Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 6 – No.1, October 2016 – www.caeaccess.org

An Improved Computer Network Access Control using Free BSD PFSENSE: A Case Study of UMaT Local Area Network

Akpah Sylvester
University of Mines and Technology
Tarkwa, Ghana

Michael Asante
Department of Computer Science
Kwame Nkrumah University of Science and Technology,
Kumasi, Ghana

Frimpong Twum
Department of Computer Science
Kwame Nkrumah University of Science and Technology,
Kumasi, Ghana

ABSTRACT
Universities in Ghana to which UMaT is no exception are under constant pressure to provide their communities with reliable internet access. As internet connectivity is increasingly becoming a strategic resource, having a robust campus network with good connectivity to the internet is no longer a luxury, but in actual sense now a basic necessity. UMaT has a robust LAN infrastructure which faces some challenges attributable to limited bandwidth of 45 MB, misuse of the bandwidth on low priority bandwidth hungry applications, and lack of effective user access control. This research aimed at studying the behavior patterns of network users and deploy an enhanced network access control using freeBSD pfSense open source software as the dedicated perimeter firewall with the introduction of squid, squidGuard, Squid Analysis Report Generator (SARG) and the setting up of an Active Directory server with user access policies to improve user access control and insulate the LAN from misuse and virus attacks.

General Terms
Network Security; Network Access Control (NAC); Access Control Models; Firewalls; NAC Architecture

Keywords
Bandwidth; freeBSD; pfSense; Squid; squidGuard; Squid Analysis Report Generator (SARG); Graphical User Interface.

1. INTRODUCTION
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. In line with one of its major action plans, UMaT has put in place a Local Area Network (LAN) infrastructure whose primary purpose is to facilitate research and teaching and learning. The network however is faced with challenges including limited bandwidth and lack of effective user access control. The problem of limited bandwidth is attributed to the universities annual increment in student enrolment, the increasing use of electronic devices and gadgets and the shifting patterns of internet access and usage. A plausible approach to address the problem of limited bandwidth is to increase the current internet capacity by purchasing additional bandwidth. This solution though viable is expensive due to the high cost associated with acquiring dedicated bandwidth in Ghana. This problem of limited bandwidth is further exacerbated by the lack of an effective user access control which enables the unwarranted misuse of bandwidth by LAN users. For example, users use the network for accessing and downloading bandwidth-hungry applications which consumes network resources to a point where users are denied access to business critical applications. This paper therefore is aimed at deploying an enhanced network access control system to assist network administrators to efficiently control access and manage the security of a LAN.

2. LITERATURE REVIEW
This section focuses greatly on reviewing the current literature relevant to this research. The areas reviewed include Local Area Network (LAN), Firewall Types, LAN standards, LAN security, Network Access Control (NAC), Access Control Models and previous related works.

2.1 Local Area Network
According to Abhimanyu [1], 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. It offers users many benefits, including shared access to devices and applications, file exchange between connected users, easy communication among users, and etc. LAN typically relies on traditional wired structures as its main transmission medium. The most widespread of LAN technology is the Ethernet, which enables the transmission of data frames across baseband cables using Carrier Sense Multiple Access/Collision Detection (CSMA/CD) 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 to the ease of setup, central management, possibility to upgrade or expand with little difficulty, better performance and many others. In spite of its lasting existence, security issues such as porous network perimeters, improperly configured firewalls, network authenticating issues and un-auditable networks proves to be major drawbacks to LAN technologies.

2.2 Attacks on LAN
According to Memon et al. [2], LAN attacks primarily focus on the security issues encountered during the transmission of data between users. Some of the common types of LAN attacks include: IP Address Spoofing, Man-in-the-Middle (MiTM), Spam Attacks, Conversation Sniffing Attacks and many others. These expose the network to eavesdropping and

jamming. As a result, strategies need to be developed to mitigate these security risks.

2.3 Network Security

According to Simmonds et. al., [3], network security is focused on the provision of policies adopted by network administrators to monitor and prevent unauthorized access, misuse, modification, or Denial of Service (DoS) to network-accessible resources. Several security strategies have been adopted to prevent unauthorized access by intruders. This includes Firewalls, Intrusion Detection Systems (IDSs), Intrusion Prevention Systems (IPSs), Network Address Translators (NATs), Virtual Private Networks (VPNs), Network Access Control, and etc. This research focuses on using Firewalls and Network Access Control (NAC).

2.3.1 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 a firewall is to protect a private network from non-legitimate traffic by monitoring all traffic leaving or coming into a private network. According to Chapman et. al., [4], a firewall is the most effective way to connect a network to the Internet and still protect that network. There are various types of firewalls, some of which are Wireshark, IPFire, IPCop, Smoothwall, Fedora, etc. Any of these helps in protecting the network by implementing larger security policies that define permitted accesses and services.

2.3.2 Network Access Control

According to Cheswick [5], Network Access Control is concerned with regulating access to protected resources in a network environment that complies with pre-defined security procedures. Generally, NAC deals with two levels of protection:

a) **Host-Based security:** protects the safety of a single client workstation that is connected to a network, and

b) **Perimeter-Based security** protects a cluster of client workstations making up a network.

2.3.2.1 Components of NAC Architecture

According to Naveen et. al [6], NAC architecture is made up of the following components: Endpoint (Agent-based Endpoint and Agentless Endpoint), Enforcement Points, Policy Servers Quarantine Server and Remediation Servers. Figure 1 describes the individual components that make up the NAC Architecture.

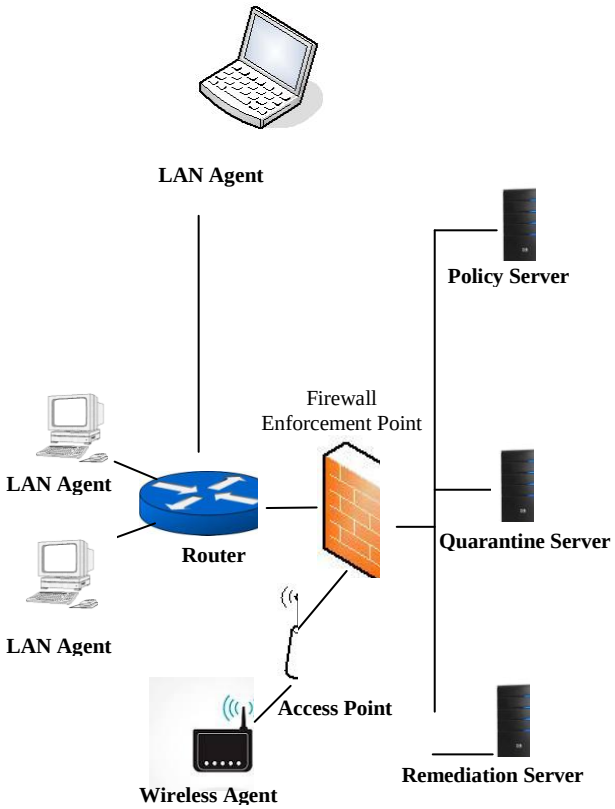

Figure 1: NAC Architecture. Source: Naveen et al [6]

Endpoint - An endpoint is a client computer that requests access to network resources from a server computer e.g. LAN agent as in Figure 1.

Enforcement Point - An enforcement point is an integral part of the NAC architecture that communicates and gains absolute control of host computers before allowing them access to a protected network environment.

Policy Server - A policy server is a security component of the NAC architecture which is directly involved in defining, administering and enforcing organization-wide network access control rules and regulations.

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.

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.

2.4 Access Control Models

According to Samarati and Vimercati [7], Access Control Model is the fundamental security backbone for managing network services by presenting a formal description of a security policy and its functionalities. It serves as the foundation for regulating and managing access to network resources based on pre-defined security policies. 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) and these are described as follows;

Mandatory Access Control (MAC) grants access privileges to network resources based on pre-defined rules and

regulations delegated by a central authority. Views shared by Bell and LaPadula [8] and Biba [9], clearly state that authorization policies can be classified into secrecy-based mandatory policies and integrity-based mandatory policies.

Discretionary Access Control (DAC) Initially proposed by Lampson [10], and further formalized by Graham and Denning and Harrison [11], 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.

Role-Based Access Control (RBAC), Proposed by Baldwin [12], 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.

3. METHODOLOGY

3.1 Study Domain

The study was conducted at the University of Mines and Technology (UMaT) which is located on a 1.60 square-kilometers of undulating land at Tarkwa, 89 kilometers from Takoradi, the Western Regional capital of Ghana, West Africa. Currently UMaT has 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 and the Center for Communication and Entrepreneurship Skills (CENCES) which currently serves as the nucleus of the future Faculty of Integrated Management Sciences.

3.2 UMaT Network Infrastructure

The Local Area Network (LAN) infrastructure on UMaT campus which spans a maximum distance of approximately 1.39 square-kilometers was simulated with wireshark packet analyzing software to ascertain the behavior pattern of network users.

The LAN interconnects the universities 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.

The LAN backbone doubles as the main base station and associates with six (6) other base stations by way of linking the respective buildings. The Internet Service Provider (ISP) provides a point to point internet connection with download and upload bandwidth stream of 45 MB which is then connected by way of Cat 6 Ethernet cables to a Linux box which serves as a firewall and doubles as a proxy server. The LAN connects an Active Directory server, Mail server and Application server.

3.3 Tools Used for Performing Analysis on the UMaT LAN

To attain the goal of this thesis, freeBSD pfSense [13] open source software was installed to act as the dedicated perimeter firewall. This software was chosen because it can be installed and entirely managed from the GUI. In addition to being a firewall and a routing platform, pfSense includes a long list of other features and packages allowing its capabilities and functionalities to be further expanded. In this case three additional open source software packages were installed on the firewall.

Squid Proxy Server: This was installed to act as an intermediary to cache/store frequently requested webpage's temporarily and make them available to other users upon request. By this it reduces bandwidth congestion as it analyses all web traffic coming or leaving the network.

SquidGuard: The squidGuard, an open source software was installed to define multiple access rules with different levels of restrictions on web contents accessed by users. It was integrated into the working squid environment to implement blacklist rules and content control by defining sites for which access maybe redirected or restricted entirely.

Squid Analysis Report Generator (SARG): This an open source squid proxy log analysis tool which was installed to provide web based log file analysis and generate reports on how much bandwidth is consumed by users on the network and also provide detailed statistics on where and what the network users are doing on the network.

Active Directory Server (ADS): Active Directory [14] was installed on a windows server to define and categorize all users on the network into four user group namely undergraduate students, postgraduate students, staff and guests. The ADS database also held login credentials of all users.

4. FINDINGS AND DISCUSSION

The study revealed the following:

4.1 Results Attained from the Implementation of Squid Proxy Server

The results showed that browser software of all client machines which were configured to trust the proxy server were able to establish connection with the Internet. Software's configured improperly were however denied access as shown by figures 2 and 3.

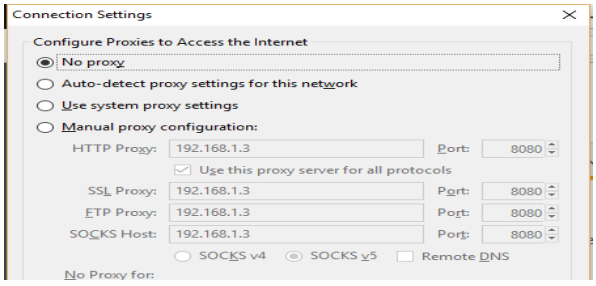

Figure 2: Proxy Settings Deactivated.

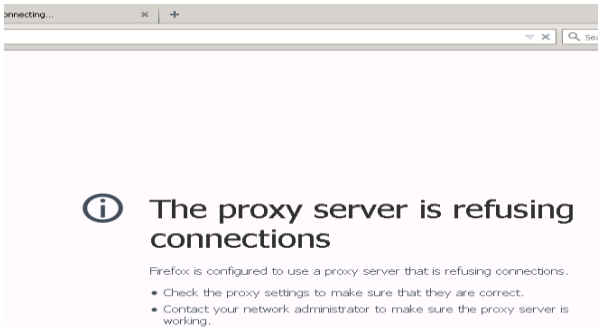

Figure 3: Proxy Server Refusing Connection to the Internet

4.2 squidGuard Implementation Results

The squidGuard deployed on the proxy server efficiently defined access control mechanisms over the network. Websites that were proven not to have an acceptable content were redirected to the University website homepage or completely blocked off. Time frames for which certain websites can be accessed were defined as shown by figure 4 and figure 5.

Figure 4: Pornographic website redirected to the University website

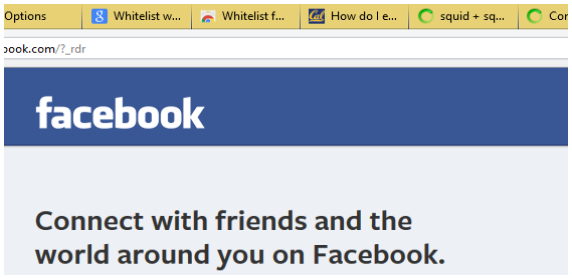

Figure 5: Student Gained Accessed to Facebook at 9:40pm

4.3 Results of Squid Analysis Report Generator (SARG)

The Squid Analysis Report Generator (SARG) deployed on the squid proxy efficiently analysed all web based log files and generated reports based on behaviour patterns of all users on the network. The SARG helped network administrators to have clear picture of the top users of the bandwidth, websites mostly accessed, number of times a particular website is accessed, amount of bandwidth consumed by a particular website, and etc. Figure 6 depicts results of the total amount of bandwidth consumed by the top users of the LAN between 25th February and 3rd March, 2015. Figure 7 shows the total individual bandwidth consumption rates of the top 19 users within one hour interval on 25th of May, 2015.

Squid User Access Report

FILE/PERIOD	CREATION DATE	USERS	BYTES
25Feb2015-03Mar2015	Tue Mar 3 20:39:05 2015	25	17,878,122,829
25Feb2015-01Mar2015	Sun Mar 1 22:00:31 2015	25	17,434,090,802
25Feb2015-28Feb2015	Sat Feb 28 01:09:58 2015	23	3,547,992,520
01Feb2015-31Feb2015	Sun Mar 1 00:00:01 2015	24	16,838,666,735
2015Feb25-2015Mar02	Mon Mar 2 22:57:55 2015	25	17,550,329,181
2015Feb25-2015Mar02.2	Mon Mar 2 21:06:46 2015	25	17,525,755,633
2015Feb25-2015Mar02.1	Mon Mar 2 20:59:41 2015	25	17,525,572,064

Figure 6: 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
1	192.168.0.63	62.98K	2.29G	10.39%	80.72%	19.28%	10:15:53
2	192.168.0.61	63.60K	1.98G	9.00%	79.36%	20.64%	05:07:48
3	192.168.0.51	56.08K	1.94G	8.80%	82.69%	17.31%	04:31:55
4	192.168.0.60	57.62K	1.91G	8.67%	78.39%	21.61%	09:17:22
5	192.168.0.53	54.43K	1.86G	8.44%	81.02%	18.98%	04:27:21
6	192.168.0.62	53.38K	1.66G	7.54%	77.22%	22.78%	04:38:46
7	192.168.0.50	51.24K	1.64G	7.46%	77.27%	22.73%	06:22:41
8	192.168.0.58	64.95K	1.49G	6.79%	58.05%	41.95%	05:21:51
9	192.168.0.64	40.23K	1.24G	5.66%	79.72%	20.28%	03:15:12
10	192.168.0.52	40.12K	1.21G	5.50%	77.82%	22.18%	03:41:46
11	192.168.0.59	64.93K	1.20G	5.45%	66.99%	33.01%	05:00:26
12	192.168.0.55	54.73K	970.83M	4.40%	70.90%	29.10%	04:31:38
13	192.168.0.57	46.92K	874.34M	3.96%	57.10%	42.90%	04:41:18
14	192.168.0.56	40.45K	852.87M	3.87%	78.26%	21.74%	03:48:01
15	192.168.0.54	19.26K	497.52M	2.26%	72.60%	27.40%	02:29:31
16	192.168.0.65	14.63K	386.71M	1.75%	71.85%	28.15%	06:43:16
17	192.168.0.46	475	17.43M	0.08%	0.00%	100.00%	00:03:47
18	192.168.1.9	2	7.35K	0.00%	0.00%	100.00%	00:01:14
19	192.168.1.13	2	251	0.00%	0.00%	100.00%	00:00:01
	TOTAL	786.10K	22.06G		75.70%	24.30%	84:19:55
	AVERAGE	41.37K	1.16G				04:26:18

Figure 7: Access Logs Depicting Top Users of the Bandwidth

5. CONCLUSIONS

Prior to installation of the Squid proxy server for this study, UMaT's computer network was observed to be facing challenges attributed to two fundamental problems as limited bandwidth and lack of an effective user access control which left the network susceptible to abuse by users and also made the network vulnerable to attack as DoS/DDoS attack, Virus, Worms, Trojans attack, and etc. After the installation of squid proxy server and the additional software packages, the problems were eradicated and the network was enhanced as follows:

i. The squid with the introduction of the squidGuard and SARG provided a centralized way of defining user access 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.

5.1 Recommendations

i. The University must put in place an ICT policy which will provide detailed guidelines on network user access and usage.

ii. The University must consider increasing the current bandwidth capacity from 45MB to at least 80 MB.

iii. The University must endeavour to introduce internet awareness education programmes which encourages positive behaviour from users on the internet.

iv. The University community must be encouraged to use its domain email addresses e.g., (sakpah@umat.edu.gh) as their primary email service rather than using public email client services as Yahoo, Gmail, Hotmail, and etc.

6. ACKNOWLEDGMENTS

Foremost appreciation goes to the Almighty God, the creator of Heaven and Earth for the knowledge bestowed upon us the grace to finish this work. Thanks goes to Dr. M. Asante for his guidance, contributions, encouragement.

7. REFERENCES

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

[2] 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.

[3] 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.

[4] Chapman, D. Brent, Zwicky, Elizabeth D. (1995), *Building Internet Firewalls*, (O'RIELLY), ISBN 1-56592-124-0, First Edition, November 1995.

[5] Cheswick, W. R., Bollovin, S. M. and Rubin, A. D. (2003). Firewalls and Internet Security: repelling the wily hacker. *2nd edition. Boston: Addison-Wesley Longman Publishing Co., Inc.*.

[6] Naveen, S. (2007), Network Access Control (NAC) CISSP. Available at http://*www.helpnetsecurity.com/2007/11/26/network-access-control-nac*, Accessed May 8, 2015

[7] 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.

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

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

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

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

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

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

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