure 4.14 also displayed the total individual bandwidth consumption rates of the top 20 users within a one hour interval on the 25th of May, 2015. Figure 4.15 also shows the various websites accessed by a particular user with the IP address 192.168.0.155. It shows the number of times the user accessed a particular website, the amount of bandwidth consumed by a particular website, the time spent accessing webpages on the website, etc. The installation of the SARG helped network administrators to clearly understand the bandwidth usage patterns of all users on the network.



Squid User Access Report

FILE/PERIOD	CREATION DATE	USERS	BYTES	AVERAGE
25Feb2015-03Mar2015	Tue Mar 3 20:39:05 2015	25	17,878,122,829	715,124,913
25Feb2015-01Mar2015	Sun Mar 1 22:00:31 2015	25	17,434,090,802	697,363,632
25Feb2015-28Feb2015	Sat Feb 28 01:09:58 2015	23	3,547,992,520	154,260,544
01Feb2015-31Feb2015	Sun Mar 1 00:00:01 2015	24	16,838,666,735	701,611,113
2015Feb25-2015Mar02	Mon Mar 2 22:57:55 2015	25	17,550,329,181	702,013,167
2015Feb25-2015Mar02.2	Mon Mar 2 21:06:46 2015	25	17,525,755,633	701,030,225
2015Feb25-2015Mar02.1	Mon Mar 2 20:59:41 2015	25	17,525,572,064	701,022,882

Figure 4.13 Squid Access Logs Created



Squid User Access Report

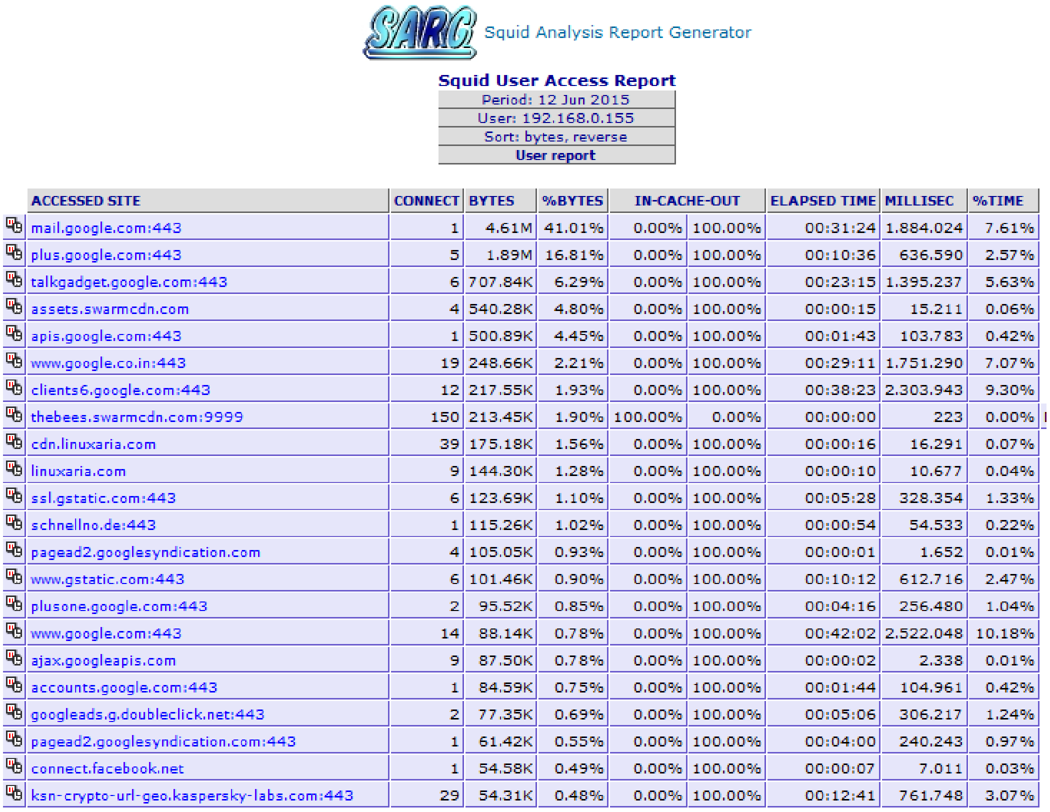
Period: 2015 May 25

Sort: bytes, reverse

Top users

NUM		USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
1		192.168.0.63	62.98K	2.29G	10.39%	80.72%	19.28%	10:15:53	36,953,782	12.17%
2		192.168.0.61	63.60K	1.98G	9.00%	79.36%	20.64%	05:07:48	18,468,196	6.08%
3		192.168.0.51	56.08K	1.94G	8.80%	82.69%	17.31%	04:31:55	16,315,382	5.37%
4		192.168.0.60	57.62K	1.91G	8.67%	78.39%	21.61%	09:17:22	33,442,009	11.02%
5		192.168.0.53	54.43K	1.86G	8.44%	81.02%	18.98%	04:27:21	16,041,721	5.28%
6		192.168.0.62	53.38K	1.66G	7.54%	77.22%	22.78%	04:38:46	16,726,184	5.51%
7		192.168.0.50	51.24K	1.64G	7.46%	77.27%	22.73%	06:22:41	22,961,859	7.56%
8		192.168.0.58	64.95K	1.49G	6.79%	58.05%	41.95%	05:21:51	19,311,806	6.36%
9		192.168.0.64	40.23K	1.24G	5.66%	79.72%	20.28%	03:15:12	11,712,137	3.86%
10		192.168.0.52	40.12K	1.21G	5.50%	77.82%	22.18%	03:41:46	13,306,193	4.38%
11		192.168.0.59	64.93K	1.20G	5.45%	66.99%	33.01%	05:00:26	18,026,194	5.94%
12		192.168.0.55	54.73K	970.83M	4.40%	70.90%	29.10%	04:31:38	16,298,544	5.37%
13		192.168.0.57	46.92K	874.34M	3.96%	57.10%	42.90%	04:41:18	16,878,322	5.56%
14		192.168.0.56	40.45K	852.87M	3.87%	78.26%	21.74%	03:48:01	13,681,590	4.51%
15		192.168.0.54	19.26K	497.52M	2.26%	72.60%	27.40%	02:29:31	8,971,132	2.95%
16		192.168.0.65	14.63K	386.71M	1.75%	71.85%	28.15%	06:43:16	24,196,181	7.97%
17		192.168.0.46	475	17.43M	0.08%	0.00%	100.00%	00:03:47	227,579	0.07%
18		192.168.1.9	2	7.35K	0.00%	0.00%	100.00%	00:01:14	74,567	0.02%
19		192.168.1.13	2	251	0.00%	0.00%	100.00%	00:00:01	1,905	0.00%
		TOTAL	786.10K	22.06G		75.70%	24.30%	84:19:55	303,595,283	
		AVERAGE	41.37K	1.16G				04:26:18	15,978,699	

Figure 4.14 Access Logs Depicting Top Users of the Bandwidth



SARC Squid Analysis Report Generator

Squid User Access Report

Period: 12 Jun 2015

User: 192.168.0.155

Sort: bytes, reverse

User report

	ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
	mail.google.com:443	1	4.61M	41.01%	0.00%	100.00%	00:31:24	1.884.024	7.61%
	plus.google.com:443	5	1.89M	16.81%	0.00%	100.00%	00:10:36	636.590	2.57%
	talkgadget.google.com:443	6	707.84K	6.29%	0.00%	100.00%	00:23:15	1.395.237	5.63%
	assets.swarmcdn.com	4	540.28K	4.80%	0.00%	100.00%	00:00:15	15.211	0.06%
	apis.google.com:443	1	500.89K	4.45%	0.00%	100.00%	00:01:43	103.783	0.42%
	www.google.co.in:443	19	248.66K	2.21%	0.00%	100.00%	00:29:11	1.751.290	7.07%
	clients6.google.com:443	12	217.55K	1.93%	0.00%	100.00%	00:38:23	2.303.943	9.30%
	thebees.swarmcdn.com:9999	150	213.45K	1.90%	100.00%	0.00%	00:00:00	223	0.00%
	cdn.linuxaria.com	39	175.18K	1.56%	0.00%	100.00%	00:00:16	16.291	0.07%
	linuxaria.com	9	144.30K	1.28%	0.00%	100.00%	00:00:10	10.677	0.04%
	ssl.gstatic.com:443	6	123.69K	1.10%	0.00%	100.00%	00:05:28	328.354	1.33%
	schnellno.de:443	1	115.26K	1.02%	0.00%	100.00%	00:00:54	54.533	0.22%
	pagead2.googlesyndication.com	4	105.05K	0.93%	0.00%	100.00%	00:00:01	1.652	0.01%
	www.gstatic.com:443	6	101.46K	0.90%	0.00%	100.00%	00:10:12	612.716	2.47%
	plusone.google.com:443	2	95.52K	0.85%	0.00%	100.00%	00:04:16	256.480	1.04%
	www.google.com:443	14	88.14K	0.78%	0.00%	100.00%	00:42:02	2.522.048	10.18%
	ajax.googleapis.com	9	87.50K	0.78%	0.00%	100.00%	00:00:02	2.338	0.01%
	accounts.google.com:443	1	84.59K	0.75%	0.00%	100.00%	00:01:44	104.961	0.42%
	googleads.g.doubleclick.net:443	2	77.35K	0.69%	0.00%	100.00%	00:05:06	306.217	1.24%
	pagead2.googlesyndication.com:443	1	61.42K	0.55%	0.00%	100.00%	00:04:00	240.243	0.97%
	connect.facebook.net	1	54.58K	0.49%	0.00%	100.00%	00:00:07	7.011	0.03%
	ksn-crypto-url-geo.kaspersky-labs.com:443	29	54.31K	0.48%	0.00%	100.00%	00:12:41	761.748	3.07%

Figure 4.15 Access Logs of a User

4.3 Proposed Solution for UMaT LAN

The assessment conducted on the existing LAN on UMaT campus spelt out the vulnerabilities in the architecture deployed. In lieu of that, a more comprehensive NAC architecture has been proposed for deployment on the campus as shown in Figure 4.16. The proposed architecture is concentrated an enhanced network access control architecture with the introduction of the 802.1X authentication to ensure that all users are identified by way of user credential verification and validation by the Active Directory Server (AD) prior to gaining full access to network resources.

The bandwidth on UMaT campus has become a strategic resource, thus its demand and overall usage continues to increase. This demand is caused by, among other things, annual increase in student enrolment, the increased use of electronic resources and the spread of desktop applications that can use practically any amount of bandwidth given to them. The bandwidth is often consumed by low priority, bandwidth hungry applications which leave the network hopelessly bogged down and prone to virus attacks from illegitimate users.

However, restricting this altogether may not be the solution since this will lead to frustration on the part of users. The core objective is to implement policies to allocate the right amount of bandwidth resources to the right set of users and critical applications in the right place at the right time on the network. In the case of UMaT, deploying a web based content filtering and monitoring policies with 802.1X authentication will be highly secure for the LAN. The reason for using 802.1X authentication is the desire for the network administrators to maintain absolute control and effectively manage all devices and users wanting to access resources on the network. To be the first line of defense, there are three parties involved in the

802.1X authentication process namely; the supplicant (the client machine), the authenticator (the switch/access point) and the authentication server (RADIUS). Primarily, the IEEE 802.1X is based on mutual authentication between supplicant and RADIUS/Authentication server. It offers a layer of defense that forces all supplicants to present user credentials for authentication prior to the creation of user sessions by the server. With the proposed solution for the UMaT LAN, there exist a Squid proxy server which sits at the heart of the Network Operating Center (NOC) and acts as a dedicated firewall through which all incoming and outgoing web traffics passes. The Active Directory server, Mail Server and DHCP Server are all configured to trust the proxy server so as to enable it filter all data packets. The Active Directory is responsible for holding all usernames and passwords of users which have been defined into two organizational units namely; staff and students. The DHCP server is responsible for the distribution IP address to all client computers on the network whilst the Mail Server is responsible for all mail correspondence within the University community.

The Active Directory (AD) is further connected to the Authentication Server (AS) to perform authentication and authorization of all user credentials. A supplicant/client (i.e. student, staff, lecturer or guest) who requires access to join the network after receiving an IP address from the DHCP server will be required to have his/her browser software configured to explicitly point to the squid proxy server deployed on the network. When a user tries to navigate to a web site, the browser will send the request to the proxy server, asking it to retrieve the requested page on its behalf.

The proxy server will then establish a new connection to the remote site and return the response to browser. The squid was put in place to allow, control and monitor all regular web traffic such as HTTP, FTP, Telnet, email, etc. that goes through it. The proxy server, also a web caching proxy server will act as a web caching agent to cache frequently-requested web pages onto its internal memory and make them available to users upon request. By this, the proxy server need not reach out to remote servers to fetch responses anytime a request is made, thereby optimizing webpage delivery to the end user. A client whose browser software is not configured to point to the squid proxy server will be denied access to the LAN indefinitely. Furthermore, the installation of the squidGuard on the firewall will considerably increase the productive use of the internet whiles cutting down on the use of the corporate resource unproductively on watching streaming live video feeds and chatting on Facebook during working hours. This will further safeguard the LAN from malware infections since most of these websites which contain pornography, gambling, anonymous proxy services, abusive contents, chat portals and inappropriate downloads from peer to peer networks will be completely blacklisted. This will go a long way to reduce bandwidth degradation and congestion on the LAN. Additionally, while it's nice to be able to control access to network resources with such great precision, it's fairly pointless to have this control if you don't know exactly what should be restricted. For instance, which websites, IP addresses or domains being accessed by your users? Who accesses them most frequently? At what time of the day are these being accessed? And so on.

Fortunately, with the introduction of the Squid Analysis Report Generator (SARG) on the firewall, the network administrators will be able to maintain thorough information on all that is happening on the network. The SARG will be used gather useful statistics from the network and generate friendly and convenient web-browsable reports that can be examined with any Web browser. This will help the network administrators to have an in depth understanding of user behaviors on the network and effectively define policies to manage and control their activities.

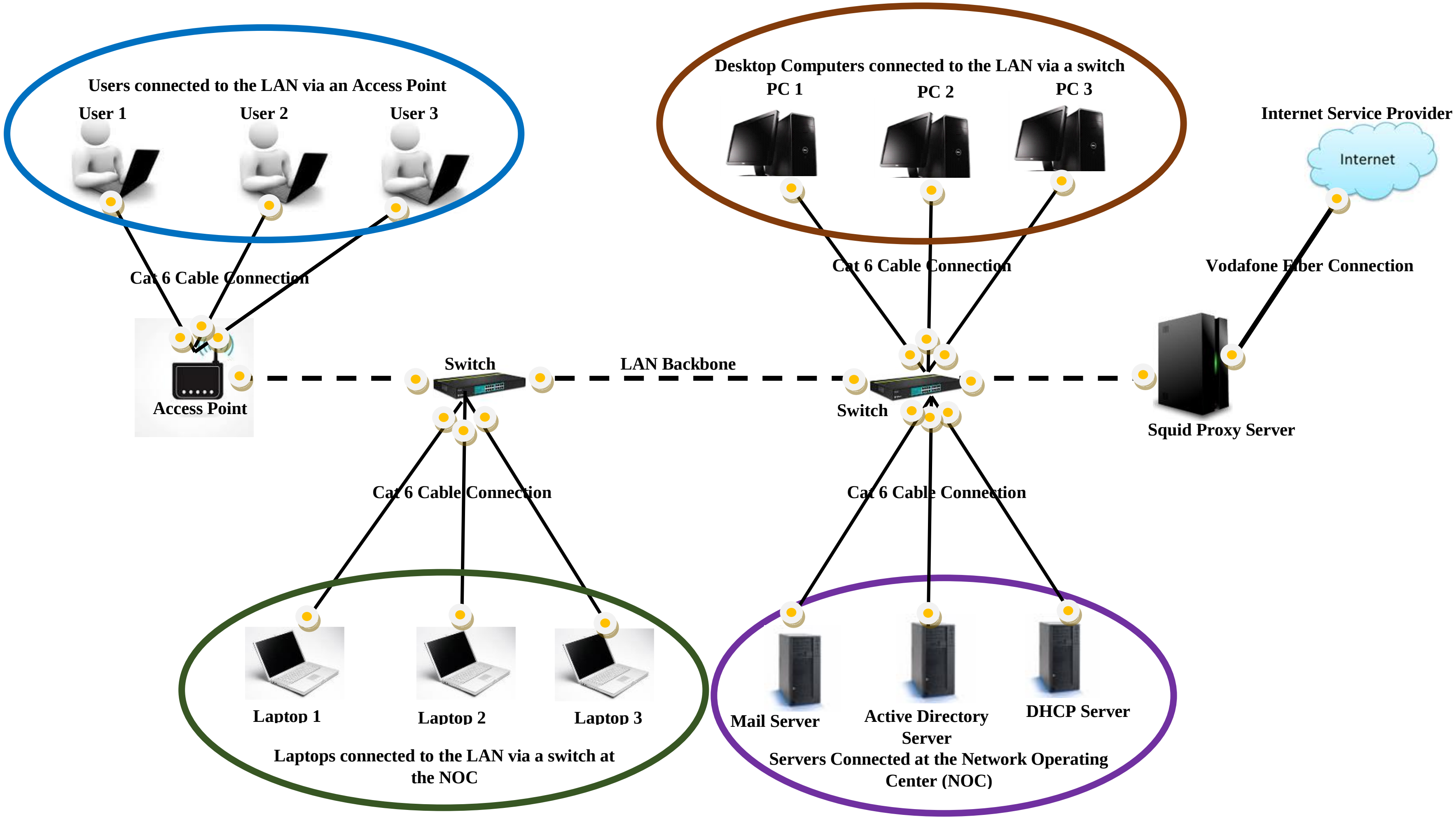

Users connected to the LAN via an Access Point
User 1
User 2
User 3
Desktop Computers connected to the LAN via a switch
PC 1
PC 2
PC 3
Internet Service Provider
Internet
Cat 6 Cable Connection
Cat 6 Cable Connection
Vodafone Fiber Connection
Switch
LAN Backbone
Access Point
Switch
Squid Proxy Server
Cat 6 Cable Connection
Cat 6 Cable Connection
Laptop 1
Laptop 2
Laptop 3
Mail Server
Active Directory Server
DHCP Server
Laptops connected to the LAN via a switch at the NOC
Servers Connected at the Network Operating Center (NOC)

Figure 4.16 A Simulated Instance of the Proposed UMaT LAN Architecture

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

a) From the research, it is concluded that, the UMaT LAN that existed before the installation of the Squid proxy server revealed two fundamental problems which are attributed to limited bandwidth and the lack of an effective user access control. The network administrators controlled the access and managed the security on LAN with per user authentication. However, this proved to be ineffective since illegitimate users after phishing out credentials of legitimate users gained unwarranted access and used the network on low priority bandwidth hungry applications which usually left the network hopelessly bogged down to the point where legitimate users were denied access to this valuable resource. The uncontrolled use further worsened the efficiency of the LAN, thus, making it susceptible to abuse by network users and also prone to virus attack.

b) After the installation of squid proxy server with the introduction of the squidGuard and SARG, the current UMaT LAN has eradicated the above stated problems and the following enhancements has been made:

    i. The successful installation of the squid with the introduction of the squidGuard and SARG has provided a centralized way of defining user access protocols/policies to monitor, analyze and limit internet use as needed to ensure that problematic or high-bandwidth consuming websites and applications are monitored, whitelisted or completely blocked off.

ii. Users on the LAN are efficiently managed and categorized into various user groups with the setting up of the Active Directory server.

iii. The introduction of the squidGuard efficiently assisted network administrators to manage and control access to web contents and further monitor activities and behavior patterns of users on the network.

5.2 Recommendations

The following recommendations are made:

a) The University must put in place an ICT policy which will provide detailed guidelines on network user access and usage. The policy must be used to determine and govern issues such as:

   i. Using the LAN for the core purpose for which it was put in place;

   ii. Monitoring the internet usage patterns and enforcing the appropriate sanctions where necessary;

   iii. Downloading and installation of internet enhancing or bandwidth hungry software; and

   iv. Protecting all campus computers connected to the LAN from virus and spam attacks.

b) The entire University community must be encouraged to use its domain email addresses (i.e.sakpah@umat.edu.gh) as their primary email service as compared to other email services such as yahoo.com, hotmail.com, inbox.com, iCloud mail, just to mention a few which consumes greater portions of the University bandwidth due to the numerous multimedia adverts they display.

c) Also the University must consider increasing the current bandwidth capacity from 45MB to at least 80 MB due to the annual increase in student enrollment. This will go a long way to reduce the burden on the existing bandwidth.

d) To further enhance the efficient use and management of the security of the LAN, the University must endeavour to introduce internet awareness education programmes which should address issues such as:

   i. Encouraging positive behaviour from users on the internet;

   ii. Encouraging appropriate use and the importance of using antivirus software at all times; and

   iii. Providing training to users as to how to effectively use the internet and conserve bandwidth.

REFERENCES

Abhimanyu K. V. (2012), Basics Of Data Communication: Part 7, Available at http://*www.itorian.com/search/label/Data%20Communication*, Accessed September 7, 2014.

Albuquerque, N. M. and Congdon P. (2000), "IEEE 802.1X Overview", Port Based Network Access Control, Available at http://*www.ieee802.org/1/files/public-/doc2000/P8021XOverview.PDF*, Accessed November 11, 2014.

Anon. (1990), Active Directory, Available at http*://en.wikipedia.org/wiki-/Active_Directory*, Accessed May 20, 2015.

Anon. (1999a), Ethernet Technologies, Available at *http://www.cisco.com/univercd-/cc/td/doc/cisintwk/ito_doc/ethernet.htm*, Accessed October 17, 2014.

Anon. (1999b), "Computer Networking", Available at https:*//www.scribd.com/doc-/31249931/Computer-Networking,* Accessed April 20, 2015.

Anon. (1999c), "Computer Networking", Available at https:*//www.scribd.com/doc-/31249931/Computer-Networking,* Accessed April 20, 2015.

Anon. (1999d), "Computer Networking", Available at https:*//www.scribd.com/doc-/31249931/Computer-Networking,* Accessed April 20, 2015.

Anon. (1999e), "Computer Networking", Available at https:*//www.scribd.com/doc-/31249931/Computer-Networking,* Accessed April 20, 2015.

Anon. (2000), "Carrier Sense Multiple Access with Collision Detection (CSMA/CD) on Access Method and Physical Layer Specifications", Available at http*://ieeexplore.ieee.org/xpl-/articleDetails.jsp?-arnumber=879000,* Accessed January 17, 2015.

Anon. (2004), “Computer Networking”, Available at https*://www.scribd.com/doc-/31249931/Computer-Networking,* Accessed April 20, 2015.

Anon. (2004), pfSense Installation, Available at https*://doc.pfsense.org/-index.php/Installing_pfSense*, Accessed March 5, 2015.

Baldwin, R. W. (1990), “Role-Based Access Control”, *Proc. of the 15th National Computer Security Conference,* pp. 554 – 563.

Bell, D. and LaPadula, L. (1973), “Secure Computer Systems: MTR 2547, MITRE”, *Journal of Computer Security*, Vol. 4(2), pp. 239-263.

Biba, K. J. (1977), “Integrity Considerations for Secure Computer Systems, Technical report*”, ACM SIGOPS Operating Systems Review 38(1),* pp. 12-23.

Cao, F. and Malik, S. (2005), “Security Analysis and Solutions for Deploying IP Telephony in the Critical Infrastructure”, *Proc. of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Network,* pp. 171-180.

Fairhurst, G. (2001a), “OSI Reference Model”, Available at http*://www.erg.abdn-.ac.uk/users/gorry/course/intro-pages/osi.html,* Accessed November 5, 2014.

Fairhurst, G. (2001b), “CSMA/CD”, Available at http*://www.erg.abdn.ac.uk-/users/gorry/course/lan-pages/csma-cd.html,* Accessed November 6, 2014.

Fairhurst, G. (2001c), “Network Interface Card”, Available at http*://www.erg.abdn-.ac.uk/users/gorry/course/lan-pages/nic.html*, Accessed November 6, 2014.

Fairhurst, G. (2001d), Medium Access Control, Available at http:/*/www.erg.abdn-.ac.uk/users/gorry/course/lan-pages/mac.html,* Accessed November 6, 2014.

Graham, G. S. and Denning, P. J. (1972), “Protection - Principles and Practice, Managing Requirements Knowledge”, *Proc. of the Spring Joint Computer Conference*, 417 pp.

Haland L. E. (1998), pfSense - Squid + Squidguard / Traffic Shapping Tutorial, Available at *https://www.howtoforge.com/pfsense-squid-squidguard-traffic-shaping-tutorial,* Accessed April 17, 2015.

Kaplan, H. and Noseworthy, B. (2000), “The Ethernet Evolution”, PowerPoint Presentation presented at the Interop Atlanta 2000 Workshop W924, Available at http:*//www.iol.unh.edu/training/ge/ethernet_evolution_index.html,* Accessed November 3, 2014.

Lampson, B. W. (1974), “On Protection in Operating Systems”, *SIGOPS Oper. Syst. Review*, Vol. 8(1), pp.18–24.

Lee, I. (2010), “A Novel Design and Implementation of DoS-Resistant Authentication and Seamless Handoff Scheme for Enterprise WLANs,” University of Canterbury, Available at http:*//hdl.handle.net/10092/5076*, Accessed January 13, 2015.

Linfo, A. (2007), "Proprietary Software is Opposite of Free Software", Available at http:*//www.linfo.org,* Accessed October 13, 2015

Memon, A. Q., Raza, A. H. and Iqbal, S. (2010) “WLAN Security”, Halmstad University Technical Report IDE 1013, Available at http:*//www.diva-portal.org/smash/get/diva2:317911/fulltext01*, Accessed January 20, 2015.

Nidal, A., Mohamed, T. R., Mohamed, E., Dasilva, L. A. and Jean-Jacques Q. (2005), “Authentication protocols for ad hoc networks: taxonomy and research issues”, *Proc. of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks,* Montreal, Canada, pp. 96-104.

Nguyen The Anh and Shorey, R. (2005) “Network sniffing tool for WLANs: Merits and Limitations”, IEEE Computer Society, Available at https*://www.scribd-.com/doc/53470470/arshad-3,* Accessed Retrieved January 13, 2015.

Patrick, C. K. and Vargas, M. (2006), “Security Issues in VOIP Applications”, *Proc. of the IASTED European Conference: Internet and Multimedia Systems and Applications*, pp. 254-259.

Pidgeon, N. (2001a), “CSMA/CD”, Available at http:/*/www.howstuffworks.com-/ethernet3.htm,* Accessed October 17, 2014.

Pidgeon, N. (2001b), “Ethernet Today”, Available at http*://www.howstuffworks.com-/ethernet7.htm,* Accessed October 18, 2014.

Pidgeon, N. (2001c), Limitations of Ethernet, Available at http*://www.howstuff-works.com/ethernet4.htm,* Accessed October 18, 2014.

Ravi S. (2015), Squid Analysis Report Generator and Internet Bandwidth Monitoring Tool, Available at http*://www.tecmint.com/sarg-squid-analysis-report-generator-and-internet-bandwidth-monitoring-tool,* Accessed March 7, 2015.

Rigney, S. W. C. (2000), "Remote Authentication Dial In User Services (RADIUS), RFC 2865". Available at https*://www.ietf.org/rfc/rfc2865.txt,* Accessed February 7, 2015.

Samarati, P and Vimercati, D. C. D. (2001), “Access Control: Policies, Models, and mechanisms”, *Revised versions of lectures given during the IFIP WG 1.7*

International School on Foundations of Security Analysis and Design (Tutorial Lectures, 2171), London, UK: Springer-Verlag, pp. 137–196.

Simmonds, A., Sandilands, P., and Van Ekert, L. (2004), “An Ontology for Network Security Attacks”, *Proc. of the 2nd Asian Applied Computing Conference (AACC), Lecture Notes in Computer Science,* Kathmandu, Nepal: Springer Berlin, Vol. 3285, pp. 317-323.

Slone, J. (1998), “Handbook of Local Area Networks”, *Boca Raton Auerbach*, Available at http*://rionhollenbeck.com/GradPortfolio/Papers/620-Ethernet/Ethernet.pdf,* Accessed January 5, 2014.

Spurgeon, C. (1995a), “Collisions”, Available at http*://www.ots.utexas.edu/ethernet-/ethernet/100quickref/ch1qr_8.html,* Accessed October 18, 2014.

Spurgeon, C. (1995b), “Network Medium”, Available at http*://www.ots.utexas-.edu/ethernet/ethernet/10quickref/ch5qr_4.html,* Accessed October 19, 2014.

St. Laurent, Andrew M. (2008), "Understanding Open Source and Free Software Licensing", *O'Reilly Media, p. 4. ISBN 9780596553951.*

APPENDIX

FILTER CONFIG FILE

```
#
=========================================================================
# SquidGuard configuration file
# This file generated automatically with SquidGuard configurator
# (C)2006 Serg Dvoriancev
# email: dv_serg@mail.ru
#
=========================================================================
logdir /var/squidGuard/log
dbhome /var/db/squidGuard
ldapbinddn cn=Administrator,cn=Users,dc=umat,dc=edu,dc=local
ldapbindpass Ponkor123
ldapprotover 3
# StudentACL
time StudentACL {
        weekly mon 08:00-16:59
        weekly tue 08:00-16:59
        weekly wed 08:00-16:59
        weekly thu 06:00-16:59
        weekly fri 08:00-16:59
}
#
src UGGroupACL {
        ldapusersearch ldap://192.168.1.1/DC=umat,DC=edu,DC=local?sAMAccountName?sub?(&(sAMAccountName=%s)(memberOf=CN=Undergraduate%2cCN=Users%2cDC=umat%2cDC=edu%2cDC=local))
        log block.log
}
#
dest blk_BL_adv {
        domainlist blk_BL_adv/domains
        urllist blk_BL_adv/urls
        redirect http://192.168.1.3:80/sgerror.php?url=blank_img&msg=&a=%a&n=%n&i=%i&s=%s&t=%t&u=%u
        log block.log
}
#
dest blk_BL_dating {
        domainlist blk_BL_dating/domains
        urllist blk_BL_dating/urls
        log block.log
}
#
dest blk_BL_downloads {
        domainlist blk_BL_downloads/domains
        urllist blk_BL_downloads/urls
        log block.log
}
#
dest blk_BL_hacking {
        domainlist blk_BL_hacking/domains
        urllist blk_BL_hacking/urls
        log block.log
}
#
dest blk_BL_porn {
        domainlist blk_BL_porn/domains
        urllist blk_BL_porn/urls
        log block.log
}
#
dest blk_BL_webtv {
        domainlist blk_BL_webtv/domains
        urllist blk_BL_webtv/urls
        log block.log
}
rew safesearch {
        s@(google..*/search?.*q=.*)@&safe=active@i
        s@(google..*/images.*q=.*)@&safe=active@i
        s@(google..*/groups.*q=.*)@&safe=active@i
        s@(google..*/news.*q=.*)@&safe=active@i
        s@(yandex..*/yandsearch?.*text=.*)@&fyandex=1@i
        s@(search.yahoo..*/search.*p=.*)@&vm=r&v=1@i
        s@(search.live..*/.*q=.*)@&adlt=strict@i
        s@(search.msn..*/.*q=.*)@&adlt=strict@i
        s@(.bing..*/.*q=.*)@&adlt=strict@i
        log block.log
}
#
acl  {
        #
        UGGroupACL  within StudentACL {
                pass !blk_BL_adv !blk_BL_anonvpn !blk_BL_downloads !blk_BL_hacking !blk_BL_movies !blk_BL_porn !blk_BL_sex_education !blk_BL_sex_lingerie !blk_BL_socialnet !blk_BL_spyware !blk_BL_tracker !blk_BL_warez all
                redirect http://www.umat.edu.gh
                rewrite safesearch
                log block.log
                } else {
                pass !blk_BL_adv !blk_BL_anonvpn !blk_BL_porn all
                redirect http://www.umat.edu.gh
                rewrite safesearch
                log block.log
        }
        #
        default  {
                pass all
                redirect http://192.168.1.3:80/sgerror.php?url=blank&msg=&a=%a&n=%n&i=%i&s=%s&t=%t&u=%u
                rewrite safesearch
                log block.log
        }
}
```

PROXY CONFIG FILE

```
# Do not edit manually!
http_port 192.168.1.3:8080
icp_port 0
pid_filename /var/run/squid.pid
cache_effective_user proxy
cache_effective_group proxy
error_directory /usr/pbi/squid-i386/etc/squid/errors/English
icon_directory /usr/pbi/squid-i386/etc/squid/icons
visible_hostname UMaT Proxy Server
cache_mgr admin@localhost
access_log /var/squid/logs/access.log
cache_log /var/squid/logs/cache.log
cache_store_log none
logfile_rotate 7
shutdown_lifetime 3 seconds
# Allow local network(s) on interface(s)
acl localnet src  192.168.1.0/255.255.255.0
httpd_suppress_version_string on
uri_whitespace strip
cache_mem 8 MB
maximum_object_size_in_memory 32 KB
```

```
memory_replacement_policy heap GDSF
cache_replacement_policy heap LFUDA
cache_dir ufs /var/squid/cache 30000 16 256
minimum_object_size 0 KB
maximum_object_size 4 KB
offline_mode off
cache_swap_low 90
cache_swap_high 95
# No redirector configured
# Setup some default acls
acl all src 0.0.0.0/0.0.0.0
acl localhost src 127.0.0.1/255.255.255.255
acl safeports port 21 70 80 210 280 443 488 563 591 631 777 901 23789 3128 1025-65535
acl sslports port 443 563 23789
acl manager proto cache_object
acl purge method PURGE
acl connect method CONNECT
acl dynamic urlpath_regex cgi-bin ?
cache deny dynamic
http_access allow manager localhost
http_access deny manager
http_access allow purge localhost
http_access deny purge
http_access deny !safeports
http_access deny CONNECT !sslports
# Always allow localhost connections
http_access allow localhost
quick_abort_min 0 KB
quick_abort_max 0 KB
request_body_max_size 100000 KB
reply_body_max_size 512000000 deny all
```

```
delay_pools 1
delay_class 1 2
delay_parameters 1 102400/102400 -1/-1
delay_initial_bucket_level 100
# Throttle extensions matched in the url
acl throttle_exts urlpath_regex -i '/var/squid/acl/throttle_exts.acl'
delay_access 1 allow throttle_exts
delay_access 1 deny all
# Custom options
redirect_program /usr/pbi/squidguard-i386/bin/squidGuard -c /usr/pbi/squidguard-i386/etc/squidGuard/squidGuard.conf
redirector_bypass off
url_rewrite_children 5
auth_param basic program /usr/pbi/squid-i386/libexec/squid/squid_ldap_auth -v 3 -b dc=umat,dc=edu,dc=local -D cn=Administrator,cn=Users,dc=umat,dc=edu,dc=local -w Ponkor123 -f '(sAMAccountName=%s)' -u uid -P 192.168.1.1:389
auth_param basic children 5
auth_param basic realm Please enter your credentials to access the proxy
auth_param basic credentialsttl 60 minutes
acl password proxy_auth REQUIRED
http_access allow password localnet
# Default block all to be sure
http_access deny all
```